Heritage of European Mathematics

Andrzej Schinzel

Selecta

Volumes I + II

European Mathematical Society

Heritage of European Mathematics

Andrzej Schinzel in Cambridge (England), 1961

Andrzej Schinzel

Selecta

Volume I

Diophantine Problems and Polynomials

Edited by
Henryk Iwaniec
Władysław Narkiewicz
Jerzy Urbanowicz

European Mathematical Society

Author:

Andrzej Schinzel
Institute of Mathematics
Polish Academy of Sciences
ul. Śniadeckich 8, skr. poczt. 21
00-956 Warszawa 10
Poland

Editors:

Henryk Iwaniec
Department of Mathematics
Rutgers University
New Brunswick, NJ 08903
U.S.A.
iwaniec@math.rutgers.edu

Władysław Narkiewicz
Institute of Mathematics
University of Wrocław
pl. Grunwaldzki 2/4
50-384 Wrocław
Poland
narkiew@math.uni.wroc.pl

Jerzy Urbanowicz
Institute of Mathematics
Polish Academy of Sciences
ul. Śniadeckich 8, skr. poczt. 21
00-956 Warszawa 10
Poland
urbanowi@impan.gov.pl

2000 Mathematics Subject Classification: 11, 12

ISBN 978-3-03719-038-8 (Set Vol I & Vol II)

The Swiss National Library lists this publication in The Swiss Book, the Swiss national bibliography, and the detailed bibliographic data are available on the Internet at http://www.helveticat.ch.

Contact address:

European Mathematical Society Publishing House
Seminar for Applied Mathematics
ETH-Zentrum FLI C4
CH-8092 Zürich
Switzerland

Phone: +41 (0)44 632 34 36
Email: info@ems-ph.org
Homepage: www.ems-ph.org

Printed in Germany

9 8 7 6 5 4 3 2 1

Preface

Andrzej Bobola Maria Schinzel, born on April 5, 1937 at Sandomierz (Poland), is well known for his original results in various areas of number theory appearing in over 200 research papers, of which the first thirty were published while he was an undergraduate at the Warsaw University. Working under the guidance of Wacław Sierpiński, he became interested in elementary number theory, and the subjects of his early papers range from properties of arithmetical functions, like Euler's φ-function or the number of divisors, to Diophantine equations. Paul Erdős, a big champion of elementary number theory, wrote in his letter to Sierpiński of October 23, 1960—when Andrzej was studying at the University of Cambridge under the supervision of Harold Davenport—*"Schinzel's completion of my proof is much simpler than anything I had in mind"*. Many mathematicians cooperating with Andrzej Schinzel could repeat the words of Erdős.

Since completing his studies at Warsaw University in 1958, Andrzej Schinzel has been employed by the Institute of Mathematics of the Polish Academy of Sciences, where he obtained his Ph.D. in 1960. On his return from a Rockefeller Foundation Fellowship at the University of Cambridge and the University of Uppsala (where he studied under Trygve Nagell) he completed his *habilitation* in 1962. In 1967 he was promoted to Associate Professor, and in 1974 to Full Professor. In 1979 he was elected to Corresponding Member of the Polish Academy of Sciences and in 1994 to Full Member.

Andrzej Schinzel's very first paper ([1])—published at the age of 17—is a postscript to a result of H.-E. Richert who proved a general theorem about partitions of integers into distinct summands from a given set which implied in particular that every integer > 33 is a sum of distinct triangular numbers. Schinzel observed that every integer > 51 is a sum of at most four distinct triangular numbers. The favorite subject of the early research of Schinzel, Euler's totient function, is considered here in five papers; the earliest one, published in 1954, is not included ([2]). In 1958 a joint work **J1** with Sierpiński appeared, analyzing various consequences of the conjecture stating that if $f_1, \dots, f_s \in \mathbb{Z}[x]$ are irreducible polynomials having positive leading coefficients and there is no natural number > 1 that is a divisor of each of the numbers $f_1(n) \cdots f_s(n)$ for n being an integer then for infinitely many natural n the values $f_1(n), \dots, f_s(n)$ are primes. This celebrated conjecture—with many unexpected consequences—is called *"Schinzel's Hypothesis H"*.

Schinzel's doctoral thesis **B1** dealt with the period of a class of continued fractions and was related (see **B2**) to a question concerning pseudo-elliptic integrals, considered already

([1]) *Sur la décomposition des nombres naturels en sommes de nombres triangulaires distincts*, Bull. Acad. Polon. Sci. Cl. III 2 (1954), 409–410.

([2]) *Sur quelques propriétés des fonctions $\varphi(n)$ et $\sigma(n)$*, Bull. Acad. Polon. Sci. Cl. III 2 (1954), 463–466 (with W. Sierpiński).

by N. H. Abel in the very first volume of Crelle's Journal. In his habilitation thesis—consisting of four papers **I1**, **I2**, **I3** and a paper not included ([3])—Schinzel generalized a classical theorem of Zsigmondy of 1892 (often called the Birkhoff–Vandiver theorem) on primitive divisors.

The central theme of Schinzel's work is arithmetical and algebraic properties of polynomials in one or several variables, in particular questions of irreducibility and zeros of polynomials. To this topic he devoted about one-third of his papers and two books ([4]). In the books Schinzel presented several classical results and included many extensions, improvements and generalizations of his own.

Undoubtedly Schinzel and his beloved journal *Acta Arithmetica* influenced many mathematicians, stimulating their thinking and mathematical careers. Andrzej Schinzel has since 1969 been the editor of this first international journal devoted exclusively to number theory, being a successor of his teacher W. Sierpiński. Among the other editors of Acta Arithmetica during these years were/are J. W. S. Cassels, H. Davenport, P. Erdős, V. Jarník, J. Kaczorowski, Yu. V. Linnik, L. J. Mordell, W. M. Schmidt, V. G. Sprindzhuk, R. Tijdeman and P. Turán. These people and the other outstanding mathematicians from the advisory board of Acta Arithmetica have determined the line of the journal.

Andrzej Schinzel's work has been influential in the development of many areas of mathematics, and his 70th birthday gives us an opportunity to honor his accomplishments by putting together his most important papers. This selection of Schinzel's papers—published during more than five decades—is divided into two volumes containing 100 articles. We have asked some outstanding mathematicians for commentaries to the selected papers. Also included is a list of unsolved problems and unproved conjectures proposed by Schinzel in the years 1956–2006, arranged chronologically. The first volume covers six themes:

A. Diophantine equations and integral forms (with commentaries by Robert Tijdeman)
B. Continued fractions (with commentaries by Eugène Dubois)
C. Algebraic number theory (with commentaries by David W. Boyd and Donald J. Lewis)
D. Polynomials in one variable (with commentaries by Michael Filaseta)
E. Polynomials in several variables (with commentaries by Umberto Zannier)
F. Hilbert's Irreducibility Theorem (with commentaries by Umberto Zannier)

The second volume contains papers covering seven themes:

G. Arithmetic functions (with commentaries by Kevin Ford)
H. Divisibility and congruences (with commentaries by Hendrik W. Lenstra, Jr.)
I. Primitive divisors (with commentaries by Cameron L. Stewart)
J. Prime numbers (with commentaries by Jerzy Kaczorowski)
K. Analytic number theory (with commentaries by Jerzy Kaczorowski)
L. Geometry of numbers (with commentaries by Wolfgang M. Schmidt)
M. Other papers (with commentaries by Stanisław Kwapień and Endre Szemerédi)

([3]) *The intrinsic divisors of Lehmer numbers in the case of negative discriminant*, Ark. Mat. 4 (1962), 413–416.

([4]) *Selected Topics on Polynomials*, XXII+250 pp., University of Michigan Press, Ann Arbor 1982, and *Polynomials with Special Regard to Reducibility*, X+558 pp., Encyclopaedia of Mathematics and its Applications 77, Cambridge Univ. Press, Cambridge 2000.

Many people helped with the editing of the volumes. First of all, we gratefully thank the authors of the commentaries we had the pleasure to work with. Second, our special thanks go to Stanisław Janeczko, Director of the Institute of Mathematics, Polish Academy of Sciences, for his support, and to Manfred Karbe, Publishing Director of the European Mathematical Society Publishing House, for his invaluable assistance during the work on the Selecta. Third, we wish to thank Jerzy Browkin for reading the papers and some corrections, and Jan K. Kowalski for retyping the papers and offering valuable suggestions for improving the presentation of the material. Finally, we wish to express our gratitude to the staff of the European Mathematical Society Publishing House, especially to Irene Zimmermann, for the very pleasant cooperation.

We have decided to unify some notations, using the "blackboard bold" type for most common sets; so $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Q}_p$ and $\mathbb{F}_p$ always stand for the complex, real, rational, p-adic and finite fields respectively; $\mathbb{Z}$, $\mathbb{Z}_p$ for the rings of integers and p-adic integers; and $\mathbb{N}$, $\mathbb{N}_0$ for the sets of positive and nonnegative integers. The greatest common divisor of integers $a_1, a_2, \dots, a_n$ is denoted by $(a_1, a_2, \dots, a_n)$. If $(a_1, a_2, \dots, a_n) = 1$, the integers are called relatively prime, and if $(a_i, a_j) = 1$ for any $1 \leqslant i \neq j \leqslant n$, the integers are called coprime. As usual, for $x \in \mathbb{R}$ set $[x] = \max\{n \in \mathbb{Z} : n \leqslant x\}$, $\lceil x \rceil = \min\{n \in \mathbb{Z} : x \leqslant n\}$ and $\|x\| = \min\{x - [x], \lceil x \rceil - x\}$. We denote by $\{x\}$ the fractional part of x. Lines where minor corrections of the original text have been made are marked "c" in the left margin.

March 2007

Henryk Iwaniec
Władysław Narkiewicz
Jerzy Urbanowicz

Contents

Volume 1

Volume 2

Part A

Diophantine equations and integral forms

Commentary on A: Diophantine equations and integral forms

by R. Tijdeman

A1. In 1960 the authors published a paper [12] in which they remark that the equation investigated in their 1956 paper is equivalent with the equation $2^n - 7 = y^2$. Already in 1915 Ramanujan claimed that the latter equation in positive integers n, x has only solutions for $n = 3, 4, 5, 7, 15$. This result follows immediately from the paper by Browkin and Schinzel and had been confirmed earlier by Nagell [34], however by a different method. For a survey of the further developments up to 1966 see Hasse [27].

In the 1960 paper the authors used the method from their 1956 paper to prove results of the following type: if $D \not\equiv 0, 4, 7 \pmod 8$, then the equation

$$2^n - D = y^2 \tag{1}$$

has one solution at the most. If any solution exists, then $n \leqslant 2$. They conjectured that if $D > 0$ and $D \neq 7, 23, 2^k - 1$ ($k \in \mathbb{N}$) then (1) has at most one solution.

The conjecture was established by Beukers [6]. By use of hypergeometric functions he first gave a good lower bound for the approximation to $\sqrt{2}$ by rationals whose denominators are a power of two. From this Beukers obtained an explicit upper bound $n < 435 + 10(\log |D| / \log 2)$ for any solution (y, n) of (1) and subsequently he proved the Browkin–Schinzel conjecture. He also dealt with the case $D < 0$ and showed that there are at most four solutions. M. Le [31] sharpened this result by proving among other results that if D is not of the form $2^{2m} - 3 \cdot 2^{m+1} + 1$, then there are at most three solutions.

In a second paper [7] Beukers extended his investigations to the equation $y^2 - D = p^n$, where D is a positive integer and p is an odd prime not dividing D. He showed that there are at most four solutions and gave a family of such equations having three solutions. That there are at most three solutions was proved much later by Bauer and Bennett [3]. For related later work, see e.g. Bender and Herzberg [4], Le [32], Yuan [62] and Bugeaud and Shorey [14].

Many papers have been written on individual Diophantine equation of Ramanujan–Nagell type (1). The theory on linear forms in logarithms of algebraic numbers made it possible to treat whole classes of such equations at the same time. By first applying this theory, next the basis reduction algorithm of Lenstra, Lenstra and Lovász, and finally the Fincke–Pohst algorithm for finding short lattice vectors, de Weger [60] extended the

theory into two directions. In the first place he studied for fixed integer k and primes $p_1, \dots, p_s$ the generalized Ramanujan–Nagell equation $y^2 + k = p_1^{z_1} \cdots p_s^{z_s}$ in $y \in \mathbb{N}$, $0 \leqslant z_1, \dots, z_s \in \mathbb{Z}$. As an illustration of his method he computed all 16 nonnegative numbers y such that $y^2 + 7$ has no prime divisors larger than 20 explicitly, the largest being $y = 273$. Secondly he considered the equation $x + z = y^2$ in integers x, y, z with $x > z$, $y > 0$, x and $|z|$ composed of fixed primes. As an illustration he computed all 388 solutions where x and $|z|$ are composed of the primes 2, 3, 5 and 7, the largest solution being $199290375 - 686 = 14117^2$. For further developments into this direction see e.g. Smart [48] and Wildanger [61].

A2. Suryanarayana and Rao [50] gave another solution to the problem of writing $3/(2n + 1)$ for any integer $n > 1$ as the sum of reciprocals of three distinct odd positive integers. They also showed that $2/(2n + 1)$ can be expressed as the sum of two such reciprocals if and only if $2n + 1$ is not a prime $\equiv 3 \pmod 4$. The result of paper **A2** has been recently rediscovered by Hagedorn [26]. See also Sierpiński [44].

A3. The result of this paper is presented in the book by Honsberger [29]. It has been generalized by Kulikowski [30] to the corresponding problem in higher dimensions.

A4. Schinzel's main result in this paper was later applied by Schinzel and Sierpiński [42] to prove that every sufficiently large integer is a sum of four powers a^b with integers $a > 1, b > 1$.

The hypothesis that the restriction $n < 101200$ in Corollaire 3 can be dropped was earlier made in E. Grosswald, A. Calloway, and J. Calloway [24] who proved that *there exists a finite set S of numbers with the following property*: *if* $n > 0$ *is not divisible by* 4, *not* $\equiv -1 \pmod 8$ *and not in S, then n is the sum of three strictly positive squares*. See further Mordell [33] and, for an application of such results to the non-relativistic quantum statistical mechanics of an ideal gas at low temperature, Baltes, Draxl and Hilf [2].

A5. An immediate consequence of Corollary 2 is that the Diophantine equation $x^2 + y^m = z^{2n}$ has infinitely many primitive solutions if $(m, n) = 1$. This observation was made by Schinzel after D. W. Boyd had proved this fact in another way. See Boyd [10].

For later work on equations $x^l + y^m = z^n$ see Darmon and Granville [19] who showed that there are only finitely many integer solutions in x, y, z with $\gcd(x, y, z) = 1$ provided that $1/l + 1/m + 1/n < 1$ by using descent arguments and Faltings' theorem, remarked that there are no solutions at all if $1/l + 1/m + 1/n = 1$, and for each case with $1/l + 1/m + 1/n > 1$ wrote down a parametrization that gives rise to infinitely many non-zero coprime integer solutions (when one plugs in integers for the parameters). For further work see Beukers [8] and Edwards [22].

A6. Theorem 1 of this paper was generalized by Schinzel in **F1** to the case of polynomials in several variables.

An immediate consequence of Theorem 1 of the above paper is that *if* $f \in \mathbb{Q}[x]$ *is an integer-valued polynomial such that every arithmetic progression contains an integer a for which* $f(a)$ *is a kth power, then* $f = g^k$, *where* $g \in \mathbb{Q}[x]$ *is integer-valued*. Berstel [5] extended this under suitable conditions to rational functions.

Perelli and Zannier [35] gave the following related version. *Let $f(x)$ be a polynomial with integral coefficients. Assume that every arithmetic progression contains an integer x such that $f(x) = A(x)y^{k(x)}$, where $A(x)$, y are integers, $k(x) \geqslant k_0$, and the prime divisors of $A(x)$ belong to a finite set S. Then $f(x) = A(P(x))^k$ identically, where A is an integral constant, $P(x)$ is a polynomial with integral coefficients and $k \geqslant k_0$.*

S. Chowla [16] proved the following variant of the Corollary to Theorem 2 in paper **A6**: *If $g(x)$ is a sum of two squares for every sufficiently large integer x, then there exist two polynomials $P_1(x)$ and $P_2(x)$ with integer coefficients such that $g(x) = P_1(x)^2 + P_2(x)^2$ for all x.*

In a subsequent paper [20] the three authors extended the Corollary to Theorem 2 as follows. *Let $F(x, y, t)$ be any polynomial with integral coefficients which is of degree at most two in x and y. Suppose that every arithmetic progression contains an integer t such that the equation $F(x, y, t) = 0$ is soluble in rationals x, y. Then there exist rational functions $x(t)$ and $y(t)$ with rational coefficients such that $F(x(t), y(t), t) = 0$ identically in t.*

Far reaching generalizations of results in the paper by Davenport, Lewis and Schinzel can be found in Theorems 51 and 57, and Corollary 4 in Section 5.6 of Schinzel [41].

A7. A refinement of Schinzel's result was given by Ayad [1] who gave explicit forms of the Puiseux expansions corresponding to the places at infinity of the associated function field.

The "only if" part of the following statement for $n = 2$ is a direct consequence of Schinzel's above paper. *Let $C/\mathbb{Q}$ be an irreducible affine curve of geometric genus 0 and fix an embedding of C into $\mathbb{A}^n$ so that the ideal of C is generated by polynomials with integer coefficients. Further, let C_∞ be the set of points "at infinity" on the projective closure $\overline{C}$ of C in $\mathbb{P}^n$, and let Σ_∞ be the points "at infinity" on the desingularization of $\overline{C}$. Assume that $C(\mathbb{Z})$ contains at least one nonsingular point. Then $C(\mathbb{Z})$ is infinite if and only if one of the following two conditions is satisfied:* (a) *Σ_∞ consists of a single point*; *or* (b) *Σ_∞ consists of exactly two points which are conjugate over a real quadratic field*. The general statement was proved by Silverman [46]. The "if" part was proved by Poulakis [38] who corrected an error of Silverman who formulated the conditions in terms of C_∞, instead of in terms of Σ_∞. Counterexamples for Silverman's statement involving Σ_∞ can be found in the review MR 2001h:11080.

For more information on Runge's method see **A14** and the added notes.

A8. The result in this paper was generalized by Shorey, van der Poorten, Tijdeman, and Schinzel in [43] as follows. *Let S be the set of all non-zero integers composed of primes from some fixed finite set. Let $f \in \mathbb{Q}[x, y]$ be a binary form with $f(1, 0) \neq 0$ such that among the linear factors in the factorization of f at least two are distinct. Let d be a positive integer. Then the equation $wz^q = f(x, y)$ in integers q, w, x, y, z with $w \in S$, $y \in S$, $(x, y) = d$, $|z| > 1$ implies $q < C$ where C is an effectively computable constant depending only on f, d and S.* As an application they proved the following generalization of a result of Mahler about the greatest prime factor of $ax^n + by^q$ tending to ∞ if $\max(|x|, |y|) \to \infty$ with $(x, y) = 1$. *Let $n \in \mathbb{Z}$, $n > 1$. Let S be as above. The equation $ux^n + vy^q = w$ in non-zero integers $q > 1$, $u \in S$, $v \in S$, $w \in S$, $x \in \mathbb{Z}$, $y \in \mathbb{Z}$ with $|x| > 1$, $|y| > 1$, $(ux, w) = 1$ and $nq \geqslant 6$ has only finitely many solutions.*

Quantitative versions of the Schinzel–Tijdeman theorem were given by Turk [53]. He proved for example: *Let $a \in \mathbb{Z}$ be non-zero and let $F \in \mathbb{Z}[X]$ have at least two distinct zeros, degree n and height H. Suppose $F(x) = ay^m$ for some $x, y \in \mathbb{Z}$ with $|y| > 1$. Then*

$$m < \exp\left\{\frac{Cn^5(\log(3H))^2}{\log(n\log 3H)}\right\}(\log 3|a|)(\log\log 3|a|)^2,$$

where C is an absolute constant. Later Pink [36] gave new explicit lower bounds for the difference $|F(x) - by^m|$ where $F(X)$ is an integer polynomial of degree $n \geqslant 2$ and x, y, b, m are non-zero integers with $m \geqslant 2$, $|y| \geqslant 2$ and $F(x) \neq by^m$.

Various results on the representation of powers by polynomials with coefficients from an algebraic number field were derived by Trelina [52]. Győry, Pink and Pintér [25] have given effectively computable upper bounds for n in the equations $f(x) = wy^n$ and $F(x, z) = wy^n$, where f is a polynomial, F a binary form, both with discriminants belonging to some set S of S-integers, x, y, w, z, n are unknown integers with $z, w \in S$, $y \notin S$ and $n \geqslant 3$. The upper bounds only depend on the product $p_1 \cdots p_s$ and on the degrees of $f(X)$ and of $F(X, Y)$.

Quantitative versions of the Schinzel–Tijdeman approach have been used to solve Diophantine equations. For example Herrmann, Járási and Pethö [28] completed the study of the Diophantine equation $x^n = Dy^2 + 1$ in variables (n, x, y) for $1 \leqslant D \leqslant 100$. Using a combination of elementary techniques, and a clever criterion due to Nagell, J. H. E. Cohn [17] had determined all solutions except for the six cases $(n, D) \in \{(3, 31), (5, 31), (3, 38), (3, 61), (5, 71), (7, 71)\}$. The remaining cases were treated by using the methods on linear forms in logarithms.

Bugeaud, Mignotte and Siksek [13] studied the equations $F_n = q^k y^p$ and $L_n = q^k y^p$, where F_n and L_n denote the nth Fibonacci and Lucas numbers, respectively, and $k > 0$ and p, q are primes. They have announced to have proved that the only Fibonacci numbers which are powers y^n with integers $y > 1$, $n > 1$ are 8 and 144.

Other examples where the Schinzel–Tijdeman theorem has been applied are Voorhoeve, Győry and Tijdeman [58], Brindza [11] for the equation $1^k + 2^k + \ldots + (x-1)^k + R(x) = by^z$, and Dilcher [21], Urbanowicz [54], [55], [56] for some generalizations of the equation, and Bilu, Kulkarni and Sury [9] for the equation $x(x+1)\cdots(x+(m-1)) + r = y^n$.

A9. Call two number fields arithmetically equivalent if they have the same zeta function. Define the normset of a number field $\boldsymbol{K}$ as the set of elements of $\mathbb{Z}$ that are norms of integers of $\boldsymbol{K}$. Coykendall [18] has given an example of arithmetically equivalent fields that have different normsets. The fields are $\boldsymbol{K} = \mathbb{Q}(\sqrt[8]{-15})$ and $\boldsymbol{L} = \mathbb{Q}(\sqrt[8]{-240})$. B. de Smit and R. Perlis [49] have shown that these fields are arithmetically equivalent and in fact have the same class number. The paper **A9** shows that there are non-isomorphic fields which are arithmetically equivalent and have class number 1, so consequently have the same normset. Thus the normset cannot, in general, distinguish between non-isomorphic arithmetically equivalent fields.

A10. Generalizations of Theorem 2 to polynomials with coefficients in a number field $\boldsymbol{K}$ can be found as Theorems 53 and 55 in Schinzel [41].

A11. Chapter 5 of Schinzel's book [41] is mainly devoted to the study of the following question. Let $\boldsymbol{K}$ be a number field. Assume that $F \in \mathbb{C}[\boldsymbol{x}, \boldsymbol{t}]$ has a zero in $\boldsymbol{K}^s$ for a sufficiently large set $t^* \in \mathbb{Z}^r$. Does it follow that F viewed as a polynomial in $\boldsymbol{x}$ has a zero in $\boldsymbol{K}(\boldsymbol{x})^s$? Schinzel proves that for $s = 1$ the answer is yes. By an example he shows that the answer is in general no for $s \geqslant 3$. The problem is open for $s = 2$. The example in the above paper shows that the answer is no provided that Selmer's conjecture is correct.

The paper induced J. Silverman [45] to conjecture that almost all ranks of the curves from a certain family he studied are at most 1.

A12. Generalizations of results from this paper to the case $t \in \mathbb{Z}^r$ for any positive integer r have been given in Schinzel [40]. Further generalizations of Theorems 1 and 2 where coefficients are taken from a number field can be found as Theorems 58 and 59 in Schinzel's book [41].

A13. Theorem 1 of this paper has been stated as Exercise 11.4 in Cassels' book [15] with the following hint: the intersection of $F_j(x, y, z) = 0$ is either (i) a conic, (ii) a line or (iii) a set of $n \leqslant 4$ points conjugate over k.

A14. Later bounds for solutions of Diophantine equations which do not satisfy Runge's condition have been given by Walsh [59] and in the special case that the irreducible polynomial is of the form $F(x) - G(y)$ where F and G are monic polynomials with rational coefficients and $\gcd(\deg F, \deg G) > 1$ by Tengely [51].

In a slightly different setting various estimates were obtained by D. Poulakis, partly in collaboration with others. For example, in [37] he obtained the following sharp bound. *Let K be a number field and denote by O_K its ring of integers. Let $F(X, Y)$ be an irreducible polynomial in $K[X, Y] \setminus K[Y]$ of total degree N and of degree $n > 0$ in Y. Suppose K is totally real, and $F_N(1, Y)$ is a polynomial of degree n without real roots, where $F_N(X, Y)$ denotes the homogeneous part of degree N of $F(X, Y)$. Denote by H the (multiplicative) absolute height. If $F(x, y) = 0$ with $(x, y) \in O_K \times K$, then* $\max\{H(x), H(y)\} < \left(2^N N\right)^{N^3} H(F)^{2N^3}$.

In [39] Poulakis improved upon Walsh's estimates especially with respect to the dependence on $\gcd(x, y)$ in the following special case: $F(X, Y)$ is an irreducible, integer polynomial of degree $\geqslant 2$ such that the curve C defined by the equation $F(X, Y) = 0$ has infinitely many integer points and the point $(0, 0)$ is simple on C whereas $d \geqslant 1$ is a real number.

A15. A general conjecture is that for all positive integers m, k with $m > k \geqslant 3$ the equations

$$\frac{m}{n} = \frac{1}{x_1} + \frac{1}{x_2} + \ldots + \frac{1}{x_k} \tag{2}$$

is solvable in positive integers $x_1, x_2, \ldots, x_k$ for all but finitely many values of n. For $(m, n) = (4, 3)$ Erdős and Straus even conjectured that there are no exceptions at all, for $m > k = 3$ it is Schinzel's conjecture, both cited in the above paper. The conjecture for $k > 3$ follows trivially from the conjecture for $k = 3$. The conjecture is still wide open.

Some authors have derived upper bounds for the number of exceptions

$$E_{m,k}(N) = |\{n \leqslant N : \text{equation (2) has no solution}\}|.$$

Vaughan [57] proved that $E_{m,3}(N) \leqslant b_m N \exp(-c_m(\log N)^{2/3})$ where b_m and c_m are positive constants. Elsholtz [23] improved upon earlier results of C. Viola and Z. Shen by generalizing Vaughan's result to $E_{m,k}(N) \leqslant c_{m,k} N \exp(-b_{m,k}(\log N)^{e_k})$ where $b_{m,k}$ and $c_{m,k}$ are positive constants and $e_k = 1 - 1/(2^{k-1} - 1)$ for all m, k specified above.

A16. This paper provides an effective method for finding points over a finite field on an elliptic curve of the form $E : Y^2 = X^3 + B$. In a subsequent paper Skałba [47] has given a deterministic polynomial time algorithm for finding points over a finite field on an elliptic curve $E : Y^2 = X^3 + AX + B$ provided that $A \neq 0$.

References

[1] M. Ayad, *Sur le théorème de Runge*. Acta Arith. 58 (1991), 203–209.

[2] H. P. Baltes, P. K. J. Draxl, E. R. Hilf, *Quadratsummen und gewisse Randwertprobleme der mathematischen Physik*. J. Reine Angew. Math. 268/269 (1974), 410–417.

[3] M. Bauer, M. A. Bennett, *Applications of the hypergeometric method to the generalized Ramanujan–Nagell equation*. Ramanujan J. 6 (2002), 209–270.

[4] E. A. Bender, N. P. Herzberg, *Some Diophantine equations related to the quadratic form* $ax^2 + by^2$. In: Studies in Algebra and Number Theory, Academic Press, New York 1979, 219–272.

[5] J. Berstel, *Sur des fractions rationnelles particulières*. In: Sém. M. P. Schützenberger, A. Lentin et M. Nivat, 1969/70: Problèmes Mathématiques de la Théorie des Automates, Exp. 2.

[6] F. Beukers, *On the generalized Ramanujan–Nagell equation* I. Acta Arith. 38 (1980/81), 389–410.

[7] —, *On the generalized Ramanujan–Nagell equation* II. Acta Arith. 39 (1981), 113–123.

[8] —, *The Diophantine equation* $Ax^p + By^q = Cz^r$. Duke Math. J. 91 (1998), 61–88.

[9] Yu. F. Bilu, M. Kulkarni, B. Sury, *The Diophantine equation* $x(x+1)\cdots(x+(m-1))+r = y^n$. Acta Arith. 113 (2004), 303–308.

[10] D. W. Boyd, *The Diophantine equation* $x^2 + y^m = z^{2n}$. Amer. Math. Monthly 95 (1988), 544–547; *Addendum*, ibid. 97 (1990), 411–412.

[11] B. Brindza, *On some generalizations of the Diophantine equation* $1^k + 2^k + \ldots + x^k = y^z$. Acta Arith. 44 (1984), 99–107.

[12] J. Browkin, A. Schinzel, *On the equation* $2^n - D = y^2$. Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys. 8 (1960), 311–318.

[13] Y. Bugeaud, M. Mignotte, S. Siksek, *Sur les nombres de Fibonacci de la forme* $q^k y^p$. C. R. Math. Acad. Sci. Paris 339 (2004), 327–330.

[14] Y. Bugeaud, T. N. Shorey, *On the number of solutions of the generalized Ramanujan–Nagell equation*. J. Reine Angew. Math. 539 (2001), 55–74.

[15] J. W. S. Cassels, *Local Fields*. Cambridge Univ. Press, Cambridge 1986.

[16] S. Chowla, *Some problems of elementary number theory*. J. Reine Angew. Math. 222 (1966), 71–74.

[17] J. H. E. Cohn, *The Diophantine equation* $x^n = Dy^2 + 1$. Acta Arith. 106 (2003), 73–83.

[18] J. Coykendall, *A remark on arithmetic equivalence and the normset*. Acta Arith. 92 (2000), 105–108.

[19] H. Darmon, A. Granville, *On the equations* $z^m = F(x, y)$ *and* $Ax^p + By^q = Cz^r$. Bull. London Math. Soc. 27 (1995), 513–543.

[20] H. Davenport, D. J. Lewis, A. Schinzel, *Quadratic Diophantine equations with a parameter*. Acta Arith. 11 (1966), 353–358.

[21] K. Dilcher, *On a Diophantine equation involving quadratic characters*. Compositio Math. 57 (1986), 383–403.

[22] J. Edwards, *A complete solution to* $X^2 + Y^3 + Z^5 = 0$. J. Reine Angew. Math. 571 (2004), 213–236.

[23] C. Elsholtz, *Sums of k unit fractions*. Trans. Amer. Math. Soc. 353 (2001), 3209–3227.

[24] E. Grosswald, A. Calloway, J. Calloway, *The representation of integers by three positive squares*. Proc. Amer. Math. Soc. 10 (1959), 451–455.

[25] K. Győry, I. Pink, A. Pintér, *Power values of polynomials and binomial Thue–Mahler equations*. Publ. Math. Debrecen 65 (2004), 341–362.

[26] Th. R. Hagedorn, *A proof of a conjecture on Egyptian fractions*. Amer. Math. Monthly 107 (2000), 62–63.

[27] H. Hasse, *Über eine diophantische Gleichung von Ramanujan–Nagell und ihre Verallgemeinerung*. Nagoya Math. J. 27 (1966), 77–102.

[28] E. Herrmann, I. Járási, A. Pethö, *Note on "The Diophantine equation* $x^n = Dy^2 + 1$*"* (*Acta Arith.* 106 (2003), 73–83) *by J. H. E. Cohn*. Acta Arith. 113 (2004), 69–76.

[29] R. Honsberger, *Mathematical Gems from Elementary Combinatorics, Number Theory, and Geometry*. The Mathematical Association of America, Buffalo 1973.

[30] Th. Kulikowski, *Sur l'existence d'une sphère passant par un nombre donné de points aux coordonnées entières*. Enseignement Math. (2) 5 (1959), 89–90.

[31] M. Le, *On the number of solutions of the generalized Ramanujan–Nagell equation* $x^2 - D = 2^{n+2}$. Acta Arith. 60 (1991), 149–167.

[32] M. Le, *A note on the number of solutions of the generalized Ramanujan–Nagell equation*. J. Number Th. 62 (1997), 100–106.

[33] L. J. Mordell, *The representation of integers by three positive squares*. Michigan Math. J. 7 (1960), 289–290.

[34] T. Nagell, *The Diophantine equation* $x^2 + 7 = 2^n$. Norsk Mat. Tidskr. 30 (1948), 62–64; English transl.: Ark. Mat. 4 (1961), 185–187.

[35] A. Perelli, U. Zannier, *An arithmetic property of polynomials*. Boll. Un. Mat. Ital. A (5) 17 (1980), 199–202.

[36] I. Pink, *On the differences between polynomial values and perfect powers*. Publ. Math. Debrecen 63 (2003), 461–472.

[37] D. Poulakis, *Polynomial bounds for the solutions of a class of Diophantine equations*. J. Number Theory 66 (1997), 271–281.

[38] —, *Affine curves with infinitely many integral points*. Proc. Amer. Math. Soc. 131 (2003), 1357–1359.

[39] —, *Integer points on rational curves with fixed gcd*. Publ. Math. Debrecen 64 (2004), 369–379.

[40] A. Schinzel, *An application of Hilbert's irreducibility theorem to Diophantine equations*. Acta Arith. 41 (1982), 203–211.

[41] A. Schinzel, *Polynomials with Special Regard to Reducibility*. Encyclopaedia of Mathematics and its Applications 77, Cambridge Univ. Press, Cambridge 2000.

[42] A. Schinzel, W. Sierpiński, *Sur les puissances propres*. Bull. Soc. Roy. Sci. Liège 34 (1965), 550–554.

[43] T. N. Shorey, A. J. van der Poorten, R. Tijdeman, A. Schinzel, *Applications of the Gel′fond–Baker method to Diophantine equations*. In: Transcendence Theory: Advances and Applications (ed. A. Baker and D. Masser), Academic Press, London 1977, 59–77.

[44] W. Sierpiński, *O rozkładach liczb wymiernych na ułamki proste* (*On Decompositions of Rational Numbers into Unit Fractions*). PWN, Warszawa 1957 (Polish).

[45] J. H. Silverman, *Divisibility of the specialization map for families of elliptic curves*. Amer. J. Math. 107 (1985), 555–565.

[46] —, *On the distribution of integer points on curves of genus zero*. Theoret. Comput. Sci. 235 (2000), 163–170.

[47] M. Skałba, *Points on elliptic curves over finite fields*. Acta Arith. 117 (2005), 293–301.

[48] N. P. Smart, *Determining the small solutions to S-unit equations*. Math. Comp. 68 (1999), 1687–1699.

[49] B. de Smit, R. Perlis, *Zeta functions do not determine class numbers*. Bull. Amer. Math. Soc. (N.S.) 31 (1994), 213–215.

[50] D. Suryanarayana, N. V. Rao, *On a paper of André Schinzel*. J. Indian Math. Soc. (N.S.) 29 (1965), 165–167.

[51] Sz. Tengely, *On the Diophantine equation* $F(x) = G(y)$. Acta Arith. 110 (2003), 185–200.

[52] L. A. Trelina, *Representation of powers by polynomials in algebraic number fields*. Dokl. Akad. Nauk BSSR 29 (1985), no. 1, 5–8 (Russian).

[53] J. Turk, *On the difference between perfect powers*. Acta Arith. 45 (1986), 289–307.

[54] J. Urbanowicz, *On the equation* $f(1)1^k + f(2)2^k + \ldots + f(x)x^k + R(x) = by^z$. Acta Arith. 51 (1988), 349–368.

[55] —, *On Diophantine equations involving sums of powers with quadratic characters as coefficients* I. Compositio Math. 92 (1994), 249–271.

[56] —, *On Diophantine equations involving sums of powers with quadratic characters as coefficients* II. Compositio Math. 102 (1996), 125–140.

[57] R. C. Vaughan, *On a problem of Erdős, Straus and Schinzel*. Mathematika 17 (1970), 193–198.

[58] M. Voorhoeve, K. Győry, R. Tijdeman, *On the Diophantine equation* $1^k+2^k+\ldots+x^k+R(x) = y^z$. Acta Math. 143 (1979), 1–8; Corr. ibid. 159 (1987), 151.

[59] P. G. Walsh, *A quantitative version of Runge's theorem for Diophantine equations*. Acta Arith. 62 (1992), 157–172; Corr. ibid. 73 (1995), 397–398.

[60] B. M. M. de Weger, *Algorithms for Diophantine equations*. CWI Tract 65, Stichting Mathematisch Centrum, Amsterdam 1989.

[61] K. Wildanger, *Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern*. J. Number Theory 82 (2000), 188–224.

[62] P. Z. Yuan, *On the number of solutions of* $x^2 - D = p^n$. Sichuan Daxue Xuebao 35 (1998), 311–316.

Originally published in
Comptes rendus des séances de l'Académie des Sciences
242, 1780–1781

Sur les nombres de Mersenne qui sont triangulaires*

avec Georges Browkin

Démonstration que l'équation $2^x - 1 = (1/2)y(y+1)$ en entiers positifs x et y n'a que les solutions $(x, y) = (1, 1), (2, 2), (4, 5)$ et $(12, 90)$.

Théorème. *Les nombres de Mersenne $M_n = 2^n - 1$ (où $n = 1, 2, \dots$) qui sont en même temps triangulaires, $t_k = (1/2)k(k+1)$, sont seulement les nombres $M_1 = t_1$, $M_2 = t_2$, $M_4 = t_5$ et $M_{12} = t_{90}$.*

Démonstration. L'équation $2^n - 1 = (1/2)k(k+1)$ équivaut à

$$\left(k + \frac{1}{2}\right)^2 + \frac{7}{4} = \left[\left(\frac{1}{2}\right)^2 + \frac{7}{4}\right]^{n+1},$$

donc à

$$\left(k + \frac{1}{2} + \frac{1}{2}\sqrt{-7}\right)\left(k + \frac{1}{2} - \frac{1}{2}\sqrt{-7}\right) = \left(\frac{1}{2} + \frac{1}{2}\sqrt{-7}\right)^{n+1}\left(\frac{1}{2} - \frac{1}{2}\sqrt{-7}\right)^{n+1}. \tag{1}$$

Les nombres $(1/2) \pm (1/2)\sqrt{-7}$ sont des entiers du corps $\mathbb{Q}(\sqrt{-7})$ et, en tant que facteurs du nombre premier rationnel 2, ils sont premiers dans le corps $\mathbb{Q}(\sqrt{-7})$.

Posons $\alpha_k = k + (1/2) + (1/2)\sqrt{-7}$ et $\beta_k = k + (1/2) - (1/2)\sqrt{-7}$. On a $\alpha_k - \beta_k = \sqrt{-7}$ et $\alpha_k\beta_k = 2^{n+1}$. Le plus grand diviseur commun des nombres α_k et β_k [dans le corps $\mathbb{Q}(\sqrt{-7})$] divise donc les normes des nombres $\sqrt{-7}$ et 2^{n+1}, c'est-à-dire les nombres 7 et 2^{n+1}, donc aussi le plus grand diviseur commun de ces derniers, c'est-à-dire le nombre 1. Or, dans le corps $\mathbb{Q}(\sqrt{-7})$ les seuls diviseurs du nombre 1 sont les nombres 1 et -1. On en conclut que les nombres α_k et β_k sont premiers entre eux [dans le corps $\mathbb{Q}(\sqrt{-7})$] et évidemment distincts des unités de ce corps. Or, puisque dans le corps $\mathbb{Q}(\sqrt{-7})$ a lieu le théorème sur l'unicité du développement en facteurs premiers, on en déduit de (1) que

$$\alpha_k = \pm\alpha_0^{n+1} \quad \text{et} \quad \beta_k = \pm\beta_0^{n+1} \quad \text{ou bien} \quad \alpha_k = \pm\beta_0^{n+1} \quad \text{et} \quad \beta_k = \pm\alpha_0^{n+1},$$

et, comme $\alpha_k - \beta_k = \sqrt{-7}$, on trouve

$$\sqrt{-7} = \pm\alpha_0^{n+1} \mp \beta_0^{n+1} \quad \text{ou bien} \quad \sqrt{-7} = \pm\beta_0^{n+1} \mp \alpha_0^{n+1}$$

* Note transmise par M. Wacław Sierpiński, séance du 27 février 1956.

et en posant $u_k = (1/\sqrt{-7})(\alpha_0^k - \beta_0^k)$ pour $k = 1, 2, \ldots$, on trouve

$$|u_{n+1}| = 1. \tag{2}$$

On a $u_1 = u_2 = 1$ et, comme l'a remarqué M. Antoine Wakulicz, $u_{k+1} = u_k - 2u_{k-1}$ pour $k = 2, 3, \ldots$. Les nombres u_k $(k = 1, 2, \ldots)$ sont donc des entiers rationnels.

Pour k et l naturels le nombre

$$\frac{u_{kl}}{u_k} = \sum_{j=1}^{l-1} \alpha_0^{k(l-j)} \beta_0^k$$

est entier dans le corps $\mathbb{Q}(\sqrt{-7})$, donc, comme nombre réel, est un entier rationnel. On a donc

$$u_k \mid u_{kl} \quad \text{pour } k \text{ et } l \text{ naturels.} \tag{3}$$

On démontre sans peine que les restes mod 64 des nombres u_k $(k = 1, 2, \ldots)$ forment une suite infinie périodique dont la période, précédée par la suite 1, 1, −1, −3, −1 est formée de 16 termes : 5, 7, −3, −17, −11, 23, −19, −1, −27, −25, 29, 15, 21, −9, 13, 31. Le nombre ± 1 pour $k > 5$ figure dans cette suite périodique seulement pour $k \equiv 13 \pmod{16}$ et alors on a $u_k \equiv -1 \pmod{64}$. Il résulte donc de (2) que $n = 0, 1, 2, 4$ ou bien

$$n + 1 \equiv 13 \pmod{16} \quad \text{et} \quad u_{n+1} = -1. \tag{4}$$

La suite $v_k = u_{16k+13}$ $(k = 0, 1, 2, \ldots)$ donne mod 17 les restes qui forment une suite périodique dont la période (commençant au premier terme de la suite) a 9 termes : −1, −5, 0, 5, 1, 2, −4, 4, −2. Le nombre −1 figure dans cette suite seulement pour $k \equiv 0 \pmod 9$, d'où l'on déduit que $n + 1 \equiv 13 \pmod{9 \cdot 16}$, donc que $n + 1 \equiv 1 \pmod 3$.

La suite $w_k = u_{3k+1}$ $(k = 0, 1, 2, \ldots)$ donne mod 79, les restes formant une suite périodique dont la période (commençant dès le premier terme de la suite) a 13 termes 1, −3, 7, −11, −1, 14, 17, −39, −20, 17, −4, −37, −20 et le nombre −1 figure dans cette suite seulement pour $k \equiv 4 \pmod{13}$, ce qui donne $n + 1 = 3k + 1 \equiv 13 \pmod{39}$, d'où $n + 1 = 13(3s + 1)$ et, d'après (3)

$$u_{3s+1} \mid u_{n+1} = -1, \quad \text{d'où} \quad |u_{3s+1}| = 1.$$

S'il était $3s = 0$, on aurait $n = 12$. Pour $3s \neq 0$, d'après $3s \neq 1, 2, 4$, on conclut comme plus haut que $3s + 1 = 13(3t + 1)$ (où s et t sont des entiers $\geqslant 0$), $n + 1 = 169(3t + 1)$ et, d'après (3)

$$u_{169} \mid u_{n+1} = -1, \quad \text{d'où} \quad u_{169} = \pm 1,$$

ce qui contredit à (4), puisque $169 \not\equiv 13 \pmod{16}$.

Notre théorème se trouve ainsi démontré.

Andrzej Schinzel
Selecta

Originally published in
Mathesis 65:4-5-6 (1956), 219–222

Sur quelques propriétés des nombres $3/n$ et $4/n$, où n est un nombre impair

En rapport avec un théorème connu des Égyptiens d'après lequel tout nombre rationnel positif est une somme d'un nombre fini de fractions primaires distinctes (c'est-à-dire de nombres $1/k$, où k est un entier positif), E. P. Starke a posé en 1952 la question de savoir si tout nombre rationnel positif au dénominateur impair est une somme d'un nombre fini de fractions primaires distinctes aux dénominateurs impairs ([1]). Deux années plus tard ce problème a été résolu positivement, entre autres par R. Breusch ([2]). Or, les démonstrations qu'on a données ne contiennent aucun renseignement sur le nombre des termes nécessaires pour représenter un nombre rationnel donné comme somme de fractions primaires distinctes aux dénominateurs impairs.

W. Sierpiński a examiné les nombres rationnels positifs aux numérateurs 1, 2 et 3. Il a démontré que aucun nombre $1/n$, où n est un nombre impair n'est une somme de deux fractions primaires aux dénominateurs impairs, et que pour tout nombre impair $n > 1$ le nombre $1/n$ est une somme de trois fractions primaires distinctes aux dénominateurs impairs. Il a aussi démontré que pour n impair > 1 le nombre $2/n$ est une somme de 4 fractions primaires distinctes aux dénominateurs impairs, et que pour aucun nombre impair n le nombre $2/n$ n'est une somme de trois fractions primaires aux dénominateurs impairs. Or pour que le nombre $2/n$, où n est un nombre impair, soit une somme de deux fractions primaires distinctes aux dénominateurs impairs, il faut et il suffit que le nombre n soit > 1 et qu'il ne soit pas un nombre premier de la forme $4k + 3$ ([3]).

Quant aux nombres $3/n$, W. Sierpiński a exprimé l'hypothèse que pour n impair > 3 ils sont des sommes de trois fractions primaires distinctes aux dénominateurs impairs. Je démontrerai ici cette hypothèse.

1. Théorème. *n étant un nombre impair > 3, le nombre $3/n$ est une somme de trois fractions primaires distinctes aux dénominateurs impairs.*

Si le nombre $3/n$ est une somme de trois fractions primaires distinctes aux dénominateurs impairs

$$\frac{3}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z},$$

([1]) *American Mathematical Monthly* 59 (1952), p. 640, problem 4512.

([2]) Ibidem, 61 (1954), p. 200–201 ; voir aussi [2], p. 785.

([3]) Les démonstrations de ces théorèmes paraîtront dans le livre [1] de W. Sierpiński, *Théorie des nombres*, vol. II (en polonais), préparé pour l'impression.

tout nombre $3/kn$, où $k = 1, 3, 5, \ldots$ jouit de la même propriété puisqu'on a alors

$$\frac{3}{kn} = \frac{1}{kx} + \frac{1}{ky} + \frac{1}{kz}.$$

Vu encore que $\frac{3}{9} = \frac{1}{5} + \frac{1}{9} + \frac{1}{45}$, il en résulte que pour démontrer notre théorème, il suffit de le démontrer pour les nombres $3/n$, où n est un nombre premier > 3. De tels nombres sont de la forme $6k \pm 1$, où k est un nombre naturel.

Si $n = 6k + 1$, la démonstration résulte tout de suite de l'identité suivante, trouvée par W. Sierpiński :

$$\frac{3}{6k+1} = \frac{1}{2k+1} + \frac{1}{(2k+1)(4k+1)} + \frac{1}{(4k+1)(6k+1)}. \tag{1}$$

Si $n = 6k - 1$, on a $n + 1 = 6k$ et $n + 1 = 3^s \cdot 2t$, où s et t sont des entiers positifs et t n'est pas divisible par 3, donc $t = 3u + 1$ ou bien $t = 3u + 2$, où u est un entier $\geqslant 0$. On a donc $n + 1 = 3^s(6u + 2)$ ou bien $n + 1 = 3^s(6u + 4)$.

Si $n + 1 = 3^s(6u + 2)$, on a, comme on le vérifie sans peine

$$\frac{3}{n} = \frac{1}{3^s(2u+1)} + \frac{1}{(2u+1)n} + \frac{1}{3^s(2u+1)n}. \tag{2}$$

Tous les dénominateurs à droite sont impairs et distincts, puisque, d'après $n > 3$ on a $n = 3^s(6u + 2) - 1 \geqslant 3^s \cdot 2 - 1 > 3^s$.

Si $n + 1 = 3^s(6u + 4)$, alors, comme on le vérifie aisément, en posant $m = 3^{s-1}(6u + 4) + 2u + 1$, on trouve

$$\frac{3}{n} = \frac{1}{m} + \frac{1}{3^s m} + \frac{1}{3^s mn} \tag{3}$$

et, comme $3^s > 1$ et $n > 3$, tous les dénominateurs à droite sont distincts.

Le théorème est ainsi démontré. Notre démonstration donne en même temps le moyen de trouver pour chaque nombre impair $n > 3$ donné une décomposition désirée.

Par exemple, pour $n = 191$, on a $n + 1 = 192 = 3(6 \cdot 10 + 4)$, d'où la décomposition

$$\frac{3}{191} = \frac{1}{85} + \frac{1}{3 \cdot 85} + \frac{1}{3 \cdot 85 \cdot 191}.$$

Pour $n = 863$, on a $n + 1 = 864 = 3^2(6 \cdot 5 + 2)$, d'où la décomposition

$$\frac{3}{863} = \frac{1}{27 \cdot 11} + \frac{1}{11 \cdot 863} + \frac{1}{27 \cdot 11 \cdot 863}.$$

Il est à remarquer qu'il peut exister d'autres décompositions que celles qui sont déterminées par notre démonstration. Par exemple, pour $n = 359$, on a $n + 1 = 360 = 3^2(6 \cdot 6 + 4)$ et notre démonstration donne la décomposition $\frac{3}{359} = \frac{1}{133} + \frac{1}{3^2 \cdot 133} + \frac{1}{3^2 \cdot 133 \cdot 359}$, mais on a aussi la décomposition $\frac{3}{359} = \frac{1}{11^2} + \frac{1}{3 \cdot 11 \cdot 359} + \frac{1}{3 \cdot 11^2 \cdot 359}$.

Vu que pour tout nombre impair $n > 1$ le nombre $1/n$ est une somme de trois fractions primaires aux dénominateurs impairs (évidemment $> n$), en partant du théorème et en appliquant cette décomposition au plus petit terme de la décomposition du nombre $3/n$ en

somme de fractions primaires distinctes aux dénominateurs impairs successivement $s-1$ fois (où s est un nombre naturel), nous obtenons le corollaire :

s étant un nombre naturel quelconque et n un nombre naturel > 3, le nombre $3/n$ est une somme de $2s+1$ fractions primaires distinctes aux dénominateurs impairs.

D'autre part, il est clair que pour n impair le nombre $3/n$ n'est pas une somme d'un nombre pair de fractions primaires aux dénominateurs impairs (puisque la somme de ces dernières est un nombre rationnel au numérateur pair et dénominateur impair, donc un nombre distinct de $3/n$).

2. Théorème. *n étant un nombre naturel tel que $n > 1$ et $n \neq 5$, le nombre $4/n$ est une somme de quatre fractions primaires distinctes aux dénominateurs impairs.*

Soit n un nombre impair > 1 et $n \neq 5$. Si $n = 3$ on a

$$\frac{4}{3} = \frac{1}{1} + \frac{1}{5} + \frac{1}{9} + \frac{1}{45},$$

d'où il résulte tout de suite que le théorème est vrai pour tout nombre impair n divisible par 3. Il nous reste donc les nombres de la forme $6k \pm 1$, où $k = 1, 2, \ldots$.

Si $n = 6k+1$, on a

$$\frac{4}{n} = \frac{1}{6k+1} + \frac{3}{6k+1}$$

et la vérité du théorème pour le nombre n résulte de la formule (1) et de la remarque que, pour k naturel, on a

$$2k+1 < 6k+1 < (2k+1)(4k+1) < (4k+1)(6k+1).$$

Si $n = 6k-1$, alors, comme dans la démonstration du premier théorème, nous distinguerons les cas $n+1 = 3^s(6u+2)$ et $n+1 = 3^s(6u+4)$, où $s = 1, 2, \ldots$ et $u = 0, 1, 2, \ldots$.

Si $n+1 = 3^s(6u+2)$ et $u = 0$, donc si $n = 3^s \cdot 2 - 1$, alors pour s pair on a $n = 8k+1$, où k est un nombre naturel et la vérité du théorème pour le nombre n résulte de l'identité de W. Sierpiński

$$\frac{4}{8k+1} = \frac{1}{2k+1} + \frac{1}{(2k+1)(4k+1)} + \frac{1}{(2k+1)(8k+1)} + \frac{1}{(2k+1)(4k+1)(8k+1)},$$

et pour s impair on a, comme on le démontre sans peine, $n = 16k+5$, où, vu que $n \neq 5$ et que n n'est pas divisible par 3, k est un entier > 1, et la vérité du théorème pour le nombre n résulte de l'identité

$$\frac{4}{16k+5} = \frac{1}{3(2k+1)} + \frac{1}{16k+5} + \frac{1}{3(16k+5)} + \frac{1}{(2k+1)(16k+5)}$$

et de la remarque que pour $k > 1$ on a

$$3(2k+1) < 16k+5 < 3(16k+5) < (2k+1)(16k+5).$$

Si $n+1 = 3^s(6u+2)$ et $u > 0$, alors, vu que $4/n = 1/n + 3/n$, la vérité du théorème pour le nombre n résulte de la formule (2) et de la remarque que les nombres n, $3^s(2u+1)$, $(2u+1)n$ et $3^s(2u+1)n$ sont tous distincts.

Enfin, si $n+1 = 3^s(6u+4)$, la vérité du théorème pour le nombre n résulte des formules $4/n = 1/n + 3/n$ et (3) [où $m = 3^{s-1}(6u+4)+2u+1$] et de la remarque que les nombres n, m, $3^s m$ et $3^s mn$ sont tous distincts.

Le théorème se trouve ainsi démontré.

Or, en ce qui concerne le nombre $n = 5$, W. Sierpiński a démontré que le nombre $4/5$ n'est pas une somme de moins de six fractions primaires aux dénominateurs impairs et qu'on a

$$\frac{4}{5} = \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{15} + \frac{1}{21} + \frac{1}{105}.$$

On peut démontrer sans peine que pour que le nombre $4/n$, où n est un nombre impair, soit une somme de deux fractions primaires aux dénominateurs impairs, il faut et il suffit que n ait un diviseur naturel de la forme $8k+3$.

Ouvrages cités

[1] W. Sierpiński, *Teoria liczb*, część 2. Monografie Matematyczne 38, PWN, Warszawa 1959.

[2] B. M. Stewart, *Sums of distinct divisors*. Amer. J. Math. 76 (1954), 779–785.

Andrzej Schinzel
Selecta

Originally published in
L'Enseignement mathématique IV:1 (1958), 71–72

Sur l'existence d'un cercle passant par un nombre donné de points aux coordonnées entières

Le but de cette Note est de démontrer ce

Théorème. *Quel que soit le nombre naturel n, il existe dans le plan un cercle dont la circonférence contient précisément n points aux coordonnées entières.*

(Ce théorème a été mentionnée dans l'article de M. W. Sierpiński *Sur quelques problèmes concernant les points aux coordonnées entières* paru dans ce fascicule, page 25.)

Démonstration. Pour n impair, $n = 2k + 1$, où k est un entier $\geqslant 0$, le cercle au centre $\left(\frac{1}{3}, 0\right)$ et au rayon $5^k/3$ satisfait à notre théorème.

En effet, d'après un théorème connu sur le nombre de décomposition en deux carrés, l'équation $x^2 + y^2 = 5^{2k}$ a $4(2k+1)$ solutions en nombres entiers x et y. Comme $5^{2k} \equiv 1 \pmod 3$ pour $k = 0, 1, 2, \ldots$, on démontre sans peine que dans chaque telle solution, un et un seul des nombres x et y est divisible par 3. Les solutions se divisent donc en $2k + 1$ quadruples disjoints : (x, y), $(x, -y)$, (y, x), $(-y, x)$, où x est un entier divisible par 3 et y un entier qui n'est pas divisible par 3. Dans chaque tel quadruple, une et une seule solution satisfait à la condition que le premier terme de la paire $\equiv -1 \pmod 3$ et le second $\equiv 0 \pmod 3$. Il existe donc précisément $2k + 1 = n$ solutions en nombres entiers z et t de l'équation $(3z - 1)^2 + (3t)^2 = 5^{2k}$, c'est-à-dire de l'équation $\left(z - \frac{1}{3}\right)^2 + t^2 = \left(\frac{5^k}{3}\right)^2$. Cela prouve qu'il existe précisément n points aux coordonnées entières sur le cercle déterminé par cette équation, ce qui démontre notre théorème pour n impair.

Pour n pair, $n = 2k$, où k est un nombre naturel, le cercle au centre $\left(\frac{1}{2}, 0\right)$ et au rayon $5^{(k-1)/2}/2$ satisfait à notre théorème. En effet, d'après le théorème mentionné plus haut, l'équation $x^2 + y^2 = 5^{k-1}$ a précisément $4k$ solutions en nombres entiers x et y. Or, des nombres x, y, un et seul un est pair et ainsi toutes les solutions se divisent en $2k$ paires disjointes (x, y) et (y, x) qui ne diffèrent entre elles que par l'ordre de leurs termes. Dans chaque telle paire précisément une solution satisfait à la condition que le premier élément est impair et le second pair. Il existe donc précisément $2k = n$ solutions en nombres entiers z, t de l'équation $(2z - 1)^2 + (2t)^2 = 5^{k-1}$, c'est-à-dire à l'équation $\left(z - \frac{1}{2}\right)^2 + t^2 = \left(\frac{5^{(k-1)/2}}{2}\right)^2$, ce qui démontre notre théorème pour n pair.

Notre théorème se trouve ainsi démontré.

Originally published in
Bulletin de l'Academie Polonaise des Sciences
Série des sci. math., astr. et phys.
VII (1959), 307–310

Sur les sommes de trois carrés

Présénte par W. Sierpiński le 18 mars 1959

Une de mes communications antérieures [1] contient la remarque que l'hypothèse de G. Pall ([2]) soutenant que tout nombre naturel de la forme $2(8n+1) > 2$ est une somme de trois carrés > 0 est en défaut pour $n = 8$.

Or, le problème suivant s'impose : quels sont les nombres naturels qui sont sommes de trois carrés positifs ? Le but de la présente communication est de démontrer le théorème qui suit.

Théorème 1. *Pour que le nombre n admette une décomposition* $n = x^2 + y^2 + z^2$, *où* $x, y, z > 0$ *et* $(x, y, z) = 1$, *il faut et il suffit que n ait à la fois deux propriétés suivantes* :
(i) $n \not\equiv 0, 4, 7 \pmod 8$;
(ii) *n a un diviseur naturel de la forme* $4k-1$ *ou bien n n'est pas un "numerus idoneus"*.

Les "numeri idonei" sont — comme on sait — des nombres naturels D vérifiant l'équation $p(-4D) = 1$, où $p(d)$ est un nombre des classes de formes binaires au discriminant d de genre principal. Une définition arithmétique de "numeri idonei" a été donnée par Euler (cf. [3], vol. 1, p. 361 ; pour les corrections voir [4]).

Démonstration. Le nombre $N_3(n)$ des réprésentations propres du nombre $n > 3$ par la forme $x^2 + y^2 + z^2$ est donné par la formule (cf. [3], vol. 2, p. 265)

$$N_3(n) = \begin{cases} 12h(-4n) & \text{pour } n \equiv 1, 2, 5, 6 \pmod 8 \\ 24h(-4n) & \text{pour } n \equiv 3 \pmod 8 \\ 0 & \text{pour } n \equiv 0, 4, 7 \pmod 8, \end{cases} \tag{1}$$

où $h(d)$ est le nombre des classes de formes binaires au discriminant d. Mais, d'après le théorème sur la duplication, on a :

$$h(d) = p(d) \cdot \begin{cases} 2^{\lambda-2} & \text{pour } d \equiv 4 \pmod{16} \\ 2^{\lambda} & \text{pour } d \equiv 0 \pmod{32} \\ 2^{\lambda-1} & \text{pour d'autres cas,} \end{cases} \tag{2}$$

où λ est le nombre des facteurs premiers du nombre d.

Pour $n > 3$, on obtient de formules (1) et (2)

$$N_3(n) = \begin{cases} 3 \cdot 2^{\mu+2} p(-4n) & \text{pour } n \equiv 1, 2, 5, 6 \pmod 8 \\ 3 \cdot 2^{\mu+2} p(-n) & \text{pour } n \equiv 3 \pmod 8 \\ 0 & \text{pour } n \equiv 0, 4, 7 \pmod 8, \end{cases} \tag{3}$$

où μ est le nombre des facteurs premiers impairs du nombre n.

D'autre part, le nombre des décompositions du nombre n en sommes de deux carrés rélativement premiers est donné par l'égalité

$$N_2(n) = \begin{cases} 0 & \text{lorsque } 4 \mid n \text{ ou } 4k - 1 \mid n \text{ pour } k = 1, 2, \ldots \\ 2^{\mu+2} & \text{en cas contraire.} \end{cases} \tag{4}$$

c

Or, si $n > 1$, le nombre des réprésentations de n dans la forme $x^2 + y^2 + z^2$, où $(x, y, z) = 1$ et $xyz = 0$, est égale à $\binom{3}{2} N_2(n) = 3N_2(n)$. La condition nécessaire et suffisante pour que le nombre $n > 1$ soit une somme de trois carrés positifs, rélativement premiers est donc l'inégalité $N_3(n) > 3N_2(n)$. En vertu de (3) et de (4) cette inégalité exprime que $n \not\equiv 0, 4, 7 \pmod 8$ et que $N_2(n) = 0$, où bien $p(-4n) > 1$. Vu (4) et la définition des "numeri idonei", la démonstration est achevée.

Corollaire 1. *Si $n \not\equiv 0, 4, 7 \pmod 8$, $n \neq 25$ et n a un diviseur quadratique > 1, n est une somme de trois carrés positifs, rélativement premiers.*

C'est une conséquence immédiate du Théorème 1 et du théorème de Grube ([4]), d'après lequel les nombres 9, 18, 25, 45, 72 sont les seuls "numeri idonei" ayant un diviseur quadratique impair > 1.

Remarque. Corollaire 1 affirme davantage que le théorème de Pall ([2]), à savoir que le réprésentation par la forme $x^2 + y^2 + z^2$ est propre.

Corollaire 2. *Tout nombre naturel $n \not\equiv 0, 4, 7 \pmod 8$ suffisamment grand est une somme de trois carrés positifs rélativement premiers.*

En effet, il résulte directement du Théorème 1 et du théorème de Chowla [5] * que $\lim_{d \to \infty} p(-d) = \infty$.

Corollaire 3. *Les seuls nombres naturels $n < 101200$ tels, que $n \not\equiv 0, 4, 7 \pmod 8$ et qui ne sont pas sommes de trois carrés > 0, sont les suivants*

$$1,\ 2,\ 5,\ 10,\ 13,\ 25,\ 37,\ 58,\ 85,\ 130.$$

La démonstration consiste à appliquer le Théorème 1 et les résultats de Cunningham et Cullen [7] sur les "numeri idonei" < 101200.

L'autre hypothèse de Pall [2], à savoir que tout nombre naturel $\neq 1, 25$ de la forme $8k + 1$ est somme de trois carrés > 0, résulte directement de l'hypothèse suivante :

* La démonstration de Chowla n'est pas effective (cf. [6]).

c **Hypothèse 1.** *Dans le Corollaire* 3 *la condition* $n < 101200$ *peut être supprimée.*

Théorème 2. *Pour qu'un nombre naturel n se décompose en une somme de trois carrés distincts et rélativement premiers, il faut et il suffit que n ait à la fois la propriété* (i) *et la suivante* :

(iii) *ou bien n a un diviseur premier* $\equiv 5, 7 \pmod 8$*, ou bien* $n \equiv 1, 2, 6 \pmod 8$ *et* $p(-4n) > 1$*, ou bien* $n \equiv 3 \pmod 8$ *et* $p(-n) > 1$.

La démonstration du Théorème 2 est tout à fait analogue à celle du Théorème 1. Elle est basée sur la formule pour le nombre des réprésentations de n dans la forme $x^2 + 2y^2$.

Corollaire 4. *Tout nombre* $n \not\equiv 0, 4, 7 \pmod 8$ *suffisament grand est une somme de trois carrés distincts et rélativement premiers.*

C'est une conséquence du Théorème 2 et de celui de Chowla [5].

Corollaire 5. *Les seuls nombres naturels* $n \not\equiv 0, 4, 7 \pmod 8$ *qui ne sont pas des sommes*
c *de trois carrés distincts sont les suivants* :

$$1,\ 2,\ 6,\ 9,\ 18,\ 22,\ 33,\ 57,\ 102,\ 177$$

(*pour* $n \equiv 1, 2, 5, 6 \pmod 8$ *et* $n < 101200$) ;

$$3,\ 11,\ 19,\ 27,\ 43,\ 51,\ 67,\ 99,\ 123,\ 163,\ 187,\ 267,\ 627$$

(*pour* $n \equiv 3 \pmod 8$ *et* $n < 23000$).

La démonstration consiste à appliquer le Théorème 2 et les résultats de Cunningham et Cullen [7] de même que ceux de S. B. Townes (cf. [8] p. 89).

Corollaire 6. *Les seuls nombres naturels* $n < 2875$ *qui ne sont pas des sommes de trois nombres triangulaires distincts sont les suivants* :

$$1,\ 2,\ 3,\ 5,\ 6,\ 8,\ 12,\ 15,\ 20,\ 23,\ 33,\ 78.$$

C'est une conséquence de la partie du Corollaire 5 concernant les nombres $n \equiv 3 \pmod 8$.

Si l'on admet l'hypothèse suivante :

Hypothèse 2. *Les inégalités* $n < 101200$ *et* $n < 23000$ *peuvent être supprimées dans le Corollaire* 5 *et l'inégalité* $n < 2875$ *peut l'être dans le Corollaire* 6*,*

le Corollaire 6 entraîne un théorème plus précis que celui établi dans ma communication précedente [1].

Ouvrages cités

[1] A. Schinzel, *Sur la décomposition des nombres naturels en sommes de nombres triangulaires distincts*. Bull. Acad. Polon. Sci. Cl. III 2 (1954), 409–410.

[2] G. Pall, *On sums of squares*. Amer. Math. Monthly 40 (1933), 10–18.

[3] L. E. Dickson, *History of the Theory of Numbers*. Chelsea, New York 1952.

[4] F. Grube, *Über einige Euler'sche Sätze aus der Theorie der quadratischen Formen*. Zeitschrift für Math. u. Phys. 19 (1874), 492–519.

[5] S. Chowla, *An extension of Heilbronn's Class-Number Theorem*. Q. J. Math. 5 (1934), 304–307.

[6] C. L. Siegel, *Über die Classenzahl quadratischer Zahlkörper*. Acta Arith. 1 (1935), 83–86.

[7] A. Cunningham, H. Cullen, Report of the British Association 1901, p. 552.

[8] L. E. Dickson, *Introduction to the Theory of Numbers*. Chicago 1936.

Originally published in Polish in
Roczniki Polskiego Towarzystwa Matematycznego
Seria I: Prace Matematyczne IV (1960), 45–51

On the Diophantine equation $\sum_{k=1}^{n} A_k x_k^{\vartheta_k} = 0$ *

The equations

$$\varphi = \sum_{k=1}^{n} A_k x_k^{\vartheta_k} = 0 \qquad (A_k, \vartheta_k, m_k \text{ are non-zero integers}), \tag{1}$$

$$\sum_{k=1}^{n} A_k X_k^{m_k} = 0 \tag{1'}$$

will be called *equivalent by a birational G transformation*, if there exists a mutually rational transformation in the sense of Georgiev [2] which transforms the function φ into the function

$$F = \prod_{r=1}^{n} X_r^{\mu_r} \sum_{k=1}^{n} A_k X_k^{m_k} \quad (\mu_r \text{ an integer}).$$

It is easy to prove that the above relation of equivalence is reflexive, symmetric and transitive.

It is also clear that if all solutions of equation (1) in non-zero rationals are known, then substituting them into the formulas of the appropriate birational G transformation we will obtain all solutions in non-zero rationals of an arbitrary equation equivalent to (1).

Georgiev proved ([2], p. 216) that for a birational G transformation which takes the function φ to F to exist, it is necessary and sufficient that the following condition be fulfilled:

(2) the numbers $\lambda_{r,p} = \mu_r/\vartheta_p (r \neq p)$ and $\lambda_{r,r} = (\mu_r + m_r)/\vartheta_r$ be integers,

and also that

$$\Big(1 + \sum_{k=1}^{n} \frac{\mu_k}{m_k}\Big) \prod_{i=1}^{n} m_i = \pm \prod_{i=1}^{n} \vartheta_i. \tag{3}$$

---

* Presented at the meeting of the Wrocław Branch of the Polish Mathematical Society on 3 June 1955. *Corrigendum*: Prace Mat. 44 (2004), 293–294.

The relevant transformation is then given by the formulas:

$$x_p = \prod_{r=1}^{n} X_r^{\lambda_{r,p}} \quad (1 \leqslant p \leqslant n). \tag{4}$$

c This has been deduced by Georgiev via his Theorems 3 and 10 from his Theorem 2, which needs a modification (allowing a permutation of terms in the considered sum). When this modification is made the condition (2) is replaced by

$$\begin{gathered} \text{there exists a permutation } \sigma \text{ of } \{1, 2, \ldots, n\} \text{ such that} \\ A_{\sigma(k)} = A_k \text{ for all } k \text{ and the numbers } \lambda_{r,p} = \mu_{\sigma(r)}/\vartheta_p \ (r \neq p) \\ \text{and } \lambda_{r,r} = \big(\mu_{\sigma(r)} + m_{\sigma(r)}\big)/\vartheta_r \text{ are integers} \end{gathered} \tag{2a}$$

and formula (4) by

$$x_p = \prod_{r=1}^{n} X_{\sigma(r)}^{\lambda_{r,p}} \quad (1 \leqslant p \leqslant n). \tag{4a}$$

The conditions (2) and (4) correspond to the case $\sigma(r) = r$.

We shall prove

Theorem 1. *Equation* (1) *is equivalent by a birational G transformation* (4) *to the equation*

$$\sum_{k=1}^{n} A_k X_k^{m_k} = 0, \ \textit{where } m_k = (\vartheta_k, [\vartheta_1, \ldots, \vartheta_{k-1}, \vartheta_{k+1}, \ldots, \vartheta_n]). \tag{5}$$

Moreover

$$\frac{x_p^p}{x_s^{\vartheta_s}} = \frac{X_p^{m_p}}{X_s^{m_s}} \quad (1 \leqslant p, s \leqslant n). \tag{6}$$

Proof. Let

$$\prod_{i=1}^{n} \vartheta_i = \vartheta, \quad [\vartheta_1, \ldots, \vartheta_{k-1}, \vartheta_{k+1}, \ldots, \vartheta_n] = \theta_k, \quad \prod_{i=1}^{n} m_i = m.$$

Suppose that the prime number q is a factor of ϑ_k with exponent e_k. Without loss of generality we can assume that $e_k \leqslant e_{k+1}$ for $k = 1, \ldots, n-1$. Therefore q is a factor of θ_k with exponent e_n for $k \leqslant n-1$, and e_{n-1} for $k = n$. The number q is a factor of (ϑ_k, θ_k) with exponent e_k for $k \leqslant n-1$ and e_{n-1} for $k = n$. The number q is a factor of $\theta_n m/m_n$ with the same exponent as that of m. Because q was arbitrary and the formula below is symmetric, it means that

$$\operatorname*{g.c.d.}_{k=1,\ldots,n} (\theta_k m/m_k) \mid m.$$

But $m \mid \vartheta - m$ and therefore the equation

$$m + \sum_{k=1}^{n} \xi_k \theta_k m/m_k = \vartheta \tag{7}$$

has a solution.

Let $\mu_k = \xi_k \theta_k$ correspond to some specific solution $\{\xi_k\}_{k=1,\ldots,n}$. We will show that for $j \neq k$ we have

$$m_j \vartheta_k \mid \theta_j m_k. \tag{8}$$

We distinguish two cases:

1° $k \leqslant n-1$. In this case $m_j \mid \theta_j$, and q is a factor of m_k with exponent e_k.

2° $k = n$. In this case q is a factor of θ_j with exponent e_n, of m_j with exponent e_j, therefore of the divisor with exponent $e_j + e_n$, and of the dividend with exponent $e_n + e_{n-1}$.

In both cases q is a factor of the dividend with exponent not smaller than it is a factor of the divisor, which is sufficient to establish formula (8).

Multiplying (8) by $m/m_j m_k$ we have

$$\vartheta_k m/m_k \mid \theta_j m/m_j \qquad (j \neq k)$$

and, because of (7), $\vartheta_k m/m_k \mid m + \mu_k m/m_k$, and therefore $\vartheta_k \mid \mu_k + m_k$ $(1 \leqslant k \leqslant n)$ and the numbers $\lambda_{r,r} = (\mu_r + m_r)/\vartheta_r$ are integers. Since the numbers

$$\lambda_{r,p} = \frac{\mu_r}{\vartheta_p} = \xi_r \frac{\theta_r}{\vartheta_p} \qquad (r \neq p),$$

are integers because of the way θ_r is defined, condition (2) holds.

From formula (7) we have

$$\left(1 + \sum_{k=1}^{n} \frac{\mu_k}{m_k}\right) m = \vartheta,$$

so also condition (3) holds, which finishes the proof of the first part of the theorem.

By formulas (4) and (2) we have

$$\frac{x_p^{\vartheta_p}}{x_s^{\vartheta_s}} = \frac{\prod_{r=1}^{n} X_r^{\vartheta_p \lambda_{r,p}}}{\prod_{r=1}^{n} X_r^{\vartheta_s \lambda_{r,s}}} = \prod_{r=1}^{n} X_r^{\vartheta_p \lambda_{r,p} - \vartheta_s \lambda_{r,s}} = \frac{X_p^{m_p}}{X_s^{m_s}}$$

which finishes the proof of the second part of the theorem. □

Theorem 2. *The equations*

$$\sum_{k=1}^{n} A_k x_k^{\vartheta_k} = 0 \tag{1}$$

and

$$\sum_{k=1}^{n} A_k y_k^{\eta_k} = 0 \qquad (\eta_k \text{ non-zero integers}) \tag{9}$$

are equivalent by a birational G transformation of the form

$$x_p = \prod_{r=1}^{n} y_r^{k_{r,p}} \qquad (1 \leqslant p \leqslant n) \tag{10}$$

if and only if, for $k = 1, \ldots, n$

(11) $$m_k = l_{\sigma(k)},$$

where $m_k = (\vartheta_k, [\vartheta_1, \ldots, \vartheta_{k-1}, \vartheta_{k+1}, \ldots, \vartheta_n])$, $l_k = (\eta_k, [\eta_1, \ldots, \eta_{k-1}, \eta_{k+1}, \ldots, \eta_n])$ *and* $\sigma(k)$ *is a permutation of* $\{1, 2, \ldots, n\}$ *such that* $A_{\sigma(k)} = A_k$ *for all* k.

Then we have

(12) $$\frac{x_p^{\vartheta_p}}{x_s^{\vartheta_s}} = \frac{y_{\sigma(p)}^{\eta_{\sigma(p)}}}{y_{\sigma(s)}^{\eta_{\sigma(s)}}}.$$

Proof. By Theorem 1, equation (1) is equivalent to

(5) $$\sum_{k=1}^{n} A_k X_k^{m_k} = 0,$$

and equation (9) is equivalent to the equation

(13) $$\sum_{k=1}^{n} A_k Y_k^{l_k} = 0.$$

By reflexivity, symmetry and transitivity of the equivalence considered, the sufficiency of condition (11) is obvious. By formula (6), formula (12) is also obvious.

To show the necessity of condition (11), suppose that equations (1) and (9) are equivalent. It then follows that equations (1) and (13) are equivalent, and (5) and (9) are equivalent too.

Replacing in condition (2a) m_r by l_r and μ_r by λ_r we have $\vartheta_p \mid \lambda_{\sigma(r)}$ $(r \neq p)$, hence $\theta_r \mid \lambda_{\sigma(r)}$ and $m_r \mid \lambda_{\sigma(r)}$ and $\vartheta_r \mid \lambda_{\sigma(r)} + l_{\sigma(r)}$, thus $m_r \mid \lambda_{\sigma(r)} + l_{\sigma(r)}$. Therefore, $m_r \mid l_{\sigma(r)}$.

From the equivalence of (5) and (9) it follows similarly that $l_r \mid m_{\tau(r)}$, where τ is a permutation of $\{1, 2, \ldots, k\}$ such that $A_{\tau(r)} = A_r$ for all r. Thus $m_r \mid m_{\tau(\sigma(r))}$ for all r, which gives $m_{\tau(\sigma(r))} = m_r$ and $l_{\sigma(r)} = m_r$. □

Theorem 2 immediately implies Theorem 12 from the quoted paper of Georgiev [2].

By formula (12) we also have:

Corollary 1. *If equations* (1) *and* (9) *are equivalent by a birational G transformation* (10)*,* A_k *are distinct, and* x_s *and* y_s *are greater than zero, then* $x_p^{\vartheta_p} > x_s^{\vartheta_s}$ *if and only if* $y_p^{\eta_p} > y_s^{\eta_s}$.

We assign the solutions $\{x_k\}_{k=1,2,\ldots,n}$, $\{x'_k\}_{k=1,2,\ldots,n}$ of equation (1) (respectively $\{y_k\}_{k=1,2,\ldots,n}$, $\{y'_k\}_{k=1,2,\ldots,n}$ of equation (9)) to the same class, if and only if

$$\frac{x'^{\vartheta_p}_p}{x_p^{\vartheta_p}} = \frac{x'^{\vartheta_1}_1}{x_1^{\vartheta_1}} \qquad \left(\text{resp.} \quad \frac{y'^{\eta_p}_p}{y_p^{\eta_p}} = \frac{y'^{\eta_1}_1}{y_1^{\eta_1}}\right) \qquad (1 \leqslant p \leqslant n).$$

Writing this condition in the form

$$\frac{x'^{\vartheta_p}_p / x'^{\vartheta_1}_1}{x_p^{\vartheta_p} / x_1^{\vartheta_1}} = 1 \qquad \left(\text{resp.} \quad \frac{y'^{\eta_p}_p / y'^{\eta_1}_1}{y_p^{\eta_p} / y_1^{\eta_1}} = 1\right)$$

by formula (12) we have

Corollary 2. *Under a birational G transformation of the form* (10)*, which gives the equivalence of* (1) *and* (9)*, every class of solutions of equation* (9) *maps to a class of solutions of equation* (1).

Now suppose that in equation (1) we have $(\vartheta_n, \vartheta_1 \cdot \dots \cdot \vartheta_{n-1}) = 1$ $(n > 1)$. Therefore $m_n = (\vartheta_n, [\vartheta_1, \dots, \vartheta_{n-1}]) = 1$, and by Theorem 1 equation (1) is equivalent by a birational G transformation to the equation

$$\sum_{k=1}^{n-1} A_k X_k^{m_k} + A_n X_n = 0, \tag{14}$$

all of whose rational solutions are given by the formulas:

$$X_k = t_k \quad (1 \leqslant k \leqslant n-1), \qquad X_n = \frac{-\sum_{k=1}^{n-1} A_k t_k^{m_k}}{A_n},$$

where t_k $(1 \leqslant k \leqslant n-1)$ are rational parameters.

The case $n = 2$ gives one class of solutions of equation (14), the case $n = 3$, $m_1 = m_2 = 1$ was considered by L. Tchacaloff and C. Karanicoloff [3], the case $n \geqslant 3$ and $m_k = g$ $(1 \leqslant k \leqslant n-1)$ was considered by N. M. Basu [1], the general case was considered by T. Vijayaraghavan [4].

For $n \geqslant 3$ equation (14) has infinitely many classes of rational solutions. Therefore from Corollary 2 and the observation that every class of rational solutions of equation (1) contains integer solutions, it follows that

Corollary 3. *If* $n \geqslant 3$ *and if* $(\vartheta_n, \vartheta_1 \cdot \dots \cdot \vartheta_{n-1}) = 1$*, then equation* (1) *has infinitely many classes of integer solutions.*

References

[1] N. M. Basu, *On a Diophantine equation*. Bull. Calcutta Math. Soc. 32 (1940), 15–20.

[2] G. Georgiev, *O rozwiązaniu w liczbach wymiernych pewnych równań diofantycznych* (*On the solution in rational numbers of certain Diophantic equations*). Prace Mat. 1 (1955), 201–238 (Polish).

[3] L. Tchacaloff et C. Karanicoloff, *Résolution de l'équation* $Ax^m + By^n = z^p$ *en nombres rationnels*. C. R. Acad. Sci. Paris 210 (1940), 281–283.

[4] T. Vijayaraghavan, *The general rational solution of some Diophantine equations of the form* $\sum_{r=1}^{k+1} A_r x_r^{n_r} = 0$. Proc. Indian Acad. Sci., Sect. A. 12 (1940), 284–289.

Originally published in
Acta Arithmetica IX (1964), 107–116

Polynomials of certain special types

with H. Davenport (Cambridge) and D. J. Lewis (Ann Arbor)*

1.

Let $f(x)$ be a polynomial with integral coefficients. It is well known that if $f(x)$ is a k-th power for every positive integer x, then $f(x) = \big(g(x)\big)^k$ identically, where $g(x)$ has integral coefficients. For proofs and references, see Pólya and Szegö [8], Section VIII, Problems 114 and 190; also Fried and Surányi [2].

In this connection, we shall prove the following general theorem:

Theorem 1. *Let $f(x, y)$ be a polynomial with integral coefficients. Suppose that every arithmetical progression contains some integer x such that the equation $f(x, y) = 0$ has an integral solution in y. Then there exists a polynomial $g(x)$ with rational coefficients such that*

$$f\big(x, g(x)\big) = 0 \tag{1}$$

identically.

Corollary. *Let $k > 1$ be an integer and let $f(x)$ be a polynomial with integral coefficients. Suppose that every arithmetical progression contains some integer x such that $f(x)$ is a k-th power. Then $f(x) = \big(g(x)\big)^k$ identically, where $g(x)$ is a polynomial with integral coefficients.*

Professor LeVeque raised the question (in conversation) whether, if $f(x)$ is representable as a sum of two squares for every positive integer x, or for every sufficiently large integer x, then $f(x)$ is identically a sum of two squares. We shall prove that this is true, and we shall deduce it from the following general theorem.

Theorem 2. *Let K be any normal algebraic number field of degree n, with integral basis $\omega_1, \omega_2, \ldots, \omega_n$, and let*

$$N(u_1, u_2, \ldots, u_n) = \operatorname{norm}(u_1\omega_1 + u_2\omega_2 + \ldots + u_n\omega_n)$$

* This author was partially supported by a grant from the National Science Foundation.

denote the norm-form corresponding to K. Let $f(x)$ be a polynomial with rational coefficients, and suppose that every arithmetical progression contains an integer x such that

$$f(x) = N(u_1, u_2, \ldots, u_n)$$

for some rational numbers $u_1, u_2, \ldots, u_n$. Suppose further that either K is cyclic or the multiplicity of every zero of $f(x)$ is relatively prime to n. Then

$$f(x) = N\big(u_1(x), u_2(x), \ldots, u_n(x)\big)$$

identically, where $u_1(x)$, $u_2(x)$, …, $u_n(x)$ are polynomials with rational coefficients.

We observe that the hypotheses on K are always satisfied if K is normal and of prime degree n.

The two alternatives in the hypothesis—one relating to K and the other to $f(x)$ —are appropriate conditions to impose, in the sense that if both are violated, the conclusion may not hold. This is shown by the example (see §6)

$$f(x) = x^2, \quad K = \mathbb{Q}(e^{2\pi i/8}),$$

where $\mathbb{Q}$ denotes the rational number field.

The property of $f(x)$ postulated in the theorem implies the solubility of the congruence

$$f(x) \equiv N(u_1, \ldots, u_n) \pmod{m}$$

in $u_1, \ldots, u_n$ for every integer x and every positive integer m. The congruence is to be understood in the multiplicative sense; see Hasse [3], 25, footnote *. If K is cyclic, then by a theorem of Hasse [4] this implies the apparently stronger statement that for every x we have

$$f(x) = N(v_1, \ldots, v_n)$$

for some rational $v_1, \ldots, v_n$. Thus when K is cyclic, we have three apparently different conditions on $f(x)$ which are in reality equivalent.

Corollary to Theorem 2. *Let $f(x)$ be a polynomial with integral coefficients, and suppose that every arithmetical progression contains an integer x such that $f(x)$ is a sum of two squares. Then*

$$f(x) = u_1^2(x) + u_2^2(x)$$

identically, where $u_1(x)$ and $u_2(x)$ are polynomials with integral coefficients.

In the particular case of Theorem 2, namely the case $K = \mathbb{Q}(i)$, which is needed for this Corollary, our method of proof has much in common with that used by Lubelski [7] in his investigation of the primes p for which $f(x) \equiv 0 \pmod{p}$ is soluble.

It will be seen that in the conclusion of the Corollary, it is asserted that $u_1(x)$, $u_2(x)$ have *integral* coefficients. In the more general Theorem 2, if it is postulated that $f(x)$ has integral coefficients and that $u_1, \ldots, u_n$ are integers, it is not in general possible to draw the conclusion with $u_1(x), \ldots, u_n(x)$ having integral coefficients. This is illustrated by

the example (see §6)

$$f(x) = 2x^2(x+1)^2 + 3x(x+1) + 4, \quad K = \mathbb{Q}(\sqrt{-23}).$$

However, it is possible to draw the conclusion stated above if the highest coefficient in $f(x)$ is 1. This can be proved by first comparing the highest terms on both sides, and then appealing to Gauss's lemma.

There are other problems, of the same general character as those considered in this paper, which we are quite unable to attack. The simplest of them is that in which $f(x)$ is representable as a sum of two integral cubes for every sufficiently large integer x.

2.

Proof of Theorem 1. We note first that the hypothesis implies that every arithmetical progression contains infinitely many integers x such that the equation has an integral solution in y. For if d is the common difference of the progression, and x_0 is one integer with the property, there exists an integer $x_n \equiv x_0 + d^n \pmod{d^{n+1}}$ for $n = 1, 2, \ldots$ which has the property, and the integers x_n are all distinct.

We factorize $f(x, y)$ into a product of powers of polynomials which are irreducible over the rational field $\mathbb{Q}$; by Gauss's lemma we can take these polynomials to have integral coefficients. We can omit any factor $f_0(x, y)$ for which the equation $f_0(x, y) = 0$ has only finitely many integral solutions, since its omission will not invalidate the hypothesis. We can also omit any factor which does not contain y. Hence we can take

$$f(x, y) = f_1(x, y) f_2(x, y) \cdots f_k(x, y), \tag{2}$$

where $f_1(x, y), \ldots, f_k(x, y)$ are irreducible over $\mathbb{Q}$ and are such that each of the equations $f_j(x, y) = 0$ has infinitely many integral solutions.

It follows from Hilbert's Irreducibility Theorem (Hilbert [5], p. 275; for references to later work, see Lang [6], pp. 163–164) that there exists an integer x_0 such that all the polynomials $f_j(x_0, y)$, considered as polynomials in y, are irreducible over $\mathbb{Q}$ and are of the same degree in y as $f_j(x, y)$. Suppose first that all these degrees are greater than 1, and let n_j denote the degree of $f_j(x_0, y)$ in y.

Let η be a root of $f_j(x_0, \eta) = 0$, and consider the prime ideal factorization of a rational prime p in $\mathbb{Q}(\eta)$ and in its least normal extension $\mathbb{Q}^*(\eta)$. Let d_r denote the density (in the Dirichlet series sense) of those primes which have exactly r prime ideal factors of the first degree in $\mathbb{Q}(\eta)$. Then (Hasse [3], p. 129)

$$\sum_{r=0}^{n} d_r = 1, \quad \sum_{r=0}^{n} r d_r = 1.$$

To prove that $d_0 > 0$, it will suffice to prove that $d_1 < 1$. Now any large prime p which has just one prime ideal factor of degree 1 in $\mathbb{Q}(\eta)$ will have some prime ideal factor of degree greater than 1 in $\mathbb{Q}(\eta)$, and so also in $\mathbb{Q}^*(\eta)$. Since $\mathbb{Q}^*(\eta)$ is normal, *all* prime ideal factors of p in $\mathbb{Q}^*(\eta)$ will be of degree greater than 1, and the density of such p is exactly $1 - 1/n_j^*$, where n_j^* denotes the degree of $\mathbb{Q}^*(\eta)$ (Hasse [3], pp. 138–139). Hence

$d_1 \leqslant 1 - 1/n_j^*$, whence the result. In particular, there are infinitely many primes which have no prime ideal factor of the first degree in $\mathbb{Q}(\eta)$.

By a well-known principle of Dedekind, if q_j is such a prime (and is sufficiently large) we have

$$f_j(x_0, y) \not\equiv 0 \pmod{q_j} \tag{3}$$

for all integers y. There is such a prime q_j for each j. On the other hand, the hypothesis of the theorem implies that the arithmetical progression

$$x \equiv x_0 \pmod{q_1 q_2 \cdots q_k}$$

contains an integer x such that $f(x, y) = 0$ for some integer y. But then $f_j(x, y) = 0$ for some j, whence

$$f_j(x_0, y) \equiv f_j(x, y) \equiv 0 \pmod{q_j},$$

contrary to (3).

It follows that there is some j for which $f_j(x, y)$ is linear in y, say

$$f_j(x, y) = yA(x) - B(x),$$

where $A(x)$, $B(x)$ are relatively prime polynomials with integral coefficients. There exist polynomials $A_1(x)$, $B_1(x)$ with integral coefficients such that

$$A(x)A_1(x) + B(x)B_1(x) = c$$

identically, where c is a non-zero constant. If x is an integer for which there is an integer y satisfying $f_j(x, y) = 0$, then $A(x)$ must divide c, and since this happens for infinitely many x, it follows that $A(x)$ is a constant. Hence

$$f_j\big(x, g(x)\big) = 0$$

identically, where $g(x)$ is the polynomial $B(x)/A$. This proves Theorem 1. □

The deduction of the Corollary is immediate, since we get $f(x) = \big(g(x)\big)^k$, where $g(x)$ has rational coefficients, and then it follows from Gauss's lemma that $g(x)$ has integral coefficients.

3.

Lemma 1. *Suppose that the hypotheses of Theorem* 2 *hold. Let*

$$f(x) = c\big(f_1(x)\big)^{e_1}\big(f_2(x)\big)^{e_2} \cdots \big(f_m(x)\big)^{e_m}, \tag{4}$$

where $c \neq 0$ is a rational number and $f_1(x)$, $f_2(x)$, …, $f_m(x)$ are distinct primitive polynomials with integral coefficients, each irreducible over $\mathbb{Q}$, and where $e_1, e_2, \ldots, e_m$ are positive integers. For any j, let q be a sufficiently large prime for which the congruence

$$f_j(x) \equiv 0 \pmod{q} \tag{5}$$

is soluble. If $(e_j, n) = 1$ then q factorizes completely in K into prime ideals of the first degree. If K is cyclic then q factorizes completely into prime ideals of the first degree in the unique subfield K_j of K of degree $n/(e_j, n)$.

Proof. Put

$$F(x) = f_1(x) f_2(x) \cdots f_m(x).$$

Since the discriminant of $F(x)$ is not zero, there exist polynomials $\varphi(x)$, $\psi(x)$ with integral coefficients such that

$$F(x)\varphi(x) + F'(x)\psi(x) = D \tag{6}$$

identically, where D is a non-zero integer.

Let q be a large prime for which the congruence (5) is soluble, and let x_0 be a solution. By (6) we have $F'(x_0) \not\equiv 0 \pmod{q}$, whence

$$F(x_0 + q) \not\equiv F(x_0) \pmod{q^2}.$$

By choice of x_1 as either x_0 or $x_0 + q$, we can ensure that

$$f_j(x_1) \equiv 0 \pmod{q}, \quad F(x_1) \not\equiv 0 \pmod{q^2},$$

whence

$$f_j(x_1) \not\equiv 0 \pmod{q^2} \quad \text{and} \quad f_i(x_1) \not\equiv 0 \pmod{q} \text{ for } i \neq j.$$

By the hypothesis of Theorem 2, there exists $x_2 \equiv x_1 \pmod{q^2}$ such that

$$f(x_2) = N(u_1, u_2, \ldots, u_n) \tag{7}$$

for some rational $u_1, u_2, \ldots, u_n$. From the preceding congruences we have

$$f_j(x_2) \equiv 0 \pmod{q}, \quad f_j(x_2) \not\equiv 0 \pmod{q^2},$$
$$f_i(x_2) \not\equiv 0 \pmod{q} \quad \text{for } i \neq j.$$

Hence

$$f(x_2) \equiv 0 \pmod{q^{e_j}}, \quad f(x_2) \not\equiv 0 \pmod{q^{e_j+1}}. \tag{8}$$

Let the prime ideal factorization of q in K be

$$q = \mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_l; \tag{9}$$

the factors are distinct since q is supposed to be sufficiently large. We note that l divides n because K is a normal field, and that

$$N\mathfrak{q}_i = q^{n/l}. \tag{10}$$

Write the prime ideal factorization of $u_1\omega_1 + \ldots + u_n\omega_n$ in K in the form

$$u_1\omega_1 + \ldots + u_n\omega_n = \mathfrak{q}_1^{\alpha_1} \cdots \mathfrak{q}_l^{\alpha_l} \mathfrak{a}\mathfrak{b}^{-1},$$

where $\mathfrak{a}$, $\mathfrak{b}$ are ideals in K which are relatively prime to q. Then

$$N(u_1\omega_1 + \ldots + u_n\omega_n) = \pm q^{n(\alpha_1+\ldots+\alpha_l)/l} N\mathfrak{a}(N\mathfrak{b})^{-1}, \tag{11}$$

and $N\mathfrak{a}$, $N\mathfrak{b}$ are relatively prime to q.

It follows from (7), (8), (11) that

$$n(\alpha_1 + \ldots + \alpha_l)/l = e_j,$$

whence

$$\frac{n}{(e_j, n)} \text{ divides } l.$$

If $(e_j, n) = 1$ we get that n divides l, whence $l = n$ and it follows from (9) and (10) that q factorizes completely in K into prime ideal factors of the first degree.

Now suppose that K is cyclic ([1]). The Galois group of K is a cyclic group $\mathscr{G}$ of order n; it has a unique subgroup $\mathscr{H}$ of order n/l, and each $\mathfrak{q}_i$ is invariant under the automorphisms of $\mathscr{H}$. The subgroup $\mathscr{H}$ determines a subfield L of K, of degree l, and $\mathscr{H}$ is the Galois group of K relative to L. A prime ideal factor of q in L cannot split further in K, since any such factors would be derived from one another by the automorphisms of $\mathscr{H}$ and so would not be distinct. Hence the factorization of q in L is also of the form (9). Comparison of norms shows that the $\mathfrak{q}_i$, considered as prime ideals in L, are of the first degree.

The unique subfield K_j of K, of degree $n/(e_j, n)$, is a subfield of L, and therefore q also factorizes completely in K_j, the number of prime ideal factors being equal to the degree of K_j and each being of the first degree.

This completes the proof of Lemma 1. □

Lemma 2. *Let $G(x)$ be a polynomial with integral coefficients, irreducible over $\mathbb{Q}$, and let $G(\theta) = 0$. Let J be any subfield of $\mathbb{Q}(\theta)$. Then*

$$G(x) = aN_J\big(H(x)\big) \tag{12}$$

identically, where $H(x)$ is a polynomial over J, and N_J denotes the norm from J to $\mathbb{Q}$, extended in the obvious way to apply to $J[x]$, and a is rational.

Proof. Let ω be a generating element of J and let $\omega^{(1)} = \omega, \ldots, \omega^{(m)}$ be the conjugates of ω, where m is the degree of J. Since J is contained in $\mathbb{Q}(\theta)$, we have

$$\omega = g(\theta),$$

where g is a polynomial with rational coefficients. Thus $G(x)$ has a zero in common with the polynomial

$$\prod_{j=1}^{m}\big(g(x) - \omega^{(j)}\big), \tag{13}$$

which has rational coefficients, and since $G(x)$ is irreducible, it must divide this polynomial.

The factors of (13) are relatively prime in pairs, since their differences are non-zero constants. Hence the polynomials

$$H^{(j)}(x) = \big(G(x), g(x) - \omega^{(j)}\big)$$

are relatively prime in pairs, and since each of them divides $G(x)$, their product must

([1]) In dealing with this case we do not need to exclude the possibility that $(e_j, n) = 1$.

divide $G(x)$. Thus

$$G(x) = A(x) \prod_{j=1}^{m} H^{(j)}(x) = A(x) N_J\big(H^{(1)}(x)\big).$$

The norm on the right is a non-constant polynomial with rational coefficients, so it follows from the irreducibility of $G(x)$ that $A(x)$ is a constant. This proves the result. □

Lemma 3 (Bauer). *Let J be a normal number field and let k be any number field. Suppose that every sufficiently large prime which has at least one prime ideal factor of the first degree in k also has at least one prime ideal factor of the first degree in J. Then J is contained in k.*

Proof. See Bauer [1] or Hasse [3], pp. 138 and 141. □

4.

Proof of Theorem 2. Let $f(x)$ be the polynomial of the theorem, and $f_j(x)$ any one of its irreducible factors, as in (4). Let θ be any zero of $f_j(x)$ and q any large prime which has at least one prime ideal factor of the first degree in $\mathbb{Q}(\theta)$. Then by Dedekind's theorem the congruence

$$f_j(x) \equiv 0 \pmod{q}$$

is soluble.

If $(e_j, n) = 1$, it follows from Lemma 1 that q factorizes completely in the field K. By Lemma 3, with $J = K$ and $k = \mathbb{Q}(\theta)$, this implies that K is contained in $\mathbb{Q}(\theta)$. It follows now from Lemma 2, with $G(x) = f_j(x)$, that $f_j(x)$ is expressible identically in the form

$$f_j(x) = a_j N_K\big(H_j(x)\big),$$

as in (12). Hence

$$\big(f_j(x)\big)^{e_j} = a_j^{e_j} N_K\big(H_j^{e_j}(x)\big) = b_j N_K\big(H_j^*(x)\big). \tag{14}$$

Now suppose that K is cyclic. It follows from Lemma 1 that q factorizes completely in the field K_j. By Lemma 3 with $J = K_j$ and $k = \mathbb{Q}(\theta)$, this implies that K_j is contained in $\mathbb{Q}(\theta)$. It follows now from Lemma 2, with $G(x) = f_j(x)$, that $f_j(x)$ is expressible identically in the form

$$f_j(x) = a_j N_{K_j}\big(H_j(x)\big).$$

Now

$$N_K\big(H_j(x)\big) = \big\{N_{K_j}\big(H_j(x)\big)\big\}^{(e_j,n)},$$

since the degree of K relative to K_j is (e_j, n). Hence

$$\big(f_j(x)\big)^{e_j} = a_j^{e_j} \big\{N_K\big(H_j(x)\big)\big\}^{e_j/(e_j,n)} = b_j N_K\big(H_j^*(x)\big). \tag{15}$$

The conclusions (14) and (15), reached on two alternative hypotheses, are the same. By (4) and the multiplicative property of the norm, we have

$$f(x) = aN_K\big(h(x)\big),$$

where $h(x)$ is a polynomial over K. By the hypothesis of the theorem, taking x to be a suitable integer, we infer that a is the norm of an element α of K. Putting

$$\alpha h(x) = \omega_1 u_1(x) + \ldots + \omega_n u_n(x),$$

we obtain

$$f(x) = N\big(u_1(x), \ldots, u_n(x)\big)$$

identically. □

5.

Proof of the Corollary to Theorem 2. It follows from the theorem, on taking $K = \mathbb{Q}(i)$, that

$$f(x) = U_1^2(x) + U_2^2(x),$$

where U_1, U_2 are polynomials with rational coefficients. Let

$$U_1(x) + iU_2(x) = \alpha v(x),$$

where $v(x)$ is a primitive polynomial whose coefficients are integers in $\mathbb{Q}(i)$ and α is an element of $\mathbb{Q}(i)$. Then

$$f(x) = |\alpha|^2 v(x)\bar{v}(x).$$

Since $v(x)$ and $\bar{v}(x)$ are both primitive and $f(x)$ has integral coefficients, it follows from Gauss's lemma that $|\alpha|^2$ is an integer. But $|\alpha|^2$ is a sum of two rational squares, and so it must be a sum of two integral squares, i.e. $|\alpha|^2 = |\beta|^2$, where β is an integer in $\mathbb{Q}(i)$. Putting

$$\beta v(x) = u_1(x) + iu_2(x),$$

where u_1, u_2 are polynomials with (rational) integral coefficients, we get

$$f(x) = u_1^2(x) + u_2^2(x).$$ □

6. Two examples

(1) Suppose that

$$f(x) = x^2, \quad K = \mathbb{Q}(e^{2\pi i/8}).$$

We prove first that every square is expressible as a value of the norm form of K. This norm form is

$$N\big(u_1 + \sqrt{i}u_2 + iu_3 + \sqrt{i^3}u_4\big) = (u_1^2 - u_3^2 + 2u_2u_4)^2 + (u_2^2 - u_4^2 - 2u_1u_3)^2.$$

Plainly 2^2 is representable with $u_1 = u_3 = 0$, $u_2 = u_4 = 1$.

Also if p is a prime and $p \equiv 1 \pmod 4$ then $p = a^2 + b^2$ and p^2 is representable with $u_1 = u_3 = 0$, $u_2 = a$, $u_4 = b$. Finally, if $p \equiv 3 \pmod 4$ then p is representable either as $a^2 - 2b^2$ or as $a^2 + 2b^2$, and we take $u_1 = b$, $u_3 = \pm b$, $u_2 = a$, $u_4 = 0$.

On the other hand, x^2 is not representable in the form

$$x^2 = N\big(u_1(x), \ldots, u_4(x)\big),$$

where $u_1(x)$, …, $u_4(x)$ are polynomials with rational coefficients. For if the greatest degree of any of these polynomials is $g \geqslant 1$, then the coefficient of x^{4g} on the right is $N(c_1, \ldots, c_4)$, where $c_1, \ldots, c_4$ are rational numbers, not all zero, and this coefficient is not 0.

In this example, K is normal but not cyclic, and the multiplicity of the zero of $f(x)$ is not relatively prime to the degree (namely 4) of K.

(2) Suppose that

$$f(x) = 2x^2(x+1)^2 + 3x(x+1) + 4, \quad K = \mathbb{Q}\big(\sqrt{-23}\big).$$

Here the norm form of K is

$$N(u_1, u_2) = u_1^2 + u_1u_2 + 6u_2^2.$$

For every integer x we have $x(x+1) = 2t$, where t is an integer, and

$$f(x) = 8t^2 + 6t + 4 = N(t+2, t).$$

On the other hand, if $u_1(x)$, $u_2(x)$ are polynomials in x with *integral* coefficients, the coefficient of the highest power of x in $N\big(u_1(x), u_2(x)\big)$ is an integer of the form

$$a^2 + ab + 6b^2,$$

and cannot be 2, since the least positive integer other than 1 represented by this form is 6.

References

[1] M. Bauer, *Zur Theorie der algebraischen Zahlkörper*. Math. Ann. 77 (1916), 353–356.

[2] E. Fried, J. Surányi, *Neuer Beweis eines zahlentheoretischen Satzes über Polynome*. Mat. Lapok 11 (1960), 75–84 (Hungarian).

[3] H. Hasse, *Bericht über Klassenkörpertheorie* II. Jahresber. Deutsch. Math.-Verein., suppl. vol. 6 (1930).

[4] —, *Beweis eines Satzes und Widerlegung einer Vermutung über das allgemeine Normenrestsymbol*. Göttinger Nachr., 1931, 64–69.

[5] D. Hilbert, *Über die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten*. J. Reine Angew. Math. 110 (1892), 104–129; Ges. Abhandlungen II, 264–286. Chelsea, New York 1965.

[6] S. Lang, *Diophantine Geometry*. Interscience, New York and London 1962.

[7] S. Lubelski, *Zur Reduzibilität von Polynomen in der Kongruenztheorie*. Acta Arith. 1 (1936), 169–183, and 2 (1938), 242–261.

[8] G. Pólya, G. Szegö, *Aufgaben und Lehrsätze aus der Analysis*, II. Springer, Berlin 1954.

Originally published in
Commentarii. Pontificia Academia Scientiarum
II:20 (1969), 1–9

An improvement of Runge's theorem on Diophantine equations

Summarium. Auctor investigat quando aequatio cum duabus variabilibus infinitum solutionum integralium numerum habere possit.

I

The first general result concerning the number of integer solutions of a Diophantine equation is due to Runge [3] and in its simplest form is as follows.

(i) If $f(x, y)$ is a polynomial with integer coefficients irreducible in the rational field and the equation $f(x, y) = 0$ has infinitely many integer solutions, then the highest homogeneous part of $f(x, y)$ is up to a constant factor a power of an irreducible form.

The more general formulation refers to the highest isobaric part of $f(x, y)$.

The final result permitting to decide whether any given equation $f(x, y) = 0$ has infinitely many integer solutions is due to Siegel [4] and is as follows.

(ii) If $f(x, y) = 0$ has infinitely many integer solutions, then there exist rational functions $R(t)$, $S(t)$ not both constant such that

$$f\big(R(t), S(t)\big) = 0 \tag{1}$$

identically in t and either

$$R(t) = \frac{A(t)}{L(t)^m}, \quad S(t) = \frac{B(t)}{L(t)^m} \tag{2}$$

or

$$R(t) = \frac{C(t)}{Q(t)^m}, \quad S(t) = \frac{D(t)}{Q(t)^m}, \tag{3}$$

where A, B, C, D, L, Q are polynomials with integer coefficients, L is linear, Q irreducible indefinite quadratic.

The aim of this note is to deduce from the two above results the following improvement of the first one.

Paper presented on October 17th, 1968 by Pontifical Academician H.E. Wacław Sierpiński.

Theorem. *If $f(x, y)$ is a polynomial with integer coefficients irreducible in the rational field and the equation $f(x, y) = 0$ has infinitely many integer solutions then the highest homogeneous part of $f(x, y)$ is up to a constant factor a power of a linear or irreducible indefinite quadratic form.*

Proof. Let $f(x, y)$ have degree n and denote by $f_n(x, y)$ its highest homogeneous part. By (i) either $f_n(x, y) = ax^n$ or $f_n(x, y) = by^n$ or

$$f_n(x, y) = ax^n + \ldots + by^n \quad (ab \neq 0). \tag{4}$$

It remains to consider the last case. By (ii) we have (1) where either

1. R, S are polynomials not both constant or
2. (2) holds with $m > 0$, $(A, B, L) = 1$ or
3. (3) holds with $m > 0$, $(C, D, Q) = 1$.

In the case 1. it follows from (1) and (4) that R and S are of the same degree. Denoting this degree by d and the leading coefficients of R and S by r and s, respectively, we get

$$f_n(r, s) = \lim_{t=\infty} t^{-nd} f\big(R(t), S(t)\big) = 0.$$

Hence $f_n(x, y)$ is divisible by $sx - ry$ and by (i)

$$f_n(x, y) = c(sx - ry)^n.$$

In the case 2. let t_0 be the zero of $L(t)$. Clearly $A(t_0) \neq 0$ or $B(t_0) \neq 0$. Multiplying (1) by $L(t)^{mn}$ and substituting afterwards $t = t_0$ we obtain

$$f_n\big(A(t_0), B(t_0)\big) = 0.$$

Hence $f_n(x, y)$ is divisible by $B(t_0)x - A(t_0)y$ and by (i)

$$f_n(x, y) = c\big(B(t_0)x - A(t_0)y\big)^n.$$

In the case 3. let t_1, t_2 be the zeros of $Q(t)$. Clearly

$$C(t_i) \neq 0 \text{ or } D(t_i) \neq 0 \quad (i = 1, 2).$$

Multiplying (1) by $Q(t)^{mn}$ and substituting afterwards $t = t_i$ we obtain

$$f_n\big(C(t_i), D(t_i)\big) = 0 \quad (i = 1, 2).$$

Hence $f_n(x, y)$ is divisible by $D(t_i)x - C(t_i)y$ and by (4) $D(t_i) \neq 0$ $(i = 1, 2)$. If $C(t_1)D(t_1)^{-1}$ is rational then by (i)

$$f_n(x, y) = c\big(D(t_1)x - C(t_1)y\big)^n.$$

If $C(t_1)D(t_1)^{-1}$ is irrational, the $C(t_i)D(t_i)^{-1}$ are conjugate in a real quadratic field and by (1)

$$f_n(x, y) = c\big[\big(D(t_1)x - C(t_1)y\big)\big(D(t_2)x - C(t_2)y\big)\big]^{n/2}.$$

Corollary. *If $f_n(x, y)$ is an irreducible form of degree $n > 2$ and $g(x, y)$ is a polynomial with integer coefficients of degree $m < n$ then the equation*

$$f_n(x, y) = g(x, y)$$

has only finitely many integer solutions.

The corollary represents an improvement on the analogous results with Roth [2] deduced from his famous theorem; this had stronger hypothesis $m < n - 2$.

I conclude by expressing my thanks to Professors H. Davenport and D. J. Lewis for their helpful suggestion and in particular for pointing out the corollary which they were
c first to prove.

II

In this second part I wish to extend the result of the first part so as to improve on Runge's theorem in its full generality.

Let $f(x, y)$ be a polynomial with integer coefficients irreducible in the rational field and suppose that the equation $f(x, y) = 0$ has infinitely many integer solutions. Then according to Runge [3] (see [6], p. 89):

(1) the highest terms in x and y occur in f separately as ax^m, by^n;

(2) each branch of the algebraic function y of x defined by $f = 0$ tends to infinity with x and is of order $x^{m/n}$, every term $cx^\rho y^\sigma$ in f has $n\rho + m\sigma \leqslant mn$;

(3) the sum $g(x, y)$ of the terms with $n\rho + m\sigma = mn$ is expressible as

$$b\prod_\beta \left(y^\nu - d^{(\beta)}x^\mu\right) \quad (\beta = 1, \ldots, \tfrac{n}{\nu}),$$

where $\prod_\beta \left(u - d^{(\beta)}\right)$ is a power of an irreducible polynomial.

Runge does not say explicitly that

$$\frac{n}{\nu} = \frac{m}{\mu} = (m, n),$$

c but what he really proves is that $g(x, y)$ is up to a constant factor a power of an irreducible polynomial (for another proof see Skolem [5]). Therefore, factorizing if necessary $y^\nu - d^{(\beta)}x^\mu$ we can conclude that

$$g(x, y) = bh\left(x^{m/d}, y^{n/d}\right)^\lambda, \quad d = (m, n), \tag{4}$$

where $h(u, v)$ is an irreducible form. We shall prove:

Theorem. *If $f(x, y)$ is a polynomial with integer coefficients irreducible in the rational field, of degree m in x and n in y, and the equation $f(x, y) = 0$ has infinitely many integer solutions then* (1) *and* (2) *hold and the sum $g(x, y)$ of all terms $cx^\rho y^\sigma$ of f with $n\rho + m\sigma = mn$ is of the form $bh\left(x^{m/d}, y^{n/d}\right)^\lambda$, where $d = (m, n)$ and h is a linear or irreducible indefinite quadratic form.*

The proof is based on the theorem of Siegel [4] quoted in part I, it will be however a little simpler if we reformulate the said theorem, examining Siegel's argument. Siegel proves that if $f(x, y) = 0$ has infinitely many integer solutions then the genus of $f(x, y) = 0$ is zero (*). In this case (cf. Skolem [6], p. 102) there is a parametrization

$$x = \frac{\varphi(u, v)}{\chi(u, v)}, \quad y = \frac{\psi(u, v)}{\chi(u, v)}, \tag{5}$$

where φ, ψ, χ are relatively prime forms of the same positive degree with rational coefficients and where the equation

$$\chi(u, v) = h$$

has infinitely many integer solutions for some $h \neq 0$. Now, as proved by Maillet [1] (cf. [6], p. 100) the last condition implies that

$$\chi(u, v) = c_1(a_1 + b_1 v)^l \quad \text{or} \quad \chi(u, v) = d_1(a_2 u^2 + b_2 uv + c_2 v^2)^l, \tag{6}$$

where $b_2^2 - 4a_2c_2$ is positive and is not a perfect square. The latter case by the substitution $u = t$, $v = 1$ leads to a parametrization

$$x(t) = \frac{C(t)}{Q(t)^\alpha}, \quad y(t) = \frac{D(t)}{Q(t)^\beta}, \quad f\big(x(t), y(t)\big) = 0, \tag{7}$$

where C, D, Q are polynomials with rational coefficients, Q is irreducible indefinite quadratic, $\alpha \geqslant 0$, $\beta \geqslant 0$ and $x(t)$, $y(t)$ are not both constant.

Moreover, and this remark of Maillet seems to have been so far overlooked, the former case leads to the same parametrization (7) with $\alpha = \beta = 0$. Indeed on substituting $u = t$, $v = b_1^{-1}(1 - a_1 t)$ we get from (5) and (6)

$$x(t) = \frac{\varphi\big(t, b_1^{-1}(1 - a_1 t)\big)}{c_1}, \quad y(t) = \frac{\psi\big(t, b_1^{-1}(1 - a_1 t)\big)}{c_1}$$

and the polynomials on the right hand side which are not both constant can be taken as $C(t)$, $B(t)$ in (7). Therefore, if $f(x, y) = 0$ has infinitely many integer solutions then (7) holds and either

$$\alpha = \beta = 0, \quad C, D \text{ are not both constant} \tag{8}$$

or

$$\alpha + \beta > 0, \quad (C, Q^\alpha) = (D, Q^\beta) = 1. \tag{9}$$

Proof of the theorem. By Runge's theorem we have (1), (2) and (4) and it remains to show that h is linear or indefinite quadratic. Set $m/d = \mu$, $n/d = \nu$.

In the case (8) let γ, δ be the degrees of C, D respectively and c_0, d_0 their leading coefficients. If t tends to infinity then x is of order t^γ, y of order t^δ and by (2) $\delta = \gamma m/n$. Thus we get from (7)

$$g(c_0, d_0) = \lim_{t=\infty} t^{-\gamma m} f\big(x(t), y(t)\big) = 0,$$

(*) The assumptions imply the absolute irreducibility of f, hence the genus is defined.

from (4)

$$h\big(c_0^{\mu}, d_0^{\nu}\big) = 0$$

and $h(u, v)$ is divisible by $d_0^{\nu}u - c_0^{\mu}v$. Since h is irreducible it must be linear.

In the case (9) let t_1, t_2 be the zeros of $Q(t)$. If t tends to t_i then x is of order $(t - t_i)^{-\alpha}$ (possibly tends to 0 if $\alpha = C(t_i) = 0$), y of order $(t - t_i)^{-\beta}$ (possibly tends to 0 if $\beta = D(t_i) = 0$) and by (2) $\beta = \alpha m/n$, $C(t_i) \neq 0 \neq D(t_i)$ $(i = 1, 2)$. Thus we get from (7)

$$g\big(C(t_i), D(t_i)\big) = \lim_{t=t_i} Q(t)^{\alpha m} f\big(x(t), y(t)\big) = 0,$$

from (4)

$$h\big(C(t_i)^{\mu}, D(t_i)^{\nu}\big) = 0$$

and $h(u, v)$ is divisible by $D(t_i)^{\nu}u - C(t_i)^{\mu}v$ $(i = 1, 2)$.

If $C(t_1)^{-\mu}D(t_1)^{\nu}$ is rational h must be linear as before.

If $C(t_1)^{-\mu}D(t_1)^{\nu}$ is irrational then $C(t_i)^{-\mu}D(t_i)^{\nu}$ are conjugate in a real quadratic field, h is divisible by

$$\big(D(t_1)^{\nu}u - C(t_1)^{\mu}v\big)\big(D(t_2)^{\nu}u - C(t_2)^{\mu}v\big)$$

and h is indefinite quadratic. This completes the proof.

It should be noted that the above proof does not share an essential advantage of Runge's proof, namely it does not permit to estimate the size of solutions of $f(x, y) = 0$ if the theorem implies the finiteness of their number. The reason for this defect is the noneffective character of Siegel's theorem.

References

[1] E. Maillet, *Détermination des points entiers des courbes algébriques unicursales à coefficients entiers*. C. R. Acad. Sci. Paris 168 (1919), 217–220.

[2] K. F. Roth, *Rational approximations to algebraic numbers*. Mathematika 2 (1955), 1–20; corrigendum, ibid., 168.

[3] C. Runge, *Über ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen*. J. Reine Angew. Math. 100 (1887), 425–435.

[4] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*. Abh. Preuss. Akad. Wiss. Phys.-math. Kl. Nr. 1 (1929); Ges. Abhandlungen I, Springer, Berlin 1966, 209–266.

[5] Th. Skolem, *Über ganzzahlige Lösungen einer Klasse unbestimmter Gleichungen*. Norsk. Mat. Forenings Skrifter (I) Nr. 10 (1922).

[6] —, *Diophantische Gleichungen*. Berlin, 1938.

Originally published in
Acta Arithmetica XXXI (1976), 199–204

On the equation $y^m = P(x)$

with R. Tijdeman (Leiden)

The aim of this paper is to prove the following

Theorem. *If a polynomial $P(x)$ with rational coefficients has at least two distinct zeros then the equation*

$$y^m = P(x), \quad x, y \text{ integers}, \quad |y| > 1, \tag{1}$$

implies $m < c(P)$ where $c(P)$ is an effectively computable constant.

For a fixed m the Diophantine equation (1) has been thoroughly investigated before (see [1] and [4]) and the known results together with the above theorem imply immediately

Corollary 1. *If a polynomial $P(x)$ with rational coefficients has at least two simple zeros then the equation* (1) *has only finitely many integer solutions m, x, y with $m > 2$, $|y| > 1$ and these solutions can be found effectively.*

Corollary 2. *If a polynomial $P(x)$ with rational coefficients has at least three simple zeros then the equation* (1) *has only finitely many integer solutions m, x, y with $m > 1$, $|y| > 1$ and these solutions can be found effectively.*

A simple proof of the special case of Corollary 1 that $P(x)$ has at least two simple rational zeros can be found in a survey paper by the second named author [6]. Corollary 2 is a step towards the following

Conjecture. *If a polynomial $P(x)$ with rational coefficients has at least three simple zeros then the equation $y^2z^3 = P(x)$ has only finitely many solutions in integers x, y, z with $yz \neq 0$.*

This conjecture lies rather deep, since it implies the existence of infinitely many primes p such that $2^{p-1} \not\equiv 1 \pmod{p^2}$.

The proof of the theorem is based on Baker's work [2] and on two lemmata. We denote by $\|x\|$ the distance from x to the nearest integer.

Lemma 1. *For any complex numbers X, Y different from 0, a positive integer h and any choice of the roots $X^{1/h}, Y^{1/h}$ we have*

$$(2)\qquad |X^{1/h} - Y^{1/h}| \geqslant \max\bigl(|X|, |Y|\bigr)^{1/h} \cdot \begin{cases} \Bigl(1 - \dfrac{1}{e}\Bigr) \min\Bigl(1, \dfrac{1}{h}\bigl|\log |XY^{-1}|\bigr|\Bigr) & \text{if } |X| \neq |Y|, \\ \dfrac{4}{h}\left\| \dfrac{\log XY^{-1}}{2\pi i} \right\| & \text{if } |X| = |Y|. \end{cases}$$

Proof. We can assume without loss of generality that

$$|X| \geqslant 1 = Y^{1/h}.$$

If $|X| > 1$ we have

$$|X^{1/h} - 1| \geqslant |X|^{1/h} - 1 = |X|^{1/h}\bigl(1 - |X|^{1/h}\bigr),$$

and if $|X| \geqslant e^h$ the inequality (2) follows immediately. To settle the case $e^h > |X| > 1$ we verify by differentiation that the function

$$f(t) = (1 - t^{-1})/\log t$$

is decreasing in the interval $(1, e)$. Since $f(e) = 1 - e^{-1}$, (2) follows on taking $t = |X|^{1/h}$.

Suppose now that $|X| = 1$,

$$X = \cos\varphi + i \sin\varphi, \quad \varphi = i^{-1} \log X.$$

Then

$$X^{1/h} = \cos\frac{\varphi + 2\pi j}{h} + i \sin\frac{\varphi + 2\pi j}{h} \quad \text{for some integer } j$$

and

$$|X^{1/h} - 1| = 2 \sin\left|\frac{\varphi + 2\pi j}{2h}\right|.$$

However, $\sin\psi/\psi$ is decreasing on $(0, \pi/2)$. Hence for all real ψ

$$|\sin\psi| \geqslant 2\left\|\frac{\psi}{\pi}\right\|$$

and

$$|X^{1/h} - 1| \geqslant 4\left\|\frac{\varphi + 2\pi j}{2\pi h}\right\| \geqslant \frac{4}{h}\left\|\frac{\log X}{2\pi i}\right\|.$$

In the following lemma we denote the height of an algebraic number x by $H(x)$.

Lemma 2. *If γ_1, γ_2 are algebraic integers of a field K of degree d then*

$$(3)\qquad H(\gamma_1/\gamma_2) \leqslant 3d2^d \prod_{\sigma} \max\bigl(|\gamma_1^{\sigma}|, |\gamma_2^{\sigma}|\bigr),$$

where σ runs through all the isomorphic injections of K into the complex field. Moreover, if $K = \overline{K}$ (the bar denoting complex conjugation) then

$$H\big(|\gamma_1/\gamma_2|^2\big) \leqslant 3d2^d \prod_{\sigma} \max\big(|\gamma_1^\sigma|, |\gamma_2^\sigma|\big)^2.$$

Proof. Clearly γ_1/γ_2 satisfies the equation

$$F(x) = \prod_{\sigma} \big(\gamma_2^\sigma x - \gamma_1^\sigma\big) = 0.$$

$F(x)$ has rational integral coefficients, but it may be reducible. We have

$$F(x) = N_{K/\mathbb{Q}}\, \gamma_2 \cdot f(x)^r,$$

where f is the minimal polynomial of γ_1/γ_2. By Gauss's lemma $F(x) = c \cdot g(x)^r$, where c is an integer, g has integral coefficients and is irreducible as a constant multiple of f. By an inequality of Gel′fond ([3], p. 139) we have

$$H(F) \geqslant \frac{1}{3dr}\, H(g)^r \geqslant \frac{1}{3d}\, H(g), \quad \text{unless } H(g) = 1,$$

where $H(P)$ denotes the height of the polynomial P.

On the other hand,

$$H(F) \leqslant \prod_{\sigma} \big(|\gamma_1^\sigma| + |\gamma_2^\sigma|\big) \leqslant 2^d \prod_{\sigma} \max\big(|\gamma_1^\sigma|, |\gamma_2^\sigma|\big).$$

This implies (3). Now if $K = \overline{K}$ we have $|\gamma_i^2| = \gamma_i \overline{\gamma}_i \in K$ $(i = 1, 2)$. Hence

$$\begin{aligned} H\big(|\gamma_1/\gamma_2|^2\big) &\leqslant 3d2^d \prod_{\sigma} \max\big(|\gamma_1^\sigma \overline{\gamma}_1^\sigma|, |\gamma_2^\sigma \overline{\gamma}_2^\sigma|\big) \\ &\leqslant 3d2^d \prod_{\sigma} \max\big(|\gamma_1^\sigma|, |\gamma_2^\sigma|\big) \cdot \prod_{\sigma} \max\big(|\overline{\gamma}_1^\sigma|, |\overline{\gamma}_2^\sigma|\big) \\ &= 3d2^d \prod_{\sigma} \max\big(|\gamma_1^\sigma|, |\gamma_2^\sigma|\big)^2. \end{aligned}$$

Proof of the Theorem. Let K be the splitting field of P and let

$$bP(x) = a \prod_{i=1}^{n} (x - \alpha_i)^{r_i} \quad (\alpha_i \text{ distinct}, b \text{ integer})$$

have integral coefficients. It follows from (1) that

$$\prod_{i=1}^{n} (ax - a\alpha_i)^{r_i} = ba^{N-1} y^m, \quad N = \sum_{i=1}^{n} r_i, \tag{4}$$

where the numbers $a\alpha_i$ are algebraic integers. Since for integer x

$$(ax - a\alpha_i, ax - a\alpha_j) \,|\, (a\alpha_i - a\alpha_j),$$

the highest common ideal divisor of any two factors on the left hand side of (4) is composed exclusively of prime ideals of K dividing

$$\Delta = \prod_{1 \leqslant i < j \leqslant n} (a\alpha_i - a\alpha_j).$$

Hence, for each $i \leqslant n$ we have

$$(ax - a\alpha_i)^{r_i} = \mathfrak{d}\mathfrak{c}^m \tag{5}$$

for some ideals $\mathfrak{d}$ and $\mathfrak{c}$ such that $\mathfrak{d}$ is composed exclusively of prime factors of $ab\Delta$ and $(\mathfrak{c}, ab\Delta) = 1$. If $\mathfrak{p}$ is a prime ideal and $\mathfrak{p}^t \parallel \mathfrak{c}^m$ then clearly $m \mid t$ and by (5) $r_i \mid t$, thus $[m, r_i] \mid t$. It follows that $\dfrac{m}{(m, r_i)} \;\Big|\; \dfrac{t}{r_i}$. Moreover $\mathfrak{d} = \mathfrak{d}_i^{r_i}$ and we get from (5)

$$(ax - a\alpha_i) = \mathfrak{d}_i \mathfrak{c}_i^s, \quad s = \frac{m}{(m, [r_1, \ldots, r_n])}. \tag{6}$$

Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ be all prime ideal divisors of $ab\Delta$ in K and let h be the class number of K. We have

$$\mathfrak{p}_j^h = (\pi_j) \qquad (1 \leqslant j \leqslant k),$$
$$\mathfrak{c}_i^h = (\gamma_i) \qquad (1 \leqslant i \leqslant n),$$

and by (6) for suitable integer exponents $y_{ij} \geqslant 0$

$$(ax - a\alpha_i)^h = \Big(\prod_{j=1}^{k} \pi_j^{y_{ij}} \gamma_i^s\Big).$$

If $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_r$ are a basis for the group of units in K we get

$$(ax - a\alpha_i)^h = \prod_{q=0}^{r} \varepsilon_q^{x_{iq}} \prod_{j=1}^{k} \pi_j^{y_{ij}} \gamma_i^s \quad (1 \leqslant i \leqslant n), \tag{7}$$

where we can suppose without loss of generality that

$$0 \leqslant x_{iq} < s, \quad 0 \leqslant y_{ij} < s, \tag{8}$$

since any product

$$\prod_{q=0}^{r} \varepsilon_q^{x_q} \prod_{j=1}^{k} \pi_j^{y_j} \quad \text{with } x_q \equiv y_j \equiv 0 \pmod{s},\ y_j \geqslant 0,$$

can be incorporated in γ_i.

By our assumption $n \geqslant 2$. We use (7) for $i = 1, 2$, denoting the right hand side of (7) by X and Y, respectively. If $X = Y$ we have

$$(ax - a\alpha_1)^h = (ax - a\alpha_2)^h$$

and it follows, from $\alpha_1 \neq \alpha_2$, that $ax - a\alpha_1 = e^{2\pi i g/h}(ax - a\alpha_2)$, $0 < g < h$, and

$$|x| \leqslant \frac{|\alpha_1| + |\alpha_2|}{2 \sin(\pi/h)}.$$

Since $|y| > 1$, equation (1) gives $m < c_1$, where c_1 as the subsequent constants $c_2, c_3, \ldots$ depends only on P and is effectively computable.

If $X \neq Y$ we have either $|X| \neq |Y|$ or $|X| = |Y|$ and $\left\| \dfrac{\log XY^{-1}}{2\pi i} \right\| \neq 0$. In the former case we infer by (8) from Baker's theorem [2] that

$$\left|\log |XY^{-1}|\right| > H\left(|\gamma_1/\gamma_2|^2\right)^{-c_2 \log s},$$

in the latter case similarly

$$\left\| \frac{\log XY^{-1}}{2\pi i} \right\| > H\left(\gamma_1/\gamma_2\right)^{-c_3 \log s},$$

where in case $H(\,) = 1$, it should be replaced by 2.

In virtue of Lemmata 1 and 2 we have in both cases

$$\begin{aligned} |a\alpha_1 - a\alpha_2| &= |X^{1/h} - Y^{1/h}| \\ &> c_4 \max\left(|X|, |Y|\right)^{1/h} \prod_\sigma \max\left(|\gamma_1^\sigma|, |\gamma_2^\sigma|\right)^{-c_5 \log s} \\ &> c_6^{-s} \max\left(|\gamma_1|, |\gamma_2|\right)^{s/h} \prod_\sigma \max\left(|\gamma_1^\sigma|, |\gamma_2^\sigma|\right)^{-c_5 \log s} \end{aligned}$$

for some constant $c_6 > 1$.

c Applying any isomorphic injection τ of K into $\mathbb{C}$ to both sides of (7) and arguing as before we get

$$|a\alpha_1^\tau - a\alpha_2^\tau| > c_6^{-s} \max\left(|\gamma_1^\tau|, |\gamma_2^\tau|\right)^{s/h} \prod_\sigma \max\left(|\gamma_1^\sigma|, |\gamma_2^\sigma|\right)^{-c_5 \log s}.$$

c On taking the product over all injections τ we obtain

$$|N_{K/\mathbb{Q}}(a\alpha_1 - a\alpha_2)| > c_6^{-ds} \prod_\sigma \max\left(|\gamma_1^\sigma|, |\gamma_2^\sigma|\right)^{s/h - c_5 d \log s}.$$

Since the left hand side is independent of s, this implies that either $s \leqslant c_7$ or

$$\prod_\sigma \max\left(|\gamma_1^\sigma|, |\gamma_2^\sigma|\right) < c_6^{2dh}.$$

In the former case we have $m \leqslant c_7[r_1, \ldots, r_n]$, in the latter case, by (7),

$$N_{K/\mathbb{Q}}\left((ax - a\alpha_1)^h (ax - a\alpha_2)^h\right) = \pm \prod_{j=1}^{k} N(\pi_j)^{y_{1j} + y_{2j}} \mathscr{G}^s, \tag{9}$$

where $\mathscr{G} = |N\gamma_1\gamma_2| < c_6^{4dh}$. The greatest prime factor of the right hand side of (9) is bounded by $ab\Delta c_6^{4dh}$. The left hand side of (9) is a polynomial in x with integer coefficients and at least two distinct zeros. It has been proved by the first named author, M. Keates, S. V. Kotov and V. G. Sprindzhuk (see [5]) that the greatest prime factor of such a polynomial exceeds $c_8 \log\log |x|$. So we obtain $|x| \leqslant c_9$ and in view of (1) with $|y| > 1$, $m \leqslant c_{10}$.

References

[1] A. Baker, *Bounds for the solutions of the hyperelliptic equation*. Proc. Cambridge Philos. Soc. 65 (1969), 439–444.

[2] —, *A sharpening of the bounds for linear forms in logarithms*. Acta Arith. 21 (1972), 117–129.

[3] A. O. Gel′fond, *Transcendental and Algebraic Numbers*. Gosudarstv. Izdat. Tekhn.-Teor. Lit., Moscow 1952 (Russian). English translation: Dover Publ., New York 1960.

[4] W. J. LeVeque, *On the equation* $y^m = f(x)$. Acta Arith. 9 (1964), 209–219.

[5] V. G. Sprindzhuk, *An effective analysis of the Thue and Thue–Mahler equations*. In: Current Problems of Analytic Number Theory (Minsk 1972), Nauka i Tekhnika, Minsk 1974, 199–222 (Russian).

[6] R. Tijdeman, *Applications of the Gel′fond–Baker method to rational number theory*. In: Topics in Number Theory (Debrecen 1974), Colloq. Math. Soc. János Bolyai 13, North-Holland, Amsterdam 1976, 399–416.

Originally published in
Journal für die reine und angewandte Mathematik
309 (1979), 176–182

Zeta functions and the equivalence of integral forms

with R. Perlis (Bonn)*

1.

Two algebraic number fields K, K' are said to be *arithmetically equivalent* when their zeta functions $\zeta_K(s)$ and $\zeta_{K'}(s)$ coincide. In this paper we give an example of two nonisomorphic arithmetically equivalent fields of class number one, and then show that the *norm forms* from the rings of integers of these fields provide a negative answer to an old conjecture concerning integral forms.

We will consider the values of integral forms when the variables run through $\mathbb{Z}$. The *fixed divisor* of a form $g \in \mathbb{Z}[X_1, \ldots, X_n]$ is the gcd of its values. Let $w(R)$ be the number of integers in the interval $(-R, R)$ which appear as values of g. Then g has *density zero* if the quotient $w(R)/R$ approaches zero as a limit as R increases to infinity. Let $\underline{X}$ denote the n-tupel of variables $(X_1, \ldots, X_n)$, let A be an n-by-n matrix, and let $\underline{X} \cdot A$ be the linear change of variables defined by A.

Chowla has made the following conjecture (see [2], and [4], p. 23):

Let g and h be irreducible integral forms of degree d in n variables, each having density zero and fixed divisor one, and representing the same numbers when the variables run through $\mathbb{Z}$. Then there is an integral matrix A of determinant ± 1 for which

$$g(\underline{X}) = h(\underline{X} \cdot A).$$

To support this conjecture, Chowla claimed it is true for binary quadratic forms, but this was due to an oversight. For example, $g = X^2 + XY + Y^2$ and $h = X^2 + 3Y^2$ satisfy all the hypotheses of the conjecture, but it is easy to check that any linear transformation taking h to g has determinant $1/2$, and hence cannot be integral.

* Supported by the *Sonderforschungsbereich „Theoretische Mathematik"* of Bonn University.

2.

There are several ways in which this conjecture can be mended for binary quadratic forms:

a) One can additionally require that g and h have the same discriminant.

b) One can additionally require that the integers represented *properly* by g (i.e., those values $g(x_1, \ldots, x_n)$ with $(x_1, \ldots, x_n) = 1$) coincide with the integers represented properly by h.

c) One can additionally require that g (and h) is integrally equivalent to any form $f \in \mathbb{Z}[X_1, \ldots, X_n]$ representing it integrally.

d) One can weaken the conclusion to assert only that g and h are equivalent via a *rational* transformation of non-zero determinant.

With each of these alterations, the validity of Chowla's conjecture for binary quadratic forms follows easily from the following reformulation of a theorem of Schering ([9]): Let g and h be two primitive binary quadratic forms with

$$|\text{disc. } g| \leqq |\text{disc. } h|.$$

Then g and h have the same sets of values if and only if *either* (i) g and h are integrally equivalent, *or* (ii) disc. $g = D \equiv 5 \pmod 8$, the equation $X^2 - DY^2 = 4$ has proper solutions, and $h(X, Y)$ is integrally equivalent to the form $g(X, 2Y)$.

Let g and h be the norm forms from the rings of integers of the fields $\mathbb{Q}\big((-3)^{1/8}\big)$ and $\mathbb{Q}\big((-48)^{1/8}\big)$. We will show below that these forms are a counterexample to the conjecture even when one adds all the extra hypotheses a), b), c), and weakens the conclusion to d).

Despite this negative result, certain special versions of Chowla's conjecture may be true. For *binary* forms of any degree the situation has been studied in [10], and results of a positive nature have been found. For more than two variables, the problem of relating the equivalence of forms to their values seems much more complicated; however, the following comment may be of some interest. Although discriminants have long been defined for forms of any degree and any number of variables (see for example [5], lecture 44, p. 159), their arithmetic meaning is far from clear in general: when the number of variables exceeds two, the discriminant is *zero* for any form that is not absolutely irreducible. In particular, it vanishes for such well-behaved forms as norm forms (the forms of our counterexample). This suggests that perhaps further investigations of Chowla's conjecture should initially be restricted to *nonsingular* forms.

3.

Let $K = \mathbb{Q}\big((-3)^{1/8}\big)$ and $K' = \mathbb{Q}\big((-48)^{1/8}\big)$. These are nonisomorphic fields of degree eight whose zeta functions coincide (see [7], p. 351). We will show in Sections 4 and 5 that both K and K' have class number one. Using this result from below, we will now construct a counterexample to Chowla's conjecture with all the variations a), b), c), and d) of Section 2.

Select a basis $\{\theta_i\}$ for the integers of K and $\{\theta_i'\}$ for the integers of K' and define

$$
\begin{aligned}
g(X_1, \ldots, X_8) &= \operatorname{norm}_{K/\mathbb{Q}}(X_1\theta_1 + \ldots + X_8\theta_8) \\
h(X_1, \ldots, X_8) &= \operatorname{norm}_{K'/\mathbb{Q}}(X_1\theta_1' + \ldots + X_8\theta_8').
\end{aligned} \tag{1}
$$

Then g and h are irreducible ([1], Th. 2, p. 80) integral forms of degree eight in eight variables, of density zero ([6]) and fixed divisor one. By the remark at the end of Section 2, they have the common discriminant zero.

To check the validity of assumption b), we will characterize the sets of numbers properly represented by either form. Consider one of these forms, say g. Any value $g(x_1, \ldots, x_8)$ is the norm of the algebraic integer $\sum x_i\theta_i$. This norm is positive, since K is totally imaginary, and equals the norm of the ideal $\left(\sum x_i\theta_i\right)$. Conversely, K has class number one, as will be shown below, so the norm of any ideal is the norm of an element, and this means that the values of g are precisely the norms of integral ideals.

One sees at once that $x_1, \ldots, x_8$ are relatively prime if and only if the corresponding ideal $\left(\sum x_i\theta_i\right)$ is *primitive*, i.e., not divisible by any rational integer. Consider two ideals $\mathfrak{A}$ and $\mathfrak{B}$ whose norms are relatively prime. If their product $\mathfrak{AB}$ is not primitive, then it is divisible by some prime number p and hence by every prime ideal factor of p. All of these latter divide exactly one of $\mathfrak{A}$ or $\mathfrak{B}$, since $(\operatorname{norm}\mathfrak{A}, \operatorname{norm}\mathfrak{B}) = 1$, and therefore p divides either $\mathfrak{A}$ or $\mathfrak{B}$. That is, the product of primitive ideals with relatively prime norms is again primitive. It is obvious that any factor of a primitive ideal is primitive, and this together with the previous fact means: g (and similarly, h) properly represents a product of relatively prime numbers if and only if it properly represents each factor. Thus, in order to know which values are properly represented by g, it suffices to know which prime powers p^t are properly represented.

Let $p = \prod_i P_i^{e_i}$ $(i = 1, \ldots, s)$ be the factorization of a prime number p in K, with ramification indices e_i and inertia degrees f_i, and suppose that p^t is the norm of an integral ideal $\mathfrak{A}$. Then this ideal necessarily has the form $\mathfrak{A} = \prod_i P_i^{v_i}$ $(i = 1, \ldots, s)$ with nonnegative v's, and is primitive if and only if at least one of these v_i is strictly less than the corresponding ramification index e_i. Taking norms then shows: p^t is properly represented by g if and only if the exponent t can be written as $t = \sum v_i f_i$ with nonnegative v's, and $v_i < e_i$ for at least one i.

The analogous characterization holds for the prime powers properly represented by the form h, of course, with the ramification indices e_i' and the inertia degrees f_i' now computed in K' instead of in K. As has already been mentioned, K and K' have equal zeta functions. From this, it automatically follows that the prime ideal factors P_i of p in K can be paired with the factors P_i' in K' so that the corresponding inertia degrees are equal, $f_i = f_i'$ $(i = 1, \ldots, s)$ (see [7], Th. 1, p. 345). In general, e_i and e_i' do not have to agree under this correspondence, but for the specific fields K, K' in question, they do. The ramified primes are 2, 3 and 3, being an eighth power, obviously ramifies totally in K. It follows from the equality of the zeta functions that there is a unique prime of K' lying over 3, and that it has inertia degree one, so 3 ramifies totally in K'. We will show in the next section that $(2) = P^4$ in K and $(2) = P'^4$ in K'. With this, it follows that either both of g and h or neither of them properly represents a given p^t, and hence they properly represent the same sets of values.

We now turn to the task of verifying assumption c). Suppose $g(\underline{X}) = f(\underline{X} \cdot A)$ with $f \in \mathbb{Z}[X_1, \ldots, X_8]$ and an integral matrix A of determinant $d \neq 0$. We will show that $d = \pm 1$. Set $B = d \cdot A^{-1}$. Then $B = (b_{ij})$ is an integral matrix of determinant d^7, and $g(\underline{X} \cdot B) = f(d\underline{X})$, which can be rewritten to give

$$\text{norm}(X_1\lambda_1 + \ldots + X_8\lambda_8) = d^8 \cdot f(\underline{X}) \tag{2}$$

where $\lambda_i = \sum_j b_{ij}\theta_j$. If $\mathfrak{A}$ is the integral ideal generated by the λ's, then (2) implies

$$\text{norm}\,\mathfrak{A} \geqq d^8. \tag{3}$$

Consider the lattice $\Lambda = \bigoplus \mathbb{Z}\lambda_i$ contained in $\mathfrak{A}$. Then B is the matrix of the transition map from the lattice $\mathcal{O} = \bigoplus \mathbb{Z}\theta_i$ of all integers in K to the lattice Λ, so the index of Λ in $\mathcal{O}$ is $[\mathcal{O} : \Lambda] = |\det B| = |d|^7$. On the other hand, $\Lambda \subseteqq \mathfrak{A}$ so $[\mathcal{O} : \Lambda] \geqq d^8$, by (3), implying $d = \pm 1$.

Suppose finally there were a rational matrix A giving a linear substitution

$$(y_1, \ldots, y_8) = (x_1, \ldots, x_8) \cdot A \tag{4}$$

for which

$$g(x_1, \ldots, x_8) = h(y_1, \ldots, y_8). \tag{5}$$

For $x_i \in \mathbb{Q}$ let y_j be defined by (4) and consider the map $T : K \to K'$ taking $\sum x_i\theta_i$ to $\sum y_j\theta'_j$. This is an additive map which preserves norm. Hence for $\alpha \in K$ and for every natural number n

$$\text{norm}(n - \alpha) = \text{norm}\big(T(1) \cdot n - T(\alpha)\big), \tag{6}$$

and this implies that the polynomials

$$s(X) = \text{norm}(X - \alpha) \quad \text{and} \quad t(X) = \text{norm}\big(T(1) \cdot X - T(\alpha)\big) \tag{7}$$

coincide. If we select α to generate K over $\mathbb{Q}$, then the roots of $s(X)$ are the conjugates of α. Since $T(\alpha) \cdot T(1)^{-1}$ lies in K' and is a root of $t(X) = s(X)$, it follows that K' contains a conjugate of α. Since K and K' have the same degree, this implies $K \cong K'$, and this contradiction shows that g and h are not rationally equivalent.

4.

It remains to show that the class numbers of $K = \mathbb{Q}\big((-3)^{1/8}\big)$ and $K' = \mathbb{Q}\big((-48)^{1/8}\big)$ are one. We begin by proving the implication

$$h_K = 1 \implies h_{K'} = 1; \tag{8}$$

then we will show in the next section that $h_K = 1$. So, assume $h_K = 1$ and let $L = K(\sqrt{2})$. Then L is also $K'(\sqrt{2})$. We contend that *each of the quadratic extensions L/K and L/K' has exactly one ramified prime*, which then necessarily ramifies totally.

Clearly any ramified prime is finite and lies over 2. Consider first K. We check easily that $(2) = P^4$ in K where $P = \big(1 + (-3)^{1/8}\big)$ has norm 4. Since 2 is inert in the subfield $\mathbb{Q}(\sqrt{-3})$ of K, it follows that P is a prime ideal, and the only prime ideal of K lying

above 2. Hence P is the only prime of K that can possibly ramify in L. Since $h_K = 1$, the abelian extension L/K must ramify, so P ramifies; i.e., 2 is the eighth power of a prime ideal in L. Intersecting this ideal with K' shows that there is only one prime P' of K' lying above 2, and P' ramifies in L. This proves the statement in italics above, and also shows that $(2) = P'^4$ in K', settling the question of ramification indices left open in Section 3.

Iwasawa has shown that the validity of the italic statement just proved suffices to conclude that

$$2 \mid h_K \iff 2 \mid h_L \iff 2 \mid h_{K'} \tag{9}$$

(see [3]). Since $h_K = 1$, it follows that $h_{K'}$ is odd. But it has been proved in [8] that the class number quotient $h_K / h_{K'} = 2^i$ for an integer i. The left side of this equality being odd, we have $i = 0$, which proves (8).

5.

It is to be shown that $h_K = 1$. Set $\theta = (-3)^{1/8}$ and let $(x_0, x_1, \ldots, x_7)$ denote $\sum_i x_i \theta^i$. By considering the tower of quadratic extensions of $\mathbb{Q}$ leading up to K, it is easy to verify that

$$\left\{ \frac{1}{2}\big(a, b, c, d, a + 2e, b + 2f, c + 2g, d + 2h\big) \,\middle|\, a, b, c, d, e, f, g, h \in \mathbb{Z} \right\} \tag{10}$$

is the full ring of integers of K. From this, we calculate the discriminant of K to be $D_K = 2^{16} \cdot 3^7$.

The ideal class group of K is generated by the prime ideals whose norm does not exceed the Minkowski bound $M_K = N! \cdot N^{-N} \cdot (4/\pi)^t \cdot \sqrt{|D_K|}$, where $t = 4$ is the number of complex valuations of K and $N = 8$ is the field degree. We have $M_K < 76$.

The ramified primes are 2 and 3. We have already seen in Section 4 that each of these has exactly one prime factor in K and this factor is principal.

Let P be a prime ideal of K whose norm p^f does not exceed 76. Excluding the ramified primes, we have $p \geqq 5$ and hence $f \leqq 2$. If $f = 2$, then p is either 5 or 7. The irreducible polynomial of θ is $F(X) = X^8 + 3$ and has the discriminant $2^{24} \cdot 3^7$. The only primes dividing this discriminant are the ramified primes 2 and 3, so there are no inessential discriminant divisors, and hence the splitting of an unramified prime number p is determined by the factorization of $F(X)$ modulo p. Since $F(X)$ is irreducible modulo 5, the prime number 5 is inert in K and hence has no prime factor of degree $f = 2$. Modulo 7, the polynomial factors as $F(X) = (X + 2)(X - 2)(X^2 + 4)(X^2 - X + 4)(X^2 + X + 4)$, so 7 splits into the product of five prime ideals in K, two of norm 7 ($f = 1$) and three of norm 49 ($f = 2$). We will show that each of these five ideals is principal. To this end, it suffices to exhibit five integers in K, two of norm 7 and three of norm 49, such that none is divisible by any of the others. These integers are given in Table 1 at the end of this paper.

With this, we know that the ideal class group of K is generated by prime ideals of degree $f = 1$, lying over prime numbers p in the range $7 < p < 76$. Now, a prime number p has a factor of degree $f = 1$ if and only if $X^8 + 3$ has a root modulo p. In particular, -3 must be a square modulo p, and with the law of quadratic reciprocity it

follows that $p \equiv 1 \pmod 3$. There are eight prime numbers satisfying this congruence and lying in our range; we divide them into three sets, as follows:

$$\begin{aligned} A &= \{p \text{ with } 2 \parallel (p-1)\} = \{19, 31, 43, 67\}; \\ B &= \{p \text{ with } 4 \parallel (p-1)\} = \{13, 37, 61\}; \\ C &= \{p \text{ with } 8 \mid (p-1)\} = \{73\}. \end{aligned} \tag{11}$$

The multiplicative group of $\mathbb{Z}/p\mathbb{Z}$ is cyclic of order $p-1$. This implies that -3, being a quadratic residue, is automatically an eighth-power residue modulo each of the four primes in the set A, and in fact it implies that each of these primes has exactly two prime factors in K of degree $f = 1$. A moment's thought shows that these two prime factors are conjugate via the automorphism of K sending θ to $-\theta$, and thus one factor is principal if and only if the other one is. Hence, for $p \in A$, we will have proved that every prime factor of p with $f = 1$ is principal as soon as we have exhibited an integer of K with norm p. These are given in Table 2.

Let p be a prime in the set B. Then -3 is an eighth power if and only if it is a fourth power modulo p. This shows that 13 has no factor of degree one in K, while each of 37 and 61 has precisely four prime factors of degree one. We will prove all these to be principal by exhibiting four non-associated integers of norm p, for $p = 37$ and 61.

The only element of C is $p = 73$. One checks directly that -3 is not a fourth power and hence certainly not an eighth power modulo 73, implying that 73 has no prime factor of degree $f = 1$.

Thus, the tables below prove that K, and consequently, as shown above in Section 4, also that K', has class number one.

We conclude with a comment of the tables. Due to the simplicity of the defining polynomial $X^8 + 3$, it is more-or-less trivial to multiply two integers of K given in the form (10) and to express the result again in this form. Computing norms via the tower of quadratic subfields leading from K down to $\mathbb{Q}$, it takes three such multiplications to check that an integer in these tables has the norm claimed for it. When this has been done, it remains to check that various entries are not divisible by others. This can be done efficiently as follows. Let I denote an integer with norm N. The entry T appearing below denotes the quotient N/I; its value can be checked by computing $T \cdot I$. Finally, to show that an integer J is not divisible by I, it suffices to multiply $J \cdot T$ and to find a single coordinate which is not divisible by N (up to a factor of $1/2$, due to the form (10) of integers in K).

Let I^σ denote the integer obtained from I by changing the sign of the second, fourth, sixth, and eighth component; i.e., by replacing θ by $-\theta$. Since the primes in these tables are unramified in K, one can show that when the norm of I is prime, then I cannot divide I^σ. With these easy observations, it is possible to check the accurracy of the following tables, and hence that $h_K = h_{K'} = 1$, in a short amount of time, by hand.

Table 1

Integer I	$N = \text{norm } I$	$T = N/I$
$I_1 = (1, 1, 1, 0, 0, 0, 0, 0)$	7	$(-2, -1, 3, -2, -1, 3, -2, -1)$
$I_1^\sigma = (1, -1, 1, 0, 0, 0, 0, 0)$	7	$(-2, 1, 3, 2, -1, -3, -2, 1)$
$I_2 = (-1, 0, 1, 0, -1, 0, 0, 0)$	49	$(-7, 0, 14, 0, 21, 0, 7, 0)$
$I_3 = (1, -1, -1, 0, -1, 1, 0, 0)$	49	$(7, 35, 14, 0, 21, 7, -7, 0)$
$I_3^\sigma = (1, -1, -1, 0, -1, -1, 0, 0)$	49	$(7, -35, 14, 0, 21, -7, -7, 0)$

Table 2

Prime p	Integer I of norm p	$T = N/I$
19	$= (2, 1, 1, 0, 0, -1, -1, -1)$	$(-25, -1, 22, -9, -11, 14, -4, -7)$
31	$= (1, -1, -1, 1, 0, -1, 0, 0)$	$(-35, 28, -10, 8, 6, -11, 15, -12)$
43	$= (1, 0, -1, 1, -1, 1, -1, 1)$	$(-29, -39, -5, 17, 11, -3, -7, -2)$
67	$= (1, 0, 0, 0, -1, 1, 0, 0)$	$(64, 42, 15, -9, -8, -22, -27, -24)$
37	$I_1 = (1, 1, 0, 1, 0, 0, 0, 0)$	$(7, -16, -11, 4, 12, -1, -3, -9)$
37	$I_1^\sigma = (1, -1, 0, -1, 0, 0, 0, 0)$	$(7, 16, -11, -4, 12, 1, -3, 9)$
37	$I_2 = (1, 1, 1, 0, 0, 0, -1, -1)$	$(31, -40, 54, -47, 32, -21, 8, 4)$
37	$I_2^\sigma = (1, -1, 1, 0, 0, 0, -1, 1)$	$(31, 40, 54, 47, 32, 21, 8, -4)$
61	$J_1 = (1, 1, 1, 1, 1, 0, 0, 0)$	$(-2, -7, 6, 21, -18, -2, -7, 6)$
61	$J_1^\sigma = (1, -1, 1, -1, 1, 0, 0, 0)$	$(-2, 7, 6, -21, -18, 2, -7, -6)$
61	$J_2 = (1, -2, \frac{3}{2}, -2, 1, -1, \frac{1}{2}, 0)$	$(\frac{59}{2}, 8, \frac{-67}{2}, \frac{-13}{2}, \frac{43}{2}, 11, \frac{7}{2}, \frac{5}{2})$
61	$J_2^\sigma = (1, 2, \frac{3}{2}, 2, 1, 1, \frac{1}{2}, 0)$	$(\frac{59}{2}, -8, \frac{-67}{2}, \frac{13}{2}, \frac{43}{2}, -11, \frac{7}{2}, \frac{-5}{2})$

References

[1] Z. I. Borevich, I. R. Shafarevich, *Number Theory*. Academic Press, New York 1966.

[2] S. Chowla, *Some problems of elementary number theory*. J. Reine Angew. Math. 222 (1966), 71–74.

[3] K. Iwasawa, *A note on class numbers of algebraic number fields*. Abh. Math. Sem. Univ. Hamburg 20 (1956), 257–258.

[4] W. J. LeVeque, *A brief survey of Diophantine equations*. In: Studies in Number Theory, Math. Assoc. Amer., Buffalo 1969, 4–24.

[5] E. Netto, *Vorlesungen über Algebra*, II. Leipzig 1900.

[6] R. W. K. Odoni, *On the norms of algebraic integers*. Mathematika 22 (1975), 71–80.

[7] R. Perlis, *On the equation* $\zeta_K(s) = \zeta_{K'}(s)$. J. Number Theory 9 (1977), 342–360.

[8] R. Perlis, *On the class numbers of arithmetically equivalent fields*. J. Number Theory 10 (1978), 489–509.

[9] E. Schering, *Théorèmes relatifs aux formes binaires quadratiques qui représentent les mêmes nombres*. J. Math. Pures Appl. (2) 4 (1859), 253–270.

[10] A. Schinzel, *On the relation between two conjectures on polynomials*. Acta Arith. 38 (1980), 285–322; this collection: J5, 1154–1191.

Originally published in
Acta Arithmetica XXXVII (1980), 133–141

Quadratic Diophantine equations with parameters

with D. J. Lewis (Ann Arbor)*

To the memory of Paul Turán

1.

In an earlier paper [3] written in collaboration with the late Harold Davenport we proved:

Theorem A. *Let $a(t)$, $b(t)$ be polynomials with integral coefficients. Suppose that every arithmetical progression contains an integer τ such that the equation $a(\tau)x^2 + b(\tau)y^2 = z^2$ has a solution in integers x, y, z, not all 0. Then there exist polynomials $x(t)$, $y(t)$, $z(t)$ in $\mathbb{Z}[t]$, not all identically 0, such that $a(t)x(t)^2 + b(t)y(t)^2 \equiv z(t)^2$ identically in t.*

From this result we derived:

Theorem B. *Let $F(x, y, t)$ be a polynomial with integral coefficients which is of degree at most 2 in x and y. Suppose that every arithmetical progression contains an integer τ such that the equation $F(x, y, \tau) = 0$ is soluble in rational numbers for x and y. Then there exist rational functions $x(t)$, $y(t)$ in $\mathbb{Q}(t)$ such that $F\big(x(t), y(t), t\big) \equiv 0$ identically in t.*

Earlier, one of us asked [6] whether a result similar to Theorem B holds if $F(x, y, t)$ is replaced by *any* polynomial $F(x, y, t_1, \ldots, t_r)$ and the stronger assumption is made that for all integral r-tuples $\tau_1, \ldots, \tau_r$, the equation $F(x, y, \tau_1, \ldots, \tau_r) = 0$ is soluble in the rational numbers for x and y. The stronger assumption is needed since the hypothesis analogous to the one of Theorem B involving arithmetical progressions is not sufficient already for $F(x, y, t) = x^2 - y^3 - t$. We shall show here that if F is of degree at most 2 in x and y a hypothesis analogous to the one of Theorem B suffices for any number of

* This paper was written while the authors were partially supported by an NSF grant.

parameters t_i. We shall also indicate an equation of an elliptic curve over $\mathbb{Q}(t)$ for which the stronger assumption involving all integers t does not seem to suffice.

As for allowing more variables, we note that in virtue of Gauss's theorem, for every integer τ, the equation

$$x^2 + y^2 + z^2 = 28\tau^2 + 1$$

is soluble in integers x, y, z, but there do not exist rational functions $x(t), y(t), z(t)$ in $\mathbb{Q}(t)$ such that

$$x(t)^2 + y(t)^2 + z(t)^2 \equiv 28t^2 + 1$$

identically in t, since 28 is not the sum of three rational squares. A. Pfister has shown us a more refined example of the equation

$$x^2 + y^2 + z^2 = 5t^2 + 13$$

which for all rational values of t is soluble with x, y, z in $\mathbb{Q}$, without being soluble with x, y, z in $\mathbb{Q}(t)$.

We now turn to the crucial lemma from which the generalization of Theorems A and B in the case of several parameters will be deduced in §3.

2.

Lemma 1. *Let $a(t_1, \ldots, t_r)$, $b(t_1, \ldots, t_r)$, $c(t_1, \ldots, t_r) \not\equiv 0$ be polynomials with integral coefficients. Suppose that for all r-tuples of integers $\tau_1, \ldots, \tau_r$ such that $c(\tau_1, \ldots, \tau_r) \neq 0$ the equation*

$$a(\tau_1, \ldots, \tau_r)x^2 + b(\tau_1, \ldots, \tau_r)y^2 = z^2 \tag{1}$$

has a solution in integers x, y, z not all 0. Then there exist polynomials $x(t_1, \ldots, t_r)$, $y(t_1, \ldots, t_r)$, $z(t_1, \ldots, t_r)$ with integral coefficients, not all identically 0, such that

$$a(t_1, \ldots, t_r)x(t_1, \ldots, t_r)^2 + b(t_1, \ldots, t_r)y(t_1, \ldots, t_r)^2 \equiv z(t_1, \ldots, t_r)^2 \tag{2}$$

identically in $t_1, \ldots, t_r$.

Proof. The proof is by induction on r. For $r = 1$ the result follows from Theorem A since clearly every arithmetical progression contains an integer τ for which $c(\tau) \neq 0$. Alternatively, with the stronger hypothesis of our lemma one can give a simpler direct proof for the case $r = 1$ following the arguments of Theorem A.

Suppose the lemma is true for fewer than r parameters. We can obviously suppose that neither $a(t_1, \ldots, t_r)$ nor $b(t_1, \ldots, t_r)$ is identically 0, since otherwise the conclusion follows trivially. Denote the degree of a polynomial q in t_r by $|q|$. We now proceed by induction on the degree of ab with respect to t_r. If $|a| + |b| = 0$, the hypothesis of the lemma holds for $c'(t_1, \ldots, t_{r-1}) = c(t_1, \ldots, t_{r-1}, \tau)$, where τ is an integer so chosen that $c' \not\equiv 0$; and, hence, the lemma is true from our induction assumption. Suppose the result holds for all a, b, c satisfying $|a| + |b| < n$ and $c \neq 0$ where n is some positive integer; we have to prove the result for polynomials a, b, c when $|a| + |b| = n$ and $c \neq 0$. We can suppose, without loss of generality, that $|a| \geqslant |b|$, and, so, in particular $|a| > 0$.

Suppose first that $a(t_1, \ldots, t_r)$ is not square free as a polynomial in t_r, say

$$a(t_1, \ldots, t_r) = k(t_1, \ldots, t_r)^2 a_1(t_1, \ldots, t_r),$$

where k has integral coefficients and $|k| \geqslant 1$. The hypothesis of the lemma regarding a, b, c insures that this hypothesis also holds for the polynomials

$$a_1(t_1, \ldots, t_r),\ b(t_1, \ldots, t_r) \text{ and } c_1(t_1, \ldots, t_r) = k(t_1, \ldots, t_r)c(t_1, \ldots, t_r).$$

Indeed, if $\tau_1, \ldots, \tau_r$ are integers such that $c_1(\tau_1, \ldots, \tau_r) \neq 0$, then the hypothesis for a, b, c asserts there are integers x, y, z, not all 0, satisfying (1). But then

$$a_1(\tau_1, \ldots, \tau_r)x^2 + b(\tau_1, \ldots, \tau_r)y^2 = z^2$$

has $xk(\tau_1, \ldots, \tau_r)$, y, z as a nontrivial integral solution. Since $|a_1| + |b| < |a| + |b| = n$, the inductive hypothesis implies the existence of polynomials $x_1(t_1, \ldots, t_r)$, $y_1(t_1, \ldots, t_r)$, $z_1(t_1, \ldots, t_r)$ with integer coefficients and not all identically 0, such that

$$a_1(t_1, \ldots, t_r)x_1(t_1, \ldots, t_r)^2 + b(t_1, \ldots, t_r)y_1(t_1, \ldots, t_r)^2 = z_1(t_1, \ldots, t_r)^2.$$

On taking

$$\begin{aligned} x(t_1, \ldots, t_r) &= x_1(t_1, \ldots, t_r), \\ y(t_1, \ldots, t_r) &= y_1(t_1, \ldots, t_r)k(t_1, \ldots, t_r), \\ z(t_1, \ldots, t_r) &= z_1(t_1, \ldots, t_r)k(t_1, \ldots, t_r), \end{aligned}$$

we obtain an identical solution of (2).

Hence we can suppose that $a(t_1, \ldots, t_r)$ is square free as a polynomial in t_r and hence its discriminant $D(t_1, \ldots, t_{r-1})$ with respect to t_r is not identically 0. Let $a_0(t_1, \ldots, t_{r-1})$, $c_0(t_1, \ldots, t_{r-1})$ be the leading coefficient of a and c with respect to t_r; taking $c_0 = c$ if $|c| = 0$. Let $\mathscr{T}$ be the set of points $\boldsymbol{t} = (t_1, \ldots, t_{r-1})$ in $(r-1)$-dimensional affine space defined by the inequality

$$a_0(t_1, \ldots, t_{r-1})c_0(t_1, \ldots, t_{r-1})D(t_1, \ldots, t_{r-1}) \neq 0,$$

and let T be the set of all integral $(r-1)$-tuples $\boldsymbol{\tau} = (\tau_1, \ldots, \tau_{r-1})$ in the set $\mathscr{T}$. For every $\boldsymbol{\tau}$ in T the polynomial $c_{\boldsymbol{\tau}}(t_r) = c(\boldsymbol{\tau}, t_r) \not\equiv 0$. Our hypothesis on a, b, c asserts that for every integer τ_r such that $c_{\boldsymbol{\tau}}(\tau_r) \neq 0$ the equation

$$a(\boldsymbol{\tau}, \tau_r)x^2 + b(\boldsymbol{\tau}, \tau_r)y^2 = z^2$$

is soluble nontrivially in integers x, y, z. Hence for each $\boldsymbol{\tau}$ in T, by the case $r = 1$ of our theorem, there exist polynomials $x_{\boldsymbol{\tau}}(t_r)$, $y_{\boldsymbol{\tau}}(t_r)$, $z_{\boldsymbol{\tau}}(t_r)$ with integral coefficients, not all identically 0, such that

$$a(\boldsymbol{\tau}, t_r)x_{\boldsymbol{\tau}}(t_r)^2 + b(\boldsymbol{\tau}, t_r)y_{\boldsymbol{\tau}}(t_r)^2 \equiv z_{\boldsymbol{\tau}}(t_r)^2 \tag{3}$$

identically in t_r. We can suppose that $\big(x_{\boldsymbol{\tau}}(t_r), y_{\boldsymbol{\tau}}(t_r), z_{\boldsymbol{\tau}}(t_r)\big) = 1$. Since $a_0(\boldsymbol{\tau})D(\boldsymbol{\tau}) \not\equiv 0$, $a(\boldsymbol{\tau}, t_r)$ has no multiple factors, thus setting

$$d_{\boldsymbol{\tau}}(t_r) = \big(a(\boldsymbol{\tau}, t_r), y_{\boldsymbol{\tau}}(t_r)\big)$$

we get successively from (3): $d_{\boldsymbol{\tau}}(t_r) \,|\, z_{\boldsymbol{\tau}}(t_r)^2$, $d_{\boldsymbol{\tau}}(t_r) \,|\, z_{\boldsymbol{\tau}}(t_r)$, $d_{\boldsymbol{\tau}}(t_r)^2 \,|\, a(\boldsymbol{\tau}, t_r)x_{\boldsymbol{\tau}}(t_r)^2$, $d_{\boldsymbol{\tau}}(t_r) \,|\, x_{\boldsymbol{\tau}}(t_r)$ and hence $d_{\boldsymbol{\tau}}(t_r) \equiv 1$. Therefore, for $\boldsymbol{\tau}$ in T we have

$$b(\boldsymbol{\tau}, t_r) \equiv \left(\frac{z_{\boldsymbol{\tau}}(t_r)}{y_{\boldsymbol{\tau}}(t_r)}\right)^2 \equiv \beta_{\boldsymbol{\tau}}(t_r)^2 \bmod a(\boldsymbol{\tau}, t_r), \tag{4}$$

where $\beta_{\boldsymbol{\tau}}$ is in $\mathbb{Q}[t_r]$ and $|\beta_{\boldsymbol{\tau}}| < |a|$ or $\beta_{\boldsymbol{\tau}} = 0$.

In order to exploit the congruence (4) we note that for all nonnegative integers h,

$$t_r^h \equiv \sum_{l=0}^{|a|-1} \alpha_{hl}(\boldsymbol{t}) t_r^l \bmod a(\boldsymbol{t}, t_r),$$

where $\alpha_{hl}(\boldsymbol{t})$ are rational functions of $t_1, \ldots, t_{r-1}$ with powers of $a_0(\boldsymbol{t})$ in the denominator. For $\boldsymbol{\tau}$ in T we have $a_0(\boldsymbol{\tau}) \neq 0$, hence $\alpha_{hl}(\boldsymbol{t})$ are defined. Let

$$\beta_{\boldsymbol{\tau}} = \sum_{i=0}^{|a|-1} \xi_i t_r^i, \quad \xi_i \in \mathbb{Q}. \tag{5}$$

From (4) we get for $\boldsymbol{\tau}$ in T,

$$b(\boldsymbol{\tau}, t_r) \equiv \sum_{l=0}^{|a|-1} t_r^l \sum_{i,j=0}^{|a|-1} \xi_i \xi_j \alpha_{i+j,l}(\boldsymbol{\tau}) \bmod a(\boldsymbol{\tau}, t_r),$$

and if

$$b(\boldsymbol{t}, t_r) = \sum_{i=0}^{|a|} b_i(\boldsymbol{t}) t_r^i, \quad b_i(\boldsymbol{t}) \text{ in } \mathbb{Z}[\boldsymbol{t}]$$

we get

$$b_l(\boldsymbol{\tau}) + b_{|a|}(\boldsymbol{\tau}) \alpha_{|a|,l}(\boldsymbol{\tau}) = \sum_{i,j=0}^{|a|-1} \xi_i \xi_j \alpha_{i+j,l}(\boldsymbol{\tau}) \quad \text{for } l \leqslant |a| - 1. \tag{6}$$

Let u be a new indeterminate and $R(\boldsymbol{t}, t_r, u)$ be the resultant of the system of polynomials

$$\begin{gathered} \big(b_l(\boldsymbol{t}) + b_{|a|}(\boldsymbol{t}) \alpha_{|a|,l}(\boldsymbol{t})\big) x_{|a|}^2 - \sum_{i,j=0}^{|a|-1} x_i x_j \alpha_{i+j,l}(\boldsymbol{t}) \quad (0 \leqslant l < |a|), \\ \sum_{i=0}^{|a|-1} x_i t_r^i - x_{|a|} u \end{gathered} \tag{7}$$

with respect to the variables $x_0, \ldots, x_{|a|}$. We shall prove that $R(\boldsymbol{t}, t_r, u) \neq 0$.

By a known property of resultants (see [4], p. 11) the coefficient of $u^{2^{|a|}}$ in R is the resultant R_0 of the system obtained from (7) by substitution $x_{|a|} = 0$. If R_0 were 0, the system of homogeneous equations

$$\sum_{i,j=0}^{|a|-1} \xi_i^* \xi_j^* \alpha_{i+j,l}(\boldsymbol{t}) = 0 \tag{8}$$

would have nontrivial solutions ξ_i^* in the algebraic closure of $\mathbb{Q}(\boldsymbol{t})$. However, it then follows from (4), (5), (6), and (8) that

$$0 \equiv \Big(\sum_{i=0}^{|a|-1} \xi_i^* t_r^i \Big)^2 \bmod a(\boldsymbol{t}, t_r). \tag{9}$$

Since $a(\boldsymbol{t}, t_r)$ is square free, (9) implies

$$\sum_{i=0}^{|a|-1} \xi_i^* t_r^i \equiv 0 \bmod a(\boldsymbol{t}, t_r);$$

which is impossible since $|a(\boldsymbol{t}, t_r)| = |a|$.

Therefore $R_0 \neq 0$ and moreover $R_0 \in \mathbb{Q}(\boldsymbol{t})$. Let m be chosen so that

$$G(\boldsymbol{t}, t_r, u) = a_0(\boldsymbol{t})^m R(\boldsymbol{t}, t_r, u) \in \mathbb{Z}[\boldsymbol{t}, t_r, u].$$

Then $a_0(\boldsymbol{t})^m R_0(\boldsymbol{t})$ is the leading coefficient of G with respect to u.

Let

$$G(\boldsymbol{t}, t_r, u) = g_0(\boldsymbol{t}) \prod_{\varrho=1}^{q} G_\varrho(\boldsymbol{t}, t_r, u)$$

where $g_0 \in \mathbb{Z}[\boldsymbol{t}]$, $G_\varrho \in \mathbb{Z}[\boldsymbol{t}, t_r, u]$ and G_ϱ are irreducible over $\mathbb{Q}$ of positive degree and with leading coefficient $g_\varrho(\boldsymbol{t})$ with respect to u. We can order G_ϱ so that G_ϱ is of degree 1 in u for $\varrho \leqslant p$ and of degree at least 2 for $\varrho > p$. If for all $\varrho \leqslant p$ we have

$$H_\varrho(\boldsymbol{t}, t_r) = G_\varrho(\boldsymbol{t}, t_r, 0)^2 - b(\boldsymbol{t}, t_r) g_\varrho(\boldsymbol{t})^2 \not\equiv 0 \bmod a(\boldsymbol{t}, t_r)$$

then let the leading coefficient of the remainder from division of H_ϱ by $a(\boldsymbol{t}, t_r)$ in the ring $\mathbb{Q}(\boldsymbol{t})[t_r]$ be $f_\varrho(\boldsymbol{t}) a_0(\boldsymbol{t})^{-m_\varrho}$, where $f_\varrho \in \mathbb{Z}[\boldsymbol{t}]$. By Hilbert's irreducibility theorem there exist integers $\tau_1^0, \ldots, \tau_{r-1}^0$ such that the polynomials $G_\varrho(\boldsymbol{\tau}^0, t_r, u)$ are irreducible and

$$a_0(\boldsymbol{\tau}^0) c_0(\boldsymbol{\tau}^0) D(\boldsymbol{\tau}^0) \prod_{\varrho=1}^{p} f_\varrho(\boldsymbol{\tau}^0) \prod_{\varrho=0}^{q} g_\varrho(\boldsymbol{\tau}^0) \neq 0.$$

Clearly $\boldsymbol{\tau}^0$ is in T. It follows from (5) and (6) that for $\boldsymbol{t} = \boldsymbol{\tau}^0$, $u = \beta_{\boldsymbol{\tau}^0}(t_r)$ the system of polynomials (7) has a common zero

$$\big(\xi_0, \ldots, \xi_{|a|-1}, 1\big).$$

Since this zero is non-trivial we get successively

$$R\big(\boldsymbol{\tau}^0, t_r, \beta_{\boldsymbol{\tau}^0}(t_r)\big) = 0, \quad G\big(\boldsymbol{\tau}^0, t_r, \beta_{\boldsymbol{\tau}^0}(t_r)\big) = 0$$

and $G_\varrho\big(\boldsymbol{\tau}^0, t_r, \beta_{\boldsymbol{\tau}^0}(t_r)\big) = 0$ for a certain $\varrho \leqslant q$. Since $G_\varrho\big(\boldsymbol{\tau}^0, t_r, u\big)$ is irreducible of degree at least 2 in u for $\varrho > p$ we get $\varrho \leqslant p$

$$g_\varrho(\boldsymbol{\tau}^0) \beta_0(t_r) + G_\varrho(\boldsymbol{\tau}^0, t_r, 0) = 0.$$

Hence by (4)

$$g_\varrho(\boldsymbol{\tau}^0)^2 b(\boldsymbol{\tau}^0, t_r) - G_\varrho(\boldsymbol{\tau}^0, t_r, 0)^2 \equiv 0 \bmod a(\boldsymbol{\tau}^0, t_r)$$

and $f_\varrho(\boldsymbol{\tau}^0)$ contrary to the choice of $\boldsymbol{\tau}^0$. The obtained contradiction shows that for a certain $\varrho \leqslant p$

$$g_\varrho(\boldsymbol{t})^2 b(\boldsymbol{t}, t_r) - G_\varrho(\boldsymbol{t}, t_r, 0)^2 \equiv 0 \bmod a(\boldsymbol{t}, t_r).$$

Reducing $G_\varrho(\boldsymbol{t}, t_r, 0) g_\varrho(\boldsymbol{t})^{-1}$ modulo $a(\boldsymbol{t}, t_r)$ in the ring $\mathbb{Q}(\boldsymbol{t})[t_r]$ we find a

$\beta(\boldsymbol{t}, t_r) \in \mathbb{Q}(\boldsymbol{t})[t_r]$ such that

$$b(\boldsymbol{t}, t_r) \equiv \beta(\boldsymbol{t}, t_r)^2 \bmod a(\boldsymbol{t}, t_r) \tag{10}$$

and

$$|\beta| < |a| \quad \text{or} \quad \beta = 0. \tag{11}$$

We write

$$\beta^2(\boldsymbol{t}, t_r) - b(\boldsymbol{t}, t_r) = h^{-2}(\boldsymbol{t}) a(\boldsymbol{t}, t_r) A(\boldsymbol{t}, t_r)$$

where $h(\boldsymbol{t}) \in \mathbb{Z}[\boldsymbol{t}]$ and $A \in \mathbb{Z}[\boldsymbol{t}, t_r]$. In particular $h(\boldsymbol{t})\beta(\boldsymbol{t}, t_r) \in \mathbb{Z}[\boldsymbol{t}, t_r]$.

If $A(\boldsymbol{t}, t_r) \equiv 0$ identically, we can satisfy (2) by taking

$$x(\boldsymbol{t}, t_r) = 0, \quad y(\boldsymbol{t}, t_r) = h(\boldsymbol{t}), \quad z(\boldsymbol{t}, t_r) = h(\boldsymbol{t})\beta(\boldsymbol{t}, t_r).$$

If $A(\boldsymbol{t}, t_r)$ is not identically 0, we have by (11) that $|A| < |a|$. We now prove the hypotheses of the lemma are satisfied for the polynomials

$$A(\boldsymbol{t}, t_r), \quad b(\boldsymbol{t}, t_r), \quad C(\boldsymbol{t}, t_r) = a(\boldsymbol{t}, t_r)h(\boldsymbol{t})c(\boldsymbol{t}, t_r)A(\boldsymbol{t}, t_r).$$

We know that for all integers $\tau_1, \ldots, \tau_r$ such that $C(\boldsymbol{\tau}, \tau_r) \neq 0$, the equation (1) has a solution in integers x, y, z, not all 0. Taking

$$X = a(\boldsymbol{\tau}, \tau_r)x, \quad Y = h(\boldsymbol{\tau})\big(z - y\beta(\boldsymbol{\tau}, \tau_r)\big), \quad Z = h(\boldsymbol{\tau})\big(b(\boldsymbol{\tau}, \tau_r)\big)y - \beta(\boldsymbol{\tau}, \tau_r)z\big)$$

we obtain

$$A(\boldsymbol{\tau}, \tau_r)X^2 + b(\boldsymbol{\tau}, \tau_r)Y^2 - Z^2 = h(\boldsymbol{\tau})^2\big(\beta(\boldsymbol{\tau}, \tau_r)^2 - b(\boldsymbol{\tau}, \tau_r)\big)(ax^2 + by^2 - z^2) = 0.$$

Also X, Y, Z are integers not all 0, since $a(\boldsymbol{\tau}, \tau_r)h(\boldsymbol{\tau})A(\boldsymbol{\tau}, \tau_r) \neq 0$. The inductive hypothesis applies to the polynomials

$$A(\boldsymbol{t}, t_r), \ b(\boldsymbol{t}, t_r), \ C(\boldsymbol{t}, t_r) \quad \text{since} \quad |A| + |b| < |a| + |b| = n.$$

Hence there exist polynomials $X(\boldsymbol{t}, t_r), Y(\boldsymbol{t}, t_r), Z(\boldsymbol{t}, t_r)$ with integral coefficients and not all identically zero, such that

$$A(\boldsymbol{t}, t_r)X(\boldsymbol{t}, t_r)^2 + b(\boldsymbol{t}, t_r)Y(\boldsymbol{t}, t_r)^2 \equiv Z(\boldsymbol{t}, t_r)^2$$

identically in $\boldsymbol{t}, t_r$. Putting

$$\begin{aligned} x(\boldsymbol{t}, t_r) &= A(\boldsymbol{t}, t_r)X(\boldsymbol{t}, t_r), \\ y(\boldsymbol{t}, t_r) &= h(\boldsymbol{t})\big(\beta(\boldsymbol{t}, t_r)Y(\boldsymbol{t}, t_r) + Z(\boldsymbol{t}, t_r)\big), \\ z(\boldsymbol{t}, t_r) &= h(\boldsymbol{t})\big(b(\boldsymbol{t}, t_r)Y(\boldsymbol{t}, t_r) + \beta(\boldsymbol{t}, t_r)Z(\boldsymbol{t}, t_r)\big) \end{aligned}$$

we obtain (2). Further $x(\boldsymbol{t}, t_r), y(\boldsymbol{t}, t_r), z(\boldsymbol{t}, t_r)$ do not all vanish identically since neither $A(\boldsymbol{t}, t_r)$ nor $b(\boldsymbol{t}, t_r) - \beta^2(\boldsymbol{t}, t_r)$ vanish identically.

Remark. The argument following formula (11) is implicit in Skolem's paper [8].

3.

Theorem 1. *Let $a(t_1, \ldots, t_r)$, $b(t_1, \ldots, t_r)$ be polynomials with integral coefficients. Suppose that for all r-tuples of arithmetical progressions $P_1, \ldots, P_r$ there exist integers $\tau_i \in P_i$ such that the equation* (1) *has a solution in integers x, y, z not all* 0. *Then*

there exist polynomials $x(t_1, \ldots, t_r)$, $y(t_1, \ldots, t_r)$, $z(t_1, \ldots, t_r)$ *with integral coefficients, not all identically* 0, *such that* (2) *holds identically in* $t_1, \ldots, t_r$.

Proof. It is enough to show that the assumption of the theorem implies the assumption of the lemma. Now take any r-tuple of integers $\tau_1, \ldots, \tau_r$, an arbitrary prime p and a positive integer m. By the assumption of the theorem the arithmetical progressions $p^m t + \tau_1, \ldots, p^m t + \tau_r$ contain integers $\tau_1^0, \ldots, \tau_r^0$ respectively such that the equation

$$a(\tau_1^0, \ldots, \tau_r^0)x^2 + b(\tau_1^0, \ldots, \tau_r^0)y^2 = z^2$$

has a solution in integers not all 0. Hence it has a solution x_0, y_0, z_0 with $(x_0, y_0, z_0) = 1$ and we get

$$a(\tau_1, \ldots, \tau_r)x_0^2 + b(\tau_1, \ldots, \tau_r)y_0^2 \equiv z_0^2 \bmod p^m.$$

By Theorem 2 of §5 of [1] it follows that (1) is soluble nontrivially in the field of p-adic numbers. By Lemma 2 in §7 ibidem it follows that (1) is soluble nontrivially also in real numbers, hence by Theorem 1 of §7 ibidem it is soluble nontrivially in integers.

Added in proof. Slightly different proof of Theorem 1 valid for arbitrary number fields will appear in a forthcoming book [7] of the second author.

Theorem 2. *Let* $F(x, y, t_1, \ldots, t_r)$ *be any polynomial with integral coefficients which is of degree at most* 2 *in* x *and* y. *Suppose that for all* r*-tuples of arithmetical progressions* $P_1, \ldots, P_r$ *there exist integers* $\tau_i \in P_i$ *such that the equation*

$$F(x, y, \tau_1, \ldots, \tau_r) = 0$$

is soluble in rationals x, y. *Then there exist rational functions* $x(t_1, \ldots, t_r)$, $y(t_1, \ldots, t_r)$ *with rational coefficients such that*

$$F\big(x(t_1, \ldots, t_r), y(t_1, \ldots, t_r), t_1, \ldots, t_r\big) \equiv 0$$

identically in $t_1, \ldots, t_r$.

Proof. Theorem 2 follows from Theorem 1 for $r > 1$ in exactly the same way as Theorem B was derived from Theorem A (see [3]). In the argument (page 357) where the Corollary to Theorem 1 of [2] is used, one has instead to apply Theorem 2 of [6].

M. Fried has observed that Theorem B implies an analogous result for curves of genus 0 defined over $\mathbb{Q}(t)$. The remark applies, *mutatis mutandis*, to Theorem 2.

One can moreover extend it to equations that define a finite union of curves of genus 0 over the algebraic closure of $\mathbb{Q}(t)$. As to the curves of genus 1 it follows from the so-called Selmer's conjecture in the theory of rational points on such curves that for every integer t there is a rational solution of the equation

$$x^4 - (8t^2 + 5)^2 = y^2 \tag{12}$$

(see [9]). On the other hand, suppose that rational functions $x(t)$, $y(t)$ in $\mathbb{Q}(t)$ satisfy (12). There exist infinitely many integer pairs $\langle u, v\rangle$ such that $5u^2 + 8v^2$ is a prime p. Take u, v such that for $\tau = 5u/8v$, $x(\tau)$, $y(\tau)$ are defined. The equation (12) gives

$$\big(4vx(\tau)\big)^2 - 100p^2 = \big(16v^2 y(\tau)\big)^2.$$

But, by a theorem of Nagell [5] the Diophantine equation

$$X^4 - 100p^2 = Y^2 \quad (p \text{ prime} \equiv 1 \bmod 4)$$

has no rational solutions.

References

[1] Z. I. Borevich, I. R. Shafarevich, *Number Theory*. Academic Press, New York 1966.

[2] H. Davenport, D. J. Lewis, A. Schinzel, *Polynomials of certain special types*. Acta Arith. 9 (1964), 107–116; this collection: A6, 27–35.

[3] —, —, —, *Quadratic Diophantine equations with a parameter*. Acta Arith. 11 (1966), 353–358.

[4] F. S. Macaulay, *The Algebraic Theory of Modular Systems*. Reprint, New York and London 1964.

[5] T. Nagell, *Zahlentheoretische Notizen* I–IV. Vid. Skrifter, I Math. Naturv. Kl. 1923, No. 13, Kristiania 1924.

[6] A. Schinzel, *On Hilbert's Irreducibility Theorem*. Ann. Polon. Math. 16 (1965), 333–340; this collection: F1, 839–845.

[7] —, *Selected Topics on Polynomials*. The University of Michigan Press, Ann Arbor 1982.

[8] Th. Skolem, *Über die Lösung der unbestimmten Gleichung* $ax^2 + by^2 + cz^2 = 0$ *in einigen einfachen Rationalitätsbereichen*. Norsk. Mat. Tidsskr. 10 (1928), 50–62.

[9] N. M. Stephens, *Congruence properties of congruent numbers*. Bull. London Math. Soc. 7 (1975), 182–184.

Originally published in
Bulletin of the London Mathematical Society
14 (1982), 345–348

Selmer's conjecture and families of elliptic curves

with J. W. S. Cassels (*Cambridge*)

1.

In this note we consider the elliptic curve

$$\mathscr{A} : y^2 = x\{x^2 - (1 + t^4)^2\} \tag{1.1}$$

over the field $\mathbb{C}(t)$ of rational functions with complex coefficients. It turns out that all $\mathbb{C}(t)$-rational points on $\mathscr{A}$ satisfy $x, y \in \mathbb{Q}(\sqrt{2}, i, t)$. As a consequence, the curve

$$\mathscr{B} : y^2 = x\{x^2 - (7 + 7t^4)^2\} \tag{1.2}$$

has only points of order 2 over $\mathbb{Q}(t)$. On the other hand, the famous conjecture of Selmer [7] is shown to imply that for every rational r the curve

$$\mathscr{B}_r : y^2 = x\{x^2 - (7 + 7r^4)^2\} \tag{1.3}$$

has infinitely many rational points.

To place this phenomenon in a more general setting, let $R = \mathbb{Q}[t]$ and let $F \in R[x, y]$ be irreducible over the algebraic closure of $\mathbb{Q}(t)$. If x, y are regarded as coordinates of affine space, the equation $F = 0$ defines an affine curve over $\mathbb{Q}(t)$ and also a family of affine curves $F(x, y, r) = 0$ over $\mathbb{Q}$, as r runs over the elements of $\mathbb{Q}$ such that $F(x, y, r)$ is absolutely irreducible (the remaining values of r form a finite set E).

Let $\mathscr{C}$ be the projective curve defined over $\mathbb{Q}(t)$ obtained from normalization of the completion of the curve $F = 0$ and let $\mathscr{C}_r$ be the normalization of the completion of the affine curve $F(x, y, r) = 0$ for $r \in \mathbb{Q} \setminus E$.

If $\mathscr{C}$ is a curve of genus 1, then for all but finitely many values $r \in \mathbb{Q} \setminus E$ the curve $\mathscr{C}_r$ is also of genus 1. Without further comment we ignore the exceptional values of r. Let $\mathscr{C}\big(\mathbb{Q}(t)\big)$ denote the set of $\mathbb{Q}(t)$-rational points on $\mathscr{C}$, and $\mathscr{C}_r(\mathbb{Q})$ the set of $\mathbb{Q}$-rational points on $\mathscr{C}_r$.

If $\mathscr{C}\big(\mathbb{Q}(t)\big)$ and $\mathscr{C}_r(\mathbb{Q})$ are nonempty, they have natural structure as groups when one point is selected as origin. They are finitely generated by virtue, respectively, of the theorems of Néron ([6], Théorème 3) and of Mordell. Let $g(\mathscr{C})$ (respectively $g(\mathscr{C}_r)$) be the reduced rank of $\mathscr{C}\big(\mathbb{Q}(t)\big)$ (respectively $\mathscr{C}_r(\mathbb{Q})$). Néron has shown (ibid., Théorème 6) that there are infinitely many $r \in \mathbb{Q}$ such that $g(\mathscr{C}_r) \geqslant g(\mathscr{C})$. Our example shows that there can be strict inequality for every rational r.

An analogous result where r is restricted to values in $\mathbb{Z}$ has been obtained by D. J. Lewis and A. Schinzel [4]. The curve $\mathscr{C}$ given by $y^2 = x^4 - (8t^2+5)^2$ has $g(\mathscr{C}) = 0$, but Selmer's Conjecture implies that $g(\mathscr{C}_r) \geqslant 1$ for every integer r. In this example, however, $g(\mathscr{C}_r) = 0$ for infinitely many rational r.

The following fundamental problem of M. Fried remains open. If, in the language above, $\mathscr{C}\big(\mathbb{Q}(t)\big)$ is empty, does there exist $r \in \mathbb{Q}$ for which $\mathscr{C}_r(\mathbb{Q})$ is empty?

The original version of this note was written by the second author (A. Schinzel). It contained proofs of the statements about the behaviour of $\mathscr{B}$ over $\mathbb{Q}(t)$ and of $\mathscr{B}_r$ over $\mathbb{Q}$ but not the more general result about $\mathscr{A}$. During the preparation of that version he was visiting the University of California, Irvine. He wishes to thank the University for its hospitality and Dr. L. J. Colliot-Thélène and Professor M. Fried for their valuable suggestions, which have been partially incorporated in the present version.

2.

In this section we prove

Theorem 1. *If $x, y \in \mathbb{C}(t)$ satisfy*

$$y^2 = x\{x^2 - (1+t^4)^2\}, \tag{2.1}$$

then $x, y \in \mathbb{Q}(i, \sqrt{2}, t)$. All solutions may be described explicitly.

Proof. We extend the base field to $\mathbb{C}(s, t)$, where $s^2 = 1 + t^4$.

Then

$$\eta^2 = \xi(\xi^2 - 1),$$

where

$$\eta = y/s^3, \quad \xi = x/s^2 = x/(1+t^4).$$

On putting

$$u = t^2 - s, \quad v = 2^{1/2}tu, \tag{2.2}$$

we have

$$s = -\tfrac{1}{2}(u + u^{-1}), \quad t = v/2^{1/2}u,$$

and

$$v^2 = u(u^2 - 1).$$

We therefore work on the elliptic curve

$$Y^2 = X(X^2 - 1), \tag{2.3}$$

whose ring of complex multiplications is $\mathbb{Z}[i]$. By hypothesis,

$$\xi, \eta \in \mathbb{C}(s, t) = \mathbb{C}(u, v).$$

Hence in terms of group addition on (2.3) we have

$$(\xi, \eta) = \alpha(u, v) + (u_0, v_0), \tag{2.4}$$

where $\alpha \in \mathbb{Z}[i]$ and (u_0, v_0) with $u_0, v_0 \in \mathbb{C}$ is a constant point. Here we use the fact that any rational map of an elliptic curve into itself is a complex multiplication followed by a translation. (For the corresponding result for abelian varieties of any dimension cf. Mumford ([5], p. 43, Corollary 1), Swinnerton-Dyer ([9], Theorem 32) or Lang ([3], Chapter II, Theorem 4).)

Let $(')$ denote the automorphism of $\mathbb{C}(s, t)/\mathbb{C}(t)$. Then

$$u' = -1/u, \quad v' = -v/u^2,$$

and so

$$(u, v)' = -(u, v) + (0, 0). \tag{2.5}$$

Here $(0, 0)$ is of order $1 + i$ on (2.3). We require that $x, y \in \mathbb{C}(t)$, and so

$$\xi' = \xi, \quad \eta' = -\eta;$$

that is

$$(\xi, \eta)' = (\xi, -\eta) = -(\xi, \eta). \tag{2.6}$$

On comparing (2.4), (2.5), (2.6) we see that a necessary and sufficient condition that $x, y \in \mathbb{C}(t)$ is

$$\alpha(0, 0) = 2(u_0, v_0). \tag{2.7}$$

Hence for given α there are precisely 4 values of $(u_0, v_0) \in \mathbb{C}^2$ which will do. More precisely, *either* (i) $\alpha(0, 0)$ is the point $\mathbf{0}$ at infinity, in which case (u_0, v_0) is $\mathbf{0}$ or a point of order 2 *or* (ii) $\alpha(0, 0) = (0, 0)$, in which case (u_0, v_0) is one of the points $\big(i, \pm(1-i)\big)$, $\big(-i, \pm(1+i)\big)$. Hence there are 4 solutions of (2.1) defined over $\mathbb{C}(t)$ for every $\alpha \in \mathbb{Z}[i]$. Since the complex multiplication is defined over $\mathbb{Q}(i)$ and the only other irrationality we have used is the $\sqrt{2}$ in (2.2), the truth of the theorem follows. □

The proof of the statement in §1 about (1.2) follows almost immediately. More generally, we have the

Corollary. *Let d be a positive integer and suppose that*

$$\mu^2 = \lambda\big\{\lambda^2 - d^2(1 + t^4)^2\big\}$$

has a solution $\lambda, \mu \in \mathbb{Q}(t)$ with $\mu \neq 0$. Then d is a square or twice a square.

Proof. The point $x = d^{-1}\lambda$, $y = d^{-3/2}\mu$ is a solution of (2.1) defined over $\mathbb{C}(t)$. It is defined over $\mathbb{Q}(i, \sqrt{2}, t)$ only if $\mu = 0$ or if d is of the shape specified. □

3.

In this section we prove the assertions in §1 about (1.3):

Theorem 2. *Selmer's Conjecture* [7] *implies that for any* $r \in \mathbb{Q}$ *the Mordell-Weil rank of*

$$y^2 = x\{x^2 - (7 + 7r^4)^2\} \tag{3.1}$$

is odd, and so there are infinitely many rational points on (3.1).

Proof. Let $r = l/m$ with $l, m \in \mathbb{Z}$, $(l, m) = 1$. Then $X = m^4 x$, $Y = m^6 y$ satisfy

$$Y^2 = X(X^2 - n^2), \tag{3.2}$$

where

$$n = 7l^4 + 7m^4 \equiv 6, 7 \pmod 8.$$

We have now only to invoke the result of Stephens [8] that, subject to the Selmer conjecture, the rank of (3.2) is odd whenever $n \equiv 5, 6, 7 \pmod 8$ is a positive integer. □

4.

We conclude with three remarks.

(i) We have been unable to find an equianharmonic curve with similar properties to (1.2). However

$$\mathscr{C} : x^3 + y^3 = 27(2t + 1)^2 + 1$$

has only finitely many points over $\mathbb{Q}(t)$, whereas on Selmer's Conjecture the specializations $\mathscr{C}_r$ for $r \in \mathbb{Z}$ all have odd rank.

(ii) The ideas of §2 rapidly show that the only solutions $x, y \in \mathbb{C}(t)$ of

$$y^2 = x\{x^2 - (1 + t^2)^2\} \tag{4.1}$$

have $y = 0$. One extends the ground field to $\mathbb{C}(s, t)$, where

$$s^2 = 1 + t^2. \tag{4.2}$$

Here (4.2) has genus 0 and Lüroth's Theorem applies.

(iii) Presumably the general techniques of Christie [2] (cf. also [1]) for elliptic curves over $\mathbb{C}(t)$ could be used to prove Theorem 1, but not so simply.

References

[1] J. W. S. Cassels, *A Diophantine equation over a function field*. J. Austral. Math. Soc. Ser. A 25 (1978), 489–496.

[2] M. R. Christie, *Positive definite functions of two variables which are not sums of three squares*. J. Number Theory 8 (1976), 224–232.

[3] S. Lang, *Abelian Varieties*. Interscience Publ., New York and London 1959.

[4] D. J. Lewis, A. Schinzel, *Quadratic Diophantine equations with parameters*. Acta Arith. 37 (1980), 133–141; this collection: A10, 54–61.

[5] D. Mumford, *Abelian Varieties*. Oxford Univ. Press, London 1970.

[6] A. Néron, *Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps*. Bull. Soc. Math. France 80 (1952), 101–166.

[7] E. Selmer, *A conjecture concerning rational points on cubic curves*. Math. Scand. 2 (1954), 49–54.

[8] N. M. Stephens, *Congruence properties of congruent numbers*. Bull. London Math. Soc. 7 (1975), 182–184.

[9] H. P. F. Swinnerton-Dyer, *Analytic Theory of Abelian Varieties*. Cambridge Univ. Press, London–New York 1974.

Originally published in
Acta Arithmetica XL (1982), 399–420

Families of curves having each an integer point

H. Davenport, D. J. Lewis and the writer [3] proved that if an equation with integral coefficients $F(x, y, t) = 0$ quadratic in x and y is solvable in rational x, y for at least one integer t from every arithmetic progression, then the equation is solvable in rational functions $x(t), y(t) \in \mathbb{Q}(t)$. The question has been raised whether the solvability of $F(x, y, t) = 0$ in integers x, y for all integers t implies the solvability of the equation in polynomials. It is the aim of the present paper to study this question in a more general context. We shall prove

Theorem 1. *If $L \in \mathbb{Z}[x, t]$ is of degree at most four in x, $M \in \mathbb{Z}[t]$ and every arithmetic progression contains an integer t^* such that $L(x, t^*) = M(t^*)y$ is solvable in integers x, y then there exist polynomials $X, Y \in \mathbb{Q}[t]$ such that $L\big(X(t), t\big) = M(t)Y(t)$.*

The theorem is no longer true in general if the degree of L is greater than four. Also for L of degree non-exceeding four the conclusion cannot in general be strenghtened to assert the existence of integer valued polynomials X, Y. The relevant examples will be given after the proof of Theorem 1. Theorem 1 easily implies

Theorem 2. *If $F \in \mathbb{Z}[x, y, t]$, the highest homogeneous part F_0 of F with respect to x, y is quadratic and singular and every arithmetic progression contains an integer t^* such that $F(x, y, t^*)$ is solvable in integers x, y, then there exist polynomials $X, Y \in \mathbb{Q}[t]$ such that $F\big(X(t), Y(t), t\big) = 0$.*

It seems likely that if we assume the solvability of $F(x, y, t) = 0$ in integers x, y for all $t^* \in \mathbb{Z}$, the conclusion remains true provided F_0 is reducible over $\mathbb{Q}(t)$. However, in general the conclusion fails as it is shown by the following

Theorem 3. *The equation $x^2-(4t^2+1)^3y^2 = -1$ is solvable in integers x, y for all $t^* \in \mathbb{Z}$, but there exist no polynomials $X, Y \in \mathbb{Q}[t]$ such that $X(t)^2 - (4t^2 + 1)^3 Y(t)^2 = -1$.*

Prompted by a question from Professor J. Leicht I have studied the possibility of modifying the assumptions of Theorem 1 so that they would imply the existence of integer valued polynomials X, Y. The result is the following

Theorem 4. *Let n be a positive integer $\not\equiv 0 \pmod 8$, $A, B, M \in \mathbb{Z}[t]$. If every arithmetic progression contains an integer t^* such that $A(t^*)x^n + B(t^*) = M(t^*)y$ is solvable in integers x, y, then there exist integer valued polynomials X, Y such that $A(t)X(t)^n + B(t) = M(t)Y(t)$.*

The condition $n \not\equiv 0 \pmod 8$ cannot be relaxed, as I shall show by an example. For $n = 1$ Theorem 4 is contained in a more general result of Skolem [8] concerning polynomials in many variables. According to Skolem the polynomials A, B, M may have any number of variables provided A and M have no common zero. I shall show by an example that already for $n = 2$ the corresponding statement is false. The possibility of extending Theorems 1, 2, and 4 to polynomials in many variables will be studied in a subsequent paper.

For the proof of the above theorems we need several lemmata.

Lemma 1. *Let D be a Dedekind domain, $f, g, h \in D[x]$, $\mathfrak{p}$ be a prime ideal of D, $f(x) \equiv g(x)h(x) \pmod{\mathfrak{p}}$. If g, h are relatively prime $\bmod \mathfrak{p}$ and the leading coefficient of g is 1, then for every integer $n \geqslant 0$ there exist polynomials $g_n, h_n \in D[x]$ such that*

$$f(x) \equiv g_n(x)h_n(x) \pmod{\mathfrak{p}^{n+1}}, \tag{1}$$

(2) *the degree of g_n equals the degree of g, the leading coefficient of g_n is 1,*

$$g_n(x) \equiv g(x), \quad h_n(x) \equiv h(x) \pmod{\mathfrak{p}}. \tag{3}$$

Proof. This lemma is closely related to Hensel's lemma and can be derived by following the proof of Hensel's lemma given by Hasse [6] up to the point where the solvability of the congruence

$$g_{n-1}z_n + h_{n-1}y_n \equiv f_n \pmod{\mathfrak{p}}, \quad f_n \in D[x]$$

in polynomials $y_n, z_n \in D[x]$ is needed. Then since g_{n-1}, h_{n-1} are relatively prime $\bmod \mathfrak{p}$ we use the fact that $D/\mathfrak{p}$ is a field. □

Lemma 2. *Let D be a principal ideal domain, $a, b, c \in D$, (p) be a prime ideal of D. If $p \nmid 2a$ and $d = b^2 - 4ac$ the congruence*

$$ax^2 + bx + c \equiv 0 \pmod{p^\nu} \tag{4}$$

is solvable in $x \in D$ if and only if either $\operatorname{ord}_p d \geqslant \nu$ or $\operatorname{ord}_p d = \delta \equiv 0 \pmod 2$ and the congruence $z^2 \equiv dp^{-\delta} \pmod p$ is solvable in D.

Proof. The congruence (4) is equivalent to

$$(2ax + b)^2 \equiv d \pmod{4ap^\nu}$$

and since $p \nmid 2a$, it is solvable if and only if $y^2 \equiv d \pmod{p^\nu}$ is.

If $\delta = \operatorname{ord}_p d \geqslant \nu$ it is enough to take $y = 0$. If $\delta < \nu$, the congruence implies $\delta = 2 \operatorname{ord}_p y \equiv 0 \pmod 2$ and $y = p^{\delta/2}z$, $z^2 \equiv dp^{-\delta} \pmod{p^{\nu-\delta}}$. Thus the necessity of the condition given in the lemma follows. On the other hand, if the condition is satisfied and $z_0^2 \equiv dp^{-\delta} \pmod p$, $z_0 \in D$, we can apply Lemma 1 with

$$f(x) = x^2 - dp^{-\delta}, \quad g(x) = x - z_0, \quad h(x) = x + z_0, \quad n = \nu - \delta - 1.$$

The congruence

$$x^2 - dp^{-\delta} \equiv g_n(x)h_n(x) \pmod{p^{n+1}},$$

where $\deg g_n = \deg g = 1$ and the leading coefficient of g_n is 1, implies that $x^2 \equiv dp^{-\delta}$ (mod p^δ) has solutions $\pm g_n(0)$. Multiplying by p^δ, we get

$$\left(p^{\delta/2} g_n(0)\right)^2 \equiv d \pmod{p^\nu}. \qquad \square$$

Remark. The lemma can easily be modified so that it would apply to all Dedekind domains. It is also possible, although not so easy, to prove analogous statements about congruences of degree three and four. For instance, if D is a principal ideal domain, $a, b \in D$, (p) is a prime ideal of D, $p \nmid 3$, then the congruence

$$x^3 + ax + b \equiv 0 \pmod{p^\nu}$$

is solvable in $x \in D$ if and only if either $\operatorname{ord}_p b \geqslant \nu$ or $2 \operatorname{ord}_p b > 3 \operatorname{ord}_p a$ or $3 \mid \beta = \operatorname{ord}_p b < \nu$, $2\beta \leqslant 3 \operatorname{ord}_p a$ and the congruence $z^3 + ap^{-2\beta/3} + bp^{-\beta} \equiv 0 \pmod{p}$ is solvable.

Lemma 3. *If $A, B \in \mathbb{Z}[t]$, $(A, B) = 1$, then for sufficiently large primes p the divisibility $p \mid A(t^*)$, $t^* \in \mathbb{Z}$, implies $p \nmid B(t^*)$.*

Proof. Let R be the resultant of A and B. Since $(A, B) = 1$, we have $R \neq 0$ and there exist polynomials $U, V \in \mathbb{Z}[t]$ such that $AU + BV = R$. Now, if $p \nmid R$ we have either $p \nmid A(t^*)$ or $p \nmid B(t^*)$. $\square$

Lemma 4. *Let K be an algebraic number field, $F \in K[x]$ be of degree at most four. If the congruence $F(x) \equiv 0 \pmod{\mathfrak{p}}$ is solvable for almost all prime ideals of degree 1 in K then the equation $F(x) = 0$ is solvable in K.*

Proof. If $F(x)$ is irreducible in K then the lemma follows from the more general result of Hasse [5]. If $F(x)$ is reducible in K but has no zero there then its degree must be four. If now the congruence $F(x) \equiv 0 \pmod{\mathfrak{p}}$ is solvable for almost all ideals $\mathfrak{p}$ of K rather than for almost all prime ideals $\mathfrak{p}$ of degree 1 in K then the assertion holds in virtue of Proposition 2 in Fujiwara [4]. However, in the proof of this proposition only prime ideals of degree 1 are needed. $\square$

Lemma 5. *Let $A_i, B_i, C_i \in \mathbb{Z}[t]$ $(i = 1, 2)$, let $P \in \mathbb{Z}[t]$ be a primitive irreducible polynomial, $A_1 A_2 \not\equiv 0 \pmod{P}$ and the polynomials $A_i(t)x^2 + B_i(t)x + C_i(t)$ $(i = 1, 2)$ be prime $\bmod P(t)$. If for all sufficiently large primes p and all integers t^* such that $p \parallel P(t^*)$ the congruence*

$$\prod_{i=1}^{2} \left(A_i(t^*)x^2 + B_i(t^*)x + C_i(t^*)\right) \equiv 0 \pmod{p^\mu} \tag{5}$$

is solvable in $x \in \mathbb{Z}$ then the congruence

$$\prod_{i=1}^{2} \left(A_i(t)x^2 + B_i(t)x + C_i(t)\right) \equiv 0 \left(\bmod P(t)^\mu\right) \tag{6}$$

is solvable in $\mathbb{Q}[t]$.

Proof. Let $D_i(t) = B_i(t)^2 - 4A_i(t)C_i(t) = P(t)^{\delta_i} E_i(t)$, where $P_i \nmid E_i$ $(i = 1, 2)$. (If $D_1 = 0$ or $D_2 = 0$ (6) is clearly solvable.) If for an $i \leqslant 2$, $\delta_i \geqslant \mu$ the congruence $A_i(t)x^2 + B_i(t)x + C_i(t) \equiv 0 \left(\mathrm{mod}\ P(t)^\mu\right)$ is solvable in virtue of Lemma 2 applied with $D = \mathbb{Q}[t]$, hence (6) is solvable also.

Let $P(\vartheta) = 0$, $K = \mathbb{Q}(\vartheta)$, $\mathfrak{p}$ be a prime ideal of degree 1 in K with norm p assumed sufficiently large. Choose $t^* \equiv \vartheta \,(\mathrm{mod}\,\mathfrak{p})$. Then $P(t^*) \equiv 0 \,(\mathrm{mod}\, p)$, $P(t^* + p) \equiv 0 \,(\mathrm{mod}\, p)$, $P(t^* + p) - P(t^*) \equiv pP'(t^*) \,(\mathrm{mod}\, p^2)$. Since $(P', P) = 1$, we have by Lemma 3 $P'(t^*) \not\equiv 0 \,(\mathrm{mod}\, p)$, thus $P(t^*) \not\equiv 0 \,(\mathrm{mod}\, p^2)$ or $P(t^* + p) \not\equiv 0 \,(\mathrm{mod}\, p^2)$. Replacing t^* by $t^* + p$ if necessary we may assume that $P(t^*) \not\equiv 0 \,(\mathrm{mod}\, p^2)$, and that (5) holds for a suitable $x = x^* \in \mathbb{Z}$.

Let $R(t)$ be the resultant of $A_i(t)x^2 + B_i(t)x + C_i(t)$ $(i = 1, 2)$ with respect to x. By the assumption we have $\big(P(t), R(t)\big) = 1$ and by Lemma 3 $R(t^*) \not\equiv 0 \,(\mathrm{mod}\, p)$. On the other hand, if we had

$$A_i(t^*)x^{*2} + B_i(t^*)x^* + C_i(t^*) \equiv 0 \,(\mathrm{mod}\, p) \quad (i = 1, 2)$$

it would follow that $R(t^*) \equiv 0 \,(\mathrm{mod}\, p)$. Thus there exists an $i \leqslant 2$ such that

$$A_i(t^*)x^{*2} + B_i(t^*)x^* + C_i(t^*) \equiv 0 \,(\mathrm{mod}\, p^\mu).$$

Since $(P, E_i) = 1$, we have by Lemma 3 $p \nmid E_i(t^*)$. Thus $\mathrm{ord}_p\, D_i(t^*) = \delta_i$ and by Lemma 2 applied with $D = \mathbb{Z}$ we have $\delta_i \equiv 0 \,(\mathrm{mod}\, 2)$ and $\left(\dfrac{D_i(t^*)p^{-\delta_i}}{p}\right) = 1$, whence $\left(\dfrac{E_i(t^*)}{p}\right) = 1$.

Now $E_i(t^*) \equiv E_i(\vartheta) \,(\mathrm{mod}\,\mathfrak{p})$ and we get $\left(\dfrac{E_i(\vartheta)}{\mathfrak{p}}\right) = 1$.

Take in Lemma 4

$$F(x) = \prod_{i=1}^{2} \left(\frac{1 + (-1)^{\delta_i}}{2} x^2 - E_i(\vartheta)\right).$$

We infer that for almost all prime ideals $\mathfrak{p}$ of degree 1 in K the congruence $F(x) \equiv 0 \,(\mathrm{mod}\,\mathfrak{p})$ is solvable in K. Hence by Lemma 4 $F(x)$ has a zero in K and since $E_1(\vartheta)E_2(\vartheta) \neq 0$, it follows that for an $i \leqslant 2$ we have $\delta_i \equiv 0 \,(\mathrm{mod}\, 2)$ and $E_i(\vartheta) = G(\vartheta)^2$ where $G \in \mathbb{Q}[t]$. Hence

$$E_i(t) \equiv G(t)^2 \left(\mathrm{mod}\ P(t)\right)$$

and by Lemma 2 the congruence $A_i(t)x^2 + B_i(t)x + C_i(t) \equiv 0 \left(\mathrm{mod}\ P(t)^\mu\right)$ is solvable in $\mathbb{Q}[t]$. □

Lemma 6. *Let $L \in \mathbb{Z}[x, t]$ be of degree at most 4 in x, let $P \in \mathbb{Z}[t]$ be irreducible and primitive. If for all sufficiently large primes p and all integers t^* such that $p \parallel P(t^*)$ the congruence $L(x, t^*) \equiv 0 \,(\mathrm{mod}\, p^\mu)$ is solvable in $\mathbb{Z}$ then $L(x, t) \equiv 0 \left(\mathrm{mod}\ P(t)^\mu\right)$ is solvable in $\mathbb{Q}[t]$.*

Proof (by induction on μ). We set $K = \mathbb{Q}(\vartheta)$, where $P(\vartheta) = 0$.

$\mu = 1$. Let $\mathfrak{p}$ be a prime ideal of degree 1 in K with norm p assumed sufficiently large, $t^* \equiv \vartheta \pmod{\mathfrak{p}}$. The argument used in the proof of Lemma 5 shows that without loss of generality we may assume $p \parallel P(t^*)$. Hence $L(x^*, t^*) \equiv 0 \pmod{p}$ for an x^* in $\mathbb{Z}$,

$$L(x^*, \vartheta) \equiv 0 \pmod{\mathfrak{p}}$$

and by Lemma 4 $L(x, \vartheta)$ has a zero in K. Denoting this zero by $X(\vartheta)$, $X \in \mathbb{Q}[t]$, we infer from $L\big(X(\vartheta), \vartheta\big) = 0$ that

$$L\big(X(t), t\big) \equiv 0 \big(\bmod P(t)\big).$$

The inductive step. Suppose that the lemma is true for exponents less than $\mu \geqslant 2$ and all polynomials L satisfying the assumptions. Let the congruence $L(x, t^*) \equiv 0 \pmod{p^\mu}$ be solvable in $\mathbb{Z}$ for all sufficiently large primes p and all integers t^* such that $p \parallel P(t^*)$. By the case $\mu = 1$, $L(x, \vartheta)$ has a zero in K. If $L(x, \vartheta) = 0$ identically then $L(x, t) = P(t)L_1(x, t)$, $L_1 \in \mathbb{Z}[x, t]$. For all sufficiently large primes p and all integers t^* such that $p \parallel P(t^*)$ the congruence $L(x, t^*) \equiv 0 \pmod{p^{\mu-1}}$ is solvable. Hence by the inductive assumption there exists an $X \in \mathbb{Q}[t]$ such that $L\big(X(t), t\big) \equiv 0 \big(\bmod p^{\mu-1}(t)\big)$ and then $L\big(X(t), t\big) \equiv 0 \big(\bmod P^\mu(t)\big)$. If $L(x, \vartheta)$ has a simple zero we have

$$L(x, \vartheta) = G(x, \vartheta)H(x, \vartheta)$$

where $G, H \in \mathbb{Q}[x, t]$, both the degree and the leading coefficient of G with respect to x are 1 and $\big(G(x, \vartheta), H(x, \vartheta)\big) = 1$. Hence

$$L(x, t) \equiv G(x, t)H(x, t) \big(\bmod P(t)\big),$$

G, H relatively prime mod P and by Lemma 1 applied with $D = \mathbb{Q}[t]$, $\mathfrak{p} = \big(P(t)\big)$ we infer that

$$L(x, t) \equiv G_{\mu-1}(x, t)H_{\mu-1}(x, t) \big(\bmod P^\mu(t)\big),$$

where $G_{\mu-1}(x, t)$ is of degree 1 in x with the leading coefficient 1. Therefore, $L\big(-G_{\mu-1}(0, t), t\big) \equiv 0 \big(\bmod P^\mu(t)\big)$.

If $L(x, \vartheta)$ is a product of two coprime quadratic factors we have $L(x, t) \equiv G(x, t)H(x, t) \big(\bmod P(t)\big)$, $G, H \in \mathbb{Q}[x, t]$, where G, H are quadratic in x, relatively prime mod $P(t)$ and we may assume without loss of generality that the leading coefficient of G with respect to x is 1. By Lemma 1 applied with $D = \mathbb{Q}[t]$, $\mathfrak{p} = \big(P(t)\big)$ we have

$$L(x, t) \equiv G_{\mu-1}(x, t)H_{\mu-1}(x, t) \big(\bmod P^\mu(t)\big), \tag{7}$$

where polynomials $G_{\mu-1}, H_{\mu-1} \in \mathbb{Q}[t]$ are quadratic with respect to x and relatively prime mod $P(t)$, moreover their leading coefficients are not divisible by $P(t)$. For a suitable integer $d \neq 0$ we have

$$dG_{\mu-1}(x, t), dH_{\mu-1}(x, t) \in \mathbb{Z}[x, t]$$

and

$$d^2 P^{-\mu}(t)\big(L(x, t) - G_{\mu-1}(x, t)H_{\mu-1}(x, t)\big) \in \mathbb{Z}[x, t].$$

Hence the solvability of the congruence $L(x, t^*) \equiv 0 \pmod{p^\mu}$, for $p \parallel P(t^*)$ implies the

solvability of the congruence

$$dG_{\mu-1}(x,t^*)dH_{\mu-1}(x,t^*)\equiv 0 \pmod{p^\mu}.$$

In virtue of Lemma 5 there exists an $X\in\mathbb{Q}[t]$ such that

$$dG_{\mu-1}\big(X(t),t\big)dH_{\mu-1}\big(X(t),t\big)\equiv 0 \pmod{P^\mu(t)}$$

and then by (7) $L\big(X(t),t\big)\equiv \pmod{P(t)^\mu}$.

There remains only the case where $L(x,\vartheta)=c(x-a)^r$, $a,c\in K$, $c\neq 0$, $r\geqslant 2$.

Let $c=C(\vartheta)$, $a=A(\vartheta)$, where $A,C\in\mathbb{Q}[t]$. We have

$$L(x,t)\equiv C(t)\big(x-A(t)\big)^r \pmod{P(t)},\quad (P,C)=1$$

and the congruence $L(x^*,t^*)\equiv 0 \pmod p$ for $p\parallel P(t^*)$ implies $x^*\equiv A(t^*) \pmod p$. (Note that $C(t^*)\not\equiv 0 \pmod p$ by Lemma 3.) Hence $x^*\equiv A(t^*)+P(t^*)y^* \pmod{p^\mu}$, $y^*\in\mathbb{Z}$ and we have

$$L\big(A(t^*)+P(t^*)y^*,t^*\big)\equiv 0 \pmod{p^\mu}. \tag{8}$$

Let $L_1(y,t)=L\big(A(t)+P(t)y,t\big)/P(t)$. We have for a suitable integer $l\neq 0$

$$lL_1(y,t)\in\mathbb{Z}[y,t].$$

The congruence (8) together with $p\parallel P(t^*)$ implies that

$$lL_1(y^*,t^*)\equiv 0 \pmod{p^{\mu-1}}.$$

By the inductive assumption there exists a polynomial $Y\in\mathbb{Q}[t]$ such that $lL_1\big(Y(t),t\big)\equiv 0 \pmod{P(t)^{\mu-1}}$ and then $L\big(A(t)+P(t)Y(t),t\big)\equiv 0 \pmod{P^\mu(t)}$. □

Proof of Theorem 1. If $M(t)=0$ the theorem follows from Theorem 1 of [2].

If $M(t)\neq 0$ let

$$M(t)=m\prod_{i=1}^{k}P_i(t)^{\mu_i}$$

be the canonical factorization of M into polynomials irreducible and primitive. Take an index $i\leqslant k$, a prime p and integer t_1^* such that $p\parallel P_i(t^*)$. The arithmetic progression $p^{\mu_i}u+t^*$ contains an integer t_1^* such that for suitable x^*, $y^*\in\mathbb{Z}$ we have $L(x^*,t_1^*)=M(t^*)y^*$. Clearly $L(x^*,t^*)\equiv L(x^*,t_1^*)\equiv 0 \pmod{p^\mu}$. Hence by Lemma 6 there exists a polynomial $X_i\in\mathbb{Q}[t]$ such that

$$L\big(X_i(t),t\big)\equiv 0 \pmod{P_i^{\mu_i}(t)}.$$

By the Chinese Remainder Theorem there exists a polynomial $X\in\mathbb{Q}[t]$ satisfying $X\equiv X_i(t) \pmod{P_i^{\mu_i}(t)}$ $(1\leqslant i\leqslant k)$. We get $L\big(X(t),t\big)\equiv 0 \pmod{\prod_{i=1}^{k}P_i^{\mu_i}(t)}$, hence

$$L\big(X(t),t\big)=M(t)Y(t),\quad Y(t)\in\mathbb{Q}[t].$$ □

Here is an example showing that Theorem 1 fails for polynomials L of degree 5 in x.

Example 1. Let $L(x,t) = (x^2+3)(x^3+3)$, $M(t) = 3t+1$. For every integer t^* we have $M(t^*) = \prod_{i=1}^{k} p_i^{\alpha_i} \prod_{j=1}^{l} q_j^{\beta_j}$, where p_i are primes $\equiv 1 \pmod 3$, q_j are primes $\equiv 2 \pmod 3$. The congruences $x^2+3 \equiv 0 \pmod{p_i^{a_i}}$ and $x^3+3 \equiv 0 \pmod{q_j^{\beta_j}}$ are solvable for all $i \leqslant k$, $j \leqslant l$. Denoting their solutions by x_i and x'_j, respectively, we can satisfy the equation $L(x,t^*) = M(t^*)y$ by taking $x \equiv x_i \pmod{p_i^{\alpha_i}}$, $x \equiv x'_j \pmod{q_j^{\beta_j}}$ $(1 \leqslant i \leqslant k$, $1 \leqslant j \leqslant l)$. On the other hand, the equation $L\big(X(t),t\big) = M(t)Y(t)$ where $X, Y \in \mathbb{Q}[t]$ would imply $X\big(-\frac{1}{3}\big)^2 + 3 = 0$ or $X\big(-\frac{1}{3}\big)^3 + 3 = 0$ hence $\sqrt{-3} \in \mathbb{Q}$ or $\sqrt[3]{-3} \in \mathbb{Q}$, which is impossible. (The idea comes from van der Waerden [12].)

The next example shows that the conclusion of Theorem 1 cannot be sharpened to assert the existence of integer valued polynomials $X(t), Y(t)$ satisfying $L\big(X(t),t\big) = M(t)Y(t)$.

Example 2. Let $L(x,t) = (2x+1)(3x+1)$, $M(t) = 5t+1$. For every integer t^* we have $M(t^*) = 2^\alpha N$, N odd. The congruences $2x+1 \equiv 0 \pmod N$, $3x+1 \equiv 0 \pmod{2^\alpha}$ are both solvable. Denoting their solutions by x_1 and x_2 respectively we can satisfy the equation $L(x,t^*) = M(t^*)y$ by taking $x \equiv x_1 \pmod N$, $x \equiv x_2 \pmod{2^\alpha}$. Suppose now that $X(t)$, $Y(t)$ are integer valued polynomials satisfying $L\big(X(t),t\big) = M(t)Y(t)$. Then clearly

$$\text{either} \quad 2X(t)+1 = (5t+1)Y_1(t) \quad \text{or} \quad 3X(t)+1 = (5t+1)Y_2(t), \qquad Y_1, Y_2 \in \mathbb{Q}[t]. \tag{9}$$

Let m be a positive integer such that $m_i Y_i \in \mathbb{Z}[t]$ $(i = 1 \text{ or } 2)$ and let $2^{\delta_1} \parallel m_1$, $3^{\delta_2} \parallel m_2$. Solving the congruence $5t+1 \equiv 0 \pmod{2^{\delta_1+1}}$ if $i = 1$ or $5t+1 \equiv 0 \pmod{3^{\delta_2+1}}$ if $i = 2$, we get from (9) a contradiction (the idea comes from Skolem [10]).

Proof of Theorem 2. By the assumption we have

$$F(x,y,t) = C(t)\big(A(t)x + B(t)y\big)^2 + D(t)x + E(t)y + F(0,0,t)$$

where $A, B, C, D, E \in \mathbb{Z}[t]$ and we can assume without loss of generality that $(A,B) = 1$.

Let R be the resultant of A and B and let $G, H \in \mathbb{Z}[t]$ be such that

$$A(t)G(t) + B(t)H(t) = R.$$

We set

$$A(t)x + B(t)y = u, \quad -H(t)x + G(t)y = v$$

and obtain

$$RF(x,y,t) = RC(t)u^2 + \big(D(t)G(t) + E(t)H(t)\big)u + \big(A(t)E(t) - B(t)D(t)\big)v + RF(0,0,t) = 0.$$

Moreover, if $x, y \in \mathbb{Z}$ we have $u, v \in \mathbb{Z}$. The assumptions of Theorem 1 are satisfied with

$$L(u,t) = RC(t)u^2 + \big(D(t)G(t) + E(t)H(t)\big)u + RF(0,0,t),$$
$$M(t) = A(t)E(t) - B(t)D(t).$$

By the said theorem there exist polynomials $U, V \in \mathbb{Q}[t]$ such that identically

$$L\big(U(t), t\big) = M(t)V(t).$$

Setting

$$X(t) = \frac{1}{R}[G(t)U(t) - B(t)V(t)],$$

$$Y(t) = \frac{1}{R}[H(t)U(t) - A(t)V(t)],$$

we get $X, Y \in \mathbb{Q}[t]$ and $F\big(X(t), Y(t), t\big) = 0$. □

Proof of Theorem 3. Setting

$$\big(2t^* + \sqrt{4t^{*2}+1}\big)^{4t^{*2}+1} = x + y(4t^{*2}+1)\sqrt{4t^{*2}+1},$$

we get for every integer t^* integers x, y satisfying

$$x^2 - (4t^{*2}+1)^3 y^2 = -1.$$

On the other hand, it has been proved already by Abel [1] that all solutions of an equation $U^2(t) - F(t)V^2(t) = \text{const} \neq 0$ are given by convergents of the continued fraction expansion of $\sqrt{F(t)}$. Since for $F(t) = 4t^2 + 1$

$$F(t) = 2t + \overline{\frac{1}{|4t} + \frac{1}{|4t} + \ldots},$$

we infer from the equation

$$X(t)^2 - (4t^2+1)^3 X(t)^2 = -1$$

that

$$X(t) + (4t^2+1)\sqrt{4t^2+1}\,Y(t) = c\big(2t \pm \sqrt{4t^2+1}\big)^n, \quad n \geqslant 0.$$

Hence

$$n(2t)^{n-1} \equiv 0 \pmod{4t^2+1},$$

$n = 0$, $X(t) = c$, $Y(t) = 0$ and $c^2 = -1$ contradicting $X \in \mathbb{Q}[t]$. □

For the proof of Theorem 4 we need four lemmata.

Lemma 7. *Let* $M(t) = m \prod_{i=1}^{k} P_i^{\mu_i}(t)$ *where polynomials* $P_i(t)$ *are coprime, irreducible and primitive,* $\mu_i > 0$. *Under the assumptions of the theorem and the conditions* $BM \neq 0$, $(A, M) = 1$ *there exist polynomials* $X_0, Y_0 \in \mathbb{Q}[t]$ *such that*

$$A(t)X_0(t)^n + B(t) = M(t)Y_0(t),$$

$$X_0(t) \equiv 0 \Big(\mathrm{mod} \prod_{i=1}^{k} P_i(t)^{-[-\beta_i/n]}\Big), \quad \textit{where} \quad P_i(t)^{\beta_i} \parallel B(t).$$

Proof. By the assumption, $P_i \nmid A$ $(1 \leqslant i \leqslant k)$. Set $B = P_i^{\beta_i} B_i$, where $P_i \nmid B$. By the Chinese Remainder Theorem for the ring $\mathbb{Q}[t]$ it is sufficient to show the solvability in this ring of each congruence

$$A(t)X(t)^n + B(t) \equiv 0 \left(\mathrm{mod}\ P_i^{\mu_i}(t)\right) \quad (1 \leqslant i \leqslant k). \tag{10}$$

Let $P_i(\vartheta) = 0$, $K = \mathbb{Q}(\vartheta)$ and let $\mathfrak{p}$ be a prime ideal of degree 1 in K with the norm p sufficiently large. We have $\vartheta \equiv t_0 \pmod{\mathfrak{p}}$ for a suitable $t_0 \in \mathbb{Z}$ and $P_i(t_0) \equiv 0 \pmod{\mathfrak{p}}$. Choosing $t_1 = t_0$ or $t_0 + p$ we can achieve that every $t^* \equiv t_1 \pmod{p^2}$ satisfies $p \parallel P_i(t^*)$. Moreover, since p is sufficiently large we have by Lemma 3 $p \nmid AB_i(t^*)$, whence $p^{\beta_i} \parallel B(t^*)$. If $\beta_i \geqslant \mu_i$ the congruence (10) has the solution $X = 0$. If $\beta_i < \mu_i$ the equality

$$A(t^*)x^n + B(t^*) = M(t^*)y$$

implies that $\beta_i \equiv 0 \pmod{n}$, $x \equiv 0 \pmod{p^{\beta_i/n}}$ and

$$\left(x P_i(t^*)^{-\beta_i/n}\right)^n \equiv -B_i(t^*)/A(t^*) \pmod{p}.$$

However,

$$\frac{B_i(t^*)}{A(t^*)} \equiv \frac{B_i(\vartheta)}{A(\vartheta)} \pmod{\mathfrak{p}}$$

and thus $-B_i(\vartheta)/A(\vartheta)$ is an nth power residue for almost all prime ideals of degree 1 in K. In virtue of Flanders' theorem [3a] $-B_i(\vartheta)/A(\vartheta) = C(\vartheta)^n$, where $C \in \mathbb{Q}[t]$ and thus

$$A(t)C(t)^n + B_i(t) \equiv 0 \left(\mathrm{mod}\ P_i(t)\right).$$

Hence

$$A(t)x^n + B_i(t) \equiv \left(x - C(t)\right)H(x,t) \left(\mathrm{mod}\ P_i(t)\right).$$

Clearly, $H\left(C(t), t\right) \not\equiv 0 \left(\mathrm{mod}\ P_i(t)\right)$; thus by Lemma 1 applied with $D = \mathbb{Q}[t]$ there exists a $C_{\mu_i - 1} \in \mathbb{Q}[t]$ such that

$$A(t)C_{\mu_i-1}(t)^n + B_i(t) \equiv 0 \left(\mathrm{mod}\ P_i^{\mu_i}(t)\right).$$

Now we can satisfy (10) by taking

$$X(t) = C_{\mu_i-1}(t) P_i^{\beta_i/n}(t). \qquad \square$$

Lemma 8. *Let under the assumptions of Lemma* 7

$$\Pi(t) = \prod_{i=1}^{k} P_i(t)^{\max\{-[-\mu_i/n], \mu_i + (n-1)[-\beta_i/n]\}},$$

$$X(t,v) = X_0(t) + v\Pi(t), \qquad Y(t,v) = \frac{A(t)X(t,v)^n + B(t)}{M(t)}.$$

If $d, e \in \mathbb{Z}$, $dX_0 \in \mathbb{Z}[t]$, $eY_0 \in \mathbb{Z}[t]$ *then* $dX(t,v) \in \mathbb{Z}[t,v]$, $[d^n m, e]Y(t,v) \in \mathbb{Z}[t,v]$.

Proof. The statement concerning $X(t,v)$ is obvious and that concerning $Y(t,v)$ follows

from the identity

$$Y(t, v) = Y_0(t) + \sum_{\nu=1}^{n} \binom{n}{\nu} A(t) X_0(t)^{n-\nu} \Pi(t)^{\nu} M(t)^{-1} v^{\nu}.$$

Indeed,

$$\operatorname{ord}_{P_i} X_0^{n-1} \Pi \geqslant -(n-1)[-\beta_i/n] + \max\{-[-\mu_i/n], \mu_i + (n-1)[-\beta_i/n]\} \geqslant \mu_i = \operatorname{ord}_{P_i} M,$$

$$\operatorname{ord}_{P_i} \Pi^n \geqslant n \max\{-[-\mu_i/n], \mu_i + (n-1)[-\beta_i/n]\} \geqslant \mu_i = \operatorname{ord}_{P_i} M;$$

hence for each $\nu = 1, 2, \ldots, n$

$$X_0(t)^{n-\nu} \Pi(t)^{\nu} P_i(t)^{-\mu_i} \in \mathbb{Q}[t].$$

Since $d X_0 \in \mathbb{Z}[t]$ and P_i is primitive we have $d^{n-\nu} X_0(t)^{n-\nu} \Pi(t)^{\nu} P_i(t)^{-\mu_i} \in \mathbb{Z}[t]$,

$$md^{n-\nu} X_0(t)^{n-\nu} \Pi(t)^{\nu} M(t)^{-1} \in \mathbb{Z}[t]. \tag{11}$$

□

Lemma 9. *Let $P \in \mathbb{Z}[t]$ be a primitive polynomial with discriminant $D \neq 0$, $t^* \in \mathbb{Z}$, p a prime. If $\operatorname{ord}_p D = d$, $\infty > \operatorname{ord}_p P(t^*) = e > 2d + 1$ then there exists a $t_0 \equiv t^* \pmod{p^{e-d-1}}$ such that*

$$\operatorname{ord}_p P(t_0) = \operatorname{ord}_p P(t^*) - 1.$$

Proof. If P is of degree 1 then $P(t^*) \equiv 0 \pmod p$ implies $P'(t^*) \not\equiv 0 \pmod p$, P being primitive. Therefore, it is enough to take $t_0 = t^* + p^{e-1}$.

If P is of degree > 1 then we have for suitable polynomials $U, V \in \mathbb{Z}[t]$ that $PU + P'V = D$ (see Rédei [7], Satz 275). Hence $e > 2d+1$ implies $\delta = \operatorname{ord}_p P'(t^*) \leqslant d$. Take $t_0 = t^* + p^{e-\delta-1}$. From the Taylor formula we get

$$P(t_0) \equiv P(t^*) + P'(t^*) p^{e-\delta-1} \pmod{p^{2(e-\delta-1)}}.$$

By the assumption $2(e - \delta - 1) \geqslant 2(e - d - 1) > e - 1 = \operatorname{ord}_p P'(t^*) p^{e-\delta-1}$. Hence

$$\operatorname{ord}_p P(t_0) = e - 1.$$

□

Remark. It may be that the lemma holds for $e > d + 1$, but the writer could not prove it.

Lemma 10. *Under the assumptions of Lemmata 7 and 8 for every prime p there exist an integer c and an integer valued function $w(\tau)$ defined on the set $\{0, 1, \ldots, p^{2c} - 1\}$ such that if $t^* \in \mathbb{Z}$, $v^* \in \mathbb{Q}$, $t^* \equiv \tau \pmod{p^{2c}}$, $p^c v^* \equiv w(\tau) \pmod{p^{2c}}$ then $X(t^*, v^*)$ and $Y(t^*, v^*)$ are p-adic integers.*

Proof. Let nonnegative integers ξ, η be chosen so that $p^{\xi} X_0$, $p^{\eta} Y_0$ have integral p-adic coefficients. Let R_{ij} for $i, j = 1, \ldots, k$ be the resultant of P_i and P_j if $i \neq j$ and the discriminant of P_i if $i = j$. Moreover, let R_{i0} be the resultant of P_i and A, $R_{i,k+1}$ the resultant of P_i and $B_i = B P_i(t)^{-\beta_i}$ $(1 \leqslant i \leqslant k)$.

Put $\varrho_{ij} = \operatorname{ord}_p R_{ij}$. Clearly, $\varrho_{ij} = \varrho_{ji} \geqslant \min\{\operatorname{ord}_p P_i(t^*), \operatorname{ord}_p P_j(t^*)\}$ for every $t^* \in \mathbb{Z}$ and $i \neq j$ $(1 \leqslant i, j \leqslant k)$. Put further

$$c_i = \varrho_{i0} + \sum_{j=1}^{k} \mu_j \varrho_{ij} + 2\varrho_{ii} + 2\varrho_{i,k+1} + n\xi + 2\eta + 2\operatorname{ord}_p n + \operatorname{ord}_p m,$$

$$c = \sum_{i=1}^{k} c_i \mu_i + \xi + \operatorname{ord}_p m.$$

For every nonnegative integer $\tau < p^{2c}$ the arithmetic progression $\tau + p^{c-\xi+1}u$ contains an integer t_τ such that for suitable integers x_τ, y_τ we have

$$A(t_\tau)x_\tau^n + B(t_\tau) = M(t_\tau)y_\tau, \quad M(t_\tau) \neq 0 \tag{12}$$

(integers t_τ, x_τ, y_τ are not determined uniquely, but any choice will do).

If for all $i \leqslant k$ we have $\operatorname{ord}_p P_i(\tau) \leqslant c_i$ then

$$o = \operatorname{ord}_p \Pi(\tau) \leqslant \sum_{i=1}^{k} \mu_i \operatorname{ord}_p P_i(\tau) \leqslant c - \xi.$$

We define

$$w(\tau) = p^{c-o-\xi} w,$$

where w is a root of the congruence

$$w \frac{\Pi(\tau)}{p^o} + p^\xi X_0(\tau) \equiv x_\tau p^\xi \pmod{p^c}.$$

If $t^* \equiv \tau \pmod{p^{2c}}$ and $p^c v^* \equiv w(\tau) \pmod{p^{2c}}$ then we have

$$\operatorname{ord}_p M(\tau) = \operatorname{ord}_p m + \sum_{i=1}^{k} \mu_i \operatorname{ord}_p P_i(\tau) \leqslant c - \xi,$$

hence

$$\operatorname{ord}_p M(t^*) = \operatorname{ord}_p M(\tau) = \operatorname{ord}_p M(t_\tau),$$

$$X(t^*, v^*) \equiv X_0(\tau) + \frac{w(\tau)}{p^c} \Pi(\tau) \pmod{p^c}.$$

By the definition of $w(\tau)$

$$X(t^*, v^*) \equiv X_0(\tau) + \frac{w}{p^{o+\xi}} \Pi(\tau) \equiv x_\tau \pmod{p^{c-\xi}},$$

$$A(t^*)X(t^*, v^*)^n + B(t^*) \equiv A(t_\tau)x_\tau^n + B(t_\tau) \equiv M(t_\tau)y_\tau \pmod{p^{c-\xi}},$$

hence

$$\operatorname{ord}_p\big(A(t^*)X(t^*, v^*)^n + B(t^*)\big) \geqslant \min\big(c - \xi, \operatorname{ord}_p M(t_\tau)\big) = \operatorname{ord}_p M(t^*).$$

This shows that $X(t^*, v^*)$ and $Y(t^*, v^*)$ are both p-adic integers.

If, for a certain $i \leqslant k$, $\operatorname{ord}_p P_i(\tau) > c_i$ then, since $c_i \geqslant \varrho_{ij}$, we have for all $j \neq i$ $(1 \leqslant j \leqslant k)$ $\operatorname{ord}_p P_j(\tau) \leqslant \varrho_{ij} \leqslant c_j$ thus i is uniquely determined. We have the following

possibilities: $\beta_i \geqslant \mu_i \equiv 0 \pmod n$, $\beta_i \geqslant \mu_i \not\equiv 0 \pmod n$ and $\beta_i < \mu_i$ which we consider successively.

1. $\beta_i \geqslant \mu_i \equiv 0 \pmod n$. Here we set $\zeta_i = \max\{\xi, \varrho_{i0}\}$,

$$\Pi_i(t) = \Pi(t) P_i^{-\mu_i/n}(t), \quad X_{0i}(t) = X_0(t) P_i^{-\mu_i/n}(t),$$
$$M_i(t) = M(t) P_i(t)^{-\mu_i}.$$

We have

$$o_i = \operatorname{ord}_p \Pi_i(\tau) \leqslant \sum_{\substack{j=1 \\ j\neq i}}^{k} \mu_j \operatorname{ord}_p P_j(\tau) \leqslant \sum_{\substack{j=1 \\ j\neq i}}^{k} \mu_j \varrho_{ij} \leqslant c_i - \zeta_i \leqslant c - \zeta_i.$$

Moreover from (12) and $\beta_i \geqslant \mu_i$ we infer that

$$P_i^{\mu_i}(t_\tau) \mid A(t_\tau) x_\tau^n$$

and since

$$\operatorname{ord}_p P_i(t_\tau) \geqslant \min\bigl(\operatorname{ord}_p P_i(\tau), c - \xi + 1\bigr) > c_i \geqslant \varrho_{i0},$$

we get

$$\operatorname{ord}_p A(t_\tau) \leqslant \varrho_{i0} \leqslant n\zeta_i,$$
$$n(\operatorname{ord}_p x_\tau + \zeta_i) \geqslant \mu_i \operatorname{ord}_p P_i(t_\tau).$$

We define

$$w(\tau) = p^{c - o_i - \zeta_i} w,$$

where w is a root of the congruence

$$\frac{\Pi_i(\tau)}{p^{o_i}} w + p^{\zeta_i} X_{0i}(\tau) \equiv \frac{x_\tau p^{\zeta_i}}{P_i^{\mu_i/n}(t_\tau)} \pmod{p^c}.$$

If $t^* \equiv \tau \pmod{p^{2c}}$, $p^c v^* \equiv w(\tau) \pmod{p^{2c}}$ we have

$$\operatorname{ord}_p M_i(\tau) = \operatorname{ord}_p m + \sum_{\substack{j=1 \\ j\neq i}}^{k} \mu_j \operatorname{ord}_p P_j(\tau) \leqslant c_i - \zeta_i \leqslant \mu_i(c_i - \zeta_i) \leqslant c - \mu_i\zeta_i - \xi,$$

hence $\operatorname{ord}_p M_i(t^*) = \operatorname{ord}_p M_i(\tau) = \operatorname{ord}_p M_i(t_\tau)$.

On the other hand, taking

$$X_i(t^*, v^*) = X_{0i}(t^*) + v^* \Pi_i(t^*),$$

we get

$$X_i(t^*, v^*) \equiv X_{0i}(\tau) + \frac{w(t)}{p^c} \Pi_i(\tau) \pmod{p^c}$$

and by the definition of $w(\tau)$

$$p^{\zeta_i} X_i(t^*, v^*) \equiv p^{\zeta_i} X_{0i}(\tau) + \frac{w}{p^{o_i}} \Pi_i(\tau) \equiv \frac{x_\tau p^{\zeta_i}}{P_i^{\mu_i/n}(t_\tau)} \pmod{p^c}.$$

Since

$$\operatorname{ord}_p P_i^{\mu_i/n}(t^*) \geqslant \min\bigl(\operatorname{ord}_p P_i(\tau), 2c\bigr) > c_i \geqslant \zeta_i$$

we infer that $X(t^*, v^*) = X_i(t^*, v^*) P_i^{\mu_i/n}(t^*)$ is a p-adic integer. Moreover

$$p^{n\zeta_i}\bigl(A(t^*)X_i(t^*, v^*)^n + P_i(t^*)^{\beta_i-\mu_i} B_i(t^*)\bigr) \equiv \frac{A(t_\tau)p^{n\zeta_i}x_\tau^n}{P_i^{\mu_i}(t_\tau)} + p^{n\zeta_i} P_i(t^*)^{\beta_i-\mu_i} B_i(t_\tau) \pmod{p^{c-\xi}}.$$

c By (12) the right hand side equals $p^{n\zeta_i} M_i(t_\tau) y_\tau$, hence

$$\operatorname{ord}_p\bigl(A(t^*)X_i(t^*, v^*)^n + P_i(t^*)^{\beta_i-\mu_i} B_i(t^*)\bigr) \geqslant \min\bigl(c - \xi - n\zeta_i, \operatorname{ord}_p M_i(t_\tau)\bigr) = \operatorname{ord}_p M_i(t^*)$$

and

$$\operatorname{ord}_p\bigl(A(t^*)X(t^*, v^*)^n + B(t^*)\bigr) \geqslant \mu_i \operatorname{ord}_p P_i(t^*) + \operatorname{ord}_p M_i(t^*) = \operatorname{ord}_p M(t^*).$$

Thus $Y(t^*, v^*)$ is a p-adic integer.

2. $\beta_i \geqslant \mu_i \not\equiv 0 \pmod n$. Here we set $w(\tau) = 0$.

If $\beta_i > \mu_i$ we have

$$X_0(t) \equiv 0 \bigl(\bmod P_i(t)^{-[-\beta_i/n]}\bigr), \quad A(t)X_0(t)^n + B(t) \equiv 0 \bigl(\bmod P_i(t)^{\mu_i+1}\bigr),$$

hence $Y_0(t) \equiv 0 \bigl(\bmod P_i(t)\bigr)$. Moreover, since $P_i(t)$ is primitive, we have

$$p^\xi X_0(t) P_i(t)^{-1} \in \mathbb{Z}_p[t], \quad p^\eta Y_0(t) P_i(t)^{-1} \in \mathbb{Z}_p[t], \tag{13}$$

where $\mathbb{Z}_p$ is the ring of p-adic integers.

If $t^* \equiv \tau \pmod{p^{2c}}$, $p^c v^* \equiv w(\tau) \pmod{p^{2c}}$, we have $v^* \equiv 0 \pmod{p^c}$,

$$X(t^*, v^*) \equiv X_0(t^*) \pmod{p^c},$$

$$Y(t^*, v^*) = Y_0(t^*) + \sum_{\nu=1}^{n} \binom{n}{\nu} \frac{A(t^*)X_0(t^*)^{n-\nu}\Pi(t^*)^\nu}{M(t^*)} v^{*\nu}.$$

c Since $\operatorname{ord}_p P_i(t^*) > c_i \geqslant \max\{\xi, \eta\}$ we infer from (13) that

$$X_0(t^*), Y_0(t^*) \in \mathbb{Z}_p.$$

c On the other hand, by (11)

$$mp^{\xi(n-\nu)} \frac{X_0(t)^{n-\nu}\Pi(t)^\nu}{M(t)} \in \mathbb{Z}_p[t] \quad (\nu = 1, 2, \ldots, n).$$

Since $\operatorname{ord}_p v^\nu \geqslant c \geqslant \xi(n-1) + \operatorname{ord}_p m$ we conclude that $X(t^*, v^*)$, $Y(t^*, v^*)$ are p-adic integers.

If $\beta_i = \mu_i$ we have as before $X_0(t) \equiv 0 \bigl(\bmod P_i(t)\bigr)$. If $t^* \equiv \tau \pmod{p^{2c}}$, $p^c v^* \equiv w(\tau) \equiv 0 \pmod{p^{2c}}$, then $X(t^*, v^*) \equiv X_0(t^*) \pmod{p^c}$ is again a p-adic integer and $Y(t^*, v^*) \in \mathbb{Z}_p$ if and only if $Y_0(t^*) \in \mathbb{Z}_p$.

The latter condition is satisfied for all $t^* \equiv \tau \pmod{p^{2c}}$ if it is satisfied for one such t^*. Since we cannot have $P_i(t^*) = 0$ for all $t^* \equiv \tau \pmod{p^{2c}}$ we may assume that $P_i(t^*) \neq 0$. If $\eta = 0$, $Y_0(t^*) \in \mathbb{Z}_p$. If $\eta > 0$ we have $\operatorname{ord}_p P_i(t^*) > c_i \geqslant 2\varrho_{ii} + 1$, hence by Lemma 9

there exists a $t_0 \equiv t^* \pmod{p^{c_i - \varrho_{ii}}}$ such that $\operatorname{ord}_p P_i(t_0) = \operatorname{ord}_p P_i(t^*) - 1$. On the other hand

$$\operatorname{ord}_p A(t^*) \leqslant \varrho_{i0} < c_i - \varrho_{ii},$$

$$\operatorname{ord}_p B_i(t^*) \leqslant \varrho_{i,k+1} < c_i - \varrho_{ii},$$

$$\operatorname{ord}_p M_i(t^*) \leqslant \operatorname{ord}_p m + \sum_{\substack{j=1 \\ j \neq i}}^{k} \mu_j \varrho_{ij} < c_i - \varrho_{ii} - n\xi,$$

hence

$$\operatorname{ord}_p A(t_0) = \operatorname{ord}_p A(t^*) < \infty, \quad \operatorname{ord}_p B_i(t_0) = \operatorname{ord}_p B_i(t^*) < \infty,$$
$$\operatorname{ord}_p M_i(t_0) = \operatorname{ord}_p M_i(t^*) < \infty.$$

Since $\mu_i \not\equiv 0 \pmod{n}$ we cannot have simultaneously

$$\mu_i \operatorname{ord}_p P_i(t^*) + \operatorname{ord}_p B_i(t^*) \equiv \operatorname{ord}_p A(t^*) \pmod{n}$$

and

$$\mu_i \operatorname{ord}_p P_i(t_0) + \operatorname{ord}_p B_i(t_0) \equiv \operatorname{ord}_p A(t_0) \pmod{n}$$

thus taking $t_1 = t^*$ or t_0 we can achieve that

$$\operatorname{ord}_p B(t_1) = \mu_i \operatorname{ord}_p P_i(t_1) + \operatorname{ord}_p B_i(t_1) \not\equiv \operatorname{ord}_p A(t_1) \pmod{n},$$
$$\infty > \operatorname{ord}_p P_i(t_1) \geqslant c_i - \varrho_{ii},$$
$$a = \max\left\{\operatorname{ord}_p A(t_1), \operatorname{ord}_p B(t_1), \operatorname{ord}_p M(t_1)\right\} < \infty.$$

The arithmetic progression $t_1 + p^{a+1}u$ contains an integer t_2 such that for suitable integers x_2, y_2 we have

$$A(t_2)x_2^n + B(t_2) = M(t_2)y_2.$$

Since

$$\operatorname{ord}_p A(t_2) = \operatorname{ord}_p A(t_1), \quad \operatorname{ord}_p P_i(t_2) = \operatorname{ord}_p P_i(t_1),$$
$$\operatorname{ord}_p B(t_2) = \operatorname{ord}_p B(t_1), \quad \operatorname{ord}_p M(t_2) = \operatorname{ord}_p M(t_1),$$

we have

$$\operatorname{ord}_p A(t_2)x_2^n \equiv \operatorname{ord}_p A(t_2) \not\equiv \operatorname{ord}_p B(t_2) \pmod{n}.$$

It follows that

$$\operatorname{ord}_p B(t_2) \geqslant \operatorname{ord}_p M(t_2)y_2 \geqslant \operatorname{ord}_p M(t_2) \quad \text{and} \quad \operatorname{ord}_p B(t_1) \geqslant \operatorname{ord}_p M(t_1).$$

On the other hand we have $\operatorname{ord}_p P_i(t_1) \geqslant c_i - \varrho_{ii} > \varrho_{ij}$ for all $j \leqslant k+1$, hence

$$\operatorname{ord}_p P_j(t_1) \leqslant \varrho_{ij} \ (j \neq i), \quad \operatorname{ord}_p M_i(t_1) \leqslant \operatorname{ord}_p m + \sum_{\substack{j=1 \\ j\neq i}}^{k} \varrho_{ij}\mu_j \leqslant c_i - n\xi - \varrho_{ii};$$

$$\begin{aligned}\operatorname{ord}_p A(t_1)X_0(t_1)^n &\geqslant -n[-\beta_i/n]\operatorname{ord}_p P_i(t_1) - n\xi \\ &\geqslant (\mu_i+1)\operatorname{ord}_p P_i(t_1) - n\xi \geqslant \mu_i \operatorname{ord}_p P_i(t_1) + c_i - n\xi - \varrho_{ii} \\ &\geqslant \mu_i \operatorname{ord}_p P_i(t_1) + \operatorname{ord}_p M_i(t_1) = \operatorname{ord}_p M(t_1).\end{aligned}$$

Since $A(t_1)X_0(t_1)^n + B(t_1) = M(t_1)Y_0(t_1)$ we get $\operatorname{ord}_p Y_0(t_1) \geqslant 0$. However $p^\eta Y_0(t_1) \equiv p^\eta Y_0(t^*) \pmod{p^{c_i-\varrho_{ii}}}$. Since $c_i - \varrho_{ii} \geqslant \eta$, $Y_0(t^*)$ is a p-adic integer and so is $Y(t^*, v^*)$.

3. $\beta_i < \mu_i$. Here we have $\beta_i \equiv 0 \pmod n$,

$$P_i(t)^{\beta_i/n} \parallel X_0(t), \quad P_i(t)^{\mu_i - \frac{n-1}{n}\beta_i} \parallel \Pi(t).$$

Let

$$X_{0i}(t) = X_0(t)P_i(t)^{-\beta_i/n}, \quad \Pi_i(t) = \Pi(t)P_i(t)^{\frac{n-1}{n}\beta_i - \mu_i},$$
$$M_i(t) = M(t)P_i(t)^{-\mu_i}.$$

We have

$$A(t)X_{0i}(t)^n + B_i(t) = P_i^{\mu_i-\beta_i}(t)M_i(t)Y_0(t)$$

and

$$\operatorname{ord}_p P_i(\tau) > c_i \geqslant \varrho_{i,k+1} + \eta \geqslant \operatorname{ord}_p B_i(\tau) + \eta,$$

hence

$$\operatorname{ord}_p P_i^{\mu_i-\beta_i}(\tau)M_i(\tau)Y_0(\tau) > \operatorname{ord}_p B_i(\tau)$$

and

$$\operatorname{ord}_p A(\tau)X_{0i}(\tau)^n = \operatorname{ord}_p B_i(\tau).$$

We get

$$\operatorname{ord}_p X_{0i}(\tau) \leqslant \frac{1}{n}\operatorname{ord}_p B_i(\tau) \leqslant \frac{1}{n}\varrho_{i,k+1}$$

and

$$(14)\quad o_i = \operatorname{ord}_p \frac{nX_{0i}(\tau)^{n-1}\Pi_i(\tau)}{M_i(\tau)} \leqslant \operatorname{ord}_p n + \varrho_{i,k+1} - \operatorname{ord}_p m \leqslant c_i - \eta \leqslant c - \eta.$$

We define

$$w(\tau) = p^{c-o_i-\eta}w,$$

where w is a root of the congruence

$$\frac{nX_{0i}(\tau)^{n-1}\Pi_i(\tau)}{M_i(\tau)p^{o_i}}\,w + p^\eta Y_0(\tau) \equiv 0 \pmod{p^\eta}.$$

If $t^* \equiv \tau \pmod{p^{2c}}$ and $p^c v^* \equiv w(\tau) \pmod{p^{2c}}$ we have

$$\operatorname{ord}_p P_i(t^*) > c_i \geqslant \sum_{j=1}^{k} \beta_j \varrho_{ij} + \varrho_{i,k+1} + \eta.$$

If $P_i(t^*) \neq 0$ then

$$\begin{aligned} \operatorname{ord}_p B(t^*) &\leqslant \beta_i \operatorname{ord}_p P_i(t^*) + \varrho_{i,k+1} < \mu_i \operatorname{ord}_p P_i(t^*) - \eta \\ &\leqslant \operatorname{ord}_p M(t^*) - \eta \leqslant \operatorname{ord}_p M(t^*) Y_0(t^*). \end{aligned} \tag{15}$$

Therefore,

$$\operatorname{ord}_p B(t^*) = \operatorname{ord}_p A(t^*) X_0(t^*)^n. \tag{16}$$

Moreover, $A(t^*)B(t^*)M(t^*) \neq 0$.

Let $b = \max\{\operatorname{ord}_p A(t^*), \operatorname{ord}_p B(t^*), \operatorname{ord}_p M(t^*)\}$ and let t_0 be an integer in the arithmetic progression $t^* + p^{b+1}u$ such that for suitable $x_0, y_0 \in \mathbb{Z}$

$$A(t_0)x_0^n + B(t_0) = M(t_0)y_0.$$

We have $\operatorname{ord}_p A(t_0) = \operatorname{ord}_p A(t^*)$, $\operatorname{ord}_p B(t_0) = \operatorname{ord}_p B(t^*)$, $\operatorname{ord}_p M(t_0) = \operatorname{ord}_p M(t^*)$ and by (15) $\operatorname{ord}_p B(t_0) < \operatorname{ord}_p M(t_0) \leqslant \operatorname{ord}_p M(t_0) y_0$. Hence

$$\operatorname{ord}_p B(t_0) = \operatorname{ord}_p A(t_0) x_0^n$$

and by (16)

$$\operatorname{ord}_p X_0(t^*) = \operatorname{ord}_p x_0 \geqslant 0. \tag{17}$$

If $P_i(t^*) = 0$ there exists a $t' \equiv t^* \pmod{p^{2c}}$ such that $P_i(t') \neq 0$. Since

$$X_0(t^*) \equiv X_0(t') \pmod{p^{2c-\xi}}$$

we have (17) in every case. On the other hand

$$\begin{aligned} \operatorname{ord}_p v^* \Pi(t^*) &\geqslant \min\Big\{c, \operatorname{ord}_p \frac{w(\tau)}{p^c} \Pi(\tau)\Big\} \\ &\geqslant \min\big\{c, \operatorname{ord}_p \Pi(\tau) - o_i - \eta\big\} \geqslant \min\{c, c_i - o_i - \eta\} \geqslant 0, \end{aligned}$$

hence

$$\operatorname{ord}_p X(t^*, v^*) \geqslant 0.$$

It remains to prove that $Y(t^*, v^*)$ is a p-adic integer. We have

$$\begin{aligned} Y(t^*, v^*) = Y_0(t^*) &+ \frac{n X_{0i}(t^*)^{n-1} \Pi_i(t^*)}{M_i(t^*)} v^* \\ &+ \sum_{\nu=2}^{n} \binom{n}{\nu} \frac{X_{0i}(t^*)^{n-\nu} \Pi_i(t^*)^{\nu}}{M_i(t^*)} P_i(t^*)^{(\nu-1)(\mu_i-\beta_i)} v^{*\nu}. \end{aligned}$$

Now

$$
\begin{aligned}
p^{\eta} Y_0(t^*) &\equiv p^{\eta} Y_0(\tau) \pmod{p^{2c}},\\
p^{(n-1)\xi} X_{0i}(t^*)^{n-1} \Pi_i(t^*) &\equiv p^{(n-1)\xi} X_{0i}(\tau)^{n-1} \Pi_i(\tau) \pmod{p^{2c}},\\
M_i(t^*) &\equiv M_i(\tau) \pmod{p^{2c}},\\
\operatorname{ord}_p M_i(\tau) &\leqslant \sum_{\substack{j=1\\ j\neq i}}^{k} \mu_j \varrho_{ij} + \operatorname{ord}_p m < c_i - n\xi + \operatorname{ord}_p m < 2c.
\end{aligned}
\tag{18}
$$

Hence

$$
\begin{aligned}
p^{\eta} \frac{n X_{0i}(t^*)^{n-1} \Pi_i(t^*)}{M_i(t^*)}\, v^* &\\
\equiv p^{\eta} \frac{n X_{0i}(\tau)^{n-1} \Pi_i(\tau)}{M_i(\tau)}\, \frac{w(\tau)}{p^c} &\left(\bmod\, p^{c-(n-1)\xi+\eta-\operatorname{ord}_p M_i(\tau)}\right)
\end{aligned}
$$

and since $c \geqslant c_i + \operatorname{ord}_p m$ we have by the definition of $w(\tau)$

$$
\begin{aligned}
p^{\eta} Y_0(t^*) + p^{\eta} \frac{n X_{0i}(t^*)^{n-1} \Pi_i(t^*)}{M_i(t^*)}\, v^* &\\
\equiv p^{\eta} Y_0(\tau) + \frac{n X_{0i}(\tau)^{n-1} \Pi_i(\tau)}{M_i(\tau)\, p^{o_i}} &\equiv 0 \pmod{p^{\eta}}.
\end{aligned}
$$

Thus

$$
Y_0(t^*) + \frac{n X_{0i}(t^*)^{n-1} \Pi_i(t^*)}{M_i(t^*)}\, v^*
$$

is a p-adic number.

Now take $\nu \geqslant 2$ and consider the term

$$
E_\nu(t^*, v^*) = \binom{n}{\nu} \frac{X_{0i}(t^*)^{n-\nu} \Pi_i(t^*)^{\nu}}{M_i(t^*)}\, P_i(t^*)^{(\nu-1)(\mu_i-\beta_i)} v^{*\nu}.
$$

We have by (18)

$$
\operatorname{ord}_p \frac{X_{0i}(t^*)^{n-\nu} \Pi_i(t^*)^{\nu}}{M_i(t^*)} \geqslant -(n-\nu)\xi - \sum_{\substack{j=1\\ j\neq i}}^{k} \mu_j \varrho_{ij} - \operatorname{ord}_p m,
$$

while by the congruence $p^c v^* \equiv w(\tau) \pmod{p^{2c}}$, by the definition of $w(\tau)$ and by (14)

$$
\operatorname{ord}_p v^* \geqslant -o_i - \eta \geqslant -\operatorname{ord}_p n - \varrho_{i,k+1} + \operatorname{ord}_p m - \eta,
$$

finally

$$
\operatorname{ord}_p P_i(t^*)^{\mu_i-\beta_i} > c_i \geqslant \sum_{\substack{j=1\\ j\neq i}}^{k} \mu_j \varrho_{ij} + 2\varrho_{i,k+1} + n\xi + 2\eta + 2\operatorname{ord}_p n.
$$

Hence

$$\begin{aligned}\operatorname{ord}_p E_\nu(t^*, v^*) > &-(n-\nu)\xi - \sum_{\substack{j=1\\ j\neq i}}^{k} \mu_j \varrho_{ij} - \operatorname{ord}_p m - \nu \operatorname{ord}_p n \\ &- \nu\varrho_{i,k+1} + \nu \operatorname{ord}_p m - \nu\eta + (\nu-1)\sum_{\substack{j=1\\ j\neq i}}^{k} \mu_j \varrho_{ij} \\ &+ 2(\nu-1)\varrho_{i,k+1} + (\nu-1)n\xi + 2(\nu-1)\eta + 2(\nu-1)\operatorname{ord}_p n \\ = &\, n(\nu-2)\xi + \nu\xi + (\nu-2)\sum_{\substack{j=1\\ j\neq i}}^{k} \mu_j \varrho_{ij} + (\nu-1)\operatorname{ord}_p m \\ &+ (\nu-2)\operatorname{ord}_p n + (\nu-2)\varrho_{i,k+1} + (\nu-2)\eta + (\nu-2)\operatorname{ord}_p n \geqslant 0.\end{aligned}$$

Thus $E_\nu(t^*, v^*)$ is a p-adic integer and so is $Y(t^*, v^*)$. □

Proof of Theorem 4. Suppose first that $BM \neq 0$, $(A, M) = 1$. Let X_0, Y_0 have the meaning of Lemma 7 and let d be chosen so that $dX_0 \in \mathbb{Z}[t]$, $dY_0 \in \mathbb{Z}[t]$. Let further $X(t, v)$, $Y(t, v)$ have the meaning of Lemma 8.

In virtue of Lemma 10 for every prime $p \mid dm$ there exists an integer c_p and an integer valued function $w_p(\tau)$ defined on the set $\{0, 1, \ldots, p^{c_p}-1\}$ such that for all $t^* \in \mathbb{Z}$, $v^* \in \mathbb{Q}$ the congruences $t^* \equiv \tau \pmod{p^{2c_p}}$, $p^c v^* \equiv w_p(\tau) \pmod{p^{2c_p}}$ imply that $X(t^*, v^*)$ and $Y(t^*, v^*)$ are p-adic integers. By a result of Skolem [8] there exists an integer valued polynomial $W_p(t)$ such that $t^* \equiv \tau \pmod{p^{2c_p}}$ implies $W_p(t^*) \equiv w_p(\tau) \pmod{p^{2c_p}}$. Now take

$$V(t) = \sum_{p\mid dm} \frac{W_p(t)}{p^{c_p}} \prod_{\substack{q\mid dm\\ q\neq p}} q^{\varphi(p^{2c_p})c_q}$$

where p, q run over primes and set

$$X(t) = X\big(t, V(t)\big), \quad Y(t) = Y\big(t, V(t)\big).$$

We assert that $X(t), Y(t)$ belong to the set I of integer valued polynomials. Indeed, by Lemma 8,

$$dX(t, v) \in \mathbb{Z}[t, v], \quad d^n m Y(t, v) \in \mathbb{Z}[t, v].$$

Moreover, since

$$V(t) \prod_{p\mid dm} p^{c_p} \in I$$

and $X(t, v)$, $Y(t, v)$ are in v of degrees 1 and n respectively, we have

$$X(t)d \prod_{p\mid dm} p^{c_p} \in I, \quad Y(t)d^n m \prod_{p\mid dm} p^{nc_p} \in I.$$

Thus for $t^* \in \mathbb{Z}$ the values $X(t^*)$ and $Y(t^*)$ are p-adic integers for each $p \nmid dm$. On the other hand if $p \mid dm$ and $t^* \equiv \tau \pmod{p^{2c_p}}$, $0 \leqslant \tau < p^{2c_p}$ we have

$$p^{c_p} V(t^*) \equiv p^{c_p} \sum_{\substack{q_1 \mid dm \\ q_1 \neq p}} \frac{W_{q_1}(t^*)}{q_1^{c_{q_1}}} \prod_{\substack{q_2 \mid dm \\ q_2 \neq q_1}} q_2^{\varphi(q_1^{2c_{q_1}})c_{q_2}} + W_p(t^*) \prod_{\substack{q \mid dm \\ q \neq p}} q^{\varphi(p^{2c_p})c_q}$$

$$\equiv W_p(t^*) \equiv W_p(\tau) \pmod{p^{2c_p}},$$

hence by the property of the polynomials $X(t, v)$, $Y(t, v)$ stated above

$$X(t^*) = X\big(t^*, V(t^*)\big), \quad Y(t^*) = Y\big(t^*, V(t^*)\big)$$

are p-adic integers.

Suppose now that $BM \neq 0$ and $(A, M) \neq 1$. Then there exists a primitive polynomial $D \in \mathbb{Z}[t]$ such that $A = DA_1$, $M = DM_1$, $A_1, M_1 \in \mathbb{Z}[t]$ and $(A_1, M_1) = 1$. Every arithmetic progression contains an integer t^* such that $A(t^*)x^n + B(t^*) = M(t^*)y$ is solvable in integers x, y hence $D(t^*) \mid B(t^*)$. It follows that $D \mid B$ and since D is primitive $B = DB_1$, where $B_1 \in \mathbb{Z}[t]$. Every arithmetic progression P contains a progression P_1 such that $D(t^*) \neq 0$ for $t \in P_1$. Therefore, for $t^* \in P_1$

$$A(t^*)x^n + B(t^*) = M(t^*)y \quad \text{implies} \quad A_1(t^*)x^n + B_1(t^*) = M_1(t^*)y$$

and from the already proved case of the theorem we infer the existence of integer valued polynomials X, Y such that $A_1(t)X(t)^n + B_1(t) = M_1(t)Y(t)$. Clearly, $A(t)X(t)^n + B(t) = M(t)Y(t)$. It remains to consider the case $BM = 0$. If $B = 0$ we can take $X = Y = 0$. If $B \neq 0$ and $M = 0$ Theorem 1 of [2] implies the existence of a polynomial $X \in \mathbb{Q}[t]$ such that $A(t)X(t)^n + B(t) = 0$. By the assumption every arithmetic progression contains an integer t^* such that either $B(t^*) = 0$ or $X(t^*)^n$ is an integer. Since $B \neq 0$, the former term of the alternative can be omitted. Let a positive integer d be chosen so that $dX \in \mathbb{Z}[t]$ and let τ be an arbitrary integer. The arithmetic progression $\tau + du$ contains an integer t^* such that $X(t^*)$ is an integer. We have $dX(\tau) \equiv dX(t^*) \pmod{d}$, hence $d \mid dX(\tau)$ and $X(\tau)$ is an integer. Thus X is an integer valued polynomial and the proof is complete. □

Now we shall show by an example that the condition $n \not\equiv 0 \pmod 8$ cannot be omitted from the assumptions of Theorem 4.

Example 3. Take $n = 8$, $A(t) = 1$, $B(t) = -16$, $M(t) = 2t + 1$. For every integer t^* we have $M(t^*) = \pm \prod_{i=1}^{k} p_i^{\alpha_i}$, where p_i are odd primes. For every $i \leqslant k$ the congruence

$$x^8 \equiv 16 \pmod{p_i^{\alpha_i}}$$

is solvable (cf. Trost [11]). Denoting a solution of this congruence by x_i and using the Chinese Remainder Theorem we find $x \equiv x_i \pmod{p_i^{\alpha_i}}$ $(1 \leqslant i \leqslant k)$, which satisfies $x^8 - 16 \equiv 0 \pmod{2t^* + 1}$. On the other hand, the existence of polynomials $X, Y \in \mathbb{Q}[t]$ satisfying $X(t)^8 - 16 = (2t + 1)Y(t)$ would imply $X\big(-\frac{1}{2}\big)^8 = 16$, $X\big(-\frac{1}{2}\big)^2 = 2$, a contradiction.

The next example shows that in Theorem 4 polynomials in one variable cannot be replaced by polynomials in two variables even if $A = 1$ and M is irreducible.

Example 4. Take $n = 2$, $A(t,u) = B(t,u) = 1$, $M(t,u) = u^2 + (4t^2+1)^2$. For every pair of integers t^*, u^* the congruence $x^2 + 1 \equiv 0 \pmod{M(t^*,u^*)}$ is solvable. Indeed, we have $M(t^*,u^*) = 2^\alpha \prod p_i^{\alpha_i}$, where $\alpha = 0$ or 1 and $p_i \equiv 1 \pmod 4$. On the other hand suppose that polynomials $X, Y \in \mathbb{Q}[t,u]$ satisfy

$$X(t,u)^2 + 1 = M(t,u)Y(t,u).$$

We get $u^2X(t,u)^2 \equiv (4t^2+1)^2 \pmod{M(t,u)}$ and since M is irreducible

$$uX(t,u) \equiv \pm(4t^2+1) \pmod{M(t,u)}.$$

The substitution $u = 0$ gives

$$4t^2 + 1 \equiv 0 \pmod{(4t^2+1)^2},$$

a contradiction.

References

[1] N. H. Abel, *Über die Integration der Differential Formel $\varrho\,dx/\sqrt{R}$ wenn R und ϱ ganze Functionen sind*. J. Reine Angew. Math. 1 (1826), 185–221; French transl. in *Oeuvres choisies*, Christiania 1881, T. I, 104–144.

[2] H. Davenport, D. J. Lewis, A. Schinzel, *Polynomials of certain special types*. Acta Arith. 9 (1964), 107–116; this collection: A6, 27–35.

[3] —, —, —, *Quadratic Diophantine equations with a parameter*. Acta Arith. 11 (1966), 353–358.

[3a] H. Flanders, *Generalization of a theorem of Ankeny and Rogers*. Ann. of Math. (2) 57 (1953), 392–400.

[4] M. Fujiwara, *Hasse principle in algebraic equations*. Acta Arith. 22 (1973), 267–276.

[5] H. Hasse, *Zwei Bemerkungen zu der Arbeit „Zur Arithmetik der Polynome" von U. Wegner in den Math. Ann. 105, S. 628–631*. Math. Ann. 106 (1932), 455–456.

[6] —, *Zahlentheorie*. Akademie-Verlag, Berlin 1969.

[7] L. Rédei, *Algebra* I. Akademische Verlagsgesellschaft, Geest & Portig, Leipzig 1959.

[8] T. Skolem, *Über die Lösbarkeit gewisser linearer Gleichungen in Bereiche der ganzwertigen Polynome*. Kong. Norske Vid. Selsk. Forh. 9 (1937), no. 34.

[9] —, *Einige Sätze über Polynome*. Avh. Norske Vid. Akad. Oslo I 1940, no. 4.

[10] —, *Unlösbarkeit von Gleichungen, deren entsprechende Kongruenz für jeden Modul lösbar ist*. Ibid. 1942, no. 4.

[11] E. Trost, *Zur Theorie von Potenzresten*. Nieuw Arch. Wisk. 18 (1934), 58–61.

[12] B. L. van der Waerden, *Noch eine Bemerkung zu der Arbeit „Zur Arithmetik der Polynome" von U. Wegner in Math. Ann. 105, S. 628–631*. Math. Ann. 109 (1934), 679–680.

Andrzej Schinzel
Selecta

Originally published in
Studia Mathematica LXXVII (1983), 103–109

Hasse's principle for systems of ternary quadratic forms and for one biquadratic form

To Professor Jan Mikusiński on the occasion of the 70th birthday

Abstract. Let K be an algebraic number field and $f_1, \dots, f_k$ ternary quadratic forms over K. If $f_1, \dots, f_k$ have a common non-trivial zero in every completion of K except at most one then—it is proved here—they have a common non-trivial zero in K. Besides an example is given of an absolutely irreducible n-ary biquadratic form ($n \geqslant 3$) that represents 0 in every completion of $\mathbb{Q}$ but not in $\mathbb{Q}$.

Let K be an algebraic number field and $f_1, \dots, f_k \in K[x_1, \dots, x_n]$ quadratic forms. *Hasse's principle* asserts that if the forms $f_1, \dots, f_k$ have a common non-trivial zero in every completion of K they have a common non-trivial zero in K. The principle holds for $k = 1$, it trivially holds for $n = 1, 2$, and it fails for $K = \mathbb{Q}$, $k = 2$, $n \geqslant 4$ (see [2]). Thus it remains to consider the case $n = 3$.

We shall prove

Theorem 1. *If quadratic forms $f_1, \dots, f_k \in K[x, y, z]$ have a common non-trivial zero in every completion of K except at most one then they have a common non-trivial zero in K.*

As to biquadratic forms over $\mathbb{Q}$ it is easy to give an example of a reducible ternary form for which Hasse's principle fails (see [1], p. 72). An example of an irreducible ternary biquadratic form with the same property can be constructed by using results of Hilbert [4], namely

$$\operatorname{norm}(x + y\sqrt{5} + z\sqrt{-31}).$$

This form, however, is reducible over the complex field. Mordell [6] has left open the question whether there exists an absolutely irreducible ternary biquadratic form not fulfilling Hasse's principle. The question is answered by

Theorem 2. *The absolutely irreducible biquadratic form $x^4 - 2y^4 - 16y^2z^2 - 49z^4$ represents 0 in every completion of $\mathbb{Q}$ but not in $\mathbb{Q}$; for all $n \geqslant 4$ the absolutely irreducible biquadratic form $x_1^4 - 17x_2^4 - 2(x_3^2 + \dots + x_n^2)^2$ represents 0 in every completion of $\mathbb{Q}$ but not in $\mathbb{Q}$.*

Lemma 1. *If a binary form over K of degree not exceeding 4 represents 0 in all but finitely many completions of K it represents 0 in K.*

Proof. See Fujiwara [3]. □

Lemma 2. *Let $R(x, y; u_1, \dots, u_k, v_1, \dots, v_k)$ be the resultant of $\sum_{i=1}^{k} u_i f_i$, $\sum_{i=1}^{k} v_i f_i$ with respect to z (u_i, v_i are indeterminates). If*

$$R(a, b; u_1, \dots, u_k, v_1, \dots, v_k) = 0, \quad a, b \in K, \ \langle a, b\rangle \neq \langle 0, 0\rangle \tag{1}$$

then either f_i have a common non-trivial zero in K or

$$(bx - ay)^2 \mid R(x, y; u_1, \dots, u_k, v_1, \dots, v_k)$$

and the forms $f_i(at, bt, z)$ differ from their highest common divisor by a constant factor.

Proof. If f_i are all of degree less than 2 with respect to z then they have a common non-trivial zero, namely $\langle 0, 0, 1\rangle$. If at least one of the forms f_i is of degree 2 with respect to z then both $\sum_{i=1}^{k} u_i f_i$ and $\sum_{i=1}^{k} v_i f_i$ are of degree 2 with respect to z with the leading coefficients independent of x, y. Therefore (1) implies that

$$\sum_{i=1}^{k} u_i f_i(a, b, z) \quad \text{and} \quad \sum_{i=1}^{k} v_i f_i(a, b, z)$$

have a common factor over the field $K(u_1, \dots, u_k, v_1, \dots, v_k)$, hence also over the ring $K[u_1, \dots, u_k, v_1, \dots, v_k]$. The factor must be independent of $u_1, \dots, u_k, v_1, \dots, v_k$. If it is of degree 1 in z it has a zero $c \in K$ and we have $f_i(a, b, c) = 0$ $(1 \leqslant i \leqslant k)$. If it is of degree 2 in z we consider the Sylvester matrix

$$S(x, y; u_1, \dots, u_k, v_1, \dots, v_k)$$

of the polynomials $\sum_{i=1}^{k} u_i f_i$, $\sum_{i=1}^{k} v_i f_i$. In virtue of a well-known theorem (see [7], Satz 114) the rank of the matrix $S(a, b; u_1, \dots, u_k, v_1, \dots, v_k)$ must be 2. Hence all the minors of degree 3 of this matrix vanish and all the minors of degree 3 of the matrix $S(x, y; u_1, \dots, u_k, v_1, \dots, v_k)$ are divisible by $bx - ay$. On the other hand, there are minors of degree 2 of the latter matrix not divisible by $bx - ay$, in fact independent of x, y. Hence by a very special case of theorem of Rédei [8]

$$R(x, y; u_1, \dots, u_k, v_1, \dots, v_k) = \det S(x, y; u_1, \dots, u_k, v_1, \dots, v_k)$$

is divisible by $(bx - ay)^2$.

The last assertion of the lemma follows from the remark that if polynomials $f_i(a, b, z)$ $(1 \leqslant i \leqslant k)$ have a common factor of degree 2 they differ from this common factor by a constant factor. □

Proof of Theorem 1. Let us consider the resultant $R(x, y; u_1, \dots, u_k, v_1, \dots, v_k)$ of $\sum u_i f_i$ and $\sum v_i f_i$ with respect to z. Viewed as a polynomial in x, y it is either 0 or a quartic form. In the first case f_i $(1 \leqslant i \leqslant k)$ have a common factor, say d. If d is of degree 2 then for each $i \leqslant k$ we have $f_i = c_i d, c_i \in K$. The solvability of $f_i(x, y, z) = 0$ $(i \leqslant k)$ in a completion K_v of K implies the solvability of $d(x, y, z) = 0$ in K_v, and if it holds for all but one completion then by the product formula and Hasse's principle for one quadratic form we get solvability in K of $d(x, y, z) = 0$ and hence of $f_i(x, y, z) = 0$ $(1 \leqslant i \leqslant k)$. If d is of degree 1 then it has again a non-trivial zero in K and the same conclusion holds.

If $R(x, y; u_1, \dots, u_k, v_1, \dots, v_k)$ is not identically 0, let $r(x, y)$ be the highest common divisor of its coefficients when viewed as a form in $u_1, \dots, u_k, v_1, \dots, v_k$. If $f_i(x, y, z)$ $(1 \leqslant i \leqslant k)$ have a common non-trivial zero $\langle a_v, b_v, c_v\rangle$ in K_v, $\sum u_i f_i$ and $\sum v_i f_i$ have it also, hence $R(a_v, b_v; u_1, \dots, u_k, v_1, \dots, v_k) = 0$, which implies

$$r(a_v, b_v) = 0. \tag{2}$$

(Here we use the fact that the coefficients of R are forms in x, y). If $a_v = b_v = 0$ we have $c_v \neq 0$; hence the coefficient of z^2 in f_i is 0 for each $i \leqslant k$ and the forms f_i $(1 \leqslant i \leqslant k)$ have in K a common non-trivial zero $\langle 0, 0, 1\rangle$. If $\langle a_v, b_v\rangle \neq \langle 0, 0\rangle$ for each valuation v of K except at most one then by Lemma 1 r has in K a zero, say $\langle a, b\rangle \neq \langle 0, 0\rangle$. Thus $bx - ay \mid r(x, y)$,

$$bx - ay \mid R(x, y; u_1, \dots, u_k, v_1, \dots, v_k)$$

and by Lemma 2 either f_i have a common non-trivial zero in K or

$$(bx - ay)^2 \mid R(x, y; u_1, \dots, u_k, v_1, \dots, v_k) \tag{3}$$

and the forms $f_i(at, bt, z)$ $(1 \leqslant i \leqslant k)$ differ from their highest common divisor by a constant factor. In the latter case, by (3)

$$(bx - ay)^2 \mid r(x, y).$$

Let

$$r(x, y) = (bx - ay)^{\alpha} s(x, y), \tag{4}$$

where $\alpha \geqslant 2$, $s(a, b) \neq 0$, $\deg s = \deg r - \alpha \leqslant 2$. For every valuation v of K except at most one we have by (2) and (4)

$$ba_v - ab_v = 0 \quad \text{or} \quad s(a_v, b_v) = 0.$$

The first equation implies $a_v = at$, $b_v = bt$ for a $t \in K_v^*$; thus

$$F(t, u) = s(t, u) \operatorname*{h.c.d.}_{1 \leqslant i \leqslant k} f_i(at, bt, u)$$

has a non-trivial zero in K_v. Since by (4)

$$\deg F = \deg s + 2 = \deg r + 2 - \alpha \leqslant 4,$$

we infer from Lemma 1 that F has in K a zero, say $\langle c, d\rangle \neq \langle 0, 0\rangle$. If this is a zero of the

h.c.d.$_{1\leqslant i\leqslant k} f_i(at, bt, u)$, then

$$f_i(ac, bc, d) = 0 \ (1 \leqslant i \leqslant k), \quad \langle ac, bc, d\rangle \neq \langle 0, 0, 0\rangle.$$

If, on the other hand, $s(c, d) = 0$ then by (4) $r(c, d) = 0$; thus

$$R(c, d; u_1, \ldots, u_k, v_1, \ldots, v_k) = 0$$

and by Lemma 2 either f_i have a common non-trivial zero in K or

$$(dx - cy)^2 \mid R(x, y; u_1, \ldots, u_k, v_1, \ldots, v_k)$$

and $f_i(ct, dt, z)$ $(1 \leqslant i \leqslant k)$ differ by a constant factor from their highest common divisor. In the latter case

$$(dx - cy)^2 \mid r(x, y)$$

and by (4)

$$r(x, y) = e(bx - ay)^2(dx - cy)^2.$$

For every valuation v of K except at most one we have by (2)

$$ba_v - ab_v = 0 \quad \text{or} \quad da_v - cb_v = 0;$$

thus for a suitable $t \in K_v^*$ either $a_v = at$, $b_v = bt$ or $a_v = ct$, $b_v = dt$. It follows that the quartic form

$$G(t, u) = \underset{1\leqslant i\leqslant k}{\text{h.c.d.}} f_i(at, bt, u) \cdot \underset{1\leqslant i\leqslant k}{\text{h.c.d.}} f_i(ct, dt, u)$$

has a non-trivial zero in K_v. By Lemma 1 $G(t, u)$ has in K a zero, say $\langle t_0, u_0\rangle \neq \langle 0, 0\rangle$. If $\langle t_0, u_0\rangle$ is a zero of the h.c.d.$_{1\leqslant i\leqslant k} f_i(at, bt, u)$ then

$$f_i(at_0, bt_0, u_0) = 0 \ (1 \leqslant i \leqslant k), \quad \langle at_0, bt_0, u_0\rangle \neq \langle 0, 0, 0\rangle;$$

if $\langle t_0, u_0\rangle$ is a zero of the h.c.d.$_{1\leqslant i\leqslant k} f_i(ct, dt, u)$ then

$$f_i(ct_0, dt_0, u_0) = 0 \ (1 \leqslant i \leqslant k), \quad \langle ct_0, dt_0, u_0\rangle \neq \langle 0, 0, 0\rangle.$$

The proof is complete. □

For the proof of Theorem 2 we need three lemmata.

Lemma 3. *The equation* $u^4 - 17v^4 = 2w^2$ *has no solutions in* $\mathbb{Q}$ *except* $\langle 0, 0, 0\rangle$.

Proof. See Lind [5] or Reichardt [10]. □

Lemma 4. *Let* $F(x_1, \ldots, x_n)$ *be a polynomial with integer p-adic coefficients and* $\gamma_1, \ldots, \gamma_n$ *p-adic integers. If for an* $i \leqslant n$ *we have*

$$F(\gamma_1, \ldots, \gamma_n) \equiv 0 \ (\text{mod } p^{2\delta+1}),$$
$$\frac{\partial F}{\partial x_i}(\gamma_1, \ldots, \gamma_n) \equiv 0 \ (\text{mod } p^{\delta}),$$
$$\frac{\partial F}{\partial x_i}(\gamma_1, \ldots, \gamma_n) \not\equiv 0 \ (\text{mod } p^{\delta+1})$$

(δ a nonnegative integer) then there exist p-adic integers $\theta_1, \ldots, \theta_n$ such that

$$F(\theta_1, \ldots, \theta_n) = 0$$

and $\theta_1 \equiv \gamma_1 \pmod{p^{\delta+1}}, \ldots, \theta_n \equiv \gamma_n \pmod{p^{\delta+1}}$.

Proof. See [1], p. 42. □

c **Lemma 5.** *$f(x, y, z) = x^4 - 2y^4 - 16y^2z^2 - 49z^4$ is irreducible over every field of characteristic different from 2 and 17.*

Proof. Let k be a field of this kind. It is enough to show that $f(x, y, z)$ is irreducible as a polynomial in x over $k(y, z)$. If it were not, then by Capelli's theorem (see [9], Satz 428) $\pm(2y^4 + 16y^2z^2 + 49z^4)$ would have to be a square in $k(y, z)$. This condition implies that

$$16^2 - 4 \cdot 2 \cdot 49 = -8 \cdot 17 = 0,$$

which is possible only if $\operatorname{char} k = 2$ or $\operatorname{char} k = 17$. □

Proof of Theorem 2. $f(x, y, z) = x^4 - 17z^4 - 2(y^2 + 4z^2)^2$; hence by Lemma 3 if $f(x, y, z) = 0$ and $x, y, z \in \mathbb{Q}$ we have $x = y^2 + 4z^2 = 0$ and thus $x = y = z = 0$. Also $x_1^4 - 17x_2^4 - 2(x_3^2 + \ldots + x_n^2)^2 = 0$ implies $x_1 = x_2 = \ldots = x_n = 0$ for $x_i \in \mathbb{Q}$.

It remains to show that $f(x, y, z)$ represents 0 in every field $\mathbb{Q}_p$ including $\mathbb{Q}_\infty = \mathbb{R}$. We verify this first using Lemma 3 for $p = \infty$, 2, 5, 7, 13 and 17.

For $p = \infty$ we take $x = \sqrt[4]{2}$, $y = 1$, $z = 0$.

c For $p = 2$ we use Lemma 4 with $\gamma_1 = 3$, $\gamma_2 = 2$, $\gamma_3 = 1$, $\delta = 2$, $i = 1$.

For $p = 5$ we use Lemma 4 with $\gamma_1 = 0$, $\gamma_2 = 2$, $\gamma_3 = 1$, $\delta = 0$, $i = 2$.

For $p = 7$ we use Lemma 4 with $\gamma_1 = 2$, $\gamma_2 = 1$, $\gamma_3 = 0$, $\delta = 0$, $i = 1$.

For $p = 13$ we use Lemma 4 with $\gamma_1 = 1$, $\gamma_2 = 2$, $\gamma_3 = 3$, $\delta = 0$, $i = 1$.

For $p = 17$ we use Lemma 4 with $\gamma_1 = 0$, $\gamma_2 = 1$, $\gamma_3 = 2$, $\delta = 0$, $i = 2$.

For $p \neq 2, 5, 7, 13, 17$ we have either $p \geqslant 37$ or for a suitable sign $(\pm 7 \mid p) = 1$.

In the latter case the congruence

$$f(x, 0, z) = (x^2 - 7z^2)(x^2 + 7z^2) \equiv 0 \pmod{p}$$

is solvable non-trivially, and denoting its solution by γ_1, γ_3 we use Lemma 4 with $\gamma_2 = 0$, $\delta = 0$, $i = 1$.

It remains to consider primes $p \geqslant 37$. For such primes f is by Lemma 5 absolutely irreducible over $\mathbb{F}_p$. Moreover, it has no singular zeros. Indeed, the equations

$$4x^3 = 0, \quad -8y^3 - 32yz^2 = 0, \quad -32y^2z - 196z^3 = 0$$

c imply $x = 0$ and either $y = 0$, $196z^3 = 0$ or $y^2 + 4z^2 = 0$, $68z^3 = 0$; thus in any case $x = y = z = 0$. By the Riemann-Hurwitz formula the curve $f(x, y, z) = 0$ is over $\mathbb{F}_p$ of genus 3.

Therefore by Weil's theorem the number of points on this curve with coordinates in $\mathbb{F}_p$ is greater than $p + 1 - 6\sqrt{p}$, i.e., at least one. Since all points are non-singular, Lemma 4 applies with $\delta = 0$ and a suitable i. □

Note added in proof. I have learned that already in 1981 A. Bremner, D. J. Lewis and P. Morton found the example $3x^4 + 4y^4 - 19z^4$ of a ternary biquadratic form for which Hasse's principle fails, but they did not publish it.

References

[1] Z. I. Borevich, I. R. Shafarevich, *Number Theory*. Academic Press, New York 1966.

[2] J.-L. Colliot-Thélène, D. Coray, J.-J. Sansuc, *Descente et principe de Hasse pour certaines variétés rationnelles*. J. Reine Angew. Math. 320 (1980), 150–191.

[3] M. Fujiwara, *Hasse principle in algebraic equations*. Acta Arith. 22 (1973), 267–276.

[4] D. Hilbert, *Über Diophantische Gleichungen*. Nachr. Königl. Gesell. Wiss. Göttingen 1897, 48–54.

[5] C. E. Lind, *Untersuchungen über die rationale Punkte der ebenen kubischen Kurven vom Geschlecht Eins*. Doctoral dissertation, Uppsala 1940.

[6] L. J. Mordell, *The Diophantine equation* $Ax^4 + By^4 + Cz^4 = 0$. Proc. Cambridge Philos. Soc. 68 (1970), 125–128.

[7] O. Perron, *Algebra* I. Walter de Gruyter, Berlin 1951.

[8] L. Rédei, *Über die Determinantenteiler*. Acta Math. Acad. Sci. Hungar. 3 (1952), 143–150.

[9] —, *Algebra* I. Akademische Verlagsgesellschaft, Geest & Portig, Leipzig 1959.

[10] H. Reichardt, *Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen*. J. Reine Angew. Math. 184 (1942), 12–18.

Originally published in
Sets, Graphs and Numbers, Budapest (Hungary), 1991
Colloquia Mathematica Societatis János Bolyai 60
North-Holland, Amsterdam 1992, 329–356

On Runge's theorem about Diophantine equations

with A. Grytczuk (Zielona Góra)

In 1887, C. Runge [14] proved the following theorem. Let $f \in \mathbb{Z}[X, Y]$ be an irreducible polynomial. If the equation $f(x, y) = 0$ has infinitely many integer solutions then the following conditions hold (*):

(C_1) the highest powers of X and Y in f occur as isolated terms aX^m and bY^n;

(C_2) for every term $cX^{\varrho}Y^{\sigma}$ of f we have $n\varrho + m\sigma \leqslant mn$;

(C_3) the sum of all terms of f for which $n\varrho + m\sigma = mn$ is up to a constant factor a power of an irreducible polynomial
(the last condition is stated by Runge in a little weaker form, but his proof gives what is asserted here).

In the course of the proof Runge established also under the same assumption the following condition which together with (C_1) is stronger than (C_2)–(C_3):

(C_4) there is only one system of conjugate Puiseux expansions at $x = \infty$ for the algebraic function $y = y(x)$ defined by $f(x, y) = 0$.

An essential feature of Runge's theorem is that if his conditions are not fulfilled, all integral solutions of the equation $f(x, y) = 0$ can be found effectively. The special case, where all real roots of the leading form of $f(X, Y)$ are simple and rational $\neq 0$ was rediscovered by E. Maillet [11] and an algorithm to find bounds for the size of solutions has been given by him in [12] under the additional assumption that all roots of the leading form of f are distinct. In the general case, bounds have been given by D. L. Hilliker and E. G. Straus [4]. If $d_0 = \min\{\deg_X f, \deg_Y f\} = 1$ and $d = \max\{\deg_X f, \deg_Y f\} > 2$ their bound given in Theorem 3.3 is false (see below). But for $d = 1$ or $d_0 > 1$ they have proved that if Runge's conditions (C_1)–(C_3), which they formulate differently, are violated then all integral solutions of the equation $f(x, y) = 0$ satisfy

$$\max\{|x|, |y|\} < \begin{cases} 4(\|f\| + 1)^2 & \text{if } d = 1, \\ (8d\|f\|)^{d^{2d^3}} & \text{if } d_0 > 1, \end{cases}$$

(*) Capital letters $X, Y, \ldots, \Xi, H, \ldots$ denote indeterminates, small letters $x, y, \ldots, \xi, \eta, \ldots$ denote elements of the relevant fields.

where $\|f\|$ is the height of f (see [4], Theorem 3.2 and Theorem 4.9). Although they do not say so the same inequality follows from their argument if (C_4) is violated (then in their notation $\deg_y Q^* \leqslant se < \deg_y f$, hence $(Q^*, f) = 1$).

Many special equations to which Runge's theorem applies have been considered. Thus for f of degree 2 the second author gave the essentially best possible bound

$$\max\{|x|, |y|\} \ll \|f\|^4$$

(see [16]) and for equations $y^2 = f(x)$, f — a monic quartic polynomial, D. W. Masser [13] gave the essentially best possible bound

$$|x| \ll \|f\|^3$$

(essentially means here up to a multiplicative constant). D. W. Masser has also called our attention to the fact that the bound of Hilliker and Straus can be improved by means of a recent result of W. Schmidt [18]. Indeed, when one combines the argument of Hilliker and Straus with Theorem 3 of [18] one obtains the following assertion.

Let $f \in \mathbb{Z}[X, Y]$ be irreducible of height $\|f\|$. Let $\deg_X f = m$, $\deg_Y f = n$, $d_0 = \min\{m, n\}$, $d = \max\{m, n\}$ and let integers x, y satisfy $f(x, y) = 0$. If (C_1) is not satisfied by the variable X or (C_4) does not hold, then

$$|x| \leqslant \left(2^{17} m^3 n^6 \|f\|\right)^{16mn^6(m+2)(n+2)}$$
$$|y| \leqslant \left(2^{17} m^3 n^6 \|f\|\right)^{16m^2n^5(m+2)(n+2)}.$$

If (C_1) holds, but (C_2) or (C_3) does not, then

$$|x| \leqslant \left(2^{17} d_0^3 d^6 \|f\|\right)^{16d_0^5 dn(m+2)(n+2)}$$
$$|y| \leqslant \left(2^{17} d_0^3 d^6 \|f\|\right)^{16d_0^5 dm(m+2)(n+2)}.$$

Hilliker and Straus have used the original Runge's approach based on the Puiseux expansions of the algebraic function defined by $f(x, y) = 0$. In 1922 Skolem [20] gave another proof of Runge's theorem based on elimination theory. In the present paper we use Skolem's approach to prove a bound for $\max\{|x|, |y|\}$ which is better for $d > 1$ than the bound of Hilliker and Straus, and often better than the assertion above, but which does not apply if only (C_4) is violated. In the course of the proof we fill in a gap that occurs in Skolem's paper. We prove the following

Theorem. *Let $f \in \mathbb{Z}[X, Y]$ be irreducible of height $\|f\|$, $m = \deg_X f$, $n = \deg_Y f$, $d_0 = \min\{m, n\}$, $d = \max\{m, n\}$ and let integers x, y satisfy $f(x, y) = 0$.*

(i) *If (C_1) is not satisfied by the variable X, then*

$$|x| \leqslant \left((m+1)(n+1)(mn+1)^{2/n}\|f\|\right)^{2n(mn+1)^3},$$
$$|y| \leqslant \left((m+1)(n+1)(mn+1)^{2/n}\|f\|\right)^{2(mn+1)^3}.$$

(ii) *If* (C_1) *holds, but* (C_2) *does not, then*

$$|x| < \left((4mnd_0)^{8mn(m,n)^{-1}}\|f\|\right)^{96m^3n^4(m,n)^{-4}d_0^4+m^{-1}d_0},$$

$$|y| < \left((4mnd_0)^{8mn(m,n)^{-1}}\|f\|\right)^{96m^4n^3(m,n)^{-4}d_0^4+n^{-1}d_0}.$$

(iii) *If* (C_1) *and* (C_2) *hold, but* (C_3) *does not, then*

$$|x| < \left((mn)^{3mn(m,n)^{-1}}\|f\|\right)^{\frac{5}{128}m^3n^4(m,n)^4+m^{-1}(m,n)^2},$$

$$|y| < \left((mn)^{3mn(m,n)^{-1}}\|f\|\right)^{\frac{5}{128}m^4n^3(m,n)^4+n^{-1}(m,n)^2}.$$

No attention should be attached to the coefficients of $\|f\|$, which in the cases (ii)–(iii) probably can be much improved. On the other hand, an effort has been made to obtain the exponents as small as the method allows.

Corollary. *In the notation of the theorem either* (C_1)–(C_3) *hold or*

$$\max\{|x|, |y|\} < \begin{cases} (45\|f\|)^{250} & \text{if } d = 2, \\ \left((4d^3)^{8d^2}\|f\|\right)^{96d^{11}} & \text{if } d > 2. \end{cases}$$

The example of the equation $xy - ty - tx^d = 0$ with a solution $x = t^{d+1} + t$, $y = (t^d + 1)^d$ shows that the exponents 250 and $96d^{11}$ in the corollary cannot be lowered below 4 or d^2 respectively. The same example shows that the bound $d(\|f\| + 1)^{2d}$ given by Hilliker and Straus in their Theorem 3.3 for the case $d_0 = 1$ is false for $d > 2$. On the other hand, the assertion on p. 93 implies that $96d^{11}$ can be replaced by $16d^7(d + 2)^2$.

The proof of the theorem falls into three main steps. (A) (Lemmas 1 to 4). We consider the special case, where the leading form of f is a monomial divisible by XY. For equations of this special type if $f(x, y) = 0$ and, say, $|x| \geqslant \max\{x_0, |y|\}$ we have such good control of y as a function of x that we can construct a polynomial $F \in \mathbb{Z}[X, Y]$ prime to f, which vanishes for all pairs (x, y) in question; this bounds the solution. (B) (Lemmas 5 to 9). Under the general assumptions of the theorem we find polynomials $G, H \in \mathbb{Z}[X, Y]$ such that the minimal equation connecting $G(x, y)$, $H(x, y)$ subject to $f(x, y) = 0$ is of the special type considered in (A). (C) (Lemmas 10, 11 and the proof of the theorem in the strict sense). We deduce the estimates in the general case from those obtained in (A) by deducing bounds for x, y from those for $G(x, y)$, $H(x, y)$.

It should be mentioned that the condition (C_3) has been sharpened by the second author [15] and the condition (C_4) by M. Ayad [1]. However their proofs do not lead to bounds for the size of possible solutions of the equation $f(x, y) = 0$, since they use an ineffective theorem of Siegel [19].

$\mathbb{N}$ and $\mathbb{N}_0$ denote the set of positive integers and of nonnegative integers, respectively. For a real number x, $\lceil x \rceil$ is the least integer greater than or equal to x.

For a polynomial F with coefficients $a_i \in \mathbb{C}$ we shall put

$$\|F\| = \max_i |a_i|, \quad \|F\|_\nu = \left(\sum_i |a_i|^\nu\right)^{1/\nu} \quad (\nu = 1, 2).$$

We conclude the introduction by expressing our thanks to Professor J. W. S. Cassels for the remarks incorporated in the present version of the paper and to Mr. K. Stefański for his remarks on an early draft.

Lemma 1. *Let* $P, Q \in \mathbb{Z}[X, y]$, $(P, Q) = 1$, $\deg_X P = p_1$, $\deg_Y P = p_2$, *and similarly for* Q. *If*

$$P(x, y) = Q(x, y) = 0 \tag{1}$$

then

$$|x| \leqslant \Big(\|P\|(p_1+1)\sqrt{p_2+1}\Big)^{q_2}\Big(\|Q\|(q_1+1)\sqrt{q_2+1}\Big)^{p_2}.$$

Proof. Since $(P, Q) = 1$ the resultant $R(X)$ of P and Q with respect to Y is not zero and clearly (1) implies that $R(x) = 0$. Since the leading coefficient of R is in absolute value $\geqslant 1$ we have by the inequality of Landau [6]

$$|x| \leqslant \|R\|_2. \tag{2}$$

Now

$$\|R\|_2 \leqslant \max_{|\xi|=1} |R(\xi)| \tag{3}$$

and using the Hadamard inequality for the determinant of the Sylvester matrix we obtain

$$\|R\|_2 \leqslant \sqrt{\prod_{j=1}^{q_2}\big(\|P\|^2(p_1+1)^2(p_2+1)\big)\prod_{j=1}^{p_2}\big(\|Q\|^2(q_1+1)^2(q_2+1)\big)}.$$

The inequalities (2) and (3) imply the lemma. □

Lemma 2. *For all integers* $n > \nu > 0$, $r \geqslant 1$, $t \geqslant 0$, $\mu \geqslant 0$, $\lambda \geqslant 1$, $k \neq 0$ *for every polynomial* $f \in \mathbb{Z}[X, Y]$ *with the leading form equal to* $kX^\nu Y^{n-\nu}$ *there exist polynomials* $B_{r,t,\mu}, C_{r,t,\lambda} \in \mathbb{Z}[X]$ *with the following properties*

$$\deg B_{r,t,\mu} \leqslant \mu, \tag{4}$$

$$\|B_{r,t,\mu}\| \leqslant n^{2(r-1)}\|f\|^r, \tag{5}$$

$$\deg C_{r,t,\lambda} \leqslant \nu r + \lambda + t - 1, \tag{6}$$

$$\|C_{r,t,\lambda}\| \leqslant 2n^{2(r-1)}\|f\|^r; \tag{7}$$

if $f(x, y) = 0$, $x \neq 0$ *then*

$$y^{n-\nu+t} = \sum_{\mu=0}^{r(\nu-1)+t} \frac{B_{r,t,\mu}(x)}{(kx^\nu)^r}\, y^{n-1+(r-1)(\nu-1)+t-\mu} + \sum_{\lambda=1}^{n-\nu} \frac{C_{r,t,\lambda}(x)}{(kx^\nu)^r}\, y^{n-\nu-\lambda}.$$

Proof. We define the polynomials $B_{r,t,\mu}$, $C_{r,t,\lambda}$ by induction on r as follows

$$\sum_{\mu=0}^{t+\nu-1} B_{1,t,\mu}(X)Y^{n-1+t-\mu} + \sum_{\lambda=1}^{n-\nu} C_{1,t,\lambda}(X)Y^{n-\nu-\lambda}$$
$$= -Y^t\big(f(X,Y) - kX^\nu Y^{n-\nu}\big) := -\sum_{j=0}^{n-1} A_j(X)Y^{n-1-j+t}$$

and

$$B_{r+1,t,\mu} = -\sum_{\substack{h+j=\mu \\ r(\nu-1)+t\geqslant h\geqslant 0 \\ n>j\geqslant 0}} B_{r,t,h}A_j \qquad (\mu \leqslant (r+1)(\nu-1)+t), \tag{8}$$

$$C_{r+1,t,\lambda} = kX^\nu C_{r,t,\lambda} - \sum_{\substack{h+j=(r+1)(\nu-1)+t+\lambda \\ r(\nu-1)+t\geqslant h\geqslant 0 \\ n>j\geqslant 0}} B_{r,t,h}A_j \qquad (1 \leqslant \lambda \leqslant n-\nu). \tag{9}$$

All assertions of the lemma follow by induction on r.

Indeed, we have

$$B_{1,t,\mu} = \begin{cases} -A_\mu & \text{if } 0 \leqslant \mu \leqslant \min\{n-1, t+\nu-1\}, \\ 0 & \text{otherwise,} \end{cases}$$

hence

$$\deg B_{1,t,\mu} \leqslant \deg A_\mu \leqslant \mu,$$
$$\|B_{1,t,\mu}\| \leqslant \|A_\mu\| \leqslant \|f\|$$

and by (8)

$$\deg B_{r+1,t,\mu} \leqslant \max_{h+j=\mu}\{\deg B_{r,t,h} + \deg A_j\} \leqslant \max_{h+j=\mu}\{h+j\} = \mu,$$
$$\|B_{r+1,t,\mu}\| \leqslant n \max_{h+j=\mu} \|B_{r,t,h}A_j\| \leqslant n^2\|f\| \max_{h\leqslant\mu} \|B_{r,t,h}\|$$
$$\leqslant n^2 \cdot n^{2(r-1)}\|f\|^{r+1} = n^{2r}\|f\|^{r+1}.$$

Similarly

$$C_{1,t,\lambda} = \begin{cases} -A_{\nu+\lambda+t-1} & \text{if } 1 \leqslant \lambda \leqslant n-\nu-t, \\ 0 & \text{otherwise,} \end{cases}$$

hence (6) and (7) follow from (9) by induction on r. Indeed, these formulae are true for $r = 1$ and assuming that (6), (7) hold for a fixed r we find from (4), (5) and (9)

$$\deg C_{r+1,t,\lambda} \leqslant \max\big\{\nu + \deg C_{r,t,\lambda}, (r+1)(\nu-1)+t+\lambda\big\}$$
$$\leqslant \max\big\{\nu(r+1)+\lambda+t-1, (r+1)(\nu-1)+t+\lambda\big\}$$
$$= \nu(r+1)+\lambda+t-1,$$

$$
\begin{aligned}
\|C_{r+1,t,\lambda}\| &\leqslant k\|C_{r,t,\lambda}\| + n \max_{h+j=(r+1)(\nu-1)+t+\lambda} \|B_{h,r,t}A_j\| \\
&\leqslant k\cdot 2n^{2(r-1)}\|f\|^r + n^2\|f\| \max_{h\leqslant(r+1)(\nu-1)+t+\lambda} \|B_{h,r,t}\| \\
&\leqslant 2n^{2(r-1)}\|f\|^{r+1} + n^2\|f\|n^{2(r-1)}\|f\|^r \\
&\leqslant \left(n^{2r} + 2n^{2(r-1)}\right)\|f\|^{r+1} \\
&\leqslant 2n^{2r}\|f\|^{r+1}.
\end{aligned}
$$

The remaining assertion of the lemma is true by definition of $B_{1,t,\mu}$, $C_{1,t,\lambda}$ for $r = 1$ and assuming its truth for a fixed r we infer by (8) and (9) from $f(x, y) = 0$

$$
\begin{aligned}
y^{n-\nu+t} &= \sum_{\mu=0}^{r(\nu-1)+t} \frac{B_{r,t,\mu}(x)}{(kx^\nu)^r}\, y^{n-1+(r-1)(\nu-1)+t-\mu} \\
&\quad + \sum_{\lambda=1}^{n-\nu} \frac{C_{r,t,\lambda}(x)}{(kx^\nu)^r}\, y^{n-\nu-\lambda} = \sum_{\mu=0}^{r(\nu-1)+t} \frac{B_{r,t,\mu}(x)}{(kx^\nu)^r}\, y^{(\nu-1)r+t-\mu} \\
&\quad \cdot \left(-\sum_{j=0}^{n-1} \frac{A_j(x)}{kx^\nu}\, y^{n-1-j}\right) + \sum_{\lambda=1}^{n-\nu} \frac{C_{r,t,\lambda}(x)}{(kx^\nu)^r}\, y^{n-\nu-\lambda} \\
&= -\sum_{\mu=0}^{(r+1)(\nu-1)+t} \frac{y^{n-1+r(\nu-1)+t-\mu}}{(kx^\nu)^{r+1}} \sum_{\substack{h+j=\mu \\ 0\leqslant j<n \\ 0\leqslant h\leqslant r(\nu-1)+t}} B_{r,t,h}(x)A_j(x) \\
&\quad - \sum_{\lambda=1}^{n-\nu} \sum_{h+j=(r+1)(\nu-1)+t+\lambda} B_{r,t,h}(x)A_j(x)\, \frac{y^{n-\nu-\lambda}}{(kx^\nu)^{r+1}} + \sum_{\lambda=1}^{n-\nu} \frac{C_{r,t,\lambda}(x)}{(kx^\nu)^{r+1}}\, kx^\nu \\
&= \sum_{\mu=0}^{(r+1)(\nu-1)+t} \frac{B_{r+1,t,\mu}(x)}{(kx^\nu)^{r+1}}\, y^{n-1+r(\nu-1)+t-\mu} \\
&\quad + \sum_{\lambda=1}^{n-\nu} \frac{C_{r+1,t,\lambda}(x)}{(kx^\nu)^{r+1}}\, y^{n-\nu-\lambda}.
\end{aligned}
$$

The inductive proof is complete. □

Lemma 3. *For all integers $n > \nu > 0$, $k \neq 0$ and every polynomial $f \in \mathbb{Z}[X, Y]$ with the leading form equal to $kX^\nu Y^{n-\nu}$ there exists a polynomial $F \in \mathbb{Z}[X, Y]$ with the following properties*

(10) *the leading form of F is a monomial in Y,*

(11) $$\deg_X F < \deg_Y F < n^2,$$

(12) $$\|F\| < \left(n^2\|f\|\right)^{2n^2}.$$

(13) *If $x, y \in \mathbb{Z}$, $|x| \geqslant |y|$ and*

(13_1) $$f(x, y) = 0$$

then either $F(x, y) = 0$ or

$$|x| < \left(n^2\|f\|\right)^{2n^3}.$$

Proof. By Lemma 2 with $r = n - \nu + t$ (13_1) implies for $x \neq 0$

$$y^{n-\nu+t} = \sum_{\mu=0}^{(n-\nu+t)(\nu-1)+t} \frac{B_{n-\nu+t,t,\mu}(x)}{(kx^{\nu})^{n-\nu+t}}\, y^{n-1+(n-\nu+t-1)(\nu-1)+t-\mu} + \sum_{\lambda=1}^{n-\nu} \frac{C_{n-\nu+t,t,\lambda}(x)}{(kx^{\nu})^{n-\nu+t}}\, y^{n-\nu-\lambda}. \tag{14}$$

Now let us write

$$C_{n-\nu+t,t,\lambda} = D_{t,\lambda} X^{\nu(n-\nu+t)} + E_{t,\lambda} X^{\nu(n-\nu+t)-n+\nu+\lambda+1} + F_{t,\lambda}, \tag{15}$$

where

$$\begin{aligned} &D_{t,\lambda},\ E_{t,\lambda},\ F_{t,\lambda} \in \mathbb{Z}[X], \\ &\deg E_{t,\lambda} < n-\nu-\lambda-1 \text{ if } \lambda < n-\nu-1, \quad E_{t,n-\nu-1} = E_{t,n-\nu} = 0, \\ &\deg F_{t,\lambda} < \nu(n-\nu+t) - n + \min\{\lambda+\nu+1, n\}. \end{aligned} \tag{16}$$

It follows by (6) that

$$\deg D_{t,\lambda} \leqslant \lambda + t - 1. \tag{17}$$

We have from (14)

$$\begin{aligned} (ky)^{n-\nu+t} = &\sum_{\mu=0}^{(n-\nu+t)(\nu-1)+t} \frac{B_{n-\nu+t,t,\mu}(x)}{x^{\nu(n-\nu+t)}}\, y^{\nu(n-\nu+t)-\mu} \\ &+ \sum_{\lambda=1}^{n-\nu} D_{t,\lambda}(x) y^{n-\nu-\lambda} + \sum_{\lambda=1}^{n-\nu} \frac{E_{t,\lambda}(x)}{x^{n-\nu-\lambda-1}}\, y^{n-\nu-\lambda} \\ &+ \sum_{\lambda=1}^{n-\nu} \frac{F_{t,\lambda}(x)}{x^{\nu(n-\nu+t)}}\, y^{n-\nu-\lambda}. \end{aligned} \tag{18}$$

For $n - \nu \geqslant 3$ let us denote all the quotients y^s/x^t, where $0 < t < s \leqslant n-\nu-1$ in whatever order by $\Theta_1, \ldots, \Theta_N$, where $N = \binom{n-\nu-1}{2}$ and let

$$\sum_{\lambda=1}^{n-\nu} \frac{E_{t,\lambda}(x)}{x^{n-\nu-\lambda-1}}\, y^{n-\nu-\lambda} = \sum_{j=1}^{N} a_{t,j}\Theta_j. \tag{19}$$

By (16) we have $a_{t,j} \in \mathbb{Z}$, by (15) and Lemma 2

$$|a_{t,j}| < 2n^{2(n-\nu+t-1)} \|f\|^{n-\nu+t}. \tag{20}$$

By virtue of the Bombieri-Vaaler theorem [2] there exists an integer solution $[C_0, C_1, \ldots, C_{2N-1}]$ of the system of equations

$$\sum_{t=0}^{2N-1} C_t a_{t,j} = 0 \quad (1 \leqslant j \leqslant N) \tag{21}$$

satisfying the condition

$$0 < \max_{0\leqslant t<2N} |C_t| \leqslant \sqrt[2N]{\det AA^t}\,,$$

where A is a submatrix of the maximal rank of $(a_{t,j})_{\substack{0\leqslant t<2N\\ 1\leqslant j\leqslant N}}$. Using (20) and the generalized Hadamard inequality (cf. [2], p. 16) we find

$$\begin{aligned}(22)\qquad \max_{0\leqslant t<2N} |C_t| &\leqslant \sqrt{\sum_{t=0}^{2N-1} 4n^{4(n-\nu+t-1)}\|f\|^{2(n-\nu+t)}}\\ &\leqslant 2^{3/2}n^{2(n-\nu+2N-2)}\|f\|^{n-\nu+2N-1} \leqslant \left(n^2\|f\|\right)^{n^2}.\end{aligned}$$

For $n-\nu \leqslant 2$ we take $N=\frac{1}{2}$, $C_0=1$, so that (22) still holds.

From (18), (19) and (21) we obtain

$$\begin{aligned}\sum_{t=0}^{2N-1} C_t(ky)^{n-\nu+t} &= \sum_{t=0}^{2N-1} C_t \sum_{\mu=0}^{(n-\nu+t)(\nu-1)+t} \frac{B_{n-\nu+t,t,\mu}(x)}{x^{\nu(n-\nu+t)}}\, y^{\nu(n-\nu+t)-\mu}\\ &\quad + \sum_{t=0}^{2N-1} C_t \sum_{\lambda=1}^{n-\nu} D_{t,\lambda}(x) y^{n-\nu-\lambda}\\ &\quad + \sum_{t=0}^{2N-1} C_t \sum_{\lambda=1}^{n-\nu} \frac{F_{t,\lambda}(x)}{x^{\nu(n-\nu+t)}}\, y^{n-\nu-\lambda}.\end{aligned}$$

If $y\neq 0$ and

$$\begin{aligned}|x| > |y| &\sum_{t=0}^{2N-1} |C_t|\\ &\cdot \left\{ \sum_{\mu=0}^{(n-\nu+t)(\nu-1)+t} (\mu+1)\|B_{n-\nu+t,t,\mu}\| + \sum_{\lambda=1}^{n-\nu} \nu(n-\nu+t)\|F_{t,\lambda}\| \right\}\end{aligned}$$

then the sum of the first and of the third term on the right hand side above is in absolute value less than 1, and since the second term is an integer and so is the left hand side, we obtain

$$(23)\qquad \sum_{t=0}^{2N-1} C_t(ky)^{n-\nu+t} = \sum_{t=0}^{2N-1} C_t \sum_{\lambda=1}^{n-\nu} D_{t,\lambda}(x) y^{n-\nu-\lambda}.$$

Therefore we take

$$(24)\qquad F = Y\sum_{t=0}^{2N-1} C_t(kY)^{n-\nu+t} - Y\sum_{\lambda=1}^{n-\nu}\left(\sum_{t=0}^{2N-1} C_t D_{t,\lambda}(X)\right) Y^{n-\nu-\lambda}.$$

By (16) $F \in \mathbb{Z}[X, Y]$. Let T be the greatest $t < 2N$ such that $C_t \neq 0$. Then by (17)

$$\deg \sum_{t=0}^{2N-1} C_t (kY)^{n-\nu+t} = n - \nu + T > \deg \sum_{\lambda=1}^{n-\nu} \left(\sum_{t=0}^{2N-1} C_t D_{t,\lambda}(X) \right) Y^{n-\nu-\lambda}$$

hence (10) holds. Besides

$$\deg_X F < \deg_Y F \leqslant n - \nu + 2N < n^2,$$

while by (7), (15) and (22)

$$\begin{aligned} \|F\| &\leqslant \max\left\{ \max_{0 \leqslant t < N} |C_t| \cdot k^{n-\nu+2N-1}, \sum_{t=0}^{2N-1} |C_t| \max_{\lambda} \|D_{t,\lambda}\| \right\} \\ &\leqslant \left(n^2 \|f\|\right)^{n^2} \max\left\{ k^{n-\nu+2N-1}, 2 \sum_{t=0}^{2N-1} n^{2(n-\nu+t-1)} \|f\|^{n-\nu+t} \right\} \\ &\leqslant \left(n^2 \|f\|\right)^{n^2} 4n^{2(n-\nu+2N-2)} \|f\|^{n-\nu+2N-1} \leqslant \left(n^2 \|f\|\right)^{2n^2}, \end{aligned}$$

which gives (11) and (12).

If (13_1) holds then by (23) and (24) either $F(x, y) = 0$ or

$$|x| \leqslant |y| \sum_{t=0}^{2N-1} |C_t| \cdot \left\{ \sum_{\mu=0}^{(n-\nu+t)(\nu-1)+t} (\mu+1) \|B_{n-\nu+t,t,\mu}\| + \sum_{\lambda=1}^{n-\nu} \nu(n-\nu+t) \|F_{t,\lambda}\| \right\}.$$

The latter relation implies by (5), (7), (15) and (22)

$$\begin{aligned} |x| \leqslant |y| \cdot \left(n^2 \|f\|\right)^{n^2} \sum_{t=0}^{2N-1} \Bigg\{ & \sum_{\mu=0}^{(n-\nu+t)(\nu-1)+t} (\mu+1) n^{2(n-\nu+t-1)} \|f\|^{n-\nu+t} \\ & + (n-\nu)\nu(n-\nu+t) \cdot 2n^{2(n-\nu+t-1)} \|f\|^{n-\nu+t} \Bigg\}. \end{aligned}$$

Now we use the principle that the sum of a series growing quicker than a geometric progression with ratio 2 does not exceed the last term taken twice, and obtain

$$\begin{aligned} |x| &\leqslant |y| \cdot \left(n^2 \|f\|\right)^{n^2} 2 \Bigg\{ \binom{(n-\nu+2N-1)(\nu-1)+2N+1}{2} n^{2(n-\nu+2N-2)} \\ &\quad \cdot \|f\|^{n-\nu+2N-1} + (n-\nu)\nu(n-\nu+2N-1) \\ &\quad \cdot 2n^{2(n-\nu+2N-2)} \|f\|^{n-\nu+2N-1} \Bigg\} \\ &\leqslant |y| \cdot \left(n^2 \|f\|\right)^{n^2} 2 \left\{ \frac{n^6}{2} n^{2n^2-10} \|f\|^{n^2} + \frac{n^4}{2} n^{2n^2-10} \|f\|^{n^2} \right\} \\ &\leqslant |y| \cdot \left(n^2 \|f\|\right)^{n^2} := B|y|. \end{aligned}$$

If $|x| \geqslant |y|$ we infer from the equation (13_1) that

$$\begin{aligned} |x|^n &\leqslant B^{n-\nu}|k|\,|x|^\nu\,|y|^{n-\nu} = B^{n-\nu}|f(x,y) - kx^\nu y^{n-\nu}| \\ &\leqslant B^{n-\nu}\binom{n+1}{2}\|f\|\,|x|^{n-1}, \end{aligned}$$

hence

$$\begin{aligned} |x| &\leqslant \binom{n+1}{2}B^{n-\nu}\|f\| < \binom{n+1}{2}\|f\|\big(n^2\|f\|\big)^{2n^2(n-1)} \\ &\leqslant \big(n^2\|f\|\big)^{2n^3}. \end{aligned}$$

□

Remark 1. Although the general idea is the same, Skolem [20] constructs the polynomial F differently. In his argument the proof is lacking, that the number $C_0 + \ldots + C_N$ occurring in his formula (9) is different from zero.

Lemma 4. *For every irreducible polynomial $f \in \mathbb{Z}[X, Y]$ with the leading form equal to $kX^\nu Y^{n-\nu}$ $(n > \nu > 0)$ all integral solutions of the equation $f(x, y) = 0$ satisfy*

$$\max\big\{|x|, |y|\big\} \leqslant \big(n^2\|f\|\big)^{2n^3}.$$

Proof. In view of symmetry it is permissible to assume that $|x| \geqslant |y|$. Let F be a polynomial with properties specified in Lemma 3. Since f is irreducible we have either $f \mid F$ or $(f, F) = 1$. The former is impossible by (10), since the leading form of f does not divide the leading form of F.

Therefore $(f, F) = 1$ and by Lemma 1 and (11) the conditions $f(x, y) = 0$, $F(x, y) = 0$ imply

$$|x| \leqslant \big(\|f\|n^{3/2}\big)^{n^2}\big(\|F\|n^3\big)^{n-1}.$$

However by (12)

$$\|F\| < \big(n^2\|f\|\big)^{2n^2}.$$

Hence

$$|x| \leqslant n^{4n^3-\frac{5}{2}n^2+3n-3}\|f\|^{2n^3-n^2} \leqslant \big(n^2\|f\|\big)^{2n^3}.$$

By (13) if $f(x, y) = 0$, $F(x, y) \neq 0$ and $|y| \leqslant |x|$ then

$$|x| \leqslant \big(n^2\|f\|\big)^{2n^3}.$$

Hence in both cases

$$|x| \leqslant \big(n^2\|f\|\big)^{2n^3}.$$

□

Remark 2. The example of the equation $xy^{n-1} - t(x + y)^{n-1} = 0$ with a solution $x = t(t + 1)^{n-1}$, $y = (t + 1)^{n-1}$ shows that the exponent $2n^3$ in the lemma cannot be lowered below n.

Lemma 5. *For the resultant* $R(\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3)$ *of homogeneous polynomials* $F_i(x_1, x_2, x_3)$ $(i = 1, 2, 3)$ *of degrees* $l_1 > 1$, $l_2 \geqslant 1$, $l_3 \geqslant 1$ *and with indeterminate coefficient vectors* $\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3$, *respectively, the following inequality holds*

$$\|R\|_1 \leqslant (l_1 + l_2 + l_3)^{l_1(18l_1l_2+7l_2^2+7l_3^2+36l_2l_3)/8}. \tag{25}$$

Proof. The resultant R is a polynomial with integral coefficients dividing the determinant D described on p. 7 of [8], the elements of which are either zeros or components of the vectors $\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3$. D is of order $\binom{l_1+l_2+l_3}{2}$, hence the number of terms in its expansion is $\binom{l_1+l_2+l_3}{2}!$ and we have

$$\|D\|_1 \leqslant \binom{l_1 + l_2 + l_3}{2}! \leqslant (l_1 + l_2 + l_3)^{(l_1+l_2+l_3)^2}. \tag{26}$$

It follows from the construction of the determinant D that it is homogeneous of degree $\binom{l_2+l_3}{2}$ in the components of $\boldsymbol{a}_1$ and homogeneous of degree $\frac{l_1(l_1+2l_3-1)}{2}$ in the components of $\boldsymbol{a}_2$.

Now $D = AR$, where $A \in \mathbb{Z}[\boldsymbol{b}_1, \boldsymbol{b}_2]$ and $\boldsymbol{b}_i$ is the coefficient vector of $F_i(x_1, x_2, 0)$ $(i = 1, 2)$, see [8], p. 11. Clearly, $\boldsymbol{b}_i$ has $l_i + 1$ components and thus

$$\begin{aligned} s = \sum_{i=1}^{2} \sum_{b} \deg_b D &\leqslant (l_1 + 1)\binom{l_2 + l_3}{2} + (l_2 + 1)\frac{l_1(l_1 + 2l_3 - 1)}{2} \\ &< \frac{1}{2}\big(l_1^2l_2 + l_1l_2^2 + l_1l_3^2 + 4l_1l_2l_3 + l_1^2 + l_2^2 + l_3^2 - 2l_1l_2 + l_1l_3 + 2l_2l_3\big), \end{aligned} \tag{27}$$

where b in the inner sum runs through all the components of $\boldsymbol{b}_i$. It follows from a theorem of Mahler [9] that

$$\|A\|_1\|R\|_1 \leqslant \|D\|_1 \cdot 2^s \leqslant \|D\|_1 \cdot (l_1 + l_2 + l_3)^{s/2}$$

and since $\|A\|_1 \geqslant 1$, $l_1 > 1$, we obtain (25) from (26) and (27). □

Remark 3. A better estimate for $\|R\|_1$ would follow from the expression for the resultant described in §7 of [7]. However this expression is given without a complete proof, therefore we do not use it.

Lemma 6. *Let* $c \in \mathbb{C} \setminus \{0\}$, $g, h \in \mathbb{C}[X, Y] \setminus \mathbb{C}$, $(g, h) = 1$, $\alpha, \beta, \gamma, \delta \in \mathbb{N}$, $g_0 = g(X^\alpha, Y^\beta)$, $h_0 = h(X^\alpha, Y^\beta)$ *be homogeneous of degrees* p_0, q_0 *respectively,* $p = \frac{p_0}{(p_0,q_0)}$, $q = \frac{q_0}{(p_0,q_0)}$.

Then the resultant R_0 *of the forms* $cg_0^\gamma h_0^\delta$, $g_0^q - \Xi Z^{p_0q}$, $h_0^p - HZ^{q_0p}$ *equals* $c_1\Xi^{\gamma p_0q_0p}H^{\delta p_0q_0q}$, *where* $c_1 \in \mathbb{C} \setminus \{0\}$.

Proof. From 5.11.2, 5.7 and 5.9 of [5] we obtain successively

$$\begin{aligned} R_0 &= c^{pqp_0q_0}\operatorname{Res}\big(g_0, g_0^q - \Xi Z^{p_0q}, h_0^p - HZ^{q_0p}\big)^\gamma \\ &\quad \cdot \operatorname{Res}\big(h_0, g_0^q - \Xi Z^{p_0q}, h_0^p - HZ^{q_0p}\big)^\delta \\ &= c^{pqp_0q_0}\operatorname{Res}\big(g_0, -\Xi Z^{p_0q}, h_0^p - HZ^{q_0p}\big)^\gamma \\ &\quad \cdot \operatorname{Res}\big(h_0, g_0^q - \Xi Z^{p_0q}, -HZ^{q_0p}\big)^\delta. \end{aligned}$$

Since $p_0q = q_0p$ we can apply 5.9 of [5] again and obtain using 5.7, 5.8, 5.11.2 of [5]

$$R_0 = c^{pqp_0q_0} \operatorname{Res}(g_0, -\Xi Z^{p_0q}, h_0^p)^\gamma \operatorname{Res}(h_0, g_0^q, -HZ^{q_0p})^\delta$$
$$= \pm c^{pqp_0q_0} \operatorname{Res}(\Xi Z^{p_0q}, g_0, h_0)^{\gamma p} \operatorname{Res}(HZ^{q_0p}, g_0, h_0)^{\delta q}.$$

Taking now in the Laplace formula ([5], 5.10)

$$f_1 = \Xi Z^{p_0q},\ f_2 = g_0,\ f_3 = h_0,\ X_1 = Z,\ X_2 = X,\ X_3 = Y,$$

we find

$$\operatorname{Res}(\Xi Z^{p_0q}, g_0, h_0) = \operatorname{Res}(\Xi Z^{p_0q})^{p_0q_0} \operatorname{Res}(g_0, h_0)^{p_0q} = \Xi^{p_0q_0} \operatorname{Res}(g_0, h_0)^{p_0q}.$$

Similarly

$$\operatorname{Res}(HZ^{q_0p}, g_0, h_0) = H^{p_0q_0} \operatorname{Res}(g_0, h_0)^{q_0p}.$$

Hence

$$R_0 = c_1 \Xi^{\gamma pp_0q_0} H^{\delta qp_0q_0},$$

where

$$c_1 = \pm c^{pqp_0q_0} \operatorname{Res}(g_0, h_0)^{\gamma pqp_0 + \delta pqq_0}.$$

Since $(g, h) = 1$ we have, e.g. by Lemma 1 on p. 110 of [17], $(g_0, h_0) = 1$, hence $\operatorname{Res}(g_0, h_0) \neq 0$ and $c_1 \neq 0$. □

Lemma 7. *Let X have weight α, Y the weight β, $f \in \mathbb{Z}[X, Y]$ and let the part of f of the greatest weight be equal to $cg^\gamma h^\delta$, where $\alpha, \beta, \gamma, \delta \in \mathbb{N}$, $c \neq 0$, $g, h \in \mathbb{Z}[X, Y] \setminus \mathbb{Z}$ have the weight p_0, q_0 and $(g, h) = 1$. Put $p = \frac{p_0}{(p_0, q_0)}$, $q = \frac{q_0}{(p_0, q_0)}$. Then the resultant R of the polynomials $f(X^\alpha, Y^\beta)$, $g(X^\alpha, Y^\beta)^q - \Xi$, $h(X^\alpha, Y^\beta)^p - H$ has the following properties*

(28) *the leading form of R equals $c_1 \Xi^{\gamma pp_0q_0} H^{\delta qp_0q_0}$, where $c_1 \neq 0$,*

(29)
$$\|R\|_1 \leqslant (\gamma p_0 + \delta q_0 + p_0q + q_0p)^{(\gamma p_0 + \delta q_0)p_0q_0(9\gamma p + 9\delta q + 25pq)/4}$$
$$\cdot \|f\|^{pqp_0q_0} \|g^q\|^{(\gamma p_0 + \delta q_0)pq_0} \|h^p\|^{(\gamma p_0 + \delta q_0)p_0q}.$$

Proof. R equals the resultant of the forms

$$Z^{\gamma p_0 + \delta q_0} f\big((X/Z)^\alpha, (Y/Z)^\beta\big),\ g(X^\alpha, Y^\beta)^q - \Xi Z^{p_0q},\ h(X^\alpha, Y^\beta)^p - HZ^{q_0p}.$$

We have

(30)
$$R = \sum a(\boldsymbol{\varepsilon}, \boldsymbol{\zeta}, \boldsymbol{\eta}) \prod_{i=1}^{I} c_i^{\varepsilon_i} \prod_{j=1}^{J} d_j^{\zeta_j} \Xi^{\zeta_{J+1}} \prod_{k=1}^{K} e_k^{\eta_k} H^{\eta_{K+1}},$$

where $c_1, \ldots, c_I, d_1, \ldots, d_J, e_1, \ldots, e_K$ are the coefficients of f, g^q, h^p, respectively (in whatever order), $\boldsymbol{\varepsilon} = [\varepsilon_1, \ldots, \varepsilon_I]$, $\boldsymbol{\zeta} = [\zeta_1, \ldots, \zeta_{J+1}]$, $\boldsymbol{\eta} = [\eta_1, \ldots, \eta_{K+1}]$ run through $\mathbb{N}_0^I, \mathbb{N}_0^{J+1}, \mathbb{N}_0^{K+1}$ and $a(\boldsymbol{\varepsilon}, \boldsymbol{\zeta}, \boldsymbol{\eta}) \neq 0$ implies

(31)
$$\sum_{i=1}^{I} \varepsilon_i = pqp_0q_0,\ \sum_{i=1}^{J+1} \zeta_j = (\gamma p_0 + \delta q_0)pq_0,\ \sum_{k=1}^{K+1} \eta_j = (\gamma p_0 + \delta q_0)qp_0$$

(see [5], 2.3, (ii) with $d_1 = \gamma p_0 + \delta q_0$, $d_2 = qp_0$, $d_3 = pq_0$),

$$\sum_{i=1}^{I} \varepsilon_i w(C_i) + \zeta_{J+1} qp_0 + \eta_{K+1} pq_0 = (\gamma p_0 + \delta q_0) pq p_0 q_0 \tag{32}$$

(see [5], 5.13.2), where $w(c_i)$ is the exponent of the power of Z by which c_i stands multiplied in $Z^{\gamma p_0 + \delta q_0} f\big((X/Z)^{\alpha}, (Y/Z)^{\beta}\big)$. By convention, we take $0^0 = 1$. We have

$$R = \sum\nolimits_1 + \sum\nolimits_2,$$

where $\sum_1$, $\sum_2$ are taken over all vectors $\boldsymbol{\varepsilon}, \boldsymbol{\zeta}, \boldsymbol{\eta}$ satisfying the condition $\sum\limits_{i=1}^{I} \varepsilon_i w(c_i) = 0$ and $\sum\limits_{i=1}^{I} \varepsilon_i w(c_i) > 0$, respectively.

However, by Lemma 6

$$\sum\nolimits_1 = R_0 = c_1 \Xi^{\gamma pp_0 q_0} H^{\delta q p_0 q_0}.$$

On the other hand, by (30) and (32) the degree of $\sum_2$ with respect to Ξ and H is less than $(\gamma p + \delta q) p_0 q_0$. (Note that $qp_0 = pq_0$.) Hence (28) holds. As to (29), it follows from Lemma 5, (30), (31) and the inequalities

$$\begin{aligned} |c_i| &\leqslant \|f\| \qquad (1 \leqslant i \leqslant I), \\ |d_j| &\leqslant \|g^q\| \qquad (1 \leqslant j \leqslant J), \\ |e_k| &\leqslant \|h^p\| \qquad (1 \leqslant k \leqslant K). \end{aligned}$$

□

Lemma 8. *Let f be irreducible. Under the assumptions of Lemma 7 there exists an irreducible polynomial $P \in \mathbb{Z}[\Xi, H]$ with the following properties*

$$P(g^q, h^p) \equiv 0 \pmod{f}; \tag{33}$$

$$\deg P \leqslant \left\lceil \frac{\gamma p_0 + \delta q_0}{\alpha\beta} \right\rceil \left\lceil \frac{p_0 q}{\alpha\beta} \right\rceil \alpha\beta = \varrho; \tag{34}$$

$$\text{the leading form of } P \text{ is of the type } k\Xi^{\mu} H^{\nu}, \text{ where } k \neq 0,\ \mu > 0,\ \nu > 0; \tag{35}$$

$$\|P\| \leqslant (\gamma p_0 + \delta q_0 + 2p_0 q)^{\varrho(9\gamma p_0 + 9\delta q_0 + 25 p_0 q)/4} \|f\|^{\varrho pq/(\gamma p + \delta q)} \|g^q\|^{\varrho} \|h^p\|^{\varrho}. \tag{36}$$

Remark 4. Skolem only outlines for $\gamma = \delta = 1$ a proof of the existence of an irreducible polynomial P with the properties (33) and (35). No estimates for its degree or height are given.

Proof. Using Proposition 7.2.1(i) of [5] with $n = 2$,

$$m_1 = \alpha,\ m_2 = \beta,\ P_1 = f,\ P_2 = g^q,\ P_3 = h^p,$$

$$d_1 = \left\lceil \frac{\gamma p_0 + \delta q_0}{\alpha\beta} \right\rceil \alpha\beta,\ d_2 = d_3 = \left\lceil \frac{p_0 q}{\alpha\beta} \right\rceil \alpha\beta$$

we infer the existence of a non-zero polynomial $\Phi \in \mathbb{Z}[T_1, T_2, T_3]$ of the type

$$\Phi = \sum_{d_1\alpha_1+d_2\alpha_2+d_3\alpha_3 \leqslant d_1d_2d_3/(\alpha\beta)} c_{\alpha_1\alpha_2\alpha_3} T_1^{\alpha_1} T_2^{\alpha_2} T_3^{\alpha_3},$$

such that

$$\Phi(f, g^q, h^p) = 0. \tag{37}$$

Let α_0 be the least nonnegative integer such that for some α_2, α_3 we have $c_{\alpha_0\alpha_2\alpha_3} \neq 0$. Put

$$Q(T_2, T_3) = \sum_{d_1\alpha_1+d_2\alpha_2+d_3\alpha_3 \leqslant d_1d_2d_3/(\alpha\beta)} c_{\alpha_0\alpha_2\alpha_3} T_2^{\alpha_2} T_3^{\alpha_3}.$$

It follows from (37) and the choice of α_0 that

$$Q(g^q, h^p) \equiv 0 \pmod{f}.$$

Moreover, since $d_2 = d_3$ we have

$$\deg Q \leqslant \frac{d_1d_2}{\alpha\beta} = \varrho.$$

Since f is irreducible there exists an irreducible factor $P \in \mathbb{Z}[\Xi, H]$ of Q such that (33) and (34) hold. Moreover, we may assume that P is primitive.

In order to prove (35) and (36) suppose that for some $\xi, \eta \in \mathbb{C}$ we have $R(\xi, \eta) = 0$, where R is the resultant described in Lemma 7. By the fundamental property of the resultant (see [8], p. 13) there exist $x, y, z \in \mathbb{C}$ not all zero such that

$$z^{\gamma p_0+\delta q_0} f\left(\left(\frac{x}{z}\right)^{\alpha}, \left(\frac{y}{z}\right)^{\beta}\right) = 0,$$

$$g(x^{\alpha}, y^{\beta})^q - \xi z^{p_0 q} = 0,$$

$$h(x^{\alpha}, y^{\beta}) - \eta z^{q_0 p} = 0.$$

However $z = 0$ is impossible, since it would give $g(x^{\alpha}, y^{\beta}) = h(x^{\alpha}, y^{\beta}) = 0$ and since $g(X^{\beta}, Y^{\alpha})$, $h(X^{\beta}, Y^{\alpha})$ are homogeneous, $\big(g(X^{\alpha}, Y^{\beta}), h(X^{\alpha}, Y^{\beta})\big) \neq 1$, hence $(g, h) \neq 1$, contrary to the assumption. Hence $z \neq 0$ and taking $x_1 = (x/z)^{\alpha}$, $y_1 = (y/z)^{\beta}$ we obtain

$$f(x_1, y_1) = g(x_1, y_1)^q - \xi = h(x_1, y_1)^p - \eta = 0.$$

From (33) it follows that $P(\xi, \eta) = 0$. Therefore, by the Hilbert-Netto theorem ([8], p. 48) we have for a positive integer m and a polynomial $S \in \mathbb{Q}[\Xi, H]$

$$P^m = RS.$$

It follows from the irreducibility of P that for a positive integer μ and a $c_2 \in \mathbb{Q}$

$$R = c_2 P^{\mu}, \tag{38}$$

which together with (28) implies (35).

However, since $R \in \mathbb{Z}[\Xi, H]$ and P is primitive, we have $c_2 \in \mathbb{Z}$. Comparing the degrees on both sides of (38) we obtain from (28) and (34)

$$\frac{1}{\mu} \leqslant \frac{\varrho}{(\gamma p + \delta q) p_0 q_0}. \tag{39}$$

On the other hand,

$$\|P\|^{\mu} \leqslant \max_{\substack{|\xi|=1\\|\eta|=1}} |P(\xi,\eta)|^{\mu} = \max_{\substack{|\xi|=1\\|\eta|=1}} \left|\frac{1}{c_2} R(\xi,\eta)\right| \leqslant \|R\|_1,$$

hence by (39)

$$\|P\| \leqslant \|R\|_1^{1/\mu} \leqslant \|R\|_1^{\varrho/((\gamma p+\delta q)p_0 q_0)}.$$

Together with (29) this gives (36). □

Lemma 9. *In the special case of Lemma* 8*, where* $g = X$, $h = Y$, $(\alpha, \beta) = 1$, *there is an irreducible polynomial* $P \in \mathbb{Z}[X, Y]$ *satisfying* (33), (35) *and such that*

$$\deg P \leqslant \alpha\gamma + \beta\delta,$$
$$\|P\| \leqslant \big((m+1)(n+1)\|f\|\big)^{\alpha\beta},\ m = \deg_X f,\ n = \deg_Y f.$$

Proof. Consider the polynomial

$$F(X,Y) = \prod_{i=0}^{\beta-1}\prod_{j=0}^{\alpha-1} f(\zeta_\beta^i X, \zeta_\alpha^j Y) \in \mathbb{Z}[\zeta_a, \zeta_\beta, X, Y],$$

where $\zeta_\alpha, \zeta_\beta$ are primitive roots of unity of order α, β, respectively. Since F is invariant with respect to the substitutions $X \to \zeta_\beta X$, $Y \to \zeta_\alpha Y$ we have $F \in \mathbb{Q}(X^\beta, Y^\alpha)$ and

$$F = Q(X^\beta, Y^\alpha), \quad \text{where } Q \in \mathbb{Z}[\Xi, H].$$

Let Q_0 be the leading form of Q. If F_0 is the part of F of the greatest weight, we have

$$F_0(X,Y) = Q_0(X^\beta, Y^\alpha),$$

hence

$$F_0(X,Y) = \prod_{i=0}^{\beta-1}\prod_{j=0}^{\alpha-1} c(\zeta_\beta^i X)^\gamma (\zeta_\alpha^j Y)^\delta = \pm c^{\alpha\beta} X^{\alpha\beta\gamma} Y^{\alpha\beta\delta}.$$

On the other hand

$$\|Q\|_1 = \|F\|_1 \leqslant \big((m+1)(n+1)\|f\|\big)^{\alpha\beta}.$$

Now, let $P \in \mathbb{Z}[X, Y]$ be an irreducible factor of Q such that $f \mid P(X^\beta, Y^\alpha)$, i.e. (33) holds. We may assume without loss of generality that P is primitive. Since $f \mid P(X^\beta, Y^\alpha)$ we have

$$F(X,Y) \mid P(X^\beta, Y^\alpha)^{\alpha\beta}, \quad \text{thus } Q \mid P^{\alpha\beta}.$$

Since P is irreducible we have $Q = c_0 P^\mu$ ($\mu \in \mathbb{N}$) and since P is primitive $c_0 \in \mathbb{Z}$. Hence $Q_0 = c_0 P_0^\mu$, where P_0 is the leading form of P and (35) follows. Moreover

$$\deg P \leqslant \deg Q_0 = \alpha\gamma + \beta\delta,$$
$$\|P\| \leqslant \max_{|\xi|=|\eta|=1} \big|P(\xi,\eta)\big| \leqslant \max_{|\xi|=|\eta|=1} \big|Q(\xi,\eta)\big| \leqslant \|Q\|_1$$

and the lemma follows. □

Lemma 10. *If $F \in \mathbb{Z}[X,Y]$ is isobaric with respect to weights α, β, $(\alpha,\beta) = 1$ and $(F, XY) = 1$, then there exists a form $\overline{F} \in \mathbb{Z}[X,Y]$ such that*

$$F(X,Y) = \overline{F}(X^\beta, Y^\alpha).$$

Proof. If $F \in \mathbb{Z}$ we take $\overline{F} = F$. If $F \notin \mathbb{Z}$, since $(F, XY) = 1$ we have $F = \sum_{j=0}^{k} c_j X^{a_j} Y^{b_j}$, where the vectors $[a_j, b_j] \in \mathbb{N}_0^2$ are distinct, $c_j \in \mathbb{Z}\setminus\{0\}$ and, say, $a_0 \neq 0, b_0 = 0$; $a_k = 0$, $b_k \neq 0$.

Since F is isobaric with respect to weights α, β we have

$$a_j\alpha + b_j\beta = a_0\alpha \quad (0 \leqslant j \leqslant k)$$

and in particular $b_k\beta = a_0\alpha$. Since $(\alpha,\beta) = 1$ we obtain $a_0 \equiv 0 \pmod\beta$ and from the equation above

$$a_j \equiv 0 \pmod\beta,\ b_j \equiv 0 \pmod\alpha \quad (0 \leqslant j \leqslant k).$$

The lemma follows with

$$\overline{F}(X,Y) = \sum_{j=0}^{k} c_j X^{a_j/\beta} Y^{b_j/\alpha}.$$ □

Lemma 11. *If $G_1, G_2 \in \mathbb{Z}[X,Y]\setminus\mathbb{Z}$, G_1, G_2 are homogeneous of degree r and $(G_1, G_2) = 1$ we have for all complex x, y*

$$\max\big\{|G_1(x,y)|, |G_2(x,y)|\big\} \geqslant \big(8r^2\|G_1\|\,\|G_2\|\big)^{-r} \max\big\{|x|^r, |y|^r\big\}. \tag{40}$$

Proof. We have $\big(G_1(X,1), G_2(X,1)\big) = 1$, hence by the result of Mahler [10] for all complex z

$$\begin{aligned}\max\big\{|G_1(z,1)|, |G_2(z,1)|\big\} &\geqslant \big(2\|G_1\|_1\|G_2\|_1\big)^{-r}\\ &\geqslant \big(2(r+1)^2\|G_1\|\,\|G_2\|\big)^{-r}\\ &\geqslant \big(8r^2\|G_1\|\,\|G_2\|\big)^{-r}.\end{aligned}$$

Thus for all complex x and y

$$\max\big\{|G_1(x,y)|, |G_2(x,y)|\big\} \geqslant \big(8r^2\|G_1\|\,\|G_2\|\big)^{-r}|y|^r$$

and by symmetry

$$\max\{|G_1(x,y)|, |G_2(x,y)|\} \geqslant \big(8r^2\|G_1\|\,\|G_2\|\big)^{-r}|x|^r,$$

which gives (40). □

Proof of the theorem. If (C_1) is not satisfied by the variable X, let the term of f containing the highest power of X occurring in f and the highest power of Y besides be $cX^\gamma Y^\delta$, where $\gamma > 0$, $\delta > 0$. Let us give X the weight $\alpha = n - \delta + 1$, Y the weight $\beta = 1$. Since $X^\gamma Y^\delta$ has the weight greater than $X^{\gamma-1}Y^n$, $cX^\gamma Y^\delta$ is the part of the greatest weight and Lemma 9 is applicable. We have

$$p = p_0 = \alpha,\ q = q_0 = 1.$$

For the polynomial P the existence of which is ensured by Lemma 9 we obtain from $f(x,y) = 0$ and (33)

$$P(x, y^\alpha) = 0. \tag{41}$$

Moreover, by Lemma 9

$$\deg P \leqslant \alpha\gamma + \delta \leqslant m(n-\delta+1) + \delta \leqslant mn + 1,$$
$$\|P\| \leqslant \big((m+1)(n+1)\|f\|\big)^\alpha.$$

Since by (35) P satisfies the assumption of Lemma 4 we have from that lemma and (41)

$$\max\{|x|, |y^\alpha|\} \leqslant \big((mn+1)^2(m+1)^\alpha(n+1)^\alpha\|f\|^\alpha\big)^{2(mn-m\delta+m+\delta)^3},$$

which implies the inequality for $|x|$ in (i). In order to prove the inequality for $|y|$ let us observe that for $m = 1$ a stronger inequality, namely

$$|y| < n\big(\|f\| + 1\big)^{2n}$$

follows on reversing the role of x and y and by the argument used by Hilliker and Straus in the proof of their false Theorem 3.3 (the argument is sound only it does not prove what is asserted in the theorem). For $m > 1$ we have

$$|y| \leqslant \Big((mn+1)^{2/(n-\delta+1)}(m+1)(n+1)\|f\|\Big)^{2(mn-m\delta+m+\delta)^3} := \varphi(\delta).$$

Now, an easy calculation shows that in the interval $(1, n-1)$

$$\varphi''(\delta) > \frac{2\varphi'(\delta)}{mn - m\delta + m + \delta},$$

hence $\varphi(\delta)$ has no local maximum in this interval and

$$|y| \leqslant \max_{1\leqslant\delta\leqslant n,\,\delta\in\mathbb{N}} \varphi(\delta) = \max\{\varphi(1), \varphi(\max\{1, n-1\}), \varphi(n)\} = \varphi(1),$$

which completes the proof of (i).

If (C_1) holds, but (C_2) does not, we give X the weight $\alpha = \frac{n}{(m,n)}$, Y the weight $\beta = \frac{m}{(m,n)}$. The part of f of the greatest weight is of the form

$$X^{\varepsilon} Y^{\zeta} f_1(X, Y),$$

where $\varepsilon > 0$, $\zeta > 0$, $\big(f_1(X, Y), XY\big) = 1$ and f_1 is isobaric. By Lemma 10

$$f_1 = \bar{f}_1(X^{\beta}, Y^{\alpha}), \tag{42}$$

where $\bar{f}_1 \in \mathbb{Z}[X, Y]$ is a form of degree k_1, say. By (C_1) $n > \zeta + \deg_Y f_1 > \alpha k_1$, hence

$$k_1 < (m, n). \tag{43}$$

Lemma 8 is applicable with

$$g = X,\ h = Y^{\zeta} f_1(X, Y),\ \gamma = \varepsilon < m,\ \delta = 1.$$

We have

$$p_0 = \alpha,\ q_0 = \beta(\zeta + \alpha k_1) < \beta n,\ p = \frac{\alpha}{(\alpha, \zeta)},\ q = \beta \frac{(\zeta + \alpha k_1)}{(\alpha, \zeta)},\ q(\alpha, \zeta) \geqslant \beta. \tag{44}$$

For the polynomial P the existence of which is ensured by Lemma 8 we obtain from $f(x, y) = 0$ and (33)

$$P\big(x^q, y^{\zeta p} f_1(x, y)^p\big) = 0. \tag{45}$$

Moreover, by (34) and (36)

$$\deg P \leqslant \varrho = \left\lceil \frac{\varepsilon\alpha + q_0}{\alpha\beta} \right\rceil \left\lceil \frac{\alpha q}{\alpha\beta} \right\rceil \alpha\beta \leqslant \frac{2mn}{(m, n)} \min\Big\{ \frac{q}{\beta} + 1, n \Big\}, \tag{46}$$

$$\|P\| \leqslant (\varepsilon\alpha + q_0 + 2\alpha q_0)^{\varrho(9\varepsilon\alpha + 9q_0 + 25\alpha q_0)/4} \|f\|^{2\alpha q m n^2 ((m,n)(\varepsilon\alpha + q_0))^{-1}} \|h^p\|^{\varrho}. \tag{47}$$

However

$$\varepsilon\alpha + q_0 + 2\alpha q_0 \leqslant \frac{2mn}{(m, n)} + \frac{2mn^2}{(m, n)^2} \leqslant \frac{4mn^2}{(m, n)^2}, \tag{48}$$

$$\begin{aligned} \varrho(9\varepsilon\alpha + 9q_0 + 25\alpha q_0) &\leqslant \frac{2mn}{(m, n)} \Big(\frac{q}{\beta} + 1 \Big)(9\varepsilon\alpha + 9q_0 + 25\alpha q_0) \\ &\leqslant \frac{2mn}{(m, n)} q \Big(\frac{9\varepsilon\alpha}{\beta} + 9n + 25\alpha n + \frac{9\varepsilon\alpha}{q} + 9\alpha + 25\alpha^2 \Big) \\ &\leqslant \frac{172mn^3}{(m, n)^2} q. \end{aligned} \tag{49}$$

Since (C_2) does not hold

$$(m, n)(\varepsilon\alpha + q_0) > mn, \quad \frac{2\alpha q m n^2}{(m, n)(\varepsilon\alpha + q_0)} \leqslant \frac{2n^2}{(m, n)} q. \tag{50}$$

By (42) and (43) the number of non-zero coefficients of f_1 does not exceed (m, n), thus

by (44)

$$\|h^p\| = \|f_1^p\| \leqslant (m,n)^{p-1}\|f_1\|^p \leqslant \big((m,n)\|f\|\big)^{\alpha(\alpha,\zeta)^{-1}} \leqslant \big((m,n)\|f\|\big)^{\min\{\alpha,\alpha q/\beta\}}. \tag{51}$$

Now, by (46)

$$\min\Big\{\alpha, \frac{\alpha}{\beta}\,q\Big\}\varrho \leqslant \frac{2mn}{(m,n)} \cdot \frac{2\alpha q}{\beta} = \frac{4n^2}{(m,n)}\,q,$$

hence by (47)–(51)

$$\begin{aligned}\|P\| &\leqslant \Big(\frac{4mn^2}{(m,n)^2}\Big)^{43mn^3(m,n)^{-2}q}(m,n)^{4n^2(m,n)^{-1}q}\|f\|^{6n^2(m,n)^{-1}q}\\ &\leqslant (4mn^2)^{43mn^3(m,n)^{-2}q}\|f\|^{6n^2(m,n)^{-1}q}.\end{aligned}$$

Since by (34) P satisfies the assumptions of Lemma 4 we obtain from that lemma and (45)

$$\begin{aligned}\max\big\{|x^q|, |y^{\zeta p} f_1(x,y)^p|\big\} &\leqslant \big(\varrho^2\|P\|\big)^{2\varrho^3}\\ &\leqslant \Big(\frac{4m^2n^4}{(m,n)^2}\,(4mn^2)^{43mn^3(m,n)^{-2}q}\|f\|^{6n^2(m,n)^{-1}q}\Big)^{16m^3n^6(m,n)^{-3}}.\end{aligned} \tag{52}$$

On the other hand,

$$G_1 = X^{q/\beta} \quad \text{and} \quad G_2 = Y^{\zeta/(\alpha,\zeta)}\bar{f}_1(X,Y)^{\alpha/(\alpha,\zeta)}$$

are homogeneous polynomials of the same degree $q/\beta \leqslant n$ and by (42)

$$x^q = G_1(x^\beta), \quad y^{\zeta p} f_1(x,y)^p = G_2(x^\beta, y^\alpha).$$

Moreover, we have $\|G_1\| = 1$ and by (51)

$$\|G_2\| = \|f_1^p\| \leqslant \big((m,n)\|f\|\big)^{n(m,n)^{-1}}.$$

Hence, by Lemma 11

$$\max\big\{|x^q|, |y^{\zeta p} f_1(x,y)^p|\big\} \geqslant \Big(8n^2\big((m,n)\|f\|\big)^{n(m,n)^{-1}}\Big)^{-q/\beta} \max\big\{|x^\beta|^{q/\beta}, |y^\alpha|^{q/\beta}\big\}.$$

On comparing this with (52) we obtain

$$\max\big\{|x^\beta|, |y^\alpha|\big\} \leqslant \big((4mn^2)^{8mn(m,n)^{-1}}\|f\|\big)^{96m^4n^8(m,n)^{-5}+n(m,n)^{-1}}.$$

By symmetry

$$\max\big\{|x^\beta|, |y^\alpha|\big\} \leqslant \big((4m^2n)^{8mn(m,n)^{-1}}\|f\|\big)^{96m^8n^4(m,n)^{-5}+m(m,n)^{-1}}.$$

Hence

$$\max\big\{|x^\beta|, |y^\alpha|\big\} \leqslant \big((4mnd_0)^{8mn(m,n)^{-1}}\|f\|\big)^{96m^4n^4d_0^4(m,n)^{-5}+d_0(m,n)^{-1}},$$

which implies (ii).

Assume now that f satisfies (C_1) and (C_2), but does not satisfy (C_3). Let X have the weight $\alpha = \frac{n}{(m,n)}$, Y the weight $\beta = \frac{m}{(m,n)}$ and let the part of f of the greatest weight

be g_1g_2, where $g_i \in \mathbb{Z}[X, Y] \setminus \mathbb{Z}$, $(g_1, g_2) = 1$. Since g_1g_2 is isobaric so are g_1, g_2, moreover by (C_1)–(C_2) we have $(g_i, XY) = 1$. Hence by Lemma 10 for suitable polynomials $\bar{g}_i \in \mathbb{Z}[X, Y]$ we have

$$g_i = \bar{g}_i(X^\beta, Y^\alpha) \quad (i = 1, 2), \tag{53}$$

where $\bar{g}_i$ is homogeneous of degree, say, $k_i > 0$. Clearly

$$k_1 + k_2 = (m, n), \tag{54}$$

whence

$$k_1k_2 \leqslant \frac{(m, n)^2}{4}. \tag{55}$$

Lemma 8 is applicable with $g = g_1$, $h = g_2$, $\gamma = \delta = 1$. We have

$$p_0 = k_1 \frac{mn}{(m, n)^2}, \ q_0 = k_2 \frac{mn}{(m, n)^2}, \ p = \frac{k_1}{(k_1, k_2)}, \ q = \frac{k_2}{(k_1, k_2)}.$$

Put

$$r = \frac{k_1k_2}{(k_1, k_2)}.$$

For the polynomial P the existence of which is ensured by Lemma 8 we obtain from $f(x, y) = 0$ and (33)

$$P\big(g_1(x, y)^q, g_2(x, y)^p\big) = 0. \tag{56}$$

Moreover, by (34) and (36)

$$\deg P \leqslant \varrho = \lceil k_1 + k_2 \rceil \left\lceil \frac{k_1k_2}{(k_1, k_2)} \right\rceil \frac{mn}{(m, n)^2} = \frac{mn}{(m, n)} r,$$

$$\|P\| \leqslant (p_0 + q_0 + 2p_0q)^{\varrho(9p_0+9q_0+25p_0q)/4} \|f\|^{\varrho r(m,n)^{-1}} \|g_1^q\|^\varrho \|g_2^p\|^\varrho.$$

However, by (54) and (55)

$$p_0 + q_0 + 2p_0q \leqslant \frac{mn}{(m, n)} + \frac{mn}{2} \leqslant mn,$$

$$9p_0 + 9q_0 + 25p_0q \leqslant \frac{9mn}{(m, n)} + \frac{25mn}{4} \leqslant \frac{43}{4} mn,$$

hence

$$\|P\| \leqslant (mn)^{\frac{43}{16} m^2n^2(m,n)^{-1}r} \|f\|^{mn(m,n)^{-2}r^2} \|g_1^q\|^{mn(m,n)^{-1}r} \|g_2^p\|^{mn(m,n)^{-1}r}.$$

Since P by (35) satisfies the assumptions of Lemma 4 we have by that lemma and (56)

$$\begin{aligned} &\max\big\{|g_1(x, y)^q|, |g_2(x, y)^p|\big\} \\ &\leqslant \Big(\frac{m^2n^2}{(m, n)^2} r^2 (mn)^{\frac{43}{16} \frac{m^2n^2}{(m,n)} r} \|f\|^{\frac{mn}{(m,n)^2} r^2} \|g_1^q\|^{\frac{mn}{(m,n)} r} \|g_2^p\|^{\frac{mn}{(m,n)} r}\Big)^{\frac{2m^3n^3r^3}{(m,n)^3}}. \end{aligned} \tag{57}$$

On the other hand, $\bar{g}_1^q$ and $\bar{g}_2^p$ are homogeneous polynomials of the same degree r. Hence

by (53) and Lemma 11 with $G_1 = \bar{g}_1^q$, $G_2 = \bar{g}_2^p$

$$\max\{|g_1(x,y)^q|, |g_2(x,y)^p|\} = \max\{|\bar{g}_1(x^\beta, y^\alpha)^q|, |\bar{g}_2(x^\beta, y^\alpha)^p|\}$$
$$\geqslant \left(8r^2\|\bar{g}_1^q\|\,\|\bar{g}_2^p\|\right)^{-r} \max\{|x^\beta|^r, |y^\alpha|^r\},$$

which together with (57) gives

$$\max\{|x^\beta|, |y^\alpha|\} \leqslant 8r^2\|\bar{g}_1^q\|\,\|\bar{g}_2^p\|$$
$$\cdot \left(\frac{m^2n^2}{(m,n)^2}\, 3^{2/3}(mn)^{\frac{43}{16}\frac{m^2n^2}{(m,n)}} \|f\|^{\frac{mn}{(m,n)^2}r} \|g_1^q\|^{\frac{mn}{(m,n)}} \|g_2^p\|^{\frac{mn}{(m,n)}}\right)^{\frac{2m^3n^3}{(m,n)^3}r^3}. \tag{58}$$

By (53) we have for every positive integer l

$$\|g_i^l\| = \|\bar{g}_i^l\| = \|\bar{g}_i(X,1)^l\| \leqslant (k_i+1)^{l-1}\|\bar{g}_i(X,1)\|^l \leqslant (m,n)^{l-1}\|\bar{g}_i(X,1)\|^l.$$

Moreover, since $\|\bar{g}_1(X,1)\bar{g}_2(X,1)\| = \|\bar{g}_1\bar{g}_2\| = \|g_1g_2\| \leqslant \|f\|$ we have by a lemma of Gelfond ([3], p. 135)

$$\|\bar{g}_i\| = \|\bar{g}_i(X,1)\| \leqslant e^{k_1+k_2}\|f\| = e^{(m,n)}\|f\|.$$

Hence

$$\|g_1^q\| = \|\bar{g}_1^q\| \leqslant \left((m,n)e^{(m,n)}\|f\|\right)^q (m,n)^{-1}$$
$$\|g_2^p\| = \|\bar{g}_2^p\| \leqslant \left((m,n)e^{(m,n)}\|f\|\right)^p (m,n)^{-1}$$

and (54), (55), (58) give

$$\max\{|x^\beta|, |y^\alpha|\} \leqslant 8\,\frac{(m,n)^2}{16}\left((m,n)e^{(m,n)}\|f\|\right)^{(m,n)}$$
$$\cdot \left(\frac{m^2n^2}{(m,n)^2}\, 3^{2/3}(mn)^{\frac{43}{16}\frac{m^2n^2}{(m,n)}} \|f\|^{\frac{mn}{4}+mn} \left((m,n)^{1-\frac{2}{(m,n)}} e^{(m,n)}\right)^{mn}\right)^{\frac{m^3n^3(m,n)^3}{32}}$$
$$\leqslant \left((mn)^{3mn(m,n)^{-1}}\|f\|\right)^{\frac{5}{128}m^4n^4(m,n)^3+(m,n)}.$$

This implies (iii). □

Proof of the corollary. For $d = 2$ the assumptions of (ii) are never satisfied and

$$\max\{|x|, |y|\} \leqslant \left(4^6\|f\|\right)^{82} < \left(45\|f\|\right)^{250} \quad \text{in the case (iii).}$$

It remains to consider the case (i). If the leading form of f is a monomial we have by Lemma 4

$$\max\{|x|, |y|\} \leqslant \left(4^2\|f\|\right)^{128} < \left(45\|f\|\right)^{250}.$$

If the leading form of f is not a monomial, it is equal either to $aX^2Y + bXY^2$ or to $aXY + bY^2$ or to $aX^2 + bXY$ ($ab \neq 0$). In the first case (C_1) is satisfied neither by X nor by Y, hence

$$\max\{|x|, |y|\} \leqslant \left(45\|f\|\right)^{250}.$$

In the second case $m = 1$, $n = 2$, hence

$$\max\{|x|, |y|\} \leqslant \big(18\|f\|\big)^{108} < \big(45\|f\|\big)^{250}.$$

The third case is symmetric to the second.

For $d > 2$ of the three estimates

$$\begin{aligned}
&\max\{|x|, |y|\} \leqslant \big((d+1)^2(d^2+1)^{2/d}\|f\|\big)^{2d(d^2+1)^3} && \text{in the case (i)},\\
&\max\{|x|, |y|\} \leqslant \big((4d^3)^{8d^2}\|f\|\big)^{96d^4(d-1)^7+1} && \text{in the case (ii)},\\
&\max\{|x|, |y|\} \leqslant \big(d^{6d^2}\|f\|\big)^{\frac{5}{128}d^{11}+d} && \text{in the case (iii)}
\end{aligned}$$

the second is the worst. □

Note added in proof. By using recent results of B. Dwork and A. J. van der Poorten, which improve upon the work of W. Schmidt, P. G. Walsh has substantially sharpened the estimates given on page 93. In most but not in all cases his results are better than our Theorem. We also owe to him two corrections incorporated in the present paper. Walsh's paper is to appear in Acta Arithmetica ([1]).

References

[1] M. Ayad, *Sur le théorème de Runge*. Acta Arith. 58 (1991), 203–209.

[2] E. Bombieri, J. D. Vaaler, *On Siegel's Lemma*. Invent. Math. 73 (1983), 11–32; *Addendum*, ibid. 75 (1984), 377.

[3] A. O. Gelfond, *Transcendental and Algebraic Numbers*. Dover Publ., New York 1960.

[4] D. L. Hilliker, E. G. Straus, *Determination of bounds for the solutions to those binary Diophantine equations that satisfy hypotheses of Runge's theorem*. Trans. Amer. Math. Soc. 280 (1983), 637–657.

[5] J. P. Jouanolou, *Le formalisme du résultant*. Publication de l'Institut de Recherche Mathématique Avancée, Strasbourg; Adv. Math. 90 (1991), 117–263.

[6] E. Landau, *Sur quelques théorèmes de M. Petrovitch relatifs aux zéros des fonctions analytiques*. Bull. Soc. Math. France 33 (1905), 1–11.

[7] F. S. Macaulay, *Some formulae in elimination*. Proc. London Math. Soc. 35 (1903), 3–27.

[8] —, *The Algebraic Theory of Modular Systems*. Cambridge 1916.

[9] K. Mahler, *On some inequalities for polynomials in several variables*. J. London Math. Soc. 37 (1962), 341–344.

[10] —, *An inequality for a pair of polynomials that are relatively prime*. J. Austral. Math. Soc. 4 (1964), 418–420.

[11] E. Maillet, *Sur les équations indéterminées à deux et trois variables qui n'ont qu'un nombre fini de solutions en nombres entiers*. J. Math. Pures Appl. 6 (1900), 261–277.

[12] —, *Sur une categorie d'équations indéterminées n'ayant en nombres entiers qu'un nombre fini de solutions*. Nouv. Ann. Math. 18 (1918), 281–292.

([1]) P. G. Walsh, *A quantitative version of Runge's theorem on Diophantine equations*. Acta Arith. 62 (1992), 157–172. *Corrections*: ibid. 73 (1995), 397–398.

[13] D. W. Masser, *Polynomial bounds for Diophantine equations*. Amer. Math. Monthly 93 (1986), 486–488.

[14] C. Runge, *Über ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen*. J. Reine Angew. Math. 100 (1887), 425–435.

[15] A. Schinzel, *An improvement of Runge's theorem on Diophantine equations*. Comment. Pontificia Acad. Sci. 2 (1969), No. 20; this collection: A7, 36–40.

[16] —, *Errata to the paper "Integer points on conics"*. Comment. Math. Prace Mat. 17 (1973), 305.

[17] —, *Selected Topics on Polynomials*. University of Michigan Press, Ann Arbor 1982.

[18] W. M. Schmidt, *Eisenstein's theorem on power series expansions of algebraic functions*. Acta Arith. 56 (1990), 161–179.

[19] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*. Abh. Preuss. Akad. Wiss. Phys.-math. Kl. Nr. 1 (1929); Ges. Abhandlungen I, Springer, Berlin 1966, 209–266.

[20] Th. Skolem, *Über ganzzahlige Lösungen einer Klasse unbestimmter Gleichungen*. Norsk. Mat. Forenings Skrifter (I) Nr. 10 (1922).

Andrzej Schinzel
Selecta

Originally published in
Functiones et Approximatio. Commentarii Mathematici
XXVIII (2000), 187–194

On sums of three unit fractions with polynomial denominators

To Professor Włodzimierz Staś on his 75th birthday

Abstract. The equation $m/(ax+b) = 1/F_1(x) + 1/F_2(x) + 1/F_3(x)$ is shown to be impossible under some conditions on polynomials $ax+b$ and F_1, F_2, F_3.

A well known conjecture of Erdős and Straus [2] asserts that for every integer $n > 1$ the equation

$$\frac{4}{n} = \frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3}$$

is solvable in positive integers x_1, x_2, x_3. Sierpiński [10] has made an analogous conjecture concerning $5/n$ and the writer has conjectured that for every positive integer m the equation

$$\frac{m}{n} = \frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} \tag{1}$$

is solvable in positive integers x_1, x_2, x_3 for all integers $n > n_0(m)$ (see [10], p. 25). For $m \leqslant 12$ one knows many identities

$$\frac{m}{ax+b} = \frac{1}{F_1(x)} + \frac{1}{F_2(x)} + \frac{1}{F_3(x)}, \tag{2}$$

where a, b are integers, $a > 0$ and F_i are polynomials with integral coefficients and the leading coefficients positive, see [1], [5], [7], [8], [11], Section 28.5. It could seem that a proof of solvability of (2) for a fixed m and $n > n_0(m)$ could be obtained by producing a finite set of identities of the form (2) with a fixed a and b running through the set of all residues $\bmod a$. The theorems given below show that this is impossible.

Theorem 1. *Let a, b be integers, $a > 0$, $(a, b) = 1$. If b is a quadratic residue $\bmod a$, then there are no polynomials F_1, F_2, F_3 in $\mathbb{Z}[x]$ with the leading coefficients positive, satisfying* (2) *with $m \equiv 0 \bmod 4$.*

Theorem 2. *Let m, a, b be integers, $a > 0$, $m > 3b > 0$. There are no polynomials F_1, F_2, F_3 in $\mathbb{Z}[x]$ with the leading coefficients positive, satisfying* (2).

Theorem 1 in the crucial case $m = 4$ has been quoted in the book [4] (earlier inaccurately in [3]), but the proof has not been published before. The theorem is closely related to a

result of Yamamoto [12] and the crucial lemma is a consequence of his work. Possibly, Theorem 2 can be generalized as follows. Let k, m, a, b be positive integers, $m > kb$. There are no polynomials $F_1, F_2, \ldots, F_k$ in $\mathbb{Z}[x]$ with the leading coefficients positive such that

$$\frac{m}{ax+b} = \sum_{i=1}^{k} \frac{1}{F_i(x)}.$$

Note that by a theorem of Sander [9] the above equation has only finitely many solutions in polynomials F_i for fixed a, b, m and k.

Notation. For $\Omega \subset \mathbb{R}[x]$ we shall denote by Ω^+ the set of polynomials in Ω with the leading coefficient positive.

For two polynomials A, B in $\mathbb{Z}[x]$, not both zero, we shall denote by (A, B) the polynomial $D \in \mathbb{Z}[x]^+$ with the greatest possible degree and the greatest possible leading coefficient such that $A/D \in \mathbb{Z}[x]$ and $B/D \in \mathbb{Z}[x]$.

Lemma 1. *If A, B, C, D are in $\mathbb{Z}[x]$, $(A, B) = 1$ and $A/B = C/D$, then $C = HA$, $D = HB$ for an $H \in \mathbb{Z}[x]$. If $(C, D) = 1$ then $H = \pm 1$.*

Proof. This follows from Theorem 44 in [6], the so called Gauss's lemma. □

Lemma 2. *The equations*

$$n^2 = 4(cs - b^*)b^*r - s \tag{3}$$

and

$$n^2 s = 4(cs - b^*)b^*r - 1 \tag{4}$$

have no solutions in positive integers b^*, c, n, r, s.

Proof. This is a consequence of Theorem 2 in [12]: according to this theorem n^2 does not satisfy either of the two congruences

$$n^2 \equiv -s \pmod{4a^*b^*}, \tag{5}$$

$$n^2 s \equiv -1 \pmod{4a^*b^*}, \tag{6}$$

where a^*, b^*, s are positive integers and $s \mid a^* + b^*$, while just such congruences follow from (3) and (4) with $a^* = cs - b^*$. The impossibility of the congruences (5) and (6) is established in [12] by evaluation of the Kronecker symbol $(-s/ab)$; instead one can use the Jacobi symbol as follows.

(3) gives $n^2 = (4b^*cr - 1)s - 4b^{*2}r$, (4) gives $(ns)^2 = (4b^*crs - 1)s - 4b^{*2}rs$, while for $e = 2^\alpha e_0 > 0$, e_0 odd, we have by the reciprocity law ([6], Section 42)

$$\left(\frac{-4b^{*2}e}{4b^*es - 1}\right) = -\left(\frac{e_0}{4b^*es - 1}\right) = -(-1)^{(e_0-1)/2}\left(\frac{4b^*es - 1}{e_0}\right)$$
$$= -(-1)^{(e_0-1)/2}\left(\frac{-1}{e_0}\right) = -1.$$

□

Proof of Theorem 1. It is clearly sufficient to prove the theorem for $m = 4$. Assume that we have (2) with $m = 4$. Thus

$$4F_1(x)F_2(x)F_3(x) = (ax+b)\big(F_2(x)F_3(x) + F_1(x)F_3(x) + F_1(x)F_2(x)\big),$$

hence

$$F_1(-b/a)F_2(-b/a)F_3(-b/a) = 0.$$

If we had $F_i(-b/a) = 0$ for each $i \leqslant 3$, then there would exist polynomials $G_i \in \mathbb{Q}[x]^+$ such that $F_i(x) = (ax+b)G_i(x)$. Since $(a,b) = 1$ it follows from Gauss's lemma that $G_i \in \mathbb{Z}[x]^+$. Choosing an integer k such that $(ak+b)G_1(k)G_2(k)G_3(k) \neq 0$ we should obtain

$$4 = \frac{1}{G_1(k)} + \frac{1}{G_2(k)} + \frac{1}{G_3(k)} \leqslant 3, \quad \text{a contradiction.}$$

Hence, up to a permutation of F_1, F_2, F_3 there are two possibilities

$$F_1(-b/a) = F_2(-b/a) = 0 \neq F_3(-b/a), \tag{7}$$

$$F_1(-b/a) = 0 \neq F_2(-b/a)F_3(-b/a). \tag{8}$$

In the case (7) $F_i(x) = (ax+b)G_i(x)$ $(i = 1, 2)$, $\big(F_3(x),\ ax+b\big) = 1$, where $G_i \in \mathbb{Z}[x]^+$. Let us put

$$D = (G_1, G_2), \quad G_i = DH_i \ (i = 1, 2),$$
$$C = (4DH_1H_2 - H_1 - H_2,\ DH_1H_2) = (H_1 + H_2,\ D),$$
$$D = CR, \quad H_1 + H_2 = CS.$$

H_i, C, R, S are in $\mathbb{Z}[x]^+$ and we have $(H_1, H_2) = 1$, $(RH_1H_2, S) = 1$. By (2) with $m = 4$

$$\frac{ax+b}{F_3} = \frac{4DH_1H_2 - H_1 - H_2}{DH_1H_2} = \frac{4RH_1H_2 - S}{RH_1H_2}.$$

Since $(ax+b, F_3) = 1 = (4RH_1H_2 - S, RH_1H_2)$ and both F_3 and RH_1H_2 are in $\mathbb{Z}[x]^+$, it follows by Lemma 1 that

$$ax + b = 4RH_1H_2 - S = 4(CS - H_2)H_2R - S. \tag{9}$$

Since b is a quadratic residue for a and C, H_2, R, S are in $\mathbb{Z}[x]^+$ there exist integers k and n such that

$$ak + b = n^2 \text{ and } b^* = H_2(k),\ c = C(k),\ r = R(k),\ s = S(k) \text{ are in } \mathbb{Z}^+,$$

which in view of (9) contradicts Lemma 2.

Consider now the case (8). We have here

$$F_1(x) = (ax+b)G_1(x),\ F_i = DH_i \ (i = 2, 3)$$

where $G_1 \in \mathbb{Z}[x]^+$, $D = (F_2, F_3)$, $(H_2, H_3) = 1$ and $(DH_i, ax+b) = 1$ $(i = 2, 3)$,

$H_i \in \mathbb{Z}[x]^+$. Hence, by (2) with $m = 4$

$$\frac{4}{ax+b} = \frac{1}{(ax+b)G_1} + \frac{H_2+H_3}{DH_2H_3}, \tag{10}$$
$$\frac{DH_2H_3}{ax+b} = \frac{G_1(H_2+H_3)}{4G_1-1}.$$

Let us put $C = (D, H_2+H_3)$, $D = CR$, $H_2+H_3 = CS$, so that C, R, S are in $\mathbb{Z}[x]^+$. Since $(DH_2H_3, ax+b) = 1$ we infer from Lemma 1 that $4G_1 - 1 = (ax+b)H_1$, where $H_1 \in \mathbb{Z}[x]^+$. Hence, by (10),

$$\frac{RH_2H_3}{S} = \frac{G_1}{H_1}.$$

Since $(RH_2H_3, S) = 1 = (G_1, H_1)$ and S and H_1 are in $\mathbb{Z}[x]^+$ it follows from Lemma 1 that $H_1 = S$, $G_1 = RH_2H_3$ and

$$(ax+b)S = 4G_1 - 1 = 4RH_2H_3 - 1 = 4(CS - H_2)H_2R - 1. \tag{11}$$

Since b is a quadratic residue $\bmod a$ and C, H_2, R, S are in $\mathbb{Z}[x]^+$ there exist integers k and n such that

$$ak + b = n^2 \text{ and } b^* = H_2(k),\ c = C(k),\ r = R(k),\ s = S(k) \text{ are in } \mathbb{Z}^+,$$

which in view of (11) contradicts Lemma 2. □

Proof of Theorem 2. If $F_i(0) \neq 0$ for all i it follows from (2) on substituting $x = 0$ that

$$\frac{m}{b} = \sum_{i=1}^{3} \frac{1}{F_i(0)} \leqslant 3,$$

contrary to the assumption $m > 3b$.

If $F_i(0) \neq 0$ for all but one i, it follows from (2) on taking the limit for $x \to 0$

$$\frac{m}{b} = \pm\infty,$$

a contradiction.

If $F_i(0) = 0$ for all i, it follows $F_i(x) = xG_i(x)$, $G_i \in \mathbb{Z}[x]^+$ and by (2)

$$\frac{mx}{ax+b} = \sum_{i=1}^{3} \frac{1}{G_i(x)}.$$

When $x \to \infty$ the terms on the left hand side are less than the limit m/a, the terms on the right hand side are greater than or equal to the limit, which contradicts the equality.

Thus $F_i(0) = 0$ for exactly two $i \leqslant 3$ and we may assume without loss of generality that

$$F_i(0) = 0\ (i = 1, 2), \quad F_3(0) \neq 0.$$

Arguing as in the proof of Theorem 1 we infer that $F_i(-b/a) = 0$ for at least one i. Hence

up to a permutation of F_1, F_2 there are the following possibilities:

$$F_i(-b/a) = 0 \ (i = 1, 2, 3); \tag{12}$$

$$F_i(-b/a) = 0 \ (i = 1, 2), \quad F_3(-b/a) \neq 0; \tag{13}$$

$$F_i(-b/a) = 0 \ (i = 1, 3), \quad F_2(-b/a) \neq 0; \tag{14}$$

$$F_i(-b/a) \neq 0 \ (i = 1, 2), \quad F_3(-b/a) = 0; \tag{15}$$

$$F_i(-b/a) \neq 0 \ (i = 1, 3), \quad F_2(-b/a) = 0. \tag{16}$$

We shall consider these cases successively.

Case (12). Here $F_i(x) = (ax+b)G_i(x)$, $G_i \in \mathbb{Q}[x]^+$ $(i = 1, 2, 3)$ and by Gauss's lemma $(a, b)G_i \in \mathbb{Z}[x]^+$. Taking an integer k such that $G_i(k) \neq 0$ we obtain from (2)

$$m = \sum_{i=1}^{3} \frac{1}{G_i(k)} \leqslant 3(a, b) \leqslant 3b,$$

contrary to the assumption.

Case (13). Here $F_i(x) = x(ax + b)G_i(x)$, $G_i \in \mathbb{Q}[x]^+$ $(i = 1, 2)$

$$m = \frac{1}{xG_1(x)} + \frac{1}{xG_2(x)} + \frac{ax + b}{F_3}$$

and taking the limit for $x \to \infty$ we infer that $F_3 = cx + d$, where $c = a/m$. Hence

$$0 = \frac{1}{xG_1} + \frac{1}{xG_2} + \frac{b - md}{cx + d}\,.$$

For x large enough the first two terms are positive, hence $b - md < 0$ and $d > 0$.

Without loss of generality $G_2(-d/c) = 0$, hence $G_2 = (cx + d)H_2(x)$, $H_2 \in \mathbb{Q}[x]^+$,

$$0 = \lim_{x\to\infty} \frac{cx + d}{xG_1(x)} + b - md,$$

thus $G_1(x) = \frac{c}{md-b}$ and

$$0 = \frac{md - b}{cx} + \frac{1}{x(cx + d)H_2} + \frac{b - md}{cx + d} = \frac{(md - b)d}{x(cx + d)} + \frac{1}{x(cx + d)H_2}\,.$$

This is impossible, since for x large enough both terms on the right hand side are positive.

Case (14). Here $F_1 = x(ax + b)G_1$, $F_2 = xG_2$, $F_3 = (ax + b)G_3$, where $G_i \in \mathbb{Q}[x]^+$ $(i = 1, 2, 3)$ and

$$m = \frac{1}{xG_1} + \frac{ax + b}{xG_2} + \frac{1}{G_3}\,.$$

The first and the second term on the right hand side are greater than their limits for $x \to \infty$, the third term is greater or equal, while the left hand side is constant: this gives a contradiction.

Case (15). Here $F_i = xG_i$ $(i = 1, 2)$, $F_3 = (ax+b)G_3$, where $G_i \in \mathbb{Z}[x]^+$, $G_i(-b/a) \neq 0$ $(i = 1, 2)$, $G_3 \in \mathbb{Q}[x]^+$ and

$$\frac{mx}{ax+b} = \frac{1}{G_1(x)} + \frac{1}{G_2(x)} + \frac{x}{(ax+b)G_3(x)}\,.$$

If $G_3 \notin \mathbb{Q}^+$ all three terms on the right hand side are greater than or equal to their limits for $x \to \infty$, while the left hand side is less than the limit, a contradiction. Hence $G_3 = g \in \mathbb{Q}^+$ and

$$\frac{(m-1/g)x}{ax+b} = \frac{1}{G_1} + \frac{1}{G_2}\,,$$

which contradicts $G_1G_2(-b/a) \neq 0$.

Case (16). Here $F_1 = xG_1$, $F_2 = x(ax+b)G_2$, where $G_1 \in \mathbb{Z}[x]^+$, $G_2 \in \mathbb{Q}[x]^+$ and

$$\frac{mx}{ax+b} = \frac{1}{G_1} + \frac{1}{(ax+b)G_2} + \frac{x}{F_3}. \tag{17}$$

If $\deg F_3 = 0$ we take the limit for $x \to \infty$ and obtain $m/a = \infty$, a contradiction.

If $\deg F_3 > 1$, when $x \to \infty$ the left hand side of (17) is less than its limit, while all three terms on the right hand side are greater than or equal to their limits, which gives a contradiction. Thus

$$\deg F_3 = 1,\ F_3 = cx + d,\ \text{where } c \in \mathbb{Z}^+,\ d/c \neq b/a. \tag{18}$$

We consider four subcases:

(i) $\deg G_1 > 1$;

(ii) $\deg G_1 = 1,\ G_1/F_3 \notin \mathbb{Q}$;

(iii) $\deg G_1 = 1,\ G_1/F_3 \in \mathbb{Q}$;

(iv) $\deg G_1 = 0$.

Subcase (i). Taking the limit for $x \to \infty$ we infer from (17) and (18) that $a = cm$ and

$$\begin{aligned} &\frac{mx}{cmx+b} = \frac{1}{G_1} + \frac{1}{(cmx+b)G_2} + \frac{x}{cx+d}\,; \\ &\frac{x(md-b)}{cx+d} = \frac{cmx+b}{G_1} + \frac{1}{G_2}\,, \end{aligned} \tag{19}$$

hence $md - b > 0$, $d > 0$. When $x \to \infty$ the left hand side of (18) is less than its limit, while both terms on the right hand side are greater than or equal to their limits, which gives a contradiction.

Subcase (ii). As in the subcase (i) we have $md - b > 0$, $d > 0$. Let $G_1 = ex + f$, $e > 0$, $f/e \neq b/a, d/c$. It follows from (19) that

$$G_2 = g^{-1}(cx+d)(ex+f),\ g \in \mathbb{Q}^+$$

and substituting $x = 0$ we obtain

$$0 = \frac{b}{f} + \frac{g}{df}\,; \quad g = -bd < 0,$$

a contradiction.

Subcase (iii). Let $G_1 = e^{-1}(cx+d)$, $e \in \mathbb{Q}^+$. We obtain from (17) and (18)

$$\frac{mx}{ax+b} = \frac{1}{(ax+b)G_2} + \frac{x+e}{cx+d},$$

hence either $G_2 = f^{-1}(cx+d)$, $f \in \mathbb{Q}^+$ and substituting $x = 0$

$$0 = \frac{f}{bd} + \frac{e}{d}; \quad f = -be < 0,$$

a contradiction, or $e = d/c$, $G_2 = -c/b$, a contradiction again.

Subcase (iv). Let $G_1 = g$. It follows from (17) and (18) that $G_2 = e^{-1}(cx+d)$, $e \in \mathbb{Q}^+$,

$$\frac{mx}{ax+b} = \frac{1}{g} + \frac{e}{(ax+b)(cx+d)} + \frac{x}{cx+d}$$

and multiplying both sides by $g(ax+b)(cx+d)$

$$(cgm - ac - ag)x^2 + (dgm - bg - ad - bc)x - bd - eg = 0.$$

Hence

$$cgm - ac - ag = 0, \tag{20}$$

$$dgm - bg - ad - bc = 0, \tag{21}$$

$$bd + eg = 0, \tag{22}$$

which is impossible, since (20) gives $gm - a = ag/c > 0$, and (21) gives $d = (bg + bc)/(gm - a) > 0$, contrary to (22). □

References

[1] A. Aigner, *Brüche als Summe von Stammbrüchen*. J. Reine Angew. Math. 214/215 (1964), 174–179.

[2] P. Erdős, *On the integer solutions of the equation* $1/x_1 + 1/x_2 + \ldots + 1/x_n = a/b$. Mat. Lapok 1 (1950), 192–210 (Hungarian).

[3] R. K. Guy, *Some unsolved problems*. In: Computers in Number Theory (ed. A. O. L. Atkin and B. J. Birch), Academic Press, London 1971, 415–422.

[4] —, *Unsolved Problems in Number Theory*, second edition. Springer, New York 1994.

[5] E. Kiss, *Remarques relatives à la représentation des fractions subunitaires en somme des fractions ayant le numérateur égal à l'unité* (Romanian). Acad. R. P. Romine Fil. Cluj Stud. Cerc. Mat. 11 (1960), 319–323.

[6] T. Nagell, *Introduction to Number Theory*, second edition. Chelsea, New York 1964.

[7] R. Obláth, *Sur l'équation diophantienne* $4/n = 1/x_1 + 1/x_2 + 1/x_3$. Mathesis 59 (1950), 308–316.

[8] G. Palamà, *Su di una congettura di Sierpiński relativa alla possibilità in numeri naturali della* $5/n = 1/x_1 + 1/x_2 + 1/x_3$. Boll. Un. Mat. Ital. (3) 13 (1958), 65–72.

[9] J. W. Sander, *Egyptian fractions and the Erdős–Straus conjecture*. Nieuw Arch. Wisk. (4) 15 (1997), 43–50.

[10] W. Sierpiński, *Sur les décompositions de nombres rationnels en fractions primaires*. Mathesis 65 (1956), 16–32; see also Oeuvres choisies, T. I, Varsovie 1974, 169–184.

[11] B. M. Stewart, *Theory of Numbers*, second edition. Macmillan, New York 1964.

[12] K. Yamamoto, *On the Diophantine equation* $4/n = 1/x + 1/y + 1/z$. Mém. Fac. Sci. Kyushu Univ. Ser. A 19 (1965), 37–47.

Originally published in
Bulletin of the Polish Academy of Sciences
Mathematics 52 (2004), 223–226

On equations $y^2 = x^n + k$ in a finite field

with M. Skałba (*Warszawa*)

Summary. Solutions of the equations $y^2 = x^n + k$ ($n = 3, 4$) in a finite field are given almost explicitly in terms of k.

Let F be a finite field. It follows easily from Hasse's theorem on the number of points on an elliptic curve over F that each of the curves

$$y^2 = x^n + k \quad (n = 3, 4;\ k \in F) \tag{1}$$

has a point (x, y) in F^2, except for $n = 4$, $F = \mathbb{F}_5$, $k = 2$. The aim of the present paper is to indicate such a point almost explicitly in terms of k. Note that if $\operatorname{char} K = 2$, then (1) is satisfied by $y = (x^n + k)^{\operatorname{card} F/2}$, and if $\operatorname{char} K = 3$, $n = 3$ then (1) is satisfied by $x = (y^2 - k)^{\operatorname{card} F/3}$. We shall prove

Theorem 1. *Let* $\operatorname{char} F > 3$ *and* $k \in F$. *Set*

$$y_1 = \begin{cases} 12 & \text{if } k + 72 = 0, \\ \frac{k}{12} + 3 & \text{if } k^2 - 72k + 72^2 = 0, \end{cases}$$

and if $k^3 + 72^3 \neq 0$, *set*

$$\begin{aligned}
y_1 &= -2^{-9}3^{-5}k^3 + 2^{-6}3^{-3}k^2 - 2^{-3}k - 3, \\
y_2 &= 2^{-8}3^{-6}k^3 - 2^{-5}3^{-3}k^2 + 2^{-2}3^{-1}k + 2, \\
y_3 &= \frac{k^6 - 288k^5 + 46656k^4 - 3732480k^3}{2^8 3^5 (k + 72)^3} \\
&\quad + \frac{134369280k^2 - 11609505792k + 139314069504}{2^8 3^5 (k + 72)^3}, \\
y_4 &= \frac{k^9 - 504k^8 + 124416k^7 - 17915904k^6 + 1558683648k^5}{2^{10} 3^5 (k^2 - 72k + 72^2)^3} \\
&\quad + \frac{-69657034752k^4 + 5851190919168k^3}{2^{10} 3^5 (k^2 - 72k + 72^2)^3} \\
&\quad + \frac{20061226008576k^2 + 2166612408926208k + 51998697814228992}{2^{10} 3^5 (k^2 - 72k + 72^2)^3}.
\end{aligned}$$

Then for at least one $j \leqslant 4$ *the equation* $y_j^2 = x^3 + k$ *is solvable in* $x \in F$.

Theorem 2. *Let* char $F \neq 2$ *and* $k \in F^*$. *If* $k - 2 = 0$ *and* char $F \neq 5$, *set*

$$u_1 = \frac{-5}{8}, \quad u_2 = 2, \quad u_3 = 5;$$

if char $F = 5$ *and* $\alpha \in F \setminus \mathbb{F}_5$, *set*

$$u_1 = \frac{4\alpha}{1+\alpha^2}, \quad u_2 = \frac{2-2\alpha^2}{1+\alpha^2}, \quad u_3 = \frac{4\alpha(2-2\alpha^2)}{(1+\alpha^2)^2};$$

if $k^2 - 4k - 4 = 0$ *and* $k^3 - 8 \neq 0$, *set*

$$u_1 = \frac{-k^6 - 16k^3 + 64}{16k^4}, \quad u_2 = \frac{1}{k}, \quad u_3 = \frac{-k^6 - 16k^3 + 64}{k(k^3-8)^2};$$

if $k^2 - 4k - 4 = k^3 - 8 = 0$, *set*

$$u_1 = u_2 = u_3 = -1;$$

and if $(k-2)(k^2 - 4k - 4) \neq 0$, *set*

$$u_1 = \frac{k^2 - 4k - 4}{16}, \quad u_2 = \frac{k}{4}, \quad u_3 = \frac{k(k^2-4k-4)}{4(k-2)^2}.$$

Then $u_j \in F^*$ $(1 \leqslant j \leqslant 3)$ *and for at least one* $j \leqslant 3$ *the equation*

$$\left(\frac{4u_j^2 + k}{4u_j}\right)^2 = x^4 + k$$

is solvable in $x \in F$.

The proof of Theorem 1 is based on the following

Lemma 1. *Let* A, B, C, D *be in* F *and*

$$z_1 = A, \quad z_2 = B, \quad z_3 = ABC^3, \quad z_4 = AB^2D^3.$$

Then for at least one $j \leqslant 4$ *the equation* $x^3 = z_j$ *is solvable in* $x \in F$.

Proof. If $ABCD = 0$ the assertion is clear and if $ABCD \neq 0$ it follows from the fact that the multiplicative group of F is cyclic and for all a, b in $\mathbb{Z}$ at least one of the numbers $a, b, a+b, a+2b$ is divisible by 3. □

Proof of Theorem 1. If $k + 72 = 0$ or $k^2 - 72k + 72^2 = 0$ we have $y_1^2 - k = 6^3$ or $(-3)^3$, respectively. If $k^3 + 72^3 \neq 0$ we put in Lemma 1

$$A = y_1^2 - k, \quad B = y_2^2 - k, \quad C = 2^6 3^4 (k+72)^{-2}, \quad D = 2^{10} 3^8 (k^2 - 72k + 72^2)$$

and verify that

$$y_3 = \frac{y_1 y_2 + k}{y_1 + y_2}, \qquad y_3^2 - k = ABC^3,$$

$$y_4 = \frac{y_1 y_2^2 + k y_1 + 2k y_2}{y_2^2 + 2y_1 y_2 + k}, \qquad y_4^2 - k = AB^2D^3.$$ □

The proof of Theorem 2 is based on the following

Lemma 2. *Let u_j be as in Theorem* 2. *Then $u_j \in F^*$ and*

$$\sqrt{4u_j^3 - ku_j} \in F \quad \text{for at least one } j \leqslant 3. \tag{2}$$

Proof. If $k-2=0$ and char $K \neq 5$, then $u_1u_2u_3 \neq 0$ and (2) holds because

$$(4u_1^3 - ku_1)(4u_2^3 - ku_2) = (4u_3^3 - ku_3)(1/8)^2.$$

If $k-2=0$ and char $K = 5$, $\alpha \in F \setminus \mathbb{F}_5$, then clearly $u_1u_2u_3 \neq 0$ and (2) holds as

$$(4u_1^3 - ku_1)(4u_2^3 - ku_2) = (4u_3^3 - ku_3)2^2.$$

If $k^2-4k-4=0$ and $k^3-8 \neq 0$, then $u_1u_2u_3 \neq 0$, since otherwise $k^6+16k^3-64=0$, while char $F \neq 2$ implies

$$(k^2-4k-4, k^6+16k^3-64) = 1.$$

Also (2) holds in view of the identity

$$(4u_1^3 - ku_1)(4u_2^3 - ku_2) = (4u_3^3 - ku_3)\left(\frac{k^3-8}{2k^2}\right)^6 (1/4)^2.$$

If $k^2-4k-4 = k^3-8 = 0$, then char $F = 7$, $k = 1$, $u_1u_2u_3 \neq 0$ and

$$4u_1^3 - ku_1 = 2^2.$$

If $(k-2)(k^2-4k-4) \neq 0$, then clearly $u_1u_2u_3 \neq 0$ and (2) holds since

$$(4u_1^3 - ku_1)(4u_2^3 - ku_2) = (4u_3^3 - ku_3)\left(\frac{k-2}{4}\right)^6 2^2. \qquad \square$$

Proof of Theorem 2. We have the identity

$$\left(\frac{4u_j^2+k}{4u_j}\right)^2 - k = \left(\frac{4u_j^2-k}{4u_j}\right)^2$$

and by Lemma 2 for at least one $j \leqslant 3$ we have $\sqrt{(4u_j^2-k)/4u_j} \in F$. $\square$

The following problem related to the proof of Lemma 2 remains open.

Problem. *Let $f \in \mathbb{Z}[x]$ have the leading coefficient positive and assume that the congruence $f(x) \equiv y^2 \pmod m$ is solvable for every natural number m. Do there exist an odd integer $k > 0$ and integers $x_1, \ldots, x_k$ such that $\prod_{i=1}^{k} f(x_i)$ is a square?*

Part B

Continued fractions

Commentary on B: Continued fractions

by Eugène Dubois

For a polynomial, $f(n)$, assuming only integral values for integers n, we denote by $[b_0, b_1, \ldots, b_{h-1}, \overline{b_h, \ldots, b_{h+k-1}}]$ the expansion of $\sqrt{f(n)}$ into continued fraction and by $\mathrm{lp}\big(\sqrt{f(n)}\big)$ the minimal period length k.

If f has odd degree or if $f(n) = a_0x^{2p} + \ldots + a_{2p}$ where the a_i are rational, a_0 not a square, A. Schinzel proves, in **B1**, that $\lim\limits_{n\to\infty} \mathrm{lp}\big(\sqrt{f(n)}\big) = +\infty$. When $f(n) = a^2n^2 + bn + c$, he finds a set E such that

$$\lim_{n\in CE, n\to\infty} \mathrm{lp}\big(\sqrt{f(n)}\big) = \infty \quad \text{and} \quad \overline{\lim_{n\in E, n\to\infty}} \mathrm{lp}\big(\sqrt{f(n)}\big) < \infty, \tag{1}$$

where CE is the complementary set to E.

This problem grew out of a result of H. Schmidt [10] in the case $f(n) = n^2 + h$. Later, explicit lower bounds for $\mathrm{lp}\big(\sqrt{f(n)}\big)$, $n \in E$, were given by S. Louboutin [8] and by A. Farhane [4].

For other polynomials $a^2n^{2p} + \ldots + a_0$ $(a \neq 0)$, A. Schinzel in **B2** reduces the problem to the existence of an expansion $\sqrt{f(n)} = [u_0(n), \overline{u_1(n), \ldots, u_K(n)}]$ where $u_i(x)$ are polynomials with rational coefficients. If such an expansion exists then A. Schinzel finds a set E for which 1 holds. Later, E. Dubois and R. Paysant-Le Roux using "formal continued fraction" gave a method to get explicit lower bound of $\mathrm{lp}\big(\sqrt{f(n)}\big)$.

The conjecture about points of finite order on elliptic curves ascribed in **B2** to Nagell has been earlier in an equivalent form proposed by B. Levi [7] and it has been finally proved by B. Mazur [9], see also J. H. Davenport [2].

In **B3**, A. Schinzel proves a conjecture of P. Chowla and S. Chowla [1] and generalises another one.

If D is a non-square positive integer, we denote by $[b_0, \overline{b_1, \ldots, b_k}]$ the continued fraction expansion of $\sqrt{D}$ with k minimal and we consider the alternating sum of the partial quotients $\Sigma_D = b_k - b_{k-1} + \ldots + (-1)^{k-1}b_1$. If k is even, $3 \nmid D$, A. Schinzel proves that $\Sigma_D \equiv 0 \bmod 3$. For the congruence mod 2, the conjecture was that $(-1)^{\Sigma_{pq}} = \left(\frac{p}{q}\right)$ where p, q are prime, $p \equiv 3 \bmod 4$ and $q \equiv 5 \bmod 8$. A. Schinzel proves a more general result: namely that $\Sigma_D \equiv v \bmod 2$ where u, v is the least non trivial solution of $u^2 - Dv^2 = 1$.

From this he get $\Sigma_{p^\alpha} \equiv 1 \bmod 2$ where α is odd and $(-1)^{\Sigma_{p^\alpha q^\beta}} = \left(\frac{p}{q}\right)$ where α, β are odd.

The results of **B3** have been generalized by H. Lang [6] and C. Friesen [5].

References

[1] P. Chowla, S. Chowla, *Problems on periodic simple continued fractions*. Proc. Nat. Acad. Sci. U.S.A. 69 (1972), 3745.

[2] J. H. Davenport, *On the Integration of Algebraic Functions*. Lecture Notes in Comput. Sci. 102, Springer, Berlin 1981.

[3] E. Dubois, R. Paysant-Le Roux, *Sur la longueur du développement en fraction continue de* $\sqrt{f(n)}$. In: Journées Arithmétiques (Luminy, 1989), Astérisque 198–200 (1991), 107–119.

[4] A. Farhane, *Minoration de la période du développement de* $\sqrt{a^2n^2 + bn + c}$ *en fraction continue*. Acta Arith. 67 (1994), 63–67.

[5] C. Friesen, *Über einfache periodische Kettenbrüche und Vermutungen von P. Chowla und S. Chowla*. Acta Arith. 59 (1991), 365–379.

[6] H. Lang, *Legendre symbols and continued fractions*. Acta Arith. 28 (1975/76), 419–428.

[7] B. Levi, *Sull' equazione indeterminata del* 3^e *ordine*. Atti IV Congresso Internaz. Mat. Rome 2 (1909), 173–177.

[8] S. Louboutin, *Une version effective d'un théorème de A. Schinzel sur les longueurs des périodes de certains développements en fractions continues*. C. R. Acad. Sci. Paris Sér. I Math. 308 (1989), 511–513.

[9] B. Mazur, *Rational points on modular curves*. In: Modular functions of one variable V, Lecture Notes in Math. 601, Springer, Berlin 1977, 107–148.

[10] H. Schmidt, *Zur Approximation und Kettenbruchentwicklung quadratischer Zahlen*. Math. Z. 52 (1950), 168–192.

Originally published in
Acta Arithmetica VI (1961), 393–413

On some problems of the arithmetical theory of continued fractions

1.

For a given quadratic surd ξ let us denote by

$$[b_0, b_1, \ldots, b_{h-1}, \overline{b_h, b_{h+1}, \ldots, b_{h+k-1}}]$$

its expansion into an arithmetical continued fraction, by $\operatorname{lp}\xi$—the length of the shortest period of this expansion, by $\operatorname{lap}\xi$—the number of terms before the period. For some polynomials $f(n)$ assuming only integral values (so-called *integer-valued* polynomials) there are known formulae for the expansion of $\sqrt{f(n)}$ into continued fractions such that the partial quotients are also integer-valued polynomials and $\operatorname{lp}\sqrt{f(n)}$ is independent of n (cf. [3], [5]). Recently H. Schmidt has proved ([3], Satz 10) that

If h is an integer $\neq 0, \pm 1, \pm 2, \pm 4$, then for each n_0 the set of all integers $\geqslant n_0$ cannot be decomposed into a finite number of classes, so that the relation

$$\sqrt{n^2+h} = [p_0(n), \overline{p_1(n), \ldots, p_k(n)}], \quad n \geqslant n_0, \quad n \in K,$$

holds for each class K (p_ν are polynomials assuming integral values for $n \in K$, k depends only upon K).

This theorem suggests the following problem P.

P. *Decide for a given integer-valued polynomial $f(n)$ whether*

$$\overline{\lim}\, \operatorname{lp}\sqrt{f(n)} < \infty.$$

An investigation of this problem is the main aim of the present paper.

In §2 we investigate the relation between $\operatorname{lp}\xi$ and $\operatorname{lp}\big((p\xi+r)/(q\xi+s)\big)$, where p, q, r, s are integers.

In §3 we give a negative solution of the problem P for polynomials of odd degree and for a large class of polynomials of even degree.

In §4 after more accurate study of the behaviour of the function $\operatorname{lp}\sqrt{n^2+h}$ and on the base of the results of §2 we give a complete solution of the problem P for polynomials of the second degree.

We shall use the following notation: ξ, ξ', ξ'' will denote either rational numbers or quadratic surds; in the latter case η, η', η'' will be corresponding conjugate numbers. Putting

$$\xi = [b_0, b_1, b_2, \dots]$$

we shall assume simultaneously

$$\begin{aligned} A_{-1} &= 1, \quad A_0 = b_0, \quad A_\nu = b_\nu A_{\nu-1} + A_{\nu-2}, \\ B_{-1} &= 0, \quad B_0 = 1, \quad B_\nu = b_\nu B_{\nu-1} + B_{\nu-2}, \end{aligned} \tag{1}$$

(whence $[b_0, b_1, \dots, b_n] = A_n/B_n$) and

$$\xi_\nu = [b_\nu, b_{\nu+1}, b_{\nu+2}, \dots]$$

(cf. [2], p. 24 and 34). For rational ξ we put $\operatorname{lp}\xi = 0$ and

$$\operatorname{lap}\xi = \begin{cases} 1 & \text{if} \quad \xi \text{ is an integer,} \\ h & \text{if} \quad \xi = [b_0, b_1, \dots, b_{h-1}], \ b_{h-1} > 1 \end{cases}$$

(the so-called *normal* expansion).

2.

Lemma 1. *Let $b > 1$, h and s be positive integers.*

If

$$\xi = [b_0, b_1, \dots, b_{h-1}] \tag{2'}$$

or

$$\xi = [b_0, b_1, \dots, b_{h-1}, \overline{b_h, b_{h+1}, \dots, b_{h+k-1}}], \tag{2''}$$

where

$$b_i < b \quad (1 \leqslant i \leqslant h-1), \tag{3}$$

then

$$i < B_i \leqslant b^i \quad (0 \leqslant i \leqslant h-1). \tag{4}$$

Moreover, if for some integers p and r

$$\xi' = (p\xi + r)/s, \tag{5}$$

then

$$\operatorname{lap}\xi' < 2sb^h. \tag{6}$$

Proof. Formula (4) follows by easy induction from (1) and (2). Hence for rational ξ we immediately get the remaining part of the lemma.

In fact, putting

$$\xi' = [b'_0, b'_1, \dots, b'_{h'-1}] = \frac{A'_{h'-1}}{B'_{h'-1}},$$

we have in view of (5)

$$\frac{A'_{h'-1}}{B'_{h'-1}} = \frac{pA_{h-1} + rB_{h-1}}{sB_{h-1}};$$

then $\operatorname{lap}\xi' = h' \leqslant B'_{h'-1} \leqslant sB_{h-1} \leqslant sb^{h-1} < 2sb^h$.

In the case $p = 0$ we have likewise

$$\frac{A'_{h'-1}}{B'_{h'-1}} = \frac{r}{s}, \quad \text{whence} \quad \operatorname{lap}\xi' = h' \leqslant B'_{h'-1} \leqslant s < 2sb^h.$$

One can therefore assume that ξ is irrational and $p \neq 0$. It follows from $(2'')$ that

$$\xi = [b_0, b_1, \ldots, b_{h-1}, \xi_h];$$

ξ_h, which has a pure period in its expansion, is by a well-known theorem, a reduced surd, i.e.

$$\xi_h > 1, \quad 0 > \eta_h > -1. \tag{7}$$

On the basis of well-known formulae (cf. [2], §13, (7)) we have:

$$\xi = \frac{A_{h-1}}{B_{h-1}} + \frac{(-1)^{h-1}}{B_{h-1}(B_{h-1}\xi_h + B_{h-2})},$$

$$\eta = \frac{A_{h-1}}{B_{h-1}} + \frac{(-1)^{h-1}}{B_{h-1}(B_{h-1}\eta_h + B_{h-2})},$$

whence

$$|\xi - \eta| = \frac{|1 - \eta_h/\xi_h|}{|B_{h-1} + B_{h-2}/\xi_h| \cdot |B_{h-1}\eta_h + B_{h-2}|}.$$

Since, in view of (7),

$$0 < -\eta_h/\xi_h, \quad 0 < B_{h-1} + B_{h-2}/\xi_h < B_{h-1} + B_{h-2} \leqslant B_h,$$
$$-B_{h-1} < B_{h-1}\eta_h + B_{h-2} < B_{h-2} < B_{h-1},$$

we get by (4)

$$|\xi - \eta| > 1/B_{h-1}B_h > 1/b^{2h-1}$$

and by (5)

$$|\xi' - \eta'| = \frac{|p|}{s}|\xi - \eta| > \frac{1}{sb^{2h-1}}.$$

If $\xi' > \eta'$, we assume $h' = 2sb^h - 2$. Therefore, in view of (4),

$$B'_{h'-1}B'_{h'-2} \geqslant h'(h'-1) = (2sb^h - 2)(2sb^h - 3) \geqslant sb^{2h-1} > \frac{1}{|\xi' - \eta'|}. \tag{8}$$

We shall prove that $\xi'_{h'}$ is a reduced surd. It follows from the formula

$$\eta' = \frac{A'_{h'-1}}{B'_{h'-1}} + \frac{(-1)^{h'-1}}{B'_{h'-1}(B'_{h'-1}\eta'_{h'} + B'_{h'-2})}$$

that

$$B'_{h'-1}(B'_{h'-1}\eta'_{h'} + B'_{h'-2}) = \frac{(-1)^{h'}}{A'_{h'-1}/B'_{h'-1} - \eta'}\,.$$

Since $h' = 2sb^h - 2$ is even, we have

$$A'_{h'-1}/B'_{h'-1} - \eta' > \xi' - \eta' > 0.$$

The last two formulae together give

$$\frac{1}{\xi' - \eta'} > (B'_{h'-1}\eta'_{h'} + B'_{h'-2})B'_{h'-1} > 0.$$

We then get, on the one hand,

$$0 < B'_{h'-1}\eta'_{h'} + B'_{h'-2}, \quad \text{whence} \quad \eta'_{h'} > -B'_{h'-2}/B'_{h'-1} > -1;$$

on the other hand, in view of (8),

$$B'_{h'-1}B'_{h'-2} > B'_{h'-1}(B'_{h'-1}\eta'_{h'} + B'_{h'-2}), \quad \text{whence} \quad \eta'_{h'} < 0.$$

Therefore $0 > \eta'_{h'} > -1$ and since $\xi'_{h'} > 1$, the surd $\xi'_{h'}$ is reduced (for $h' = 2sb^h - 2$).

In the case $\eta' > \xi'$ we prove similarly that the surd $\xi'_{h'}$ is reduced for $h' = 2sb^h - 1$. Since a reduced surd gives in its expansion a pure period, we have in both cases

$$\operatorname{lap}\xi' = h' < 2sb^h. \qquad \square$$

Remark. Inequalities (4) and (6) can be greatly improved; however, it is without any importance for the applications intended.

In the following we shall profit by a theorem used in the investigation of Hurwitz's continued fractions and due to A. Hurwitz and A. Châtelet. We quote this theorem according to Perron's monograph ([2], Satz 4.1) with slight changes in his notation to avoid confusion with ours.

H. *Let* $[b_0, b_1, b_2, \dots]$ *be the arithmetical continued fraction for a quadratic surd* ξ_0, A_λ, B_λ*—the numerators and denominators of its convergents, and* ξ_λ*—its complete quotients. Further, let*

$$\xi' = \frac{p_0\xi + r_0}{s_0} \quad (p_0, r_0, s_0\text{—integers},\ p_0 > 0,\ s_0 > 0,\ p_0 s_0 = d > 1).$$

For any index ν $(\geqslant 1)$ *the number*

$$\frac{p_0[b_0, b_1, \dots, b_{\nu-1}] + r_0}{s_0} = \frac{p_0 A_{\nu-1} + r_0 B_{\nu-1}}{s_0 B_{\nu-1}}$$

can be developed in an arithmetical continued fraction $[d_0, d_1, \dots, d_{\mu-1}]$ *and besides the number of its terms can be chosen so that* $\mu \equiv \nu \pmod 2$; *let* C_λ, D_λ *be the numerators and denominators of its convergents, so that in particular*

$$\frac{p_0 A_{\nu-1} + r_0 B_{\nu-1}}{s_0 B_{\nu-1}} = \frac{C_{\mu-1}}{D_{\mu-1}}\,.$$

Then there exist three uniquely determined integers p_1, r_1, s_1 *such that the formula*

$$\begin{pmatrix} p_0 & r_0 \\ 0 & s_0 \end{pmatrix} \begin{pmatrix} A_{\nu-1} & A_{\nu-2} \\ B_{\nu-1} & B_{\nu-2} \end{pmatrix} = \begin{pmatrix} C_{\mu-1} & C_{\mu-2} \\ D_{\mu-1} & D_{\mu-2} \end{pmatrix} \begin{pmatrix} p_1 & r_1 \\ 0 & s_1 \end{pmatrix}$$

holds and besides

$$p_1 > 0, \quad s_1 > 0, \quad p_1 s_1 = d, \quad -s_1 \leqslant r_1 \leqslant p_1,$$

$$\xi' = [d_0, d_1, \ldots, d_{\mu-1}, \xi'_\mu], \quad \textit{where} \quad \xi'_\mu = \frac{p_1 \xi_\nu + r_1}{s_1}.$$

The theorem quoted obviously preserves its validity for $d = 1$ as well as for rational ξ; in the latter case under the condition $\nu \leqslant \operatorname{lap} \xi$.

On the basis of Lemma 1 and theorem H we shall show

Theorem 1. *For arbitrary positive integers* m *and* d *there exists a number* $M = M(m, d)$ *such that if* $\operatorname{lap} \xi \leqslant m$ *and*

$$\xi' = \frac{p_0 \xi + r_0}{s_0} \quad (p_0, r_0, s_0\text{—integers}, \ p_0, s_0 > 0, \ p_0 s_0 = d) \tag{9}$$

then $\operatorname{lap} \xi' \leqslant M$.

Proof. We shall prove it by induction with respect to m. For $m = 1$ the theorem follows immediately from Lemma 1, whence after the substitution $b = 2$, $h = 1$ (assumption (3) being satisfied in emptiness), $p = p_0$, $r = r_0$, $s = s_0$ we get

$$\operatorname{lap} \xi' < 4 s_0.$$

Assume now that the theorem is valid for $m = h - 1$ $(h > 1)$; we shall show that it is valid for $m = h$.

By hypothesis there exists a number $M(h-1, d)$ such that if $\operatorname{lap} \xi \leqslant h - 1$ and $\xi' = (p\xi + r)/s$ $(p, r, s$—integers, $p > 0, s > 0, ps = d)$, then

$$\operatorname{lap} \xi' \leqslant M(h-1, d).$$

Let $M = 2M(h-1, d) + 2^{h+1} d^{h+1}$. The proof will be complete if we show that for any ξ such that $\operatorname{lap} \xi \leqslant h$ the number ξ' defined by (9) satisfies the inequality

$$\operatorname{lap} \xi' \leqslant M.$$

Since $M(h-1, d) < M$, we can assume that $\operatorname{lap} \xi = h$ and that ξ is given by one of the formulae (2).

c If for each positive $i < h$ is $b_i < 2d$, then putting in Lemma 1 $b = 2d$, $p = p_0, r = r_0$, $s = s_0$, we get

$$\operatorname{lap} \xi' \leqslant 2 s_0 (2d)^h \leqslant 2^{h+1} d^{h+1} \leqslant M.$$

c It remains to consider the case where for some positive $\nu < h$: $b_\nu \geqslant 2d$. We then have

$$\xi = [b_0, b_1, \ldots, b_{\nu-1}, \xi_\nu], \quad \xi_\nu \geqslant b_\nu \geqslant 2d. \tag{10}$$

In virtue of theorem H there exist integers p_1, r_1, s_1 such that

$$p_1 > 0, \quad s_1 > 0, \quad p_1 s_1 = d, \quad -s_1 \leqslant r_1 \leqslant p_1, \tag{11}$$

$$\frac{p_0[b_0, b_1, \dots, b_{\nu-1}] + r_0}{s_0} = [d_0, d_1, \dots, d_{\mu-1}], \tag{12}$$

$$\xi' = \frac{p_0\xi + r_0}{s_0} = [d_0, d_1, \dots, d_{\mu-1}, \xi'_\mu], \quad \xi'_\mu = \frac{p_1\xi_\nu + r_1}{s_1}. \tag{13}$$

From (10) and (11) we get

$$\xi'_\mu \geqslant \xi_\nu/s_1 - 1 \geqslant \xi_\nu/d - 1 \geqslant 1,$$

which together with formula (13) proves that numbers $d_0, d_1, \dots, d_{\mu-1}$ are the initial partial quotients of the number ξ'. Hence

$$\operatorname{lap}\xi' \leqslant \mu + \operatorname{lap}\xi'_\mu. \tag{14}$$

Meanwhile, by (12)

$$\mu \leqslant 1 + \operatorname{lap}\frac{p_0[b_0, b_1, \dots, b_{\nu-1}] + r_0}{s_0}$$

and since $\operatorname{lap}[b_0, b_1, \dots, b_{\nu-1}] \leqslant \nu < h$, we have in virtue of the inductive assumption

$$\mu \leqslant 1 + M(h-1, d). \tag{15}$$

On the other hand, since $\operatorname{lap}\xi_\nu = \operatorname{lap}\xi - \nu < h$, we have

$$\operatorname{lap}\xi'_\mu \leqslant M(h-1, d) \tag{16}$$

and finally by (14), (15), (16) we get

$$\operatorname{lap}\xi' \leqslant 1 + 2M(h-1, d) \leqslant M. \qquad \square$$

Corollary. *For any positive integer m and arbitrary integers d and q there exists a number $M = M(m, d, q)$ such that if*

$$\operatorname{lap}\xi \leqslant m, \quad \xi' = \frac{p\xi + r}{q\xi + s} \quad (p, r, s\text{—integers}, \ q\xi + s \neq 0)$$

and $ps - qr = d$, then $\operatorname{lap}\xi' \leqslant M$.

Proof. The case $d = 0$ is trivial; thus let $d \neq 0$. It is easy to verify the equality (cf. [2], p. 56):

$$-[b_0, b_1, b_2, b_3, \dots] = \begin{cases} [-(b_0+1), 1, b_1 - 1, b_2, b_3, \dots] & \text{for } b_1 > 1, \\ [-(b_0+1), b_2 + 1, b_3, b_4, \dots] & \text{for } b_1 = 1, \end{cases}$$

whence

$$\operatorname{lap}(-\xi) \leqslant 3 + \operatorname{lap}\xi. \tag{17}$$

If $q = 0$, then $s \neq 0$ and we have

$$\xi' = \frac{\operatorname{sgn} p}{\operatorname{sgn} s} \cdot \frac{|p|\xi + r \operatorname{sgn} p}{|s|};$$

the corollary follows therefore directly from Theorem 1 and formula (17).

If $q \neq 0$, then

$$\xi' = \operatorname{sgn} q \cdot \frac{\zeta^{-1} + p}{|q|}, \qquad \zeta = -\frac{\operatorname{sgn} q}{\operatorname{sgn} d} \cdot \frac{|q|\xi + s \cdot \operatorname{sgn} q}{|d|},$$

and we obtain the corollary applying Theorem 1 successively to the numbers ζ and ξ', using formula (17) and the obvious inequality

$$\operatorname{lap} \zeta^{-1} \leqslant 1 + \operatorname{lap} \zeta. \qquad \square$$

Lemma 2. *Let b, k, p and s be positive integers. If ξ is given by* (2″) *and ξ' by* (5) *and if*

$$b_i < b \quad (h \leqslant i \leqslant h + k - 1), \tag{18}$$

then $\operatorname{lp} \xi' \leqslant 8(ps)^2 b^{2k}$.

Proof. It follows from (2″) that

$$\xi_h = [b_h, b_{h+1}, \ldots, b_{h+k-1}, \xi_h];$$

the number ξ_h satisfies therefore the equation

$$B_{k-1,h}x^2 + (B_{k-2,h} - A_{k-1,h})x - A_{k-2,h} = 0, \tag{19}$$

where numbers $A_{\lambda,h}$ and $B_{\lambda,h}$ are respectively the numerator and the denominator of the λth convergent of $[b_h, b_{h+1}, \ldots]$.

Denoting by Δ the discriminant of the equation (19) we have

$$\Delta = (B_{k-2,h} - A_{k-1,h})^2 + 4B_{k-1,h}A_{k-2,h} = (A_{k-1,h} + B_{k-2,h})^2 + 4(-1)^{k-1},$$

and since from (18) easily follows

$$A_{k-1,h} < b^k, \quad B_{k-2,h} < b^k,$$

we get

$$\Delta \leqslant 4b^{2k}. \tag{20}$$

It follows from the formulae

$$\xi' = \frac{p\xi + r}{s}, \quad \xi = \frac{A_{h-1}\xi_h + A_{h-2}}{B_{h-1}\xi_h + B_{h-2}}$$

and from equation (19) for ξ_h that the number ξ' satisfies the equation

$$Ax^2 + Bx + C = 0, \tag{21}$$

where integers A, B, C are defined by the formula

$$\begin{pmatrix} 2A & B \\ B & 2C \end{pmatrix} = \begin{pmatrix} s & 0 \\ -r & p \end{pmatrix} \begin{pmatrix} B_{h-2} & -B_{h-1} \\ -A_{h-2} & A_{h-1} \end{pmatrix} \tag{22}$$

$$\times \begin{pmatrix} 2B_{k-1,h} & B_{k-2,h} - A_{k-1,h} \\ B_{k-2,h} - A_{k-1,h} & -2A_{k-2,h} \end{pmatrix} \begin{pmatrix} B_{h-2} & -A_{h-2} \\ -B_{h-1} & A_{h-1} \end{pmatrix} \begin{pmatrix} s & -r \\ 0 & p \end{pmatrix}.$$

On the other hand, as can easily be seen from Lagrange's proof of his well-known theorem about periodical expansions of quadratic surds (cf. [2], pp. 66–68), if ξ' is a root of equation (21), then

$$\operatorname{lp}\xi' \leqslant 2\Delta',$$

where Δ' is the discriminant of that very equation. But, as follows from (22),

$$\Delta' = -\begin{vmatrix} 2A & B \\ B & 2C \end{vmatrix} = (ps)^2(A_{h-1}B_{h-2} - B_{h-1}A_{h-2})^2\Delta = (ps)^2\Delta.$$

The last two formulae together with (20) finally give

$$\operatorname{lp}\xi' \leqslant 8(ps)^2 b^{2k}. \qquad \square$$

Theorem 2. *For arbitrary integers $n > 0$ and d, there exists a number $N = N(n, d)$ such that if*

$$\operatorname{lp}\xi \leqslant n, \quad \xi' = \frac{p\xi + r}{q\xi + s} \quad (p, q, r, s\text{—integers},\ q\xi + s \neq 0) \text{ and } ps - qr = d, \tag{23}$$

then $\operatorname{lp}\xi' \leqslant N$.

Proof. The case of ξ—rational or $d = 0$ is trivial; let ξ be a quadratic surd, $d \neq 0$.
c On the basis of Theorem 1 there exists a number $M(n, |d|) \geqslant (d+1)^2$ such that, if p, r, s—integers, $p > 0$, $s > 0$, $ps = |d|$ and $\operatorname{lap}\zeta \leqslant n$, then

c
$$\operatorname{lap}\frac{p\zeta + r}{s} \leqslant M(n, |d|).$$

Let $N = M(n, |d|)(|d|+1)^2 + 2^{2n+3}d^{2n+2}$. We shall show that if conditions (23) hold, then

$$\operatorname{lp}\xi' \leqslant N.$$

Put

$$\beta = q/(p, q), \quad \delta = -p/(p, q).$$

Since $(\beta, \delta) = 1$, there exist integers α and γ such that

$$\alpha\delta - \beta\gamma = \operatorname{sgn} d. \tag{24}$$

Putting

$$\xi'' = \frac{\alpha\xi' + \gamma}{\beta\xi' + \delta} \tag{25}$$

we get

$$\xi'' = \frac{p_0\xi + r_0}{s_0},$$

where the integers p_0, r_0, s_0 are defined by the formula

$$\begin{pmatrix} p_0 & r_0 \\ 0 & s_0 \end{pmatrix} = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}\begin{pmatrix} p & r \\ q & s \end{pmatrix};$$

thus $p_0 s_0 = (\alpha\delta - \beta\gamma)(ps - qr) = d \operatorname{sgn} d = |d|$.

In view of formulae (24) and (25), the surds ξ' and ξ'' are equivalent, whence

$$\operatorname{lp}\xi' = \operatorname{lp}\xi'' = \operatorname{lp}\frac{p_0\xi + r_0}{s_0}.$$

Changing, if necessary, the signs of p_0, r_0, s_0 we can therefore assume that

$$\xi' = \frac{p_0\xi + r_0}{s_0}, \quad p_0 > 0, \quad s_0 > 0, \quad p_0 s_0 = d > 0.$$

Let ξ be given by formula $(2'')$, where $k \leqslant n$. If for each i such that $h \leqslant i \leqslant h + k - 1$ we have $b_i < 2d$, then, putting in Lemma 2 $b = 2d$, $p = p_0$, $s = s_0$, we get

$$\operatorname{lp}\xi' \leqslant 8(p_0 s_0)^2 (2d)^{2k} \leqslant 8d^2(2d)^{2n} = 2^{2n+3}d^{2n+2} \leqslant N.$$

It remains to consider the case, where for some $\nu \geqslant h$ holds $b_\nu \geqslant 2d$. We then have

$$\xi = [b_0, b_1, \ldots, b_{\nu-1}, b_\nu, b_{\nu+1}, \ldots, b_{\nu+k-1}, b_\nu, b_{\nu+1}, \ldots, b_{\nu+k-1}, \ldots].$$

Using theorem H we get

$$\frac{p_0[b_0, b_1, \ldots, b_{\nu-1}] + r_0}{s_0} = [d_0, \ldots, d_{\mu_1 - 1}],$$

$$\xi' = [d_0, \ldots, d_{\mu_1-1}, \xi'_{\mu_1}], \quad \xi'_{\mu_1} = \frac{p_1\xi_\nu + r_1}{s_1}, \tag{26}$$

$$p_1 > 0, \quad s_1 > 0, \quad p_1 s_1 = d, \quad -s_1 \leqslant r_1 \leqslant p_1, \tag{27}$$

and for all $i \geqslant 1$

$$\frac{p_i[b_\nu, \ldots, b_{\nu+k-1}] + r_i}{s_i} = [d_{\mu_i}, \ldots, d_{\mu_{i+1}-1}], \tag{28}$$

$$\xi'_{\mu_i} = [d_{\mu_i}, \ldots, d_{\mu_{i+1}-1}, \xi'_{\mu_{i+1}}], \quad \xi'_{\mu_{i+1}} = \frac{p_{i+1}\xi_\nu + r_{i+1}}{s_{i+1}}, \tag{29}$$

$$p_{i+1} > 0, \quad s_{i+1} > 0, \quad p_{i+1}s_{i+1} = d, \quad -s_{i+1} \leqslant r_{i+1} \leqslant p_{i+1}. \tag{30}$$

In view of the inequality $\xi_\nu > b_\nu \geqslant 2d$, it follows from (27) and (30) that $\xi_{\mu_i} > 1$ $(i = 1, 2, \ldots)$; the number ξ' has therefore the following expansion into an arithmetical continued fraction;

$$\xi' = [d_0, \ldots, d_{\mu_1-1}, d_{\mu_1}, \ldots, d_{\mu_2-1}, d_{\mu_2}, \ldots, d_{\mu_3-1}, d_{\mu_3}, \ldots].$$

It follows from (27) and (30) that the number of all possible different systems (p_i, r_i, s_i) does not exceed $d(d+2)$. Thus, among the systems (p_i, r_i, s_i) $(i = 1, 2, \ldots, (d+1)^2)$ there must be at least two identical ones; there exist therefore positive integers $g < j \leqslant (d+1)^2$ such that

$$p_g = p_j, \quad r_g = r_j, \quad s_g = s_j.$$

On the basis of (26) and (29) it follows hence that

$$\xi'_{\mu_j} = \xi'_{\mu_g};$$

thus

$$\operatorname{lp}\xi' \leqslant \mu_j - \mu_g = \sum_{i=g}^{j-1}(\mu_{i+1} - \mu_i).$$

On the other hand, in virtue of formula (28), the definition of the number $M(n, |d|)$ and the condition $k \leqslant n$,

$$\mu_{i+1} - \mu_i \leqslant 1 + \operatorname{lap}\frac{p_i[b_\nu, \dots, b_{\nu+k-1}] + r_i}{s_i} \leqslant M(n, |d|) + 1.$$

In view of $j - g < (d+1)^2 \leqslant M(n, |d|)$, we thus get

$$\operatorname{lp}\xi' \leqslant (j-g)\big(M(n, |d|) + 1\big) \leqslant (d+1)^2 M(n, |d|) \leqslant N. \qquad \square$$

Remark. As can easily be seen, we use in the proof given above only a special case of Theorem 1. We proved it in full generality only for a more complete characterization of the relation between continued fractions and rational homographic transformations.

3.

Lemma 3. *If* $\xi^{(n)} \to \zeta$ ($\xi^{(n)}$ *are quadratic surds,* ζ *an arbitary irrational number*) *and*

$$\xi^{(n)} \neq \zeta, \tag{31}$$

then

$$\lim\big(\operatorname{lap}\xi^{(n)} + \operatorname{lp}\xi^{(n)}\big) = \infty. \tag{32}$$

Proof. If formula (32) does not hold, the sequence $\xi^{(n)}$ contains a subsequence for which

$$\operatorname{lap}\xi^{(n)} + \operatorname{lp}\xi^{(n)} \leqslant L < \infty. \tag{33}$$

Proving Lemma 3 by reduction to absurdity we can therefore assume at once that inequality (33) holds. Let

$$\xi^{(n)} = \big[b_0^{(n)}, b_1^{(n)}, \dots, b_{h_n-1}^{(n)}, \overline{b_{h_n}^{(n)}, b_{h_n+1}^{(n)}, \dots, b_{h_n+k_n-1}^{(n)}}\big],$$
$$h_n = \operatorname{lap}\xi^{(n)}, \quad k_n = \operatorname{lp}\xi^{(n)}, \quad \zeta = [b_0, b_1, \dots].$$

Since ζ is irrational, we have

$$\lim b_i^{(n)} = b_i \quad (i = 0, 1, 2, \dots);$$

thus for every i there exists an n_i such that

$$b_i^{(n)} = b_i \quad (n \geqslant n_i). \tag{34}$$

By (33) we have $h_n + k_n \leqslant L$. Putting $K = L!$ we have, for every n, $h_n \leqslant L$, $k_n \mid K$, whence

$$b_i^{(n)} = b_{i+Kt}^{(n)} \quad (i \geqslant L,\ n \geqslant 1,\ t \geqslant 0). \tag{35}$$

Let $M = \max(n_0, n_1, \ldots, n_{K+L-1})$. We shall show that, contrary to assumption (31), for $n \geqslant M$, $\xi^{(n)} = \zeta$.

In fact, by (34) we have for $n \geqslant M$

$$b_i^{(n)} = b_i \quad (0 \leqslant i < L + K). \tag{36}$$

Assume now that $j \geqslant L + K$. We obviously have $j = tK + i$, where t is an integer $\geqslant 0$, $L < i < L + K$ and according to (35)

$$b_j^{(n)} = b_i^{(n)} \quad (n \geqslant 1). \tag{37}$$

Put $m = \max(M, n_j)$. By (36) we have

$$b_i^{(n)} = b_i^{(m)} \quad (0 \leqslant i < L + K,\ n \geqslant M). \tag{38}$$

c Applying successively formulae (37), (38), (37) and (34) we get for $n \geqslant M$

$$b_j^{(n)} = b_i^{(n)} = b_i^{(m)} = b_j^{(m)} = b_j \quad (j \geqslant L + K),$$

whence by (36) it follows at last that for $n \geqslant M$

$$\xi^{(n)} = \zeta. \qquad \square$$

Remark. One can easily deduce from the lemma proved above Satz 11 and Satz 12 of [3]. There is no inverse implication, but the argumentation given above is a direct generalization of the method used by Schmidt in his proofs.

Theorem 3. *Let* $f(x) = a_0 x^p + a_1 x^{p-1} + \ldots + a_p$ *be an integer-valued polynomial with* $a_0 > 0$. *If*

1. $p \equiv 1 \pmod 2$ *or*
2. $p \equiv 0 \pmod 2$ *and* a_0 *is not a rational square,*

then

$$\overline{\lim}\, \operatorname{lp} \sqrt{f(n)} = \infty.$$

Proof. In view of Lemma 3 and the equality $\operatorname{lap} \sqrt{f(n)} = 1$, it is sufficient to show that the set F of all residues mod 1 of numbers $\sqrt{f(n)}$, $n = 1, 2, \ldots$, has at least one irrational point of accumulation. We shall prove more: that the set F is dense in $(0, 1)$.

c In case 1 put $p = 2m + 1$, $m \geqslant 0$. As can easily be seen, we have in the neighbourhood of ∞

$$\frac{d^k \sqrt{f(x)}}{dx^k} \sim \sqrt{a_0} \binom{m + \frac{1}{2}}{k} k!\, x^{m-k+1/2}.$$

On the other hand, by a well-known theorem of the theory of finite differences (cf. [4], p. 229, th. 221), we have

$$\Delta^k g(x) = \Delta x^k g^{(k)}(x + \Theta k \Delta x), \quad 0 < \Theta < 1,$$

where $g(x)$ is an arbitrary real function with the kth derivative continuous in the interval $(x, x + k\Delta x)$. Putting

$$g(x) = \sqrt{f(x)}, \quad \Delta x = 1,$$

we obtain by a comparison of the preceding two formulae

$$\Delta^k \sqrt{f(x)} \sim \sqrt{a_0} \binom{m+\frac{1}{2}}{k} k!\, x^{m-k+1/2},$$

whence for sufficiently large x

$$\Delta^m \sqrt{f(x)} \sim \sqrt{a_0} \binom{m+\frac{1}{2}}{m} m!\, x^{1/2},$$

$$\Delta^{m+1} \sqrt{f(x)} \sim \sqrt{a_0} \binom{m+\frac{1}{2}}{m+1} (m+1)!\, x^{-1/2};$$

thus

$$\Delta^m \sqrt{f(x)} \to \infty, \quad \Delta^{m+1} \sqrt{f(x)} \to 0.$$

The density of the set F follows immediately in virtue of a theorem of Csillag ([1], p. 152).

In case 2, we have, as can easily be seen,

$$f(x) = u^2(x) + v(x), \tag{39'}$$

where u and v are polynomials with coefficients from $\mathbb{Q}(\sqrt{a_0})$ and

$$\text{degree } v < \text{degree } u = \tfrac{1}{2} \text{ degree } f, \quad u(\infty) = \infty. \tag{39''}$$

Putting $p = 2m$, $u(x) = a_0 x^m + a_1 x^{m-1} + \ldots + a_m$, we find from formulae (39) that $\alpha_0^2 = a_0$, whence according to the assumption about a_0 it follows that α_0 is irrational. In virtue of a well-known theorem of Weyl, the set of all the residues mod 1 of numbers $u(n)$ $(n = 1, 2, \ldots)$ is dense in $(0, 1)$. Since, in view of (39)

$$\lim\left(\sqrt{f(x)} - u(x)\right) = 0,$$

the set F has the same property. □

Remark. In both cases, 1 and 2, it is easy to give examples of polynomials $f(x)$ such that

$$\underline{\lim}\, \operatorname{lp} \sqrt{f(n)} < \infty. \tag{40}$$

It suffices to assume $f_1(x) = x$, $f_2(x) = 2x^2$. The proof of inequality (40) for the polynomial $f_1(x)$ is immediate; for the polynomial $f_2(x)$ we use the fact that for an infinite sequence of positive integers x_k is $f_2(x_k) = y_k^2 + 1$ (y_k—integers), whence in view of the expansion

$$\sqrt{y^2+1} = (y, \overline{2y})$$

it follows that

$$\operatorname{lp} \sqrt{f_2(x_k)} = 1.$$

4.

Lemma 4. *Let $f(n)$ be an integer-valued polynomial and let*

$$\sqrt{f(n)} = u_0(n) + \cfrac{1}{\left| u_1(n) \right|} + \cfrac{1}{\left| u_2(n) \right|} + \ldots + \cfrac{1}{\left| u_j(n) \right|} + \cfrac{1}{\left| w(n) \right|} \tag{41}$$

where u_i are polynomials of a positive degree with rational coefficients and

$$\lim_{n\to\infty} w(n) = \infty. \tag{42}$$

Put

$$\begin{aligned} &T_{-1}(n) = 1, \quad T_0(n) = u_0(n), \quad T_\nu(n) = u_\nu(n)T_{\nu-1}(n) + T_{\nu-2}(n), \\ &U_{-1}(n) = 0, \quad U_0(n) = 1, \qquad U_\nu(n) = u_\nu(n)U_{\nu-1}(n) + U_{\nu-2}(n), \end{aligned} \tag{43}$$

$$\sqrt{f(n)} = \xi = [b_0, b_1, b_2, \ldots], \quad b_i\text{—positive integers}. \tag{44}$$

Then, for every j and $n > n_0(j)$, there exists a $k = k(j, n)$ such that

$$\frac{A_k}{B_k} = \frac{T_j(n)}{U_j(n)}, \tag{45}$$

$$\xi_{k+1}(n) = (-1)^{j-k}\,\frac{U_j^2(n)}{B_k^2}\,w(n) + \frac{(-1)^{j-k}U_j(n)U_{j-1}(n) - B_kB_{k-1}}{B_k^2}. \tag{46}$$

Proof. Since the polynomials u_i have rational coefficients, there exists a positive integer m such that

$$T_j(n) = P(n)/m, \quad U_j(n) = Q(n)/m, \tag{47}$$

where $P(n)$, $Q(n)$ are polynomials with integral coefficients.

From formulae (41) and (43) we get

$$\sqrt{f(n)} = \frac{T_j(n)}{U_j(n)} + \frac{(-1)^j}{U_j(n)\big(U_j(n)w(n) + U_{j-1}(n)\big)}, \tag{48}$$

whence in view of (47)

$$\left|\sqrt{f(n)} - \frac{P(n)}{Q(n)}\right| = \frac{1}{Q^2(n)}\left|\frac{m^2}{w(n) + U_{j-1}(n)/U_j(n)}\right|.$$

Since in view of (42) and (43)

$$w(n) + U_{j-1}(n)/U_j(n) \to \infty,$$

we have for sufficiently large n

$$\left|\sqrt{f(n)} - \frac{P(n)}{Q(n)}\right| < \frac{1}{2Q^2(n)}.$$

In virtue of a well-known theorem (cf. [2], Satz 2.14), $P(n)/Q(n)$ is therefore equal to some convergent of expansion (44). Then, for some k, equality (45) holds and since

$$\sqrt{f(n)} = \frac{A_k}{B_k} + \frac{(-1)^k}{B_k[B_k\xi_{k+1} + B_{k-1}]},$$

we get also (46) in view of (48).

Definition. For a given prime p and a given rational number $r \neq 0$ we shall denote by $\exp(p, r)$ the exponent with which p comes into the canonical expansion of r.

Lemma 5. *Suppose we are given a prime p and integers n and h, both $\neq 0$. Let then*

$$\begin{aligned} P_{-1} &= h, \quad P_0 = n, \quad P_\nu = 2nP_{\nu-1} + hP_{\nu-2}, \\ Q_{-1} &= 0, \quad Q_0 = 1, \quad Q_\nu = 2nQ_{\nu-1} + hQ_{\nu-2}. \end{aligned} \tag{49}$$

If $\exp(p, h) > 2\exp(p, 2n)$, then for every integer $\nu \geqslant 0$

$$\begin{aligned} \exp(p, P_\nu) &= \exp(p, n) + \nu \exp(p, 2n), \\ \exp(p, Q_\nu) &= \nu \exp(p, 2n). \end{aligned} \tag{50}$$

Proof by induction with respect to ν. For $\nu = 0$ the lemma follows directly from formulae (49).

For $\nu = 1$ we have $P_1 = 2n^2 + h$, $Q_1 = 2n$; thus $\exp(p, Q_1) = \exp(p, 2n)$. Since, by hypothesis,

$$\exp(p, h) > 2\exp(p, 2n) \geqslant \exp(p, 2n^2),$$

it follows that

$$\exp(p, P_1) = \exp(p, 2n^2) = \exp(p, n) + \exp(p, 2n)$$

and formulae (50) hold also for $\nu = 1$.

Assume now that the lemma is right for the numbers $\nu - 2$ and $\nu - 1$ ($\nu \geqslant 2$); we shall show its validity for ν.

It follows easily from the inductive assumption that

$$\begin{aligned} e_1 &= \exp(p, 2nP_{\nu-1}) = \exp(p, n) + \nu \exp(p, 2n), \\ e_2 &= \exp(p, hP_{\nu-2}) = \exp(p, n) + (\nu - 2)\exp(p, 2n) + \exp(p, h), \\ e_3 &= \exp(p, 2nQ_{\nu-1}) = \nu \exp(p, 2n), \\ e_4 &= \exp(p, hQ_{\nu-2}) = (\nu - 2)\exp(p, 2n) + \exp(p, h). \end{aligned}$$

In view of the inequality $\exp(p, h) > 2\exp(p, 2n)$ we therefore have $e_1 < e_2, e_3 < e_4$, whence it follows by (49) that

$$\begin{aligned} \exp(p, P_\nu) &= e_1 = \exp(p, n) + \nu \exp(p, 2n), \\ \exp(p, Q_\nu) &= e_3 = \nu \exp(p, 2n). \end{aligned}$$

□

Theorem 4. *Suppose we are given an integer $h \neq 0$. Denote by E the set of all integers n such that $h \mid 4n^2$. We have*

$$\lim_{\substack{n \to \infty \\ n \notin E}} \operatorname{lp} \sqrt{n^2 + h} = \infty, \tag{51}$$

$$\overline{\lim_{\substack{n \to \infty \\ n \in E}}} \operatorname{lp} \sqrt{n^2 + h} < \infty. \tag{52}$$

Proof. We begin with a proof of equality (51). Choose an arbitrary g; we shall show that for sufficiently large $n \notin E$

$$\operatorname{lp}\sqrt{n^2+h} \geqslant g.$$

It is easy to verify the identity

$$\sqrt{n^2+h} = n + \frac{1}{\lfloor 2n/h \rfloor} + \frac{1}{\lfloor n+\sqrt{n^2+h} \rfloor},$$

from which we immediately obtain

$$\sqrt{n^2+h} = n + \frac{1}{\lfloor 2n/h \rfloor} + \frac{1}{\lfloor 2n \rfloor} + \ldots + \frac{1}{\lfloor 2n/h \rfloor} + \frac{1}{\lfloor n+\sqrt{n^2+h} \rfloor}. \tag{53}$$

Put in Lemma 4 $u_0 = n$,

$$u_\nu = \begin{cases} 2n/h & (\nu \text{ odd } \leqslant 2g-1), \\ 2n & (\nu \text{ even } < 2g-1). \end{cases}$$

Comparing polynomials T_ν, U_ν determined by these u_ν by formulae (43) and polynomials P_ν, Q_ν defined by (49), we find by an easy induction

$$T_\nu = P_\nu h^{-[(\nu+1)/2]}, \quad U_\nu = Q_\nu h^{-[(\nu+1)/2]}, \tag{54}$$

whence

$$\frac{T_\nu}{U_\nu} = \frac{P_\nu}{Q_\nu}. \tag{55}$$

Assume now that $n \notin E$, n so large that $\sqrt{n^2+h}$ is irrational, and

$$\sqrt{n^2+h} = \xi = [b_0, b_1, \ldots]. \tag{56}$$

In virtue of Lemma 4 for sufficiently large n for each $i \leqslant g$ there exists a k_i such that

$$\frac{A_{k_i}}{B_{k_i}} = \frac{T_{2i-1}}{U_{2i-1}}, \tag{57}$$

$$\xi_{k_i+1} = (-1)^{k_i-1}\frac{U_{2i-1}^2}{B_{k_i}^2}\left(n+\sqrt{n^2+h}\right) + \frac{(-1)^{k_i-1}U_{2i-1}U_{2i-2} - B_{k_i}B_{k_i-1}}{B_{k_i}^2}. \tag{58}$$

Since $n \notin E$, there exists a prime p such that

$$\exp(p,h) > 2\exp(p,2n) \tag{59}$$

and in virtue of Lemma 5

$$\begin{aligned} \exp(p, P_{2i-1}) &= \exp(p,n) + (2i-1)\exp(p,2n), \\ \exp(p, Q_{2i-1}) &= (2i-1)\exp(p,2n). \end{aligned} \tag{60}$$

In view of (55) and (57), we therefore have

$$\exp\left(p, \frac{A_{k_i}}{B_{k_i}}\right) = \exp\left(p, \frac{P_{2i-1}}{Q_{2i-1}}\right) = \exp(p,n)$$

and since the fraction A_{k_i}/B_{k_i} is irreducible, it follows that

$$\exp(p,\, B_{k_i}) = 0.$$

On the basis of (54) and (60) we get hence

$$\exp\left(p,\, \frac{U_{2i-1}}{B_{k_i}}\right) = \exp(p,\, U_{2i-1}) = (2i-1)\exp(p,\, 2n) - i\exp(p,\, h)$$
$$= -\exp(p,\, 2n) - i\big(\exp(p,\, h) - 2\exp(p,\, 2n)\big).$$

Then, in view of inequality (59), the numbers $\exp(p,\, U_{2i-1}/B_{k_i})$ are for $i = 1, 2, \ldots, g$ all different; since $\sqrt{n^2+h}$ is irrational and (58) holds, the numbers ξ_{k_i+1} have the same property. Since $k_i + 1 \geqslant 1 = \operatorname{lap}\sqrt{n^2+h}$, at least g different complete quotients occur in the period of expansion (56); we then have $\operatorname{lp}\xi \geqslant g$, which completes the proof of (51).

In order to prove formula (52) we shall use Theorem 2. From that theorem follows the existence of a number $N = N(h)$ such that if for positive integers D_1, D_2 and l

$$\sqrt{D_2} = \tfrac{1}{2}l\sqrt{D_1}, \quad 0 < l \leqslant |h| \quad \text{and} \quad \operatorname{lp}\sqrt{D_1} \leqslant 12,$$

then $\operatorname{lp}\sqrt{D_2} \leqslant N$.

We shall show that for sufficiently large $n \in E$

$$\operatorname{lp}\sqrt{n^2+h} \leqslant N. \tag{61}$$

In fact, since $n \in E$, $h \mid 4n^2$, there exist—as can easily be seen—integers α, $\beta \neq 0$ and positive integer x such that

$$2n = \alpha\beta x, \quad h = \alpha\beta^2.$$

We obviously have

$$\sqrt{n^2+h} = \tfrac{1}{2}|\beta|\sqrt{(\alpha x)^2 + 4\alpha}, \quad |\beta| \leqslant |h|. \tag{62}$$

On the other hand, as can be verified, the following expansions hold for $x \geqslant 5$:

$\alpha > 0$, x—even

$$\sqrt{(\alpha x)^2+4\alpha} = [\alpha x,\, \overline{\tfrac{1}{2}x,\, 2\alpha x}];$$

$\alpha > 0$ even, x—odd

$$\sqrt{(\alpha x)^2+4\alpha} = [\alpha x,\, \overline{\tfrac{1}{2}(x-1),\, 1,\, 1,\, \tfrac{1}{2}(\alpha x - 2),\, 1,\, 1,\, \tfrac{1}{2}(x-1),\, 2\alpha x}];$$

$\alpha > 0$ odd, x—odd

$$\sqrt{(\alpha x)^2+4\alpha} = [\alpha x,\, \overline{\tfrac{1}{2}(x-1),\, 1,\, 1,\, \tfrac{1}{2}(\alpha x - 1),\, 2x,\, \tfrac{1}{2}(\alpha x - 1),\, 1,\, 1,\, \tfrac{1}{2}(x-1),\, 2\alpha x}];$$

$\alpha < 0$, x—even

$$\sqrt{(\alpha x)^2+4\alpha} = [|\alpha|x - 1,\, \overline{1,\, \tfrac{1}{2}(x-4),\, 1,\, 2|\alpha|x - 2}];$$

$\alpha < 0$ even, x—odd

$$\sqrt{(\alpha x)^2+4\alpha} = [|\alpha|x - 1,\, \overline{1,\, \tfrac{1}{2}(x-3),\, 2,\, \tfrac{1}{2}(|\alpha|x - 2),\, 2,\, \tfrac{1}{2}(x-3),\, 1,\, 2|\alpha|x - 2}];$$

$\alpha < 0$ odd, x—odd

c $$\sqrt{(\alpha x)^2 + 4\alpha} = [|\alpha|x - 1, \overline{1, \tfrac{1}{2}(x-3), 2, \tfrac{1}{2}(|\alpha|x-3), 1, 2x-2, 1, \tfrac{1}{2}(|\alpha|x-3), 2, \tfrac{1}{2}(x-3), 1, 2|\alpha|x-2}].$$

Thus, we always have $\operatorname{lp}\sqrt{(\alpha x)^2 + 4\alpha} \leqslant 12$ and formula (61) follows immediately from (62) and the definition of N. □

Theorem 5. *Let $f(n) = \alpha^2 n^2 + bn + c$, α, b, c—integers, $\alpha > 0$, $\Delta = b^2 - 4\alpha^2 c \neq 0$. The inequality*

$$\overline{\lim}\operatorname{lp}\sqrt{f(n)} < \infty \tag{63}$$

holds if and only if

$$\Delta \mid 4(2\alpha^2, b)^2. \tag{64}$$

Proof. We obviously have

$$\sqrt{f(n)} = \frac{1}{2\alpha}\sqrt{(2\alpha^2 n + b)^2 - \Delta}$$

and in virtue of Theorem 2 inequality (63) is equivalent to the following

$$\overline{\lim}\operatorname{lp}\sqrt{(2\alpha^2 n + b)^2 - \Delta} < \infty.$$

But in virtue of Theorem 4 the last inequality holds if and only if for some n_0

$$\Delta \mid 4(2\alpha^2 n + b)^2 \quad \text{for} \quad n > n_0. \tag{65}$$

We have

$$4(2\alpha^2 n + b)^2 = 4(2\alpha^2, b)^2\left(\frac{2\alpha^2}{(2\alpha^2, b)}n + \frac{b}{(2\alpha^2, b)}\right)^2.$$

Since the arithmetical progression

$$\frac{2\alpha^2}{(2\alpha^2, b)}n + \frac{b}{(2\alpha^2, b)} \quad (n = 0, 1, \dots)$$

whose first term and difference are relatively prime, contains infinitely many numbers coprime with Δ, divisibility (64) is a necessary and sufficient condition of (65) and therefore also of (63). □

Theorems 3 and 5 give together a complete solution of the problem P for polynomials of the second degree (the case $\Delta = 0$ is trivial).

In order to obtain by a similar method a complete solution for polynomials of higher degree, it would be necessary to have for $\sqrt{f(n)}$ an expansion analogous to (53), i.e. an expansion of form (41) and then to know whether it is periodical.

Now, for polynomials $f(n)$ of the form

$$\alpha^2 n^{2m} + a_1 n^{2m-1} + \dots + a_{2m}$$

an expansion of form (41) is uniquely determined. In fact, let

$$\sqrt{f(n)} = u_0(n) + \cfrac{1}{\left| u_1(n) \right.} + \cfrac{1}{\left| u_2(n) \right.} + \ldots + \cfrac{1}{\left| u_j(n) \right.} + \cfrac{1}{\left| w_{j+1}(n) \right.}$$

and put for $i \leqslant j$

$$w_i(n) = u_i(n) + \cfrac{1}{\left| u_{i+1}(n) \right.} + \ldots + \cfrac{1}{\left| u_j(n) \right.} + \cfrac{1}{\left| w_{j+1}(n) \right.}.$$

Since $u_0(n)$ is the unique polynomial g such that $\lim\limits_{n\to\infty}\left(\sqrt{f(n)} - g(n)\right) = 0$, we have $u_0(n) = u(n)$, where $u(n)$ is defined by formulae (39). Suppose now that we have
c determined polynomials $u_0(n), \ldots, u_{i-1}(n)$; we easily find

$$w_i(n) = \frac{\sqrt{f(n)} + p_i(n)}{q_i(n)}$$

where p_i, q_i are polynomials with rational coefficients, and then $u_i(n)$ is uniquely determined by the conditions

$$u(n) + p_i(n) = q_i(n)u_i(n) + r_i(n), \quad \text{degree}\, r_i < \text{degree}\, q_i.$$

The construction of the sequence $u_i(n)$ is therefore easy, but the decision whether the sequence thus determined u_i is periodical presents a considerable difficulty even for polynomials of degree 4.

Thus, the investigation of the problem P has led us to the following problem P_1:

P_1. *To decide whether for a given polynomial $f(n)$ of the form*

$$\alpha^2 n^{2m} + a_1 n^{2m-1} + \ldots + a_{2m} \quad (m, \alpha, a_i \text{ are integers, } m \geqslant 2,\ \alpha \neq 0)$$

there exist polynomials u_i of positive degree with rational coefficients such that

$$\sqrt{f(n)} = u_0(n) + \overline{\cfrac{1}{\left| u_1(n) \right.} + \cfrac{1}{\left| u_2(n) \right.} + \ldots + \cfrac{1}{\left| u_k(n) \right.}}$$

c *(the bar denotes period).*

References

[1] P. Csillag, *Über die Verteilung iterierter Summen von positiven Nullfolgen* mod 1. Acta Litt. Sci. Szeged 4 (1929), 151–154.

[2] O. Perron, *Die Lehre von den Kettenbrüchen* I. Teubner, Stuttgart 1954.

[3] H. Schmidt, *Zur Approximation und Kettenbruchentwicklung quadratischer Zahlen*. Math. Z. 52 (1950), 168–192.

[4] W. Sierpiński, *Rachunek różniczkowy*. Monogr. Mat. 14, Czytelnik, Warszawa 1947.

[5] F. Tano, *Sur quelques points de la théorie des nombres*. Bull. Sci. Math. (2) 14 (1890), 215–218.

Originally published in
Acta Arithmetica VII (1962), 287–298

On some problems of the arithmetical theory of continued fractions II*

To Professor Wacław Sierpiński on his 80-th birthday

1.

In the preceding paper [5], I considered the following two problems

P. *Decide for a given integer-valued polynomial* $f(n)$ *whether*

$$\overline{\lim}\, \mathrm{lp}\sqrt{f(n)} < \infty.$$

($\mathrm{lp}\sqrt{f(n)}$ denotes the length of the shortest period of the expansion of $\sqrt{f(n)}$ into an arithmetic continued fraction).

P$_1$. *Decide whether for a given polynomial* $f(n)$ *of the form*

$$\alpha^2 n^{2\mu} + a_1 n^{2\mu-1} + \ldots + a_{2\mu} \quad (\mu, \alpha, a_i\text{—integers, } \mu \geqslant 2,\ \alpha \neq 0) \tag{1}$$

there exist polynomials u_i *of positive degree with rational coefficients such that*

$$\sqrt{f(n)} = u_0(n) + \overline{\left|\frac{1}{u_1(n)}\right| + \left|\frac{1}{u_2(n)}\right| + \ldots + \left|\frac{1}{u_K(n)}\right|} \tag{2}$$

(the bar denotes the period).

I indicated a connection between them. Now I prove (in §2) that for polynomials f of the form (1) problem P can be completely reduced to problem P$_1$. The proof follows the ideas of H. Schmidt [6] rather than those of paper [5]. Since for polynomials f not of form (1) problem P is solved (negatively) by Theorem 3 [5], one can limit oneself to the investigation of problem P$_1$. In §3 I show how problem P$_1$ can be reduced to the case where the polynomial $f(n)$ has no multiple factors. Finally (§4), I discuss the results concerning problem P$_1$ which I have found in papers about pseudo-elliptic integrals (they contain in fact a complete solution of problem P$_1$ for polynomials f of degree 4 without multiple

* This paper was written when the author was Rockefeller Foundation Fellow at Uppsala University.

factors) and I generalise some of them to the hyperelliptic case ($\mu > 2$). The connection between problem P_1 and the theory of Abelian integrals was already established by Abel [1], who also proved that the answer to P_1 is positive if and only if the equation

$$X^2 - fY^2 = \text{const}$$

is solvable in polynomials X, Y where $Y \neq 0$. Furthermore, if X, Y is a solution of the above equation and $\frac{X}{Y}(\infty) = \infty$, then $\frac{X}{Y}$ is necessarily equal to one of the convergents of expansion (2). I shall make frequent use of these theorems.

As to notation, I shall follow [5]; in particular, I shall denote throughout by $[b_0(n), b_1(n), \dots]$ the expansion of $\sqrt{f(n)}$ into an arithmetic continued fraction, by $A_i(n)/B_i(n)$ the corresponding convergents. Besides, I shall put $\mathrm{LP}\sqrt{f} = K$ if K is the smallest number $\geqslant 0$ for which (2) holds, and $\mathrm{LP}\sqrt{f} = \infty$ if such a number does not exist. Putting

$$\sqrt{f} = u_0 + \frac{1}{|\,u_1} + \frac{1}{|\,u_2} + \dots$$

I shall assume simultaneously

$$\begin{aligned} T_{-1} &= 1, \quad & T_0 &= u_0, \quad & T_\nu &= u_\nu T_{\nu-1} + T_{\nu-2}, \\ U_{-1} &= 0, \quad & U_0 &= 1, \quad & U_\nu &= u_\nu U_{\nu-1} + U_{\nu-2}. \end{aligned}$$

$[q]$ and (q) will denote the integral the fractional part of q, respectively, $\Phi_n(x)$—the n-th cyclotomic polynomial.

2.

Lemma 1. *For every polynomial f of form* (1) *which is not a perfect square and every $k \geqslant 0$ there exists a finite set of s_k systems of polynomials with rational coefficients $[b_0^{(j)}, b_1^{(j)}, \dots, b_k^{(j)}]$ $(1 \leqslant j \leqslant s_k)$ such that integers $> n_0(k)$ can be divided into s_k classes $K_1, K_2, \dots, K_{s_k}$ so that if $n \in K_j$ then $b_i(n) = b_i^{(j)}(n)$ $(0 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant s_k)$.*

Proof by induction with respect to k. To avoid the repetition of the argument, we shall start the induction from $k = -1$, where for all n we can assume $b_{-1}(n) = 0$ and no division into classes is necessary. Suppose now that the theorem is proved for $k-1$ $(k \geqslant 0)$, and let $K_1, K_2, \dots, K_s$ be corresponding classes and $[b_0^{(j)}, b_1^{(j)}, \dots, b_{k-1}^{(j)}]$ $(j \leqslant s)$ corresponding systems of polynomials. For $n \in K_j$ we have

$$\sqrt{f(n)} = [b_0^{(j)}(n), b_1^{(j)}(n), \dots, b_{k-1}^{(j)}(n), \xi_k(n)],$$

where evidently $\xi_k(n) = \big(\sqrt{f(n)} + r(n)\big)/s(n)$, $r(n)$ and $s(n)$ being polynomials with rational coefficients completely determined by the class K_j (this is true also for $k = 0$). Now

$$\frac{\sqrt{f(n)} + r(n)}{s(n)} = q(n) + \varrho(n),$$

where $q(n)$ is a polynomial with rational coefficients, $\varrho(n) = o(1)$ and, for sufficiently large n, $\varrho(n)$ has a fixed sign. Therefore for $n > n_0(k)$

$$b_k(n) = \begin{cases} q(n) - 1 & \text{if } q(n) \text{ is integral and } \dfrac{1}{\varrho}(\infty) = -\infty, \\ [q(n)] & \text{otherwise.} \end{cases}$$

Put $q(n) = Q(n)/m$, where $Q(n)$ is a polynomial with integral coefficients and m a positive integer. If $n \equiv r \pmod m$, we have $[q(n)] = q(n) - \big(q(r)\big)$. Therefore, putting for $0 \leqslant r < m$

$$b_k^{(j,r)}(n) = \begin{cases} q(n) - 1 & \text{if } \big(q(r)\big) = 0 \text{ and } \dfrac{1}{\varrho}(\infty) = -\infty, \\ q(n) - \big(q(r)\big) & \text{otherwise,} \end{cases}$$

we have for $n \in K_j$, $n > n_0(k)$, $n \equiv r \pmod m$,

$$b_k(n) = b_k^{(j,r)}(n).$$

This determines the required subdivision of the class K_j into a finite number of classes and completes the proof. □

Theorem 1. *If* $\mathrm{LP}\sqrt{f} = \infty$, *then* $\lim \mathrm{lp}\sqrt{f(n)} = \infty$.

Proof. Let k be an arbitrary integer $\geqslant 0$. For all classes $K_1, K_2, \ldots, K_{s_k}$ whose existence is stated in Lemma 1, we form polynomials $A_{i,j}(n)$, $B_{i,j}(n)$ defined by the formulae $(0 \leqslant i \leqslant k, 1 \leqslant j \leqslant s_k)$

$$\begin{aligned} &A_{-1,j}(n) = 1, \quad A_{0,j}(n) = b_0^{(j)}(n), \quad A_{i,j}(n) = b_i^{(j)}(n)A_{i-1,j}(n) + A_{i-2,j}(n), \\ &B_{-1,j}(n) = 0, \quad B_{0,j}(n) = 1, \quad\quad B_{i,j}(n) = b_i^{(j)}(n)B_{i-1,j}(n) + B_{i-2,j}(n). \end{aligned} \tag{3}$$

Since $\mathrm{LP}\sqrt{f} = \infty$, among the polynomials $A_{i,j}(n)$, $B_{i,j}(n)$ there is no pair satisfying identically the equation

$$A_{i,j}^2(n) - f(n)B_{i,j}^2(n) = \text{const.}$$

It follows that if $n > n_1(k)$, we have for all $i \leqslant k$, $j \leqslant s_k$:

$$A_{i,j}^2(n) - f(n)B_{i,j}^2(n) \neq \pm 1.$$

On the other hand, by Lemma 1, for $n > n_0(k)$, $b_i(n) = b_i^{(j)}(n)$ for some $j \leqslant s_k$ and all $i \leqslant k$, and thus $A_i(n) = A_{i,j}(n)$ and $B_i(n) = B_{i,j}(n)$. The last inequality implies therefore that for all $n > \max\big(n_0(k), n_1(k)\big)$

$$A_i^2(n) - f(n)B_i^2(n) \neq \pm 1 \quad (0 \leqslant i \leqslant k),$$

whence $\mathrm{lp}\sqrt{f(n)} > k$. □

Lemma 2. *If* $R(n)$ *is any rational function with rational coefficients, then*

$$\overline{\lim}\,\mathrm{lap}\,R(n) < \infty.$$

Proof. We shall prove it by induction with respect to the degree d of the denominator of $R(n)$ in its irreducible form. If $d = 0$, we have $R(n) = P(n)/m$, where $P(n)$ is a c polynomial with integral coefficients and m is a positive integer. Obviously

$$\operatorname{lap} R(n) \leqslant \max_{0 \leqslant r < m} \operatorname{lap} R(r).$$

Suppose now that the lemma is valid for all rational functions with denominators of degree $< d$ and let $R(n) = P(n)/Q(n)$ where P, Q are polynomials and the degree of Q is equal to d. We have

$$R(n) = q(n) + \frac{r(n)}{Q(n)},$$

where q, r are polynomials and r is of degree $< d$. Putting $q(n) = q_1(n)/m$, where $q_1(n)$ c is a polynomial with integral coefficients and m is a positive integer, we have for $n \equiv r \pmod m$

$$\operatorname{lap} R(n) = \operatorname{lap}\Big(\frac{q_1(r)}{m} + \frac{r(n)}{Q(n)}\Big) = \operatorname{lap}\Big(\frac{q_1(r)\xi(n) + m}{m\xi(n)}\Big),$$

where $\xi(n) = Q(n)/r(n)$. Since by the inductive assumption: $\overline{\lim}\, \operatorname{lap} \xi(n) < \infty$, it follows immediately from Theorem 1 [5] that $\overline{\lim}\, \operatorname{lap} R(n) < \infty$, which completes the proof. □

Theorem 2. *If* $\operatorname{LP} \sqrt{f} = K > 0$ *and*

$$\sqrt{f} = u_0 + \cfrac{1}{|u_1| + \cfrac{1}{|u_2| + \ldots + \cfrac{1}{|u_K|}}},$$

denote by E *the set of all integers* n *such that* $2T_{K-1}(n)$ *is integral, and by* $\mathrm{C}E$ *its complement. Then*

$$\lim_{\substack{n \to \infty \\ n \in \mathrm{C}E}} \operatorname{lp} \sqrt{f(n)} = \infty, \tag{4}$$

$$\overline{\lim_{\substack{n \to \infty \\ n \in E}}} \operatorname{lp} \sqrt{f(n)} < \infty. \tag{5}$$

Proof. We begin with a proof of equation (4). Let k be an arbitrary integer > 0, and define K_j, $A_{i,j}(n)$, $B_{i,j}(n)$ $(0 \leqslant i \leqslant k, 0 \leqslant j \leqslant s_k)$ as in the proof of Theorem 1. Suppose that c for some i, j we have $K_j \cap \mathrm{C}E \neq \varnothing$ and identically

$$A_{i,j}^2(n) - f(n) B_{i,j}^2(n) = \pm 1.$$

Since the continued fraction expansion furnishes the fundamental solution $T_{K-1}(n)$, $U_{K-1}(n)$ of the Pell equation $X^2 - f(n)Y^2 = \pm 1$, we must have, for some l and suitably chosen signs, identically

$$\pm A_{i,j}(n) \pm \sqrt{f(n)}\, B_{i,j}(n) = T_{lK-1} + \sqrt{f(n)}\, U_{lK-1} = \big(T_{K-1} + \sqrt{f(n)}\, U_{K-1}\big)^l$$

c [this is not always true, for the correct statement and the necessary addition to the following argument see corrigendum on page 160].

c Now let $n_0 \in K_j \cap \mathrm{C}E$. Since $n_0 \in K_j$, $\sqrt{f(n_0)}$ is irrational; $A_{i,j}(n_0) = A_i(n_0)$, $B_{i,j}(n_0) = B_i(n_0)$ are integers, whence $\pm A_{i,j}(n_0) \pm \sqrt{f(n_0)}\, B_{i,j}(n_0)$ is an integer

of the field $\mathbb{Q}\big(\sqrt{f(n_0)}\big)$. On the other hand, since $2T_{K-1}(n_0)$ is not a rational integer, $T_{K-1}(n_0)+\sqrt{f(n_0)}\,U_{K-1}(n_0)$ and therefore also $\big(T_{K-1}(n_0)+\sqrt{f(n_0)}\,U_{K-1}(n_0)\big)^l$ cannot be an integer of the field $\mathbb{Q}\big(\sqrt{f(n_0)}\big)$.

The contradiction obtained proves that, for all j such that $K_j \cap \mathrm{C}E \neq \varnothing$ and all $i \leqslant k$,

$$A_{i,j}^2(n) - f(n)B_{i,j}^2(n) = \pm 1$$

does not hold identically. There exists therefore a number $n_1(k)$ such that for all $n > n_1(k)$

$$A_{i,j}^2(n) - f(n)B_{i,j}^2(n) \neq \pm 1.$$

Thus if $n > \max\big(n_0(k), n_1(k)\big)$, $n \in \mathrm{C}E$, then

$$A_i^2(n) - f(n)B_i^2(n) \neq \pm 1$$

for all $i \leqslant k$, whence $\mathrm{lp}\sqrt{f(n)} > k$, which completes the proof of (4).

To prove inequality (5) put $U_{K-1}(n) = W(n)/m$, where $W(n)$ is an integer-valued polynomial and m is an integer and consider all rational functions

$$\frac{T_{lK-1}}{U_{lK-1}},\ \frac{T_{3lK-1}}{U_{3lK-1}} \quad (l = 1, 2, \ldots, m^2).$$

By Lemma 2, there exists a number M such that for all $i \leqslant 3m^2$

$$\mathrm{lap}\,\varepsilon\frac{T_{iK-1}}{U_{iK-1}} \leqslant M \quad (\varepsilon = 1 \text{ or } -1).$$

We shall prove (5) by showing that for all $n \in E$

$$\mathrm{lp}\sqrt{f(n)} \leqslant M + 2.$$

In fact, if $n \in E$, $2T_{K-1}(n)$ is an integer. If $T_{K-1}(n)$ is itself an integer, then it follows from the equation

$$T_{K-1}^2 - f(n)U_{K-1}^2 = (-1)^K$$

that $f(n)U_{K-1}^2(n)$ is also an integer. Therefore if $m_n \mid m$ is the denominator of $U_{K-1}(n)$ represented as an irreducible fraction, the number $f(n)/m_n^2$ must be integral. The equation

$$T_{lK-1}(n) + \sqrt{\frac{f(n)}{m_n^2}}\,m_n U_{lK-1}(n) = \left(T_{K-1}(n) + \sqrt{\frac{f(n)}{m_n^2}}\,m_n U_{K-1}(n)\right)^l$$

implies that $T_{lK-1}(n)$ and $m_n U_{lK-1}$ are integers and, *a fortiori*, $T_{lK-1}(n)$ and $mU_{lK-1}(n)$ are integers.

Consider therefore all systems $\big(T_{lK-1}(n), mU_{lK-1}(n)\big)$ reduced $\bmod m$. Since the number of all systems (a, b) different $\bmod m$ is m^2, we have for some $1 \leqslant i < j \leqslant m^2+1$

$$T_{iK-1}(n) \equiv T_{jK-1}(n) \pmod m,$$
$$mU_{iK-1}(n) \equiv U_{jK-1}(n) \pmod m.$$

Hence

$$T_{K(j-i)-1}(n) + \sqrt{f(n)}\, U_{K(j-i)-1} = \big(T_{Kj-1}(n)T_{Ki-1}(n) - f(n)U_{Kj-1}U_{Ki-1}\big) + \frac{\sqrt{f(n)}}{m}\big(T_{Kj-1}mU_{Kj-1} - T_{Ki-1}mU_{Kj-1}\big).$$

Since

$$T_{Kj-1}mU_{Kj-1} - T_{Ki-1}mU_{Kj-1} \equiv 0 \,(\mathrm{mod}\, m),$$

the number $U_{K(j-1)-1}$ is an integer.

Since the numbers $T_{K(j-i)-1}(n)$ and $U_{K(j-i)-1}(n)$ form an integral solution of the equation

$$x^2 - f(n)y^2 = \pm 1,$$

the number $\left|\dfrac{T_{K(j-i)-1}(n)}{U_{K(j-i)-1}(n)}\right|$ must be a convergent of the arithmetic continued fraction for $\sqrt{f(n)}$, and if $\mathrm{lp}\sqrt{f(n)} = k$, we must have

$$\left|\frac{T_{K(j-i)-1}(n)}{U_{K(j-i)-1}(n)}\right| = \frac{A_{kt-1}}{B_{kt-1}},$$

whence

$$k \leqslant kt \leqslant \mathrm{lap}\left|\frac{T_{K(j-i)-1}(n)}{U_{K(j-i)-1}(n)}\right| + 2 \leqslant M + 2.$$

If $2T_{K-1}(n)$ is an integer but $T_{K-1}(n)$ is not, then it is evident from the formula

$$T_{3K-1} = T_{K-1}\big(4T_{K-1}^2 - 3(-1)^K\big)$$

that $T_{3K-1}(n)$ is an integer. *Mutatis mutandis*, the whole previous argument applies. □

Theorem 2 immediately implies

Theorem 3. *If* $\mathrm{LP}\sqrt{f} = K < \infty$ *and formula* (2) *holds, then* $\lim \mathrm{lp}\sqrt{f(n)} < \infty$ *if and only if* $2T_{K-1}(n)$ *is an integer-valued polynomial.*

Theorems 2 and 3 generalise Theorems 4 and 5 of [5]. Their proofs furnish also independent proofs of the latter theorems.

In view of Theorem 3 [5], problem P is now completely reduced to problem P_1.

3.

Theorem 4. *If* $f(x) = g^2(x)h(x)$ *where* $h(x)$ *has no multiple roots, then* $\mathrm{LP}\sqrt{f} < \infty$ *implies* $\mathrm{LP}\sqrt{h} < \infty$. *Furthermore, if* $g(x) = g_1^{\alpha_1}(x)g_2^{\alpha_2}(x)\cdots g_s^{\alpha_s}(x)$, *where* g_i *are distinct irreducible polynomials of degree* γ_i *respectively,* $\mathrm{LP}\sqrt{h} < \infty$ *and* T, U *is the fundamental solution of the Pell equation*

$$X^2 - h(x)Y^2 = 1, \tag{6}$$

then $\mathrm{LP}\sqrt{f} < \infty$ *if and only if for each* $i \leqslant s$ *we have*

(i) $U \equiv 0 \pmod{g_i^{\alpha_i}}$ *if* $g_i \mid hU$,

(ii) $\prod_{\substack{r \\ g_i(r)=0}} [x^2 - 2T(r)x + 1] = \Phi_n(x)^{2\gamma_i/\varphi(n)}$ *for some* n *satisfying* $\varphi(n) \mid 2\gamma_i$ *and* $T' \equiv 0 \pmod{g_i^{\alpha_i - 1}}$ *if* $g_i \nmid hU$.

Proof. If polynomials X_0, Y_0 satisfy the equation

$$X^2 - f(x)Y^2 = 1, \tag{7}$$

then polynomials X_0, $g(x)Y_0$ satisfy equation (6) and thus $\mathrm{LP}\sqrt{f} < \infty$ implies $\mathrm{LP}\sqrt{h} < \infty$.

In order to prove that conditions (i)–(ii) are necessary, let us observe that for some l and suitably chosen signs we must have

$$\pm X_0 \pm \sqrt{h}\, gY_0 = \left(T + \sqrt{h}\, U\right)^l. \tag{8}$$

If $g_i \mid hU$, we have $(T, g_i) = 1$ because polynomials T, U satisfy (6). On the other hand,

$$\pm gY_0 = \sum_{i \geqslant 0} \binom{l}{2i+1} T^{l-2i-1} h^i U^{2i+1},$$

and thus g_i divides gY_0 in exactly the same power as it divides lT^lU. Hence condition (i).

If $g_i \nmid hU$, let r be any of the roots of g_i. Since polynomials X_0, Y_0 satisfy (7),

$$X_0^2 \equiv 1 \left(\mathrm{mod}\ (x-r)^{2\alpha_i}\right),$$

whence for some $\varepsilon = \pm 1$ we have

$$X_0 \equiv \varepsilon \left(\mathrm{mod}\ (x-r)^{2\alpha_i}\right). \tag{9}$$

From (8) and (9) it follows first of all that $T(r) + \sqrt{h(r)}\, U(r) = \zeta$ satisfies the cyclotomic equation $\Phi_n(x) = 0$ for some $n \mid 2l$. Since $T^2 - hU^2 = 1$, $T(r) - \sqrt{h(r)}\, U(r) = \zeta^{-1}$ satisfies the same equation. Therefore

$$(x - \zeta)(x - \zeta^{-1}) = x^2 - 2T(r)x + 1 \mid \Phi_n(x)$$

and the same divisibility holds for each root r of g_i. Since both polynomials g_i and Φ_n are irreducible, $\prod_{g_i(r)=0} \left(x^2 - 2T(r)x + 1\right)$ must be a power of $\Phi_n(x)$.

By comparing the degrees we obtain

$$\prod_{\substack{r \\ g_i(r)=0}} \left(x^2 - 2T(r)x + 1\right) = \Phi_n(x)^{2\gamma_i/\varphi(n)},$$

i.e. the first part of condition (ii).

Further it follows from (9) that

$$X_0^{(j)}(r) = 0 \quad (j = 1, 2, \ldots, 2\alpha_i - 1),$$

and since $g^{(j)}(r) = 0$ $(j = 1, 2, \ldots, \alpha_i - 1)$, $h(r) \neq 0$, we have

$$\left[\frac{d^j}{dx^j}\left(\pm X_0(x) \pm \sqrt{h(x)}\, g(x) Y_0(x)\right)\right]_{x=r} = 0 \quad (j = 1, 2, \ldots, \alpha_i - 1).$$

It follows from (8) by easy induction that

$$\left[\frac{d^j}{dx^j}\left(T(x)+\sqrt{h(x)}\,U(x)\right)\right]_{x=r}=0 \quad (j=1,2,\ldots,\alpha_i-1),$$

and hence $T^{(j)}(r)=0$ $(j=1,2,\ldots,\alpha_i-1)$, i.e.

$$T'(x)\equiv 0\left(\mathrm{mod}\,(x-r)^{\alpha_i-1}\right).$$

Since the last divisibility holds for each root r of g_i, we have

$$T'\equiv 0\left(\mathrm{mod}\,g_i^{\alpha_i-1}\right),$$

i.e. the second part of condition (ii).

It remains to prove that conditions (i)–(ii) are sufficient. Suppose therefore that they are fulfilled.

If $g_i \nmid hU$, denote by $n(i)$ the index of the cyclotomic polynomial that occurs in condition (ii) and let m be the least common multiple of all numbers $n(i)$. Define polynomials V, W by the identity

$$V+\sqrt{h}\,W=\left(T+\sqrt{h}\,U\right)^m. \tag{10}$$

In view of (ii) we have for each root r of $g_i \nmid hU$

$$\left(T(r)\pm\sqrt{h(r)}\,U(r)\right)^{n(i)}=1,$$

and thus for each root r of each $g_i \nmid hU$:

$$V(r)\pm\sqrt{h(r)}\,W(r)=1, \quad W(r)=0$$

and

$$W(x)\equiv 0\Big(\mathrm{mod}\prod_{g_i\nmid hU} g_i\Big). \tag{11}$$

Now since for all $g_i \nmid hU$, $T'\equiv 0\ (\mathrm{mod}\ g_i^{\alpha_i-1})$, we have $T^{(j)}(r)=0$ for each root r of g_i $(g_i \nmid hU,\ 1\leqslant j\leqslant \alpha_i-1)$. This, in view of $T^2-hU^2=1$, gives also

$$\left[\frac{d^j}{dx^j}\left(h(x)U^2(x)\right)\right]_{x=r}=0 \quad (j=1,2,\ldots,\alpha_i-1),$$

and since $h(r)U(r)\neq 0$,

$$\left[\frac{d^j}{dx^j}\left(\sqrt{h(x)}\,U(x)\right)\right]_{x=r}=0 \quad (j=1,2,\ldots,\alpha_i-1).$$

By identity (10) we get

$$\left[\frac{d^j}{dx^j}\left(\sqrt{h(x)}\,W(x)\right)\right]_{x=r}=0 \quad (j=1,2,\ldots,\alpha_i-1),$$

which, in view of (11) and since $h(r)\neq 0$, gives

$$W(x)\equiv 0\Big(\mathrm{mod}\prod_{g_i\nmid hU} g_i^{\alpha_i}\Big).$$

On the other hand, it follows from condition (i) and identity (10) that

$$W(x) \equiv 0\Big(\mathrm{mod} \prod_{g_i \mid hU} g_i^{\alpha_i}\Big),$$

so that $W(x) \equiv 0 \pmod{g(x)}$ and equation (7) has the solution $V(x)$, $W(x)/g(x)$, which completes the proof. □

Corollary. *If $h \neq 0$, $\mathrm{LP}(x-a)\sqrt{x^2-h} < \infty$ holds if and only if $a = 0$ or $h = \frac{4}{3}a^2$, $2a^2$ or $4a^2$.*

Proof. We have here $T(x) = 1-2x^2/h, U(x) = -2x/h$. Conditions (i)–(ii) take the shape

$$h \neq a^2$$

and

$$a = 0 \quad \text{or} \quad x^2 - 2\Big(1 - \frac{2a^2}{h}\Big)x + 1 = \Phi_1^2(x),\ \Phi_2^2(x) \text{ or } \Phi_3(x),\ \Phi_4(x),\ \Phi_6(x).$$

The last identity gives $1 - 2a^2/h = \pm 1, \pm\frac{1}{2}$ or 0, which leads to the four cases stated in the corollary. □

4.

Now we shall make some remarks about problem P_1 in the really important case where the polynomial f has no multiple factors. Suppose that $\mathrm{LP}\sqrt{f} = K$ and (2) holds, so that

$$T_{K-1}^2 - f(x)U_{K-1}^2 = (-1)^K,$$

and let T_{K-1} be of degree λ.

Applying the theorem of Abel to the function

$$T_{K-1}(x) + yU_{K-1}(x)$$

on the Riemann surface S defined by equation $y^2 = f(x)$, we find

$$\lambda \int_A^{P_2} w\,dx - \lambda \int_A^{P_1} w\,dx = \text{a period},$$

where $\int w\,dx$ is any integral of the first kind on S, A is an arbitrary place and P_1, P_2 are two places in infinity on S. Taking $A = P_1$ we get

$$\lambda \int_{P_1}^{P_2} w\,dx = \text{a period},$$

which means that

If $\mathrm{LP}\sqrt{f} < \infty$, then the value of $\int_{P_1}^{P_2} w\,dx$ is commensurable with the periods of the integral $\int w\,dx$, w being any integrand of the first kind.

For polynomials f of degree 4, the inverse of the above statement is also true, which has been known for a very long time ([2], Vol. II, p. 592). Furthermore, if r is the smallest

integer such that

$$r\int_{P_1}^{P_2}\frac{dx}{\sqrt{f(x)}} = \text{a period},$$

then LP $\sqrt{f} = r-1$ or $2(r-1)$. More precisely, r is the smallest integer $\geqslant 2$ such that

$$T_{r-2}^2(x) - f(x)U_{r-2}^2(x) = \mathrm{C} = \text{const}$$

and LP $\sqrt{f} = r-1$ or $2(r-1)$ if $\mathrm{C} = (-1)^{r-1}$ or not, respectively ([1]). According to Abel ([1], p. 213), if r is odd, we have necessarily $\mathrm{C} = 1$ and LP $\sqrt{f} = r-1$.

These statements in themselves do not form a solution of problem P_1 for polynomials of degree 4, since they do not supply any method of deciding whether the value of $\int_{P_1}^{P_2}\frac{dx}{\sqrt{f(x)}}$ is commensurable with the periods or not.

A method of deciding that was given by Chebyshev [8], and its justification was later furnished by Zolotarev [9].

Now, after the theory of rational points on curves of genus 1 has been developed, another method can be indicated, actually based on the same idea but leading to the end more rapidly. Without loss of generality we can assume that

$$f(x) = x^4 + 6\alpha_2 x^2 + 4\alpha_3 x + \alpha_4.$$

According to Halphen ([2], Vol. I, p. 120 and Vol. II, p. 591),

$$r\int_{P_1}^{P_2}\frac{dx}{\sqrt{f(x)}} = \text{a period}$$

if and only if

$$r\nu = \text{a period},$$

where if $\wp$ is the function of Weierstrass,

$$g_2 = 3\alpha_2^2 + \alpha_4, \quad g_3 = \alpha_2\alpha_4 - \alpha_2^3 - \alpha_3^2; \quad \wp(\nu; g_2, g_3) = -\alpha_2, \quad \wp'(\nu; g_1, g_3) = \alpha_3.$$

This means that the point $(-\alpha_2, \alpha_3)$ is exceptional of the order r on the cubic $y^2 = 4x^3 - g_2x - g_3$. Now, a method has been given by T. Nagell [3] which permits us not only to decide whether a given point is exceptional or not but also to find all exceptional points on a given cubic of Weierstrass. This method seems to work more rapidly than the method of Chebyshev, however, it is noteworthy that, with the use of completely different terminology, the first problem concerning exceptional points mentioned above was already solved by Chebyshev.

From known results regarding exceptional points further conclusions may be drawn regarding the functional LP $\sqrt{f}$, f of degree 4. It follows in particular that LP $\sqrt{f}$ can take the values 1, 2, 3, 4, 6, 8, 10, 14, 18, 22 and possibly also 5, 7, 9, 11 (I have not verified this) and, if the conjecture of Nagell [4] is true, no other values.

For polynomials f of degree > 4 I do not know any method which would always lead to the solution of problem P_1. However, the following rule solves the problem for almost all (in an adequate sense) polynomials f.

([1]) For a modern treatment see the paper [c1], in particular Corollary 3.

If LP $\sqrt{f} < \infty$, *then* f *is reducible in a certain quadratic field*.

The proof given below does not differ essentially from Chebyshev's proof [7] of an analogous theorem for polynomials f of degree 4.

Suppose that LP $\sqrt{f} < \infty$, (2) holds and s is the smallest integer $\geqslant 0$ such that

$$T_s^2 - f(x)U_s^2 = \mathrm{C}.$$

Since T_s, U_s have rational coefficients, C is rational. We have

$$f(x)U_s^2 = T_s^2 - \mathrm{C} = \big(T_s - \sqrt{\mathrm{C}}\big)\big(T_s + \sqrt{\mathrm{C}}\big).$$

c If $f(x)$ were irreducible in the field $\mathbb{Q}\big(\sqrt{\mathrm{C}}\big)$, we should have

$$\begin{aligned} &f(x) \mid T_s - \varepsilon\sqrt{\mathrm{C}} \quad (\varepsilon = 1 \text{ or } -1), \quad \text{whence} \\ &T_s - \varepsilon\sqrt{\mathrm{C}} = f(x)W^2, \quad T_s + \varepsilon\sqrt{\mathrm{C}} = V^2 \quad \text{and} \\ &V^2 - f(x)W^2 = 2\varepsilon\sqrt{\mathrm{C}}. \end{aligned} \tag{12}$$

In virtue of the theorem quoted in §1, one of the fractions V/W and $-V/W$ must be
c a convergent of expansion (2), and thus we have, for some $r \geqslant 0$: $\pm V/W = T_r/U_r$,

$$T_r^2 - fU_r^2 = \text{const}\,,$$

and the degree of T_r, equal to the degree of V, is less than the degree of T_s by (12). Since
c this is incompatible with the definition of s, $f(x)$ must be reducible in the field $\mathbb{Q}\big(\sqrt{\mathrm{C}}\big)$, which completes the proof. □

References

[1] N. H. Abel, *Über die Integration der Differential Formel* $\varrho\,dx/\sqrt{R}$ *wenn* R *und* ϱ *ganze Functionen sind*. J. Reine Angew. Math. 1 (1826), 185–221.

[2] G. H. Halphen, *Traité des fonctions elliptiques et de leurs applications*. Paris 1886–1891.

[3] T. Nagell, *Solution de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre*. Vid. Akad. Skrifter Oslo I, 1935, Nr. 1.

[4] —, *Problems in the theory of exceptional points on plane cubics of genus one*. In: Den 11te Skandinaviske Matematikerkongress (Trondheim 1949), Johan Grundt Tanums Forlag, Oslo 1952, 71–76.

[5] A. Schinzel, *On some problems of the arithmetical theory of continued fractions*. Acta Arith. 6 (1961), 393–413; this collection: B1, 131–148.

[6] H. Schmidt, *Zur Approximation und Kettenbruchentwicklung quadratischer Zahlen*. Math. Z. 52 (1950), 168–192.

[7] P. Tchebicheff, *Sur l'intégration des différentielles qui contiennent une racine carrée d'un polynome du troisième ou du quatrième degré*. J. Math. Pures Appl. (2) 2 (1857), 1–42.

[8] —, *Sur l'integration de la differentielle* $\dfrac{x + A}{\sqrt{x^4 + \alpha x^3 + \beta x^2 + \gamma x + \delta}}\,dx$. J. Math. Pures Appl. (2) 9 (1864), 225–246.

[9] G. Zolotareff, *Sur la méthode d'intégration de M. Tchebicheff*. J. Math. Pures Appl. (2) 19 (1874), 161–188.

Corrigendum*

Miss M. Lozach has pointed out an error in the proof of Theorem 2. Contrary to what is stated on the bottom of p. 152 the fundamental solution of the polynomial Pell equation $X^2 - f(x)Y^2 = \pm 1$ may be furnished not by the shortest period of the continued fraction expansion of $\sqrt{f(x)}$, but the shortest pseudoperiod. To be precise, if k is the least non-
c negative integer such that T_k/U_k is a convergent of the expansion of $\sqrt{f(x)}$ and for some constant c we have $T_k^2 - f(x)U_k^2 = c$ then the fundamental solution of the polynomial Pell equation is given by $T_k/\sqrt{|c|}$, $U_k/\sqrt{|c|}$, even though $k+1$ is not the length K of the shortest period of the said expansion. M. Lozach has proved (see [c1], Appendice, pp. 93–95) that in such a case $K = 2(k+1)$. This however has no influence on the validity of Theorem 2. Indeed we have then

$$T_{K-1} + U_{K-1}\sqrt{f(x)} = \left(\frac{T_k + U_k\sqrt{f(x)}}{\sqrt{c}}\right)^2$$

hence

$$2T_{K-1} = \frac{2T_k^2 + 2U_k^2 f(x)}{c} = \frac{4T_K^2 - 2c}{c} = \pm\left(\frac{2T_k}{\sqrt{|c|}}\right)^2 - 2$$

and if $2T_{K-1}(n)$ is not a rational integer, $2T_k/\sqrt{|c|}$ also is not. The argument given in the paper applies.

Reference

[c1] Y. Hellegouarch, M. Lozach, *Équation de Pell et points d'ordre fini*. In: Analytic and Elementary Number Theory (Marseille, 1983), Publ. Math. Orsay 86-1, Univ. Paris XI, Orsay 1986, 72–95.

* *Acta Arithmetica* XLVII (1986), 295.

Andrzej Schinzel
Selecta

Originally published in
Annali di Matematica pura ed applicata Serie IV
XCVIII (1974), 111–117

On two conjectures of P. Chowla and S. Chowla concerning continued fractions

To Professor Beniamino Segre on his 70-th birthday

Summary. The alternating sum of the partial quotients in the primitive period of a continued fraction expansion of $\sqrt{D}$ is determined mod 2 and mod 3.

Let D be a non-square positive integer and set

$$\sqrt{D} = b_0 + \overline{\frac{1}{\left| b_1 \right.} + \ldots + \frac{1}{\left| b_k \right.}} = [b_0, \overline{b_1, \ldots, b_k}],$$

where the bar denotes the primitive period,

$$\Sigma_D = b_k - b_{k-1} + \ldots + (-1)^{k-1} b_1.$$

P. Chowla and S. Chowla [1] have made among others the following conjectures:

if $D \equiv 3 \bmod 4$, $3 \nmid D$ then $\Sigma_D \equiv 0 \bmod 3$,

if p, q are primes, $p \equiv 3 \bmod 4$, $q \equiv 5 \bmod 8$ then

$$(-1)^{\Sigma_{pq}} = \left(\frac{p}{q}\right).$$

The aim of this paper is to prove two theorems which generalize the above conjectures (note that $D \equiv 3 \bmod 4$ implies $k \equiv 0 \bmod 2$).

Theorem 1. *If k is even, $3 \nmid D$ then $\Sigma_D \equiv 0 \bmod 3$.*

Theorem 2. $\Sigma_D \equiv v \bmod 2$, *where u, v is the least non-trivial solution of $U^2 - DV^2 = 1$. Moreover, let $2 \nmid D$, $k(D)$ be the square-free kernel of D and C any divisor of $2k(D)$ different from 1 and $-k(D)$ such that $U^2 - k(D)V^2 = C$ is soluble. If either $C \equiv 1 \bmod 2$ or each prime factor of D divides $k(D)$ then $\Sigma_D \equiv C + 1 \bmod 2$.*

Remark. If both conditions given in Theorem 2 for odd D are violated the conclusion may fail, e.g. for $D = 147 = 3 \cdot 7^2$ we have $\Sigma_D = 16 \equiv 0 \bmod 2$, although $u^2 - 3v^2 = -2$ is soluble.

Corollary 1. *If $D \not\equiv 0, 3, 7 \bmod 8$ then $\Sigma_D \equiv 0 \bmod 2$.*

Corollary 2. *If p is a prime, $p \equiv 3 \bmod 4$, α is odd then $\Sigma_{p^\alpha} \equiv 1 \bmod 2$.*

Corollary 3. *If p, q are primes, $p \equiv 3 \bmod 4$, $q \equiv 5 \bmod 8$, α, β are odd then*

$$(-1)^{\Sigma_{p^\alpha q^\beta}} = \left(\frac{p}{q}\right).$$

Proof is based on several known facts from the classical theory of continued fractions which we quote below in form of lemmata from the book of Perron [4]. First however we must recall Perron's notation. For a given regular continued fraction $[b_0, b_1, \ldots, b_n]$ the Muir symbol $K\begin{pmatrix} 1, 1, \ldots, 1 \\ b_0, b_1, b_2, \ldots, b_n \end{pmatrix}$ denotes its numerator A_n computed from the formulae

$$A_{-1} = 1, \quad A_0 = b_0, \quad A_\nu = b_\nu A_{\nu-1} + A_{\nu-2}.$$

Then we set

$$A_{\nu,\lambda} = K\begin{pmatrix} 1, \ldots, 1 \\ b_\lambda, b_{\lambda+1}, \ldots, b_{\lambda+\nu} \end{pmatrix}, \qquad A_{\nu,0} = A_\nu,$$
$$B_{\nu,\lambda} = K\begin{pmatrix} 1, \ldots, 1 \\ b_{\lambda+1}, b_{\lambda+2}, \ldots, b_{\lambda+\nu} \end{pmatrix}, \qquad B_{\nu,0} = B_\nu.$$

Lemma 1. *The following formulae hold*

(1) $$A_{\nu,\lambda} = b_{\nu+\lambda} A_{\nu-1,\lambda} + A_{\nu-2,\lambda},$$

(2) $$B_{\nu,\lambda} = A_{\nu-1,\lambda+1},$$

(3) $$A_{\nu,\lambda} = b_\lambda A_{\nu-1,\lambda+1} + B_{\nu-1,\lambda+1},$$

(4) $$A_{\nu,\lambda} B_{\nu-1,\lambda} - A_{\nu-1,\lambda} B_{\nu,\lambda} = (-1)^{\nu-1}.$$

Proof. (1) follows directly from the definition of $A_{\nu,\lambda}$. For the remaining formulae see [4] p. 15, formulae (25) and (29); p. 17, formula (35). □

Lemma 2. *If for all positive $\lambda < k$, $b_\lambda = b_{k-\lambda}$ then for all $\lambda \leqslant k/2$*

(5) $$B_{k-2\lambda,\lambda} = A_{k-2\lambda-1,\lambda}.$$

Proof. We have by definition

$$B_{k-2\lambda,\lambda} = K\begin{pmatrix} 1, \ldots, 1 \\ b_{\lambda+1}, b_{\lambda+2}, \ldots, b_{k-\lambda} \end{pmatrix}, \quad A_{k-2\lambda-1,\lambda} = K\begin{pmatrix} 1, \ldots, 1 \\ b_\lambda, b_{\lambda+1}, \ldots, b_{k-\lambda-1} \end{pmatrix}$$

and the lemma follows from the symmetry property of the Muir symbol ([4], p. 12). □

Lemma 3. *The symmetric part of the continued fraction*

$$\xi_0 = [b_0, \overline{b_1, b_2, \ldots, b_2, b_1, 2b_0}]$$

with period of length k being given, the necessary and sufficient condition for ξ_0 to be a quadratic root of an integer is that b_0 should have the form

(6) $$b_0 = \frac{m A_{k-2,1} - (-1)^k A_{k-3,1} B_{k-3,1}}{2},$$

where m is an integer. Then

$$\xi_0 = \sqrt{D} = \sqrt{b_0^2 + mA_{k-3,1} - (-1)^k B_{k-3,1}^2}\,.$$

Proof. See [4], p. 98, Satz 17. □

Proof of Theorem 1. If $D \not\equiv 0 \bmod 3$ then in the notation of Lemma 3

$$mA_{k-2,1} \equiv A_{k-3,1}A_{k-2,1} \bmod 3. \tag{7}$$

Indeed, it is clear if $A_{k-2,1} \equiv 0 \bmod 3$, otherwise we have

$$\begin{aligned} D &\equiv (-mA_{k-2,1} + A_{k-3,1}B_{k-3,1})^2 + mA_{k-3,1} - B_{k-3,1}^2 \\ &\equiv m^2 - 2mA_{k-2,1}A_{k-3,1}B_{k-3,1} + A_{k-3,1}^2 B_{k-3,1}^2 + mA_{k-3,1} - B_{k-3,1}^2 \bmod 3 \end{aligned}$$

and since by (4) and (5), for $\lambda = 1$, $\nu = k-2$,

$$A_{k-2,1}B_{k-3,1} = A_{k-3,1}^2 - 1$$

it follows

$$D \equiv \begin{cases} m^2 - 1 \bmod 3 & \text{if } A_{k-3,1} \equiv 0 \bmod 3, \\ m^2 + mA_{k-3,1} \bmod 3 & \text{if } A_{k-3,1} \not\equiv 0 \bmod 3. \end{cases}$$

Thus $DA_{k-2,1} \not\equiv 0 \bmod 3$ implies $m \equiv A_{k-3,1} \bmod 3$ and *a fortiori* the congruence (7). Since

$$\Sigma_D = 2b_0 - 2b_1 + \ldots + (-1)^{k/2-1}2b_{k/2-1} + (-1)^{k/2}b_{k/2},$$

in view of (6) and (7) it remains to show that

$$\begin{aligned} &\tfrac{1}{2}A_{k-3,1}(A_{k-2,1} - B_{k-3,1}) \\ &\qquad \equiv b_1 - b_2 + \ldots + (-1)^{k/2}b_{k/2-1} + (-1)^{k/2}b_{k/2} \bmod 3. \end{aligned} \tag{8}$$

This we prove by induction with respect to k. For $k = 2$

$$A_{k-3,1} = 1, \quad B_{k-3,1} = 0, \quad A_{k-2,1} = b_1$$

and (8) takes the form $-b_1 \equiv -b_1 \bmod 3$. Assume (8) is true for any symmetric sequence of positive integers $b_1, \ldots, b_{k-3}$ (k even $\geqslant 4$). We have by (1), (3) and (5)

$$\begin{aligned} A_{k-3,1} &= b_1A_{k-4,2} + B_{k-4,2} = b_1A_{k-4,2} + A_{k-5,2}, \\ A_{k-2,1} &= b_{k-1}A_{k-3,1} + A_{k-4,1} = b_1(b_1A_{k-4,2} + A_{k-5,2}) + b_1A_{k-5,2} + B_{k-5,2} \\ &= b_1^2A_{k-4,2} + 2b_1A_{k-5,2} + B_{k-5,2}; \end{aligned}$$

by (2) $B_{k-3,1} = A_{k-4,2}$. Hence

$$\begin{aligned}
&\tfrac{1}{2}A_{k-2,1}(A_{k-2,1} - B_{k-3,1}) \\
&\quad = \tfrac{1}{2}(b_1 A_{k-4,2} + A_{k-5,2})(b_1^2 A_{k-4,2} + 2b_1 A_{k-5,2} + B_{k-5,2} - A_{k-4,2}) \\
&\quad = \tfrac{1}{2}(b_1^3 A_{k-4,2}^2 + 3b_1^2 A_{k-4,2}A_{k-5,2} + b_1 A_{k-4,2}B_{k-5,2} \\
&\qquad - b_1 A_{k-4,2}^2 + 2b_1 A_{k-5,2}^2 + A_{k-5,2}B_{k-5,2} - A_{k-4,2}A_{k-5,2}) \\
&\quad \equiv b_1(-A_{k-4,2}B_{k-5,2} + A_{k-5,2}^2) + A_{k-5,2}(A_{k-5,2} - B_{k-5,2}) \bmod 3.
\end{aligned}$$

However, by (4) and (5)

$$b_1(-A_{k-4,2}B_{k-5,2} + A_{k-5,2}^2) \equiv b_1(-1)^{k-4} \equiv b_1 \bmod 3,$$

by the inductive assumption applied to the sequence $b_2, \ldots, b_{k-2}$

$$A_{k-5,2}(A_{k-4,2} - B_{k-5,2}) \equiv 2(b_2 - b_3 + \ldots) \equiv -b_2 + b_3 - \ldots + (-1)^{k/2} b_{k/2} \bmod 3$$

and (8) follows. □

Lemma 4. *If* $\sqrt{D} = [b_0, b_1, \ldots, b_{\nu-1}, \xi_\nu]$ *then*

$$\xi_\nu = \frac{\sqrt{D} + P_\nu}{Q_\nu},$$

where P_ν, Q_ν *are positive integers*

$$D - P_{\nu+1}^2 = Q_\nu Q_{\nu+1} \tag{9}$$

and for $\nu = 1, \ldots, k-1$

$$2 \leqslant Q_\nu \leqslant 2b_0. \tag{10}$$

Proof. See [4] p. 83, formula (5); p. 33, formulae (4), (5). □

Lemma 5. *If* k *is even,* $k = 2r$ *then*

$$2P_r = b_r Q_r, \tag{11}$$

$$2A_{r-1} = (B_{r-1}b_r + 2B_{r-2})Q_r, \tag{12_1}$$

$$B_{2r-1} = B_{r-1}(B_{r-1}b_r + 2B_{r-2}), \tag{12_2}$$

Q_r *is a divisor of* $(2A_{r-1}, 2D)$ *and*

$$Q_r\Big(\frac{2A_{r-1}}{Q_r}\Big)^2 - \frac{2D}{Q_r} \cdot 2B_{r-1}^2 = (-1)^r 4. \tag{13}$$

Proof. See [4] p. 107, formulae (9) and (10); p. 115, the third formula from below. □

Lemma 6. *If* D *is square-free there are exactly two values of* C *which divide* $2D$ *such that* $C \neq 1, -D$ *and* $U^2 - DV^2 = C$ *is soluble. The product of these two values of* C *equals* $-4D$ *when* D *is odd and* C *is even, in all other cases the product equals* $-D$.

Proof. See [3] p. 12, Theorem 11 part 3. □

Proof of Theorem 2. If k is odd then $U^2 - DV^2 = -1$ is soluble, $v \equiv 0 \bmod 2$ and $C \equiv 1 \bmod 2$. On the other hand $\Sigma_D = 2b_0$ thus $\Sigma_D \equiv v \equiv C + 1 \bmod 2$.

c If k is even, $k = 2r$ then

$$\Sigma_D = 2b_0 - 2b_1 + \ldots + (-1)^{r-1}2b_{r-1} + (-1)^r b_r \equiv b_r \bmod 2.$$

We have clearly $v = B_{2r-1}$ and we first prove $b_r \equiv B_{2r-1} \bmod 2$. Indeed, if $b_r \equiv 0 \bmod 2$ we have $B_{2r-1} \equiv 0 \bmod 2$ by (12_2). If $b_r \equiv 1 \bmod 2$ then by (11) $Q_r \equiv 0 \bmod 2$. If we had $B_{r-1} \equiv 0 \bmod 2$, (12_1) would give $2A_{r-1}/Q_r \equiv 0 \bmod 2$ and the left hand side of (13) would be divisible by 8. Therefore, $B_{r-1} \equiv 1 \bmod 2$ and by (12_2) $B_{2r-1} \equiv b_r \bmod 2$.

We now assume that D is odd.

If $Q_r \equiv 0 \bmod 2$ then by (9) applied for $\nu = r - 1$ it follows that $P_r \equiv 1 \bmod 2$ and by (11) $b_r \equiv 1 \bmod 2$. If $Q_r \equiv 1 \bmod 2$ then $b_r \equiv 0 \bmod 2$. Thus

$$\Sigma_D \equiv Q_r + 1 \bmod 2. \tag{14}$$

Let $Q_r = q^2 k(Q_r)$. By Lemma 5 $Q_r \mid 2D$ hence q is odd, $k(Q_r) \mid 2k(D)$. By (13)

$$(A_{r-1}/q)^2 - (D/q^2)B_{r-1}^2 = (-1)^r k(Q_r),$$

thus $U^2 - k(D)V^2 = (-1)^r k(Q_r)$ is soluble. By Lemma 6 we have the following possibilities

$$(-1)^r k(Q_r) = 1, \tag{15}$$

$$(-1)^r k(Q_r) = -k(D), \tag{16}$$

$$(-1)^r k(Q_r) = C,$$

$$(-1)^r k(Q_r) = \begin{cases} -k(D)C^{-1} & \text{if } C \equiv 1 \bmod 2, \\ -4k(D)C^{-1} & \text{if } C \equiv 0 \bmod 2. \end{cases}$$

If $C \equiv 1 \bmod 2$ then

$$Q_r \equiv k(Q_r) \equiv C \bmod 2. \tag{17}$$

c If each prime factor of D divides $k(D)$ then (15) and (16) are impossible. Indeed, then each odd prime factor of Q_r divides $k(D)$ hence if $Q_r = q^2$ it divides also D/Q_r. In view of (13) this implies $Q_r = 1$, contrary to (10). Also each odd prime factor of $2D/Q_r$ divides $k(D)$ hence if $Q_r = q^2 k(D)$ it divides also Q_r. In view of (13) this implies $Q_r = D > 2b_0$ again contrary to (10). Since

$$C \equiv \begin{cases} -k(D)C^{-1} \bmod 2 & \text{if } C \equiv 1 \bmod 2, \\ -4k(D)C^{-1} \bmod 2 & \text{if } C \equiv 0 \bmod 2, \end{cases}$$

we obtain again the congruence (17). The theorem follows from (14) and (17). □

Proof of Corollary 1. If $D \not\equiv 0, 3, 7 \bmod 8$ then $u^2 - Dv^2 \equiv 1 \bmod 8$ implies $v \equiv 0 \bmod 2$ thus $\Sigma_D \equiv v \equiv 0 \bmod 2$. □

Proof of Corollary 2. If $D = p^\alpha$ where p is a prime, $p \equiv 3 \bmod 4$, $\alpha \equiv 1 \bmod 2$ then each prime factor of D divides $k(D) = p$. The only divisors of $2p$ besides 1 and $-p$ are -1, ± 2, p and $\pm 2p$. However the equations

$$U^2 - pV^2 = -1, \quad U^2 - pV^2 = p$$

are impossible $\bmod p$ and p^2, respectively, because $(-1/p) = -1$.

Thus $C = \pm 2$ or $\pm 2p$ and $\Sigma_D \equiv C + 1 \equiv 1 \bmod 2$. □

Proof of Corollary 3. If $D = p^\alpha q^\beta$ where p, q are primes, $p \equiv 3 \bmod 4$, $q \equiv 5 \bmod 8$, $\alpha \equiv \beta \equiv 1 \bmod 2$ then each prime factor of D divides $k(D) = pq$. The only divisors of $2pq$ besides 1 and $-pq$ are $-1, \pm 2, \pm p, \pm 2p, \pm q, \pm 2q, pq, \pm 2pq$.

The equations

$$U^2 - pqV^2 = -1, \quad U^2 - pqV^2 = pq$$

are impossible $\bmod p$ and p^2, respectively, because $(-1/p) = -1$.

The equations

$$U^2 - pqV^2 = \pm 2, \quad U^2 - pqV^2 = \pm 2pq$$

are impossible $\bmod q$ and q^2, respectively, because $(\pm 2/q) = -1$.

If $(p/q) = 1$ the equations

$$U^2 - pqV^2 = \pm 2p, \quad U^2 - pqV^2 = \pm 2q$$

are impossible $\bmod q$ and q^2, respectively, because $(\pm 2p/q) = -1$.

Then $C = \pm p$ or $\pm q$ and $\Sigma_D \equiv C + 1 \equiv 0 \bmod 2$.

If $(p/q) = -1$ the equations

$$U^2 - pqV^2 = \pm p, \quad U^2 - pqV^2 = \pm q$$

are impossible $\bmod q$ and q^2, respectively.

Then $C = \pm 2p$ or $\pm 2q$ and $\Sigma_D \equiv C + 1 \equiv 1 \bmod 2$. □

Remark. The congruence $\Sigma_D \equiv v \bmod 2$ has been suggested to me by H. Lang, who established a similar congruence for the relevant Dedekind sums (see his forthcoming paper [2]).

References

[1] P. Chowla, S. Chowla, *Problems on periodic simple continued fractions*. Proc. Nat. Acad. Sci. U.S.A. 69 (1972), 3745.

[2] H. Lang, *Über die Klassenzahlen eines imaginären bizyklischen biquadratischen Zahlkörpers und seines reell-quadratischen Teilkörpers* I. J. Reine Angew. Math. 262/263 (1973), 18–40.

[3] T. Nagell, *Contributions to the theory of a category of Diophantine equations of the second degree with two unknowns*. Nova Acta Soc. Sci. Upsal. (4) 16 (1955), no. 2.

[4] O. Perron, *Die Lehre von den Kettenbrüchen*. Zweite Auflage, reprinted by Chelsea, New York 1950.

Part C

Algebraic number theory

Commentary on C: Algebraic numbers

by David W. Boyd and D. J. Lewis

C1, **C6**, **C10**

If α is an algebraic integer of degree d, with conjugates $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_d$, define

$$\boxed{\alpha} = \max_i |\alpha_i|, \quad M(\alpha) = \prod \max(1, |\alpha_i|) \leqslant \boxed{\alpha}^d,$$

known as the "house" and "Mahler measure" of α, respectively.

In **C1**, the authors proved that there is no α having $2s > 0$ complex conjugates for which

$$1 < \boxed{\alpha} < 1 + 4^{-s-2}$$

and no totally real α for which

$$2 < \boxed{\alpha} < 2 + 4^{-2d-3}.$$

Implicitly they asked if there existed an absolute constant $c > 0$ such that, if α is not a root of unity, then

$$\boxed{\alpha} > 1 + c/d.$$

An affirmative answer to this question has come to be known as the Schinzel–Zassenhaus conjecture.

This is related to a question of D. H. Lehmer [17] who asked if there is an absolute constant $C > 1$ such that

$$M(\alpha) > C,$$

for every non-zero algebraic integer α, not a root of unity. An affirmative answer to this question has come to be known as Lehmer's conjecture. It is clear that Lehmer's conjecture implies the Schinzel–Zassenhaus conjecture (with $c = \log C$), but not conversely.

An extensive literature has been developed seeking to answer these two questions and related ones. R. Breusch [4] proved Lehmer's conjecture for α which are non-reciprocal, i.e. α and α^{-1} are not conjugate, showing that $M(\alpha) \geqslant c_0$ for such α, where $c_0 = 1.1796\ldots$ is the positive zero of the polynomial $x^3 - x^2 - 1/4$. Lehmer had already given an example of a reciprocal α of degree 10 for which $M(\alpha) = \sigma_0 = 1.1762\ldots$ which combines with Breusch's result to show that the extremal examples for Lehmer's conjecture must be

reciprocal. C. Smyth [27] proved a sharp form of Lehmer's conjecture for non-reciprocal α by proving $M(\alpha) \geqslant \theta_0$, where $\theta_0 = 1.3247\ldots$ is the positive zero of the polynomial $x^3 - x - 1$.

Computational evidence obtained by Boyd [3] strongly suggests that, in contrast to Lehmer's question, the extremal examples for the Schinzel–Zassenhaus question are *non-reciprocal* and indeed that for $d = 3k$ the minimum of $\boxed{\alpha}$ is attained for a root of $x^{3k} + x^{2k} - 1$, suggesting that the Schinzel–Zassenhaus conjecture is true with the best possible constant being $(3/2)\log\theta_0 = 0.4217\ldots$. Smyth's inequality $M(\alpha) \geqslant \theta_0$ implies that $\boxed{\alpha} \geqslant 1 + \log\theta_0/d$, for non-reciprocal α, where $\log\theta_0 = 0.2811\ldots$. A. Dubickas [9] has improved the constant to $0.3096\ldots$ for sufficiently large d.

For reciprocal α, the best results concerning either conjecture are elaborations on the fundamental result of E. Dobrowolski [7] who showed that there is a explicit constant $a > 0$ such that if α is not a root of unity and of degree d, then

$$M(\alpha) > 1 + a\left(\frac{\log\log d}{\log d}\right)^3.$$

R. Louboutin [20] has shown that for sufficiently large d, $a = 9/4 - \varepsilon$ suffices. This would imply that

$$\boxed{\alpha} > 1 + \frac{a}{d}\left(\frac{\log\log d}{\log d}\right)^3,$$

with $a = 9/2 - \varepsilon$. A. Dubickas [8] has improved the constant in this latter inequality from $9/2 = 4.5$ to $64/\pi^2 = 6.4845\ldots$.

If $P(x)$ is the minimal polynomial of α then one defines $M(P) = M(\alpha)$. Then Smyth's inequality states that for non-reciprocal polynomials with integral coefficients, $M(P) \geqslant \theta_0$. In paper **C6**, Schinzel generalizes Smyth's inequality to polynomials $P(x)$ with coefficients in a totally real number field K. He shows that if $k = [K : \mathbb{Q}]$ and $P(x) = P_1(x), \ldots, P_k(x)$ are the conjugates of the non-reciprocal polynomial $P(x)$ then

$$\max_{1\leqslant j\leqslant k} M(P_j) \geqslant \theta_0.$$

Furthermore, one has

$$\prod_{1\leqslant j\leqslant k} M(P_j) \geqslant \left(\frac{1+\sqrt{5}}{2}\right)^{k/2}.$$

He applies this to give an upper bound for the number of non-reciprocal, irreducible factors of a polynomial with coefficients in a totally real algebraic number field or a totally complex extension of such a field.

The Mahler measure $\beta = M(\alpha)$ is an algebraic integer. It is an interesting question to decide for a given algebraic integer β whether or not it is of the form $M(\alpha)$ for some α. The definitive work on this question is the recent paper by J. Dixon and A. Dubickas [6]. Among the questions that they were unable to answer in their paper was whether or not $\beta = 3(3+\sqrt{5})/2$ is the Mahler measure of some α. In the paper **C10**, Schinzel answers this and other questions raised in the paper of Dixon and Dubickas. He shows that if

p is a prime then $p(3+\sqrt{5})/2$ is a Mahler measure if and only if $p=2$, $p=5$ or $p \equiv \pm 1 \pmod 5$.

C2, **C3**, **C5**

In [5], H. Davenport, D. J. Lewis and A. Schinzel made use of a theorem of M. Bauer [1] to prove: *If K is a normal extension of $\mathbb{Q}$ and $\mathcal{N} = \{N_{K/\mathbb{Q}}(\omega) \mid \omega \in K\}$ and $f(x) \in \mathbb{Q}[x]$ has the property that every arithmetic progression in $\mathbb{Z}$ contains an integer a such that $f(a) \in \mathcal{N}$, then $f(x) = N_{K/\mathbb{Q}}(\varphi(x))$, for some $\varphi \in K[x]$.*

If K is a number field, let $\mathcal{P}(K)$ denote the set of rational primes which have a first degree prime ideal of K as a factor. The theorem of Bauer asserts: If K, H are number fields such that $\mathcal{P}(H) \subset \mathcal{P}(K)$ with possibly a finite number of exceptions, and if K is normal, then $K \subset H$. If K is not normal, the conclusion need not hold, indeed F. Gassmann [10] exhibited two non-conjugate fields H, K of degree 180 for which $\mathcal{P}(H) = \mathcal{P}(K)$.

Schinzel had observed that it was sufficient for the proof of the polynomial problem to know that a conjugate of K lie in H. He defined K to be a Bauerian field if $\mathcal{P}(H) \subset \mathcal{P}(K)$, with possibly a finite number of exceptions, implies some conjugate K^σ of K lie in H. These three papers provide various criteria for a field to be Bauerian and then prove various theorems when the set of values of a polynomial, in one or more variables, might determine the shape of the polynomial.

J. Wójcik [31] extended the class of fields that are Bauerian to include quasi-normal fields, i.e. fields whose normal closure is the composite of any two of its conjugates.

C4

Let β be a cyclotomic integer so that β is representable as a sum of roots of unity. In this paper, Schinzel answers a question of R. M. Robinson [25], by showing that a cyclotomic integer of degree d is a sum of n roots of unity only if it is a sum of n roots of unity all of common degree less than an explicitly given function $c(d, n)$ of d and n only. In a footnote to this paper Schinzel indicates that one could obtain a better estimate by use of a theorem of Henry Mann [22]. This was done by J. H. Loxton [21].

Timo Ojala [24] refines Corollary 5, showing that if $|\overline{\beta}|^2 < 6$, then β is the sum of at most 3 roots of unity or belongs to one of three infinite sets of equivalent numbers ($\alpha \sim \beta$ if $\alpha\beta^{-1}$ = root of identity) or one of a finite set.

C7

A finite extension L/K is a radical extension provided there is a group C and integer n such that $K^\times \subset C \subset L^\times$, $C^n \subseteq K^\times$ for some n, and $L = K(C)$. Further, if K contains the n-th roots of unity and $(n, \text{char } K) = 1$, then L/K is a Kummer extension and

$$[C : K^\times] = [L : K] = [C^n : K^n]$$

and further the groups $C/K^\times$ and $Gal(L/K)$ are isomorphic and there exists a bijection between the subgroups of $C/K^\times$ and the subfields of L containing K. These conditions fail for most radical extensions.

In this paper, Schinzel gave necessary and sufficient conditions for radical extensions to have $[C : K^\times] = [L : K]$. See also Kneser [14]. Schinzel's paper [26] should be viewed as an extension of this paper. F. Halter-Koch [11] gave necessary and sufficient

conditions for a radical extension to satisfy $[L : K] = [C^n : K^n]$. The essential ingredient in these papers is the location of the roots of unity with respect to K. In [12] Halter-Koch explored conditions for radical extensions L/K that imply if $L \supset E \supset K$ then there exists a subgroup $C_1 \subset C$ such that E is conjugate to $K(C_1)$.

C8

For a finite abelian group A denote by $r_2(A)$ the 2-rank of A, i.e. the number of cyclic direct summands of the Sylow 2-subgroup of A. Let O_F be the ring of integers of the number field F and let K_2 denote the functor of Milnor. The authors provide an explicit formula for $r_2(K_2 O_F)$ in the case when F is a quadratic field. If $F = \mathbb{Q}(\sqrt{D})$, where D square-free has t odd prime factors and 2^s is the number of elements of the set $\{\pm 1, \pm 2\}$ that are norms of an element of F, then they proved that

$$r_2(K_2 O_F) = \begin{cases} t + s, & \text{if } D \geq 2, \\ t + s - 1, & \text{if } D \leq -1. \end{cases}$$

Browkin and Schinzel derived from the obtained formulas some results on the structure of the Sylow 2-subgroup of $K_2 O_F$ and gave an explicit form of elements of order 2 in this group. The formula has been used extensively in many papers concerning the Sylow 2-subgroup of $K_2(O_F)$ as well as it was generalized and extended in many ways. In particular, results of the paper **C8** implied the correctness of the Birch–Tate formula for the order of $K_2 O_F$ for infinitely many real quadratic fields; e.g. J. Hurrelbrink [13], M. Kolster [15] and J. Urbanowicz [29]. The Birch–Tate conjecture asserts for a totally real field E,

$$\operatorname{card}(K_2 \mathcal{O}_E) = 2\,|\zeta_E(-1)| \prod_p p^{n(p)},$$

where ζ_E is the Dedekind zeta function for E and $n(p)$ is the largest integer $n \geq 0$ such that $\mathbb{Q}(\zeta_{p^n})^+ \subset E$. See B. J. Birch [2] and J. Tate [28]. B. Mazur and A. Wiles [23] (see also A. Wiles [30]) have shown that the Birch–Tate conjecture is true for totally real abelian E. The Birch–Tate conjecture is a special case of the conjecture of S. Lichtenbaum [18].

C9

I. Korec [16] defined a K-system to be a vector $(\alpha_1, \ldots, \alpha_m)$ of positive real numbers for which there are nonnegative integers c_{ijk} satisfying $\alpha_i \alpha_j = \sum_{k=1}^{m} c_{ijk} \alpha_k$ for all $1 \leqslant i, j \leqslant m$. He called α a K-number if there is a K-system and nonnegative integers a_k such that $\alpha = \sum_{k=1}^{m} a_k \alpha_k$. Korec proved that K-numbers are algebraic integers. Here Schinzel proves that a nonnegative real number α is a K-number if and only if it is an algebraic integer and it is not less in absolute value than any of its conjugates. In Lemma 4, he shows that if α is a K-number there is an exponent e for which α^e is a Perron number, that is a positive algebraic integer which is strictly larger than the absolute value of any other conjugate. The terminology is due to D. Lind [19], who showed that these algebraic integers are exactly those occurring as the spectral radii of irreducible non-negative integral matrices.

References

[1] M. Bauer, *Zur Theorie der algebraischen Zahlkörper*. Math. Ann. 77 (1916), 353–356.

[2] B. J. Birch, *K_2 of global fields*. In: 1969 Number Theory Institute, Proc. Sympos. Pure Math. 20, Amer. Math. Soc., Providence 1971, 87–95.

[3] D. W. Boyd, *The maximal modulus of an algebraic integer*. Math. Comp. 45 (1985), 243–249.

[4] R. Breusch, *On the distribution of the roots of a polynomial with integral coefficients*. Proc. Amer. Math. Soc. 2 (1951), 939–941.

[5] H. Davenport, D. J. Lewis, A. Schinzel, *Polynomials of certain special types*. Acta Arith. 9 (1964), 107–116; this collection: A6, 27–35.

[6] J. D. Dixon, A. Dubickas, *The values of Mahler measures*. Mathematika 51 (2004), 131–148.

[7] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*. Acta Arith. 34 (1979), 391–401.

[8] A. Dubickas, *On a conjecture of A. Schinzel and H. Zassenhaus*. Acta Arith. 63 (1993), 15–20.

[9] —, *The maximal conjugate of a non-reciprocal algebraic integer*. Liet. Mat. Rink. 37 (1997), 168–174; Lithuanian Math. J. 37 (1997), 129–133.

[10] F. Gassmann, *Bemerkungen zu der vorstehenden Arbeit von Hurwitz*. Math. Z. 25 (1926), 665–675.

[11] F. Halter-Koch, *Über Radikalerweiterungen*. Acta Arith. 36 (1980), 43–58.

[12] —, *Eine Galoiskorrespondenz für Radikalerweiterungen*. J. Algebra 63 (1980), 318–330.

[13] J. Hurrelbrink, *$K_2(\mathcal{O})$ for two totally real fields of degree three and four*. In: Algebraic K-theory, Part I, Lecture Notes in Math. 966, Springer, Berlin 1982, 112–114.

[14] M. Kneser, *Lineare Abhängigkeit von Wurzeln*. Acta Arith. 26 (1975), 307–308.

[15] M. Kolster, *On the Birch–Tate conjecture for maximal real subfields of cyclotomic fields*. In: Algebraic K-theory, Number Theory, Geometry and Analysis, Lecture Notes in Math. 1046, Springer, Berlin 1984, 229–234.

[16] I. Korec, *Irrational speeds of configuration growth in generalized Pascal triangles*. Theoret. Comput. Sci. 112 (1993), 399–412.

[17] D. H. Lehmer, *Factorization of certain cyclotomic functions*. Ann. of Math. (2) 34 (1933), 461–479.

[18] S. Lichtenbaum, *On the values of zeta and L-functions*. Ann. of Math. (2) 96 (1972), 338–360.

[19] D. A. Lind, *The entropies of topological Markov shifts and a related class of algebraic integers*. Ergodic Theory Dynam. Systems 4 (1984), 283–300.

[20] R. Louboutin, *Sur la mesure de Mahler d'un nombre algébrique*. C. R. Acad. Sci. Paris Sér. I Math. 296 (1983), 707–708.

[21] J. H. Loxton, *On two problems of R. W. Robinson about sums of roots of unity*. Acta Arith. 26 (1974/75), 159–174.

[22] H. B. Mann, *On linear relations between roots of unity*. Mathematika 12 (1965), 107–117.

[23] B. Mazur, A. Wiles, *Class fields of abelian extensions of $\mathbb{Q}$*. Invent. Math. 76 (1984), 179–330.

[24] T. Ojala, *S*ums of roots of unity. Math. Scand. 37 (1975), 83–104.

[25] R. M. Robinson, *Intervals containing infinitely many sets of conjugate algebraic integers*. In: Studies in Mathematical Analysis and Related Topics, Essays in Honor of George Pólya, Stanford Univ. Press, Stanford 1962, 305–315.

[26] A. Schinzel, *Abelian binomials, power residues and exponential congruences*. Acta Arith. 32 (1977), 245–274; *Addendum*, ibid. 36 (1980), 101–104; this collection: H5, 939–970.

[27] C. J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*. Bull. London Math. Soc. 3 (1971), 169–175.

[28] J. Tate, *Symbols in Arithmetic*. In: Actes du Congrès International des Mathèmaticiens (Nice 1970), t. I, Gauthier–Villars, Paris 1971, 201–211.

[29] J. Urbanowicz, *On the* 2*-primary part of a conjecture of Birch and Tate*. Acta Arith. 43 (1983), 69–81.

[30] A. Wiles, *The Iwasawa conjecture for totally real fields*. Ann. of Math. (2) 131 (1990), 493–540.

[31] J. Wójcik, *A purely algebraic proof of special cases of Tchebotarev's theorem*. Acta Arith. 28 (1976/77), 137–145.

Andrzej Schinzel
Selecta

Originally published in
Michigan Mathematical Journal 12 (1965), 81–85

A refinement of two theorems of Kronecker

with H. Zassenhaus (*Columbus*)

Kronecker [1] proved in 1857 that if an algebraic integer α different from zero is not a root of unity, then at least one of its conjugates has absolute value greater than 1. He proved also that if α is a totally real algebraic integer and $\alpha \neq 2\cos\rho\pi$ (ρ rational), then at least one of its conjugates has absolute value greater than 2. The aim of this paper is to refine the above statements as follows.

Theorem 1. *If an algebraic integer $\alpha \neq 0$ is not a root of unity, and if $2s$ among its conjugates α_i $(i = 1, \ldots, n)$ are complex, then*

$$\max_{1\leqslant i\leqslant n} |\alpha_i| > 1 + 4^{-s-2}. \tag{1}$$

Theorem 2. *If a totally real algebraic integer β is different from $2\cos\rho\pi$ (ρ rational), and $\{\beta_i\}$ $(i = 1, \ldots, n)$ is the set of its conjugates, then*

$$\max_{1\leqslant i\leqslant n} |\beta_i| > 2 + 4^{-2n-3}. \tag{2}$$

It would be possible to improve 4^{-s-2} and 4^{-2n-3} on the right hand side of inequalities (1) and (2) by constant factors. This, however, seems of no interest, since probably the order of magnitude of

$$\max_{1\leqslant i\leqslant n} |\alpha_i| - 1 \quad \text{and} \quad \max_{1\leqslant i\leqslant n} |\beta_i| - 2$$

is much greater than that given by (1) and (2), respectively. In fact, for α satisfying the assumptions of Theorem 1, we cannot disprove the inequality

$$\max_{1\leqslant i\leqslant n} |\alpha_i| > 1 + \frac{c}{n}, \tag{3}$$

where $c > 0$ is an absolute constant.

Such a disproof would give an affirmative answer to a question of D. H. Lehmer ([2], p. 476), open since 1933, namely, whether to every $\varepsilon > 0$ there corresponds an algebraic integer α such that

$$1 < \prod_{i=1}^{n} \max\bigl(1, |\alpha_i|\bigr) < 1 + \varepsilon.$$

Inequality (3), if true, is the best possible, as the example $\alpha = 2^{1/n}$ shows. Concerning inequality (2), we observe that there exist totally real algebraic integers, not of the form $2\cos\rho\pi$ (ρ rational), for which

$$\max_{1\leqslant i\leqslant n}\big\{|\beta_i| - 2\big\}$$

is arbitrarily small. This follows from a theorem of R. M. Robinson [3], according to which there are infinitely many systems of conjugate totally real algebraic integers in every interval of length greater than 4, in particular, in $[-2+\varepsilon, 2+2\varepsilon]$, for every $\varepsilon > 0$.

In the subsequent proof of Theorem 1 we make frequent use of the following inequalities, valid for all positive integers m:

$$(1+x)^m < \frac{1}{1-mx} \quad \Big(0 < x < \frac{1}{m}\Big), \tag{4}$$

$$\Big(1+\frac{1}{y}\Big)^{1/m} > 1 + \frac{1}{m(y+1)} \quad (0 < y). \tag{5}$$

Proof of Theorem 1. Let α_i be real for $i = 1, \dots, r$ and complex for $i = r+1, \dots, \dots, r+2s = n$ with $\alpha_i = \overline{\alpha_{i+s}}$ $(i = r+1, \dots, r+s)$. Let

$$|\alpha_\mu| = \max_{1\leqslant i\leqslant n} |\alpha_i| \geqslant 1.$$

Suppose first that $\mu \leqslant r$. If $|\alpha_i^2 - 1| \geqslant 1$ for some $i \leqslant r$, then $\alpha_i^2 \geqslant 2$, hence

$$|\alpha_\mu| \geqslant |\alpha_i| \geqslant \sqrt{2} \geqslant 1 + 4^{-s-2}.$$

If $|\alpha_i^2 - 1| < 1$, for all $i \leqslant r$, then, noting that $|\alpha_\mu^2 - 1| = |\alpha_\mu|^2 - 1$ and $|\alpha_i^2 - 1| \leqslant |\alpha_\mu|^2 + 1$ $(r < i \leqslant r+2s)$, we deduce from (4) that either

$$\prod_{i=1}^{n} |\alpha_i^2 - 1| \leqslant \big(|\alpha_\mu|^2 - 1\big)\big(|\alpha_\mu|^2 + 1\big)^{2s}$$
$$\leqslant \big(|\alpha_\mu|^2 - 1\big)2^{2s}\Big(1 + \frac{|\alpha_\mu|^2 - 1}{2}\Big)^{2s} \leqslant 2^{2s}\,\frac{|\alpha_\mu|^2 - 1}{1 - s\big(|\alpha_\mu|^2 - 1\big)}$$

or

$$s\big(|\alpha_\mu|^2 - 1\big) \geqslant 1.$$

In the second case, (5) implies that

$$|\alpha_\mu| \geqslant \Big(1 + \frac{1}{s}\Big)^{1/2} > 1 + \frac{1}{2(s+1)} > 1 + 4^{-s-2}.$$

Since no α_i is a root of unity, $\prod_{i=1}^n |\alpha_i^2 - 1|$ is a positive integer. Thus in the first case $s\big(|\alpha_\mu|^2 - 1\big) \leqslant 1$, and so

$$1 - s\big(|\alpha_\mu|^2 - 1\big) \leqslant 2^{2s}\big(|\alpha_\mu|^2 - 1\big).$$

But then by (5)

$$|\alpha_\mu| \geqslant \Big(1 + \frac{1}{s + 2^{2s}}\Big)^{1/2} > 1 + \frac{1}{2(s + 2^{2s} + 1)} > 1 + 4^{-s-2}.$$

Next, suppose $r < \mu \leqslant r+s$. Let $\alpha_\mu = |\alpha_\mu| e^{2\pi i\theta}$. By Dirichlet's approximation theorem, there exist integers p and q such that

$$|2\theta q - p| < \frac{1}{9\cdot 2^{s-1}} \quad \text{and} \quad 1 \leqslant q \leqslant 9\cdot 2^{s-1}. \tag{6}$$

Hence

$$|4q\theta\pi - 2\pi p| < \frac{2\pi}{9\cdot 2^{s-1}} < 2^{-s+1/2}$$

and

$$\cos 4q\theta\pi > \cos 2^{-s+1/2} > 1 - \tfrac{1}{2}(2^{-s+1/2})^2 = 1 - 2^{-2s}.$$

This gives the estimate

$$\begin{aligned} \left|(\alpha_\mu^{2q}-1)(\alpha_{\mu+s}^{2q}-1)\right| &= |\alpha_\mu|^{4q} - (\alpha_\mu^{2q} + \overline{\alpha}_\mu^{2q}) + 1 \\ &= |\alpha_\mu|^{4q} - 2|\alpha_\mu|^{2q}\cos 4q\theta\pi + 1 \\ &\leqslant |\alpha_\mu|^{4q} - 2|\alpha_\mu|^{2q}(1-2^{-2s}) + 1. \end{aligned} \tag{7}$$

If $|\alpha_i^{2q}-1| \geqslant 1$, for some $i \leqslant r$, then $|\alpha_\mu|^{2q} \geqslant |\alpha_i|^{2q} \geqslant 2$. Hence, by (5) and (6),

$$|\alpha_\mu| \geqslant 2^{1/2q} \geqslant 2^{-9\cdot 2^s} \geqslant 1 + 9^{-1}2^{-s-1} > 1 + 4^{-s-2}.$$

If $|\alpha_i^{2q}-1| < 1$, for all $i \leqslant r$, we use (4) and (7) and obtain the inequality

$$\begin{aligned} \prod_{i=1}^{n} |\alpha_i^{2q}-1| &\leqslant \left\{|\alpha_\mu|^{4q} - 2|\alpha_\mu|^{2q}(1-2^{-2s}) + 1\right\}\left(|\alpha_\mu|^{2q}+1\right)^{2s-2} \\ &\leqslant \left\{|\alpha_\mu|^{4q} - 2(1-2^{-2s})|\alpha_\mu|^{2q} + 1\right\}\frac{2^{2s-2}}{1-(s-1)\left(|\alpha_\mu|^{2q}-1\right)}, \end{aligned}$$

or

$$(s-1)\left(|\alpha_\mu|^{2q}-1\right) \geqslant 1.$$

In the second case, using (5) and (6), we obtain the estimate

$$|\alpha_\mu| \geqslant 1 + \frac{1}{2qs} \geqslant 1 + \frac{1}{9s\cdot 2^s} > 1 + 4^{-s-2}.$$

If the second case does not occur, then $1-(s-1)\left(|\alpha_\mu|^{2q}-1\right) > 0$. Since no α_i is a root of unity, $\prod_{i=1}^{n}|\alpha_i^{2q}-1|$ is a positive integer. Thus

$$2^{2s-2}\left\{|\alpha_\mu|^{4q} - 2(1-2^{-2s})|\alpha_\mu|^{2q} + 1\right\} \geqslant 1 - (s-1)\left(|\alpha_\mu|^{2q}-1\right),$$

hence

$$|\alpha_\mu^{2q}|^2 - |\alpha_\mu|^{2q}\left(2 - \frac{2s-1}{2^{2s-1}}\right) + \left(1 - \frac{s}{2^{2s-2}}\right) \geqslant 0.$$

Since $|\alpha_\mu^{2q}| \geqslant 1$ and

$$1 - \left(2 - \frac{2s-1}{2^{2s-1}}\right) + \left(1 - \frac{s}{2^{2s-2}}\right) = -2^{-2s+1} < 0,$$

it follows that

$$|\alpha_\mu|^{2q} \geqslant 1 - (2s-1)2^{-2s} + \sqrt{\left\{1-(2s-1)2^{-2s}\right\}^2 - (1 - s\cdot 2^{-2s+2})}$$
$$= 1 + \frac{1}{s - \frac{1}{2} + \sqrt{2^{2s-1} + \left(s-\frac{1}{2}\right)^2}}\,.$$

Now (6) implies that

$$2q\left(s + \tfrac{1}{2} + \sqrt{2^{2s-1} + \left(s-\tfrac{1}{2}\right)^2}\right) \leqslant 9\cdot 2^s\left(s + \tfrac{1}{2} + \sqrt{2^{2s-1} + \left(s-\tfrac{1}{2}\right)^2}\right) < 4^{s+2}.$$

It follows from (5) and the last two inequalities that

$$|\alpha_\mu| \geqslant 1 + \frac{1}{2q\left(s + \frac{1}{2} + \sqrt{2^{2s-1} + \left(s-\frac{1}{2}\right)^2}\right)} > 1 + 4^{-s-2}.$$

This completes the proof of Theorem 1. □

Proof of Theorem 2. Let β be a totally real algebraic integer satisfying the assumptions of the theorem, and put

$$\alpha = \beta/2 + \sqrt{(\beta/2)^2 - 1}\,.$$

Then α is an algebraic integer and $\alpha^2 - \beta\alpha + 1 = 0$. All the conjugates of α are zeros of polynomials $g_i(x) = x^2 - \beta_i x + 1$ $(i = 1, 2, \ldots, n)$. At most $2n-2$ of them are complex, since otherwise $|\beta_i| \leqslant 2$, contrary to the original theorem of Kronecker. Thus α is not a root of unity, and by Theorem 1,

$$\max_{1\leqslant j\leqslant 2n} |\alpha^{(j)}| \geqslant 1 + 4^{-n-1}.$$

The complex conjugates of α have absolute value 1. It follows that for some $i \leqslant n$,

$$|\beta_i|/2 + \sqrt{|\beta_i/2|^2 - 1} > 1 + 4^{-n-1} > |\beta_i|/2 - \sqrt{|\beta_i/2|^2 - 1}\,,$$

hence $g_i\left(\operatorname{sgn}\beta_i(1+4^{-n-1})\right) < 0$. But then

$$|\beta_i| > (1+4^{-n-1}) + \frac{1}{1+4^{-n-1}} > 1 + 4^{-n-1} + 1 - 4^{-n-1} + 4^{-2n-3} = 2 + 4^{-2n-3}.$$

This completes the proof. □

References

[1] L. Kronecker, *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten*. J. Reine Angew. Math. 53 (1857), 173–175.

[2] D. H. Lehmer, *Factorization of certain cyclotomic functions*. Ann. of Math. (2) 34 (1933), 461–479.

[3] R. M. Robinson, *Intervals containing infinitely many sets of conjugate algebraic integers*. In: Studies in Mathematical Analysis and Related Topics, Essays in Honor of George Pólya, Stanford Univ. Press, Stanford 1962, 305–315.

Originally published in
Acta Arithmetica XI (1966), 333–344

On a theorem of Bauer and some of its applications

1.

For a given algebraic number field K let us denote by $P(K)$ the set of those rational primes which have a prime ideal factor of the first degree in K. M. Bauer [1] proved in 1916 the following theorem.

If K is normal, then $P(\Omega) \subset P(K)$ implies $\Omega \supset K$ (the converse implication is immediate).

In this theorem inclusion $P(\Omega) \subset P(K)$ can be replaced by a weaker assumption that the set of primes $P(\Omega) - P(K)$ is finite, which following Hasse [5] I shall denote by $P(\Omega) \leqslant P(K)$. An obvious question to ask is whether on omitting the assumption that K is normal it is true that $P(\Omega) \leqslant P(K)$ implies Ω contains a conjugate of K. This question was answered negatively by F. Gassmann [3] in 1926 when he gave an example of two non-conjugate fields Ω and K of degree 180 such that $P(\Omega) = P(K)$. The two fields found by Gassmann have the even more remarkable property $P_A(\Omega) = P_A(K)$ for every A, where $P_A(K)$ denotes the set of those rational primes which decompose into prime ideals in K in a prescribed way A.

The first aim of this paper is to characterize all fields K for which the extension of Bauer's theorem mentioned above is nevertheless true. Such fields will be called *Bauerian*. It follows easily from the definition that if K_1, K_2 are two Bauerian fields and $|K_1K_2| = |K_1|\,|K_2|$, then K_1K_2 is also Bauerian ($|\ |$ denotes the degree). We have

Theorem 1. *Let K, Ω be two algebraic number fields, $\overline{K}$ the normal closure of K, $\mathfrak{G}$—its Galois group, $\mathfrak{H}$ and $\mathfrak{J}$ subgroups of $\mathfrak{G}$ belonging to K and $\Omega \cap \overline{K}$, respectively, and $\mathfrak{H}_1, \mathfrak{H}_2, \ldots, \mathfrak{H}_n$ all the subgroups of $\mathfrak{G}$ conjugate to $\mathfrak{H}$. $P(\Omega) \leqslant P(K)$ is equivalent to $\mathfrak{J} \subset \bigcup_{i=1}^{n} \mathfrak{H}_i$.*

The field K is Bauerian if and only if every subgroup of $\mathfrak{G}$ contained in $\bigcup_{i=1}^{n} \mathfrak{H}_i$ is contained in one of the $\mathfrak{H}_i$.

Text corrected following *Corrigenda*, Acta Arith. 12 (1967), 425, and Acta Arith. 22 (1973), 231.

The second part of this theorem enables us to decide for any given field in a finite number of steps whether it is Bauerian or not. A field K is said to be *solvable* if the Galois group of its normal closure is solvable. We obtain in particular

Theorem 2. *Every cubic and quartic field and every solvable field K, such that $\big(|\overline{K}|/|K|, |K|\big) = 1$, is Bauerian. Fields K of degree $n \geqslant 5$ such that the Galois group of $\overline{K}$ is the alternating group $\mathfrak{A}_n$ or the symmetric group $\mathfrak{S}_n$ are not Bauerian.*

Theorem 2 gives complete information about fields of degree $\leqslant 5$. For such fields, Bauerian fields coincide with solvable ones. The following example which I owe to Professor H. Zassenhaus shows that this is no longer true for fields of degree six. Let $\overline{K}$ be any field with group $\mathfrak{A}_4$ (such fields exist, cf. §5) and let K belong to a subgroup $\mathfrak{H}$ of order two. Here $\bigcup \mathfrak{H}_i$ is itself a subgroup (the four-group) and clearly is not contained in any of the $\mathfrak{H}_i$. Taking Ω to be the field corresponding to $\bigcup \mathfrak{H}_i$ we see that Ω is normal and $\Omega \subset K$, thus in this case

$$P(\Omega) = P(K) \quad \text{but} \quad \overline{\Omega} \neq \overline{K} \quad \text{and} \quad |\Omega| \neq |K|.$$

This shows that the condition $P(\Omega) = P(K)$ is much weaker than the condition $P_A(\Omega) = P_A(K)$ for every A. The latter according to Gassmann [3] implies that $\overline{\Omega} = \overline{K}$ and $|\Omega| = |K|$.

The theorem of Bauer has been applied in [2] to characterize polynomials $f(x)$ with the property that for a given normal field K in every arithmetical progression there is an integer x such that $f(x)$ is a norm of an element of K. The same method combined with Theorem 2 gives

Theorem 3. (i) *Let K be a cubic or quartic field or a solvable field such that $\big(|\overline{K}|/|K|, |K|\big) = 1$ and let $N_{K/\mathbb{Q}}$ denote the norm from K to the rational field $\mathbb{Q}$. Let $f(x)$ be a polynomial with rational coefficients, and suppose that every arithmetical progression contains an integer x such that*

$$f(x) = N_{K/\mathbb{Q}}(\omega) \quad \text{for some} \quad \omega \in K.$$

If either $n = |K|$ is square-free or the multiplicity of every zero of $f(x)$ is relatively prime to n, then $f(x) = N_{K/\mathbb{Q}}\big(\omega(x)\big)$ identically for some $\omega(x) \in K[x]$.

(ii) *Let K be a field of degree $n \geqslant 5$, $n \neq 6$ such that the Galois group of $\overline{K}$ is alternating $\mathfrak{A}_n$ or symmetric $\mathfrak{S}_n$. Then there exists an irreducible polynomial $f(x)$ such that for every integer x and some $\omega \in K$, $f(x) = N_{K/\mathbb{Q}}(\omega)$ but $f(x)$ cannot be represented as $N_{K/\mathbb{Q}}\big(\omega(x)\big)$ for any $\omega(x) \in K[x]$.*

Since every group of square-free order is solvable, we get immediately from Theorem 3(i)

Corollary. *Let K be a field such that $|\overline{K}|$ is square-free and let $f(x)$ be a polynomial with rational coefficients. If every arithmetical progression contains an integer x such that $f(x) = N_{K/\mathbb{Q}}(\omega)$ for some $\omega \in K$, then $f(x) = N_{K/\mathbb{Q}}\big(\omega(x)\big)$ identically for some $\omega(x) \in K[x]$.*

If $f(x)$ is to be represented only as a norm of a rational function, not of a polynomial, the conditions on the field K can be weakened. We have

Theorem 4. *Let K be a field of degree $n = p$ or p^2 (p prime) and let $g(x)$ be a rational function over $\mathbb{Q}$ with the multiplicity of each zero and pole prime to n/p ([1]). If in every arithmetical progression there is an integer x such that*

$$g(x) = N_{K/\mathbb{Q}}(\omega) \quad \textit{for some} \quad \omega \in K,$$

then

$$g(x) = N_{K/\mathbb{Q}}\big(\omega(x)\big) \quad \textit{for some} \quad \omega(x) \in K(x).$$

There exist fields of degree 6 for which an analogue of Theorem 4 does not hold. We have in fact

Theorem 5. *Let $K = \mathbb{Q}\big(\sqrt{2\cos\frac{2}{7}\pi}\big)$, $f(x) = x^3 + x^2 - 2x - 1$. For every integer x, $f(x)$ is a norm of an integer in K, but $f(x)$ cannot be represented as $N_{K/\mathbb{Q}}\big(\omega(x)\big)$ for any $\omega(x) \in K(x)$.*

The proofs of Theorems 1 and 2 are given in §2, those of Theorems 3, 4 and 5 in §3, 4 and 5, respectively.

I shall like to express my thanks to Professors D. J. Lewis, H. Zassenhaus and Dr. R. T. Bumby for their valuable suggestions and to Dr. Sedarshan Sehgal whom I owe the proof of Lemma 3.

2.

Proof of Theorem 1. This proof follows easily from a generalization of Bauer's theorem given by Hasse [5], p. 144. For a given prime p, let $\left(\frac{\overline{K}}{p}\right)$ be the Artin symbol (the class of conjugate elements of $\mathfrak{G}$, to which p belongs). The theorem in question can be stated in our notation in the following way. $\mathfrak{C}$ being any class of conjugate elements in $\mathfrak{G}$, the set $\left\{p \in P(\Omega) : \left(\frac{\overline{K}}{p}\right) = \mathfrak{C}\right\}$ is infinite if and only if $\mathfrak{C} \subset \bigcup_{j=1}^{m} \mathfrak{J}_j$, where $\mathfrak{J}_j$ ($j = 1, 2, \ldots, m$) are all the subgroups of $\mathfrak{G}$ conjugate to $\mathfrak{J}$.

Suppose now that $P(\Omega) \leqslant P(K)$ and let $\mathfrak{C}$ be any class of conjugate elements of $\mathfrak{G}$ such that $\mathfrak{C} \subset \bigcup_{j=1}^{m} \mathfrak{J}_j$. By the theorem of Hasse, the set $\left\{p \in P(\Omega) : \left(\frac{\overline{K}}{p}\right) = \mathfrak{C}\right\}$ is infinite and since $P(\Omega) \leqslant P(K)$ the same applies to $\left\{p \in P(K) : \left(\frac{\overline{K}}{p}\right) = \mathfrak{C}\right\}$. Applying the

([1]) Without the last assumption the theorem is false, as the example (1) of [2] shows.

theorem in the opposite direction and with K instead of Ω we infer that $\mathfrak{C} \subset \bigcup_{i=1}^{n} \mathfrak{H}_i$. The set $\bigcup_{j=1}^{m} \mathfrak{J}_j$ consists of the union of full conjugate classes. Hence $\bigcup_{j=1}^{m} \mathfrak{J}_j \subset \bigcup_{i=1}^{n} \mathfrak{H}_i$ and a fortiori $\mathfrak{J} \subset \bigcup_{i=1}^{n} \mathfrak{H}_i$.

In order to prove the converse implication, let us notice that according to [5], p. 144, the symmetric difference

$$P(K) \doteq \left\{ p : \left(\frac{\overline{K}}{p}\right) \subset \bigcup_{i=1}^{n} \mathfrak{H}_i \right\} \quad \text{is finite} \tag{1}$$

and similarly

$$P(\Omega \cap \overline{K}) \doteq \left\{ p : \left(\frac{\overline{K}}{p}\right) \subset \bigcup_{j=1}^{m} \mathfrak{J}_j \right\} \quad \text{is finite.} \tag{2}$$

Hence if $\mathfrak{J} \subset \bigcup_{i=1}^{n} \mathfrak{H}_i$ we get $\bigcup_{j=1}^{m} \mathfrak{J}_j \subset \bigcup_{i=1}^{n} \mathfrak{H}_i$ and by (1) and (2) $P(\Omega \cap \overline{K}) \leqslant P(K)$ and a fortiori $P(\Omega) \leqslant P(K)$.

This completes the proof of the first part of Theorem 1. The second part follows immediately from the first after taking into account that every subgroup of $\mathfrak{G}$ belongs to some field and this field can be set as Ω. □

Proof of Theorem 2. Suppose first that the Galois group of $\overline{K}$ is solvable and $\left(|\overline{K}|/|K|, |K|\right) = 1$. Let $\mathfrak{H}$ be the subgroup of $\mathfrak{G}$ belonging to K and let Π be the set of all primes dividing $|\mathfrak{H}|$, i.e. the order of $\mathfrak{H}$. If for a subgroup $\mathfrak{J}$, $\mathfrak{J} \subset \bigcup_{i=1}^{n} \mathfrak{H}_i$, then clearly $\mathfrak{J}$ is a Π-group. Since $\mathfrak{H}$ is a maximal Π-group by a theorem of P. Hall (cf. [4], Th. 9.3.1), $\mathfrak{J}$ must be contained in one of $\mathfrak{H}_i$. This shows according to Theorem 1 that field K is Bauerian. In particular every cubic field and every quartic field K having $\mathfrak{A}_4$ as Galois group of $\overline{K}$ is Bauerian. It remains to consider quartic fields K such that Galois group of $\overline{K}$ is either dihedral group of order 8 or $\mathfrak{S}_4$. In the first case $\bigcup_{i=1}^{4} \mathfrak{H}_i$ consists of 3 elements and does not contain any subgroup except the $\mathfrak{H}_i$ and the identity group. In the second case $\mathfrak{H}_i$ ($i = 1, 2, 3, 4$) is the ith stability group and $\bigcup_{i=1}^{4} \mathfrak{H}_i$ contains besides the $\mathfrak{H}_i$ and the identity group only cyclic subgroups of order two or three. These are clearly contained in one of the $\mathfrak{H}_i$. Thus every quartic field is Bauerian.

In order to prove that fields K of degree $n \geqslant 5$ such that $\mathfrak{A}_n$ or $\mathfrak{S}_n$ is Galois group of $\overline{K}$ are not Bauerian we consider the following subgroups of $\mathfrak{A}_n$:

$$\begin{aligned} &\big\{(123), (12)(45)\big\} \times \mathfrak{A}_{n-5} && \text{for } n = 5 \text{ or } n \geqslant 8, \\ &\big\{(12)(34), (12)(56)\big\} && \text{for } n = 6, \\ &\big\{(12345), (1243)(67)\big\} && \text{for } n = 7. \end{aligned} \tag{3}$$

They are contained in the union of stability subgroups of $\mathfrak{S}_n$ but not in any one of them, and the desired result follows immediately from the second part of Theorem 1. □

3.

Lemma 1. *Suppose that the hypotheses of Theorem* 3(i) *hold. Let*

$$f(x) = cf_1(x)^{e_1} f_2(x)^{e_2} \cdots f_m(x)^{e_m} \tag{4}$$

where $c \neq 0$ is a rational number and $f_1(x), f_2(x), \ldots, f_m(x)$ are coprime polynomials with integral coefficients each irreducible over $\mathbb{Q}$ and where $e_1, e_2, \ldots, e_m$ are positive integers. For any j, let q be a sufficiently large prime for which the congruence

$$f_j(x) \equiv 0 \pmod{q} \tag{5}$$

is solvable.

If $(e_j, n) = 1$, then $q \in P(K)$. If n is square-free then $q \in P(K_j)$, where K_j is any subfield of K of degree $n/(e_j, n)$. (Such subfields exist.)

Proof. Put $F(x) = f_1(x) f_2(x) \cdots f_m(x)$. Since the discriminant of $F(x)$ is not zero, there exist polynomials $\varphi(x)$, $\psi(x)$ with integral coefficients such that

$$F(x)\varphi(x) + F'(x)\psi(x) = D \tag{6}$$

identically, where D is a non-zero integer.

Let q be a large prime for which the congruence (5) is soluble and let x_0 be a solution. By (6) we have $F'(x_0) \not\equiv 0 \pmod{q}$, whence

$$F(x_0 + q) \not\equiv F(x_0) \pmod{q^2}.$$

By choice of x_1 as either x_0 or $x_0 + q$, we can ensure that

$$f_j(x_1) \equiv 0 \pmod{q}, \quad F(x_1) \not\equiv 0 \pmod{q^2},$$

whence

$$f_j(x_1) \not\equiv 0 \pmod{q^2} \quad \text{and} \quad f_i(x_1) \not\equiv 0 \pmod{q} \quad \text{for} \quad i \neq j.$$

By the hypothesis of Theorem 3, there exists $x_2 \equiv x_1 \pmod{q^2}$ such that

$$f(x_2) = N_{K/\mathbb{Q}}(\omega) \quad \text{for some } \omega \in K. \tag{7}$$

From the preceding congruences we have

$$f_j(x_2) \equiv 0 \pmod{q}, \quad f_j(x_2) \not\equiv 0 \pmod{q^2},$$
$$f_i(x_2) \not\equiv 0 \pmod{q} \quad \text{for} \quad i \neq j.$$

Hence

$$f(x_2) \equiv 0 \pmod{q^{e_j}}, \quad f(x_2) \not\equiv 0 \pmod{q^{e_j+1}}. \tag{8}$$

If $n = 4$ and q does not belong to $P(K)$ then q remains prime in K or factorizes into two prime ideals of degree two. In either case q divides $N_{K/\mathbb{Q}}(\omega)$ for any $\omega \in K$ in an even power. In view of (4) and (8) this contradicts the assumption that $(e_j, n) = 1$.

If $\overline{K}$ is solvable and $\left(|\overline{K}|/|K|, |K|\right) = 1$, let

$$q = \mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_g \tag{9}$$

be the prime ideal factorization of q in $\overline{K}$; the factors are distinct since q is supposed to be sufficiently large. We note that g divides $|\overline{K}|$ because $\overline{K}$ is a normal field and that

$$N_{\overline{K}/\mathbb{Q}}\mathfrak{q}_i = q^{|\overline{K}|/g}. \tag{10}$$

Write the prime ideal factorization of ω in K in the form

$$(\omega) = \mathfrak{q}_1^{\alpha_1}\mathfrak{q}_2^{\alpha_2}\cdots\mathfrak{q}_g^{\alpha_g}\mathfrak{a}\mathfrak{b}^{-1},$$

where $\mathfrak{a}$, $\mathfrak{b}$ are ideals in K which are relatively prime to q. Then

$$N_{K/\mathbb{Q}}(\omega) = \pm q^{n(\alpha_1+\alpha_2+\ldots+\alpha_g)/g} N_{K/\mathbb{Q}}\mathfrak{a}(N_{K/\mathbb{Q}}\mathfrak{b})^{-1} \tag{11}$$

and $N_{K/\mathbb{Q}}\mathfrak{a}$, $N_{K/\mathbb{Q}}\mathfrak{b}$ are relatively prime to q. It follows from (7), (8) and (11) that

$$n(\alpha_1 + \alpha_2 + \ldots + \alpha_g)/g = e_j,$$

whence

$$\frac{n}{(e_j, n)} \quad \text{divides} \quad g.$$

If $(e_j, n) = 1$ we get that n divides g. Let $\mathfrak{G}_s$ be the splitting group of the ideal $\mathfrak{q}_1$. We have $[\mathfrak{G} : \mathfrak{G}_s] = g$, thus $|\mathfrak{G}_s|$ divides $\dfrac{|\mathfrak{G}|}{n}$, that is the order of the group $\mathfrak{H}$ belonging to field K. Since

$$\left(n, \frac{|\mathfrak{G}|}{n}\right) = \left(n, \frac{|\overline{K}|}{n}\right) = 1$$

it follows from the theorem of Hall that $\mathfrak{G}_s$ is contained in one of the conjugates of $\mathfrak{H}$. Therefore the splitting field F_s of $\mathfrak{q}_1$ contains a conjugate of K and since $q \in P(F_s)$, $q \in P(K)$.

Suppose now that n is square-free and let $\mathfrak{G}_s$ and F_s have the same meaning as before. Since

$$\left(\frac{|\mathfrak{G}|}{n}(e_j, n), \frac{n}{(e_j, n)}\right) = 1$$

there exist in $\mathfrak{G}$, by the theorem of Hall, subgroups of order $\dfrac{|\mathfrak{G}|}{n}(e_j, n)$ and they are all conjugate. Moreover since $|\mathfrak{G}_s| \;\Big|\; \dfrac{|\mathfrak{G}|}{n}(e_j, n)$, $\mathfrak{G}_s$ must be contained in one of them, thus F_s must contain a subfield K' of $\overline{K}$ of degree $\dfrac{n}{(n, e_j)}$.

Since all such fields are conjugate, and since $q \in P(F_s)$ it follows that $q \in P(K_j)$, where K_j is any subfield of K of degree $\dfrac{n}{(n, e_j)}$. Such fields exist again by the theorem of Hall since $\left(\dfrac{|\mathfrak{G}|}{n}, (e_j, n)\right) = 1$. □

Proof of Theorem 3(i). Lemma 1 being established the proof does not differ from the proof of Theorem 2 of [2]. Instead of Lemma 3 of that paper which was the original Bauer theorem one uses Theorem 2. □

Proof of Theorem 3(ii). Let the Galois group of $\overline{K}$ be represented as the permutation group on the n fields conjugate to K: $K_1, K_2, \ldots, K_n$. Consider a subfield Ω of $\overline{K}$ belonging to a subgroup $\mathfrak{J}_n$ of $\mathfrak{A}_n$ defined by formula (3). It is clear that if $\mathfrak{H}_{ni}$ denotes the subgroup of $\mathfrak{G}$ belonging to K_i, then

$$\frac{|\mathfrak{J}_n|}{|\mathfrak{J}_n \cap \mathfrak{H}_{ni}|} = \begin{cases} 3 & \text{for } i = 1, 2, 3, \\ 2 & \text{for } i = 4 \text{ or } 5, \\ n-5 & \text{for } i = 6, \ldots, n \end{cases} \qquad (n = 5 \text{ or } n \geqslant 8), \tag{12}$$

$$\frac{|\mathfrak{J}_n|}{|\mathfrak{J}_n \cap \mathfrak{H}_{ni}|} = \begin{cases} 5 & \text{for } i \leqslant 5, \\ 2 & \text{for } i = 6 \text{ or } 7 \end{cases} \qquad (n = 7).$$

We have

$$\frac{|\mathfrak{J}_n|}{|\mathfrak{J}_n \cap \mathfrak{H}_{ni}|} = \frac{|K_i \Omega|}{|\Omega|}$$

and the equalities (12) mean that $F(x)$—the polynomial generating K factorizes over Ω into irreducible factors of degrees 3, 2 and $n-5$ ($n = 5$ or $n \geqslant 8$) or 5 and 2 ($n = 7$). It follows by the theorem of Kronecker and Kneser (cf. [7], p. 239) that $f(x)$—the polynomial generating Ω factorizes in K into irreducible factors of degrees $3\,\frac{|\Omega|}{n}$, $2\,\frac{|\Omega|}{n}$ and $(n-5)\,\frac{|\Omega|}{n}$ ($n = 5$ or $n \geqslant 8$) or $5\,\frac{|\Omega|}{n}$ and $2\,\frac{|\Omega|}{n}$ ($n = 7$). The norms of these factors with respect to K are $f^3(x)$, $f^2(x)$, $f^{n-5}(x)$ ($n = 5$ or $n \geqslant 8$) and $f^5(x)$, $f^2(x)$ ($n = 7$). None of them is $f(x)$, thus $f(x)$ cannot be represented as a norm of a polynomial over K. On the other hand $f(x) = f^3(x)/f^2(x) = f^5(x)/\big(f^2(x)\big)^2$, whence it follows by the multiplicative property of the norm that $f(x)$ is a norm of a rational function over K and so for every integer x, $f(x) = N_{K/\mathbb{Q}}(\omega)$ for some $\omega \in K$. □

4.

Lemma 2. *Suppose that the hypotheses of Theorem* 4 *hold. Let*

$$g(x) = c f_1(x)^{e_1} f_2(x)^{e_2} \cdots f_m(x)^{e_m} \tag{13}$$

where $c \neq 0$ is a rational number and $f_1(x)$, $f_2(x)$, ..., $f_m(x)$ are coprime polynomials with integral coefficients each irreducible over $\mathbb{Q}$ and where $e_1, e_2, \ldots, e_m$ are integers relatively prime to n. For any j, let q be a sufficiently large prime for which the congruence

$$f_j(x) \equiv 0 \pmod{q}$$

is soluble. Then q factorizes in K into a product of ideals, whose degrees are relatively prime.

Proof. We infer as in the proof of Lemma 1 that there exists an integer x_2 with the following properties

$$g(x_2) = N_{K/\mathbb{Q}}(\omega) \quad \text{for some } \omega \in K, \tag{14}$$

$$g(x_2) = q^{e_j} a b^{-1}, \quad \text{where } a, b \text{ are integers and } (ab, q) = 1. \tag{15}$$

Let $q = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_l$ be the factorization of q in K, the factors are distinct since q is sufficiently large and let $N_{K/\mathbb{Q}}\mathfrak{p}_i = q^{f_i}$. Clearly

$$\sum_{i=1}^{l} f_i = n. \tag{16}$$

Write the prime ideal factorization of ω in K in the form

$$(\omega) = \mathfrak{p}_1^{\alpha_1}\mathfrak{p}_2^{\alpha_2}\cdots\mathfrak{p}_l^{\alpha_l}\mathfrak{a}\mathfrak{b}^{-1},$$

where $(\mathfrak{a}\mathfrak{b}, q) = 1$. Then

$$N_{K/\mathbb{Q}}(\omega) = \pm q^{\alpha_1 f_1+\alpha_2 f_2+\ldots+\alpha_l f_l} N_{K/\mathbb{Q}}\mathfrak{a}(N_{K/\mathbb{Q}}\mathfrak{b})^{-1} \tag{17}$$

and $N_{K/\mathbb{Q}}\mathfrak{a}$, $N_{K/\mathbb{Q}}\mathfrak{b}$ are relatively prime to q. It follows from (14), (15) and (17) that

$$\alpha_1 f_1 + \alpha_2 f_2 + \ldots + \alpha_l f_l = e_j.$$

Thus $(f_1, f_2, \ldots, f_l) \mid e_j$ and by (16) $(f_1, f_2, \ldots, f_l) \mid n$. Since $(e_j, n) = 1$, $(f_1, f_2, \ldots, f_l) = 1$. □

Lemma 3. *Let $\mathfrak{J}$ be a group of permutations of n letters, where $n = p$ or p^2 (p—prime). If the lengths of orbits of $\mathfrak{J}$ are not relatively prime there exists in $\mathfrak{J}$ a permutation whose disjoint cycles are of lengths $\lambda_1, \lambda_2, \ldots, \lambda_\varrho$ where $(\lambda_1, \lambda_2, \ldots, \lambda_\varrho) \neq 1$.*

Proof (due to Sedarshan Sehgal). Let the lengths of orbits of $\mathfrak{J}$ be $l_1, l_2, \ldots, l_r$. Since $l_1 + l_2 + \ldots + l_r = n$, if $(l_1, l_2, \ldots, l_r) \neq 1$, we must have $p \mid l_i$ $(i = 1, 2, \ldots, r)$. Thus the order of group $\mathfrak{J}$ is divisible by p and it contains a Sylow subgroup S_p. Moreover, the lengths of orbits of S_p are again divisible by p (cf. [8], Theorem 3.4). The number of these orbits r' is $\leqslant n/p \leqslant p$. Permutations of S_p leave on the average r' letters fixed (ibid. Theorem 3.9). Since the identity fixes n letters there must be a permutation in S_p which fixes less than p letters. Since $|S_p|$ has no prime factor less than p, the permutation in question leaves no letter fixed and all its disjoint cycles must have lengths divisible by p.□

Remark. If $n \neq p, p^2$, there exist groups of degree n for which the lemma does not hold, as shown by the following construction. Let $n = pq$, where p—prime and $q > p$. We put

$$\mathfrak{J} = \left\{P_{\alpha,\beta,\gamma}\right\}_{\substack{\alpha=1,2,\ldots,p \\ \beta=1,2,\ldots,p \\ \gamma=1,2,\ldots,p(q-p-1)}},$$

where

$$P_{\alpha,\beta,\gamma} = (1, 2, \ldots, p)^\alpha \prod_{k=1}^{p}\big(kp+1, \ldots, (k+1)p\big)^{k\alpha+\beta}(p^2+p+1, \ldots, pq)^\gamma.$$

The orbits here are $(1, 2, \ldots, p)$, ..., $(p^2+1, \ldots, p^2+p)$, $(p^2+p+1, \ldots, pq)$, their lengths are therefore all divisible by p. On the other hand, for every triple α, β, γ either $\alpha = p$ or there exists a k such that $1 \leqslant k \leqslant p$ and $k\alpha + \beta \equiv 0 \pmod{p}$. In either case $P_{\alpha,\beta,\gamma}$ leaves at least p letters fixed.

Proof of Theorem 4. Let the Galois group $\mathfrak{G}$ of $\overline{K}$ be represented as a permutation group on the n fields conjugate to K. Let $f_j(x)$ be any one of irreducible factors of $g(x)$ as in (13), Ω_j be a field generated by a root of $f_j(x)$ and $\mathfrak{J}_j$ be a subgroup of $\mathfrak{G}$ belonging to field $\Omega_j \cap \overline{K}$. By the theorem of Hasse quoted in the proof of Theorem 1 for every class $\mathfrak{C} \subset \bigcup \mathfrak{J}$ (summation over all conjugates of $\mathfrak{J}_j$), there exist infinitely many primes $q \in P(\Omega_j)$ such that $\left(\frac{\overline{K}}{q}\right) = \mathfrak{C}$. If such a prime is sufficiently large, we infer by the principle of Dedekind and Lemma 2 that q factorizes in K into prime ideals of relatively prime degrees. The degrees in question are equal to the lengths of the cycles in the decomposition of class $\mathfrak{C}$. Thus in every permutation of $\mathfrak{J}_j$, the lengths of the cycles are relatively prime. By Lemma 3 this implies that the lengths of the orbits of $\mathfrak{J}_j$ are relatively prime.

Let $k(x)$ be an irreducible polynomial over $\mathbb{Q}$, whose root generates K. $\mathfrak{J}_j$ is the Galois group of the equation $k(x) = 0$ over Ω_j. The lengths of the orbits of $\mathfrak{J}_j$ are equal to the degrees of irreducible factors of $k(x)$ over Ω_j. Thus

$$k(x) = k_{j1}(x)k_{j2}(x)\cdots k_{jr_j}(x)$$

where k_{ji} is a polynomial irreducible over Ω_j of degree $|k_{ji}|$ and

$$\left(|k_{j1}|, |k_{j2}|, \ldots, |k_{jr_j}|\right) = 1. \tag{18}$$

By the theorem of Kronecker and Kneser it follows that

$$f_j(x) = c_j f_{j1}(x) f_{j2}(x)\cdots f_{jr_j}(x), \quad \text{where} \quad c_j \in \mathbb{Q},$$

$$f_{ji} \in K[x] \quad \text{and} \quad N_{K/\mathbb{Q}} f_{ji}(x) = \left(\frac{f_j(x)}{c_j}\right)^{|k_{ji}|}. \tag{19}$$

In view of (18), there exist integers a_i $(i = 1, 2, \ldots, r_j)$ such that

$$\sum_{i=1}^{r_j} a_i |k_{ji}| = 1. \tag{20}$$

We get from (19) and (20)

$$f_j(x) = c_j N_{K/\mathbb{Q}} \prod_{i=1}^{r_j} f_{ji}^{a_i}(x). \tag{21}$$

It follows from (13), (21) and the multiplicative property of the norm that

$$g(x) = a N_{K/\mathbb{Q}} h(x), \quad \text{where} \quad h(x) \in K(x).$$

By the hypothesis of the theorem taking x to be a suitable integer, we infer that $a = N_{K/\mathbb{Q}}(\alpha)$, where $\alpha \in K$. Putting $\omega(x) = \alpha h(x)$ we obtain $g(x) = N_{K/\mathbb{Q}}\big(\omega(x)\big)$, identically. □

Lemma 4. *The class number of the* $K = \mathbb{Q}\left(\sqrt{2\cos\frac{2}{7}\pi}\right)$ *is one and the rational primes* p *factorize in* K *in the same way, as the polynomial* $f(x^2)$ *factorizes* mod p, f *being defined in Theorem* 5.

Proof. The field $\Omega = \mathbb{Q}(2\cos\frac{2}{7}\pi)$ is a cyclic field of discriminant 7^2. 2 remains a prime in this field, hence $2\cos\frac{2}{7}\pi = \left(2\cos\frac{8}{7}\pi\right)^2 - 2$ is in $\mathbb{Q}$ a quadratic non-residue $\bmod 4$. Since $2\cos\frac{2}{7}\pi$ is a unit, it follows by the conventional methods that $1, \sqrt{2\cos\frac{2}{7}\pi}$ is an integral basis for K over Ω, thus $d_{K/\Omega}$ equals $(8\cos\frac{2}{7}\pi)$ and for the discriminant of K we obtain the value

$$d_{K/\mathbb{Q}} = d^2_{\Omega/\mathbb{Q}} N_{\Omega/\mathbb{Q}}(d_{K/\Omega}) = 2^6 \cdot 7^4.$$

This number coincides with the discriminant of $f(x^2)$, which has $\sqrt{2\cos\frac{2}{7}\pi}$ as one of its zeros. Therefore, by the principle of Dedekind the factorization of primes in K is the same as factorization of $f(x^2) \bmod p$. In particular we have

$$\begin{aligned}
(2) &= \mathfrak{P}_1^2, & N\mathfrak{P}_1 &= 8,\\
(3) &= \mathfrak{P}_2\mathfrak{P}_3, & N\mathfrak{P}_2 &= N\mathfrak{P}_3 = 3^3,\\
(5) &= \mathfrak{P}_4\mathfrak{P}_5, & N\mathfrak{P}_4 &= N\mathfrak{P}_5 = 5^3,\\
(7) &= \mathfrak{P}_6^3\mathfrak{P}_7^3, & N\mathfrak{P}_6 &= N\mathfrak{P}_7 = 7.
\end{aligned}$$

Now, by the theorem of Minkowski, in every class of ideals of K there is an ideal with norm not exceeding

$$\left(\frac{4}{\pi}\right)^2 \frac{6!}{6^6}\sqrt{d_{K/\mathbb{Q}}} < 11.$$

If therefore the field K had class number greater than 1, then there would be a non-principal ideal with a norm < 11. This is however impossible since

$$\begin{aligned}
(2) &= \left(2\cos\tfrac{8}{7}\pi + \sqrt{2\cos\tfrac{8}{7}\pi}\right)^2,\\
(7) &= \left(1 + 2\cos\tfrac{8}{7}\pi + \sqrt{2\cos\tfrac{2}{7}\pi}\right)^3\left(1 + 2\cos\tfrac{8}{7}\pi - \sqrt{2\cos\tfrac{2}{7}\pi}\right)^3.
\end{aligned}$$

□

Proof of Theorem 5. Since the degree of $f(x)$ is not divisible by 6, $f(x)$ cannot be represented as $N_{K/\mathbb{Q}}\big(\omega(x)\big)$, where $\omega(x) \in K(x)$. It remains to show that for every integer x, $f(x) = N_{K/\mathbb{Q}}(\omega)$ for some integer $\omega \in K$. Let

$$f(x) = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \tag{22}$$

where α_i are positive integers. Since the discriminant of $\Omega = \mathbb{Q}\big(2\cos\frac{2}{7}\pi\big)$ coincides with the discriminant of $f(x)$, by the principle of Dedekind each prime p_i has a prime ideal factor $\mathfrak{P}_i$ of first degree in Ω. Since

$$\left(2\cos\tfrac{2}{7}\pi\right)\left(2\cos\tfrac{4}{7}\pi\right)\left(2\cos\tfrac{8}{7}\pi\right) = 1,$$

at least one of the factors on the left hand side is a quadratic residue $\bmod \mathfrak{P}_i$. It follows that for some $x_0 \in \Omega$

$$f(x_0^2) = \left(x_0^2 - 2\cos\tfrac{2}{7}\pi\right)\left(x_0^2 - 2\cos\tfrac{4}{7}\pi\right)\left(x_0^2 - 2\cos\tfrac{8}{7}\pi\right) \equiv 0 \,(\bmod \mathfrak{P}_i).$$

Since $\mathfrak{P}_i$ is of first degree, there exists a rational integer x_1 such that $x_1 \equiv x_0 \,(\bmod \mathfrak{P}_i)$ and we get $f(x_1^2) \equiv 0 \,(\bmod p_i)$. By Lemma 4, $p_i \in P(K)$ and since every ideal of K

is principal,

$$p_i = \pm N_{K/\mathbb{Q}}\omega_i, \tag{23}$$

where ω_i is an integer of K. Since

$$-1 = N_{K/\mathbb{Q}}\big(\sqrt{2\cos\tfrac{2}{7}\pi}\big),$$

the conclusion follows from (22), (23) and the multiplicative property of the norm.

Remark. In connection with Theorem 5 let us remark that the theorem of Bauer gives an answer to a question of D. H. Lehmer ([6], p. 436) concerning possible types of homogeneous polynomials $F(x, y)$ of degree $\frac{1}{2}\varphi(n)$ such that when $(x, y) = 1$, the prime factors of $F(x, y)$ either divide n or are of the form $nk \pm 1$. (If $f(x) = x^3 + x^2 - 2x - 1$, then $y^3 f(x/y)$ is an example of such polynomial for $n = 7$.) The answer is that all such polynomials must be of the form $A \prod_{i=1}^{\varphi(n)/2} (x - \alpha_i y)$, where α_i runs through all conjugates of a primitive element of the field $\mathbb{Q}\big(2\cos\frac{2}{n}\pi\big)$ and A is a rational integer.

Note added in proof. In connection with Theorem 2 a question arises whether solvable fields of degree p^2 (p prime) are Bauerian. J. L. Alperin has proved that the answer is positive if the field is primitive and $p > 3$. P. Roquette has found a proof for the case where the Galois group of the normal closure is a p-group (oral communication).

References

[1] M. Bauer, *Zur Theorie der algebraischen Zahlkörper*. Math. Ann. 77 (1916), 353–356.

[2] H. Davenport, D. J. Lewis, A. Schinzel, *Polynomials of certain special types*. Acta Arith. 9 (1964), 107–116; this collection: A6, 27–35.

[3] F. Gassmann, *Bemerkungen zu der vorstehenden Arbeit von Hurwitz*. Math. Z. 25 (1926), 665–675.

[4] M. Hall, *The Theory of Groups*. Macmillan, New York 1959.

[5] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper* II. Jahresber. Deutsch. Math.-Verein. 6 (1930).

[6] D. H. Lehmer, *An extended theory of Lucas' functions*. Ann. of Math. (2) 31 (1930), 419–448.

[7] N. Tschebotaröw, *Grundzüge der Galoisschen Theorie*. Übersetzt und bearbeitet von H. Schwerdtfeger, Noordhoff, Groningen–Djakarta 1950.

[8] H. Wielandt, *Finite Permutation Groups*. Academic Press, New York–London 1964.

Originally published in
Acta Arithmetica XI (1966), 345–352

An extension of the theorem of Bauer and polynomials of certain special types

with D. J. Lewis (Ann Arbor) and H. Zassenhaus (Columbus)*

1.

For a given algebraic number field K let us denote by $P(K)$ the set of those rational primes which have a prime ideal factor of the first degree in K. M. Bauer [1] proved in 1916 the following theorem.

If K is normal, then $P(\Omega) \subset P(K)$ implies $\Omega \supset K$ (the converse implication is immediate).

In this theorem, inclusion $P(\Omega) \subset P(K)$ can be replaced by a weaker assumption that the set of primes $P(\Omega) - P(K)$ is finite, which following Hasse we shall denote by $P(\Omega) \leqslant P(K)$.

In the preceding paper [8], one of us characterized all the fields K for which $P(\Omega) \leqslant P(K)$ implies that Ω contains one of the conjugates of K and has called such fields *Bauerian*. The characterization is in terms of the Galois group of the normal closure $\overline{K}$ of K and is not quite explicit. Examples of non-normal Bauerian fields given in that paper are the following: fields K such that $\overline{K}$ is solvable and $\left(\frac{|\overline{K}|}{|K|}, |K|\right) = 1$ ([1]), fields of degree 4. The aim of the present paper is to exhibit a class of Bauerian fields that contains all normal and some non-normal fields. We say that a field K has property (N) if there exists a normal field L of degree relatively prime to the degree of K such that the composition KL is the normal closure of K. We have

Theorem 1. *If K and Ω are algebraic number fields and K has property* (N) *then $P(\Omega) \leqslant P(K)$ implies that Ω contains one of the conjugates of K.*

Not all fields K such that $\overline{K}$ is solvable and $\left(\frac{|\overline{K}|}{|K|}, |K|\right) = 1$ possess property (N).

* This paper was written while the first author received support from the National Science Foundation.

([1]) We let $|\ |$ denote both the degree of the field over $\mathbb{Q}$ and the order of the group.

We have however

Theorem 2. *If K is a number field such that $\left(\frac{|\overline{K}|}{|K|}, |K|\right) = 1$ and the Galois group of $\overline{K}$ is supersolvable, then K has property* (N).

In particular K can be any field of prime degree such that $\overline{K}$ is solvable or any field generated by $\sqrt[n]{a}$, where a, n are rational integers and $\big(n, \varphi(n)\big) = 1$. The field $\mathbb{Q}\big(\sqrt[6]{2}\big)$ does not possess property (N), it is however Bauerian. (It follows from a theorem of Flanders (cf. [7], Th. 167) and results of the preceding paper that $\mathbb{Q}\big(\sqrt[n]{a}\big)$ is Bauerian if $n \not\equiv 0 \pmod 8$.) We have no example of non-normal field K with property (N), such that $\overline{K}$ is non-solvable however one could construct such a field provided there are fields corresponding to every Galois group.

The original Bauer's theorem has been applied in [2] to characterize polynomials $f(x)$ with the property that in every arithmetical progression there is an integer x such that $f(x)$ is a norm of an element of a given number field K. The method used in [2] can be modified in order to obtain

Theorem 3. *Let K be a field having property* (N) *and let $N_{K/\mathbb{Q}}(\omega)$ denote the norm from K to the rational field $\mathbb{Q}$. Let $f(x)$ be a polynomial over $\mathbb{Q}$ such that the multiplicity of each zero of $f(x)$ is relatively prime to $|K|$. If in every arithmetical progression there is an integer x such that*

$$f(x) = N_{K/\mathbb{Q}}(\omega) \quad \text{for some } \omega \in K,$$

then

$$f(x) = N_{K/\mathbb{Q}}\big(\omega(x)\big) \quad \text{for some } \omega(x) \in K[x].$$

The proofs of Theorems 1–3 given in §3 are independent of the preceding paper [8] and assume only the original Bauer's theorem. They are preceded in §2 by some lemmata of seemingly independent interest. Theorems 1 and 3 could be proved by the methods and results of [8]. We retain the present proofs since they use, as do the statements of the theorems, only the language of field theory. We refer to [8] for examples showing that an extension of the theorems to an arbitrary field K is impossible.

2.

Lemma 1. *Let fields K and L have the following properties: L is normal,* (degree K, degree L) $= 1$, *KL is normal. Then for any field Ω the inclusion*

$$\Omega L \supset KL \tag{1}$$

implies that Ω contains one of the conjugates of K.

Proof. It follows from (1) that

$$\Omega KL = \Omega L. \tag{2}$$

Since KL is normal and L is normal, we have

$$|\Omega KL| = \frac{|\Omega|\,|KL|}{|\Omega \cap KL|}, \tag{3}$$

$$|\Omega L| = \frac{|\Omega|\,|L|}{|\Omega \cap L|}. \tag{4}$$

(Cf. [6], §19.5, Satz 1.)

Since clearly $|KL| = |K|\,|L|$, we get from (2), (3) and (4)

$$|\Omega \cap KL| = |K|\,|\Omega \cap L|. \tag{5}$$

Let $\mathfrak{G}$ be the Galois group of KL. And let $\mathfrak{H}$, $\mathfrak{J}$, $\mathfrak{N}$ be subgroups of $\mathfrak{G}$ corresponding to K, $\Omega \cap KL$ and L, respectively.

In view of (5)

$$[\mathfrak{G} : \mathfrak{H}] \,\big|\, [\mathfrak{G} : \mathfrak{J}], \quad \text{thus} \quad |\mathfrak{J}| \,\big|\, |\mathfrak{H}| \quad \text{and} \quad \big(|\mathfrak{J}|, |\mathfrak{N}|\big) = 1.$$

On the other hand, since $\mathfrak{H}\mathfrak{N} = \mathfrak{G}$, and $\mathfrak{N}$ is normal, it can be easily shown that

$$\mathfrak{J}\mathfrak{N} = (\mathfrak{J}\mathfrak{N} \cap \mathfrak{H})\mathfrak{N}.$$

Thus $\mathfrak{J}$ and $\mathfrak{J}\mathfrak{N} \cap \mathfrak{H}$ are two representative subgroups of $\mathfrak{J}\mathfrak{N}$ over $\mathfrak{N}$ and by Theorem 27 ([9], Chapter IV) they are conjugate. The theorem in question had been deduced from the conjecture now proven [3] that all groups of odd orders are solvable. It follows that $\mathfrak{J}$ is contained in a certain conjugate of $\mathfrak{H}$, thus $\Omega \cap KL$ contains a suitable conjugate of K and the same applies to Ω. □

The first two assumptions of Lemma 1 are necessary as shown by the following examples

1. $K = \mathbb{Q}\big(e^{2\pi i/3}\big)$, $L = \mathbb{Q}\big(\sqrt[3]{2}\big)$, $\Omega = \mathbb{Q}\big(e^{2\pi i/3}\sqrt[3]{2}\big)$ ([2]),
2. $K = \mathbb{Q}(i)$, $L = \mathbb{Q}\big(\sqrt{2}\big)$, $\Omega = \mathbb{Q}\big(\sqrt{-2}\big)$.

As to the third assumption, namely that KL is normal, we can show that it is necessary provided that there exists a field with Galois group $\mathfrak{G}$, where $\mathfrak{G}$ is the wreath product of $\mathfrak{S}_4$ acting on 4 isomorphic copies of the simple group $\mathfrak{G}_{168}$. Then in the counterexample, K is a field of degree 7^4 corresponding to the wreath product of $\mathfrak{S}_4$ acting on 4 isomorphic copies of a subgroup $\mathfrak{H}$ of $\mathfrak{G}_{168}$ of index 7, L is a normal field of degree 24 corresponding to the product of 4 copies of $\mathfrak{G}_{168}$. The construction of Ω and the proof that it furnishes a counterexample is complicated and will be omitted.

Lemma 2. *In any supersolvable group $\mathfrak{G}$ for each set Π of primes either there is a normal Π-subgroup $\neq 1$ or there is a normal Hall ([3]) $\hat{\Pi}$-group $\neq 1$ ($\hat{\Pi}$ is the set of all prime divisors of $|\mathfrak{G}|$ not contained in Π).*

Proof. If this lemma would be false, then there would be a supersolvable group $\mathfrak{G} \neq 1$ of minimal order for which it would be false.

([2]) We owe this example to Mr. Surinder Sehgal.

([3]) A Hall subgroup is a subgroup whose order and index are relatively prime.

If Π or $\hat{\Pi}$ are empty then the statement is trivial. Let Π and $\hat{\Pi}$ be non-empty. Since $\mathfrak{G} \neq 1$, there is a maximal normal subgroup $\mathfrak{M} \neq \mathfrak{G}$. Since $\mathfrak{G}$ is solvable $[\mathfrak{G} : \mathfrak{M}]$ is a prime p. If $\mathfrak{M}$ contains a normal Π-subgroup $\mathfrak{N} \neq 1$, then $\langle \mathfrak{N}^{\mathfrak{G}} \rangle$ is a normal Π-subgroup $\neq 1$ of $\mathfrak{G}$, a contradiction. Hence $\mathfrak{M}$ contains no normal Π-subgroup. Since $\mathfrak{M}$, a subgroup of a supersolvable group, itself is supersolvable, it follows from the minimal property of $\mathfrak{G}$ that $\mathfrak{M}$ contains a normal Hall $\hat{\Pi}$-group $\mathfrak{J}$. A normal Hall subgroup of a solvable group is the unique subgroup of its order (cf. [4], Th. 9.3.1). Therefore $\mathfrak{J}$ must be a characteristic subgroup of $\mathfrak{M}$ and hence a normal subgroup of $\mathfrak{G}$. If $p \in \Pi$ then $\mathfrak{J}$ is normal Hall $\hat{\Pi}$-group of $\mathfrak{G}$, a contradiction. Hence $p \in \hat{\Pi}$. It follows that

(6) the index of every maximal normal subgroup of $\mathfrak{G}$

is a prime number belonging to $\hat{\Pi}$.

Now let $\mathfrak{N} \neq 1$ be a minimal normal subgroup of $\mathfrak{G}$. Since $\mathfrak{G}$ is supersolvable, it follows that $\mathfrak{N}$ is of prime order, say q. Since we have assumed $\mathfrak{G}$ does not have a normal Π-subgroup, $q \in \hat{\Pi}$. Suppose $\mathfrak{G}/\mathfrak{N}$ contains a normal Π-subgroup $\mathfrak{H}/\mathfrak{N} \neq 1$. Since $\mathfrak{H}$ is solvable it contains a q-complement $\mathfrak{J} \neq 1$. The group $\mathfrak{J}$ is a Hall Π-subgroup of $\mathfrak{H}$. If $\mathfrak{J}$ is normal in $\mathfrak{H}$, it follows (cf. [4], Th. 9.3.1) that $\mathfrak{J}$ is a characteristic subgroup of $\mathfrak{H}$ and hence $\mathfrak{J} \neq 1$ would be a normal Π-subgroup of $\mathfrak{G}$ contrary to hypothesis. It follows that $\mathfrak{J}$ is not normal in $\mathfrak{H}$. In particular $\mathfrak{J}$ does not commute elementwise with $\mathfrak{N}$. Thus $\mathfrak{J}$ is not contained in $\mathfrak{Z}_{\mathfrak{N}}$ the centralizer of $\mathfrak{N}$.

The group $\mathfrak{Z}_{\mathfrak{N}}$ is normal in $\mathfrak{G}$. It follows that the index $[\mathfrak{G} : \mathfrak{Z}_{\mathfrak{N}}]$ is divisible by a prime $r \in \Pi$.

On the other hand, the factor group of the normalizer over the centralizer satisfies

$$\mathfrak{N}_{\mathfrak{N}}/\mathfrak{Z}_{\mathfrak{N}} \cong \mathfrak{G}/\mathfrak{Z}_{\mathfrak{N}}$$

so that it is isomorphic to a subgroup of the automorphism group of the cyclic group $\mathfrak{N}$. Hence $\mathfrak{G}/\mathfrak{Z}_{\mathfrak{N}}$ is abelian and therefore contains a normal subgroup $\mathfrak{M}_1/\mathfrak{Z}_{\mathfrak{N}}$ of index r. Hence $\mathfrak{G}$ contains a maximal normal subgroup $\mathfrak{M}_1$, of prime index r, where $r \in \Pi$, contrary to (6). It follows that $\mathfrak{G}/\mathfrak{N}$ does not contain a non-trivial normal Π-subgroup.

Since $\mathfrak{G}/\mathfrak{N}$ is also supersolvable, it follows from the minimal property of $\mathfrak{G}$ that $\mathfrak{G}/\mathfrak{N}$ contains a normal Hall $\hat{\Pi}$-subgroup, say $\mathfrak{H}/\mathfrak{N}$. But then $\mathfrak{H}$ is a normal Hall $\hat{\Pi}$-subgroup of $\mathfrak{G}$, contrary to hypothesis. □

Not all solvable groups possess the property enunciated in the lemma, e.g. $\mathfrak{S}_4$. On the other hand groups possessing this property need not be solvable, e.g. the direct product of $\mathfrak{A}_5$ and $\mathbb{Z}_{30}$. We have not found another well known class of finite groups which possess the property besides supersolvable groups.

Lemma 3. *Let $G(x)$ be a polynomial with integral coefficients, irreducible over $\mathbb{Q}$ and let $G(\theta) = 0$. Let J be any subfield of $\mathbb{Q}(\theta)$. Then*

$$G(x) = a N_{J/\mathbb{Q}}\big(H(x)\big)$$

identically, where $H(x)$ is a polynomial over J.

Proof. See [2], Lemma 2. □

3.

Proof of Theorem 1. Let L be a normal field such that $\big(|K|, |L|\big) = 1$ and $KL = \overline{K}$. Assume that $P(\Omega) \leqslant P(K)$. We have

$$P(\Omega L) \subset P(\Omega) \cap P(L) \leqslant P(K) \cap P(L). \tag{7}$$

Let q be a large prime, $q \in P(K) \cap P(L)$ and let

$$q = \mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_g$$

be its factorization in $\overline{K}$. Since $\overline{K}$ is normal we have

$$N_{\overline{K}/\mathbb{Q}}(\mathfrak{q}_i) = q^{|\overline{K}|/g}.$$

Now, let $\mathfrak{p}$ be the prime ideal factor of q of degree 1 in L. We have

$$N_{\overline{K}/\mathbb{Q}}\mathfrak{p} = N_{L/\mathbb{Q}} N_{KL/L}\mathfrak{p} = q^{|K|}. \tag{8}$$

On the other hand,

$$\mathfrak{p} = \mathfrak{q}_{i_1} \mathfrak{q}_{i_2} \cdots \mathfrak{q}_{i_s},$$

whence

$$N_{\overline{K}/\mathbb{Q}}\mathfrak{p} = \prod_{j=1}^{s} N_{\overline{K}/\mathbb{Q}}\mathfrak{q}_{i_j} = q^{|\overline{K}|s/g}. \tag{9}$$

It follows from (8) and (9) that

$$|K| = \frac{|\overline{K}|}{g}\, s = \frac{|K|\,|L|}{g}\, s;$$

hence

$$|L| \,\big|\, g. \tag{10}$$

In the proof the fact that L is normal has not been used, thus by symmetry

$$|K| \,\big|\, g.$$

Since $\big(|K|, |L|\big) = 1$, $|K|\,|L| \,\big|\, g$, thus $g = |KL| = |\overline{K}|$ and $q \in P(KL)$. This shows that $P(K) \cap P(L) \leqslant P(KL)$ and we get from (7)

$$P(\Omega L) \leqslant P(KL).$$

By the theorem of Bauer it follows that $\Omega L \supset KL$ and by Lemma 1, Ω contains a conjugate of K. □

Proof of Theorem 2. Let $\mathfrak{G}$ be the Galois group of $\overline{K}$, $\mathfrak{H}$ the subgroup of $\mathfrak{G}$ belonging to K, Π the set of primes dividing the order of $\mathfrak{H}$. Since $|\mathfrak{G}| = nm$, with $(n, m) = 1$, $\mathfrak{H}$ is a Hall Π-subgroup of $\mathfrak{G}$ and hence (cf. [4], Th. 9.3.1) any normal Π-subgroup of $\mathfrak{G}$ is a subgroup of $\mathfrak{H}$. By Lemma 2 either there is in $\mathfrak{G}$ a normal Π-subgroup $\neq 1$ or there is a normal Hall $\hat{\Pi}$-subgroup. The first case is impossible since then $\mathfrak{H}$ would contain a non-trivial normal

subgroup of $\mathfrak{G}$, thus there would be a normal field between K and $\overline{K}$. Therefore, there is in $\mathfrak{G}$ a normal subgroup $\mathfrak{N}$ such that $|\mathfrak{N}|\,|\mathfrak{H}| = |\mathfrak{G}|$. Let L be the field belonging to $\mathfrak{N}$. Clearly L is normal, $\big(|K|, |L|\big) = 1$, $KL = \overline{K}$ and therefore the field K has property (N).□

Proof of Theorem 3. Let

$$f(x) = cf_1(x)^{e_1} f_2(x)^{e_2} \cdots f_r(x)^{e_r}, \tag{11}$$

where $c \neq 0$ is a rational number and $f_1(x)$, $f_2(x)$, …, $f_r(x)$ are coprime polynomials with integral coefficients, each irreducible over $\mathbb{Q}$, and where $e_1, e_2, \ldots, e_r$ are non-zero integers. Put

$$F(x) = f_1(x) f_2(x) \cdots f_r(x).$$

Since the discriminant of $F(x)$ is not zero, there exist polynomials $A(x)$, $B(x)$ with integral coefficients such that

$$F(x)A(x) + F'(x)B(x) = D \tag{12}$$

identically, where D is a non-zero integer.

Let θ be a zero of some $f_j(x)$ and set $\Omega = \mathbb{Q}(\theta)$. Let L be a normal field postulated by the assumption that K has property (N) and let $q \in P(\Omega L)$ be a large prime. Clearly $q \in P(\Omega)$ and by the theorem of Dedekind, the congruence

$$f_j(x) \equiv 0 \pmod{q}$$

is soluble. Let x_0 be a solution. By (12) we have $F'(x_0) \not\equiv 0 \pmod{q}$, whence

$$F(x_0 + q) \not\equiv F(x_0) \pmod{q^2}.$$

By choosing x_1 to be either x_0 or $x_0 + q$, we can ensure that

$$f_j(x_1) \equiv 0 \pmod{q}, \quad F(x_1) \not\equiv 0 \pmod{q^2},$$

whence $f_j(x_1) \not\equiv 0 \pmod{q^2}$ and $f_i(x_1) \not\equiv 0 \pmod{q}$ for $i \neq j$. By the hypothesis of the theorem there exists $x_2 \equiv x_1 \pmod{q^2}$ such that

$$f(x_2) \equiv N_{K/\mathbb{Q}}(\omega) \quad \text{for some} \quad \omega \in K. \tag{13}$$

From the preceding congruences we have

$$f(x_2) \equiv 0 \pmod{q^{e_j}}, \quad f(x_2) \not\equiv 0 \pmod{q^{e_j+1}}. \tag{14}$$

Let the prime ideal factorization of q in $\overline{K} = KL$ be

$$q = \mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_g.$$

Since $\overline{K}$ is normal, we have

$$N_{\overline{K}/\mathbb{Q}} \mathfrak{q}_i = q^{|\overline{K}|/g}.$$

Write the prime ideal factorization of ω in $\overline{K}$ in the form

$$(\omega) = \mathfrak{q}_1^{\alpha_1} \mathfrak{q}_2^{\alpha_2} \cdots \mathfrak{q}_g^{\alpha_g} \mathfrak{A}\mathfrak{B}^{-1},$$

where $\mathfrak{A}$, $\mathfrak{B}$ are ideals in K relatively prime to q. Then

$$N_{K/\mathbb{Q}}(\omega) = q^{|K|(\alpha_1+\alpha_2+\ldots+\alpha_g)/g} N_{K/\mathbb{Q}}(\mathfrak{A}) N_{K/\mathbb{Q}}(\mathfrak{B})^{-1} \tag{15}$$

and $N_{K/\mathbb{Q}}(\mathfrak{A})$, $N_{K/\mathbb{Q}}(\mathfrak{B})$ are relatively prime to q.

It follows from (13), (14) and (15) that

$$|K|(\alpha_1 + \alpha_2 + \ldots + \alpha_g)/g = e_j, \quad \text{thus} \quad |K| \,\big|\, e_j g.$$

However, we assumed $\big(|K|, e_j\big) = 1$, whence $|K| \,\big|\, g$. On the other hand $q \in P(L)$ and so by the argument in the paragraph culminating with (10), $|L| \,\big|\, g$. Since $\big(|K|, |L|\big) = 1$, $|K|\,|L| \,\big|\, g$, thus $g = |KL|$ and $q \in P(KL)$. This shows that $P(\Omega L) \leqslant P(KL)$. By the theorem of Bauer it follows that $\Omega L \supset KL$ and by Lemma 1, Ω contains a conjugate of K, say K'. Applying Lemma 3 with $G(x) = f_j(x)$, $J = K'$ we conclude that

$$f_j(x) = a_j N_{K'/\mathbb{Q}}\big(H_j(x)\big),$$

where $H_j(x)$ is a polynomial over K'. Clearly

$$f_j(x) = a_j N_{K/\mathbb{Q}}\big(H'_j(x)\big),$$

where $H'_j(x)$ is a conjugate of H_j with coefficients in K.

By (11) and the multiplicative property of the norm, we get

$$f(x) = a N_{K/\mathbb{Q}}\big(h(x)\big),$$

where $h(x)$ is a polynomial over K. By the hypothesis of the theorem, taking x to be a suitable integer, we infer that a is the norm of an element α of K. Putting $\omega(x) = \alpha h(x)$, we obtain $f(x) = N_{K/\mathbb{Q}}\big(\omega(x)\big)$, identically. □

References

[1] M. Bauer, *Zur Theorie der algebraischen Zahlkörper*. Math. Ann. 77 (1916), 353–356.

[2] H. Davenport, D. J. Lewis, A. Schinzel, *Polynomials of certain special types*. Acta Arith. 9 (1964), 107–116; this collection: A6, 27–35.

[3] W. Feit, J. G. Thompson, *Solvability of groups of odd order*. Pacific J. Math. 13 (1963), 775–1029.

[4] M. Hall, *The Theory of Groups*. Macmillan, New York 1959.

[5] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper* II. Jahresber. Deutsch. Math.-Verein. 6 (1930).

[6] O. Haupt, *Einführung in die Algebra* II. Akademische Verlagsgesellschaft Geest & Portig, Leipzig 1954.

[7] H. Mann, *Introduction to Algebraic Number Theory*. The Ohio Univ. Press, Columbus 1955.

[8] A. Schinzel, *On a theorem of Bauer and some of its applications*. Acta Arith. 11 (1966), 333–344; *Corrigendum* ibid. 12 (1967), 425; this collection: C2, 179–189.

[9] H. Zassenhaus, *The Theory of Groups*, second edition. Chelsea, New York 1958.

Originally published in
Acta Arithmetica XI (1966), 419–432

On sums of roots of unity
(Solution of two problems of R. M. Robinson)

To Professor Viggo Brun on his 80th birthday

R. M. Robinson ([4]) proposed the following problem:

"How can we tell whether a given cyclotomic integer can be expressed as a sum of a prescribed number of roots of unity?"

An answer to this problem follows as Corollary 1 from the theorem below.

Theorem 1. *Let* $\sum_{i=1}^{k} a_i \zeta_N^{\alpha_i} = \vartheta$, *where the* a_i *are rational integers,* $\zeta_N = e^{2\pi i/N}$. *Suppose that* ϑ *is an algebraic integer of degree* d *and that* $(N, \alpha_1, \alpha_2, \ldots, \alpha_k) = 1$. *Then either there is a non-empty set* $I \subset \{1, 2, \ldots, k\}$ *such that*

$$\sum_{i \in I} a_i \zeta_N^{\alpha_i} = 0$$

or

$$N < d(2 \log d + 200k^2 \log 2k)^{20k^2}.$$

Corollary 1. *An algebraic integer of degree* d *is a sum of* k *roots of unity only if it is a sum of* k *roots of unity of common degree less than* $d(2 \log d + 200k^2 \log 2k)^{20k^2}$.

Corollary 2. *An algebraic integer* $\neq 0$ *is a sum of* k *roots of unity in infinitely many ways if and only if it is a sum of* $k - 2$ *roots of unity.*

Corollary 3. *If* $1 + \sum_{i=1}^{k} \zeta_N^{\alpha_i} = 0$, *and* $(N, \alpha_1, \ldots, \alpha_k) = 1$ *then either there is a non-empty set* $I \subset \{1, 2, \ldots, k\}$ *such that* $\sum_{i \in I} \zeta_N^{\alpha_i} = 0$ *or* $N < (200k^2 \log 2k)^{20k^2}$.

The proofs of Theorem 1, Corollary 1 and 2 are given later, Corollary 3 follows immediately from the theorem and is stated with the purpose of asking the question how much the inequality for N can be improved.

There is a statement in the literature ([2], p. 228) from which it would follow that $(200k^2 \log 2k)^{20k^2}$ can be replaced by $k + 2$. This is true for $k < 5$ but false for $k = 5$ as

the following example due to Robinson shows

$$1 + \zeta_{30} + \zeta_{30}^{7} + \zeta_{30}^{13} + \zeta_{30}^{19} + \zeta_{30}^{20} = 0.$$

Robinson made a conjecture ([4], §4) about the numbers $\sqrt{5}\cos(\pi/M) + i\sin(\pi/M)$. I prove this conjecture as the following

Theorem 2. *The number* $\sqrt{5}\cos(\pi/M) + i\sin(\pi/M)$ *is a sum of three roots of unity if and only if* $M = 2, 3, 5, 10,$ *or* 30.

According to Robinson two algebraic integers ξ and η are equivalent if for a suitable conjugate ξ' of ξ, η/ξ' is a root of unity. Theorem 2 implies

Corollary 4 (Conjecture 3 from [4]). *The numbers* $1+2i\cos(\pi/M)$ *and* $\sqrt{5}\cos(\pi/M)+i\sin(\pi/M)$ *are equivalent only for* $M = 2, 10$ *or* 30.

Corollary 5. *There exist infinitely many inequivalent cyclotomic integers which lie with all their conjugates in the circle* $|z| < 3$ *and are not sums of three roots of unity.*

The last corollary, which follows immediately from the fact that the numbers $\sqrt{5}\cos(\pi/M) + i\sin(\pi/M)$ for different M have different absolute values, disproves a conjecture made by Robinson at Boulder 1959 (cf. [4], §4). An analogous conjecture for the circle $|z| < 2$ is still unproved (l. c. Conjecture 1).

I conclude this introduction by expressing my thanks to Professor Robinson who let me have his manuscript before publication, to Professor Davenport who kindly supplied the proof of Lemma 2 and to Dr. A. Białynicki-Birula and Professor D. J. Lewis who discussed the subject with me and read my manuscript.

In the sequel $\mathbb{Q}$ denotes the rational field, $[K_2 : K_1]$ the degree of a field K_2 over a field K_1, and $|K| = [K : \mathbb{Q}]$. The empty sums are 0, the empty products 1.

Lemma 1. *For all positive integers* h *and* $N \geqslant 3$ *there exists an integer* D *satisfying the conditions*

$$1 \leqslant D \leqslant (\log N)^{20h}, \tag{1}$$

$$(iD + 1, N) = 1 \quad \textit{for} \quad i = 1, 2, \ldots, h. \tag{2}$$

Proof. For $h = 1$ we can take $D = q - 1$, where q is the least prime not dividing N. Since in that case $\sum_{p \leqslant D} \log p \leqslant \log N$, we get from [5], Theorem 10

$$D \leqslant 100 \quad \text{or} \quad 0.84D \leqslant \log N.$$

On the other hand $D \leqslant N$, which implies $D \leqslant (\log N)^{20}$ for all $N \geqslant 3$.

Therefore we can assume $h \geqslant 2$. Since $D = N$ satisfies the condition (2) we can assume further $N > (\log N)^{20h}$, which implies

$$\log N > 107h, \quad \log\log N > 5. \tag{3}$$

Let A be the product of all primes not exceeding $10h$, and let $p_1 < p_2 < \ldots < p_r$ be all the other primes dividing N. Let $P(A, X, p_1, \ldots, p_r)$ be the number of all integers x satisfying the conditions

$$1 \leqslant x \leqslant X, \quad x \equiv 0 \pmod{A},$$
$$ix + 1 \not\equiv 0 \pmod{p_j} \quad (1 \leqslant i \leqslant h,\ 1 \leqslant j \leqslant r).$$

The second condition above is equivalent to h conditions of the form $x \not\equiv a_{ij} \pmod{p_j}$. Thus by Brun's method ([1], cf. [6], Lemma 7) for any given sequence of integers $r = r_0 \geqslant r_1 \geqslant \ldots \geqslant r_t = 1$ we have

$$P(A, X, p_1, \ldots, p_r) > \frac{E}{A} X - R, \tag{4}$$

where

$$E = 1 - h \sum_{\alpha=1}^{r} \frac{1}{p_\alpha} + h^2 \sum_{\alpha=1}^{r} \sum_{\substack{\alpha_1 \leqslant r \\ \alpha_1 < \alpha}} \frac{1}{p_\alpha p_{\alpha_1}} - h^3 \sum_{\alpha=1}^{r} \sum_{\substack{\alpha_1 \leqslant r \\ \alpha_1 < \alpha}} \sum_{\substack{\beta_1 \leqslant r \\ \beta_1 < \alpha_1}} \frac{1}{p_\alpha p_{\alpha_1} p_{\beta_1}}$$
$$+ \ldots + \sum_{\alpha=1}^{r} \sum_{\substack{\alpha_1 \leqslant r_1 \\ \alpha_1 < \alpha}} \sum_{\substack{\beta_1 \leqslant r_1 \\ \beta_1 < \alpha_1}} \cdots \sum_{\substack{\alpha_{t-1} \leqslant r_{t-1} \\ \alpha_{t-1} < \beta_{t-2}}} \sum_{\substack{\beta_{t-1} \leqslant r_{t-1} \\ \beta_{t-1} < \alpha_{t-1}}} \sum_{\substack{\alpha_t \leqslant r_t \\ \alpha_t < \beta_{t-1}}} \frac{1}{p_\alpha p_{\alpha_1} \cdots p_{\alpha_t}}$$

and

$$R \leqslant (1 + hr) \prod_{n=1}^{t} (1 + hr_n)^2. \tag{5}$$

Denote by r_n $(1 \leqslant n \leqslant t)$ the least positive integer such that

$$\pi_n = \prod_{r_n < s \leqslant r_{n-1}} \left(1 - \frac{h}{p_s}\right) \geqslant \frac{1}{1.3}$$

and choose t so that

$$\pi_t = \prod_{s \leqslant r_{t-1}} \left(1 - \frac{h}{p_s}\right) \geqslant \frac{1}{1.3}.$$

It follows hence (cf. [6], formulae (18) and (32))

$$\pi_n \leqslant \frac{10}{9} \cdot \frac{1}{1.3} = \frac{1}{1.17} < \frac{8}{9} \tag{6}$$

and

$$E > 0.5 \prod_{s=1}^{r} \left(1 - \frac{h}{p_s}\right). \tag{7}$$

We shall show that

$$\log \prod_{s=1}^{r} \left(1 - \frac{h}{p_s}\right) > -\frac{h \log\log N}{e \log eh} > -0.22h \log\log N. \tag{8}$$

c

Indeed, since $p_1 > 10h$ we have by [5] (formula at the bottom of p. 87)

$$\sum_{s=1}^{r} \frac{1}{p_s^2} \leqslant \frac{2.04}{10h \log 10h}\,.$$

Hence

$$\log \prod_{s=1}^{r}\Big(1-\frac{h}{p_s}\Big) + \log \prod_{s=1}^{r}\Big(1-\frac{1}{p_s}\Big)^{-h} \geqslant -\sum_{s=1}^{r}\sum_{m=2}^{\infty}\frac{1}{m}\Big(\frac{h}{p_s}\Big)^m \tag{9}$$
$$\geqslant -\frac{1}{2}\sum_{s=1}^{r}\Big(\frac{h}{p_s}\Big)^2\frac{1}{1-h/p_s} \geqslant -\frac{5}{9}h^2\sum_{s=1}^{r}\frac{1}{p_s^2} \geqslant -\frac{0.2h}{\log 10h}\,.$$

On the other hand, by [5], Theorem 15

$$\frac{A}{\varphi(A)}\prod_{s=1}^{r}\Big(1-\frac{1}{p_s}\Big)^{-1} = \frac{AN}{\varphi(AN)} < e^C \log\log AN + \frac{2.51}{\log\log AN}\,. \tag{10}$$

Since by [5], Theorem 9, and by (3)

$$\log A < 11h < \frac{11}{107}\log N \tag{11}$$

we get

$$e^C \log\log AN + \frac{2.51}{\log\log AN} < e^C \log\log N + \frac{11e^C}{107} + \frac{2.51}{5} < e^C\,(\log\log N + 0.4)\,.$$

Further by [5], Theorem 8

$$\frac{A}{\varphi(A)} > e^C \log 10h\Big(1-\frac{1}{2\log^2 10h}\Big) > e^C(\log h + 2.1).$$

Since by (3) $\log\log N > \log 10h$ we get from (9), (10) and the last two inequalities

$$\log\prod_{s=1}^{r}\Big(1-\frac{h}{p_s}\Big) > -h\Big(\log(\log\log N + 0.4) - \log(\log h + 2.1) + \frac{0.2}{\log 10h}\Big) \tag{12}$$
$$> -h(\log\log\log N - \log\log eh).$$

Clearly, $\log x - \log a = 1 + \log(x/ae) \leqslant x/ae$. Thus (12) implies (8). Now by (6) and (8)

$$(t-1)\log 1.17 \leqslant \frac{h\log\log N}{e\log eh} < \frac{h\log\log N}{e\log(h+1)}\,,$$

hence

$$(2t+1)\log(h+1) < 3\log(h+1) + \frac{2h\log\log N}{e\log 1.17} \tag{13}$$
$$< 3\log(h+1) + 4.7h\log\log N.$$

This inequality permits to estimate R. The estimation of R given in [6] is not quite correct and not applicable under the present circumstances. Since p_s is certainly greater than the

sth prime, we have by [5], Corollary to Theorem 3, $p_s > s \log s$. Hence

$$\log \pi_n = \sum_{r_{n-1} \geqslant s > r_n} \log\Big(1 - \frac{h}{p_s}\Big) > -\frac{10}{9} \sum_{r_{n-1} \geqslant s > r_n} \frac{h}{p_s}$$
$$> -\frac{10}{9} h \int_{r_n}^{r_{n-1}} \frac{dt}{t \log t} = -\frac{10}{9} h \log \frac{\log r_{n-1}}{\log r_n}.$$

It follows by (6)

$$\frac{\log r_n}{\log r_{n-1}} < \Big(\frac{1}{1.17}\Big)^{9/10h} < \Big(1 + \frac{9}{10h} \log 1.17\Big)^{-1} \leqslant (1 + 0.141 h^{-1})^{-1},$$

and by induction

$$\frac{\log r_n}{\log r} < (1 + 0.141 h^{-1})^{-n} \quad (1 \leqslant n \leqslant t - 1). \tag{14}$$

On the other hand

$$\log N \geqslant \sum_{s=1}^{r} \log p_s > r \log 10h \geqslant r \log 20,$$

thus $\log r < \log \log N - 1$.

It follows from (5), (13) and (14) that

$$\log R \leqslant (2t + 1) \log(h + 1) + \log r + 2 \sum_{n=1}^{t-1} \log r_n$$
$$< 3 \log(h + 1) + 4.7 h \log \log N + (\log \log N - 1)\Big(2 \sum_{n=0}^{\infty} (1 + 0.141 h^{-1})^{-n} - 1\Big)$$
$$< 3 \log(h + 1) + 4.7 h \log \log N + (\log \log N - 1)(14.2h + 1)$$
$$< 19.4 h \log \log N - 11h - 1.$$

Since by (11) $\log A < 11h$, we have

$$\log R < 19.4 h \log \log N - \log A - 1. \tag{15}$$

It follows from (7), (8) and (15) that

$$\log\Big(\frac{E}{A} (\log N)^{20h}\Big) > \log R$$

thus by (4)

$$P\big(A, (\log N)^{20h}, p_1, \ldots, p_r\big) > 0$$

and by the definition of P there exists an integer D satisfying (1) and (2). □

Lemma 2. *Let $f_j(x_1, \ldots, x_n)$ $(1 \leqslant j \leqslant n)$ be polynomials of degrees $m_1, \ldots, m_n$ respectively, with coefficients in a number field K. If*

$$f_j(\xi_1, \ldots, \xi_n) = 0 \quad (1 \leqslant j \leqslant n)$$

and

$$\frac{\partial(f_1,\ldots,f_n)}{\partial(x_1,\ldots,x_n)}(\xi_1,\ldots,\xi_n)\neq 0 \tag{16}$$

then

$$[K(\xi_1,\ldots,\xi_n):K]\leqslant m_1m_2\cdots m_n.$$

Proof (due to H. Davenport). Let $\varphi_1(x_1,\ldots,x_n),\ldots,\varphi_n(x_1,\ldots,x_n)$ be complete polynomials of degrees $m_1,\ldots,m_n$ respectively, with arbitrary complex coefficients which differ by less than ε in absolute value from the corresponding coefficients of $f_1,\ldots,f_n$. By Bezout's theorem, the equations $\varphi_1=0$, ..., $\varphi_n=0$ have exactly $m_1m_2\cdots m_n$ distinct solutions for "general" values of all the coefficients. We shall prove that one of these solutions tends to $\xi_1,\ldots,\xi_n$ as $\varepsilon\to 0$.

This will suffice to prove the result. Indeed, the equations $f_j(x_1,\ldots,x_n)=0$ $(j=1,\ldots,n)$ define a union of algebraic varieties over K. If the point $(\xi_1,\ldots,\xi_n)$ were on a variety of positive dimension, defined by the equations $g_i(x_1,\ldots,x_n)=0$ $(i=1,\ldots,N)$, where $g_i=f_i$ for $i\leqslant n$, then by a known theorem ([3], p. 84) the rank of the matrix

$$\left[\frac{\partial g_i}{\partial x_j}(\xi_1,\ldots,\xi_n)\right]$$

would be less than n, contrary to (16). Hence $(\xi_1,\ldots,\xi_n)$ is an isolated point, and therefore the ξ_i are algebraic over K. Now consider the points $\left(\xi_1^{(\nu)},\ldots,\xi_n^{(\nu)}\right)$ which are algebraically conjugate to $(\xi_1,\ldots,\xi_n)$ over K. These are distinct and their number is $[K(\xi_1,\ldots,\xi_n):K]$. Also each of them satisfies the equations $f_j=0$ and the condition $\dfrac{\partial(f_1,\ldots,f_n)}{\partial(x_1,\ldots,x_n)}\neq 0$.

Hence it will follow from the result stated above that near each of them there is one of the solutions of $\varphi_1=0,\ldots,\varphi_n=0$ and so their number is at most $m_1m_2\cdots m_n$.

The value of $\varphi_j(\xi_1,\ldots,\xi_n)$, or of any derivative of $\varphi_j(x_1,\ldots,x_n)$ at $(\xi_1,\ldots,\xi_n)$, differs from the corresponding value for $f_j(\xi_1,\ldots,\xi_n)$ by an amount that is $O(\varepsilon)$. Hence

$$\varphi_j(\xi_1+\eta_1,\ldots,\xi_n+\eta_n)$$
$$=\varepsilon_j+\sum_{i=1}^{n}(\lambda_{ij}+\varepsilon_{ij})\eta_i+\sum_{i_1=1}^{n}\sum_{i_2=1}^{n}\left(\lambda_{i_1i_2j}+\varepsilon_{i_1i_2j}\right)\eta_{i_1}\eta_{i_2}+\ldots,$$

where all $\varepsilon_j,\varepsilon_{ij},\ldots$ are $O(\varepsilon)$ and where the numbers $\lambda_{ij},\lambda_{i_1i_2j},\ldots$ are partial derivatives of f_j at $(\xi_1,\ldots,\xi_n)$ and so are independent of ε. Also

$$\det\lambda_{ij}=\frac{\partial(f_1,\ldots,f_n)}{\partial(x_1,\ldots,x_n)}(\xi_1,\ldots,\xi_n)\neq 0.$$

It follows from the well known process for the inversion of power series (e.g. by iteration) that the equations

$$\varphi_j(\xi_1+\eta_1,\ldots,\xi_n+\eta_n)=0\quad\text{for}\quad j=1,\ldots,n$$

have a solution with $\eta_1,\ldots,\eta_n=O(\varepsilon)$. Hence the result. □

Remark. The above proof fails if K has characteristic different from 0. However, Mr. Swinnerton-Dyer tells me that the lemma is still valid and can be proved by using Weil's theory of intersections.

Proof of Theorem 1. The theorem clearly holds for $N < 3$. Assume that $N \geqslant 3$,

$$\sum_{i=1}^{k} a_i \zeta_N^{\alpha_i} = \vartheta, \quad |\mathbb{Q}(\vartheta)| = d, \quad (N, \alpha_1, \ldots, \alpha_k) = 1. \tag{17}$$

Let D be an integer whose existence is ensured by Lemma 1 for $h = k - 1$. Among the numbers α_i let there be exactly n that are distinct mod $N_1 = N/(N, D)$. By a suitable permutation of the terms in (17) we can achieve that $\alpha_{s_1}, \alpha_{s_2}, \ldots, \alpha_{s_n}$ are all distinct mod N_1, $0 = s_0 < s_1 < \ldots < s_n = k$ and

$$\alpha_i \equiv \alpha_{s_\nu} \pmod{N_1} \quad \text{if} \quad s_{\nu-1} < i \leqslant s_\nu \ (1 \leqslant \nu \leqslant n). \tag{18}$$

Let us choose numbers γ_ν, such that

$$\gamma_\nu \equiv \alpha_{s_\nu} \pmod{N_1}, \quad (\gamma_\nu, N) = (\alpha_{s_\nu}, N_1) \quad (1 \leqslant \nu \leqslant n). \tag{19}$$

It follows from elementary congruence considerations that such choice is possible.

We write equation (17) in the form

$$\sum_{\nu=1}^{n} \zeta_N^{\gamma_\nu} S_\nu = \vartheta, \tag{20}$$

where

$$S_\nu = \sum_{i=s_{\nu-1}+1}^{s} a_i \zeta_N^{\alpha_i - \gamma_\nu} \quad (1 \leqslant \nu \leqslant n).$$

By (18) and (19)

$$S_\nu \in \mathbb{Q}(\zeta_D) \quad (1 \leqslant \nu \leqslant n).$$

By (2) $(N, jD - D + 1) = 1$ thus ζ_N^{jD-D+1} is for each positive $j \leqslant k$ a conjugate of ζ_N. Clearly

$$\zeta_N^{(\alpha_i - \gamma_\nu)(jD-D+1)} = \zeta_N^{\alpha_i - \gamma_\nu} \quad (s_{\nu-1} < i \leqslant s_\nu).$$

Substituting ζ_N^{jD-D+1} for ζ_N in (20) we get

$$\sum_{\nu=1}^{n} \zeta_N^{\gamma_\nu (jD-D+1)} S_\nu = \vartheta_j \quad (1 \leqslant j \leqslant n),$$

where ϑ_j is a suitable conjugate of ϑ. Since $\mathbb{Q}(\vartheta)$ is an Abelian field, $\vartheta_j \in \mathbb{Q}(\vartheta)$.

In Lemma 2 we take:

$$f_j(x_1, \ldots, x_n) = \sum_{\nu=1}^{n} x_\nu^{jD-D+1} S_\nu - \vartheta_j \quad (1 \leqslant j \leqslant n),$$

$$K = \mathbb{Q}(\zeta_D, \vartheta), \quad \xi_\nu = \zeta_N^{\gamma_\nu} \quad (1 \leqslant \nu \leqslant n).$$

Hence

$$\frac{\partial(f_1,\dots,f_n)}{\partial(x_1,\dots,x_n)}(\xi_1,\dots,\xi_n) = \prod_{j=1}^{n}(jD-D+1)\prod_{\nu=1}^{n}S_\nu \prod_{1\leqslant\nu''<\nu'\leqslant n}\left(\zeta_N^{\gamma_{\nu'}D}-\zeta_N^{\gamma_{\nu''}D}\right). \tag{21}$$

If $S_\nu = 0$ for some $\nu \leqslant n$ then

$$\sum_{i=s_{\nu-1}+1}^{s_\nu} a_i\zeta_N^{\alpha_i} = 0$$

and the theorem holds with $I = \{s_{\nu-1}+1,\dots,s_\nu\}$.

If $S_\nu \neq 0$ for all $\nu \leqslant n$, then by (21) and the choice of γ_ν we have

$$\frac{\partial(f_1,\dots,f_n)}{\partial(x_1,\dots,x_n)}(\xi_1,\dots,\xi_n) \neq 0.$$

Therefore, by Lemma 2

$$\left|\mathbb{Q}\left(\zeta_N^{\gamma_1},\zeta_N^{\gamma_2},\dots,\zeta_N^{\gamma_n}\right)\right| \leqslant \left|\mathbb{Q}(\zeta_D,\vartheta)\right|\prod_{j=0}^{n-1}(jD+1) < n!D^n d \leqslant k!D^k d. \tag{22}$$

On the other hand by (18) and (19)

$$(N,\gamma_\nu) = \left(N_1,\alpha_{s_\nu}\right) = \left(N_1,\alpha_{s_{\nu-1}+1},\dots,\alpha_{s_\nu}\right),$$

hence

$$(N,\gamma_1,\dots,\gamma_n) = (N_1,\alpha_1,\dots,\alpha_k) = 1$$

and

$$\left|\mathbb{Q}\left(\zeta_N^{\gamma_1},\dots,\zeta_N^{\gamma_n}\right)\right| = \varphi(N).$$

It follows now from (22) and (1) (applied with $h = k-1$)

$$\varphi(N) \leqslant k!(\log N)^{20k(k-1)}d. \tag{23}$$

If $N < (200k^2\log 2k)^{20k^2}$ the theorem certainly holds.

If $N \geqslant (200k^2\log 2k)^{20k^2} > 10^{42}$, it follows from [5], Theorem 15, that

$$\varphi(N) > \frac{N}{\log N}. \tag{24}$$

Also, if $N \geqslant (200k^2\log 2k)^{20k^2}$

$$k! < (\log N)^k. \tag{25}$$

It follows from (23), (24) and (25) that

$$N(\log N)^{-20k^2} \leqslant d.$$

Taking $N_0 = d\big(2\log d + 200k^2\log 2k\big)^{20k^2}$ we find that

$$N_0(\log N_0)^{-20k^2} = d\left(\frac{2\log d + 200k^2\log 2k}{\log d + 20k^2\log(2\log d + 200k^2\log 2k)}\right)^{20k^2} > d,$$

[c] because $200k^2\log 2k > 20k^2\log(400k^2\log 2k)$.

Since the function $N(\log N)^{-20k^2}$ is increasing for $N > e^{20k^2}$ it follows that $N < N_0$. The proof is complete. □

Proof of Corollary 1. Assume that

$$\vartheta = \sum_{i=1}^{k} \zeta_N^{\alpha_i}.$$

Let I be a set contained in $\{1, 2, \ldots, k\}$ saturated with respect to the property that $\sum_{i\in I} \zeta_N^{\alpha_i} = 0$. We have $\vartheta = \sum_{i\in I} \zeta_N^{\alpha_i}$ and by the choice of I and Theorem 1

$$\frac{N}{(N, \operatorname*{GCD}_{i\in I} \alpha_i)} < d(2\log d + 200k^2\log 2k)^{20(k-\kappa)^2},$$

where κ is the number of elements in I. If $\kappa = 0$ we have the desired conclusion, if $\kappa > 0$ then $\kappa \geqslant 2$ and

$$\vartheta = \begin{cases} \displaystyle\sum_{i\in I} \zeta_N^{\alpha_i} + \sum_{j=1}^{\kappa/2} 1 + \sum_{j=1}^{\kappa/2}(-1), & \kappa \text{ even}, \\ \displaystyle\sum_{i\in I} \zeta_N^{\alpha_i} + \zeta_3 + \zeta_3^{-1} + \sum_{j=1}^{(\kappa-1)/2} 1 + \sum_{j=1}^{(\kappa-3)/2}(-1), & \kappa \text{ odd} \geqslant 3. \end{cases}$$

The least common degree of all k roots of unity occurring in the above representation of ϑ does not exceed

$$6d(2\log d + 200k^2\log 2k)^{20(k-\kappa)^2} < d(2\log d + 200k^2\log 2k)^{20k^2},$$

which completes the proof. □

Proof of Corollary 2. The sufficiency of the condition is immediate since

$$\sum_{i=1}^{k-2} \zeta_N^{\alpha_i} = \sum_{i=1}^{k-2} \zeta_N^{\alpha_i} + \zeta_M - \zeta_M,$$

where M is arbitary. On the other hand, if ϑ has infinitely many representations as the sum of k roots of unity, then there must be among them a representation

$$\vartheta = \sum_{i=1}^{k} \zeta_N^{\alpha_i}, \quad (N, \alpha_1, \ldots, \alpha_k) = 1$$

not satisfying the inequality

$$N < d(2\log d + 200k^2\log 2k)^{20k^2}.$$

By Theorem 1 there is a non-empty set $I \subset \{1, 2, \dots, k\}$ such that $\sum_{i \in I} \zeta_N^{\alpha_i} = 0$ and denoting by κ the number of elements in I we have $k > \kappa \geqslant 2$. Since

$$1 = \begin{cases} \sum_{j=1}^{\kappa/2} 1 + \sum_{j=1}^{(\kappa-2)/2} (-1), & \kappa \text{ even}, \\ \zeta_6 + \zeta_6^{-1} + \sum_{j=1}^{(\kappa-3)/2} 1 + \sum_{j=1}^{(\kappa-3)/2} (-1), & \kappa \text{ odd} \geqslant 3, \end{cases}$$

we can replace one of the $k - \kappa$ terms in the sum $\sum_{i \in I} \zeta_N^{\alpha_i} = \vartheta$ by a sum of $\kappa - 1$ roots of unity, thus obtaining a representation of ϑ as the sum of $k - 2$ roots of unity. □

Proof of Theorem 2. Suppose that

$$\sqrt{5} \cos \frac{\pi}{M} + i \sin \frac{\pi}{M} = \zeta_{m_1}^{\alpha_1} + \zeta_{m_2}^{\alpha_2} + \zeta_{m_3}^{\alpha_3}, \quad \text{where} \quad (\alpha_i, m_i) = 1. \tag{26}$$

Put $N = 5\,[2M, m_1, m_2, m_3]$, $\alpha = \dfrac{N}{2M}$, $\beta = \dfrac{N\alpha_1}{m_1}$, $\gamma = \dfrac{N\alpha_2}{m_2}$, $\delta = \dfrac{N\alpha_3}{m_3}$. Then

$$(\alpha, \beta, \gamma, \delta) = 5. \tag{27}$$

Since $\frac{1}{2}(\sqrt{5} - 1) = \zeta_5 + \zeta_5^{-1} = \zeta_N^{N/5} + \zeta_N^{-N/5}$ (26) can be written in the form

$$\left(\zeta_N^{N/5} + \zeta_N^{-N/5}\right)\left(\zeta_N^{\alpha} + \zeta_N^{-\alpha}\right) + \zeta_N^{\alpha} = \zeta_N^{\beta} + \zeta_N^{\gamma} + \zeta_N^{\delta}. \tag{28}$$

Now we distinguish two cases according as $3 \mid N$ and $3 \nmid N$. In the first case at least one of the numbers $\pm\frac{1}{3}N + 1$ is relatively prime to N. Hence one of the numbers $\zeta_3^{\pm 1}\zeta_N$ is conjugate to ζ_N. Denote it for simplicity by $\varrho\zeta_N$ and substitute for ζ_N into (28). Since $\varrho^{N/5} = 1$, we get

$$\left(\zeta_N^{N/5} + \zeta_N^{-N/5}\right)\left(\varrho^{\alpha}\zeta_N^{\alpha} + \varrho^{-\alpha}\zeta_N^{-\alpha}\right) + \varrho^{\alpha}\zeta_N^{\alpha} = \varrho^{\beta}\zeta_N^{\beta} + \varrho^{\gamma}\zeta_N^{\gamma} + \varrho^{\delta}\zeta_N^{\delta}. \tag{29}$$

By taking complex conjugates of (28) and (29) and substituting afterwards

$$y = \zeta_N^{\beta}, \quad z = \zeta_N^{\gamma}, \quad t = \zeta_N^{\delta};$$

$$A = \tfrac{1}{2}(\sqrt{5} + 1)\zeta_{2M} + \tfrac{1}{2}(\sqrt{5} - 1)\zeta_{2M}^{-1}, \quad B = \tfrac{1}{2}(\sqrt{5} - 1)\zeta_{2M} + \tfrac{1}{2}(\sqrt{5} + 1)\zeta_{2M}^{-1},$$

$$C = \tfrac{1}{2}(\sqrt{5} + 1)\varrho^{\alpha}\zeta_{2M} + \tfrac{1}{2}(\sqrt{5} - 1)\varrho^{-\alpha}\zeta_{2M}^{-1}, \tag{30}$$

$$D = \tfrac{1}{2}(\sqrt{5} - 1)\varrho^{\alpha}\zeta_{2M} + \tfrac{1}{2}(\sqrt{5} + 1)\varrho^{-\alpha}\zeta_{2M}^{-1},$$

we get the following system of equations

$$A = y + z + t, \tag{31}$$

$$B = y^{-1} + z^{-1} + t^{-1}, \tag{32}$$

$$C = \varrho^{\beta} y + \varrho^{\gamma} z + \varrho^{\delta} t, \tag{33}$$

$$D = \varrho^{-\beta} y^{-1} + \varrho^{-\gamma} z^{-1} + \varrho^{-\delta} t^{-1}. \tag{34}$$

If $\beta \equiv \gamma \equiv \delta \pmod 3$ it follows from (31) and (33) that $C = \varrho^{\beta} A$. Hence by (30)

$$\tfrac{1}{2}(\sqrt{5} + 1)(\varrho^{\alpha} - \varrho^{\beta})\zeta_{2M} + \tfrac{1}{2}(\sqrt{5} - 1)(\varrho^{-\alpha} - \varrho^{\beta})\zeta_{2M}^{-1} = 0. \tag{35}$$

The coefficients of ζ_{2M} and ζ_{2M}^{-1} do not both vanish, since that would give $\alpha \equiv \beta \equiv 0 \pmod 3$ and $\alpha \equiv \beta \equiv \gamma \equiv \delta \equiv 0 \pmod 3$ contrary to (27). Thus they have different absolute values, and (35) is impossible.

Consider now the case when exactly two among the numbers β, γ, δ are congruent mod 3, e.g. $\beta \equiv \gamma \not\equiv \delta \pmod 3$. Eliminating y, z and t from the equations (31) to (34) we get

$$(C - \varrho^{\beta}A)(D - \varrho^{-\beta}B) = |\varrho^{\delta} - \varrho^{\beta}|^2 = 3. \tag{36}$$

Substituting the values for A, B, C, D from (30) we obtain

$$\begin{aligned}(\varrho^{\alpha} - \varrho^{\beta})(\varrho^{\alpha} - \varrho^{-\beta})\zeta_M + \tfrac{1}{2}\big(3 + \sqrt{5}\big)|\varrho^{\alpha} - \varrho^{\beta}|^2 \\ + \tfrac{1}{2}\big(3 - \sqrt{5}\big)|\varrho^{-\alpha} - \varrho^{\beta}|^2 - 3 + (\varrho^{-\alpha} - \varrho^{\beta})(\varrho^{-\alpha} - \varrho^{-\beta})\zeta_M^{-1} = 0.\end{aligned} \tag{37}$$

If $\beta \equiv \pm\alpha \pmod 3$, we get $\frac{1}{2}\big(3 \mp \sqrt{5}\big)\big|\varrho^{\mp\alpha} - \varrho^{\beta}\big|^2 - 3 = 0$, which is impossible. Hence $\beta \not\equiv \pm\alpha \pmod 3$ and (37) takes the form

$$3\zeta_M + 6 + 3\zeta_M^{-1} = 0, \qquad \text{if} \quad \beta \not\equiv 0 \pmod 3; \tag{38}$$

$$-3\varrho^{\alpha}\zeta_M + 6 - 3\varrho^{-\alpha}\zeta_M^{-1} = 0, \quad \text{if} \quad \beta \equiv 0 \not\equiv \alpha \pmod 3. \tag{39}$$

It follows from (38) that $\zeta_M = -1$, $M = 2$ and from (39) $\varrho^{\alpha}\zeta_M = 1$, $M = 3$.

Consider next the case when β, γ, δ are all different mod 3. We can assume without loss of generality that $\beta \equiv 0 \pmod 3$, $\gamma \equiv 1 \pmod 3$, $\delta \equiv 2 \pmod 3$.

If $\alpha \equiv 0 \pmod 3$, then $C = A$ and it follows from (31) and (33) that

$$A - y = z + t = \varrho z + \varrho^2 t,$$

hence $t = \varrho z$ and

$$A = y - \varrho^2 z, \quad B = y^{-1} - \varrho z^{-1}. \tag{40}$$

Since y and z are roots of unity, $|y - \varrho^2 z| \leqslant 2$. On the other hand by (30)

$$|A| = \big|\sqrt{5}\cos(\pi/M) + i\sin(\pi/M)\big| = \sqrt{5 - 4\sin^2(\pi/M)}\,.$$

It follows that

$$5 - 4\sin^2(\pi/M) \leqslant 4, \quad |\sin(\pi/M)| \geqslant \tfrac{1}{2},$$

and $6 \geqslant M > 1$. Further, by (40)

$$-\varrho^2 yz = \frac{A}{B} = \frac{\sqrt{5}\cos(\pi/M) + i\sin(\pi/M)}{\sqrt{5}\cos(\pi/M) - i\sin(\pi/M)}\,.$$

It can easily be verified that for $M = 3, 4$ or 6 the quotient on the right hand side is not an algebraic integer, hence the only possible values for M here are $M = 2$ or 5.

If $\alpha \not\equiv 0 \pmod 3$, then eliminating y, z and t from (31) to (34) we get

$$A^3 - C^3 = 3yzt(AB - CD) \quad \text{and} \quad (AB - CD)^2 - \tfrac{1}{9}(A^3 - C^3)(B^3 - D^3) = 0.$$

The substitution of the values for A, B, C, D from (30) gives

$$-3\varrho^{-\alpha}\zeta_M^2 + 3\varrho^{\alpha}\zeta_M - 3 + 3\varrho^{-\alpha}\zeta_M^{-1} - 3\varrho^{\alpha}\zeta_M^{-2} = 0.$$

Hence

$$(\varrho^{\alpha}\zeta_M)^4 - (\varrho^{\alpha}\zeta_M)^3 + (\varrho^{\alpha}\zeta_M)^2 - (\varrho^{\alpha}\zeta_M) + 1 = 0, \quad \varrho^{\alpha}\zeta_M = \zeta_{10}^{\varepsilon},$$

where $(\varepsilon, 10) = 1$ and $\zeta_M = \varrho^{-\alpha}\zeta_{10}^{\varepsilon}$. This gives $M = 30$.

It remains to consider the case when $3 \nmid N$. In this case ζ_N^3 is a conjugate of ζ_N and substituting it for ζ_N in the equation (28) we get

$$\left(\zeta_N^{3N/5} + \zeta_N^{-3N/5}\right)\left(\zeta_N^{3\alpha} + \zeta_N^{-3\alpha}\right) + \zeta_N^{3\alpha} = \zeta_N^{3\beta} + \zeta_N^{3\gamma} + \zeta_N^{3\delta}. \tag{41}$$

Now,

$$\zeta_N^{3N/5} + \zeta_N^{-3N/5} = \tfrac{1}{2}(-\sqrt{5} - 1).$$

By taking the complex conjugate of (41) and substituting afterwards

$$\begin{aligned} E &= \tfrac{1}{2}(-\sqrt{5}+1)\zeta_{2M}^3 + \tfrac{1}{2}(-\sqrt{5}-1)\zeta_{2M}^{-3}, \\ F &= \tfrac{1}{2}(-\sqrt{5}-1)\zeta_{2M}^3 + \tfrac{1}{2}(-\sqrt{5}+1)\zeta_{2M}^{-3} \end{aligned} \tag{42}$$

we get the following system of equations

$$\begin{aligned} A &= y + z + t, \\ B &= y^{-1} + z^{-1} + t^{-1}, \\ E &= y^3 + z^3 + t^3, \\ F &= y^{-3} + z^{-3} + t^{-3}. \end{aligned}$$

Eliminating y, z and t we obtain

$$A^3 - E = 3yzt(AB - 1) \quad \text{and} \quad (AB-1)^2 - \tfrac{1}{9}(A^3 - E)(B^3 - F) = 0.$$

The substitution of the values of A, B, E, F from (30) and (42) gives

$$-\zeta_M^3 - \zeta_M^2 - \zeta_M^{-2} - \zeta_M^{-3} = 0.$$

Hence

$$\begin{gathered} \zeta_M^6 + \zeta_M^5 + \zeta_M + 1 = (\zeta_M + 1)(\zeta_M^5 + 1) = 0, \\ \zeta_M = -1 \text{ or } \zeta_M^5 = -1, \quad \text{and} \quad M = 2 \text{ or } M = 10. \end{gathered}$$

This completes the proof that the only values M for which $\eta_M = \sqrt{5}\cos(\pi/M) + i\sin(\pi/M)$ can be a sum of three roots of unity are 2, 3, 5, 10, or 30. On the other hand, it is easy to verify that

$$\begin{gathered} \eta_2 = 1 + \zeta_2 + \zeta_4, \quad \eta_3 = \zeta_5 + \zeta_5^{-1} + \zeta_6, \quad \eta_5 = \zeta_6 + \zeta_6^{-1} + \zeta_{10}, \\ \eta_{10} = \zeta_{20} + \zeta_{20}^3 + \zeta_{20}^{-3}, \quad \eta_{30} = \zeta_{12}^{-1} + \zeta_{20}^{-1} + \zeta_{60}^{11}. \end{gathered}$$

□

Proof of Corollary 4. Since $1+2i\cos(\pi/M) = 1+i(\zeta_{2M}+\zeta_{2M}^{-1})$, any number equivalent to $1 + 2i\cos(\pi/M)$ is a sum of three roots of unity. It follows by Theorem 2 that the numbers $\xi_M = 1 + 2i\cos(\pi/M)$ and $\eta_M = \sqrt{5}\cos(\pi/M) + i\sin(\pi/M)$ can be equivalent only for $M = 2, 3, 5, 10$ or 30.

If the numbers ξ_3 and η_3 or ξ_5 and η_5 were equivalent then since $\xi_3 = 1 + i$ and $\eta_5 = 1 + \zeta_{10}$, η_3 or ξ_5 would be a sum of two roots of unity. However if $\vartheta \neq 0$ is such

a sum and $\overline{\vartheta}$ is its complex conjugate, then $\vartheta/\overline{\vartheta}$ is a root of unity. Since neither of the numbers $\eta_3/\overline{\eta_3}$ and $\xi_5/\overline{\xi_5}$ is an algebraic integer, the proof is complete.

Added in proof. 1. H. B. Mann has proved in [3a] that under the assumptions of Corollary 3, N divides the product of all primes $\leqslant k+1$. This leads to a much better estimation of N than that stated in the corollary. Mann's method could also be used to solve both Robinson's problems considered in this paper.

2. In connection with Lemma 1 the question arises how much inequality (1) can be improved. Y. Wang has proved by Brun's method in a manuscript kindly placed at my disposal that for $N > N_0(h)$ one can replace $(\log N)^{20h}$ by $c(h)(\log N)^{4h+3}$. According to H. Halberstam (written communication), there is a possibility of reducing the exponent $4h+3$ to $2h+1$ by Selberg's method.

References

[1] V. Brun, *Le crible d'Eratosthène et le théorème de Goldbach*. Norsk Videnskaps Selskabs Skrifter, Kristiania 1920.

[2] R. D. Carmichael, *Introduction to the Theory of Groups of Finite Order*. Ginn, Boston 1937.

[3] W. Hodge, D. Pedoe, *Methods of Algebraic Geometry* II. Cambridge Univ. Press, Cambridge 1952.

[3a] H. B. Mann, *On linear relations between roots of unity*. Mathematika 12 (1965), 107–117.

[4] R. M. Robinson, *Some conjectures about cyclotomic integers*. Math. Comp. 19 (1965), 210–217.

[5] J. B. Rosser, L. Schoenfeld, *Approximate formulas for some functions of prime numbers*. Illinois J. Math. 6 (1962), 64–94.

[6] A. Schinzel, Y. Wang, *A note on some properties of the functions $\varphi(n)$, $\sigma(n)$ and $\theta(n)$*. Ann. Polon. Math. 4 (1958), 201–213; *Corrigendum*, ibid. 19 (1967), 115.

Andrzej Schinzel
Selecta

Originally published in
Acta Arithmetica XXII (1973), 221–231

On a theorem of Bauer and some of its applications II

The aim of this paper is to extend to polynomials in many variables the results of papers [1] and [6]. It is convenient to first restate these results in a concise form.

Let K be an algebraic number field, $|K|$ its degree, $\overline{K}$ its normal closure. We denote by $P(K)$ the set of primes which have in K at least one prime ideal factor of the first degree, and by $N_{K/\mathbb{Q}}$ the norm from K to the rational field $\mathbb{Q}$. We say that K *has property* (P) if for all but finitely many primes q and for every $\omega \in K$ $\left(\operatorname{ord}_q N_{K/\mathbb{Q}}(\omega), |K|\right) = 1$ implies $q \in P(K)$. A field K is called *Bauerian* if for every Ω, $P(\Omega) \leqslant P(K)$ implies that Ω contains one of the conjugates of K ($P(\Omega) \leqslant P(K)$ means that $P(\Omega) \setminus P(K)$ is finite).

Several types of Bauerian fields have been described in [6], it happens so that all those fields have property (P). For some of them (cubic and quartic fields, solvable fields K with $\left(\frac{|\overline{K}|}{|K|}, |K|\right) = 1$) this has been established in the course of proof of Lemma 1 ([6]), for the others (certain solvable fields of degree p^2) it follows from Lemma 3 and Theorem 4 below. For normal fields the fact is obvious and for Bauerian fields of the types described in [4] (fields with property (N), fields $\mathbb{Q}\left(\sqrt[n]{A}\right)$ with $n \not\equiv 0 \pmod 8$) it is also true (see Corollary 2 and p. 219). In Theorem 5 I give a new class of Bauerian fields (normal extensions of quadratic fields) which need not have property (P).

Apart from the description of Bauerian fields, from Theorem 1 of [1] which has been generalized in [5] and various counterexamples the results of papers [1] and [6] can be summarized as follows.

Theorem A. *If K is a cyclic field or a solvable field such that $|K|$ is square-free and $\left(\frac{|\overline{K}|}{|K|}, |K|\right) = 1$, $f(x) \in \mathbb{Q}[x]$ and in every arithmetic progression there is an integer x such that*

$$f(x) = N_{K/\mathbb{Q}}(\omega), \quad \omega \in K,$$

then

$$f(x) = N_{K/\mathbb{Q}}\big(\varphi(x)\big), \quad \text{where} \quad \varphi(x) \in K[x].$$

Theorem B. *If K is a Bauerian field with property* (P)*, $f(x) \in \mathbb{Q}[x]$, the multiplicity of each zero of f is relatively prime to $|K|$ and in every arithmetic progression there is an*

integer x such that

$$f(x) = N_{K/\mathbb{Q}}(\omega), \quad \omega \in K,$$

then

$$f(x) = N_{K/\mathbb{Q}}\big(\varphi(x)\big), \quad \text{where} \quad \varphi(x) \in K[x].$$

Theorem C. *If K is any field of degree p or p^2 (p prime), $f(x) \in \mathbb{Q}(x)$, the multiplicity of each zero and pole of f is relatively prime to $|K|p^{-1}$ and in every arithmetic progression there is an integer x such that*

$$f(x) = N_{K/\mathbb{Q}}(\omega), \quad \omega \in K,$$

then

$$f(x) = N_{K/\mathbb{Q}}\big(\varphi(x)\big), \quad \text{where} \quad \varphi(x) \in K(x).$$

The proof of all these theorems passes through the same stage which we formulate below as

Lemma 1. *Let K and the multiplicities of the factors of f satisfy the assumptions of Theorems* A, B *or* C. *If for every integer x and every prime q there exists $\omega \in K$ such that*

$$\operatorname{ord}_q f(x) = \operatorname{ord}_q N_{K/\mathbb{Q}}(\omega)$$

(*provided the left hand side is defined*) *and f_1 is an irreducible factor of f then*

$$f_1(x)^e = \alpha N_{K/\mathbb{Q}}\big(\varphi(x)\big),$$

where $\alpha \in \mathbb{Q}$, $\varphi(x) \in K[x]$ and $e = \operatorname{ord}_{f_1} f$ in case A, B, $\big(e, |K|\big) = \big(\operatorname{ord}_{f_1} f, |K|\big)$ *in case* C.

We generalize Theorems A, B and C as follows.

Theorem 1. *If K is a cyclic field or a solvable field such that $|K|$ is square-free and $\left(|K|, \dfrac{|\overline{K}|}{|K|}\right) = 1$, $f \in \mathbb{Q}[x_1, \dots, x_k]$ and for any arithmetic progressions $P_1, \dots, P_k$ there are integers $x_1, \dots, x_k$, such that $x_i \in P_i$ $(1 \leqslant i \leqslant k)$,*

$$f(x_1, \dots, x_k) = N_{K/\mathbb{Q}}(\omega), \quad \omega \in K,$$

then

$$f(x_1, \dots, x_k) = N_{K/\mathbb{Q}}\big(\varphi(x_1, \dots, x_k)\big), \quad \varphi(x_1, \dots, x_k) \in K[x_1, \dots, x_k].$$

Theorem 2. *If K is a Bauerian field with property* (P), *$f \in \mathbb{Q}[x_1, \dots, x_k]$, the multiplicity of each irreducible factor of f is relatively prime to $|K|$ and for any arithmetic progressions $P_1, \dots, P_k$ there are integers $x_1, \dots, x_k$ such that $x_i \in P_i$,*

$$f(x_1, \dots, x_k) = N_{K/\mathbb{Q}}(\omega), \quad \omega \in K,$$

then

$$f(x_1, \dots, x_k) = N_{K/\mathbb{Q}}\big(\varphi(x_1, \dots, x_k)\big), \quad \varphi \in K[x_1, \dots, x_k].$$

c **Theorem 3.** *If K is any field of degree p or p^2 (p prime), $f \in \mathbb{Q}(x_1, \dots, x_k)$, the multiplicity of each irreducible factor of f is relatively prime to $|K|p^{-1}$ and for any arithmetic progressions $P_1, \dots, P_k$ there are integers $x_1, \dots, x_k$, such that $x_i \in P_i$ $(1 \leqslant i \leqslant k)$,*

$$f(x_1, \dots, x_k) = N_{K/\mathbb{Q}}(\omega), \quad \omega \in K,$$

then

$$f(x_1, \dots, x_k) = N_{K/\mathbb{Q}}\big(\varphi(x_1, \dots, x_k)\big), \quad \varphi(x) \in K(x_1, \dots, x_k).$$

All the three theorems can be deduced from Lemma 1 by means of Hilbert's Irreducibility Theorem. The idea of using Hilbert's theorem in this connection is due to H. Davenport.

We prove first a generalization of Lemma 1.

Lemma 2. *Let K and the multiplicities of the factors of f satisfy the assumptions of Theorems* 1, 2 *or* 3. *If for any integers $x_1, \dots, x_k$ and every prime q there exists $\omega \in K$ such that*

c $$\operatorname{ord}_q f(x_1, \dots, x_k) = \operatorname{ord}_q N_{K/\mathbb{Q}}(\omega)$$

(*provided the left hand side is defined*) *and f_1 is an irreducible factor of f then*

$$f_1(x_1, \dots, x_k)^e = \alpha N_{K/\mathbb{Q}}\big(\varphi(x_1, \dots, x_k)\big),$$

where $\alpha \in \mathbb{Q}$, $\varphi \in K[x_1, \dots, x_k]$ and $e = \operatorname{ord}_{f_1} f$ in case 1 *and* 2, $\big(e, |K|\big) = \big(\operatorname{ord}_{f_1} f, |K|\big)$ *in case* 3 (1, 2 *and* 3 *refer to numbers of the theorems*).

Proof. Let

$$f = c f_1^{e_1} f_2^{e_2} \cdots f_m^{e_m} \tag{1}$$

and

$$f_1 = c_1 \varphi_1^{\varepsilon_1} \varphi_2^{\varepsilon_2} \cdots \varphi_n^{\varepsilon_n} \tag{2}$$

by the factorization of f and f_1 into irreducible factors over $\mathbb{Q}$ and K respectively. We have

$$N_{K/\mathbb{Q}} \varphi_l(x_1, \dots, x_k) = \gamma_l f_1(x_1, \dots, x_k)^{\delta_l}. \tag{3}$$

We may assume without loss of generality that x_k really occurs in f_1. Denote the coefficient of the highest power of x_k in f_1 by $h(x_1, \dots, x_{k-1}) \neq 0$ and the discriminant of $f_1 f_2 \cdots f_m$ with respect to x_k by $D(x_1, \dots, x_{k-1})$. By Hilbert's Irreducibility Theorem there exist integers x_i' $(1 \leqslant i < k)$ such that $h(x_1', \dots, x_{k-1}') D(x_1', \dots, x_{k-1}') \neq 0$, $f_j(x_1', \dots, x_{k-1}', x_k)$ are irreducible over $\mathbb{Q}$ and $\varphi_l(x_1', \dots, x_{k-1}', x_k)$ are irreducible over K

as polynomials in x_k ($1 \leqslant j \leqslant m$, $1 \leqslant l \leqslant n$). Therefore by (1), in case 2 or 3 the multiplicity of each factor of $f(x_1', \dots, x_{k-1}', x_k)$ is relatively prime to $|K|$ or $|K|p^{-1}$, respectively. On the other hand, for every integer x_k and every prime q there exists $\omega \in K$ such that

$$\operatorname{ord}_q f(x_1', \dots, x_{k-1}', x_k) = \operatorname{ord}_q N_{K/\mathbb{Q}}(\omega)$$

(provided the left hand side is defined). By Lemma 1 we infer

$$f_1(x_1', \dots, x_{k-1}', x_k)^e = \alpha' N_{K/\mathbb{Q}}\big(\varphi'(x_k)\big), \tag{4}$$

where $\alpha' \in \mathbb{Q}$, $\varphi' \in K[x_k]$ and $e = \operatorname{ord}_{f_1} f$ in case 1 and 2, $\big(e, |K|\big) = \big(\operatorname{ord}_{f_1} f, |K|\big)$ in case 3. In virtue of (2) and of the choice of x_i' ($1 \leqslant i < k$) we have for some nonnegative integers $\eta_1, \dots, \eta_n$ and some $\beta \in K$

$$\varphi'(x_k) = \beta \prod_{l=1}^{n} \varphi_l(x_1', \dots, x_{k-1}', x_k)^{\eta_l}. \tag{5}$$

It follows from (3), (4) and (5) that

$$f_1(x_1', \dots, x_{k-1}', x_k)^e = \alpha' N_{K/\mathbb{Q}}(\beta) \prod_{l=1}^{n} \gamma_l^{\eta_l} f_1(x_1', \dots, x_{k-1}', x_k)^{\delta_l \eta_l}. \tag{6}$$

Since $h(x_1', \dots, x_{k-1}') \neq 0$, $f_1(x_1', \dots, x_{k-1}', x_k)$ is not constant and (6) implies $\sum_{l=1}^{n} \delta_l \eta_l = e$, which proves the lemma with $\varphi = \prod_{l=1}^{n} \varphi_l^{\eta_l}$. □

Proof of Theorems 1, 2 *and* 3. Let

$$f(x_1, \dots, x_k) = \frac{g(x_1, \dots, x_k)}{h(x_1, \dots, x_k)},$$

where the polynomials g and h have integer coefficients and $(g, h) = 1$. Take any k integers $x_1, \dots, x_k$ such that $h(x_1, \dots, x_k) \neq 0$. If

$$g(x_1, \dots, x_k) = 0$$

we have for any prime q

$$\operatorname{ord}_q f(x_1, \dots, x_k) = \infty = \operatorname{ord}_q N_{K/\mathbb{Q}}(0).$$

If $g(x_1, \dots, x_k) \neq 0$ set

$$\operatorname{ord}_q g(x_1, \dots, x_k) = \mu, \quad \operatorname{ord}_q h(x_1, \dots, x_k) = \nu.$$

By the assumptions there exist integers $t_1, \dots, t_k$ such that

$$f(x_1 + q^{\mu+\nu+1}t_1, \dots, x_k + q^{\mu+\nu+1}t_k) = N_{K/\mathbb{Q}}(\omega), \quad \omega \in K.$$

Hence

$$\begin{aligned} N_{K/\mathbb{Q}}(\omega) &= \operatorname{ord}_q g(x_1 + q^{\mu+\nu+1}t_1, \dots, x_k + q^{\mu+\nu+1}t_k) \\ &\qquad - \operatorname{ord}_q h(x_1 + q^{\mu+\nu+1}t_1, \dots, x_k + q^{\mu+\nu+1}t_k) \\ &= \operatorname{ord}_q g(x_1, \dots, x_k) - \operatorname{ord}_q h(x_1, \dots, x_k) = \operatorname{ord}_q f(x_1, \dots, x_k). \end{aligned}$$

c Let (1) be the factorization of f into irreducible factors over $\mathbb{Q}$. By Lemma 2 we have for each $j \leqslant m$

$$f_j(x_1, \ldots, x_k)^{e'_j} = \alpha_j N_{K/\mathbb{Q}}\big(\varphi_j(x_1, \ldots, x_k)\big),$$

where $\alpha_j \in \mathbb{Q}$, $\varphi_j \in K[x_1, \ldots, x_k]$ and $e'_j = e_j$ in case 1 and 2, $\big(e'_j, |K|\big) = \big(e_j, |K|\big)$ in case 3. In the last case there exist integers a_j and b_j such that

$$e'_j a_j - |K| b_j = e_j.$$

It follows

$$f_j(x_1, \ldots, x_k)^{e_j} = \alpha_j^{a_j} N_{K/\mathbb{Q}}\big(\varphi_j(x_1, \ldots, x_k)^{a_j} f_j(x_1, \ldots, x_k)^{-b_j}\big)$$

and we obtain from (1)

$$f(x_1, \ldots, x_k) = \begin{cases} c \prod_{j=1}^{m} \alpha_j N_{K/\mathbb{Q}}\Big(\prod_{j=1}^{m} \varphi_j(x_1, \ldots, x_k)\Big) & \text{in case 1 and 2,} \\ c \prod_{j=1}^{m} \alpha_j^{a_j} N_{K/\mathbb{Q}}\Big(\prod_{j=1}^{m} \varphi_j(x_1, \ldots, x_k)^{a_j} f_j(x_1, \ldots, x_k)^{-b_j}\Big) & \text{in case 3.} \end{cases}$$

Choosing $x_1, \ldots, x_k$ so that $f(x_1, \ldots, x_k) = N_{K/\mathbb{Q}}(\omega) \neq 0$ we infer that $c \prod_{j=1}^{m} \alpha_j$ or $c \prod_{j=1}^{m} \alpha_j^{a_j}$ in case 1 and 2 or 3 respectively, is a norm of an element of K and the theorems follow. □

It seems more difficult to generalize to polynomials in many variables the results of [2]. In particular I do not know whether the solubility in rationals x, y of an equation

$$a(t, u)x^2 + b(t, u)y^2 = 1$$

for all integer values of t, u implies the existence of rational functions $\varphi(t, u)$, $\psi(t, u)$ such that identically

$$a(t, u)\varphi^2(t, u) + b(t, u)\psi^2(t, u) = 1.$$

Now we shall prove a result on fields of degree p^2 announced in the introduction. We show first

Lemma 3. *Let the Galois group $\mathfrak{G}$ of $\overline{K}$ be represented as permutation group on the conjugates of K. The field K has property* (P) *if and only if every permutation of $\mathfrak{G}$ for which the lengths of cycles are relatively prime fixes at least one element.*

Proof. Necessity. Suppose that a permutation σ of $\mathfrak{G}$ has the cycles of lengths $f_1, \ldots, f_k$ and $(f_1, \ldots, f_k) = 1$. By Chebotarev's density theorem there exist infinitely many primes q not dividing the discriminant of K such that $\left(\frac{\overline{K}}{q}\right)$ is the class of σ. By the well known Artin's result (see [3], p. 126) these primes factorize in K into prime ideals of degrees

$f_1, \ldots, f_k$. Let $q = \mathfrak{q}_1 \cdots \mathfrak{q}_k$, where $\mathfrak{q}_i$ is of degree f_i. Since $(f_1, \ldots, f_k) = 1$ there exist integers $\alpha_1, \ldots, \alpha_k$ such that

$$\alpha_1 f_1 + \ldots + \alpha_k f_k = 1,$$

there exists also an ideal $\mathfrak{a}$ relatively prime to q such that the ideal $\mathfrak{q}_1^{\alpha_1} \cdots \mathfrak{q}_k^{\alpha_k} \mathfrak{a}$ is principal equal to (ω), say. Then

$$\operatorname{ord}_q N_{K/\mathbb{Q}}(\omega) = 1$$

and by the assumption at least one of the numbers $f_1, \ldots, f_k$ is 1.

Sufficiency. Suppose that q does not divide the discriminant of K and

$$\big(\operatorname{ord}_q N_{K/\mathbb{Q}}(\omega), |K|\big) = 1. \tag{7}$$

Let $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_l$ be all the prime ideal factors of q in K and let

$$(\omega) = \mathfrak{q}_1^{\alpha_1} \cdots \mathfrak{q}_l^{\alpha_l} \mathfrak{a}\mathfrak{b}^{-1},$$

where $(\mathfrak{a}\mathfrak{b}, q) = 1$. If $\mathfrak{q}_i$ is of degree f_i we have

$$\operatorname{ord}_q N_{K/\mathbb{Q}}(\omega) = \alpha_1 f_1 + \ldots + \alpha_l f_l$$

and since $f_1 + \ldots + f_l = |K|$, by (7)

$$(f_1, \ldots, f_l) = 1. \tag{8}$$

By Artin's theorem quoted above, any permutation σ of $\mathfrak{G}$ belonging to $\left(\dfrac{\overline{K}}{q}\right)$ factorizes into cycles of lengths $f_1, \ldots, f_l$. By (8) and the assumption one of these lengths is 1, thus $q \in P(K)$.

Corollary 1. *Every field K with the Galois group of $\overline{K}$ being a p-group has property* (P).

Proof. It is clear that the lengths of cycles of the permutations in question can only be powers of p. □

Corollary 2. *Every pure field $K = \mathbb{Q}\big(\sqrt[m]{A}\big)$ has property* (P).

Proof. The Galois group of $\overline{K}$ can be represented by permutations of residue classes mod m given by $\sigma(x) \equiv ax + b \pmod m$. Suppose that for some f: $\sigma^f(x) = x$. Then

$$\frac{a^f - 1}{a - 1}\big((a-1)x + b\big) \equiv 0 \pmod m$$

and

$$(a - 1, m) \mid b\,\frac{a^f - 1}{a - 1}\,.$$

If the lenghts of the cycles of σ: $f_1, \ldots, f_k$ are relatively prime then

$$(a - 1, m) \mid b\,\frac{a^{f_i} - 1}{a - 1} \quad (i = 1, \ldots, k)$$

implies

$$(a-1, m) \mid b,$$

and $\sigma(x) = x$ is soluble. □

Corollary 1 establishes property (P) for one class of Bauerian fields of degree p^2 found by P. Roquette and mentioned in [6]. For the other class found by L. Alperin (primitive solvable fields of degree p^2, $p > 3$) the same holds in virtue of

Theorem 4. *Let K be a field of degree p^k (p prime) and assume that the Galois group $\mathfrak{G}$ of $\overline{K}$ represented as a permutation group on the points of $\mathbb{F}_p^k$ consists of affine transformations. Then K has property* (P) *and if $k \leqslant 2$ or $k = 3$, $p = 2$, it is Bauerian. For $k \geqslant 3$, $p \geqslant 3$ or $k \geqslant 4$ there are non-Bauerian fields of this type.*

Proof. Let σ be a permutation of the points of $\mathbb{F}_p^k$ given by an affine transformation. If the lengths of cycles of σ are relatively prime, one of them is not divisible by p. Let the relevant cycle be $(p_1, \ldots, p_l)$. Then

$$\sigma\Big(l^{-1}\sum_{i=1}^{l} p_i\Big) = l^{-1}\sum_{i=1}^{l}\sigma(p_i) = l^{-1}\sum_{i=1}^{l} p_i, \tag{9}$$

thus σ has a fixed point.

Assume now that $k \leqslant 2$ and $\mathfrak{J}$ is a subgroup of $\mathfrak{G}$ contained in the union of stability groups. If the lengths of orbits of $\mathfrak{J}$ were not relatively prime then by Lemma 3 of [6] there would exist in $\mathfrak{J}$ a permutation with the lengths of cycles not relatively prime, against the assumption. Therefore the lengths of orbits are relatively prime and one of them is not divisible by p. Let the relevant orbit be $(p_1, \ldots, p_l)$. Then for any σ from $\mathfrak{J}$ the formula (9) holds and $\mathfrak{J}$ is contained in the stabilizer of $l^{-1}\sum_{i=1}^{l} p_i$. It follows by Theorem 1 of [6] that K is a Bauerian field.

Now, let $k = 3$, $p = 2$ and let $\mathfrak{J}$ have its former meaning. If the lengths of orbits of $\mathfrak{J}$ are relatively prime the former argument applies. Otherwise all lengths are even and by Theorem 3.4 of [8], a Sylow 2-subgroup S of $\mathfrak{J}$ has also all orbits of even length. Since S is contained in the union of stability subgroups it is not cyclic and does not contain any translation. It follows that S is of order 4 or 8. The computation shows that all groups of order 8 of affine transformations of $\mathbb{F}_2^3$ without translations are of the form $\sigma\,\langle\sigma_1, \sigma_2\rangle\,\sigma^{-1}$, where

$$\sigma_1(\boldsymbol{x}) = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}\boldsymbol{x} + \begin{bmatrix} a \\ b \\ c \end{bmatrix}, \quad \sigma_2(\boldsymbol{x}) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}\boldsymbol{x} + \begin{bmatrix} d \\ b+c \\ 0 \end{bmatrix}.$$

If $\sigma^{-1}S\sigma$ contains σ_1^2 and σ_2 then the existence of fixed points of these transformations implies that $c = d = 0$ and S has the fixed point $\sigma(0, a, b)$. Otherwise $\sigma^{-1}S\sigma$ is the group

of order 4 generated by σ_1^2 and $\sigma_2\sigma_1$, where

$$\sigma_2\sigma_1(\boldsymbol{x}) = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \boldsymbol{x} + \begin{bmatrix} a+b+c+d \\ c \\ c \end{bmatrix}.$$

We infer again that $c = 0$ and S has the fixed point $\sigma(0, a+d, b)$. The contradiction obtained shows that K is a Bauerian field.

If $k \geqslant 3$, $p \geqslant 3$ consider the group $\mathfrak{J} = \{\sigma_{i,j}\}$, where

$$\sigma_{i,j} : \ y_1 = x_1 + jx_2 + \left(\binom{j}{2} + i\right)x_3 + i, \ y_2 = x_2 + jx_3, \ y_i = x_i \ (3 \leqslant i \leqslant k).$$

(We have $\sigma_{i_1,j_1}\sigma_{i_2,j_2} = \sigma_{i_1+i_2,j_1+j_2}$.) All fixed points of $\sigma_{i,j}$ are given by $x_2 = -ij^{-1}$, $x_3 = 0$ if $j \neq 0$ and $x_3 = -1$ if $j = 0$, thus $\mathfrak{J}$ has no fixed point. Taking for $\mathfrak{G}$ the group generated by $\mathfrak{J}$ and all the translations we get corresponding to a stability subgroup of $\mathfrak{G}$ a solvable field of degree p^k which is not Bauerian.

If $k \geqslant 4$ consider the group $\mathfrak{J} = \{1, \sigma_1, \sigma_2, \sigma_3\}$, where σ_i are the following affine transformations of $\mathbb{F}_2^k$:

σ_1: $y_1 = x_1 + x_2 + x_3 + 1, \ y_i = x_i \ (2 \leqslant i \leqslant k)$,

σ_2: $y_1 = x_1 + x_4, \ y_2 = x_3, \ y_3 = x_2, \ y_i = x_i \ (4 \leqslant i \leqslant k)$,

σ_3: $y_1 = x_1 + x_2 + x_3 + x_4 + 1, \ y_2 = x_3, \ y_3 = x_2, \ y_i = x_i \ (4 \leqslant i \leqslant k)$.

Each σ_i has fixed points but there is none in common.

Taking for $\mathfrak{G}$ the group generated by $\mathfrak{J}$ and all the translations, we get corresponding to a stability subgroup of $\mathfrak{G}$ a solvable field of degree 2^k which is not Bauerian. □

Remark. The assertion of Theorem 4 concerning property (P) is a special case of the following theorem due to Professor H. Wielandt (written communication). *If a permutation group $\mathfrak{G}$ of prime power degree p^k has a regular normal subgroup* (*regular means that it is transitive and stabilizer of any point is trivial*) *then every element of $\mathfrak{G}$ whose cycle lengths are relatively prime has a fixed point.*

Corollary 3. *Every primitive solvable field of degree p^k (p prime) has property* (P) *and if $k \leqslant 2$ or $k = 3$, $p = 2$, it is Bauerian.*

Proof. If K is a primitive solvable field of degree p^k then the Galois group of $\overline{K}$ represented as a permutation group on $\mathbb{F}_p^k$ consists of affine transformations (see [7], p. 364). □

Imprimitive solvable fields of degree p^2 need neither be Bauerian nor have property (P). It is shown by the example of a field K of degree 9 with the Galois group of $\overline{K}$ being the wreath product of S_3 acting on three isomorphic copies of S_3. It remains unsettled whether every primitive solvable field is Bauerian.

Theorem 5. *Every normal extension of a quadratic field is Bauerian. There are fields of this type without property* (P).

Proof. Let K be a normal extension of a quadratic field L and $\overline{K}$ the normal closure of K. We can assume that $\overline{K} \neq K$. Let $\mathfrak{G}$ be the Galois group of $\overline{K}$ and $\mathfrak{H}, \mathfrak{N}$ the subgroups

of $\mathfrak{G}$ corresponding to K and L, respectively. By the assumption $\mathfrak{H}$ is a normal subgroup of $\mathfrak{N}$, and since $\mathfrak{N}$ is of index two in $\mathfrak{G}$ there is only one subgroup of $\mathfrak{G}$ conjugate to $\mathfrak{H}$ and different from it; let us denote it by $\mathfrak{H}'$. If the field K were not Bauerian then by Theorem 1 of [6] one could find a subgroup $\mathfrak{J}$ of $\mathfrak{G}$ such that

$$\mathfrak{J} \subset \mathfrak{H} \cup \mathfrak{H}', \quad \mathfrak{J} \not\subset \mathfrak{H}, \quad \mathfrak{J} \not\subset \mathfrak{H}'. \tag{10}$$

On taking

$$j_1 \in \mathfrak{J} \setminus \mathfrak{H} \subset \mathfrak{H}', \quad j_2 \in \mathfrak{J} \setminus \mathfrak{H}' \subset \mathfrak{H}$$

one obtains

$$j_1 j_2 \in \mathfrak{J} \setminus \mathfrak{H} \setminus \mathfrak{H}'$$

which contradicts (10).

Consider now a group $\mathfrak{G}$ consisting of the following permutations $\sigma_{a,b}$ of residue classes mod 12:

$$\sigma_{a,b}(2n) \equiv 2n + a \pmod{12}, \quad \sigma_{a,b}(2n+1) \equiv 2n + 1 + b \pmod{12} \quad (0 \leqslant n \leqslant 5),$$

where (a, b) runs through all pairs of residues mod 12 of the same parity. This group is transitive and it has an abelian subgroup of index two namely $\mathfrak{N} = \{\sigma_{a,b} : a \equiv b \equiv 0 \pmod 2\}$. Therefore there exists an algebraic number field Ω with $\mathfrak{G}$ as its Galois group. The stability subgroups

$$\mathfrak{H} = \{\sigma_{a,0} : a \equiv 0 \pmod 2\} \quad \text{and} \quad \mathfrak{H}' = \{\sigma_{0,b} : b \equiv 0 \pmod 2\}$$

are normal subgroups of $\mathfrak{N}$. Thus the subfield K of Ω corresponding to $\mathfrak{H}$ is Bauerian. On the other hand it does not possess property (P) since

$$\sigma_{4,6} = (0, 4, 8)(1, 7)(2, 6, 10)(3, 9)(5, 11);$$

the lengths of cycles are relatively prime but none of them is 1. □

Finally we prove that for fields K without property (P) Theorem B and *a fortiori* Theorem 2 does not hold.

Theorem 6. *If a field K does not possess property* (P) *then there exists an irreducible polynomial $f(x)$ such that, for every integer x, $f(x) = N_{K/\mathbb{Q}}(\omega)$ with $\omega \in K$ but for no polynomial $\varphi(x) \in K[x]$*

$$f(x) = N_{K/\mathbb{Q}}\big(\varphi(x)\big). \tag{11}$$

Proof. Let $\mathfrak{G}$ be the Galois group of $\overline{K}$ represented as the permutation group on the conjugates of K and $\mathfrak{H}$ be the subgroup of $\mathfrak{G}$ corresponding to K. Let $\sigma \in \mathfrak{G}$ have the cycles of lengths $f_1, \ldots, f_k$, where $(f_1, \ldots, f_k) = 1$ and $f_i > 1$ $(1 \leqslant i \leqslant k)$. To the group $\mathfrak{J}$ generated by σ there corresponds a field Ω, say.

Let $\Omega = \mathbb{Q}(\vartheta)$ and f be the minimal polynomial of ϑ. Assume (11). Then for a certain $\tau \in \mathfrak{G}$ we have $\varphi^{(\tau)}(\vartheta) = 0$ and for a suitable $i \leqslant k$

$$\big|\mathfrak{J} \cap \tau \mathfrak{H} \tau^{-1}\big| = \frac{|\mathfrak{J}|}{f_i}.$$

Hence

$$\frac{|\Omega K^{(\tau)}|}{|K^{(\tau)}|} = \frac{|\mathfrak{H}|}{|\mathfrak{J} \cap \tau \mathfrak{H} \tau^{-1}|} = \frac{|\mathfrak{H}|}{|\mathfrak{J}|} f_i = \frac{|\Omega|}{|K|} f_i$$

and it follows that $\varphi^{(\tau)}(x)$ is of degree $\frac{|\Omega|}{|K|} f_i$. By comparison of degrees we get

$$N_{K/\mathbb{Q}}\big(\varphi(x)\big) = f(x)^{f_i},$$

which contradicts (11) since $f_i > 1$. On the other hand, since $(f_1, \ldots, f_k) = 1$ there exist integers $a_1, \ldots, a_k$ such that

$$a_1 f_1 + \ldots + a_k f_k = 1.$$

Hence

$$N_{K/\mathbb{Q}}\big(\varphi_i(x)^{a_i}\big) = f(x),$$

which proves that for every integer x, $f(x) = N_{K/\mathbb{Q}}(\omega)$ for some $\omega \in K$. □

It follows by Theorem 3 of [4] that property (N) implies property (P).

Note added in proof. 1. Theorem 4 suggests the following question about the family F_Ω of groups of affine transformations of Ω^2, where Ω is a field: If every element of $\mathfrak{G} \in F_\Omega$ has a fixed point, is there a fixed point for the whole $\mathfrak{G}$? If $\Omega = \mathbb{F}_p$ the answer is affirmative by the said theorem. If Ω is not simple the answer is negative and a counterexample is given by the abelian group $\mathfrak{G}_0 = \{\sigma_a : a \in \Omega\}$, where

$$\sigma_a(\boldsymbol{x}) = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \boldsymbol{x} + \begin{bmatrix} f(a) \\ 0 \end{bmatrix}$$

and where f is a nontrivial solution of the equation $f(x+y) = f(x) + f(y)$ in Ω. In the remaining case $\Omega = \mathbb{Q}$ the answer is again negative and a more recondite counterexample is given by

$$\mathfrak{G}_1 = \left\langle \begin{bmatrix} 23 \\ 35 \end{bmatrix} \boldsymbol{x}, \begin{bmatrix} 21 \\ 11 \end{bmatrix} \boldsymbol{x} + \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\rangle.$$

$\mathfrak{G}_1$ clearly has no fixed point. The existence of fixed points for all elements of $\mathfrak{G}_1$ follows from the fact kindly communicated to the writer by Professor R. A. Rankin that the group $\left\langle \begin{bmatrix} 23 \\ 35 \end{bmatrix}, \begin{bmatrix} 21 \\ 11 \end{bmatrix} \right\rangle$ is free without parabolic elements. On the other hand, J. Browkin has shown that there is no abelian counterexample.

2. It can be verified using the explicit determination of all primitive solvable groups of degree p^4 by G. Bucht (Arkiv f. Mat. 11 (1916)) and of degree p^q (q prime) by D. Suprunenko [6a] that all primitive solvable fields of the above degrees are Bauerian.

References

[1] H. Davenport, D. J. Lewis, A. Schinzel, *Polynomials of certain special types*. Acta Arith. 9 (1964), 107–116; this collection: A6, 27–35.

[2] —, —, —, *Quadratic Diophantine equations with a parameter*. Acta Arith. 11 (1966), 353–358.

[3] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil II: *Reziprozitätsgesetz*. Physica-Verlag, Würzburg–Wien 1965.

[4] D. J. Lewis, A. Schinzel, H. Zassenhaus, *An extension of the theorem of Bauer and polynomials of certain special types*. Acta Arith. 11 (1966), 345–352; this collection: C3, 190–196.

[5] A. Schinzel, *On Hilbert's Irreducibility Theorem*. Ann. Polon. Math. 16 (1965), 333–340; this collection: F1, 839–845.

[6] —, *On a theorem of Bauer and some of its applications*. Acta Arith. 11 (1966), 333–344; *Corrigendum* ibid. 12 (1967), 425; this collection: C2, 179–189.

[6a] D. Suprunenko, *Soluble and Nilpotent Linear Groups*. Amer. Math. Soc., Providence 1963.

[7] H. Weber, *Lehrbuch der Algebra*, Bd. II. New York 1964.

[8] H. Wielandt, *Finite Permutation Groups*. Academic Press, New York–London 1964.

Originally published in
Acta Arithmetica XXIV (1973), 385–399

On the product of the conjugates outside the unit circle of an algebraic number

To Professor Carl Ludwig Siegel

C. J. Smyth [7] has recently proved the following theorem.

If $P(x) \neq x$ is a monic non-reciprocal irreducible polynomial with integral coefficients, then

$$\prod_{|\alpha_j|>1} |\alpha_j| \geqslant \theta_0,$$

where α_j are the zeros of $P(x)$ and θ_0 is the real root of the equation $\theta^3 = \theta + 1$. (A polynomial P of degree $|P|$ is called *reciprocal* if $x^{|P|}P(x^{-1}) = \pm P(x)$.)

This theorem is a far reaching generalization of Siegel's theorem [6] about the least Pisot–Vijayaraghvan number being θ_0. On the other hand, it has interesting applications to the arithmetic of polynomials. The aim of this paper is to prove two extensions of Smyth's result to polynomials with coefficients in an algebraic number field and to apply one of them to reducibility questions. For a given polynomial F we denote by $|F|$ its degree, by $C(F)$ its content and by $\|F\|$ the sum of squares of the absolute values of the coefficients. $\mathbb{Q}$ denotes the rational field and $N_{K/\mathbb{Q}}$ the norm from a number field K to $\mathbb{Q}$. ζ_m is a primitive mth root of unity.

Theorem 1. *Let K be a totally real algebraic number field, P a monic non-reciprocal polynomial with coefficients integers in K and $P(0) \neq 0$. Then*

$$\max_{i=1,\ldots,|K|} \prod_{|\alpha_{ij}|>1} |\alpha_{ij}| \geqslant \theta_0, \tag{1}$$

where $|K|$ is the degree of K, $P^{(i)}$ $(i = 1, \ldots, |K|)$ the polynomials conjugate to $P(z)$ and α_{ij} the zeros of $P^{(i)}(z)$.

Theorem 2. *Let K be a totally real algebraic number field or a totally complex quadratic extension of such a field and $P \in K[z]$ a polynomial with the leading coefficient p_0 such*

Text corrected following the *Addendum*, Acta Arith. XXVI (1975), 329–331.

that $z^{|P|}\overline{P}(z^{-1}) \neq \text{const}\ P(z),\ P(0) \neq 0$. *Then in the notation of Theorem* 1

$$(2)\qquad \prod_{i=1}^{|K|} \prod_{|\alpha_{ij}|>1} |\alpha_{ij}|$$

$$\geqslant \begin{cases} \left(\frac{1+\sqrt{5}}{2}\right)^{|K|/2} \left(N_{K/\mathbb{Q}} \frac{C(P)}{(p_0)}\right)^{(1+\sqrt{5})/2} \left(N_{K/\mathbb{Q}} \frac{(P(0))}{C(P)}\right)^{(1-\sqrt{5})/2} \\ \qquad\qquad \text{if } |P(0)| \neq |p_0|, \\ \left(\frac{1+\sqrt{17}}{4}\right)^{|K|} \left(N_{K/\mathbb{Q}} \frac{C(P)}{(p_0)}\right)^{1/\sqrt{17}} \\ \qquad\qquad \text{if } |P(0)| = |p_0| \text{ and } (\overline{P(0)})C(P) = (p_0)C(\overline{P}), \\ \left(\frac{1+\sqrt{17}}{4}\right)^{|K|/2} \left(N_{K/\mathbb{Q}} \frac{C(P)}{(p_0)}\right)^{1/\sqrt{17}} \\ \qquad\qquad \text{if } |P(0)| = |p_0|, \text{ and } P \text{ is irreducible,} \end{cases}$$

where the equality can hold only if $\sqrt{5} \in K$, $C(P) = (p_0)$ *and* $|P(0)/p_0| = (\pm 1+\sqrt{5})/2$. (The bar denotes the complex conjugation.)

Corollary 1. *If* $z^{|P|}\overline{P}(z^{-1}) \neq \text{const}\ P(z),\ P(0) \neq 0$ *then*

$$\prod_{i=1}^{|K|} \prod_{|\alpha_{ij}|>1} |\alpha_{ij}| > \left(\frac{1+\sqrt{17}}{4}\right)^{|K|/2} N_{K/\mathbb{Q}} \frac{C(P)}{(p_0)}.$$

It seems likely that the equality in (2) holds if and only if $P(z)/p_0$ is a product of cyclotomic factors and of a binomial $z^j - \frac{1 \pm \sqrt{5}}{2}\zeta_i$. (This has just been proved by A. Bazylewicz.) It is also conjectured that in Corollary 1 $(1+\sqrt{17})/4$ can be replaced by $(1+\sqrt{5})/2$ provided the equality is allowed [1].

Theorem 3. *Let* K *satisfy the assumptions of Theorem* 2, L *be a subfield of* K, $f(z) \in L[z]$ *and* f_0 *be the leading coefficient of* f. *The number* n *of irreducible over* K *factors* P *of* f *such that* $z^{|P|}\overline{P}(z^{-1}) \neq \text{const}\ P(z),\ P(0) \neq 0$, *counted with their multiplicities satisfies the inequality*

$$(3_1)\qquad n < \frac{\log\left(N_{L/\mathbb{Q}} \| f \| N_{L/\mathbb{Q}}^{-2} C(f)\right)}{|L| \log \frac{1+\sqrt{17}}{4}}.$$

If all prime ideal factors $\mathfrak{p}$ *of* $\left(f_0, f(0)\right)C(f)^{-1}$ *in* K *satisfy* $\overline{\mathfrak{p}} = \mathfrak{p}$ *then the following stronger inequality holds*

$$(3_2)\qquad \left(\frac{1+\sqrt{5}}{2}\right)^{n|L|} + \left(\frac{1+\sqrt{5}}{2}\right)^{-n|L|} \leqslant N_{L/\mathbb{Q}} \| f \| N_{L/\mathbb{Q}}^{-2} C(f)$$

[1] See the *Addendum*, p. 235.

with the equality attained if and only if either $L = \mathbb{Q}$, $f(z) = c\big(z^{|f|} \pm 1\big)$ *or* $K \supset \mathbb{Q}(\sqrt{5}, \zeta_m)$, $L = \mathbb{Q}$,

$$z^{|f|} f(z) f\Big(\frac{1}{z}\Big) = c\Big(z^{4lm} - \Big[\Big(\frac{1+\sqrt{5}}{2}\Big)^{2m} + \Big(\frac{1-\sqrt{5}}{2}\Big)^{2m}\Big] z^{2lm} + 1\Big), \tag{4}$$

l, m *integers,* m *odd.*

Corollary 2. *If* K *satisfies the assumptions of Theorem* 2 *then*

$$\varphi(x) = x^p + \varepsilon x^q + \eta \quad (\varepsilon = \pm 1,\ \eta = \pm 1)$$

divided by its largest cyclotomic factor is irreducible in K *except when* $\sqrt{5} \in K$ *and*

$$\varphi(x) = x^{2q} \pm x^q - 1 = \Big(x^q \pm \frac{1+\sqrt{5}}{2}\Big)\Big(x^q \pm \frac{1-\sqrt{5}}{2}\Big).$$

The constant $(1 + \sqrt{17})/4$ occurring in the first assertion of Theorem 3 can probably be replaced by $(1 + \sqrt{5})/2$ ([2]). Further improvement is impossible since for every pair l, m (m odd) there exists a polynomial $f(z)$ satisfying (4) namely

$$f(z) = z^{2lm} \pm \Big[\Big(\frac{1+\sqrt{5}}{2}\Big)^m + \Big(\frac{1-\sqrt{5}}{2}\Big)^m\Big] z^{lm} - 1.$$

(There are also other instances of such polynomials, e.g. for $l = 1$, $m = 3$

$$f(z) = z^6 - 2z^5 + 2z^4 - 2z^2 - 2z - 1.)$$

The major problem is to find an estimate analogous to that given in Theorem 3 for the number of all non-cyclotomic factors of f.

Corollary 2 for $K = \mathbb{Q}$ has been proved by W. Ljunggren [4] and H. Tverberg [8] by different methods and by Smyth on the same lines two years ago (in a letter to the writer).

Proofs are based on two lemmata both essentially due to Smyth. Formula (5) of Lemma 1 is due to F. Wiener, see [1a]. (I owe this reference to Prof. E. Bombieri.)

Lemma 1. *Let* $f(z) = \sum_{i=0}^{\infty} e_i z^i$ *be holomorphic in an open disc containing* $|z| \leqslant 1$, *and satisfy* $|f(z)| \leqslant 1$ *on* $|z| = 1$. *Then*

$$|e_i| \leqslant 1 - |e_0|^2 \quad (i = 1, 2, \dots) \tag{5}$$

and if e_i *are real* ($i = 0, 1, \dots$), $e_0 \neq 0$, *then*

$$-\Big(1 - e_0^2 - \frac{e_i^2}{1+e_0}\Big) \leqslant e_{2i} \leqslant 1 - e_0^2 - \frac{e_i^2}{1-e_0} \quad (i = 1, 2, \dots). \tag{6}$$

([2]) See the *Addendum*, p. 235.

Proof. To prove (5) we exclude the trivial case $e_0 = 0$, apply Parseval's Formula to $f(z)(\beta + z^i)$ and obtain

$$|e_0\beta|^2 + |e_1\beta|^2 + \ldots + |e_{i-1}\beta|^2 + |e_0 + e_i\beta|^2 + \ldots$$
$$= \frac{1}{2\pi}\int_0^{2\pi} |f(z)(\beta + z^i)|^2\, d\varphi \qquad (z = e^{i\varphi})$$
$$\leqslant \frac{1}{2\pi}\int_0^{2\pi} |\beta + z^i|^2\, d\varphi = |\beta|^2 + 1.$$

So

$$|e_0\beta|^2 + |e_0 + e_i\beta|^2 \leqslant 1 + |\beta|^2.$$

Putting $\beta = |e_i|/\bar{e}_0 e_i$ (this choice of β was suggested by Dr. H. Iwaniec; Smyth considered only real e_i) we get

$$\left| e_0 + \frac{|e_i|}{\bar{e}_0} \right| \leqslant |e_0|^{-1}$$

and hence (5) holds. The proof of (6) is given by Smyth [7], p. 170. □

Lemma 2. *If $P(z)$ is a polynomial with the leading coefficient p_0, $|P(0)| = |p_0|$, $Q(z) = z^{|P|}\overline{P}(z^{-1}) \neq \text{const}\, P(z)$ then*

$$\frac{\overline{P(0)}P(z)}{p_0 Q(z)} = \frac{f(z)}{g(z)}$$

where $f(z)$ and $g(z)$ are holomorphic in an open disc containing $|z| \leqslant 1$, have absolute value 1 on $|z| = 1$ and $f(0) = g(0) = \pm \prod_{|\alpha_j|>1} \alpha_j^{-1}$ where α_j runs over the zeros of P.

Moreover if $P(z)$ has real coefficients then the Taylor coefficients of f and g are also real, $f(0) = g(0)$ is positive.

Proof. We set

$$f(z) = \pm\frac{p_0}{P(0)} \prod_{|\alpha_j|<1} \left(\frac{z - \alpha_j}{1 - \overline{\alpha}_j z}\right), \quad g(z) = \pm \prod_{|\alpha_j|>1} \left(\frac{1 - \overline{\alpha}_j z}{z - \alpha_j}\right)$$

and verify directly all the statements of the lemma, but the last one. To see the latter notice that for P with real coefficients the sequence $\{\overline{\alpha}_j\}$ is a permutation of $\{\alpha_j\}$, hence

$$\overline{f(z)} = f(\overline{z}), \quad \overline{g(z)} = g(\overline{z});$$

$f(0) > 0$ can be achieved by a suitable choice of the sign $\pm$. □

Proof of Theorem 1 follows closely Smyth's proof of his own theorem. We set

$$\Lambda = \max_{i=1,2,\ldots,n} \prod_{|\alpha_{ij}|>1} |\alpha_{ij}|,$$

and denote the zeros of P by α_j. Since $\sqrt{2} > \theta_0$ we are entitled to assume that $\Lambda < \sqrt{2}$. First of all we must have $P(0) = \pm 1$ for otherwise by a theorem of Kronecker [3] about the conjugates of a totally real algebraic integer

$$\Lambda \geqslant \overline{|P(0)|} \geqslant \sqrt{2}$$

($\overline{|\alpha|}$ denotes the maximum absolute value of the conjugates of α). Secondly $\dfrac{P(z)}{Q(z)}$ is non-constant. Accordingly, put

$$\frac{P(0)P(z)}{Q(z)} = 1 + a_k z^k + a_l z^l + \dots \tag{7}$$

where k, l are the first two indices for which the corresponding a's are non-zero. Since a_k, a_l are totally real algebraic integers we have by the theorem of Kronecker $\overline{|a_l|} \geqslant 1$ and either $\overline{|a_k|} \geqslant \sqrt{2}$ or $a_k = \pm 1$. If $\overline{|a_k|} \geqslant \sqrt{2}$ we may assume that $|a_k| \geqslant \sqrt{2}$, otherwise if $|a_k^{(i)}| \geqslant \sqrt{2}$ we replace $P(z)$ by $P^{(i)}(z)$, which does not affect the value of Λ.

Now by Lemma 2

$$\frac{P(0)P(z)}{Q(z)} = \frac{f(z)}{g(z)} = \frac{c + c_1 z + c_2 z^2 + \dots}{d + d_1 z + d_2 z^2 + \dots} \tag{8}$$

where $f(z) = c + c_1 z + c_2 z^2 + \dots$, $g(z) = d + d_1 z + d_2 z^2 + \dots$ are functions holomorphic in an open disc containing $|z| \leqslant 1$, have real coefficients and

$$|f(z)| = |g(z)| = 1 \quad \text{for} \quad |z| = 1, \tag{9}$$

$$c = d = \prod_{|\alpha_j|>1} |\alpha_j|^{-1}. \tag{10}$$

c On comparing the series in (7) and (8) we obtain

$$c_i = d_i \quad (i = 1, 2, \dots, k-1);$$

$$\begin{cases} a_k c + d_k = c_k, \\ a_k d_i + d_{k+i} = c_{k+i} \quad (i = 1, 2, \dots, l-k-1); \end{cases} \tag{11}$$

$$a_l c + a_k d_{l-k} + d_l = c_l. \tag{12}$$

Now if $|a_k| \geqslant \sqrt{2}$, $\max\bigl(|c_k|, |d_k|\bigr) \geqslant c/\sqrt{2}$ by (11) and so from (5), $c/\sqrt{2} \leqslant 1 - c^2$. This gives by (10) $\Lambda \geqslant c^{-1} \geqslant \sqrt{2}$ a contradiction. Therefore $a_k = \pm 1$. We may assume that $a_k = 1$; otherwise, by interchanging the roles of $P(z)$ and $Q(z)$ (this does not affect the value of Λ), we may replace $1 + a_k z^k + a_l z^l + \dots$ by its formal reciprocal, and so change the sign of a_k.

Further, we may assume that $|a_l| \geqslant 1$, otherwise if $\bigl|a_l^{(i)}\bigr| \geqslant 1$ we replace $P(z)$ by $P^{(i)}(z)$ which affects neither the value of Λ nor $a_k = 1$. It follows from (11) that

$$|c_k| + |d_k| = c \tag{13}$$

for otherwise we would have $\max\bigl(|c_k|, |d_k|\bigr) \geqslant c \geqslant c/\sqrt{2}$ and again $\Lambda \geqslant \sqrt{2}$. Thus c $\max\bigl(|c_k|, |d_k|\bigr) \geqslant c/2$ and from (5) $c/2 \leqslant 1 - c^2$, $c \leqslant \bigl(\sqrt{17} - 1\bigr)/4$. Since by (10) c^{-1} is

an algebraic integer

$$c < \left(\sqrt{17} - 1\right)/4. \tag{14}$$

The argument now divides into two cases.

The case $l < 2k$. Following Smyth [7], pp. 172–173, we get from (9), (11), (12) and $a_k = 1$ that for all real β, γ

$$E = \frac{5}{4}c^2 + \left(c_{l-k} + \gamma c\right)^2 + \left(\frac{a_l c + c_{l-k}}{2}\right) + \left(\frac{\gamma c}{2} - c_{l-k} + \beta c\right)^2 \leqslant 2 + \gamma^2 + \beta^2. \tag{15}$$

$E - \gamma^2 - \beta^2$ is a quadratic polynomial, say, $F(\beta, \gamma, c_{l-k})$. The matrix of the corresponding quadratic form $t^2 F\left(\frac{\beta}{t}, \frac{\gamma}{t}, \frac{c_{l-k}}{t}\right)$ is

$$\begin{bmatrix} c^2 - 1 & \frac{c^2}{2} & -\frac{c}{2} & \frac{a_l c^2}{2} \\ \frac{c^2}{2} & \frac{5}{4}c^2 - 1 & \frac{3}{4}c & \frac{a_l c^2}{4} \\ -\frac{c}{2} & \frac{3}{4}c & \frac{5}{4} & -\frac{a_l c}{4} \\ \frac{a_l c^2}{2} & \frac{a_l c^2}{4} & -\frac{a_l c}{4} & \frac{a_l c^2}{4} + \frac{5}{4}c^2 \end{bmatrix}.$$

The diagonal minors satisfy in virtue of (14) and of $|a_l| \geqslant 1$

$$\begin{gathered} M_1 = c^2 - 1 < 0, \quad M_2 = c^4 - \frac{9}{4}c^2 + 1 > 0, \quad M_3 = \frac{5}{4} - 2c^2 > 0, \\ M_4 = \frac{25}{16}c^2 - \frac{5}{2}c^4 + \frac{c^2 a_l^2}{4} \geqslant \frac{29}{16}c^2 - \frac{5}{2}c^4. \end{gathered} \tag{16}$$

It follows (cf. [1], p. 160) that

$$F\left(\beta, \gamma, c_{l-k}\right) = M_1(\beta + \ldots)^2 + \frac{M_2}{M_1}(\gamma + \ldots)^2 + \frac{M_3}{M_2}(c_{l-k} + \ldots)^2 + \frac{M_4}{M_3}$$

and by (15)

$$\frac{M_4}{M_3} = \min_{c_{l-k}} \max_{\beta, \gamma} F(\beta, \gamma, c_{l-k}) \leqslant 2,$$

which gives by (16)

$$40c^4 - 93c^2 + 40 \geqslant 16(2M_3 - M_4) \geqslant 0$$

and (cf. [7], p. 174)

$$\Lambda \geqslant c^{-1} > \theta_0.$$

The case $l \geqslant 2k$. It follows from (11), (12) and $a_k = 1$ that

$$a_{2k}c + d_k + d_{2k} = c_{2k}. \tag{17}$$

We now apply (6) to f and g, and obtain

$$-\Big(1-c^2-\frac{c_k^2}{1+c}\Big) \leqslant c_{2k} \leqslant 1-c^2-\frac{c_k^2}{1-c}\,,$$
$$-\Big(1-c^2-\frac{d_k^2}{1-c}\Big) \leqslant -d_{2k} \leqslant 1-c^2-\frac{d_k^2}{1+c}\,.$$

Adding these inequalities, and using (17), we have

$$-2(1-c^2)+\frac{d_k^2}{1-c}+\frac{c_k^2}{1+c} \leqslant a_{2k}c+d_k \leqslant 2(1-c^2)-\Big(\frac{d_k^2}{1+c}+\frac{c_k^2}{1-c}\Big). \tag{18}$$

Now from (5) and (13) we know that

$$1-c^2 \geqslant |d_k| \geqslant c^2+c-1.$$

If $l=2k$, $a_{2k} \geqslant 1$ we use the right hand side inequality of (18) and obtain

$$c^2+c-1 \leqslant c-|d_k| \leqslant 2(1-c^2)-\Big(\frac{d_k^2}{1+c}+\frac{c_k^2}{1-c}\Big) \leqslant M,$$

where

$$M=\max_{c^2+c-1\leqslant x\leqslant 1-c^2}\Big(2(1-c^2)-\frac{x^2}{1+c}-\frac{(c-x)^2}{1-c}\Big).$$

If $l=2k$, $a_{2k} \leqslant -1$ we use the left hand side inequality of (18) and obtain

$$c^2+c-1 \leqslant c-|d_k| \leqslant 2(1-c^2)-\Big(\frac{d_k^2}{1-c}+\frac{c_k^2}{1+c}\Big) \leqslant M.$$

If $l>2k$ the inequality $c^2+c-1 \leqslant M$ follows at once from (18). However as Smyth has shown ([7], p. 175) this inequality implies $1-c-c^3 \geqslant 0$, thus $\Lambda \geqslant c^{-1} \geqslant \theta_0$. The proof is complete. □

Lemma 3. *The following inequalities hold*:

$$\prod_{i=1}^{n}(y_i-1) \leqslant \big((y_1\cdots y_n)^{1/n}-1\big)^n \quad \textit{for} \quad y_i>1, \tag{19}$$

with the equality attained only if $y_1=y_2=\ldots=y_n$;

$$y+\sqrt{c+y^2} \geqslant \big(1+\sqrt{c+1}\big)y^{1/\sqrt{c+1}} \quad (c>0,\ y>0) \tag{20}$$

with the equality attained only for $y=1$.

Proof. We have

$$\frac{d^2}{dx^2}\log(e^x-1)=\frac{-e^x}{(e^x-1)^2}<0,$$
$$\frac{d^2}{dx^2}\log\big(e^x+\sqrt{c+e^{2x}}\big)=\frac{ce^x}{\big(c+e^{2x}\big)^{3/2}}>0.$$

The inequality (19) as well as the subsequent statement follows by the substitution $y = e^x$ from the concavity of $\log(e^x - 1)$. The inequality (20) and the subsequent statement follow by the same substitution from the Taylor expansion of $\log\bigl(e^x + \sqrt{c + e^{2x}}\bigr)$ at $x = 0$.

Proof of Theorem 2. Note first that if $a \in K$ then $\bar{a} \in K$ and

(21) $$\bar{a}^{(i)} = \overline{a^{(i)}}, \quad |a^{(i)}|^2 = \bigl(|a|^2\bigr)^{(i)}.$$

Since the conditions on P and the inequality (2) are invariant with respect to multiplication of P by a constant factor we assume that the coefficients of P are integers. If $|P(0)| \neq |p_0|$ we consider the product

(22) $$\prod_{i=1}^{|K|} \bigl||P^{(i)}(0)|^2 - |p_0^{(i)}|^2\bigr| = \bigl|N_{K/\mathbb{Q}}\bigl(|P(0)|^2 - |p_0|^2\bigr)\bigr| \geqslant N_{K/\mathbb{Q}}\bigl(C(P)C(\overline{P})\bigr) = N_{K/\mathbb{Q}}\bigl(C(P)\bigr)^2.$$

Let $\Pi = \prod_{i=1}^{|K|} \max\bigl(\bigl|P^{(i)}(0)/p_0^{(i)}\bigr|, 1\bigr)$ have k factors equal to $\bigl|P^{(i)}(0)/p_0^{(i)}\bigr|$ corresponding to $i = 1, \ldots, k$ and set $N_{K/\mathbb{Q}}(p_0) = N_0$, $N_{K/\mathbb{Q}}\bigl(P(0)\bigr) = N_1$, $N_{K/\mathbb{Q}}\bigl(C(P)\bigr) = N_2$.

We have the identities

$$\prod_{i=1}^{|K|}\Bigl||P^{(i)}(0)|^2 - |p_0^{(i)}|^2\Bigr| = \frac{N_1^2}{\Pi^2}\prod_{i=1}^{k}\Bigl|\Bigl|\frac{P^{(i)}(0)}{p_0^{(i)}}\Bigr|^2 - 1\Bigr| \cdot \prod_{i=k+1}^{|K|}\Bigl|\Bigl|\frac{p_0^{(i)}}{P^{(i)}(0)}\Bigr|^2 - 1\Bigr|,$$

$$\prod_{i=1}^{k}\Bigl|\frac{P^{(i)}(0)}{p_0^{(i)}}\Bigr| \cdot \prod_{i=k+1}^{|K|}\Bigl|\frac{p_0^{(i)}}{P^{(i)}(0)}\Bigr| = \Pi^2\Bigl|\frac{N_0}{N_1}\Bigr|.$$

Hence by (21), (22) and (19)

(23) $$N_2^2 \leqslant \frac{N_1^2}{\Pi^2}\bigl(\Pi^{4/|K|}|N_0N_1^{-1}|^{2/|K|} - 1\bigr)^{|K|} = \bigl((\Pi N_0)^{2/|K|} - |N_1|^{2/|K|}\Pi^{-2/|K|}\bigr)^{|K|};$$

$$N_2^{2/|K|} \leqslant (\Pi N_0)^{2/|K|} - |N_1|^{2/|K|}\Pi^{-2/|K|};$$

$$\Pi^{2/|K|} \geqslant \frac{N_2^{2/|K|} + \sqrt{4|N_0N_1|^{2/|K|} + N_2^{4/|K|}}}{2N_0^{2/|K|}}.$$

Thus by (20) with $c = 4$, $y = |N_2^2/N_0N_1|$

(24) $$\Pi^{2/|K|}\Bigl|\frac{N_0}{N_1}\Bigr|^{1/|K|} \geqslant \frac{1+\sqrt{5}}{2}\Bigl|\frac{N_2^2}{N_0N_1}\Bigr|^{1/|K|\sqrt{5}},$$

$$\Pi \geqslant \Bigl(\frac{1+\sqrt{5}}{2}\Bigr)^{|K|/2}\Bigl|\frac{N_2}{N_0}\Bigr|^{1/2+1/2\sqrt{5}}\Bigl|\frac{N_1}{N_2}\Bigr|^{1/2-1/2\sqrt{5}}$$

and since $\prod_{|\alpha_{ij}|>1} |\alpha_{ij}| \geqslant \max\bigl(|P^{(i)}(0)/p_0^{(i)}|, 1\bigr)$ the inequality (2) follows.

The equality is possible only if we have equality in (23) and (24) hence by Lemma 3 only if

$$\left|\frac{P^{(i)}(0)|}{p_0^{(i)}}\right| = \begin{cases} |P^{(1)}(0)/p_0^{(1)}| & \text{for } i = 1, \dots, k, \\ |P^{(1)}(0)/p_0^{(1)}|^{-1} & \text{for } i = k+1, \dots, |K|; \end{cases} \tag{25}$$

$$N_2^2 = |N_0 N_1|.$$

Since $N_2 \mid N_0$ and $N_2 \mid N_1$ the last equality implies $|N_0| = |N_1| = N_2$ and $C(P) = (p_0)$. Moreover by (25) the equality in (24) gives

$$\left|\frac{P^{(1)}(0)}{p_0^{(1)}}\right|^{2k} = \left(\frac{1+\sqrt{5}}{2}\right)^{|K|}$$

hence $\sqrt{5} \in K$. Besides by (25)

$$\left|\frac{P^{(i)}(0)}{p_0^{(i)}}\right|^{2k} = \begin{cases} \left(\frac{1+\sqrt{5}}{2}\right)^{|K|} & \text{for } i = 1, \dots, k, \\ \left(\frac{1-\sqrt{5}}{2}\right)^{|K|} & \text{for } i = k+1, \dots, |K|, \end{cases}$$

which implies $k = |K|/2$, $|P(0)/p_0| = \dfrac{\pm 1 + \sqrt{5}}{2}$.

In this way the theorem is proved in full for the case where $|P(0)| \neq |p_0|$. If $|P(0)| = |p_0|$ then by Lemma 2

$$\frac{\overline{P^{(i)}(0)}P^{(i)}(z)}{p_0^{(i)} Q_i(z)} = \frac{f_i(z)}{g_i(z)}, \tag{26}$$

where $Q_i(z) = z^{|P|}\overline{P^{(i)}}(z^{-1})$; $f_i(z)$, $g_i(z)$ are holomorphic in an open disc containing $|z| \leqslant 1$, have absolute value 1 on $|z| = 1$ and

$$f_i(0) = g_i(0) = \pm \prod_{|\alpha_{ij}|>1} \alpha_{ij}^{-1}. \tag{27}$$

However by (21) $\overline{P^{(i)}(0)} = \overline{P(0)}^{(i)}$, $Q_i(z) = Q^{(i)}(z)$, thus

$$\frac{\overline{P^{(i)}(0)}P^{(i)}(z)}{p_0^{(i)} Q_i(z)} = 1 + a_k^{(i)} z^k + \dots \tag{28}$$

where $a_k^{(i)}$ is the first non-zero coefficient. Setting

$$f_i(z) = c_{i0} + c_{i1} z + c_{i2} z^2 + \dots,$$
$$g_i(z) = d_{i0} + d_{i1} z + d_{i2} z^2 + \dots,$$

we get from (27) and (28)

$$a_k^{(i)} c_{i0} + d_{ik} = c_{ik}.$$

By (5)

$$|c_{ik}| \leqslant 1 - |c_{i0}|^2, \quad |d_{ik}| \leqslant 1 - |d_{i0}|^2,$$

hence

$$|a_k^{(i)}|\,|c_{i0}| \leqslant 2 - 2|c_{i0}|^2,$$

and by (20) with $c = 16$, $y = |a_k^{(i)}|$

$$|c_{i0}|^{-1} \geqslant \frac{|a_k^{(i)}|}{4} + \sqrt{1 + \left(\frac{|a_k^{(i)}|}{4}\right)^2} \geqslant \frac{1+\sqrt{17}}{4}\,|a_k^{(i)}|^{1/\sqrt{17}}.$$

Hence by (27)

$$(\#) \qquad \prod_{i=1}^{|K|} \prod_{|\alpha_{ij}|>1} |\alpha_{ij}| = \prod_{i=1}^{|K|} |c_{i0}|^{-1} \geqslant \left(\frac{1+\sqrt{17}}{4}\right)^{|K|} \left|N_{K/\mathbb{Q}} a_k^{(1)}\right|^{1/\sqrt{17}}.$$

c Now, if $\overline{(P(0))}C(P) = (p_0)C(\overline{P})$ then by (28) $\overline{p}_0^{(i)} a_k^{(i)}$ is an integer divisible by
c $C(\overline{P}^{(i)})$, thus

$$\left|N_{K/\mathbb{Q}} a_k^{(1)}\right| \geqslant N_{K/\mathbb{Q}} \frac{C(P)}{(p_0)}$$

and

$$\prod_{i=1}^{|K|} \prod_{|\alpha_{ij}|>1} |\alpha_{ij}| \geqslant \left(\frac{1+\sqrt{17}}{4}\right)^{|K|} \left(N_{K/\mathbb{Q}} \frac{C(P)}{(p_0)}\right)^{1/\sqrt{17}}.$$

The equality is impossible here since it implies by Lemma 3 that $a_k^{(i)} = 1$ and $C(P) = (p_0)$, but then the left hand side is an algebraic integer while the right hand side is not.

It remains to consider the case where $|P(0)| = |p_0|$ and P is irreducible.

Let m be the greatest integer such that $P(z) = R(z^{2^m})$ with $R \in K[z]$. Then $R(z) \neq R(-z)$. Since P and R have the same leading coefficients, $R(0) = P(0)$, $C(R) = C(P)$ and both sides of (2) have the same value for P and for R we may assume at once that $P(z) \neq P(-z)$. Also $P(z) \neq -P(-z)$ since $P(0) \neq 0$ and we can choose $\varepsilon = \pm 1$ such that $z^{|P|}P(z^{-1}) \neq \text{const}\, P(\varepsilon z)$.

Consider now the polynomial $S(z) = P(z)\overline{P}(\varepsilon z)$. It satisfies the condition

$$z^{|S|}\overline{S}(z^{-1}) \neq \text{const}\, S(z),$$

since the irreducible factor $z^{|P|}\overline{P}(z^{-1})$ of the left hand side is not proportional to either factor of the right hand side. Moreover the leading coefficient s_0 of S equals $\pm|p_0|^2 = \pm|P(0)|^2 = \pm S(0)$, $C(S) = C(P)C(\overline{P})$ and $\overline{(S(0))}C(S) = (s_0)C(\overline{S})$.

Applying to S the part of (2) already proved and using the fact that the zeros of S

coincide in absolute value with those of P we get

$$\prod_{i=1}^{|K|}\Big(\prod_{|\alpha_{ij}|>1}|\alpha_{ij}|\Big)^2 > \left(\frac{1+\sqrt{17}}{4}\right)^{|K|}\left(N_{K/\mathbb{Q}}\frac{C(S)}{(s_0)}\right)^{1/\sqrt{17}},$$

hence

$$\prod_{i=1}^{|K|}\prod_{|\alpha_{ij}|>1}|\alpha_{ij}| \geqslant \left(\frac{1+\sqrt{17}}{4}\right)^{|K|/2}\left(N_{K/\mathbb{Q}}\frac{C(P)}{(p_0)}\right)^{1/\sqrt{17}}$$

and the proof is complete. □

Proof of Corollary 1. Since $z^{|P|}\overline{P}(z^{-1}) \neq \text{const}\ P(z)$ at least one irreducible factor of P, say R, satisfies $z^{|R|}\overline{R}(z^{-1}) \neq \text{const}\ R(z)$. Denoting the leading coefficient of R by r_0 and the zeros of $R^{(i)}$ by β_{ij} we have

$$\begin{aligned}\prod_{i=1}^{|K|}\prod_{|\alpha_{ij}|>1}|\alpha_{ij}| &\geqslant \prod_{i=1}^{|K|}\prod_{|\beta_{ij}|>1}|\beta_{ij}| \\ &\geqslant \min\left\{\left(\frac{1+\sqrt{5}}{2}\right)^{|K|/2}\left(N_{K/\mathbb{Q}}\,\frac{C(R)}{(r_0)}\right)^{1/2+1/2\sqrt{5}},\right. \\ &\qquad \left.\left(\frac{1+\sqrt{17}}{4}\right)^{|K|/2}\left(N_{K/\mathbb{Q}}\,\frac{C(R)}{(r_0)}\right)^{1/\sqrt{17}}\right\} \\ &\geqslant \left(\frac{1+\sqrt{17}}{4}\right)^{|K|/2} N_{K/\mathbb{Q}}\,\frac{C(P)}{(p_0)},\end{aligned}$$

since by the multiplicative property of the content $(p_0)C(P)^{-1}$ is divisible by $(r_0)C(R)^{-1}$. In the above sequence of inequalities at least one must be strict, which proves the corollary. □

Lemma 4. *If f is a monic polynomial with complex coefficients and the zeros z_j then*

$$\prod_{|z_j|>1}|z_j|^2 + \prod_{|z_j|<1}|z_j|^2 \leqslant \|f\| \tag{29}$$

(*empty products denote* 1) *with the equality attained only if*

$$z^{|f|}f(z)\overline{f}(z^{-1}) = \overline{f(0)}z^{2|f|} + \|f\|z^{|f|} + f(0).$$

Proof. The inequality (29) is due to J. V. Gonçalves [2], it is only the last assertion of the lemma, which requires the proof. This is obtained easily from Ostrowski's proof of (29). Ostrowski [5] shows namely that $\|f\| = \|g\|$, where

$$g(z) = \prod_{|z_j|>1}(z-z_j)\prod_{|z_j|<1}(1-z\bar{z}_j) = z^{|f|}\prod_{|z_j|<1}(-\bar{z}_j) + \ldots + \prod_{|z_j|>1}(-z_j).$$

Therefore equality in (23) implies that

$$g(z) = z^{|f|} \prod_{|z_j|<1} (-z_j) + \prod_{|z_j|>1} (-z_j),$$

whence

$$z^{|f|} f(z)\overline{f}(z^{-1}) = \overline{f(0)} z^{2\|f\|} + \|f\| z^{|f|} + f(0). \qquad \square$$

Proof of Theorem 3. Since the inequalities (3) are invariant with respect to multiplication of f by a constant factor we may assume that f is monic. Let the conjugates of K be numbered so that all different conjugates of f occur equally often among $f^{(i)}$ $(i = 1, \dots, |L|)$.

Let z_{ij} be the zeros of $f^{(i)}$. Let finally

$$f = P_0 P_1 \cdots P_n,$$

where P_ν are monic and for $\nu > 0$ satisfy $z^{|P_\nu|}\overline{P}_\nu(z^{-1}) \neq \text{const } P_\nu(z)$. We have

$$N_{K/\mathbb{Q}}\big(C(P_0)\big) \leqslant 1 \quad \text{and} \quad \prod_{\nu=0}^{n} C(P_\nu) = C(f).$$

Hence by Corollary 1

$$\left(\prod_{i=1}^{|L|} \prod_{|z_{ij}|>1} |z_{ij}|\right)^{|K|/|L|} = \prod_{i=1}^{|K|} \prod_{|z_{ij}|>1} |z_{ij}| = \prod_{\nu=0}^{n} \prod_{i=1}^{|K|} \prod_{\substack{P_\nu^{(i)}(z_{ij})=0 \\ |z_{ij}|>1}} |z_{ij}|$$

$$\geqslant \left(\frac{1+\sqrt{17}}{4}\right)^{|K|n/2} \prod_{\nu=0}^{n} N_{K/\mathbb{Q}}\big(C(P_\nu)\big) = \left(\frac{1+\sqrt{17}}{4}\right)^{|K|n/2} N_{L/\mathbb{Q}}\big(C(f)\big)^{|K|/|L|}$$

and

$$(30_1) \qquad \Pi = \prod_{i=1}^{|L|} \prod_{|z_{ij}|>1} |z_{ij}| \geqslant \left(\frac{1+\sqrt{17}}{4}\right)^{|L|n/2} N_{L/\mathbb{Q}}\big(C(f)\big).$$

If all prime ideal factors $\mathfrak{p}$ of $\big(1, f(0)\big)C(f)^{-1}$ in K satisfy $\overline{\mathfrak{p}} = \mathfrak{p}$ then in view of the divisibility

$$\big(1, P_\nu(0)\big)C(P_\nu)^{-1} \,\big|\, \big(1, f(0)\big)C(f)^{-1}$$

we have $\big(1, P_\nu(0)\big)C(P_\nu)^{-1} = \big(1, \overline{P_\nu(0)}\big)C(\overline{P_\nu})^{-1} = \mathfrak{a}_\nu$. Hence either $|P_\nu(0)| \neq 1$ or

$$\big(\overline{P_\nu(0)}\big)C(P_\nu) = \big(\overline{P_\nu(0)}\big)\big(1, P_\nu(0)\big)\mathfrak{a}_\nu^{-1}$$
$$= \big(\overline{P_\nu(0)}, |P_\nu(0)|^2\big)\mathfrak{a}_\nu^{-1} = \big(\overline{P_\nu(0)}, 1\big)\mathfrak{a}_\nu^{-1} = C(\overline{P_\nu})$$

and using Theorem 2 instead of Corollary 1 we get

$$\Pi = \prod_{i=1}^{|L|} \prod_{|z_{ij}|>1} |z_{ij}| \geqslant \Big(\frac{1+\sqrt{5}}{2}\Big)^{|L|n/2} N_{L/\mathbb{Q}}\big(C(f)\big). \tag{30_2}$$

On the other hand, by Lemma 4

$$\prod_{|z_{ij}|>1} |z_{ij}|^2 + \prod_{|z_{ij}|<1} |z_{ij}|^2 \leqslant \|f^{(i)}\| \quad (i = 1, \dots, |L|), \tag{31}$$

hence

$$\prod_{i=1}^{|L|} \prod_{|z_{ij}|>1} |z_{ij}|^2 + \prod_{i=1}^{|L|} \prod_{|z_{ij}|<1} |z_{ij}|^2 \leqslant N_{L/\mathbb{Q}}\|f\|. \tag{32}$$

However

$$\prod_{i=1}^{|L|} \prod_{|z_{ij}|<1} |z_{ij}|^2 = \Pi^{-2} N_{L/\mathbb{Q}} |f(0)|^2 \geqslant \Pi^{-2} N_{L/\mathbb{Q}}^4\big(C(f)\big) \tag{33}$$

for $N_{L/\mathbb{Q}}\big(C(f)\big) \leqslant \min\big(1, |Nf(0)|\big)$. Thus

$$\Pi^2 + N_{L/\mathbb{Q}}^4\big(C(f)\big)\Pi^{-2} \leqslant N_{L/\mathbb{Q}}\|f\|$$

and by (30) the inequalities (3) follow. The equality in (3_2) implies the equality in (30_2), (31), (32) and (33). The equality in (31) and (32) imply that $|L| = 1$. The equality in (33) implies $C(f) = |f(0)| = 1$. By Lemma 4 the equality in (31) implies

$$z^{|f|} f(z) f\Big(\frac{1}{z}\Big) = \pm z^{2|f|} + \bigg[\Big(\frac{1+\sqrt{5}}{2}\Big)^n + \Big(\frac{1+\sqrt{5}}{2}\Big)^{-n}\bigg] z^{|f|} \pm 1. \tag{34}$$

Since $\Big(\frac{1+\sqrt{5}}{2}\Big)^n + \Big(\frac{1+\sqrt{5}}{2}\Big)^{-n}$ is an integer, n must be even, $n = 2m$. If $n = 0$ then

$$z^{|f|} f(z) f\Big(\frac{1}{z}\Big) = \pm\big(z^{|f|} \pm 1\big)^2$$

and since all cyclotomic polynomials are reciprocal

$$z^{|f|} f\Big(\frac{1}{z}\Big) = \pm f(z); \quad f(z)^2 = (z^{|f|} \pm 1)^2; \quad f(z) = z^{|f|} \pm 1.$$

If $n > 0$ then the equality in (30_2) implies in virtue of Theorem 2 that $\sqrt{5} \in K$ and $|P_\nu(0)| = \dfrac{1+\sqrt{5}}{2}$ for $\nu = 1, 2, \dots, n$.

Now, the right hand side of (34) equals

$$\pm\bigg(z^{|f|} \pm \Big(\frac{1+\sqrt{5}}{2}\Big)^{2m}\bigg)\bigg(z^{|f|} \pm \Big(\frac{1-\sqrt{5}}{2}\Big)^{2m}\bigg)$$

hence $g(z) = z^{|f|} \pm \Big(\dfrac{1+\sqrt{5}}{2}\Big)^{2m}$ has in K $2m$ monic factors P such that $|P(0)| = \dfrac{1+\sqrt{5}}{2}$.

Since the zeros of $g(z)$ have absolute value $\left(\frac{1+\sqrt{5}}{2}\right)^{2m/|f|}$ it follows that the degree of each factor is $|f|/2m$, hence $|f| = 2lm$, l integer. Let $\alpha = \operatorname{ord}_2 m + \frac{1}{2} \pm \frac{1}{2}$, where the sign is that occurring in (34). We have

$$g_1(z) = z^{2^{\alpha_l}} + \left(\frac{1+\sqrt{5}}{2}\right)^{2^\alpha} \Big| g(z).$$

By Capelli's theorem $g_1(z)$ is irreducible in $\mathbb{Q}(\sqrt{5})$ hence by (34)

$$g_1(z) \,|\, f(z) \quad \text{or} \quad g_1(z) \,|\, z^{|f|} f\left(\frac{1}{z}\right).$$

Assuming without loss of generality the first possibility we get

$$z^{2^{\alpha_l}} + \left(\frac{1-\sqrt{5}}{2}\right)^{2^\alpha} \Big| f(z),$$

$$z^{2^{\alpha_l}} + (-1)^{2^\alpha}\left(\frac{1+\sqrt{5}}{2}\right)^{2^\alpha} \Big| z^{|f|} f\left(\frac{1}{z}\right)$$

and if $\alpha > 0$

$$g_1(z)^2 \,|\, \pm z^{2|f|} + \left[\left(\frac{1+\sqrt{5}}{2}\right)^{2m} + \left(\frac{1+\sqrt{5}}{2}\right)^{-2m}\right] z^{|f|} \pm 1,$$

which is impossible. Therefore $\alpha = 0$, the sign is lower and m is odd. It remains to show that $K \supset \mathbb{Q}\left(\sqrt{5}, e^{2\pi i/m}\right)$. Assume that any of the considered factors of $g(z)$ in K is not binomial. Then it has a coefficient of the form $c\left(\frac{1+\sqrt{5}}{2}\right)^{k/l}$, where $0 < k < l$, $c \neq 0$ and $c \in \mathbb{Q}(\zeta_{2lm})$. It follows that

$$\left(\frac{1+\sqrt{5}}{2}\right)^{k/l} \in K(\zeta_{2lm}),$$

which is impossible since the field $K(\zeta_{2lm})$ satisfies again the assumptions of Theorem 2 and $\left(\frac{1+\sqrt{5}}{2}\right)^{k/l}$ has some real and some complex conjugates. Thus the required factorization of $g(x)$ in K is

$$z^{2lm} - \left(\frac{1+\sqrt{5}}{2}\right)^{2m} = \prod_{j=0}^{2m-1}\left(z^l - \frac{1+\sqrt{5}}{2}\,\zeta_{2m}^j\right)$$

and $K \supset \mathbb{Q}\left(\sqrt{5}, \zeta_m\right)$. Conversely, if $K \supset \mathbb{Q}\left(\sqrt{5}, \zeta_m\right)$, $L = \mathbb{Q}$ and f satisfies (4) then $z^{|f|} f(z) f(z^{-1})$ has $4m$ factors in K, $f(z)$ has $2m$ factors and the equality holds in (3_2).□

Proof of Corollary 2. $\varphi(z)$ satisfies the conditions of (3_2). If $z^{|P|}\overline{P}(z^{-1}) = \text{const}\, P(z)$ and $P(z) \,|\, \varphi(z)$ then $P(z) \,|\, z^{|\varphi|}\varphi(z^{-1})$, thus

$$P(z) \,|\, (z^p + \varepsilon z^q + \eta) - (z^p + \varepsilon\eta z^{p-q} + \eta) = \varepsilon z^q - \varepsilon\eta z^{p-q}$$

and P is cyclotomic. Therefore, it remains to consider the case where n occurring in (3_2)

for $f = \varphi$, $L = \mathbb{Q}$ equals 2. Then (3_2) becomes an equality and by Theorem 3 $\sqrt{5} \in K$,

$$z^p \varphi(z) \varphi\Big(\frac{1}{z}\Big) = c(z^{2p} - 3z^p + 1).$$

It follows that $\varphi(z) = z^{2q} \pm z^q - 1$. □

Addendum

The aim of this Addendum is to formulate two theorems which go further than Theorems 2 and 3 and have been practically proved above, but the fact has been overlooked by the writer. The notation is retained. In particular for a given polynomial F we denote by $|F|$ its degree, by $C(F)$ its content and by $\|F\|$ the sum of squares of the absolute values of the coefficients.

Theorem 2′. *Let K be a totally real algebraic number field or a totally complex quadratic extension of such a field and $P \in K[z]$ a polynomial with the leading coefficient p_0 such that $z^{|P|}\overline{P}(z^{-1}) \neq \text{const}\, P(z)$, $P(0) \neq 0$.*

Let $|K|$ be the degree of K, $P^{(i)}$ $(i = 1, \ldots, |K|)$ the polynomials conjugate to $P(z)$ and α_{ij} the zeros of $P^{(i)}(z)$. Then

$$\prod_{i=1}^{|K|} \prod_{|\alpha_{ij}|>1} |\alpha_{ij}| \geqslant \begin{cases} \Big(\dfrac{1+\sqrt{5}}{2}\Big)^{|K|/2} \Big(N_{K/\mathbb{Q}} \dfrac{C(P)}{(p_0)}\Big)^{(1+\sqrt{5})/2} \Big(N_{K/\mathbb{Q}} \dfrac{(P(0))}{C(P)}\Big)^{(1-\sqrt{5})/2} \\ \qquad\qquad \text{if } |P(0)| \neq |p_0|, \\ \Big(\dfrac{1+\sqrt{17}}{4}\Big)^{|K|} \Big(N_{K/\mathbb{Q}} \dfrac{(\overline{P(0)}C(P),\, p_0 C(\overline{P}))}{(p_0 \overline{p}_0)}\Big)^{1/\sqrt{17}} \\ \qquad\qquad \text{if } |P(0)| = |p_0|. \end{cases}$$

Corollary 1′. *If $z^{|P|}\overline{P}(z^{-1}) \neq \text{const}\, P(z)$, $P(0) \neq 0$ then*

$$\prod_{i=1}^{|K|} \prod_{|\alpha_{ij}|>1} |\alpha_{ij}| \geqslant \Big(\frac{1+\sqrt{5}}{2}\Big)^{|K|/2} N_{K/\mathbb{Q}} \frac{C(P)}{(p_0)}.$$

Theorem 3′. *Let K satisfy the assumptions of Theorem 2′, L be a subfield of K, $f(z) \in L[z]$. The number n of irreducible over K factors P of f such that $z^{|P|}\overline{P}(z^{-1}) \neq \text{const}\, P(z)$, $P(0) \neq 0$, counted with their multiplicities satisfies the inequality*

$$(*) \qquad \Big(\frac{1+\sqrt{5}}{2}\Big)^{n|L|} + \Big(\frac{1+\sqrt{5}}{2}\Big)^{-n|L|} \leqslant N_{L/\mathbb{Q}} \|f\| N_{L/\mathbb{Q}}^{-2} C(f)$$

with the equality attained only if either $L = \mathbb{Q}$, $f(z) = c\big(z^{|f|} \pm 1\big)$ *or* $K \supset \mathbb{Q}\big(\sqrt{5}, \zeta_m\big)$, $L = \mathbb{Q}$,

$$(**) \qquad z^{|f|} f(z) f\Big(\frac{1}{z}\Big) = c\bigg(z^{4lm} - \bigg[\Big(\frac{1+\sqrt{5}}{2}\Big)^{2m} + \Big(\frac{1-\sqrt{5}}{2}\Big)^{2m}\bigg] z^{2lm} + 1\bigg),$$

l, m *integers,* m *odd.*

Corollary 2′. *The number* n *occurring in Theorem* 3′ *satisfies the inequality*

$$n < \frac{\log\big(N_{L/\mathbb{Q}} \| f \| N_{L/\mathbb{Q}}^{-2} C(f)\big)}{|L| \log((1+\sqrt{5})/2)}$$

where the constant $\log((1+\sqrt{5})/2)$ *is best possible.*

To see Theorem 2′ it is enough to note that by (28) $p_0^{(i)} \overline{p}_0^{(i)} a_k^{(i)}$ is an integer divisible by

$$\big(\overline{P^{(i)}(0)} C(P^{(i)}),\ p_0^{(i)} C(\overline{P}^{(i)})\big).$$

(In particular if $\overline{P}(0) C(P) = (p_0) C(\overline{P})$ then $\overline{p}_0^{(i)} a_k^{(i)}$ is divisible by $C(\overline{P}^{(i)})$.) Hence

$$|N_{K/\mathbb{Q}} a_k^{(1)}| \geqslant N_{K/\mathbb{Q}} \frac{\big(\overline{P(0)} C(P),\ p_0 C(\overline{P})\big)}{(p_0 \overline{p}_0)}$$

and the assertion of Theorem 2′ in the case $|P(0)| = |p_0|$ follows from formula (#) on page 230. The case $|P(0)| \neq |p_0|$ has been settled in the main part of the paper.

To see Corollary 1′ it is enough to note that

$$\Big(\frac{1+\sqrt{17}}{4}\Big)^{|K|} N_{K/\mathbb{Q}}\bigg(\frac{\big(\overline{P(0)} C(P),\ p_0 C(\overline{P})\big)}{(p_0 \overline{p}_0)}\bigg)^{1/\sqrt{17}} > \Big(\frac{1+\sqrt{5}}{2}\Big)^{|K|/2} \Big(N_{K/\mathbb{Q}} \frac{C(P)}{(p_0)}\Big)^{2/\sqrt{17}}.$$

Theorem 3′ follows from Corollary 1′ in the same way as Theorem 3 from Theorem 2 under the assumption about prime ideal factors of $\big(f_0, f(0)\big) C(f)^{-1}$, where f_0 is the leading coefficient of f.

Corollary 2′ follows directly from $(*)$ and the existence of polynomials satisfying $(**)$, e.g.

$$f(z) = z^{2lm} \pm \bigg[\Big(\frac{1+\sqrt{5}}{2}\Big)^{m} + \Big(\frac{1-\sqrt{5}}{2}\Big)^{m}\bigg] z^{lm} - 1.$$

Note that the bound given in Corollary 2′ is independent of K.

References

[1a] H. Bohr, *A theorem concerning power series*, Proc. London Math. Soc. (2) 13 (1914), 1–5.

[1] R. Fricke, *Lehrbuch der Algebra* I. Braunschweig 1924.

[2] J. Vicente Gonçalves, *L'inégalité de W. Specht*. Univ. Lisboa Revista Fac. Ci. A (2) 1 (1956), 167–171.

[3] L. Kronecker, *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten*. J. Reine Angew. Math. 53 (1857), 173–175.

[4] W. Ljunggren, *On the irreducibility of certain trinomials and quadrinomials*. Math. Scand. 8 (1960), 65–70.

[5] A. M. Ostrowski, *On an inequality of J. Vicente Gonçalves*. Univ. Lisboa Revista Fac. Ci. A (2) 8 (1960), 115–119.

[6] C. L. Siegel, *Algebraic integers whose conjugates lie in the unit circle*. Duke Math. J. 11 (1944), 597–602.

[7] C. J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*. Bull. London Math. Soc. 3 (1971), 169–175.

[8] H. Tverberg, *On the irreducibility of the trinomials* $x^n \pm x^m \pm 1$. Math. Scand. 8 (1960), 121–126.

Originally published in
Acta Arithmetica XXVIII (1975), 161–175

On linear dependence of roots

In memory of Professor L. J. Mordell

L. J. Mordell [4] proved in 1953 the following theorem. Let K be an algebraic number field, $\alpha_1, \dots, \alpha_k$ elements of K, $n_1, \dots, n_k$ positive integers, $\xi_i^{n_i} = \alpha_i$ $(1 \leqslant i \leqslant k)$. If $\prod_{i=1}^{k} \xi_i^{x_i} \in K$ implies $x_i \equiv 0 \bmod n_i$ and either the numbers ξ_i are real or K contains n_ith roots of unity $(1 \leqslant i \leqslant k)$ then the degree of the extension $K(\xi_1, \dots, \xi_k)$ over K is $n_1 \cdots n_k$. This theorem has been recently extended by C. L. Siegel [7] and M. Kneser [3].

The latter obtained the following purely algebraic result. Let K be any field, $K(\xi_1, \dots, \xi_k)$ a separable extension of K and $K^* \langle \xi_1, \dots, \xi_k \rangle$ the multiplicative group generated by $\xi_1, \dots, \xi_k$, all of finite order, over K^*. The degree $[K(\xi_1, \dots, , \xi_k) : K]$ is equal to the index $[K^* \langle \xi_1, \dots, \xi_k \rangle : K^*]$ if and only if for every prime p, $\zeta_p \in K^* \langle \xi_1, \dots, \xi_k \rangle$ implies $\zeta_p \in K$ and $1 + \zeta_4 \in K^* \langle \xi_1, \dots, \xi_k \rangle$ implies $\zeta_4 \in K$, where ζ_q is a primitive qth root of unity.

We shall use Kneser's theorem to get a necessary and sufficient condition for the field $K(\xi_1, \dots, \xi_k)$ to be of degree $n_1 \cdots n_k$ over K.

Theorem 1. *Let K be any field. Assume that the characteristic of K does not divide $n_1 \cdots n_k$ and $\xi_i^{n_i} = \alpha_i \in K^*$. $[K(\xi_1, \dots, \xi_k) : K] = n_1 \cdots n_k$ if and only if, for all primes p, $\prod_{p \mid n_i} \alpha_i^{x_i} = \gamma^p$ implies $x_i \equiv 0 \bmod p$ $(p \mid n_i)$ and $\prod_{2 \mid n_i} \alpha_i^{x_i} = -4\gamma^4$, $n_i x_i \equiv 0 \bmod 4$ $(2 \mid n_i)$ implies $x_i \equiv 0 \bmod 4$ $(2 \mid n_i)$* ([1]).

The above theorem can be regarded as a generalization of Capelli's theorem which corresponds to the case $k = 1$. It should however be noted that Capelli's theorem holds without any condition on the characteristic of K (see [5], Theorem 428) while Theorem 1 does not, as it is shown by the example $K = Z_2(t)$, $n_1 = n_2 = 2$, $\alpha_1 = t$, $\alpha_2 = t + 1$.

We have further

Theorem 2. *Assume that the characteristic of K does not divide $n_1 \cdots n_k$. If either $\zeta_4 \in K$ or $n_i x_i \equiv 0 \bmod 4$ $(2 \mid n_i)$ implies $\prod_{2 \mid n_i} \alpha_i^{x_i} \neq -\gamma^4, -4\gamma^4$ then there exist elements $\xi_1, \dots, \xi_k$ such that $\xi_i^{n_i} = \alpha_i$ and*

$$[K(\xi_1, \dots, \xi_k) : K] = [K^* \langle \xi_1, \dots, \xi_k \rangle : K^*]. \tag{1}$$

([1]) $(p \mid n_i)$ means here "for all i such that $p \mid n_i$".

It follows from Kneser's theorem that if $\zeta_4 \notin K$ and for some $x_i, n_i x_i \equiv 0 \bmod 4\,(2 \mid n_i)$, $\prod_{2\mid n_i} \alpha_i^{x_i} = -4\gamma^4$ then for no choice of $\xi_1, \ldots, \xi_k$ satisfying $\xi_i^{n_i} = \alpha_i$ the equality (1) holds. The example $K = \mathbb{Q}$, $n_1 = n_2 = 8$, $\alpha_1 = -1$, $\alpha_2 = -16$ shows that the converse is not true. Indeed for any choice of ξ_1, ξ_2 we get

$$[K(\xi_1, \xi_2) : K] = 8 < [K^* \langle \xi_1, \xi_2 \rangle : K^*] = 16.$$

It seems difficult to give a simple necessary and sufficient condition for the existence of $\xi_1, \ldots, \xi_k$ satisfying (1). On the other hand Theorem 1 combined with some results of [6] leads to a necessary and sufficient condition for the following phenomenon: each of the fields $K(\xi_1, \ldots, \xi_k)$ contains at least one η with $\eta^n = \beta$ (β and n fixed, $n_i \mid n$). Condition given in [6] was necessary but not always sufficient. We shall prove even a more precise result.

Theorem 3. *Let τ be the largest integer such that $\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} \in K$, if there are only finitely many of them, otherwise $\tau = \infty$. Let $n_1, \ldots, n_k$ be positive integers, $\alpha_1, \ldots, \alpha_k$ non-zero elements of K. There exist elements $\xi_1, \ldots, \xi_k$ with $\xi_i^{n_i} = \alpha_i$ $(1 \leqslant i \leqslant k)$ such that for all n divisible by $n_1, \ldots, n_k$, but not by the characteristic of K and for all $\beta \in K$: if $K(\xi_1, \ldots, \xi_k)$ contains at least one η with $\eta^n = \beta$ then at least one of the following three conditions is satisfied for suitable rational integers $l_1, \ldots, l_k, q_1, \ldots, q_k$ and suitable $\gamma, \delta \in K$.*

(i) $\beta \prod_{i=1}^{k} \alpha_i^{q_i n/n_i} = \gamma^n$,

(ii) $n \not\equiv 0 \bmod 2^\tau$, $\prod_{2\mid n_i} \alpha_i^{l_i} = -\delta^2$, $\beta \prod_{i=1}^{k} \alpha_i^{q_i n/n_i} = -\gamma^n$,

(iii) $n \equiv 0 \bmod 2^\tau$, $\prod_{2\mid n_i} \alpha_i^{l_i} = -\delta^2$, $\beta \prod_{i=1}^{k} \alpha_i^{q_i n/n_i} = (-1)^{n/2^\tau}\left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{n/2}\gamma^n$.

Conversely if any of the above conditions is satisfied then each of the fields $K(\xi_1, \ldots, \xi_k)$ where $\xi_i^{n_i} = \alpha_i$ contains at least one η with $\eta^n = \beta$.

If $\zeta_4 \in K$ the conditions (ii), (iii) *imply* (i); *if $\tau = 2$* (ii) *implies* (i) *for not necessarily the same $q_1, \ldots, q_k$ and γ.*

This theorem can be regarded as an extension of the classical result concerning Kummer fields ([2], p. 42).

Let us write for two irreducible polynomials f and g over K: $f \sim g$ if $f(\alpha_1) = 0$ and $g(\alpha_2) = 0$ where $K(\alpha_1) = K(\alpha_2)$. The relation $\sim$ introduced by Gerst [1] is reflexive, symmetric and transitive.

Theorem 3 implies

Corollary. *Two polynomials $f(x) = x^n - \alpha$ and $g(x) = x^n - \beta$ irreducible over K satisfy $f \sim g$ if and only if either $\beta\alpha^r = \gamma^n$ or $n \equiv 0 \bmod 2^{\tau+1}$, $\alpha = -\delta_1^2$, $\beta = -\delta_2^2$ and $\beta\alpha^r = \left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{n/2}\gamma^n$ with $\gamma, \delta_1, \delta_2 \in K$.*

This is a generalization of Theorem 5 of Gerst [1] corresponding to the case $K = \mathbb{Q}$. (Note that the irreducibility of g implies $(r, n) = 1$.)

For the proof we need several lemmata.

Lemma 1. *If* $(a_i, b_i) = 1$ *and* $b_i \mid m$ $(1 \leqslant i \leqslant k)$ *then*

$$\left(m\frac{a_1}{b_1}, \ldots, m\frac{a_k}{b_k}\right) = m\frac{(a_1, \ldots, a_k)}{[b_1, \ldots, b_k]}.$$

Proof (by induction with respect to k). For $k = 1$ the formula is obvious, for $k = 2$ we have

$$\left(m\frac{a_1}{b_1}, m\frac{a_2}{b_2}\right) = \frac{m}{b_1b_2}(a_1b_2, a_2b_1) = \frac{m}{b_1b_2}(a_1, a_2)(b_1, b_2) = m\frac{(a_1, a_2)}{[b_1, b_2]}.$$

Now assume that the lemma holds for k terms. Then if $b_i \mid m$ $(1 \leqslant i \leqslant k+1)$ we have

$$\left(m\frac{a_1}{b_1}, \ldots, m\frac{a_{k+1}}{b_{k+1}}\right) = \left(m\frac{(a_1, \ldots, a_k)}{[b_1, \ldots, b_k]}, m\frac{a_{k+1}}{b_{k+1}}\right) = m\frac{(a_1, \ldots, a_k, a_{k+1})}{[b_1, \ldots, b_{k+1}]},$$

and the proof is complete. □

Proof of Theorem 1. *Necessity*. Suppose that for a certain prime p, a certain $\gamma \in K$ and some x_i, $\prod_{p \mid n_i} \alpha_i^{x_i} = \gamma^p$, but, for a certain i, $p \mid n_i$, $p \nmid x_i$.

Then for a suitable j

$$\prod_{p \mid n_i} \xi_i^{x_i n_i/p} = \zeta_p^j \gamma, \tag{2}$$

$\zeta_p^j \in K^*\langle \xi_1, \ldots, \xi_k\rangle$ and by Kneser's theorem either $\zeta_p^j \in K$ or $[K(\xi_1, \ldots, \xi_k) : K] < [K^*\langle \xi_1, \ldots, \xi_k\rangle : K^*]$.

In the former case, by (2), $[K^*\langle \xi_1, \ldots, \xi_k\rangle : K^*] < n_1 \cdots n_k$, in both cases $[K(\xi_1, \ldots, \xi_k) : K] < n_1 \cdots n_k$.

Suppose now that, for some x_i and a certain $\gamma \in K$, $\prod_{2 \mid n_i} \alpha_i^{x_i} = -4\gamma^4$, $n_i x_i \equiv 0 \bmod 4$ $(2 \mid n_i)$ but, for a certain i, $2 \mid n_i$, $4 \nmid x_i$. Then for a suitable j

$$\prod_{2 \mid n_i} \xi_i^{x_i n_i/4} = \zeta_4^j (1 + \zeta_4)\gamma, \tag{3}$$

$1 + \zeta_4 \in K\langle \xi_1, \ldots, \xi_k\rangle$ (note that $\zeta_4(1 + \zeta_4) = -2(1 + \zeta_4)^{-1}$) and by Kneser's theorem either $\zeta_4 \in K$ or $[K(\xi_1, \ldots, \xi_k) : K] < [K^*\langle \xi_1, \ldots, \xi_k\rangle : K^*]$.

In the former case by (3) $[K^*\langle \xi_1, \ldots, \xi_k\rangle : K^*] < n_1 \cdots n_k$, in both cases $[K(\xi_1, \ldots, \xi_k) : K] < n_1 n_2 \cdots n_k$.

Sufficiency. Suppose that for a certain prime p and a $\gamma \in K$

$$\zeta_p = \gamma \prod_{i=1}^{k} \xi_i^{x_i}.$$

Let $m = [n_1/(n_1, x_1), \ldots, n_k/(n_k, x_k)]$. If $p \mid m$ we get

$$\prod_{i=1}^{k} \alpha_i^{mx_i/n_i} = \left(\gamma^{-m/p}\right)^p$$

and by the assumption $mx_i/n_i \equiv 0 \bmod p$ $(1 \leqslant i \leqslant k)$. This gives by Lemma 1 $\left(x_1/(n_1, x_1), \ldots, x_k/(n_k, x_k)\right) \equiv 0 \bmod p$, and for an $i \leqslant k$:

$$\frac{x_i}{(n_i, x_i)} \equiv \frac{n_i}{(n_i, x_i)} \equiv 0 \bmod p,$$

a contradiction.

If $p \nmid m$ we have

$$\zeta_p^m = \gamma^m \prod_{i=1}^{k} \alpha_i^{mx_i/n_i} \in K, \quad \zeta_p \in K.$$

Suppose now that for a $\gamma \in K$

$$1 + \zeta_4 = \gamma \prod_{i=1}^{k} \xi_i^{x_i} \tag{4}$$

and again $m = [n_1/(n_1, x_1), \ldots, n_k/(n_k, x_k)]$. If $4 \mid m$ then

$$(-4)^{m/4} = \gamma^m \prod_{i=1}^{k} \alpha_i^{x_i m/n_i}$$

and by the assumption $x_i m/n_i \equiv 0 \bmod 2$ $(1 \leqslant i \leqslant k)$. This gives by Lemma 1 $\left(x_1/(n_1, x_1), \ldots, x_k/(n_k, x_k)\right) \equiv 0 \bmod 2$ and for an $i \leqslant k$:

$$\frac{x_i}{(n_i, x_i)} \equiv \frac{n_i}{(n_i, x_i)} \equiv 0 \bmod 2,$$

a contradiction.

If $4 \nmid m$ then (4) gives

$$(2\zeta_4)^{m/(2,m)} = \gamma^{[m,2]} \prod_{i=1}^{k} \alpha_i^{[m,2]x_i/n_i} \in K; \quad \zeta_4 \in K.$$

Thus by Kneser's theorem $[K(\xi_1, \ldots, \xi_k) : K] = [K^* \langle \xi_1, \ldots, \xi_k \rangle : K^*]$. Suppose now that

$$\prod_{i=1}^{k} \xi_i^{x_i} = \gamma \in K \quad \text{and} \quad m = [n_1/(n_1, x_1), \ldots, n_k/(n_k, x_k)] \neq 1.$$

Then for a certain prime p, $p \mid m$ and

$$\prod_{i=1}^{k} \alpha_i^{x_i m/n_i} = \left(\gamma^{m/p}\right)^p$$

thus by the assumption $mx_i/n_i \equiv 0 \bmod p$ $(1 \leqslant i \leqslant k)$. This as before leads to a contradiction. Therefore $m = 1$, $x_i \equiv 0 \bmod n_i$ and we infer that $[K^* \langle \xi_1, \ldots, \xi_k \rangle : K^*] = n_1 \cdots n_k$, which completes the proof. □

Lemma 2. *Let g be 0 or a power of 2, $\mathscr{G}$ a subgroup of K^* containing K^{*g}. If $n_i x_i \equiv 0 \bmod g$ $(1 \leqslant i \leqslant k)$ implies $-\prod_{i=1}^{k} \alpha_i^{x_i} \notin \mathscr{G}$ then there exist elements $\xi_1, \ldots, \xi_k, \eta_1, \ldots, \eta_l$ and positive integers $m_1, \ldots, m_l$ such that*

$$\xi_i^{n_i} = \alpha_i \ (1 \leqslant i \leqslant k), \quad \eta_j^{m_j} = \beta_j \in K^* \ (1 \leqslant j \leqslant l),$$

$$\langle \xi_1, \ldots, \xi_k \rangle = \langle \eta_1, \ldots, \eta_l \rangle,$$

$$[m_1, \ldots, m_l] \,|\, [n_1, \ldots, n_k], \tag{5}$$

$$\prod_{p \mid m_j} \beta_j^{x_j} = \gamma^p \quad \textit{implies} \quad x_j \equiv 0 \bmod p \quad (p \mid m_j) \tag{6}$$

for all primes p and

$$m_j y_j \equiv 0 \bmod g \ (1 \leqslant j \leqslant l) \quad \textit{implies} \quad -\prod_{j=1}^{l} \beta_j^{y_j} \notin \mathscr{G} \ (^2). \tag{7}$$

Proof. Assume first that all n_i are powers of the same prime q. Consider all systems $\eta_1, \ldots, \eta_k, m_1, \ldots, m_k$ satisfying the following conditions: for suitable ξ_i and integral e_{ij}

$$\xi_i^{n_i} = \alpha_i, \quad \xi_i = \prod_{j=1}^{k} \eta_j^{e_{ij}}, \quad \eta_j^{m_j} = \beta_j \in K^*;$$

$$\det[e_{ij}] = \pm 1, \quad m_j \mid n_i e_{ij} \tag{8}$$

and

$$m_j y_j \equiv 0 \bmod g \ (1 \leqslant j \leqslant k) \quad \text{implies} \quad -\prod_{j=1}^{k} \beta_j^{y_j} \notin \mathscr{G}. \tag{9}$$

Such systems do exist, e.g. $\eta_j = \xi_j$, where $\xi_j^{n_j} = \alpha_j$, $m_j = n_j$; we take one with the least product $m_1 \cdots m_k$ and assert that it has the required property. We note that by (8)

$$m_j \,\Big|\, \sum_{i=1}^{k} \frac{\max\limits_{1 \leqslant i \leqslant k} n_i}{n_i} n_i e_{ij} E_{ij} = \pm \max_{1 \leqslant i \leqslant k} n_i,$$

E_{ij} being the algebraic complement of e_{ij}, hence (5) holds and each m_j is a power of q. We can assume without loss of generality that $m_1 \geqslant m_2 \geqslant \ldots \geqslant m_k$. The only prime p for which (6) needs verification is $p = q$.

---

(2) $a \equiv 0 \bmod 0$ means $a = 0$.

Suppose that $\prod_{p\mid m_j} \beta_j^{x_j} = \gamma^p$ but for some j $p \mid m_j$, $p \nmid x_j$. Let s be the greatest such j and let t satisfy the congruence

$$tx_s \equiv 1 \bmod p.$$

Then

$$\prod_{j=1}^{s-1} \beta_j^{tx_j} \cdot \beta_s = \delta^p. \tag{10}$$

Consider first the case $p = q = 2$. If $m_s \equiv 0 \bmod 2g$ there exists an $\varepsilon = \pm 1$ such that for every choice of z_j satisfying $z_s \equiv 1 \bmod 2$, $m_j z_j \equiv 0 \bmod g$ $(j > s)$ we have

$$-(\varepsilon\delta)^{z_s} \prod_{j\neq s} \beta_j^{z_j} \notin \mathscr{G}.$$

Indeed if

$$z_s \equiv 1 \bmod 2, \quad m_j z_j \equiv 0 \bmod g \ (j > s), \quad -\delta^{z_s} \prod_{j\neq s} \beta_j^{z_j} \in \mathscr{G}$$

and

$$z_s' \equiv 1 \bmod 2, \quad m_j z_j' \equiv 0 \bmod g \ (j > s), \quad -(-\delta)^{z_s'} \prod_{j\neq s} \beta_j^{z_j'} \in \mathscr{G}$$

then

$$z_s - z_s' \equiv 0 \bmod 2, \quad -\delta^{z_s - z_s'} \prod_{j\neq s} \beta_j^{z_j - z_j'} \in \mathscr{G}$$

and by (10)

$$-\prod_{j=1}^{s-1} \beta_j^{tx_j(z_s - z_s')/2 + z_j - z_j'} \beta_s^{(z_s - z_s')/2} \prod_{j=s+1}^{k} \beta_j^{z_j - z_j'} \in \mathscr{G}$$

which contradicts (9) since

$$m_j \equiv 0 \bmod g \ (j \leqslant s), \quad m_j(z_j - z_j') \equiv 0 \bmod g \ (j > s).$$

Let us choose a root of unity $\zeta_{m_s}^r$ so that

$$\eta_s' = \zeta_{m_s}^r \eta_s \prod_{j=1}^{s-1} \eta_j^{tx_j m_j/m_s}$$

satisfies

$$\eta_s'^{m_s/2} = \beta_s' = \begin{cases} \delta & \text{if } m_s \not\equiv 0 \bmod 2g, \\ \varepsilon\delta & \text{otherwise,} \end{cases} \tag{11}$$

and set $m'_s = m_s/2$,

$$\eta'_j = \eta_j, \quad m'_j = m_j, \quad \beta'_j = \beta_j \quad (j \neq s); \tag{12}$$

$$e'_{ij} = \begin{cases} e_{ij} - e_{is} t x_j \dfrac{m_j}{m_s} & \text{if } j < s, \\ e_{ij} & \text{if } j \geqslant s; \end{cases} \tag{13}$$

$$\xi'_i = \prod_{j=1}^{k} \eta_j'^{e'_{ij}}. \tag{14}$$

We find

$$\xi'_i = \xi_i \zeta_{m_s}^{r e_{is}} \quad \text{and} \quad \xi_i'^{n_i} = \alpha_i \quad (1 \leqslant i \leqslant k)$$

because of (8).

The conditions $\det[e'_{ij}] = \pm 1$ and $m'_j \mid n_i e'_{ij}$ follow also from (8) since by (13)

$$[e'_{ij}] = [e_{ij}] \begin{bmatrix} 1 & 0 & \dots & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \ddots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 & \dots & 0 & 0 \\ -t x_1 \dfrac{m_1}{m_s} & -t x_2 \dfrac{m_2}{m_s} & \dots & -t x_{s-1} \dfrac{m_{s-1}}{m_s} & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \ddots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 & 1 \end{bmatrix},$$

$\det[e'_{ij}] = \det[e_{ij}]$ and $m_j \mid n_i e'_{ij}$.

Finally suppose that $m'_j y_j \equiv 0 \bmod g$ $(1 \leqslant j \leqslant k)$ and $-\prod_{j=1}^{k} \beta_j'^{y_j} \in \mathscr{G}$.

If $y_s \equiv 0 \bmod 2$ we have by (10), (11) and (12)

$$-\prod_{j=1}^{s-1} \beta_j^{t x_j y_s/2 + y_j} \beta_s^{y_s/2} \prod_{j=s+1}^{k} \beta_j^{y_j} \in \mathscr{G}$$

which contradicts (9) since

$$m_j \frac{y_s}{2} = \frac{m_j}{m_s} m'_s y_s \equiv 0 \bmod g \ (j \leqslant s) \quad \text{and} \quad m_j y_j \equiv 0 \bmod g \ (j > s).$$

If $y_s \equiv 1 \bmod 2$ we have $m_s \equiv 0 \bmod 2g$ and by (11) and (12)

$$-(\varepsilon\delta)^{y_s} \prod_{j \neq s} \beta_j^{y_j} \in \mathscr{G}$$

contrary to the choice of ε.

Thus $\eta'_1, \dots, \eta'_k, m'_1, \dots, m'_k$ satisfy all conditions imposed on $\eta_1, \dots, \eta_k, m_1, \dots, m_k$ and $m'_1 \cdots m'_k < m_1 \cdots m_k$, a contradiction.

Consider next the case $p = q > 2$. Let us choose a root of unity $\zeta_{m_s}^r$ so that

$$\eta_s' = \zeta_{m_s}^r \eta_s \prod_{j=1}^{s-1} \eta_j^{t x_j m_j/m_s} \quad \text{satisfies} \quad \eta_s'^{m_s/p} = \delta.$$

Set $m_s' = m_s/p$ and define η_j', m_j' $(j \neq s)$, e_{ij}', ξ_i' by the formulae (12), (13), (14). We find as before that $\xi_i'^{n_i} = \alpha_i$ $(1 \leqslant i \leqslant k)$, $\det[e_{ij}'] = \pm 1$ and $m_j' \mid n_i e_{ij}'$. If now $m_j' y_j \equiv 0 \bmod g$ $(1 \leqslant j \leqslant k)$ then $y_j \equiv 0 \bmod g$ $(1 \leqslant j \leqslant k)$ and since $K^{*g} \subset \mathscr{G}$, $-\prod_{j=1}^{k} \beta_j'^{y_j} \in \mathscr{G}$ implies $-1 \in \mathscr{G}$ which is impossible by (9). Since $m_1' \cdots m_k' < m_1 \cdots m_k$ we get a contradiction.

Consider now the general case. Let $n_i = \prod_{h=1}^{H} p_h^{r_{hi}}$ $(1 \leqslant i \leqslant k)$, where $p_1, \ldots, p_H$ are distinct primes. By the already proved case of the lemma for each $h \leqslant H$ there exist ξ_{hi}, η_{hi} and m_{hi} $(1 \leqslant i \leqslant k)$ such that

$$\xi_{hi}^{p_h^{r_{hi}}} = \alpha_i, \quad \eta_{hi}^{m_{hi}} = \beta_{hi},$$

$$\langle \xi_{h1}, \ldots, \xi_{hk} \rangle = \langle \eta_{h1}, \ldots, \eta_{hk} \rangle,$$

$$[m_{h1}, \ldots, m_{hk}] \mid p_h^{\max r_{hi}}, \tag{15}$$

$$\prod_{p_h \mid m_{hi}} \beta_{hi}^{x_i} = \gamma^{p_h} \quad \text{implies} \quad x_i \equiv 0 \bmod p_h \ (p_h \mid m_{hi}) \tag{16}$$

and

$$m_h y_i \equiv 0 \bmod g \quad \text{implies} \quad -\prod_{i=1}^{k} \beta_{hi}^{y_i} \notin \mathscr{G}. \tag{17}$$

We get

$$\langle \eta_{11}, \ldots, \eta_{1k}, \eta_{21}, \ldots, \eta_{2k}, \ldots, \eta_{H1}, \ldots, \eta_{Hk} \rangle = \langle \xi_{11}, \ldots, \xi_{1k}, \xi_{21}, \ldots, \xi_{2k}, \ldots, \xi_{H1}, \ldots, \xi_{Hk} \rangle,$$

$$[m_{11}, \ldots, m_{1k}, m_{21}, \ldots, m_{2k}, \ldots, m_{H1}, \ldots, m_{Hk}] \mid [n_1, \ldots, n_k].$$

Let us choose integers t_{hi} so that $\dfrac{1}{n_i} = \sum_{h=1}^{H} \dfrac{t_{hi}}{p_h^{r_{hi}}}$. Then

$$\Big(\prod_{h=1}^{H} \xi_{hi}^{t_{hi}}\Big)^{n_i} = \alpha_i, \quad \xi_{ji} = \Big(\prod_{h=1}^{H} \xi_{hi}^{t_{hi}}\Big)^{n_i/p_j^{r_{ji}}} \quad (1 \leqslant i \leqslant k),$$

hence

$$\langle \eta_1, \ldots, \eta_{Hk} \rangle = \Big\langle \prod_{h=1}^{H} \xi_{h1}^{t_{h1}}, \ldots, \prod_{h=1}^{H} \xi_{hk}^{t_{hk}} \Big\rangle.$$

Moreover

$$\prod_{p\mid m_h} \beta_{hi}^{x_{hi}} = \gamma^p$$

implies by (15) and (16) $x_{hi} \equiv 0 \bmod p$ $(p \mid m_{hi})$. Finally $m_{hi} y_{hi} \equiv 0 \bmod g$ implies $y_{hi} \equiv 0 \bmod g$ unless $p_h = 2$. Since $\mathscr{G} \supset K^{*g}$ the conditions

$$m_{hi} y_{hi} \equiv 0 \bmod g \ (1 \leqslant h \leqslant H,\ 1 \leqslant i \leqslant k) \quad \text{and} \quad -\prod_{h=1}^{H} \prod_{i=1}^{k} \beta_{hi}^{y_{hi}} \in \mathscr{G}$$

imply for $p_h = 2$

$$-\prod_{i=1}^{k} \beta_{hi}^{y_{hi}} \in \mathscr{G}$$

which contradicts (17). The proof is complete. □

Remark. It is possible but not worthwhile to obtain $l = k$ in the general case.

Proof of Theorem 2. We apply Lemma 2 with $g = 0$, $\mathscr{G} = \{1\}$ if $\zeta_4 \in K$; with $g = 4$, $\mathscr{G} = K^{*4} \cup 4K^{*4}$ otherwise and find that for suitable $\xi_1, \ldots, \xi_k, \eta_1, \ldots, \eta_l$

$$\xi_i^{n_i} = \alpha_i, \quad \eta_j^{m_j} = \beta_j \quad (1 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant l), \qquad \langle \xi_1, \ldots, \xi_k \rangle = \langle \eta_1, \ldots, \eta_l \rangle,$$

$$\prod_{p\mid m_j} \beta_j^{x_j} = \gamma^p \quad \text{implies} \quad x_j \equiv 0 \bmod p \ (p \mid m_j) \tag{18}$$

and if $\zeta_4 \notin K$

$$m_j y_j \equiv 0 \bmod 4 \ (1 \leqslant j \leqslant k) \quad \text{implies} \quad \prod_{j=1}^{k} \beta_j^{y_j} \neq -\gamma^4, -4\gamma^4.$$

If $\zeta_4 \notin K$ we see at once that the conditions of Theorem 1 are satisfied; if $\zeta_4 \in K$ they are also satisfied since then by (18)

$$\prod_{2\mid n_i} \beta_i^{x_i} = -4\gamma^4,\ n_i x_i \equiv 0 \bmod 4 \ (2 \mid n_i) \quad \text{implies} \quad \prod_{2\mid n_i} \beta_i^{x_i} = (2\zeta_4 \gamma^2)^2,$$

$x_i \equiv 0 \bmod 2$, $\prod_{2\mid n_i} \beta_i^{x_i/2} = \pm 2\zeta_4 \gamma^2 = \big((1 \pm \zeta_4)\gamma\big)^2$, $x_i/2 \equiv 0 \bmod 2$, $x_i \equiv 0 \bmod 4$ $(1 \leqslant i \leqslant k)$.

By Theorem 1 we have $[K(\eta_1, \ldots, \eta_l) : K] = m_1 \cdots m_l = [K^* \langle \eta_1, \ldots, \eta_l \rangle : K^*]$, hence the theorem. □

Lemma 3. *If $n_1, \ldots, n_l, m_1, \ldots, m_l$ satisfy the conditions of Lemma 2 with $g = 2$, $\mathscr{G} = K^{*2}$; $\delta \in K^*$ and $\sqrt{\delta} \in K(\eta_1, \ldots, \eta_l)$ then*

$$\sqrt{\delta} \in K^* \langle \eta_1, \ldots, \eta_l \rangle \quad \textit{and} \quad \delta \neq -1.$$

Proof. If $\sqrt{\delta} \in K(\eta_1, \ldots, \eta_l)$ but $\sqrt{\delta} \notin K^* \langle \eta_1, \ldots, \eta_l \rangle$ then

$$[K^*\langle\sqrt{\delta}, \eta_1, \ldots, \eta_l\rangle : K^*] > [K^* \langle \eta_1, \ldots, \eta_l \rangle : K^*]$$
$$\geqslant [K(\eta_1, \ldots, \eta_l) : K] = [K\big(\sqrt{\delta}, \eta_1, \ldots, \eta_l\big) : K]$$

thus by Kneser's theorem we have for a certain prime p

$$\zeta_p \in K^*\langle\sqrt{\delta}, \eta_1, \ldots, \eta_l\rangle, \quad \zeta_p \notin K,$$

or

$$1 + \zeta_4 \in K^*\langle\sqrt{\delta}, \eta_1, \ldots, \eta_l\rangle, \quad \zeta_4 \notin K.$$

However $\zeta_p = \gamma\sqrt{\delta^{x_0}} \prod_{j=1}^{l} \eta_j^{x_j}$, $\gamma \in K$, gives

$$\sqrt{\delta} \in K^* \langle \eta_1, \ldots, \eta_l \rangle$$

unless $x_0 \equiv 0 \bmod 2$. In the latter case let

$$m = [m_1/(m_1, x_1), \ldots, m_l/(m_l, x_l)].$$

If $p \mid m$ we get

$$\prod_{j=1}^{l} \beta_j^{mx_j/m_j} = \big(\gamma^{-m/p}\delta^{-(m/p)(x_0/2)}\big)^p$$

and by the assumption

$$\frac{mx_j}{m_j} \equiv 0 \bmod p \ (1 \leqslant j \leqslant l).$$

This gives by Lemma 1 $\big(x_1/(m_1, x_1), \ldots, x_l/(m_l, x_l)\big) \equiv 0 \bmod p$ and, for a $j \leqslant l$, $x_j/(m_j, x_j) \equiv m_j/(m_j, x_j) \equiv 0 \bmod p$, a contradiction.

If $p \nmid m$ we have

$$\zeta_p^m = \big(\gamma\delta^{x_0/2}\big)^m \prod_{j=1}^{l} \beta_j^{mx_j/m_j} \in K; \quad \zeta_p \in K.$$

Suppose now that $\gamma \in K$,

$$1 + \zeta_4 = \gamma\sqrt{\delta^{x_0}} \prod_{j=1}^{l} \eta_j^{x_j} \quad \text{or} \quad \zeta_4 = \gamma \prod_{j=1}^{l} \eta_j^{x_j} \tag{19}$$

and set again $m = [m_1/(m_1, x_1), \ldots, m_l/(m_l, x_l)]$.

If $4 \mid m$ then

$$(-4)^{m/4} = \gamma^m \delta^{x_0 m/2} \prod_{j=1}^{l} \beta_j^{x_j m/m_j} \quad \text{or} \quad 1 = \gamma^m \prod_{j=1}^{l} \beta_j^{x_j m/m_j}$$

and by the assumption $x_j m/m_j \equiv 0 \,(\mathrm{mod}\, 2)$ $(1 \leqslant j \leqslant l)$. This gives by Lemma 1

$\big(x_1/(m_1, x_1), \ldots, x_l/(m_l, x_l)\big) \equiv 0 \bmod 2$ and for a $j \leqslant l$

$$\frac{x_j}{(m_j, x_j)} \equiv \frac{m_j}{(m_j, x_j)} \equiv 0 \bmod 2,$$

a contradiction.

If $4 \nmid m$ then (19) gives

$$(2\zeta_4)^{m/(m,2)} = \gamma^{[m,2]}\delta^{x_0 m/(m,2)} \prod_{j=1}^{l} \beta_j^{x_j[m,2]/m_j} \in K; \quad \zeta_4 \in K,$$

or

$$(-1)^{m/(m,2)} = \gamma^{[m,2]} \prod_{j=1}^{l} \beta_j^{x_j[m,2]/m_j}; \quad \prod_{2|m_j} \beta_j^{x_j[m,2]/m_j} = -\delta_1^2.$$

The contradiction obtained completes the proof. □

Lemma 4. *Let K be an arbitrary field, n a positive integer not divisible by the characteristic of K, m_j divisors of n and $\beta_1, \ldots, \beta_l, \beta$ non-zero elements of K. If each of the fields $K(\eta_1, \ldots, \eta_l)$, where $\eta_j^{m_j} = \beta_j$ $(1 \leqslant j \leqslant l)$ contains at least one η with $\eta^n = \beta$ then for any choice of η_j and η and for suitable exponents $r_0, r_1, \ldots, r_l$*

$$\zeta_n^{r_0}\eta\eta_1^{r_1}\cdots\eta_l^{r_l} \in K(\zeta_4).$$

Proof. This is an immediate consequence of Lemma 6 of [6]. □

Lemma 5. *Let K be an arbitrary field of characteristic different from 2 and τ be defined as in Theorem 3. $\Theta \in K$ is of the form ϑ^n, where $\vartheta \in K(\zeta_4)$ if and only if at least one of the following three conditions is satisfied for a suitable $\gamma \in K$:*

$$\Theta = \gamma^n,$$

$$n \not\equiv 0 \bmod 2^\tau, \quad \Theta = -\gamma^n,$$

$$n \equiv 0 \bmod 2^\tau, \quad \Theta = (-1)^{n/2^\tau}\big(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\big)^{n/2}\gamma^n.$$

If $\zeta_4 \in K$ the last two conditions imply the first.

Proof. Necessity follows at once from Lemma 7 of [6]. Sufficiency of the first condition is obvious. In order to prove sufficiency of the other two note that if $n \not\equiv 0 \bmod 2^\tau$ and $qn \equiv 2^{\tau-1} \bmod 2^\tau$ then

$$-1 = \big(\zeta_{2^\tau}^q\big)^n$$

and if $n \equiv 0 \bmod 2^\tau$ then

$$(-1)^{n/2^\tau}\big(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\big)^{n/2} = \big(\zeta_{2^\tau} + 1\big)^n.$$

On the other hand since $\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} \in K$,

$$\zeta_{2^\tau} = \tfrac{1}{2}\big(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1}\big) \pm \tfrac{1}{2}\zeta_4\big(\zeta_{2^\tau}^{1-2^{\tau-2}} + \zeta_{2^\tau}^{-1+2^{\tau-2}}\big) \in K(\zeta_4).$$

The last assertion of the lemma is obvious. □

Proof of Theorem 3. Let us assume first that for all l_i

$$\prod_{2|n_i} \alpha_i^{l_i} \neq -\delta^2. \tag{20}$$

Then by Lemma 2 applied with $g = 2$, $\mathscr{G} = K^{*2}$ there exist $\xi_1, \ldots, \xi_k$, $\eta_1, \ldots, \eta_l$, $m_1, \ldots, m_l$ such that

$$\xi_i^{n_i} = \alpha_i \ (1 \leqslant i \leqslant k), \quad \eta_j^{m_j} = \beta_j \in K \ (1 \leqslant j \leqslant l),$$

$$\langle \xi_1, \ldots, \xi_k \rangle = \langle \eta_1, \ldots, \eta_l \rangle, \tag{21}$$

$$[m_1, \ldots, m_l] \,|\, [n_1, \ldots, n_k], \tag{22}$$

$$\prod_{p|m_j} \beta_j^{x_j} = \gamma^p \quad \text{implies} \quad p \,|\, x_j \ (p \,|\, m_j)$$

for all primes p and

$$\prod_{2|m_j} \beta_j^{y_j} \neq -\gamma^2 \quad \text{for any choice of } y_j. \tag{23}$$

By Theorem 1 $[K(\eta_1, \ldots, \eta_l) : K] = m_1 \cdots m_l$ and thus all fields $K(\eta_1, \ldots, \eta_l)$, where $\eta_j^{m_j} = \beta_j$ are conjugate over K. If now $K(\xi_1, \ldots, \xi_k) = K(\eta_1, \ldots, \eta_l)$ contains an η with $\eta^n = \beta$ then each field $K(\eta_1, \ldots, \eta_l)$ contains such an η and by Lemma 4, Lemma 5, (22) and (23) we have either

$$\beta \prod_{j=1}^{l} \beta_j^{r_j n/m_j} = \gamma^n \tag{24}$$

or

$$n \equiv 0 \bmod 2^{\tau+1} \quad \text{and} \quad \beta \prod_{j=1}^{l} \beta_j^{r_j n/m_j} = \left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{n/2} \gamma^n \tag{25}$$

for suitable integers $r_1, \ldots, r_l$ and a suitable $\gamma \in K$. Indeed, if $n \equiv 0 \bmod 2$, $\beta \prod_{j=1}^{l} \beta_j^{r_j n/m_j} = -\gamma^n$, or $n \equiv 2^\tau \bmod 2^{\tau+1}$, $\beta \prod_{j=1}^{l} \beta_j^{r_j n/m_j} = -\left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{n/2} \gamma^n$, we get on taking square roots $\zeta_4 \in K(\eta, \eta_1, \ldots, \eta_l) = K(\eta_1, \ldots, \eta_l)$ contrary to Lemma 3.

The condition (21) implies that

$$\prod_{j=1}^{l} \beta_j^{r_j n/m_j} = \prod_{i=1}^{k} \alpha_i^{q_i n/n_i} \tag{26}$$

for suitable integers $q_1, \ldots, q_k$. Hence (24) leads to (i).

It remains to consider (25). If $L = K(\eta_1, \ldots, \eta_l)$ contains an η with $\eta^n = \beta$ then by (25) it contains $\zeta_n^r \sqrt{\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2}$ for a certain r.

If $n/(n, 2r) \equiv 1 \bmod 2$ then L contains

$$\zeta_n^{rn/(n,2r)} \sqrt{\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2} = \pm \sqrt{\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2}\,;$$

if $n/(n,2r) \equiv 2 \bmod 4$ then L contains

$$\zeta_n^{rn/2(n,2r)}\sqrt{\zeta_{2^\tau}+\zeta_{2^\tau}^{-1}+2} = \pm\sqrt{-\left(\zeta_{2^\tau}+\zeta_{2^\tau}^{-1}+2\right)};$$

if $n/(n,2r) \equiv 0 \bmod 4$ then L contains $\zeta_n^{rn/2(n,2r)} = \pm\zeta_4$.

By Lemma 3 the last case is impossible and in the first two cases

$$\sqrt{\pm\left(\zeta_{2^\tau}+\zeta_{2^\tau}^{-1}+2\right)} \in K^*\langle\eta_1,\ldots,\eta_l\rangle = K^*\langle\xi_1,\ldots,\xi_k\rangle.$$

Hence we obtain

$$\left(\zeta_{2^\tau}+\zeta_{2^\tau}^{-1}+2\right)^{n/2} = \vartheta^n\prod_{i=1}^{k}\alpha_i^{s_i n/n_i}, \quad \vartheta \in K,$$

which together with (25) and (26) gives again (i).

Assume now that for some $l_1,\ldots,l_k$

$$\prod_{2\mid n_i}\alpha_i^{l_i} = -\delta^2, \quad \delta \in K.$$

Then we apply Lemma 2 for the field $K(\zeta_4)$ with $g=0, \mathscr{G}=\{1\}$ and we infer the existence of $\xi_1,\ldots,\xi_k,\eta_1,\ldots,\eta_l,m_1,\ldots,m_l$ such that

$$\begin{gathered}\xi_i^{n_i} = \alpha_i\ (1\leqslant i\leqslant k), \quad \eta_j^{m_j} = \beta_j \in K(\zeta_4)\ (1\leqslant j\leqslant l),\\ \langle\xi_1,\ldots,\xi_k\rangle = \langle\eta_1,\ldots,\eta_l\rangle,\\ [m_1,\ldots,m_l]\,|\,[n_1,\ldots,n_k],\\ \prod_{p\mid m_j}\beta_j^{x_j} = \gamma^p,\ \gamma\in K(\zeta_4) \quad \text{implies} \quad p\,|\,x_j\ (p\,|\,m_j)\end{gathered} \tag{27}$$

for all primes p.

By Theorem 1 $\left[K(\zeta_4,\eta_1,\ldots,\eta_l) : K(\zeta_4)\right] = m_1\cdots m_l$ (see the end of the proof of Theorem 2) and thus all fields $K(\zeta_4,\eta_1,\ldots,\eta_l)$, where $\eta_j^{m_j} = \beta_j$, are conjugate over $K(\zeta_4)$.

If now $K(\xi_1,\ldots,\xi_k)\subset K(\zeta_4,\eta_1,\ldots,\eta_l)$ contains an η with $\eta^n=\beta$ then each field $K(\zeta_4,\overline{\eta}_1,\ldots,\overline{\eta}_l)$ contains such an η and by Lemma 4 we have

$$\beta\prod_{j=1}^{l}\beta_j^{r_j n/m_j} = \vartheta^n, \quad \vartheta\in K(\zeta_4).$$

The condition (27) implies that

$$\prod_{j=1}^{l}\beta_j^{r_j n/m_j} = \prod_{i=1}^{k}\alpha_i^{q_i n/n_i}$$

for suitable integers $q_1,\ldots,q_k$. Hence $\vartheta^n\in K$ and using Lemma 5 we get one of the cases (i)–(iii).

Conversely if (i) is satisfied then any field $K(\xi_1, \dots, \xi_k)$, where $\xi_i^{n_i} = \alpha_i$ $(1 \leqslant i \leqslant k)$, contains $\eta = \gamma \prod_{i=1}^{k} \xi_i^{-q_i}$ with $\eta^n = \beta$.

If (ii) or (iii) is satisfied then by Lemma 5

$$\beta \prod_{i=1}^{k} \alpha_i^{q_i n/n_i} = \vartheta^n$$

where $\vartheta \in K(\zeta_4)$. On the other hand, the equality $\prod_{2|n_i} \alpha_i^{l_i} = -\delta^2$ implies $\zeta_4 = \pm \prod_{2|n_i} \xi_i^{n_i l_i/2} \delta^{-1}$.

Thus $\vartheta \in K(\xi_1, \dots, \xi_k)$ and $K(\xi_1, \dots, \xi_k)$ contains $\eta = \vartheta \prod_{i=1}^{k} \xi_i^{-q_i}$ with $\eta^n = \beta$.

The last assertion of the Theorem if $\zeta_4 \in K$ follows from the last assertion of Lemma 5.

If $\tau = 2$ and $n \not\equiv 0 \bmod 2^\tau$ we have either $n \equiv 1 \bmod 2$, in which case $-\gamma^n = (-\gamma)^n$, or $n \equiv 2 \bmod 4$. In the latter case we get from (ii)

$$\beta \prod_{i=1}^{k} \alpha_i^{q_i n/n_i} \prod_{2|n_i} \alpha_i^{l_i n/2} = (\gamma\delta)^n$$

which leads to (i). The proof is complete. □

Proof of Corollary. If the irreducible polynomials $f(x) = x^n - \alpha$ and $g(x) = x^n - \beta$ satisfy the relation $f \sim g$ we have by Theorem 3 the following five possibilities

$$\alpha \overset{n}{=} \beta^t, \quad \beta \overset{n}{=} \alpha^s; \tag{28}$$

$$n \not\equiv 0 \bmod 2^\tau, \quad \alpha = -\delta^2 \overset{n}{=} \beta^t, \quad \beta \overset{n}{=} -\alpha^s; \tag{29}$$

$$n \equiv 0 \bmod 2^\tau, \quad \alpha = -\delta^2 \overset{n}{=} \beta^t, \quad \beta \overset{n}{=} \varepsilon\omega\alpha^s; \tag{30}$$

$$n \not\equiv 0 \bmod 2^\tau, \quad \alpha = -\delta_1^2 \overset{n}{=} -\beta^t, \quad \beta = -\delta_2^2 \overset{n}{=} \alpha^s; \tag{31}$$

$$n \equiv 0 \bmod 2^\tau, \quad \alpha = -\delta_1^2 \overset{n}{=} \varepsilon\omega\beta^t, \quad \beta = -\delta_2^2 \overset{n}{=} \varepsilon\omega\alpha^s, \tag{32}$$

and two other possibilities obtained by the permutation of α and β in (29) and (30). Here $\gamma \overset{n}{=} \delta$ means that γ/δ is an nth power in K, $\varepsilon = (-1)^{n/2^\tau}$ and $\omega = \left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{n/2}$.

Moreover in (29) to (32) it is assumed that $n \equiv 0 \bmod 2$, $\zeta_4 \notin K$. Now, (29) gives $t \equiv 1 \bmod 2$, $\alpha \overset{n}{=} -\alpha^{st}$, $\alpha^{st-1} \overset{n}{=} -1$, $\beta \overset{n}{=} \alpha^{s+st-1}$.

(30) gives $t \equiv 1 \bmod 2$, $\alpha \overset{n}{=} \varepsilon\omega\alpha^{st}$, $\alpha^{st-1} \overset{n}{=} \varepsilon\omega$, $\beta \overset{n}{=} \alpha^{s+st-1}$.

(31) gives $s \equiv t \equiv 0 \bmod 2$. Indeed, if for instance $t \equiv 1 \bmod 2$ then

$$-\delta_1^2 \overset{n}{=} -\beta^t \overset{n}{=} \delta_2^{2t} \quad \text{and} \quad \zeta_4 \in K.$$

If $s \equiv t \equiv 0 \bmod 2$ then

$$\alpha \overset{n}{=} -\alpha^{st}, \quad \alpha^{st-1} \overset{n}{=} -1, \quad \beta \overset{n}{=} \alpha^{s+st-1}.$$

(32) with $\varepsilon = -1$ gives like (31) that $s \equiv t \equiv 0 \bmod 2$. In that case

$$\alpha \overset{n}{=} -\omega\alpha^{st}, \quad \alpha^{st-1} \overset{n}{=} -\omega, \quad \beta \overset{n}{=} \alpha^{s+st-1}.$$

Thus in any case we have either $\beta \overset{n}{=} \alpha^r$ or $n \equiv 0 \bmod 2^{\tau+1}$, $\alpha = -\delta^2$, $\beta = \omega\alpha^r$. On the other hand if at least one of these conditions is satisfied then by Theorem 3 each of the fields $K(\xi)$ with $f(\eta) = 0$ contains an η with $g(\eta) = 0$ and since f and g are irreducible and of the same degree $K(\xi) = K(\eta)$.

Note added in proof. Theorem 3 is incompatible with Theorem 2 of [4a], p. 63. However already the special case of the latter theorem given by Nagell as his Theorem 3 is not valid in general, as shown by the example $\Omega = \mathbb{Q}$, $n = 8$, $a = -1$, $b = -16$ contained in Theorem 6 of Gerst [1].

References

[1] I. Gerst, *On the theory of n-th power residues and a conjecture of Kronecker*. Acta Arith. 17 (1970), 121–139.

[2] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil II: *Reziprozitätsgesetz*. Physica-Verlag, Würzburg–Wien 1965.

[3] M. Kneser, *Lineare Abhängigkeit von Wurzeln*. Acta Arith. 26 (1975), 307–308.

[4] L. J. Mordell, *On the linear independence of algebraic numbers*. Pacific J. Math. 3 (1953), 625–630.

[4a] T. Nagell, *Bestimmung des Grades gewisser relativ-algebraischen Zahlen*. Monatsh. Math. Phys. 48 (1939), 61–74.

[5] L. Rédei, *Algebra* I. Akadémiai Kiadó, Budapest 1967.

[6] A. Schinzel, *On power residues and exponential congruences*, Acta Arith. 27 (1975), 397–420; this collection: H4, 915–938.

[7] C. L. Siegel, *Algebraische Abhängigkeit von Wurzeln*. Acta Arith. 21 (1972), 59–64.

Andrzej Schinzel
Selecta

Originally published in
Journal für die reine und angewandte Mathematik
331 (1982), 104–113

On Sylow 2-subgroups of K_2O_F for quadratic number fields F

with J. Browkin (*Warsaw*)

1. Introduction

Let O_F be the ring of integers of a number field F. For a finite abelian group A denote by A_2 its Sylow 2-subgroup, and by $r_2(A)$—the 2-rank of A, i.e. the number of cyclic direct summands of A_2.

H. Garland [2] proved that the group K_2O_F is finite, where K_2 is the functor of Milnor. It is also known [1] that

$$r_2(K_2O_F) = r_1 + g(2) - 1 + r, \tag{1}$$

where r_1 is the number of real embeddings of the field F, $g(2)$ is the number of distinct prime ideals of O_F dividing (2), and $r = r_2\big(\mathrm{Cl}(F)/\mathrm{Cl}_2(F)\big)$, where $\mathrm{Cl}(F)$ is the group of ideal classes of the field F, and $\mathrm{Cl}_2(F)$ is its subgroup generated by classes containing prime ideals dividing (2).

In the present paper we investigate the Sylow 2-subgroup of the group K_2O_F for quadratic number fields $F = \mathbb{Q}(\sqrt{d})$, where d is a square-free integer.

For real quadratic fields F it follows from (1) that

$$r_2(K_2O_F) = g(2) + 1 + r \geqslant 2.$$

We determine all real quadratic fields F with $(K_2O_F)_2 = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. On the other hand we prove that for every n there exists such a real quadratic field F that in $(K_2O_F)_2$ there is an element of order $\geqslant n$.

For imaginary quadratic fields F it follows from (1) that

$$r_2(K_2O_F) = g(2) - 1 + r \geqslant 0.$$

Hence $r_2(K_2O_F) = 0$ if $g(2) = 1$ and $r = 0$, i.e. $d \not\equiv 1 \bmod 8$ and the Sylow 2-subgroup of the class group of F is generated by classes containing divisors of 2. This has been proved by J. Tate [7]. He proved also that for $r = 0$ and $d \equiv 1 \bmod 8$ we have $(K_2O_F)_2 = \mathbb{Z}/2\mathbb{Z}$.

We extend these results and prove that for $d \equiv 1 \bmod 8$ the 2-rank of the Hilbert kernel of K_2O_F is by 1 less than $r_2(K_2O_F)$ (for $d \not\equiv 1 \bmod 8$ the two ranks are equal).

2. Notations

For a normalized discrete valuation v of the field F let $(a, b)_v$ be the tame symbol defined by the formula

$$(a, b)_v = (-1)^{v(a)v(b)} a^{v(b)} b^{-v(a)} \bmod v \quad \text{for} \quad a, b \in F^*.$$

The tame symbol induces a homomorphism of the Milnor group K_2F onto the multiplicative group of the residue class field $\overline{F}_v^*$ of the valuation v, defined by

$$\{a, b\} \mapsto (a, b)_v \quad \text{for} \quad a, b \in F^*.$$

It is known (see e.g. [5] or [6]) that $K_2 O_F = \operatorname{Ker} \tau$, where $\tau : K_2F \to \bigoplus_v \overline{F}_v^*$ is the homomorphism defined by the tame symbols and the sum is extended over all discrete valuations v of F.

For a non-complex valuation v of the field F let $[a, b]_v$ be the corresponding Hilbert symbol, and let

$$\eta : K_2F \to \bigoplus_v \mu_v$$

be the homomorphism defined by Hilbert symbols, where the sum is extended over all non-complex valuations v of F, and μ_v is the group of roots of unity in the completion F_v of the field F at v. Denote the Hilbert kernel $\operatorname{Ker} \eta$ by $\mathfrak{K}_2 F$. It is a subgroup of $K_2 O_F$; the factorgroup $K_2 O_F / \mathfrak{K}_2 F$ for every algebraic number field F has been determined in [1].

Let e_n be the number of cyclic components of $K_2 O_F$ of order divisible by n. Put $\Delta = \{a \in F^* : \{-1, a\} = 1\}$. We have $2 \in \Delta$, because $\{-1, 2\} = 1$. J. Tate [6] proved that $(\Delta : F^{*2}) = 2^{1+r_2}$ for every algebraic number field, where r_2 is the number of complex valuations of F. Consequently

$$\Delta = F^{*2} \cup 2F^{*2}$$

for every totally real field not containing $\sqrt{2}$.

3. Real quadratic fields

Theorem 1. *Let $F = \mathbb{Q}(\sqrt{d})$, $d > 2$ square-free have t odd prime factors. Then $e_2 = s+t$, where 2^s is the number of elements of the set $\{\pm 1, \pm 2\}$ that are norms of an element of F.*

Proof. Let $H_0(F)$ be the group of narrow classes of ideals in F, A be the narrow class containing the ideal $(\sqrt{d})$ and B the narrow class containing a prime ideal dividing 2. Put $H_2(F) = \langle A, B \rangle$, the group generated by A and B. We have

$$\mathrm{Cl}(F) = H_0(F)/\langle A \rangle, \quad \mathrm{Cl}_2(F) = H_2(F)/\langle A \rangle,$$

hence

$$\mathrm{Cl}(F)/\mathrm{Cl}_2(F) = H_0(F)/H_2(F).$$

If r is the 2-rank of $H_0(F)/H_2(F)$ then 2^r is the number of classes $C \in H_0(F)$ satisfying the condition $C^2 \in H_2(F)$ and distinct $\bmod H_2(F)$.

If N_0 is the number of solutions of $C^2 \in H_2(F)$ then

$$2^r \cdot |H_2(F)| = N_0,$$

on the other hand

$$N_0 = \left|H_2(F) \cap H_0(F)^2\right| \cdot 2^{r_2(H_0(F))}.$$

Hence

$$2^{r_2(H_0(F))-r} = \left(H_2(F) : H_2(F) \cap H_0(F)^2\right).$$

Now $e_2 = g(2) + r + 1$,

$$r_2\left(H_0(F)\right) + g(2) = \begin{cases} t+1 & \text{if } d \not\equiv 5 \bmod 8, \\ t & \text{if } d \equiv 5 \bmod 8. \end{cases}$$

Thus $e_2 = s + t$ is equivalent to the formula

$$q = \left(H_2(F) : H_2(F) \cap H_0(F)^2\right) = \begin{cases} 2^{2-s} & \text{if } d \not\equiv 5 \bmod 8, \\ 2^{1-s} & \text{if } d \equiv 5 \bmod 8. \end{cases} \tag{2}$$

In order to prove this formula observe that by Gauss's theorem the class of an ideal $\mathfrak{a}$ belongs to $H_0(F)^2$ if and only if $N\mathfrak{a} = Nc$ for some $c \in F$, which we shall denote simpler $N\mathfrak{a} \in NF$.

Therefore

$A \in H_0(F)^2$ if and only if $-1 \in NF$,

$B \in H_0(F)^2$ if and only if either $d \equiv 5 \bmod 8$, or $2 \in NF$,

$AB \in H_0(F)^2$ if and only if either $d \equiv 5 \bmod 8$, $-1 \in NF$, or $2 \in NF$.

If $A \in \langle B\rangle$ then either $A \in H_0(F)^2$, or $AB \in H_0(F)^2$, thus $-1 \in NF$ or $-2 \in NF$. On the other hand

$$q = \left(\langle B\rangle : \langle B\rangle \cap H_0(F)^2\right) = \begin{cases} 1 & \text{if } d \equiv 5 \bmod 8 \text{ or } 2 \in NF, \\ 2 & \text{if } d \not\equiv 5 \bmod 8 \text{ and } 2 \notin NF, \end{cases}$$

which confirms (2).

If B is of odd order then $B \in H_0(F)^2$ thus either $d \equiv 5 \bmod 8$ or $2 \in NF$. On the other hand

$$q = \frac{|\langle A\rangle| \cdot |\langle B\rangle|}{\left|\langle A\rangle \cap H_0(F)^2\right| \cdot |\langle B\rangle|} = \begin{cases} 1 & \text{if } -1 \in NF, \\ 2 & \text{if } -1 \notin NF, \end{cases}$$

which confirms (2).

Finally if $A \notin \langle B\rangle$ and B is of even order $2k$ then $d \not\equiv 5 \bmod 8$ and we have the disjoint decomposition

$$\langle A, B\rangle = \bigcup_{i=0}^{k-1} B^{2i}\{1, A, B, AB\}.$$

Hence

$$q = \frac{\big|\{1, A, B, AB\}\big|}{\big|\{1, A, B, AB\} \cap H_0(F)^2\big|} = 2^{2-s},$$

which proves (2). □

Theorem 2. *Let $F = \mathbb{Q}(\sqrt{d})$, $d > 2$ square-free have t odd prime factors, and let $\mathfrak{K}_2 F$ be the Hilbert kernel. We have*

if $d \not\equiv 1 \bmod 8$, then

$$e_4 \leqslant r_2(\mathfrak{K}_2 F) = \begin{cases} t-1 & \text{if } 2 \notin NF, \\ t & \text{if } 2 \in NF, \end{cases}$$

if $d \equiv 1 \bmod 8$, then

$$e_4 \leqslant r_2(\mathfrak{K}_2 F) = \begin{cases} t-2 & \text{if } -1 \notin NF,\ 2 \notin NF, \\ t & \text{if } -1 \in NF,\ d = u^2 - 2w^2,\ u > 0, \\ & \quad u \equiv 1 \bmod 4,\ w \equiv 0 \bmod 4, \\ t-1 & \text{otherwise.} \end{cases}$$

Proof. We proceed to write out all 2^{s+t} elements $\{-1, a\}$ of order $\leqslant 2$ in $K_2 O_F$. Let $c_1 = 1$, $c_i \in \{-1, 2, -2\}$, $c_i \in NF$ $(2 \leqslant i \leqslant 2^s)$ and be distinct. By the reciprocity for the norm residue symbols we have $d \in N\mathbb{Q}(\sqrt{c_i})$ and since $\mathbb{Z}[\sqrt{c_i}]$ is the unique factorization domain $d \in N\mathbb{Z}[\sqrt{c_i}]$, $d = u_i^2 - c_i w_i^2$, $u_i > 0$ $(2 \leqslant i \leqslant 2^s)$, $u_i \equiv 1 \bmod 2$ for $d \equiv 1 \bmod 4$. If $d \equiv 1 \bmod 4$, $c_i = 2$ one can always assume that $w_i \equiv 0 \bmod 4$.

Consider now all elements $\{-1, \gamma_i \delta\}$, where $\gamma_1 = 1$ and for $2 \leqslant i \leqslant 2^s$

$$\gamma_i = \begin{cases} \frac{1}{2}(u_i + \sqrt{d}) & \text{if } d \equiv 1 \bmod 4, \\ u_i + \sqrt{d} & \text{if } d \equiv 2 \text{ or } 3 \bmod 4, \end{cases}$$

and δ is an odd divisor of d positive or negative but not divisible by a fixed odd prime factor p of d. The number of relevant pairs $\langle i, \delta \rangle$ is 2^{s+t}. The elements themselves belong to $\operatorname{Ker} \tau$ since $(\gamma_i \delta) = \mathfrak{a} \cdot \mathfrak{q}^2$, where $\mathfrak{a} \mid 2$. Moreover to different pairs $\langle i, \delta \rangle$ there correspond elements distinct $\bmod \Delta = F^{*2} \cup 2F^{*2}$.

Indeed, suppose that $\gamma_i \delta / \gamma_j \delta' \in \Delta$ and $\langle i, \delta \rangle \neq \langle j, \delta' \rangle$. If $i \neq j$, we take norms and get $N\gamma_i / N\gamma_j \in \mathbb{Q}^{*2}$, i.e. $c_i / c_j \in \mathbb{Q}^{*2}$, which is impossible. If $i = j$, then $\delta \neq \delta'$ and $\delta / \delta' \in \Delta$ is impossible, since δ, δ' are not divisible by p.

Therefore $2^{r_2(\mathfrak{K}_2 F)}$ is the number of elements $\{-1, \gamma_i \delta\}$ in question that belong to $\mathfrak{K}_2 F$, i.e. satisfy $[-1, \gamma_i \delta]_v = 1$ for every non-complex valuation v of F. Taking for v the real valuations we infer that $\gamma_i \delta$ is totally positive, hence $\delta > 0$, $i = 1$ or $c_i = 2$ and

$$\gamma = \gamma_i = \begin{cases} 1 & \text{if } 2 \notin NF, \text{ i.e. } d \neq u^2 - 2w^2, \\ 1 \text{ or } u + \sqrt{d} & \text{if } d = u^2 - 2w^2,\ u > 0,\ d \equiv 2 \text{ or } 3 \bmod 4, \\ 1 \text{ or } \frac{1}{2}(u + \sqrt{d}) & \text{if } d = u^2 - 2w^2,\ u > 0,\ d \equiv 1 \bmod 4. \end{cases}$$

If v is a discrete valuation induced by a prime ideal $\mathfrak{p}$ of F and m_v is the number of roots of unity contained in the completion F_v, then either $m_v = N\mathfrak{p} - 1$ or $\mathfrak{p} \mid 3$, $d \equiv -3 \bmod 9$,

$m_v = 6$ or $\mathfrak{p} \mid 2$,

$$m_v = \begin{cases} 2(N\mathfrak{p} - 1) & \text{if } d \not\equiv -1 \bmod 8, \\ 4 & \text{if } d \equiv -1 \bmod 8. \end{cases}$$

In the first case $[-1, \gamma\delta]_v = (-1, \gamma\delta)_v = 1$. In the second case $[-1, \gamma\delta]_v^3 = (-1, \gamma\delta)_v = 1$ and since also $[-1, \gamma\delta]_v^2 = 1$ we get $[-1, \gamma\delta]_v = 1$.

In the third case if $d \not\equiv 1 \bmod 8$ there is only one prime ideal $\mathfrak{p}$ of F dividing 2. By the product formula for Hilbert symbols we get $[-1, \gamma\delta]_v^{m_v/2} = 1$ which for $d \not\equiv -1 \bmod 8$ gives $[-1, \gamma\delta]_v^3 = 1$ and again $[-1, \gamma\delta]_v = 1$.

Thus if $d \not\equiv \pm 1 \bmod 8$, $\{-1, \gamma\delta\} \in \mathfrak{K}_2 F$ if and only if $\gamma\delta \gg 0$, which gives

$$2^{r_2(\mathfrak{K}_2 F)} = \begin{cases} 2^{t-1} & \text{if } 2 \notin NF, \\ 2^t & \text{if } 2 \in NF. \end{cases}$$

Moreover since the Hilbert symbols for which $[-1, \gamma\delta]_v$ happened to be -1 were real and so quadratic, we have

$$e_4 \leqslant r_2(\mathfrak{K}_2 F).$$

If $d \equiv 1 \bmod 8$ there are two valuations corresponding to prime ideal factors of 2 in F. An easy computation shows that $[-1, \gamma\delta]_v = 1$ is equivalent to

$$\gamma\delta \equiv 1 \bmod \frac{4}{(2, \gamma)^2}. \tag{3}$$

If $-1 \notin NF$ then d has prime factors of the form $4k + 3$ and at least two of them since $d \equiv 1 \bmod 8$. Hence the number of positive δ's in each residue class $\pm 1 \bmod 4$ is 2^{t-2} and we get

$$2^{r_2(\mathfrak{K}_2 F)} = \begin{cases} 2^{t-2} & \text{if } 2 \notin NF, \\ 2^{t-1} & \text{if } 2 \in NF. \end{cases}$$

If $-1 \in NF$ then all 2^{t-1} positive δ's are of the form $4k + 1$ and the condition (3) takes the form

$$\gamma \equiv 1 \bmod \frac{4}{(2, \gamma)^2}.$$

This gives either $\gamma = 1$ or

$$\gamma = \frac{u + \sqrt{d}}{2} \equiv 1 \bmod \left(2, \frac{u - \sqrt{d}}{2}\right)^2.$$

In the latter case since $w \equiv 0 \bmod 4$ we have

$$\frac{u + \sqrt{d}}{2} \frac{u - \sqrt{d}}{2} = \frac{w^2}{2} \equiv 0 \bmod \left(2, \frac{u - \sqrt{d}}{2}\right)^2.$$

Hence

$$\frac{u - \sqrt{d}}{2} \equiv 0 \bmod \left(2, \frac{u - \sqrt{d}}{2}\right)^2$$

and by addition, $u \equiv 1 \bmod \left(2, \dfrac{u-\sqrt{d}}{2}\right)^2$, and since $u \in \mathbb{Z}$, $u \equiv 1 \bmod 4$. Therefore

$$2^{r_2(\mathfrak{K}_2 F)} = \begin{cases} 2^t & \text{if } 2 \in NF, \\ 2^{t-1} & \text{otherwise.} \end{cases}$$

This completes the proof for $d \equiv 1 \bmod 8$ since Hilbert symbols used in the proof are quadratic.

If $d \equiv -1 \bmod 8$, then $(2) = \mathfrak{p}^2$ in F and if v is the valuation induced by $\mathfrak{p}$ we have to consider Hilbert symbol $[a, b]_v$ of exponent 4, connected with the biquadratic residue symbol for the field $\mathbb{Q}_2(i)$ in which F can be embedded.

Let for an element a of F, $\bar{a}$ be its image in $\mathbb{Q}_2(i)$ and $\bar{v}$ be the valuation of $\mathbb{Q}_2(i)$ corresponding to v, so that $[a, b]_v = [\bar{a}, \bar{b}]_{\bar{v}}$. If $\bar{a}$ is a $\bar{v}$-adic unit then

$$[-1, \bar{a}]_{\bar{v}} = (-1)^{(N\bar{a}-1)/4}$$

depends only on the residue of $\bar{a} \bmod 4$ (see H. Hasse [4], p. 86).

For every odd rational integer δ we have

$$[-1, \delta]_v = [-1, \delta]_{\bar{v}} = (-1)^{(\delta^2-1)/4} = 1.$$

It remains to compute $[-1, u + \sqrt{d}]_v$. Since

$$\overline{\sqrt{d}} \equiv i\,\frac{d-1}{2} \bmod 8,$$

we have $\overline{(u+\sqrt{d})}/(1-i) \equiv \dfrac{2u-d+1}{4} + i\,\dfrac{2u+d-1}{4} \bmod 4$ and the number on the right hand side is a $\bar{v}$-adic unit. Hence

$$\begin{aligned}[-1, u+\sqrt{d}]_v &= [-1, \overline{u+\sqrt{d}}]_{\bar{v}} = [i, \overline{u+\sqrt{d}}]_{\bar{v}}^2 \\ &= [i, 1-i]_{\bar{v}}^2 \cdot \left[i, \frac{2u-d+1}{4} + i\,\frac{2u+d-1}{4}\right]_{\bar{v}}^2 = (-1)^{(M-1)/4},\end{aligned}$$

where

$$M = \left(\frac{2u-d+1}{4}\right)^2 + \left(\frac{2u+d-1}{4}\right)^2 = \frac{u^2}{2} + \frac{(d-1)^2}{8}.$$

Since $d = u^2 - 2w^2$, we have $d - 1 \equiv u^2 - 3 \bmod 16$, $(d-1)^2 \equiv (u^2-3)^2 \bmod 64$ and

$$M \equiv \frac{u^2}{2} + \frac{(u^2-3)^2}{8} = 1 + \frac{(u^2-1)^2}{8} \equiv 1 \bmod 8,$$

thus $[-1, \gamma]_v = 1$. We get the same inequality as for $d \not\equiv \pm 1 \bmod 8$. □

Corollary 1. *If $d \not\equiv \pm 1 \bmod 8$, $d > 2$, then $|(K_2 O_F)_2| \geqslant 8$ unless $d = p$ or $2p$, $p \equiv \pm 3 \bmod 8$ a prime, in which case $(K_2 O_F)_2 = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.*

Proof. If $d \not\equiv \pm 1 \bmod 8$ we have $\left(K_2 O_F / \mathfrak{K}_2 F\right)_2 = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ by the result of [1], on the other hand $r_2(\mathfrak{K}_2 F) \geqslant 1$ unless $d = p$ or $2p$, $p \equiv \pm 3 \bmod 8$ a prime. □

Corollary 2. *If $d \equiv \pm 1 \bmod 8$, then $|(K_2O_F)_2| \geqslant 16$ unless $d = pq$, $p \equiv q \equiv 3 \bmod 8$ primes or $d = p = u^2 - 2w^2$, $u > 0$, $u \equiv 3 \bmod 4$, $w \equiv 0 \bmod 4$ in which case*

$$(K_2O_F)_2 = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Proof. If $d \equiv \pm 1 \bmod 8$ we have $|K_2O_F/\mathfrak{K}_2F| \geqslant 8$ by the result of [1]. On the other hand $r_2(\mathfrak{K}_2F) \geqslant 1$ unless $d = pq$, $p \equiv q \equiv 3 \bmod 8$ primes or $d = p = u^2 - 2w^2$, $u > 0$, $u \equiv 3 \bmod 4$, $w \equiv 0 \bmod 4$, and then we apply [1] again. □

Corollary 3. *$e_4 \geqslant 1$ provided either $-1 \notin NF$, $-2 \notin NF$,*
or $-1 \in NF$, $-2 \notin NF$, $d \equiv 1 \bmod 8$,
or $-1 \in NF$, $-2 \in NF$, $d = u^2 - 2w^2$, $u > 0$, $u \equiv 1 \bmod 4$, $w \equiv 0 \bmod 4$.

Proof. In these cases $r_2(K_2O_F) < r_2(K_2O_F/\mathfrak{K}_2F) + r_2(\mathfrak{K}_2F)$. □

Corollary 4. *$e_8 \geqslant 1$ provided $d = pq$, $p \equiv -q \equiv 3 \bmod 8$ primes or $p \equiv -1 \bmod 8$, a prime.*

Proof. In both cases $r_2(K_2O_F) = 2$, $\left|(K_2O_F)_2\right| \geqslant 16$ by Corollary 2, and $e_4 \leqslant 1$. □

Corollary 5. *Sylow 2-subgroup of K_2O_F is generated by symbols if and only if $d = 2$, p or $2p$, $p \equiv -3 \bmod 8$ a prime.*

Proof. The only symbols in K_2O_F are 1, $\{-1, -1\}$, $\{-1, \varepsilon\}$, $\{-1, -\varepsilon\}$, where ε is the fundamental unit in F. Thus from Corollaries 1 and 2 it follows that if K_2O_F is generated by symbols, then $d = 2$, p or $2p$, $p \equiv -3 \bmod 8$ a prime.

Evidently $\{-1, -1\} \neq 1$ and in the case $p \equiv -3 \bmod 8$ we have $\pm 2 \notin NF$. Consequently $2\varepsilon \notin F^{*2}$, $\varepsilon \notin \Delta$, $\{-1, \varepsilon\} \neq 1$.

If $d = p$ or $2p$, $p \equiv 3 \bmod 8$, then $-2 \in NF$. Since 2 ramifies in F, we have $\varepsilon \in 2F^{*2}$, i.e. $\{-1, \varepsilon\} = 1$ and there are only two symbols in K_2O_F. □

Theorem 3. *If the fundamental unit $\varepsilon = \alpha + \beta\sqrt{d}$ of F satisfies $N\varepsilon = 1$, $\alpha, \beta \in \mathbb{Z}$, $\alpha \pm 1$ is not the square of an integer, and*

$$\alpha = 2^{k \cdot 2^{r-1}-1} \cdot c^{2^r} \quad \text{for some positive integers } k, r, c, \tag{4}$$

then in K_2O_F there is an element of order 2^{r+1}.

Proof. Suppose that $2\varepsilon \in F^{*2}$. Then 2 ramifies in F and we have $d \equiv 2$ or $3 \bmod 4$. Hence $2\alpha + 2\beta\sqrt{d} = \left(\gamma + \delta\sqrt{d}\right)^2$ for some $\gamma, \delta \in \mathbb{Z}$. Consequently $2\alpha = \gamma^2 + \delta^2 d$, $4 = (\gamma^2 - \delta^2 d)^2$, $\pm 2 = \gamma^2 - \delta^2 d$, $\alpha \pm 1 = \gamma^2$ contrary to the assumption.

It follows that $2\varepsilon \notin F^{*2}$, and hence $\varepsilon \notin \Delta$, i.e. $\{-1, \varepsilon\} \neq 1$.

Evidently $\varepsilon = \alpha + \beta\sqrt{d}$ satisfies $\varepsilon^2 - 2\alpha\varepsilon + 1 = 0$. Hence $1 = -\varepsilon^2 + 2\alpha\varepsilon$. From the properties of symbols $\{x, y\}$ it follows that $\{-1, 2\} = 1$, $\{\varepsilon^2, \varepsilon\} = \{\varepsilon, \varepsilon\}^2 = \{\varepsilon, -1\}^2 = 1$. Consequently

$$1 = \{-\varepsilon^2, 2\alpha\varepsilon\} = \{-1, \varepsilon\}\{-1, \alpha\}\{\varepsilon^2, 2\alpha\}$$

and hence

$$\{-1, \varepsilon\} = \{-1, \alpha\}\{\varepsilon^2, 2\alpha\}.$$

Now from (4) it follows that $\{-1, \alpha\} = \{-1, 2\}^s \{-1, c\}^{2r} = 1$ where $s = k \cdot 2^{r-1} - 1$, and

$$\{\varepsilon^2, 2\alpha\} = \{\varepsilon^2, 2^{k \cdot 2^{r-1}} \cdot c^{2^r}\} = \{\varepsilon, 2\}^{k \cdot 2^r} \{-\varepsilon^2, c\}^{2^r},$$

because $\{-1, c^{2^r}\} = 1$.

Moreover $\{\varepsilon, 2\}\{-\varepsilon^2, c\} \in \operatorname{Ker} \tau$, because $-\varepsilon^2 = 1 - 2\alpha\varepsilon \equiv 1 \bmod \alpha$ and hence $-\varepsilon^2 \equiv 1 \bmod c$. It follows that every tame symbol $(-\varepsilon^2, c)_v$ is trivial.

Therefore

$$\{-1, \varepsilon\} = \big(\{\varepsilon, 2^k\}\{-\varepsilon^2, c\}\big)^{2^r}. \tag{5}$$

Since the element $\{-1, \varepsilon\}$ has order 2, from (5) it follows that the element

$$\{\varepsilon, 2^k\}\{-\varepsilon^2, c\} \in K_2 O_F$$

has order 2^{r+1}. □

The next Lemma enables us to give examples of fields satisfying assumptions of Theorem 3.

Lemma. *A unit of the form* $2^a h + \sqrt{2^{2a} h^2 - 1}$, *where* $a \geqslant 1$, $h \geqslant 1$, *is fundamental in its field provided* $h < 2^{2a+2} - 3$.

Proof. Suppose that

$$2^a h + \sqrt{2^{2a} h^2 - 1} = \big(u + v\sqrt{d}\big)^n,$$

where $n > 1$, $u, v \in \mathbb{Z}$, $u, v > 0$. Clearly n is odd and $u^2 - dv^2 = 1$. It follows that $u \mid 2^a h$, $v^2 d \mid 2^{2a} h^2 - 1$. Hence $vd \equiv 1 \bmod 2$, $u \equiv 0 \bmod 2$. If $u = 2^s m$, m odd, then

$$2^a h = \frac{1}{2}\Big[\big(u + v\sqrt{d}\big)^n + \big(u - v\sqrt{d}\big)^n\Big] \equiv 2^s \bmod 2^{s+1},$$

thus $s \geqslant a$, and $u \geqslant 2^s \geqslant 2^a$. We have

$$\begin{aligned} 2^a h = \frac{1}{2}\Big[\big(u + v\sqrt{d}\big)^n + \big(u - v\sqrt{d}\big)^n\Big] &\geqslant \frac{1}{2}\Big[\big(u + v\sqrt{d}\big)^3 + \big(u - v\sqrt{d}\big)^3\Big] \\ &= u^3 + 3uv^2 d = 4u^3 - 3u \geqslant 2^{3a+2} - 3 \cdot 2^2. \end{aligned}$$

Hence $h \geqslant 2^{2a+2} - 3$, a contradiction. □

Corollary 6. *If* $\langle a_1, h_1\rangle \neq \langle a_2, h_2\rangle$, h_1, h_2 *odd,* $h_i < 2^{2a_i+2} - 3$, *then the fields*

$$\mathbb{Q}\big(\sqrt{2^{2a_i} \cdot h_i^2 - 1}\big)$$

are different.

Corollary 7. *If* $F = \mathbb{Q}\big(\sqrt{4^a - 1}\big)$, $a = 2^{r-1} - 1$, $r \geqslant 4$, *then in* $K_2 O_F$ *there is an element of order* 2^{r+1}.

Proof. Taking in Lemma $h = 1$ we infer that the unit $2^a + \sqrt{4^a - 1}$ is fundamental in F. It satisfies the assumptions of Theorem 3 provided $2^a \pm 1$ is not the square of an integer. The latter condition is equivalent in virtue of an old theorem of Gerono to $a \neq 1,\ 3$, which holds for $r \geqslant 4$. □

4. Imaginary quadratic fields

Theorem 4. *Let $F = \mathbb{Q}(\sqrt{d})$, $d < -2$ square-free have t odd prime factors. Then*

$$e_2 = \begin{cases} t & \text{if } 2 \in NF, \\ t-1 & \text{if } 2 \notin NF, \end{cases} \tag{6}$$

$$e_4 \leqslant r_2(\mathfrak{K}_2 F) = \begin{cases} e_2 & \text{if } d \not\equiv 1 \bmod 8, \\ e_2 - 1 & \text{if } d \equiv 1 \bmod 8. \end{cases} \tag{7}$$

Proof. If r is the 2-rank of $\mathrm{Cl}(F)/\mathrm{Cl}_2(F)$, then 2^r is the number of classes $C \in \mathrm{Cl}(F)$ satisfying the condition $C^2 \in \mathrm{Cl}_2(F)$ and distinct $\bmod \mathrm{Cl}_2(F)$.

If N_1 is the number of solutions of $C^2 \in \mathrm{Cl}_2(F)$, then

$$2^r \cdot |\mathrm{Cl}_2(F)| = N_1,$$

on the other hand

$$N_1 = \left|\mathrm{Cl}_2(F) \cap \mathrm{Cl}(F)^2\right| \cdot 2^{r_2(\mathrm{Cl}(F))}.$$

Hence

$$2^{r_2(\mathrm{Cl}(F))-r} = \big(\mathrm{Cl}_2(F) : \mathrm{Cl}_2(F) \cap \mathrm{Cl}(F)^2\big).$$

Now $e_2 = g(2) + r - 1$,

$$r_2\big(\mathrm{Cl}(F)\big) + g(2) = \begin{cases} t+1 & \text{if } d \not\equiv 5 \bmod 8, \\ t & \text{if } d \equiv 5 \bmod 8. \end{cases}$$

Thus (6) is equivalent to the formula

$$q = \big(\mathrm{Cl}_2(F) : \mathrm{Cl}_2(F) \cap \mathrm{Cl}(F)^2\big) = \begin{cases} 2 & \text{if } d \not\equiv 5 \bmod 8,\ 2 \notin NF, \\ 1 & \text{otherwise.} \end{cases} \tag{8}$$

In order to prove this formula observe that by Gauss's theorem the class of an ideal $\mathfrak{a}$ belongs to $\mathrm{Cl}(F)^2$ if and only if $N\mathfrak{a} \in NF$. Therefore $\mathrm{Cl}_2(F) \subset \mathrm{Cl}(F)^2$ if and only if either $d \equiv 5 \bmod 8$ (then $\mathrm{Cl}_2(F)$ is trivial) or $2 \in NF$. This confirms (8).

In order to prove (7) we proceed to write out all elements $\{-1, a\}$ of order $\leqslant 2$ in $K_2 O_F$.

If $2 \in NF$, by the reciprocity law for the norm residue symbols we have $d \in N\mathbb{Q}(\sqrt{2})$ and since $\mathbb{Z}[\sqrt{2}]$ is the unique factorization domain $d \in N\mathbb{Z}[\sqrt{2}]$, $d = u^2 - 2w^2$.

Consider now all elements $\{-1, \gamma\delta\}$, where

$$\gamma = \begin{cases} 1 & \text{if } 2 \notin NF, \\ 1 \text{ or } u + \sqrt{d} & \text{if } d = u^2 - 2w^2,\ u > 0,\ d \equiv 2 \text{ or } 3 \bmod 4, \\ 1 \text{ or } \frac{1}{2}(u + \sqrt{d}) & \text{if } d = u^2 - 2w^2,\ u > 0,\ d \equiv 1 \bmod 4, \end{cases}$$

and δ is an odd divisor of d positive or negative, but not divisible by a fixed prime factor of d.

The number of such elements is 2^{t+1} if $2 \in NF$, 2^t if $2 \notin NF$, that is 2^{e_2+1}. They belong to Ker τ since $(\gamma\delta) = \mathfrak{a}\mathfrak{q}^2$, where $\mathfrak{a} \mid 2$. Moreover, different elements $\gamma\delta$ are distinct mod $F^{*2} \cup 2F^{*2}$. Since $F^{*2} \cup 2F^{*2}$ is a subgroup of index 2 in Δ, the set of numbers $\gamma\delta$ can contain at most two elements from each class of equivalence mod Δ. But the number of equivalence classes is 2^{e_2}, hence among numbers $\gamma\delta$ each equivalence class mod Δ is represented exactly twice. Therefore $2^{r_2(\mathfrak{K}_2F)+1}$ is the number of elements $\{-1, \gamma\delta\}$ in question that belong to $\mathfrak{K}_2F$, i.e. satisfy

$$[-1, \gamma\delta]_v = 1 \text{ for every non-complex valuation } v \text{ of } F.$$

Since F is imaginary there are no real valuations. If v is a discrete valuation then we infer in the same way as for real quadratic fields in the proof of Theorem 2 that $[-1, \gamma\delta]_v = 1$ if either $d \not\equiv 1 \bmod 8$ or $d \equiv 1 \bmod 8$, $\gamma\delta \equiv 1 \bmod \dfrac{4}{(2, \gamma)^2}$.

If $d \equiv 1 \bmod 8$ and $\gamma\delta \not\equiv 1 \bmod \dfrac{4}{(2, \gamma)^2}$ then there exists a discrete valuation v and a quadratic Hilbert symbol such that

$$[-1, \gamma\delta]_v \neq 1. \tag{9}$$

Hence if $d \not\equiv 1 \bmod 8$ we have $r_2(\mathfrak{K}_2F) = e_2$. If $d \equiv 1 \bmod 8$ the number of δ's (positive or negative) in each residue class $\pm 1 \bmod 4$ is 2^{t-1}. Hence

$$2^{r_2(\mathfrak{K}_2F)+1} = 2^{e_2}, \quad r_2(\mathfrak{K}_2F) = e_2 - 1.$$

Moreover since the symbol $[-1, \gamma\delta]_v$ that satisfies (9) is quadratic, we have $e_4 \leqslant r_2(\mathfrak{K}_2F)$. The proof is complete. □

Corollary 8. $\left|(K_2O_F)_2\right| \geqslant 2$ *unless* $d = -1, -2, -p$ *or* $-2p$, $p \equiv \pm 3 \bmod 8$ *a prime, in which case* $|K_2O_F|$ *is odd.*

Proof. $|K_2O_F|$ odd is equivalent in virtue of Theorem 4 to $t = 1$, $2 \notin NF$. □

Corollary 9. *If* $d \equiv 1 \bmod 8$, *then* $\left|(K_2O_F)_2\right| \geqslant 4$ *unless* $d = -p$ ($p \equiv -1 \bmod 8$ *a prime*) *or* $d = -pq$ ($p \equiv -q \equiv 3 \bmod 8$ *primes*), *in which case* $(K_2O_F)_2 = \mathbb{Z}/2\mathbb{Z}$.

Proof. $\left|(K_2O_F)_2\right| < 4$ implies $e_2 = 0$ or 1. The first case is excluded by Corollary 8, the second case gives $t = 1$, $2 \in NF$ or $t = 2$, $2 \notin NF$. Together with $d \equiv 1 \bmod 8$ this condition is equivalent to $d = -p$, $p \equiv -1 \bmod 8$ a prime or $d = -pq$, p, q primes satisfying $p \equiv -q \equiv 3 \bmod 8$. However by (7) $e_4 = 0$, hence in these cases $(K_2O_F)_2 = \mathbb{Z}/2\mathbb{Z}$. □

Added in proof. In view of recent results of B. Mazur and A. Wiles, and J. Hurrelbrink it can be deduced from Corollary 5 that K_2O_F is generated by symbols iff $d = 2$, 5 or 13.

References

[1] J. Browkin, *The functor K_2 for the ring of integers of a number field*. In: Universal Algebra and Applications (Warsaw, 1978), Banach Center Publ. 9, PWN, Warsaw 1982, 187–195.

[2] H. Garland, *A finiteness theorem for K_2 of a number field*. Ann. of Math. (2) 94 (1971), 534–548.

[3] H.-M. Gebhardt, *Zur Berechnung des Funktors K_2 von einigen euklidischen Ringen*. Schr. Math. Inst. Univ. Münster (2) Heft 13 (1977).

[4] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil II: *Reziprozitätsgesetz*. Physica-Verlag, Würzburg–Wien 1965.

[5] D. Quillen, *Higher algebraic K-theory* I. In: Algebraic K-theory I. Higher K-theories (Seattle, 1972), Lecture Notes in Math. 341, Springer, Berlin 1973, 85–147.

[6] J. Tate, *Relations between K_2 and Galois cohomology*. Invent. Math. 36 (1976), 257–274.

[7] —, Appendix to: H. Bass, J. Tate, *The Milnor ring of a global field*. In: Algebraic K-theory II. "Classical" Algebraic K-theory, and Connections with Arithmetic (Seattle, 1972), Lecture Notes in Math. 342, Springer, Berlin 1973, 429–446.

Andrzej Schinzel
Selecta

Originally published in
Tatra Mountains Mathematical Publications
11 (1997), 35–42

A class of algebraic numbers

To Władysław Narkiewicz on his sixtieth birthday

Abstract. It is shown that a nonnegative real number is a K-number in the sense of Korec [2] if and only if it is an algebraic integer not less in absolute value than any of its conjugates.

I. Korec [2] has introduced a class of K-numbers defined as follows.

A *K-system* is a vector $\langle \alpha_1, \dots, \alpha_m \rangle \in \mathbb{R}_+^m$ such that for all $i \leqslant m$ and $j \leqslant m$ we have

$$\alpha_i \alpha_j = \sum_{k=1}^{m} c_{ijk} \alpha_k, \quad \text{where } c_{ijk} \in \mathbb{N}_0, \tag{1}$$

($\mathbb{R}_+$ is the set of positive real numbers, $\mathbb{N}_0$ the set of nonnegative integers);

α is a *K-number* if there exists a K-system $\langle \alpha_1, \dots, \alpha_m \rangle$ such that

$$\alpha = \sum_{k=1}^{m} a_k \alpha_k, \quad a_k \in \mathbb{N}_0.$$

It follows that $\alpha \in \mathbb{R}_+ \cup \{0\}$.

Korec proved that all K-numbers are algebraic integers and asked several questions about them, e.g., if $3 - \sqrt{2}$ is a K-number. The following characterization of K-numbers allows one to decide whether a given algebraic integer is a K-number.

Theorem. *A nonnegative real number is a K-number if and only if it is an algebraic integer and it is not less in absolute value than any of its conjugates.*

The proof presented here depends only on Dirichlet's approximation theorem.

Lemma 1. *If*

$$\alpha = \sum_{k=1}^{m} a_k \alpha_k, \text{ where } \langle \alpha_1, \dots, \alpha_m \rangle \text{ is a } K\text{-system}, \quad a_k \in \mathbb{N}_0 \tag{2}$$

then α is an algebraic integer and for each $l \in \mathbb{N}$ we have

$$\alpha^l = \sum_{k=1}^{m} a_{kl} \alpha_k, \quad a_{kl} \in \mathbb{N}_0. \tag{3}$$

Proof. The formula (1) shows that α_i is a characteristic root of the matrix $(c_{ijk})_{jk}$. Thus α_i is a zero of a polynomial over $\mathbb{Z}$ with the leading coefficient ± 1, hence α_i is an algebraic integer for all $i \leqslant m$ and so is α by (2).

To prove (3) we proceed by induction on l. For $l = 1$, (3) follows from (2) with $a_{kl} = a_k$. Assume that (3) holds for an exponent l. Then by (2) and (1)

$$\alpha^{l+1} = \Big(\sum_{i=1}^{m} a_i\alpha_i\Big)\Big(\sum_{j=1}^{m} a_{jl}\alpha_j\Big) = \sum_{i,j=1}^{m} (a_i a_{jl})\alpha_i\alpha_j$$
$$= \sum_{i,j=1}^{m} a_i a_{jl} \sum_{k=1}^{m} c_{ijk}\alpha_k$$

and (3) holds for the exponent $l+1$ with

$$a_{k,l+1} = \sum_{i,j=1}^{m} a_i a_{jl} c_{ijk}. \qquad \square$$

Lemma 2. *Let $k_1, k_2 \in \mathbb{N}_0$,*

$$f_j(x) = \begin{cases} x + a_j & \text{for } j \leqslant k_1, \\ x^2 + a_j x + b_j & \text{for } k_1 < j \leqslant k_1 + k_2, \end{cases}$$

where $a_j \in \mathbb{R}_+$, $b_j \in \mathbb{R}_+$ and let

$$\prod_{j=1}^{k_1+k_2} f_j(x) = \sum_{\lambda=0}^{l} A_\lambda x^{l-\lambda}.$$

Then $A_0 = 1$ and for $\lambda < l$ we have

$$0 < \frac{A_{\lambda+1}}{A_\lambda} \leqslant \sum_{j=1}^{k_1+k_2} \max\{a_j, b_j/a_j\}, \tag{4}$$

where here and below maximum applies only to terms that are defined.

Proof. We proceed by induction on k_2. For $k_2 = 0$, (4) follows from the inequality

$$\tau_{\lambda+1}(a_1, \ldots, a_{k_1}) \leqslant \tau_\lambda(a_1, \ldots, a_{k_1})(a_1 + \ldots + a_{k_1}),$$

where τ_λ is the λ-th fundamental symmetric function. Assume that (4) holds for arbitrary k_1, and k_2 replaced by $k_2 - 1$ ($k_2 \geqslant 1$). Thus

$$\prod_{j=1}^{k_1+k_2-1} f_j(x) = \sum_{\mu=0}^{m} B_\mu x^{m-\mu},$$

where

$$0 < \frac{B_{\mu+1}}{B_\mu} \leqslant \sum_{j=1}^{k_1+k_2-1} \max\{a_j, b_j/a_j\}.$$

Thus $l = m + 2$ and putting $k_1 + k_2 = \kappa$ we have

$$A_0 = 1, \quad A_1 = B_1 + a_\kappa, \quad A_\lambda = B_\lambda + a_\kappa B_{\lambda-1} + b_\kappa B_{\lambda-2} \qquad (2 \leqslant \lambda \leqslant l-2),$$
$$A_{l-1} = a_\kappa B_{l-2} + b_\kappa B_{l-3}, \quad A_l = b_\kappa B_{l-2}.$$

Hence

$$\frac{A_1}{A_0} = \frac{B_1}{B_0} + a_\kappa \leqslant \sum_{j=1}^{\kappa-1} \max\{a_j, b_j/a_j\} + a_\kappa \leqslant \sum_{j=1}^{\kappa} \max\{a_j, b_j/a_j\}$$

$$\frac{A_2}{A_1} \leqslant \max\left\{\frac{B_2}{B_1}, \frac{B_1}{B_0}\right\} + \frac{b_\kappa}{a_\kappa} \leqslant \sum_{j=1}^{\kappa-1} \max\left\{a_j, \frac{b_j}{a_j}\right\} + \frac{b_\kappa}{a_\kappa}$$

$$\leqslant \sum_{j=1}^{\kappa} \max\left\{a_j, \frac{b_j}{a_j}\right\}$$

and if $2 \leqslant \lambda < l$

$$\frac{A_{\lambda+1}}{A_\lambda} \leqslant \max\left\{\frac{B_{\lambda+1}}{B_\lambda}, \frac{B_\lambda}{B_{\lambda-1}}, \frac{B_{\lambda-1}}{B_{\lambda-2}}\right\} \leqslant \sum_{j=1}^{\kappa-1} \max\left\{a_j, \frac{b_j}{a_j}\right\}$$

$$\leqslant \sum_{j=1}^{\kappa} \max\left\{a_j, \frac{b_j}{a_j}\right\}$$

which completes the inductive proof. □

Lemma 3. *Let $\beta_j \in \mathbb{C}$ and $\Re\beta_j < 0$ $(2 \leqslant j \leqslant k)$. For infinitely many $\nu \in \mathbb{N}_0$ we have*

$$\Re\beta_j^{\nu+1} \leqslant \tfrac{1}{2}|\beta_j|^\nu \Re\beta_j \qquad (2 \leqslant j \leqslant k).$$

Proof. Let $\beta_j = |\beta_j| \exp(2\pi i \varphi_j)$ $(2 \leqslant j \leqslant k)$. By the assumption we have

$$\|\varphi_j\| > \tfrac{1}{4} \qquad (2 \leqslant j \leqslant k).$$

Here $\|x\| = \min\{\{x\}, 1 - \{x\}\}$, where $\{x\}$ is the fractional part of x. By Dirichlet's approximation theorem there exist infinitely many $\nu \in \mathbb{N}_0$ such that

$$\|\varphi_j \nu\| \leqslant \tfrac{1}{2}\|\varphi_j\| - \tfrac{1}{8} \quad (2 \leqslant j \leqslant k).$$

Hence

$$\|\varphi_j(\nu+1)\| \geqslant \|\varphi_j\| - \|\varphi_j \nu\| \geqslant \tfrac{1}{2}\|\varphi_j\| + \tfrac{1}{8}$$

which gives

$$\cos 2\pi\varphi_j(\nu+1) \leqslant \cos\pi(\|\varphi_j\| + \tfrac{1}{4}) = \frac{1}{\sqrt{2}}(\cos\pi\|\varphi_j\| - \sin\pi\|\varphi_j\|)$$

$$= \frac{1}{\sqrt{2}} \frac{\cos 2\pi\|\varphi_j\|}{\cos\pi\|\varphi_j\| + \sin\pi\|\varphi_j\|} \leqslant \frac{1}{2}\frac{\Re\beta_j}{|\beta_j|},$$

and thus

$$\Re\beta_j^{\nu+1} = \|\beta_j\|^{\nu+1}\cos 2\pi\varphi_j(\nu+1) \leqslant \tfrac{1}{2}|\beta_j|^{\nu}\Re\beta_j \quad (2 \leqslant j \leqslant k). \qquad \square$$

Lemma 4. *Let $\alpha \in \mathbb{R}_+$ be an algebraic number, $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ be all its conjugates. If $\alpha \geqslant |\alpha_i|$ $(1 \leqslant i \leqslant n)$, then there exists a positive integer e such that for all i either $\alpha^e > |\alpha_i^e|$ or $\alpha^e = \alpha_i^e$.*

Proof. Put

$$\beta = \prod_{\substack{i=1\\ |\alpha_i|=\alpha}}^{n} \alpha_i^2.$$

We have $\beta \in \mathbb{R}_+$, because in the above product every non-real α_i appears together with its complex conjugate. Hence we have

$$\beta = \prod_{\substack{i=1\\ |\alpha_i|=\alpha}}^{n} |\alpha_i|^2 = \alpha^e, \qquad e = 2\#\{1 \leqslant i \leqslant n : |\alpha_i| = \alpha\}.$$

On the other hand, if σ is any isomorphism of $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ we have

$$\alpha^e \geqslant |\alpha^\sigma|^e$$

and

$$\alpha^e = |\alpha^\sigma|^e$$

implies

$$\beta = \alpha^e = \left| \prod_{\substack{i=1\\ |\alpha_i|=\alpha}}^{n} (\alpha_i^\sigma)^2 \right| = |\beta^\sigma|.$$

Since $|\alpha_i^\sigma| \leqslant \alpha$, it follows that $|\alpha_i^\sigma| = \alpha$ whenever $|\alpha_i| = \alpha$ and thus

$$\{\alpha_i : |\alpha_i| = \alpha\} = \{\alpha_i^\sigma : |\alpha_i| = \alpha\}, \quad \beta = \beta^\sigma. \qquad \square$$

Remark. This lemma follows easily from a theorem of Boyd [1], however, the above proof is shorter than Boyd's proof.

Lemma 5. *Let $\alpha, \alpha_1, \ldots, \alpha_n$ have the meaning of Lemma 4. If $\alpha > 1$, $\alpha \geqslant |\alpha_i|$ $(1 \leqslant i \leqslant n)$, then there exist positive integers l and L such that for each i*

$$\text{either} \quad \alpha^l - L > |\alpha_i^l - L| \quad \text{and} \quad \Re(\alpha_i^l - L) < 0 \quad \text{or} \quad \alpha_i^l = \alpha^l. \tag{5}$$

Proof. Using Lemma 4 and replacing, if necessary, α by α^e, and n by the number of conjugates of α^e, we may assume that $n > 1$, $\alpha > |\alpha_i|$ $(2 \leqslant i \leqslant n)$. Since also $\alpha > 1$, there is a positive integer l such that

$$\left(\frac{\alpha}{\max\limits_{2\leqslant i\leqslant n} |\alpha_i|}\right)^l > 4 \quad \text{and} \quad \alpha^l \geqslant 8.$$

Then

$$\frac{1}{2}\Big(\alpha^l - \max_{2\leqslant i\leqslant n} |\alpha_i|^l\Big) - \max_{2\leqslant i\leqslant n} |\alpha_i|^l > \frac{\alpha^l}{8} \geqslant 1$$

and there exists a positive integer L such that

$$\frac{1}{2}\Big(\alpha^l - \max_{2\leqslant i\leqslant n} |\alpha_i|^l\Big) > L > \max_{2\leqslant i\leqslant n} |\alpha_i|^l.$$

The numbers l and L satisfy the conditions of the lemma, because for each $i > 1$

$$\alpha^l - L > L + \max_{2\leqslant i\leqslant n} |\alpha_i|^l \geqslant |\alpha_i^l - L|$$

and

$$\Re(\alpha_i^l - L) = \Re\alpha_i^l - L \leqslant \max_{2\leqslant i\leqslant n} |\alpha_i|^l - L < 0. \qquad \square$$

Proof of the Theorem. We begin by proving the necessity of the condition.

Assume that α is a K-number and (2) holds. By Lemma 1, α is an algebraic integer. Suppose that α is less in absolute value than α^σ, where σ is an embedding of $\mathbb{Q}(\alpha_1, \ldots, \alpha_m)$ into $\mathbb{C}$. Clearly $\alpha \neq 0$. Choose l so large that

$$\left(\frac{|\alpha^\sigma|}{\alpha}\right)^l > \max_{1\leqslant k\leqslant m} \frac{|\alpha_k^\sigma|}{\alpha_k}.$$

Then from (3) we get a contradiction. Indeed,

$$(\alpha^\sigma)^l = \sum_{k=1}^m a_{kl}\alpha_k^\sigma$$

and since $\alpha \neq 0$, at least one a_{kl} is positive, hence it follows that

$$|\alpha^\sigma|^l \leqslant \sum_{k=1}^m a_{kl}|\alpha_k^\sigma| < \sum_{k=1}^m a_{kl}\alpha_k\left(\frac{|\alpha^\sigma|}{\alpha}\right)^l = \alpha^l\left(\frac{|\alpha^\sigma|}{\alpha}\right)^l = |\alpha^\sigma|^l.$$

The obtained contradiction shows that $\alpha \geqslant |\alpha^\sigma|$ for all embeddings σ of $\mathbb{Q}(\alpha)$ into $\mathbb{C}$.

We proceed to prove the sufficiency of the condition. Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ be all the conjugates of α. Assume that α is an algebraic integer and $\alpha \geqslant |\alpha_i|$ $(1 \leqslant i \leqslant n)$. If $n = 1$, α clearly is a K-number. If $n > 1$, we have $\alpha \neq 1$ and since $\alpha < 1$ would imply

$$0 < \left|\prod_{i=1}^n \alpha_i\right| < 1,$$

which contradicts $\prod_{i=1}^n \alpha_i = N_{\mathbb{Q}(\alpha)/\mathbb{Q}}\alpha \in \mathbb{Z}$, we have $\alpha > 1$. By Lemma 5 there exist positive integers l and L such that for each $i \leqslant n$, (5) holds. Let $\beta = \alpha^l - L, \beta_2, \ldots, \beta_k$ be all conjugates of β different from it. By (5) we have

$$\beta > |\beta_j| \quad \text{and} \quad \Re\beta_j < 0 \qquad (2 \leqslant j \leqslant k).$$

We may assume without loss of generality that β_j is real for $j \leqslant r$, and complex for $r < j \leqslant r + 2s = k$, $\beta_{r+s+j} = \overline{\beta}_{r+j}$. By Lemma 3 there exists a $\nu \in \mathbb{N}$ such that

$$\Re\beta_j^\nu \leqslant \tfrac{1}{2}|\beta_j|^{\nu-1}\Re\beta_j < 0 \qquad (2 \leqslant j \leqslant k) \tag{6}$$

and, moreover,

$$\left(\frac{\beta}{\max\limits_{2\leqslant j\leqslant k}|\beta_j|}\right)^\nu \geqslant \sum_{j=1}^{r+s-1} \max\left\{2, \frac{|\beta_{j+1}|}{-\Re\beta_{j+1}}\right\}. \tag{7}$$

Now we apply Lemma 2 with $k_1 = r-1$, $k_2 = s$

$$\begin{aligned} f_j(x) &= x - \beta_{j+1}^\nu && (1 \leqslant j \leqslant r-1),\\ f_j(x) &= (x-\beta_{j+1}^\nu)(x-\beta_{j+s+1}^\nu)\\ &= \left(x^2 - 2\Re\beta_{j+1}^\nu x + |\beta_{j+1}|^{2\nu}\right) && (r \leqslant j \leqslant r+s-1). \end{aligned}$$

By (6), the assumptions of Lemma 2 are satisfied and we infer that

$$\prod_{j=1}^{r+s-1} f_j(x) = \sum_{\lambda=0}^{k-1} A_\lambda x^{k-1-\lambda},$$

where $A_0 = 1$ and for $\lambda < k-1$

$$0 < \frac{A_{\lambda+1}}{A_\lambda} \leqslant \sum_{j=1}^{r+s-1} \max\left\{-2\Re\beta_{j+1}^\nu, \frac{|\beta_{j+1}|^{2\nu}}{-2\Re\beta_{j+1}^\nu}\right\}. \tag{8}$$

However, by (6)

$$\max\left\{-2\Re\beta_{j+1}^\nu, \frac{|\beta_{j+1}|^{2\nu}}{-2\Re\beta_{j+1}^\nu}\right\} \leqslant |\beta_{j+1}|^\nu \max\left\{2, \frac{|\beta_{j+1}|}{-\Re\beta_{j+1}}\right\},$$

hence by (7) and (8)

$$0 < \frac{A_{\lambda+1}}{A_\lambda} \leqslant \beta^\nu.$$

It follows that all coefficients of the polynomial

$$F(x) = x^k - (x-\beta^\nu)\prod_{j=1}^{r+s-1} f_j(x) =: \sum_{j=0}^{k-1} c_j x^j$$

are nonnegative. On the other hand, since α is an algebraic integer, so is β^ν and

$$(x-\beta^\nu)\prod_{j=1}^{r+s-1} f_j(x) = N_{\mathbb{Q}(\beta,x)/\mathbb{Q}(x)}(x-\beta^\nu) \in \mathbb{Z}[x].$$

Therefore, $c_j \in \mathbb{N}_0 \quad (0 \leqslant j < k)$,

$$(\beta^v)^k = \sum_{j=0}^{k-1} c_j (\beta^v)^j. \tag{9}$$

We shall show that the vector

$$\langle 1, \alpha, \ldots, \alpha^{l-1}, \beta, \beta\alpha, \ldots, \beta\alpha^{l-1}, \ldots, \beta^{kv-1}, \beta^{kv-1}\alpha, \ldots, \beta^{kv-1}\alpha^{l-1}\rangle$$
$$=: \langle \gamma_1, \ldots, \gamma_{klv}\rangle$$

is a K-system. Indeed, we have by (9)

$$\alpha\gamma_i = \begin{cases} \gamma_{i+1} & \text{if } i \not\equiv 0 \bmod l, \\ L\gamma_{i-l+1} + \gamma_{i+l} & \text{if } i \equiv 0 \bmod l,\ i \neq klv, \\ L\gamma_{klv-l+1} + \sum\limits_{j=0}^{k-1} c_j \gamma_{jlv+1} & \text{if } i = klv; \end{cases}$$

$$\beta\gamma_i = \begin{cases} \gamma_{i+l} & \text{if } i \leqslant klv - l, \\ \sum\limits_{j=0}^{k-1} c_j \gamma_{jlv+l\{(i-1)/l\}+1} & \text{if } i > klv - l, \end{cases}$$

hence by induction on $i + j$:

$$\alpha^i\beta^j \text{ is a combination of } \gamma_p \text{ with coefficients in } \mathbb{N}_0 \text{ for all } i, j \in \mathbb{N}_0,$$

and thus $\gamma_i\gamma_j$ is such a combination for all $i, j \leqslant klv$. It follows that α is a K-number. □

Corollary 1. *If $\alpha \neq 0$ is a K-number, it is an element of a K-system consisting of elements of $\mathbb{Z}[\alpha]$.*

Proof. This follows from the construction of a K-system in the second part of the proof of Theorem. □

Corollary 2. *If α, β are K-numbers then $\mathbb{Q}(\alpha + \beta) = \mathbb{Q}(\alpha, \beta)$.*

Proof. Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ be all the conjugates of α, $\beta_1 = \beta, \beta_2, \ldots, \beta_p$ be all the conjugates of β. By the Theorem, $\alpha \geqslant |\alpha_i|$, $\beta \geqslant |\beta_j|$, hence if $\alpha + \beta = \alpha_i + \beta_j$, we have $|\alpha_i| = \alpha$, $|\beta_j| = \beta$. However, since α, β are real, we have also $\Re\alpha_i = \alpha$, $\Re\beta_j = \beta$, thus $\alpha_i = \alpha$, $\beta_j = \beta$. This shows that $[\mathbb{Q}(\alpha + \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$, and since $\alpha + \beta \in \mathbb{Q}(\alpha, \beta)$, it follows that $\mathbb{Q}(\alpha + \beta) = \mathbb{Q}(\alpha, \beta)$. □

Corollary 3. *If α, β are K-numbers and $\alpha\beta \in \mathbb{N}$, then there exists an $e \in \mathbb{N}$ such that $\alpha^e \in \mathbb{N}$, $\beta^e \in \mathbb{N}$.*

Proof. Since $\alpha\beta \in \mathbb{N}$, we have for every embedding σ of $\mathbb{Q}(\alpha, \beta)$ in $\mathbb{C}$: $\alpha^\sigma\beta^\sigma = \alpha\beta$, and because by the Theorem $\alpha \geqslant |\alpha^\sigma|$, $\beta \geqslant |\beta^\sigma|$, it follows that $\alpha = |\alpha^\sigma|$, $\beta = |\beta^\sigma|$. By Lemma 4 there exists an exponent $e \in \mathbb{N}$ such that $\alpha^e = |\alpha^\sigma|^e$ implies $\alpha^e = (\alpha^e)^\sigma$, and

$\beta^e = |\beta^\sigma|^e$ implies $\beta^e = (\beta^e)^\sigma$. Hence $\alpha^e \in \mathbb{Q}$, $\beta^e \in \mathbb{Q}$ and since α, β are positive algebraic integers, $\mathbb{Q}$ can be replaced by $\mathbb{N}$. □

Remark. Corollaries 2 and 3 establish the conjectures made by Korec (cf. [3]).

References

[1] D. W. Boyd, *Irreducible polynomials with many roots of maximal modulus*. Acta Arith. 68 (1994), 85–88.

[2] I. Korec, *Irrational speeds of configuration growth in generalized Pascal triangles*. Theoret. Comput. Sci. 112 (1993), 399–412.

[3] —, *Open problems more or less related to generalized Pascal triangles*. Preprint, June 1995.

Andrzej Schinzel
Selecta

Originally published in
Acta Arithmetica 113 (2004), 401–408

On values of the Mahler measure in a quadratic field (solution of a problem of Dixon and Dubickas)

To Robert Tijdeman at the occasion of his 60th birthday

For an algebraic number α, let $M(\alpha)$ be the Mahler measure of α and let $\mathcal{M} = \{M(\alpha) \mid \alpha \in \overline{\mathbb{Q}}\}$. No method is known to decide whether a given algebraic integer β is in $\mathcal{M}$. Partial results have been obtained by Adler and Marcus [1], Boyd [2]–[4], Dubickas [6]–[8] and Dixon and Dubickas [5], but the problem has not been solved even for β of degree two. The following theorem, similar to, but not identical with Theorem 9 of [5], is an easy consequence of [7].

Theorem 1. *A primitive real quadratic integer β is in $\mathcal{M}$ if and only if there exists a rational integer a such that $\beta > a > |\beta'|$ and $a \mid \beta\beta'$, where β' is the conjugate of β. If the condition is satisfied, then $\beta = M(\beta/a)$ and $a = N(a, \beta)$, where N denotes the absolute norm.*

There remain to be considered quadratic integers that are not primitive. The following theorem deals with the simplest class of such numbers.

Theorem 2. *Let K be a quadratic field with discriminant $\Delta > 0$, β, β' be conjugate primitive integers of K and p a prime. If*

$$p\beta \in \mathcal{M}, \tag{1}$$

then either there exists an integer r such that

$$p\beta > r > p\left|\beta'\right| \quad \text{and} \quad r \mid \beta\beta', \ p \nmid r \tag{2}$$

or

$$\beta \in \mathcal{M} \quad \text{and} \quad p \text{ splits in } K. \tag{3}$$

Conversely (2) *implies* (1)*, while* (3) *implies* (1) *provided either*

$$\beta > \max\left\{-4\beta', \left(\frac{1+\sqrt{\Delta}}{4}\right)^2\right\} \tag{4}$$

or

$$p > \sqrt{\Delta}. \tag{5}$$

Remark 1. (2) implies $\beta > p\beta|\beta'|/r \geqslant p$.

Theorem 2 answers two questions raised in [5].

Corollary 1. *For all primes p we have $p\frac{3+\sqrt{5}}{2} \in \mathcal{M}$ if and only if either $p = 2$, or $p = 5$, or $p \equiv \pm 1 \pmod 5$.*

Corollary 2. *For every real quadratic field K there is an irreducible polynomial $f \in \mathbb{Z}[x]$, basal in the sense of* [5]*, such that $M(f) \in K$, but the zeros of f do not lie in K.*

Corollary 3. *In every real quadratic field K there are only finitely many integers $p\beta$, where p is prime, while β is primitive and totally positive, for which the condition $p\beta \in \mathcal{M}$ is not equivalent to the alternative of* (2) *and* (3)*.*

Proof of Theorem 1. *Necessity.* Let $\beta = M(\alpha)$, let f be the minimal polynomial of α over $\mathbb{Z}$, $a > 0$ its leading coefficient, D its degree, and $\alpha_1, \ldots, \alpha_D$ all its zeros. By Lemma 2 of [7] applied with $d = 2$,

$$\beta\beta' = a^2 \prod_{i=1}^{D} \alpha_i = (-1)^D a f(0). \tag{6}$$

Moreover, by formula (3) of [7], $D = 2s$, where s is the number of $i \leqslant D$ with $|\alpha_i| > 1$. Without loss of generality we may assume that $|\alpha_i| > 1$ precisely for $i \leqslant s$. For some $\eta \in \{1, -1\}$ we have

$$\prod_{i=1}^{s} \alpha_i = \eta\beta/a, \tag{7}$$

hence, by (6),

$$\prod_{i=s+1}^{D} \alpha_i = \eta\beta'/a, \tag{8}$$

which gives

$$\beta > a > \left|\beta'\right|. \tag{9}$$

Also, by (6),

$$a \mid \beta\beta'. \tag{10}$$

Sufficiency. Assume the existence of an integer a satisfying (9) and (10) and consider the polynomial

$$g(x) = ax^2 - (\beta + \beta')x + \beta\beta'/a.$$

If g is not primitive, there exists a prime p such that $p \mid a$, $p \mid \beta + \beta'$ and $p \mid \beta\beta'/a$. However, then $p^2 \mid \beta\beta'$ and β/p is a zero of the polynomial $x^2 - \frac{\beta+\beta'}{p}x + \frac{\beta\beta'}{p^2}$ belonging to $\mathbb{Z}[x]$,

contrary to the assumption that β is primitive. Therefore, g is the minimal polynomial of β/a over $\mathbb{Z}$ and $\beta = M(\beta/a)$. Also,

$$(a) \mid (a^2, a\beta, a\beta', \beta\beta') \mid (a^2, a(\beta+\beta'), \beta\beta') = (a),$$

hence

$$(a) = (a^2, a\beta, a\beta', \beta\beta') = (a, \beta)(a, \beta'). \qquad \square$$

The proof of Theorem 2 is based on three lemmas.

Lemma 1. *If an integer β of K is the Mahler measure of an algebraic number whose minimal polynomial over $\mathbb{Z}$ has leading coefficient a, then a is the norm of an ideal of K.*

Proof. In the notation of the proof of Theorem 1 (necessity part) we have (7) and (8). Since $\eta\beta'/a$ is the only conjugate of $\eta\beta/a$, every automorphism of the splitting field of f that sends an α_i $(i \leqslant s)$ to an α_j $(j > s)$ sends the set $\{\alpha_1, \ldots, \alpha_s\}$ onto $\{\alpha_{s+1}, \ldots, \alpha_D\}$ (compare the proof of Lemma 2 in [7]). Hence $\{\alpha_1, \ldots, \alpha_s\}$ and $\{\alpha_{s+1}, \ldots, \alpha_D\}$ are blocks of imprimitivity of the Galois group of f and the coefficients of the polynomials

$$P(x) = \prod_{i=1}^{s}(x - \alpha_i), \quad P'(x) = \prod_{i=s+1}^{D}(x - \alpha_i)$$

belong to a quadratic field, which clearly is K. Let the contents of P and P' be $\mathfrak{a}^{-1}$ and $\mathfrak{a}'^{-1}$, where $\mathfrak{a}$ and $\mathfrak{a}'$ are conjugate ideals of K. Since f is primitive, we have

$$(1) = \operatorname{cont} f = \operatorname{cont}(aPP') = (a)/\mathfrak{a}\mathfrak{a}'$$

and, since $a > 0$, $a = N\mathfrak{a}$. $\square$

Lemma 2. *If the dash denotes conjugation in K, δ, ε are elements of K such that*

$$\delta > 1 > \delta' > -1/2, \tag{11}$$

$$(1, \delta) \mid \varepsilon, \quad \varepsilon \neq \varepsilon', \tag{12}$$

$$|\varepsilon - \varepsilon'| + 1 < 4\sqrt{\delta}, \tag{13}$$

while $\mathfrak{p}$ is an ideal of K, then there exists $\gamma \in K$ such that

$$(1, \gamma, \delta) = \frac{(1, \delta)}{\mathfrak{p}}, \tag{14}$$

$$|\gamma| < 2\sqrt{\delta}, \ |\gamma'| < 1 + \delta'. \tag{15}$$

Proof. Take an integer α of K divisible by $\mathfrak{p}(1, \delta)^{-1}$. Applying Theorem 74 of [9] with

$$\mathfrak{a} = \frac{(\alpha)(1, \delta)}{\mathfrak{p}}, \quad \mathfrak{b} = \frac{\mathfrak{p}}{(1, \delta)}$$

we find an integer ω of K, such that $(\alpha, \omega) = \mathfrak{a}$, hence

$$\left(1, \frac{\omega}{\alpha}\right) = \frac{(1, \delta)}{\mathfrak{p}}. \tag{16}$$

Taking

$$b = \left\lfloor \left(\frac{\omega}{\alpha} - \frac{\omega'}{\alpha'}\right)/(\varepsilon - \varepsilon') + \frac{1}{2} \right\rfloor, \quad a = \left\lfloor \frac{\omega'}{\alpha'} - b\varepsilon' + \frac{1}{2} \right\rfloor$$

we find

$$\left|\frac{\omega}{\alpha} - \frac{\omega'}{\alpha'} - b(\varepsilon - \varepsilon')\right| \leqslant \frac{|\varepsilon - \varepsilon'|}{2}, \quad \left|\frac{\omega'}{\alpha'} - a - b\varepsilon'\right| \leqslant \frac{1}{2} < 1 + \delta', \tag{17}$$

hence on addition, by (13),

$$\left|\frac{\omega}{\alpha} - a - b\varepsilon\right| \leqslant \frac{|\varepsilon - \varepsilon'|}{2} + \frac{1}{2} < 2\sqrt{\delta} \tag{18}$$

and for $\gamma = \omega/\alpha - a - b\varepsilon$, (14) follows from (16), while (15) from (17) and (18). □

Lemma 3. *If, in the notation of Lemma* 2, $\mathfrak{p}$ *is a prime ideal dividing a rational prime* p, *then the conclusion of the lemma holds, provided*

$$p > \frac{N(1,\delta)\sqrt{\Delta}}{\min\{N(1,\delta), 2\sqrt{\delta}(1+\delta')\}}. \tag{19}$$

Proof. Let the ideal $(1, \delta)$ considered as a module over $\mathbb{Z}$ have the basis $[\eta, \zeta]$. The system of inequalities

$$|c| < p, \quad \left|c\,\frac{\omega}{\alpha} - a\eta - b\zeta\right| < 2\sqrt{\delta}, \quad \left|c\,\frac{\omega'}{\alpha'} - a\eta' - b\zeta'\right| < \min\left\{\frac{N(1,\delta)}{2\sqrt{\delta}}, 1 + \delta'\right\}$$

has a non-zero integer solution by Minkowski's theorem (Theorem 94 of [9]), since by Theorem 76 of [9], which applies also to fractional ideals (see §31, formula (47))

$$|\eta\zeta' - \eta'\zeta| = N(1,\delta)\sqrt{\Delta} < \min\{N(1,\delta), 2\sqrt{\delta}(1+\delta')\}p.$$

If in this solution we had $c = 0$ it would follow that $a\eta + b\zeta \neq 0$ and

$$N(1,\delta) \leqslant |N(a\eta + b\zeta)| < 2\sqrt{\delta}\,\frac{N(1,\delta)}{2\sqrt{\delta}} = N(1,\delta),$$

a contradiction. Therefore $c \neq 0$, $c \not\equiv 0 \pmod{\mathfrak{p}}$ and $\gamma = c\frac{\omega}{\alpha} - a\eta - b\zeta$ has the required properties. □

Proof of Theorem 2. Assume first that (1) holds and let f be the minimal polynomial of α over $\mathbb{Z}$, $a > 0$ its leading coefficient, and D its degree. By (6) and (7) with β replaced by $p\beta$, we have

$$p^2\beta\beta' = (-1)^D a f(0), \tag{20}$$

$$p\beta > \max\{a, |f(0)|\} \geqslant \min\{a, |f(0)|\} > p|\beta'|. \tag{21}$$

Let $p^\mu \parallel a$, $p^\nu \parallel \beta\beta'$. If $\mu = 0$ or $\mu = \nu + 2$, then (2) follows with $r = a$ or $r = |f(0)|$, respectively. Therefore, assume

$$1 \leqslant \mu \leqslant \nu + 1. \tag{22}$$

Let $a = p^{\mu}b$. By (20) and (22),

$$p^{\mu-1}b \mid \beta\beta',$$

while by (21),

$$\beta > p^{\mu-1}b > |\beta'|.$$

By Theorem 1 we have $\beta \in \mathcal{M}$. If $\nu > 0$, then $p \mid \beta\beta'$ and since β is primitive, p splits in K. If $\nu = 0$ we have, by (22), $\mu = 1$ and since, by Lemma 1, a is the norm of an ideal of K, p splits in K. This proves (3).

In the opposite direction, (2) implies $p\beta = M(p\beta/r) \in \mathcal{M}$. Indeed, the minimal polynomial of $p\beta/r$ is $rx^2 - p(\beta+\beta')x + \beta\beta'/r$, where $(r, \beta+\beta', \beta\beta'/r) = 1$, since β is primitive (see the proof of Theorem 1). Assume now that (3) holds. By Theorem 1 we have $\beta = M(\beta/b)$, where

$$b \in \mathbb{N}, \quad \beta > b > |\beta'|, \quad b = N(b, \beta). \tag{23}$$

Replacing b by $\beta|\beta'|/b$, if necessary, we may assume

$$b \geqslant \sqrt{\beta|\beta'|}. \tag{24}$$

First, assume (4). Since β is primitive all prime ideal factors of (b, β) are of degree one and no two of them are conjugate. Hence there exists $c \in \mathbb{Z}$ such that

$$\omega := \frac{\Delta + \sqrt{\Delta}}{2} \equiv -c \pmod{(b, \beta)}. \tag{25}$$

We put $\delta = \beta/b$, $\varepsilon = (c+\omega)/b$. In order to apply Lemma 2 we have to check the assumptions. Now, (11) follows from (23), (24) and $\beta > -4\beta'$, (12) follows from (25), and (13) is equivalent to the inequality

$$\sqrt{\Delta}/\sqrt{b} + \sqrt{b} < 4\sqrt{\beta}.$$

The left hand side considered as a function of b on the interval $[1, \beta]$ takes its maximum at an end of the interval. We have $\sqrt{\Delta} + 1 < 4\sqrt{\beta}$ by (4) and $\sqrt{\Delta}/\sqrt{\beta} + \sqrt{\beta} < 4\sqrt{\beta}$ since $\beta \geqslant (1 + \sqrt{\Delta})/2$.

The assumptions of Lemma 2 being satisfied there exists $\gamma \in K$ such that

$$(1, \gamma, \delta) = \frac{(b, \beta)}{(b)\mathfrak{p}} = \frac{1}{(b, \beta')\mathfrak{p}}, \quad |\gamma| < 2\sqrt{\delta}, \quad |\gamma'| < 1 + \delta'. \tag{26}$$

Let us consider the polynomial

$$P(x) = x^2 + \gamma x + \delta.$$

The discriminant of P, $\gamma^2 - 4\delta$, is negative, hence P is irreducible over the real field K, moreover its zeros are equal to $\sqrt{\delta} > 1$ in absolute value. On the other hand, the zeros of the polynomial

$$P'(x) = x^2 + \gamma' x + \delta'$$

are less than 1 in absolute value. This is clear if $\gamma'^2 - 4\delta' < 0$, since $|\delta'| < 1$ and if $\gamma'^2 - 4\delta' \geqslant 0$ the inequality

$$\frac{|\gamma'| + \sqrt{\gamma'^2 - 4\delta'}}{2} < 1$$

follows from the condition $|\gamma'| < 1 + \delta'$. Taking for α a zero of P we obtain, by (23) and (26),

$$M(\alpha) = \frac{M(PP')}{N \operatorname{cont} P} = \delta N(b, \beta') N\mathfrak{p} = \frac{\beta}{b} \cdot bp = p\beta.$$

Now, assume (5) and let again $\delta = \beta/b$. In order to apply Lemma 3 we have to check (19).

Consider first the case

$$\beta \notin \left\{ \frac{1 + \sqrt{4e+1}}{2} : e \in \mathbb{N} \right\}. \tag{27}$$

Then

$$\beta - |\beta'| \geqslant 2, \quad \beta \geqslant 1 + \sqrt{2} \tag{28}$$

and by (24),

$$R := \frac{2\sqrt{\delta}(1+\delta')}{N(1,\delta)} = 2\sqrt{\frac{\beta}{b}}\,(b + \beta') \geqslant 2\sqrt{\beta}\big(\sqrt[4]{\beta|\beta'|} + \operatorname{sgn}\beta' \sqrt[4]{|\beta'|^3/\beta}\big).$$

If $\beta' > 0$ we clearly have $R > 1$, if $\beta' < 0$ we have, by (26),

$$R = 2\sqrt[4]{\beta|\beta'|}\big(\sqrt{\beta} - \sqrt{|\beta'|}\big) \geqslant 4\sqrt[4]{\beta|\beta'|}/\big(\sqrt{\beta} + \sqrt{|\beta'|}\big).$$

If $\sqrt{|\beta'|} \leqslant \frac{1}{2}\sqrt{\beta}$, it follows that

$$R \geqslant \sqrt[4]{\beta|\beta'|}\sqrt{\beta} > 1,$$

while if $\sqrt{|\beta'|} > \frac{1}{2}\sqrt{\beta}$, it follows that

$$R > \frac{4}{\sqrt{2}} \frac{\sqrt{\beta}}{2\sqrt{\beta}} = \sqrt{2} > 1;$$

thus (27) implies

$$\min\big\{N(1,\delta), 2\sqrt{\delta}(1+\delta')\big\} = N(1,\delta)$$

and (19) follows from (5).

Consider now the case

$$\beta = \frac{1 + \sqrt{4e+1}}{2}.$$

By (23), $b^2 + b > e > b^2 - b$, $b \mid e$, which implies $e = b^2$. On the other hand, $4e+1 = f^2\Delta$

for some $f \in \mathbb{N}$. The inequality

$$p > \sqrt{\Delta} = \frac{\sqrt{4b^2+1}}{f}$$

implies by a tedious computation

$$p \geqslant \frac{2b+1}{f} > \frac{\sqrt{\Delta}}{2\sqrt{\frac{\beta}{b}}(b+\beta')} = \frac{N(1,\delta)\sqrt{\Delta}}{\min\{N(1,\delta), 2\sqrt{\delta}(1+\delta')\}},$$

hence (19) holds.

The assumptions of Lemma 3 being satisfied there exists $\gamma \in K$ satisfying (26) and arguing as before we obtain

$$p\beta = M(\alpha),$$

where α is a zero of $x^2 + \gamma x + \delta$. □

Proof of Corollary 1. For $\beta = (3+\sqrt{5})/2$ the condition (4) is satisfied. Now, (2) is fulfilled by $p = 2$ only, and (3) is fulfilled by $p = 5$ and $p \equiv \pm 1 \pmod 5$ only. □

Proof of Corollary 2. Take a totally positive unit $\varepsilon > 1$ of K and a prime $p > \varepsilon$ that splits in K. Then by Theorem 2, $p\varepsilon \in \mathcal{M}$. Assume that the basal irreducible polynomial f of $p\varepsilon$ has all its zeros in K. Hence

$$f(x) = a\Big(x \pm \frac{p\varepsilon}{a}\Big)\Big(x \pm \frac{p\varepsilon'}{a}\Big), \quad p\varepsilon > a > p\varepsilon', \quad a \in \mathbb{N}$$

and the condition $p^2/a \in \mathbb{Z}$ together with $p > \varepsilon$ imply $a = p$. However, for $a = p$, f is not primitive. □

Example 1. For $K = \mathbb{Q}(\sqrt{2})$ we can take

$$p\varepsilon = 21 + 14\sqrt{2} = M(7x^4 + 2x^3 + 41x^2 + 22x + 7).$$

Proof of Corollary 3. There are only finitely many totally positive integers β of K, which are Perron numbers, but do not satisfy (4). □

Remark 2. By a more complicated argument one can show that for β totally positive, (3) implies (1) unless

$$\sqrt[4]{N\beta} + \frac{\sqrt{\Delta}}{\sqrt[4]{N\beta}} \geqslant 4\sqrt{\beta} \quad \text{and} \quad p < 1 + \frac{1}{2\sqrt{\beta}}\Big(\sqrt[4]{N\beta} + \frac{\sqrt{\Delta}}{\sqrt[4]{N\beta}}\Big).$$

Example 2. Theorem 2 does not allow us to decide whether $1 + \sqrt{17} \in \mathcal{M}$. This question is open, as is a more general question, whether (3) implies (1).

References

[1] R. L. Adler, B. Marcus, *Topological entropy and equivalence of dynamical systems*. Mem. Amer. Math. Soc. 20 (1979), no. 219.

[2] D. W. Boyd, *Inverse problems for Mahler's measure*. In: Diophantine Analysis (ed. J. H. Loxton and A. J. van der Poorten), London Math. Soc. Lecture Note Ser. 109, Cambridge Univ. Press, Cambridge 1986, 147–158.

[3] —, *Perron units which are not Mahler measures*. Ergodic Theory Dynam. Systems 6 (1986), 485–488.

[4] —, *Reciprocal algebraic integers whose Mahler measures are non-reciprocal*. Canad. Math. Bull. 30 (1987), 3–8.

[5] J. D. Dixon, A. Dubickas, *The values of Mahler measures*. Mathematika 51 (2004), 131–148.

[6] A. Dubickas, *Mahler measures close to an integer*. Canad. Math. Bull. 45 (2002), 196–203.

[7] —, *On numbers which are Mahler measures*. Monatsh. Math. 141 (2004), 119–126.

[8] —, *Mahler measures generate the largest possible groups*. Math. Res. Lett. 11 (2004), 279–283.

[9] E. Hecke, *Lectures on the Theory of Algebraic Numbers*. Springer, New York–Berlin 1981.

Part D

Polynomials in one variable

Commentary on D: Polynomials in one variable

by Michael Filaseta

D1. If $q_0 = (1+\sqrt{5})/2$, then $1, q_0^2$ and q_0^3 form a three term arithmetic progression. K. Zarankiewicz posed the problem of determining whether an irrational number q exists such that the infinite sequence $1, q, q^2, q^3, \ldots$ contains four numbers that are in arithmetic progression. In this paper, Schinzel resolves the problem by showing that for any complex number q, if four numbers from the sequence $1, q, q^2, q^3, \ldots$ are in arithmetic progression, then the four numbers are equal and are either all 0 or a root of unity.

The problem of Zarankiewicz can be found, for example, in [43].

For integers a, b and c satisfying $0 \leqslant a < b < c$ and $q \neq 0$, observe that q^a, q^b and q^c are in arithmetic progression precisely when q is a root of $x^{c-a} - 2x^{b-a} + 1$. Schinzel consequently looks at the factorization of $f(x) = x^n - 2x^m + 1$. It is not difficult to see that both α and $1/\alpha$ are roots of $f(x)$ if and only if α is a root of $x^d - 1$ where $d = \gcd(n, m)$. A method of W. Ljunggren in [23] then applies to determine the factorization of $f(x)/(x^d - 1)$. Schinzel thus obtains the factorization of $f(x)/(x^d - 1)$ given in Theorem 1.

The factorization of $f(x)/(x^d - 1)$, as described above, is of significance to the problem of Zarankiewicz as whenever q^a, q^b, q^c and q^d (with $0 \leqslant a < b < c < d$ integers) form a four term arithmetic progression and $q \neq 0$, the number q must simultaneously be a root of $x^{c-a} - 2x^{b-a} + 1$ and $x^{d-b} - 2x^{c-b} + 1$. Knowing the factorization of $f(x)/(x^d - 1)$ allows Schinzel to determine the precise value of $\gcd\left(x^{c-a} - 2x^{b-a} + 1, x^{d-b} - 2x^{c-b} + 1\right)$. In particular, if q is a root of unity, then $q^{c-a} = q^{b-a} = q^{d-b} = q^{c-b} = 1$ and, consequently $q^a = q^b = q^c = q^d$. If, on the other hand, q is not a root of unity, then one is led to a contradiction as a, b, c and d will not themselves form a four term arithmetic progression and Theorem 2 implies the only common roots of $x^{c-a} - 2x^{b-a} + 1$ and $x^{d-b} - 2x^{c-b} + 1$ are $\gcd(c-a, b-a, d-b, c-b)$ roots of unity.

D2. This paper sets a foundation for future investigations done by Schinzel, in particular for his work on trinomials and his sequence of papers on the reducibility of lacunary polynomials. The paper is an initial attempt at describing effectively the canonical factorization of polynomials with fixed coefficients and variable exponents by associating each factorization with a corresponding factorization of a polynomial from a finite list of polynomials in several variables. The canonical factorization is not of the polynomials

themselves but rather come in two forms. Underlying the literature on this subject and the forms of the canonical factorizations obtained is some important notation. These are explained thoroughly in Schinzel's own work. In particular, the reader can consult **D4** or Schinzel's book [37]. A brief, but not completely adequate, explanation is that KF denotes the polynomial F with every (multivariate) cyclotomic factor removed, and LF denotes the polynomial F with every (multivariate) self-inverse factor removed. The polynomials KF and LF should also be normalized to have the same leading coefficient as F. This paper concerns the canonical factorization of KF which in its most general form has proved to be more difficult to handle than the canonical factorization of LF. The latter is given a satisfactory answer by Schinzel in **D4**; the former is not given a satisfactory answer until 30 years later, with additional assumptions, in **D12**.

The paper contains a conjecture concerning the factorization of KF which motivates much of Schinzel's later work on the reducibility of lacunary polynomials. The present paper gives a partial answer to the conjecture in the case that the number of variables involved is $\leqslant 2$ and the polynomials considered are over the field of rational numbers. This leads to an application to the factorization of $K(ax^n+bx^m+c)$, that is a determination of how ax^n+bx^m+c factors after its cyclotomic factors are removed. In addition, Schinzel describes the cyclotomic factors of the trinomials ax^n+bx^m+c. As indicated, **D2** considers the case where the coefficients of the polynomials are fixed and the exponents are variable. The reverse situation, with fixed exponents and variable coefficients, is considered in later papers; in particular, the factorization of trinomials in this manner is done rather thoroughly in his works **D10**, **D13**, **D14**.

Theorem 5 is a consequence of the main result in the paper combined with Capelli's theorem and gives information about the factorization of polynomials of the form $x^n+f(x)$, which later played a crucial role in his finding a connection between the factorization of $x^n + f(x)$ and covering systems of congruences in **D3**. An alternative approach for establishing Theorem 5 has been found by M. Filaseta, K. Ford and S. Konyagin in [14].

D3. Using the notation of $D_0(f)$ and e_0 (later below) as given in Lemma 4, one can extend Theorem 1 to include the additional equivalent statement:

A′. *For every polynomial $f(x)$ with integer coefficients such that $f(0) \neq 0$, $f(1) \neq -1$ and $f(x) \neq 1$, there exists an integer $n > \max\{D_0(f), \deg f\}$ such that $x^n + f(x)$ is irreducible over the rationals.*

In other words, each of A, A′ and B are equivalent. To see this, note that A clearly implies A′ so that, by Theorem 1, one needs only show that A′ implies A. Suppose then that A′ holds. Fix $f(x)$ and n as in A′. The proof that B implies A begins by showing that the conditions in A must hold if $f(x)$ is of the form $4h(x)^4$. Therefore, we consider only the case that $f(x)$ is not of this form. Furthermore, we define the set M as in the sentence containing the display (31). As noted M is finite. We take M' to be the product of all μ where $(\mu, \alpha) \in M$. In particular, for all positive integers m and m', if $\zeta_{m'}$ is a root of $x^m + f(x)$, then m' divides M'. We consider two cases depending on whether $(n, e_0) = 1$ or $(n, e_0) \neq 1$.

If $(n, e_0) = 1$, we appeal to Lemma 4. As both $x^n + f(x)$ and $K(x^n + f(x))$ are irreducible, we deduce that $x^n + f(x) = K(x^n + f(x))$. In particular, $x^n + f(x)$ cannot

have a cyclotomic factor. For any positive integer t, we deduce that $x^{n+tM'e_0} + f(x)$ does not have a cyclotomic factor. Hence, Lemma 4 implies that $x^{n+tM'e_0} + f(x)$ is irreducible for every positive integer t, and A follows.

In the case that $(n, e_0) \neq 1$, we obtain a contradiction by showing that in fact $x^n + f(x)$ is reducible. As $e_0 \neq 1$, there is a prime p dividing e_0 and we can write $f(x) = -w_0(x)^p$ for some polynomial $w_0(x) \in \mathbb{Z}[x]$. Further, $n = pv$ for some positive integer v. Thus, $x^n + f(x)$ can be written as a product of $x^v - w_0(x)$ and

$$w_1(x) = x^{(p-1)v} + x^{(p-2)v} w_0(x) + \ldots + x^v w_0(x)^{p-2} + w_0(x)^{p-1}.$$

As $pv = n > \deg f = p \cdot \deg w_0$, we see that $\deg(x^v - w_0(x)) > 0$. On the other hand, if $\deg w_1 = 0$, then there is a constant $c \in \mathbb{Z}$ such that

$$x^{pv} - w_0(x)^p = c\big(x^v - w_0(x)\big),$$

which implies $\deg w_0 = v$ and $w_0(x)$ is monic. Setting $d = \deg(x^v - w_0(x))$, we see that the left side above has degree $(p-1)v + d$ and the right side has degree d. This leads to $v = 0$ and $w_0(x) = 1$, contradicting that $f(1) \neq -1$. This completes the argument that A′ can be added as an additional equivalence in Theorem 1.

The odd covering problem, that is the problem of finding a finite covering system of the integers consisting of distinct odd moduli > 1, goes back over 40 years and has an interesting history. P. Erdős and J. Selfridge after discussing the problem had different opinions about whether such a covering should exist. Erdős felt that such a covering probably does exist and offered \$25 to anyone who could prove him wrong, that is for a proof that no such covering exists. Selfridge thought (at the time) that no such covering exists and offered \$300 for an explicit example of such an odd covering (an example that would demonstrate that he was wrong). No monetary award was offered for a non-constructive proof that there is an odd covering. Selfridge over the years raised the amount he was willing to give for an explicit example of an odd covering. In an email message dated November 16, 1998, to M. Filaseta, Selfridge raised the offer to \$2000. The problem remains open.

Turán's conjecture, as mentioned in the introduction, is to show that for every polynomial $f(x) \in \mathbb{Z}[x]$, there is a polynomial $g(x) \in \mathbb{Z}[x]$ which is irreducible over the rationals, satisfies $\deg g \leqslant \deg f$, and is close to $f(x)$ in the sense that the sum of the absolute values of the coefficients of $f(x) - g(x)$ is bounded by an absolute constant, say C. This form of the conjecture remains open. However, in **D5**, Schinzel shows the existence of such a $g(x)$ with $C = 3$ provided one removes the requirement that $\deg g \leqslant \deg f$. A natural first attempt at constructing such a $g(x)$ is to consider the polynomials of the form $x^n + f(x)$ or of the form $x^n + f(x) \pm 1$ with the hope of possibly showing that one of these must always satisfy the requirements imposed on $g(x)$. The present paper shows that if one can get away with taking $g(x)$ in one of these forms, even without the requirement that $\deg g \leqslant \deg f$, then condition B in Theorem 1 holds and that this in turn implies that there is an odd covering of the integers. Given the long history with the odd covering problem, this paper speaks to the difficulty of one likely being able to determine if $g(x)$ can be taken to be of one of the forms $x^n + f(x)$ and $x^n + f(x) \pm 1$.

With the requirement that $\deg g \leqslant \deg f$, Turán's conjecture has been verified with $C = 4$ for all polynomials $f(x) \in \mathbb{Z}[x]$ of degree $\leqslant 24$ by A. Bérczes and L. Hajdu in the two papers [2] and [3].

The example at the beginning of the paper of an $f_0(x) \in \mathbb{Q}[x]$ for which $x^n + f_0(x)$ has a cyclotomic factor for every positive integer n can be demonstrated by considering when each of the cyclotomic polynomials $\Phi_m(x)$ divides $f_0(x)$ where m runs through the divisors > 1 of 12. This example was already noted in **D2**. Here, $12 f_0(x) \in \mathbb{Z}[x]$. A similar example, say $f_1(x)$, with different cyclotomic factors, is shown to exist with $4 f_1(x) \in \mathbb{Z}[x]$ by M. Filaseta in [13]. There one can also find a different exposition of the connection between the irreducibility of $x^n + f(x)$ and the odd covering problem.

Schinzel's problem suggested by D in this paper, to determine whether in every finite covering system there must exist two distinct moduli m and n with m dividing n, has become a popular open problem associated with finite covering systems; see, for example, Richard Guy's book [19], Section F13 (this is an expanded third edition, but the problem appears in the same section in the second edition).

The paper ends with a comment that Selfridge had an argument for C implying D. We note that this is fairly simple. Suppose $a_j \pmod{m_j}$, for $j = 1, 2, \ldots, r$, is a finite covering system that does not satisfy the conditions in D. Write $m_j = 2^{e_j} m'_j$ with m'_j odd. Then the m'_j are distinct (otherwise, some modulus would divide another). It follows that either $a_j \pmod{m'_j}$, for $j = 1, 2, \ldots, r$, is a finite odd covering of the integers with moduli > 1, and C does not hold, or for some j, we have $m'_j = 1$ and $e_j \geqslant 1$. In the latter case, we may suppose $j = 1$. Then we claim $a_j \pmod{m'_j}$, for $j = 2, \ldots, r$, is a finite odd covering of the integers with moduli > 1. Indeed, if $x \equiv a_1 \pmod{m_1}$, then $x + m'_2 \cdots m'_r \not\equiv a_1 \pmod{m_1}$ which implies there must be some $j \in \{2, \ldots, r\}$ such that $x \equiv x + m'_2 \cdots m'_r \equiv a_j \pmod{m'_j}$.

D4, **D6**. To put this work in perspective, consider that there was at the time a bit of literature concerning classes of lacunary polynomials having a few prescribed coefficients for which the factorization was rather well understood. More than a decade earlier, E. S. Selmer in [42] established that $x^n - x - 1$ is irreducible for all integers $n > 1$ and that $x^n + x + 1$ is irreducible for $n \geqslant 1$ unless $n > 2$ and $n \equiv 2 \pmod 3$ (when it is divisible by $x^2 + x + 1$). Shortly afterwards, H. Tverberg in [46] generalized the approach of Selmer to handle the factorization of polynomials of the more general form $x^n \pm x^m \pm 1$; and at the same time, W. Ljunggren in [23] worked out an elegant approach to determine the factorization of polynomials of the form $x^n \pm x^m \pm 1$ and $x^n \pm x^m \pm x^k \pm 1$. Later, in [24], Ljunggren also determined with the same method the factorization of $x^n \pm x^m \pm x^k \pm p$, where p is an arbitrary prime. In particular, in each case, the polynomial is irreducible unless it has a cyclotomic factor. Schinzel **D1** himself had already taken advantage of Ljunggren's approach to obtain information about the factorization of $x^n - 2x^m + 1$, and A. T. Jonassen [22] had applied Ljunggren's approach to the trinomials $x^n \pm x^m \pm 4$. We note that some time later, W. H. Mills in [26] observed that although Ljunggren's approach was correct, the paper that developed the approach had an error. Ljunggren incorrectly claimed that a quadrinomial $x^n \pm x^m \pm x^k \pm 1$ removed of its cyclotomic factors is either 1 or irreducible. Mills himself used Ljunggren's approach to obtain a correct result, classifying

the cases where the quadrinomials removed of their cyclotomic factors are reducible. Also, later, M. Filaseta and I. Solan in [17] pointed out Ljunggren's approach easily applies to the quintics $f(x) = x^n + x^m + x^k + x^\ell + 1$ allowing one to show that Lf, in the notation of **D4**, is always 1 or irreducible in this case. The ability to determine when particular classes of polynomials, containing fixed coefficients and variable exponents, are reducible was underway at the time of Schinzel's work in **D4**, but only with regard to specific cases where the coefficients were few and small in absolute value.

This remarkable paper of Schinzel's went far beyond what was done in the above papers and got to the core of these investigations. By taking, for example, $F(x_1, x_2, \ldots, x_k) = a_0 + a_1x_1 + \ldots + a_kx_k$ in Theorem 2 in **D4**, where $a_0, a_1, \ldots, a_k$ are arbitrary fixed non-zero integers, one can effectively determine a precise classification of the positive integers $n_1 < \ldots < n_k$ for which Lf is reducible and, in these cases, the factorization of Lf into a product of irreducibles, where $f(x) = \sum_{j=0}^{k} a_j x^{n_j}$. Thus, in theory, any result similar to the above stated theorems can be obtained, at least when dealing with the factorization of Lf. Some of the results above address instead the issue of factoring Kf, but a look at these results shows that in those instances it is not difficult to analyze the contribution cyclotomic factors make to the factorization of f. Indeed, in those instances, one can deduce the cyclotomic factors through consideration of $f(x) - x^{n_k} f(1/x)$. In general, it is more difficult to obtain information about the factorization of Kf. For a different approach to obtaining the above consequence of Theorem 2 see [12].

Note that the interesting corollary to Theorem 2 in **D4** is improved in a later paper by Schinzel on the subject, specifically in the corollary to Lemma 1 in **D7**. Further investigations into this subject can be found in the commentary for **D7**.

D5, **D7**, **D8**, **D12**. A discussion of Turán's problem and the implication of **D5** already appears in the commentary for **D3**. The result achieved by Schinzel in **D5** remains the strongest published result toward the validity of Turán's conjecture for arbitrary $f \in \mathbb{Z}[x]$.

In **D7**, Schinzel improves on work in **D2** concerning the factorization of KF. In particular, **D7** describes the canonical factorization for $KF(x_1^{n_1}, \ldots, x_k^{n_k})$ (see Theorem 2). This result is extended to the field of coefficients being any finitely generated field in Theorem 43 of Schinzel's book [37]. In **D7**, Schinzel also obtains information about the number of irreducible factors, counted with multiplicity, of KF based on the now classical estimates for roots off the unit circle in the complex plane by P. E. Blanksby and H. L. Montgomery [4], by C. J. Smyth [44] and (in an added note at the end of the paper) by E. Dobrowolski [9]. This subject has been explored further, specifically by Schinzel in [33] and in [35], as well as by C. Pinner and J. Vaaler in [27], [28] and [29]. Also, note that **D7** obtains information about the factorization of non-reciprocal quadrinomials. The factorization of non-reciprocal quadrinomials is handled in detail in [36] (see also Theorem 78 of Schinzel's book [37]).

In **D8**, Schinzel's main theorem bounds the number of reciprocal non-cyclotomic factors of an arbitrary polynomial $f \in \mathbb{Z}[x]$ under conditions which hold, for example, provided the coefficients are not too large and f has one term that has degree sufficiently large compared to the degrees of its other terms. In particular, this result implies that the

polynomial $\sum_{j=0}^{n} x^{2^j}$ has no reciprocal non-cyclotomic factors. He uses this to resolve a problem posed by K. Mahler in [25].

In **D12**, Schinzel shows how work of E. Bombieri and U. Zannier (see Schinzel's book [37] and, in particular, the appendix written by Zannier there) implies improvements on various of the prior results in his serious of papers on the reducibility of lacunary polynomials. In particular, the canonical factorization of $KF(x^{n_1}, \ldots, x^{n_k})$ is dealt with in a rather general form for the first time and in an elegant way here. One nice example of an improvement in prior work is Corollary 2 which (even in its previous form) implies that one can typically expect that a lacunary (or sparse) reducible polynomial removed of its cyclotomic factors is irreducible. To put the result in a more precise perspective, fix integers $A \geqslant 2$ and $r \geqslant 3$ and consider all polynomials f in $\mathbb{Z}[x]$ with coefficients in absolute value bound by A, with $f(0) \neq 0$, with f consisting of $\leqslant r$ terms and with $\deg f \leqslant N$. Then as N tends to infinity, the density of such f having a cyclotomic factor (and even simply divisible by $x-1$) is positive whereas Corollary 2 is asserting in a strong sense that the density of such f for which Kf is reducible is zero. It follows then that a typical lacunary reducible polynomial not divisible by x is divisible by a cyclotomic polynomial.

D9. This problem concerns a problem of Rényi dating back to around 1949. The problem itself has an illusion of seeming like it should have a simple solution, but the problem is apparently quite difficult and is resolved for the first time, after approximately 40 years, in this paper. In its simplest form, the problem asks whether Q_k tends to infinity where Q_k is defined as the minimum number of terms (by definition, non-zero) that can appear in the square of a polynomial with exactly k terms. Here, one can take the polynomials to have real coefficients, though other variations of the problem are possible. Schinzel's argument that

$$Q_k > \frac{\log\log k}{\log 2},$$

gives not only the strongest lower bound on Q_k but also still provides the only published argument for a lower bound that tends to infinity with k.

That Q_k can be $< k$ is not even completely obvious. The simple example

$$w(x) = 1 + 2x - 2x^2 + 4x^3 + 4x^4$$

shows that $w(x)^2$ can have the same number of terms as $w(x)$. Observe that if one takes

$$h(x) = w(x)^2 = 1 + 4x + 28x^4 + 32x^7 + 16x^8,$$

then it is clear that $w(x) \cdot w(x^7)$ has $5 \cdot 5 = 25$ terms whereas $h(x) \cdot h(x^7)$ has fewer than 25 terms (since the product of the constant term of either $h(x)$ or $h(x^7)$ times the term of degree 7 in the other combine to give one term of degree 7 with coefficient 36 in the product). Thus, $w(x) \cdot w(x^7)$ is an example of a polynomial whose square contains fewer terms than itself. One can check that this polynomial has 25 terms and its square has 21 terms. Examples involving smaller values of k exist. D. Coppersmith and J. Davenport

in [8] give the example

$$(125x^6 + 50x^5 - 10x^4 + 4x^3 - 2x^2 + 2x + 1)(-110x^6 + 1),$$

which is a polynomial of degree 12 having 13 non-zero terms, and the square of this polynomial has 12 non-zero terms. J. Abbott in [1] has shown using computations with Gröbner bases that every polynomial in $\mathbb{Z}[x]$ of smaller degree than 12 cannot have a square with fewer terms than itself. It is still possible that a polynomial in $\mathbb{Z}[x]$ with fewer than 13 non-zero terms (apparently of degree at least 12) could have a square with fewer terms than itself, and it would be of interest to determine what is the fewest non-zero terms such a polynomial can have.

There is an extensive history concerning Rényi's problem. A. Rényi's initial work associated with the problem is [30], though he notes some contributions on the size of Q_k given by L. Rédei and L. Kalmár. It is noted that $Q_{29} \leqslant 28$. Based on this example and a lemma, Rényi shows that the average of Q_k/k, where k ranges from 1 to n tends to 0. This implies that $\liminf_{k\to\infty} Q_k/k = 0$. Rényi conjectures here that $\lim_{k\to\infty} Q_k/k = 0$. P. Erdős in [11] resolves this problem of Rényi and indicates that Rényi has also asked for a proof that $\lim_{k\to\infty} Q_k = \infty$, the problem resolved by Schinzel in **D9**. Erdős also shows, as mentioned in Schinzel's paper, that $Q_k < c_1 k^{1-c_2}$ for some positive constants c_1 and c_2. W. Verdenius in [47] showed that one can take $c_2 = \log_{13} 8$. Further investigations were made by D. Coppersmith and J. Davenport in the paper quoted above. In particular, they establish an analog to Erdős's result for higher powers of polynomials. These authors, other than Schinzel, restricted attention to the case that the polynomials have real coefficients. R. Freud in [18] extended the results of Erdős to polynomials with integer coefficients. The interested reader should consult Schinzel's book [37]. There rather general theorems over arbitrary fields are discussed.

There has been recent very nice progress in this area due to U. Zannier [48]. He has shown that for each positive integer k, there is a computable number $B(k)$ such that if $g(x)$ and $h(x)$ are non-constant polynomials in $\mathbb{C}[x]$ with $g(h(x))$ having $\leqslant k$ terms, then $h(x)$ has $\leqslant B(k)$ terms. In particular, as the number of terms of $h(x) \in \mathbb{C}[x]$ tends to infinity, the number of terms of $g(h(x))$ must also tend to infinity and uniformly over non-constant $g(x) \in \mathbb{C}[x]$.

D11. This solution to an approximately 30 year old problem has led to several further investigations. H. P. Schlickewei and C. Viola in [39] showed that the bound given by (1) can be replaced by $2^{44000}(\deg p)^{1000}$. Their methods would easily allow for smaller exponents. In particular, they make use of a preprint of H. P. Schlickewei and W. M. Schmidt which later appeared in print as [38]. This paper has some slight improvements over the preprint that was used. H. P. Schlickewei and C. Viola, in [41] obtain a result which replaces the role of Schlickewei and Schmidt's when conducting analogous investigations for k-nomials which is treated by H. P. Schlickewei and C. Viola in [40].

The problem posed by Győry and Schinzel at the end of the introduction was resolved negatively in the case that $k \geqslant 6$ by L. Hajdu in [20]. Further investigations of this type can be found in L. Hajdu and R. Tijdeman's paper [21].

D10, **D13**, **D14**. The motivation of these papers is explained in **D10**. The factorization of binomials has been well understood; in particular, over any field K, the binomial $x^n - a \in K[x]$ is reducible if and only if either a is a pth power in K for some prime p dividing n or $4 \mid n$ and $a = -4b^4$ for some $b \in K$. For a proof of this result, one can consult Section 13 of Schinzel's book [34] or Section 2.1 of Schinzel's more recent book [37]. In **D10**, Schinzel offers corresponding results for the factorization of trinomials $x^n + ax^m + b$. As elaborated on in **D13**, the condition $n \geqslant 2m$ is made as the trinomials $x^n + ax^m + b$ and $x^n + ab^{-1}x^{n-m} + b^{-1}$ are either both irreducible or both reducible and either $n \geqslant 2m$ or $n \geqslant 2(n-m)$ must hold.

Consequence 1 of **D10** implies that for a field K with characteristic $\pi \geqslant 0$, there is a constant C depending only on K such that if n and m are integers such that $\pi \nmid nm(n-m)$ and $n/(n,m) > C$, then for every non-zero a and b in K, the trinomial $x^n + ax^m + b$ is either irreducible or it has a non-trivial binomial or trinomial factor. This motivates in part the goals of **D13** and **D14** where we find Schinzel going beyond examining which trinomials $x^n + ax^m + b$ are reducible or irreducible and determining instead more detailed information about the factorization of these trinomials. Specifically, **D13** provides necessary and sufficient conditions for the trinomial $x^n + ax^m + b$ divided by a certain binomial factor to be reducible, and **D14** provides necessary and sufficient conditions for the trinomial $x^n + ax^m + b$ divided by a certain proper trinomial factor to be reducible.

There is a tremendous amount of literature surrounding the factorization of trinomials which would be impossible to cover in any detail here. Some discussions of these results occur elsewhere in the commentaries (for example, the commentaries on **D2**, **D4**, **D11**, **D12**, **D16**). An intriguing problem in A. Schinzel [32] is to determine whether or not there is an absolute constant C such that every trinomial in $\mathbb{Q}[x]$ has an irreducible factor with $\leqslant C$ terms. J. Abbott (private communication) has noted that the trinomial $64x^{20} + 7x^2 + 4$ factors as the product of the two irreducible polynomials $f(x)$ and $f(-x)$, where

$$f(x) = 8x^{10} + 16x^9 + 16x^8 + 8x^7 + 4x^4 + 8x^3 + 8x^2 + 5x + 2.$$

This shows that if C exists, then $C \geqslant 9$, which is the current best known lower bound. For more on this problem, see A. Bremner [6], or A. Choudhry and A. Schinzel [7].

D15, **D16**. Having dealt with the greatest common divisor of two trinomials of a rather specific form in **D1**, it is natural that Schinzel would take up the task of resolving a related intriguing problem posed by P. Weinberger in 1976. The problem, as indicated in **D15**, is to determine, for fixed positive integers r and s, the supremum of the number of terms that can occur in $\gcd(f, g)$, where f and g run over all polynomials in $K[x]$, for some given field K, with f consisting of r terms and g consisting of s terms. In **D15**, the problem is resolved entirely except for the case that K has characteristic 0 and $r = s = 3$. In **D16**, results related to the latter case are obtained, but the problem in this situation remains open. It is possible that $\gcd(f, g)$ always consists of $\leqslant 6$ terms in this case.

D17. Beginning with some measure $L(f)$ of the size of a polynomial f, one can ask to determine the infimum $\ell(P)$ on the sizes of the multiples of a given polynomial P or, more precisely, on $L(PG)$ where G ranges over a specific collection of polynomials. In this paper, $L(f)$ denotes the sum of the absolute values of the coefficients of f, $P \in \mathbb{R}[x]$

and $G(x)$ is restricted to monic polynomials in $\mathbb{R}[x]$. The condition that G is monic is necessary to avoid the infimum trivially being 0. One focus of the paper is to determine for what P the value of $\ell(P)$ is attained, that is to determine for what $P \in \mathbb{R}[x]$, there exists a monic polynomial $G(x) \in \mathbb{R}[x]$ that minimizes the value of $L(PG)$. Another focus of the paper is to obtain an effective approach for computing $\ell(P)$. Complete answers are given in many instances; as examples, $\ell(P)$ is attained and computable in the case that P has no roots on the unit circle and $\ell(P)$ is computable for all quadratic P. An intriguing question is raised as to how to establish the value of $\ell(P)$ in the specific case that $P = 2x^3 + 3x^2 + 4$.

The problem was investigated previously by A. Dubickas [10]. Similar problems have been considered by others. A result due to G. Szegö [45] in 1914 is that the infimum above is precisely the Mahler measure of P if one uses as a measure of the size of the polynomial the squareroot of the sum of the squares of the absolute values of the coefficients. For Szegö's result, one can consider $P \in \mathbb{R}[x]$ and multiples of the form PG where $G(x)$ is monic in $\mathbb{R}[x]$ or one can consider the analog with P and G in $\mathbb{C}[x]$. I. Z. Ruzsa [31] has generalized Szegö's result to polynomials in several variables (see also Theorem 38 on page 227 of [37]).

The analogous problem with $P \in \mathbb{Z}[x]$ and the requirement that $G \in \mathbb{Z}[x]$, $G \neq 0$ with G not necessarily monic, has been investigated by M. Filaseta, M. L. Robinson and F. S. Wheeler in [15] and by M. Filaseta and I. Solan in [16]. The first of these papers handles the case where P is irreducible, and the second handles the case where P is not divisible by a cyclotomic polynomial. In particular, in these cases, the infimum is attained and is computable. The methods apply to rather general notions for the size of a polynomial and, in particular, one can use the two sizes described above; the proofs, however, are restricted to the norm given by the squareroot of the sum of the squares of the coefficients.

We note that finding multiples of polynomials with restrictions on the coefficients and, in particular, with small norm has applications to the Prouhet–Tarry–Escott Problem. Let n be a positive integer. Suppose $P(x) = (x-1)^n$ and that there is a polynomial $G(x) \in \mathbb{R}[x]$ such that $L(f) = 2n$ where $f = PG$ and $L(f)$ is the sum of the absolute values of the coefficients of f. Suppose further that the coefficients of f are restricted to $\{0, \pm 1\}$. Then $f(1) = 0$ implies that f has n coefficients that are 1 and n coefficients that are -1. It follows that there are $2n$ distinct nonnegative integers $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ such that

$$f(x) = \sum_{i=1}^{n} x^{a_i} - \sum_{j=1}^{n} x^{b_j}.$$

As $(x-1)^n$ is a factor of f, we have $f^{(k)}(1) = 0$ for $k \in \{1, 2, \ldots, n-1\}$. A simple argument implies that

$$\sum_{i=1}^{n} a_i^k = \sum_{j=1}^{n} b_j^k \quad \text{for } k \in \{1, 2, \ldots, n-1\}.$$

Observe also that if we begin with $2n$ distinct nonnegative integers a_j and b_j that satisfy this last string of equalities and define $f(x)$ as the difference of the two sums, as above, with these exponents, then $f(x)$ is a multiple of $P(x) = (x-1)^n$ with $L(f) = 2n$. It is

unknown whether or not such a_j and b_j exist for $n \geqslant 13$. The example

$$\begin{aligned} f(x) = 1 &+ x^{11} + x^{24} + x^{65} + x^{90} + x^{129} + x^{173} \\ &+ x^{212} + x^{237} + x^{278} + x^{291} + x^{302} \\ - x^3 &- x^5 - x^{30} - x^{57} - x^{104} - x^{116} - x^{186} \\ &- x^{198} - x^{245} - x^{272} - x^{297} - x^{299}, \end{aligned}$$

divisible by $(x-1)^{12}$, is based on a combination of observations by Nuutti Kuosa, Jean-Charles Meyrignac and Chen Shuwen. Whether such a_j and b_j exist for general n is a form of the Prouhet–Tarry–Escott Problem. Thus, it is of interest to know whether an algorithm exists for finding a multiple f of P as above, but the methods described in the papers here do not resolve this issue. For a somewhat recent paper on this subject, we mention the work of P. Borwein, P. Lisoněk, and C. Percival [5].

References

[1] J. Abbott, *Sparse squares of polynomials*. Math. Comp. 71 (2002), 407–413.

[2] A. Bérczes, L. Hajdu, *Computational experiences on the distances of polynomials to irreducible polynomials*. Math. Comp. 66 (1997), 391–398.

[3] —, —, *On a problem of P. Turán concerning irreducible polynomials*. In: Number Theory (Eger, 1996), de Gruyter, Berlin 1998, 95–100.

[4] P. E. Blanksby, H. L. Montgomery, *Algebraic integers near the unit circle*. Acta Arith. 18 (1971), 355–369.

[5] P. Borwein, P. Lisoněk, C. Percival, *Computational investigations of the Prouhet–Tarry–Escott problem*. Math. Comp. 72 (2003), 2063–2070.

[6] A. Bremner, *On reducibility of trinomials*. Glasgow Math. J. 22 (1981), 155–156.

[7] A. Choudhry, A. Schinzel, *On the number of terms in the irreducible factors of a polynomial over* $\mathbb{Q}$. Glasgow Math. J. 34 (1992), 11–15.

[8] D. Coppersmith, J. Davenport, *Polynomials whose powers are sparse*. Acta Arith. 58 (1991), 79–87.

[9] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*. Acta Arith. 34 (1979), 391–401.

[10] A. Dubickas, *Arithmetical properties of powers of algebraic numbers*. Bull. London Math. Soc. 38 (2006), 70–80.

[11] P. Erdős, *On the number of terms of the square of a polynomial*. Nieuw Arch. Wiskunde (2) 23 (1949), 63–65.

[12] M. Filaseta, *On the factorization of polynomials with small Euclidean norm*. In: Number Theory in Progress, Vol. 1 (Zakopane–Kościelisko, 1997), de Gruyter, Berlin 1999, 143–163.

[13] —, *Coverings of the integers associated with an irreducibility theorem of A. Schinzel*. In: Number Theory for the Millennium, II (Urbana, 2000), A K Peters, Natick 2002, 1–24.

[14] M. Filaseta, K. Ford, S. Konyagin, *On an irreducibility theorem of A. Schinzel associated with coverings of the integers*. Illinois J. Math. 44 (2000), 633–643.

[15] M. Filaseta, M. L. Robinson, F. S. Wheeler, *The minimal Euclidean norm of an algebraic number is effectively computable*. J. Algorithms 16 (1994), 309–333.

[16] M. Filaseta, I. Solan, *Norms of factors of polynomials*. Acta Arith. 82 (1997), 243–255.

[17] —, —, *An extension of a theorem of Ljunggren*. Math. Scand. 84 (1999), 5–10.

[18] R. Freud, *On the minimum number of terms in the square of a polynomial*. Mat. Lapok 24 (1973), 95–98 (Hungarian).

[19] R. K. Guy, *Unsolved Problems in Number Theory*, third edition. Problem Books in Math., Springer, New York 2004.

[20] L. Hajdu, *On a problem of Győry and Schinzel concerning polynomials*. Acta Arith. 78 (1997), 287–295.

[21] L. Hajdu, R. Tijdeman, *Polynomials dividing infinitely many quadrinomials or quintinomials*. Acta Arith. 107 (2003), 381–404.

[22] A. T. Jonassen, *On the irreducibility of the trinomials* $x^m \pm x^n \pm 4$. Math. Scand. 21 (1967), 177–189.

[23] W. Ljunggren, *On the irreducibility of certain trinomials and quadrinomials*. Math. Scand. 8 (1960), 65–70.

[24] —, *On the irreducibility of certain lacunary polynomials*. Norske Vid. Selsk. Forh. (Trondheim) 36 (1963), 159–164.

[25] K. Mahler, *On the zeros of a special sequence of polynomials*. Math. Comp. 39 (1982), 207–212.

[26] W. H. Mills, *The factorization of certain quadrinomials*. Math. Scand. 57 (1985), 44–50.

[27] C. G. Pinner, J. D. Vaaler, *The number of irreducible factors of a polynomial* I. Trans. Amer. Math. Soc. 339 (1993), 809–834.

[28] —, —, *The number of irreducible factors of a polynomial* II. Acta Arith. 78 (1996), 125–142.

[29] —, —, *The number of irreducible factors of a polynomial* III. In: Number Theory in Progress, Vol. 1 (Zakopane–Kościelisko, 1997), de Gruyter, Berlin 1999, 395–405.

[30] A. Rényi, *On the minimal number of terms of the square of a polynomial*. Hungarica Acta Math. 1 (1947), 30–34.

[31] I. Z. Ruzsa, *On Mahler's measure for polynomials in several variables* In: Number Theory in Progress, Vol. 1 (Zakopane–Kościelisko, 1997), de Gruyter, Berlin 1999, 431–444.

[32] A. Schinzel, *Some unsolved problems on polynomials*. In: Neki nerešeni problemi u matematici, Matematička Biblioteka 25, Beograd 1963, 63–70; this collection: E1, 703–708.

[33] —, *On the number of irreducible factors of a polynomial*. in: Topics in Number Theory, Colloq. Math. Soc. János Bolyai 13, North-Holland, Amsterdam 1976, 305–314.

[34] —, *Selected Topics on Polynomials*. University of Michigan Press, Ann Arbor 1982.

[35] —, *On the number of irreducible factors of a polynomial, II*. Ann. Polon. Math. 42 (1983), 309–320,

[36] —, *Reducibility of lacunary polynomials* VI. Acta Arith. 47 (1986), 277–293.

[37] —, *Polynomials with Special Regard to Reducibility*. Encyclopaedia of Mathematics and its Applications 77, Cambridge Univ. Press, Cambridge 2000.

[38] H. P. Schlickewei, W. M. Schmidt, *The number of solutions of polynomial-exponential equations*. Compositio Math. 120 (2000), 193–225.

[39] H. P. Schlickewei, C. Viola, *Polynomials that divide many trinomials*. Acta Arith. 78 (1997), 267–273.

[40] —, —, *Polynomials that divide many k-nomials*. In: Number Theory in Progress, Vol. 1 (Zakopane–Kościelisko, 1997), de Gruyter, Berlin 1999, 445–450.

[41] —, —, *Generalized Vandermonde determinants*. Acta Arith. 95 (2000), 123–137.

[42] E. S. Selmer, *On the irreducibility of certain trinomials*. Math. Scand. 4 (1956), 287–302.

[43] W. Sierpiński, *Remarques sur les progressions arithmétiques*. Colloquium Math. 3 (1954), 44–49.

[44] C. J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*. Bull. London Math. Soc. 3 (1971), 169–175.

[45] G. Szegö, *Ein Grenzwertsatz über die Toeplitzschen Determinanten einer reellen positiven Funktion*. Math. Ann. 76 (1915), 490–503.

[46] H. Tverberg, *On the irreducibility of the trinomials $x^n \pm x^m \pm 1$*. Math. Scand. 8 (1960), 121–126.

[47] W. Verdenius, *On the number of terms of the square and the cube of polynomials*. Indag. Math. 11 (1949), 546–565.

[48] U. Zannier, *On composite lacunary polynomials and the proof of a conjecture of Schinzel*. Preprint.

Originally published in
Colloquium Mathematicum IX (1962), 291–296

Solution d'un problème de K. Zarankiewicz sur les suites de puissances consécutives de nombres irrationnels

Dédié à la mémoire de K. Zarankiewicz

K. Zarankiewicz a posé le problème : existe-il un nombre irrationnel q tel qu'on puisse extraire de la suite $q, q^2, \ldots$ quatre termes formant une progression arithmétique ? (cf. [2], p. 44, P 115).

La réponse négative à ce problème (même quand on admet q complexe, les quatre termes correspondants étant distincts) est une conséquence immédiate du théorème 2, qui va suivre.

En appliquant la méthode ingénieuse de W. Ljunggren [1], le théorème suivant sera d'abord établi :

Théorème 1. *Les nombres n et m étant des entiers tels que $n > m > 0$ et $n \neq 2m$, le polynôme*

$$g(x) = \frac{x^n - 2x^m + 1}{x^{(n,m)} - 1}$$

est irréductible, à l'exception des cas $n = 7k$, $m = 2k$ et $n = 7k$, $m = 5k$, dans lesquels $g(x)$ est un produit de deux facteurs irréductibles, à savoir

$$(x^{3k} + x^{2k} - 1)(x^{3k} + x^k + 1) \quad et \quad (x^{3k} + x^{2k} + 1)(x^{3k} - x^k - 1)$$

respectivement.

Lemme. *Soit*

$$f(x) = x^n - 2x^m + 1 = \varphi_r(x)\psi_s(x) \quad où \quad r + s = n, \tag{1}$$

$\varphi_r(x)$ et $\psi_s(x)$ étant des polynômes unitaires de degré r et s respectivement, et aux coefficients entiers. Soit en outre

$$\langle 7k, 2k\rangle \neq \langle n, m\rangle \neq \langle 7k, 5k\rangle.$$

Alors au moins l'un des deux facteurs de (1) *est un polynôme réciproque.*

Correction: *Colloq. Math.* XII (1964), 289.

Démonstration du lemme. Il suffit de considérer le cas où $n > 2m$. En posant

$$f_1(x) = x^r \varphi_r(x^{-1})\psi_s(x) = \sum_{i=0}^{n} c_i x^{n-i} \quad \text{et} \quad f_2(x) = x^s \psi_s(x^{-1})\varphi_r(x), \tag{2}$$

il vient

$$f_2(x) = x^n f_1(x^{-1}) = \sum_{i=0}^{n} c_{n-i} x^{n-i}, \tag{3}$$

$$f_1(x) f_2(x) = (x^n - 2x^m + 1)(x^n - 2x^{n-m} + 1). \tag{4}$$

En comparant les coefficients de x^{2n} et de x^n dans (2) et (3), nous trouvons $c_0 c_n = 1$ et $c_0^2 + c_1^2 + c_2^2 + \ldots + c_n^2 = 6$, d'où

$$c_n = c_0 = \pm 1 \quad \text{et} \quad c_1^2 + c_2^2 + \ldots + c_{n-1}^2 = 4. \tag{5}$$

Il résulte de (5) que deux cas sont possibles :

Cas I. L'un des nombres c_i, où $i = 1, 2, \ldots, n-1$, soit c_k, est égal à ± 2 et les autres sont égaux à 0.

Cas II. Quatre des nombres c_i, soit $c_{k_1}, c_{k_2}, c_{k_3}$ et c_{k_4}, où $k_1 < k_2 < k_3 < k_4$, sont égaux à ± 1 et les autres sont égaux á 0.

Considérons ces deux cas successivement.

Dans le cas I, on peut admettre sans restreindre la généralité que $n \geqslant 2k$. On a d'après (2) et (3) pour le polynôme réciproque $f_1(x) f_2(x)$

$$f_1(x) f_2(x) = x^{2n} + c_0 c_k x^{2n-k} + c_0 c_k x^{n+k} + 6x^n + c_0 c_k x^{n-k} + c_0 c_k x^k + 1 \tag{6}$$

et d'après (4)

$$f_1(x) f_2(x) = x^{2n} - 2x^{2n-m} - 2x^{n+m} + 6x^n - 2x^{n-m} - 2x^m + 1. \tag{7}$$

En comparant (6) à (7), on trouve $k = m$ et $c_0 c_k = -2$, d'où

$$f_2(x) = c_0(x^n - 2x^m + 1) = c_0 f(x) \quad \text{et} \quad x^s \psi_s(x^{-1}) = c_0 \psi_s(x);$$

ainsi $\psi_s(x)$ est un polynôme réciproque.

Dans le cas II, on peut admettre sans restreindre la généralité que $n \geqslant k_1 + k_4$. Alors le polynôme réciproque $f_1(x) f_2(x)$ se réduit d'après (2) et (3) à la somme

$$\begin{aligned} f_1(x) f_2(x) = {} & x^{2n} + c_0 c_{k_4} x^{n+k_4} + c_0 c_{k_3} x^{n+k_3} + c_0 c_{k_2} x^{n+k_2} + c_0 c_{k_1} x^{n+k_1} \\ & + c_0 c_{k_1} x^{2n-k_1} + c_{k_1} c_{k_4} x^{n+k_4-k_1} + c_{k_1} c_{k_3} x^{n+k_3-k_1} + c_{k_1} c_{k_2} x^{n+k_2-k_1} \\ & + c_0 c_{k_2} x^{2n-k_2} + c_{k_2} c_{k_4} x^{n+k_4-k_2} + c_{k_2} c_{k_3} x^{n+k_3-k_2} + c_0 c_{k_3} x^{2n-k_3} \\ & + c_{k_3} c_{k_4} x^{n+k_4-k_3} + c_0 c_{k_4} x^{2n-k_4} + 6x^n + \ldots. \end{aligned} \tag{8}$$

En comparant (7) à (8), on constate que chaque exposant sauf $2n$ se présente dans (8) un nombre pair de fois. L'exposant $2n - k_1$ n'apparaissant qu'une seule fois lorsque $2n - k_1 > n + k_4$, on a donc $2n - k_1 = n + k_4$, d'où $k_4 = n - k_1$. On peut admettre sans restreindre la généralité que $n \geqslant k_2 + k_3$. La condition que l'exposant $\max(n + k_3, n + k_4 - k_1, 2n - k_2)$

figure dans la somme (8) nécessairement un nombre pair de fois entraîne deux possibilités : 1° $k_3 = n - k_2$ et $k_2 < 2k_1$, 2° $k_2 = 2k_1$ et $k_3 < n - 2k_1$.

Considérons ces deux possibilités successivement.

Dans 1°, les relations

$$\begin{aligned}\min(n + k_4, n + k_3, 2n - k_1, 2n - k_2) &> n + k_4 - k_1\\ > \max(n + k_3 - k_1, n + k_2 - k_1, n + k_4 - k_2, n + k_3 - k_2, n + k_4 - k_3),&\\ n + k_2 = 2n - k_3 \quad \text{et} \quad n + k_1 = 2n - k_4&\end{aligned}$$

entraîneraient que l'exposant $n + k_4 - k_1$ doit se présenter un nombre impair de fois, ce qui vient d'être constaté comme impossible.

Dans 2°, les relations

$$\begin{aligned}\min(n + k_4, n + k_3, n + k_2, 2n - k_1, n + k_4 - k_1,&\\ n + k_3 - k_1, 2n - k_2, n + k_4 - k_2, 2n - k_3, n + k_4 - k_3)&\\ > n + k_1 = n + k_2 - k_1 = 2n - k_4&\end{aligned}$$

entraînent que $n + k_1 = n + k_3 - k_2$, d'où $k_3 = 3k_1$. On a maintenant

$$\begin{gathered}n + k_4 = 2n - k_1, \quad n + k_2 = n + k_3 - k_1,\\ n + k_1 = n + k_2 - k_1 = n + k_3 - k_2 = 2n - k_4,\\ n + k_4 - k_1 = 2n - k_2 \quad \text{et} \quad n + k_4 - k_2 = 2n - k_3.\end{gathered}$$

Il en résulte que $n + k_3 = n + k_4 - k_3$, c'est-à-dire

$$n = k_1 + k_4 = k_1 + 2k_3 = 7k_1$$

et (8) se réduit à la forme

$$\begin{aligned}f_1(x) f_2(x) = x^{14k_1} &+ \big(c_0c_{k_4} + c_0c_{k_1}\big)x^{13k_1}\\ &+ \big(c_{k_1}c_{k_4} + c_0c_{k_2}\big)x^{12k_1} + \big(c_0c_{k_3} + c_{k_2}c_{k_4}\big)x^{11k_1}\\ &+ \big(c_0c_{k_3} + c_{k_3}c_{k_4}\big)x^{10k_1} + \big(c_0c_{k_2} + c_{k_1}c_{k_3}\big)x^{9k_1}\\ &+ \big(c_0c_{k_1} + c_{k_1}c_{k_2} + c_{k_2}c_{k_3} + c_0c_{k_4}\big)x^{8k_1} + 6x^{7k_1} + \dots.\end{aligned} \tag{9}$$

Enfin, la comparaison de (7) à (9) montre qu'il y a encore deux éventualités à considérer, à savoir

$$\text{(A)} \quad m = k_1 \qquad \text{et} \qquad \text{(B)} \quad m = 3k_1,$$

l'égalité $m = 2k_1$ étant exclue par l'hypothèse.

Si l'on a (A), il vient en comparant les coefficients dans (7) et (9),

$$\begin{gathered}c_0c_{k_4} = c_0c_{k_1} = -1, \quad c_{k_1}c_{k_4} = -c_0c_{k_2}, \quad c_0c_{k_3} = -c_{k_2}c_{k_4},\\ c_0c_{k_1} + c_{k_1}c_{k_2} + c_{k_2}c_{k_3} + c_0c_{k_4} = -2,\end{gathered}$$

d'où $c_{k_4} = c_{k_3} = c_{k_2} = c_{k_1} = -c_0$, ce qui entraîne

$$c_0c_{k_1} + c_{k_1}c_{k_2} + c_{k_2}c_{k_3} + c_0c_{k_4} = 0,$$

donc une contradiction avec la formule précédente.

Si l'on a (B), la comparaison de ces coefficients donne

$$c_0c_{k_4} = -c_0c_{k_1}, \quad c_{k_1}c_{k_4} = -c_0c_{k_2}, \quad c_0c_{k_3} = c_{k_2}c_{k_4} = -1,$$

c $$c_0c_{k_3} + c_{k_3}c_{k_4} = -2,$$

d'où $c_{k_4} = c_{k_3} = -c_0$, ce qui entraîne

$$c_0c_{k_3} + c_{k_3}c_{k_4} = 0,$$

donc également une contradiction avec la formule précédente.

Ainsi le cas II est démontré impossible et le lemme se trouve établi. □

Démonstration du théorème 1. Si $\langle n, m\rangle = \langle 7k, 2k\rangle$ ou bien $\langle 7k, 5k\rangle$, on a $(n, m) = k$ et on vérifie aisément que

$$g(x) = \big(x^{3k} + x^{2k} - 1\big)\big(x^{3k} + x^k + 1\big) \quad \text{ou} \quad \big(x^{3k} + x^{2k} + 1\big)\big(x^{3k} + x^k - 1\big)$$

respectivement. Or les polynômes $x^{3k} + x^{2k} \pm 1$ et $x^{3k} \pm x^k \pm 1$ sont irréductibles en vertu du théorème 3 de Ljunggren (voir [1]). En supposant, par contre, que $\langle 7k, 2k\rangle \neq \langle n, m\rangle \neq \langle 7k, 5k\rangle$, au moins l'un des facteurs du membre droit de (1) aurait en vertu du lemme la propriété suivante : si λ est une racine de ce facteur, il en est de même de λ^{-1}. La réductibilité du polynôme $g(x)$ entraînerait donc que

$$g(\lambda) = g(\lambda^{-1}) = 0 \tag{10}$$

pour un certain λ complexe. Il en résulte que $\lambda^n - 2\lambda^m + 1 = 0$ et $\lambda^n - 2\lambda^{n-m} + 1 = 0$, d'où successivement $\lambda^{n-2m} = 1$, $\lambda^{2m} - 2\lambda^m + 1 = 0$, $\lambda^m = 1$ et $\lambda^n = 1$, donc $\lambda^{(n,m)} = 1$. En même temps, l'hypothèse $n \neq 2m$ entraîne $n\lambda^{n-1} \neq 2m\lambda^{m-1}$; par conséquent λ serait une racine simple de $x^n - 2x^m + 1$. Vu que $\lambda^{(n,m)} = 1$, on aurait donc

$$g(\lambda) = \frac{\lambda^n - 2\lambda^m + 1}{\lambda^{(n,m)} - 1} \neq 0,$$

contrairement à (10). La démonstration du théorème 1 est ainsi achevée. □

Théorème 2. *Les nombres n, m, p et q étant des entiers tels que $n > m > 0$, $p > q > 0$ et $\langle n, m\rangle \neq \langle p, q\rangle$, on a*

$$(x^n - 2x^m + 1, x^p - 2x^q + 1) = \begin{cases} x^{(n,m,p,q)} - 1 & \text{si } \langle n, p\rangle \neq \langle 2m, 2q\rangle, \\ \big(x^{(m,q)} - 1\big)^2 & \text{si } \langle n, p\rangle = \langle 2m, 2q\rangle. \end{cases}$$

Démonstration. On a pour $r > s$

$$g_{r,s}(x) = \frac{x^r - 2x^s + 1}{x^{(r,s)} - 1} = \sum_{i=s/(r,s)}^{r/(r,s)-1} x^{(r,s)i} - \sum_{i=0}^{s/(r,s)-1} x^{(r,s)i};$$

si $r \neq 2s$, les polynômes $g_{r,s}(x)$ et les facteurs irréductibles de $g_{7k,2k}(x)$ et de $g_{7k,5k}(x)$ sont donc deux à deux distinct et différents des facteurs irréductibles de $x^l - 1$, quel que

soit l'entier l. Il en résulte que l'on a pour $n \neq 2m$ et $p \neq 2q$

$$(x^n - 2x^m + 1, x^p - 2x^q + 1) = \left(x^{(n,m)} - 1, x^{(p,q)} - 1\right) = x^{(n,m,p,q)} - 1,$$

et on voit aisément que la même formule subsiste lorsqu'on a l'une des égalités $n = 2m$ et $p = 2q$.

Par contre, pour $\langle n, p\rangle = \langle 2m, 2q\rangle$, il vient

$$(x^n - 2x^m + 1, x^p - 2x^q + 1) = \left((x^m - 1)^2, (x^q - 1)^2\right) = (x^m - 1, x^q - 1)^2 = \left(x^{(m,q)} - 1\right)^2,$$

ce qui achève la démonstration du théorème 2. □

Pour en déduire la solution du problème précité de Zarankiewicz, il suffit de remarquer que si les nombres $q^\alpha, q^\beta, q^\gamma$ et q^δ, où $\alpha < \beta < \gamma < \delta$, forment une progression arithmétique, on a

$$q^{\gamma-\alpha} - 2q^{\beta-\alpha} + 1 = 0 \quad \text{et} \quad q^{\delta-\beta} - 2q^{\gamma-\beta} + 1 = 0;$$

si, au contraire, $q^{(\gamma-\alpha,\beta-\alpha,\delta-\beta,\gamma-\beta)} - 1 = 0$, on a

$$q^\alpha = q^\beta = q^\gamma = q^\delta.$$

Le théorème suivant peut être établi d'une façon tout à fait analogue que le théorème 1 :

Théorème 3. *Les nombres n et m étant des entiers tels que $n > m > 0$, le polynôme $f(x) = x^n + 2\varepsilon_1 x^m + \varepsilon_2$, où $\varepsilon_1, \varepsilon_2 = \pm 1$, est un produit de deux facteurs dont le premier a pour racines précisément celles des racines de f qui sont des racines de l'unité, et le second, soit $g(x)$, satisfait aux conditions* :

(α) *si $\varepsilon_1 = -\varepsilon_2$, $n = 7k$ et $m = 2k$, on a*

$$g(x) = (x^{3k} + \varepsilon_2 x^{2k} + \varepsilon_1)(x^{3k} + x^k + \varepsilon_2);$$

(β) *si $\varepsilon_1 = -1$, $n = 7k$ et $m = 5k$, on a*

$$g(x) = (x^{3k} + \varepsilon_2 x^{2k} + \varepsilon_2)(x^{3k} - x^k - \varepsilon_2);$$

(γ) *si $\varepsilon_1 = 1$, $n = 7k$ et $m = 3k$, on a*

$$g(x) = (x^{3k} - \varepsilon_2 x^{2k} + \varepsilon_2)(x^{4k} + \varepsilon_2 x^{3k} + x^{2k} + 1);$$

(δ) *si $\varepsilon_1 = \varepsilon_2$, $n = 7k$ et $m = 4k$, on a*

$$g(x) = (x^{3k} - x^k + \varepsilon_2)(x^{4k} + x^{2k} + \varepsilon_2 x^k + 1)$$

et hors des cas (α)–(δ) le polynôme $g(x)$ est irréductible.

Notons enfin que toutes les racines de $f(x)$ qui sont en même temps celles de l'unité (s'il en existe)

(a) sont simples à l'exception du cas où $n = 2m$ et $\varepsilon_2 = 1$, dans lequel elles sont doubles,

(b) satisfont à l'équation

$$x^d = \begin{cases} 1 & \text{si } \varepsilon_1 = -1 \qquad\qquad \text{et } \varepsilon_2 = 1, \\ -1 & \text{si } \varepsilon_1 = (-1)^{n_1+m_1+1} \text{ et } \varepsilon_2 = (-1)^{n_1}, \end{cases}$$

dans laquelle $d = (n, m)$, $n = dn_1$ et $m = dm_1$.

Cela élargit partiellement les résultats de Ljunggren (voir [1]), qui a étudié la réductibilité des polynômes

$$f(x) = x^n + \varepsilon_1 x^m + \varepsilon_2 x^p + \varepsilon_3 \quad \text{où} \quad n > m > p > 0 \quad \text{et} \quad \varepsilon_1, \varepsilon_2, \varepsilon_3 = \pm 1.$$

Travaux cités

[1] W. Ljunggren, *On the irreducibility of certain trinomials and quadrinomials*. Math. Scand. 8 (1960), 65–70.

[2] W. Sierpiński, *Remarques sur les progressions arithmétiques*. Colloquium Math. 3 (1954), 44–49.

Originally published in
Acta Arithmetica XI (1965), 1–34

On the reducibility of polynomials and in particular of trinomials

1.

In the course of this paper *reducibility* means reducibility over the rational field $\mathbb{Q}$ unless stated to the contrary. Constants are considered neither reducible nor irreducible. A factorization of a polynomial into a product of a constant and of coprime powers of irreducible polynomials is called its *standard form*. For a given polynomial $f(x) \neq 0$, $Kf(x)$ denotes the factor of $f(x)$ of the greatest possible degree, whose no root is 0 or a root of unity and whose leading coefficient is equal to the leading coefficient of $f(x)$. Clearly

$$Kf(x) = \frac{f(x)}{\left(f(x), x^d \prod\limits_{\varphi(\delta)\leqslant d} (x^\delta - 1)^d\right)},$$

where d is the degree of $f(x)$. The paper is emerged from the efforts to solve the following problem formulated in [4]:

Do there exist integers $a, b \neq 0$ *such that for infinitely many rational* r *one can find integers* m, n *satisfying*

(i) $m/n = r$,
(ii) $K(x^n + ax^m + b)$ *is reducible*?

The negative answer to this problem follows at once from Theorem 3 below; however, more general results are obtained. To state them I use the following notation:

If $\Phi(x_1, \ldots, x_k)$ is a rational function of the form $\sum\limits_{i=0}^{I} a_i \prod\limits_{j=1}^{k} x_j^{\alpha_{i,j}}$, where $a_i \neq 0$, $\alpha_{i,j}$ are integers and the systems $\langle \alpha_{i,1}, \ldots, \alpha_{i,k} \rangle$ are all different for $i \leqslant I$, then

$$J\Phi(x_1, \ldots, x_k) = \Phi(x_1, \ldots, x_k) \prod_{j=1}^{k} x_j^{-\min_i \alpha_{i,j}}.$$

Corrected following *Errata*, Acta Arith. 11 (1965), 491; and *Corrigenda*, ibid. 16 (1969), 159.

It is clear that $J\Phi(x_1, \ldots, x_k)$ is a polynomial and that the operation J as well as K is distributive with respect to multiplication. I prove

Theorem 1. *For every irreducible polynomial $F(x)$ not dividing $x^\delta - x$ ($\delta > 1$) and every positive integer n there exists an integer v satisfying the following conditions*:

(i) $0 < v \leqslant C(F)$;

(ii) $n = vu$, *u integer*;

(iii) *if $F(x^v) = F_1(x)F_2(x)\cdots F_r(x)$ is a standard form of $F(x^v)$, then*

$$F(x^n) = F_1(x^u)F_2(x^u)\cdots F_r(x^u)$$

is a standard form of $F(x^n)$.

$C(F)$ is an effectively computable constant independent of n.

Theorem 2. *For every irreducible polynomial $F(y, z)$ satisfying $JF(y, z) \neq \pm JF(y^{-1}, z^{-1})$ and for every pair of positive integers n, m there exists an integral non-singular matrix*

$$\begin{bmatrix} \nu_1 & \mu_1 \\ \nu_2 & \mu_2 \end{bmatrix}$$

satisfying the following conditions:

(i) $0 \leqslant \nu_i \leqslant C_1(F)$, $0 \leqslant \mu_i \leqslant C_1(F)$ $(i = 1, 2)$;

(ii) $n = \nu_1 u + \nu_2 v$, $m = \mu_1 u + \mu_2 v$, *u, v integers* $\geqslant 0$;

(iii) *if*

$$JF(y^{\nu_1}z^{\nu_2}, y^{\mu_1}z^{\mu_2}) = \text{const}\, F_1(y, z)^{e_1}F_2(y, z)^{e_2}\cdots F_r(y, z)^{e_r}$$

is a standard form of $JF(y^{\nu_1}z^{\nu_2}, y^{\mu_1}z^{\mu_2})$, then either

$$KF(x^n, x^m) = \text{const}\, KF_1(x^u, x^v)^{e_1}KF_2(x^u, x^v)^{e_2}\cdots KF_r(x^u, x^v)^{e_r}$$

is a standard form of $KF(x^n, x^m)$ or

$$\max\{n, m\} \leqslant C_0(F)(n, m).$$

$C_0(F)$ and $C_1(F)$ are effectively computable constants independent of n, m.

For every polynomial $F(x)$ to which Theorem 1 applies the number of irreducible factors of $F(x^n)$ remains bounded as n tends to infinity. On the other hand, if $F(x)$ is any cyclotomic polynomial $X_k(x)$ and $(n, k) = 1$, then

$$F(x^n) = X_k(x^n) = \prod_{d\,|\,n} X_{kd}(x);$$

thus the number of irreducible factors of $F(x^n)$ can be arbitrarily large. Therefore, the condition in Theorem 1 that $F(x)$ does not divide $x^\delta - x$ is necessary. On the other hand, it seems that the condition in Theorem 2: $JF(y, z) \neq \pm JF(y^{-1}, z^{-1})$, is too strong and could be replaced by the condition that $F(y, z)$ does not divide $yzJ(y^{\delta_1}z^{\delta_2} - 1)$ for any integers δ_1, δ_2 not both zero. Moreover, the following conjecture seems to me plausible.

Conjecture. *Let $F(y_1, \ldots, y_k)$ be an irreducible polynomial which does not divide $y_1 \cdots y_k J(y_1^{\delta_1} y_2^{\delta_2} \cdots y_k^{\delta_k} - 1)$ for any integers $\delta_1, \ldots, \delta_k$ not all zero.*

For every system of k positive integers $n_1, \ldots, n_k$ there exists an integral non-singular matrix $[v_{i,j}]$ $(1 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant k)$ satisfying the following conditions:

(i) $0 \leqslant v_{i,j} \leqslant C_1(F)$ $(1 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant k)$;

(ii) $n_i = \sum_{j=1}^{k} v_{i,j} u_j$ $(1 \leqslant i \leqslant k)$, *$u_j$ integers* $\geqslant 0$ $(1 \leqslant j \leqslant k)$;

(iii) *if*

$$JF\Big(\prod_{j=1}^{k} y_j^{v_{1,j}}, \prod_{j=1}^{k} y_j^{v_{2,j}}, \ldots, \prod_{j=1}^{k} y_j^{v_{k,j}}\Big) = \text{const}\, F_1(y_1, \ldots, y_k)^{e_1} \cdots F_r(y_1, \ldots, y_k)^{e_r}$$

is a standard form of $JF\Big(\prod_{j=1}^{k} y_j^{v_{1,j}}, \prod_{j=1}^{k} y_j^{v_{2,j}}, \ldots, \prod_{j=1}^{k} y_j^{v_{k,j}}\Big)$, then either

$$KF(x^{n_1}, \ldots, x^{n_k}) = \text{const}\, KF_1(x^{u_1}, \ldots, x^{u_k})^{e_1} \cdots KF_r(x^{u_1}, \ldots, x^{u_k})^{e_r}$$

is a standard form of $KF(x^{n_1}, \ldots, x^{n_k})$ or

$$\alpha_1 n_1 + \ldots + \alpha_k n_k = 0,$$

where α_i are integers not all zero and $|\alpha_i| \leqslant C_0(F)$ $(1 \leqslant i \leqslant k)$.

$C_0(F)$ and $C_1(F)$ are constants independent of $n_1, \ldots, n_k$.

The method of proof in Theorem 1 permits us to obtain an analogous result for reducibility in an arbitrary algebraic number field. The method of proof in Theorem 2 is valid only for totally real number fields and their totally complex quadratic extensions (in the latter case the condition $JF(y, z) \neq \pm JF(y^{-1}, z^{-1})$ should be replaced by $JF(y, z) \neq \text{const}\, \overline{JF(y^{-1}, z^{-1})}$). I do not know, however, any algebraic number field in which the Conjecture could be disproved.

The following theorem can easily be inferred from Theorems 1 and 2.

Theorem 3. *For any given non-zero integers a, b, c there exist two effectively computable constants $A(a, b, c)$ and $B(a, b, c)$ such that if $n > m > 0$ and $K(ax^n + bx^m + c)$ is reducible, then*

(i) $n/(n, m) \leqslant A(a, b, c)$,

(ii) *there exist integers ν and μ such that $m/\mu = n/\nu$ is integral, $0 < \mu < \nu \leqslant B(a, b, c)$ and if*

$$K(ax^{\nu} + bx^{\mu} + c) = \text{const}\, F_1^{e_1}(x) \cdots F_r^{e_r}(x)$$

is a standard form of $K(ax^{\nu} + bx^{\mu} + c)$, then

$$K(ax^n + bx^m + c) = \text{const}\, F_1^{e_1}(x^{n/\nu}) \cdots F_r^{e_r}(x^{n/\nu})$$

is a standard form of $K(ax^n + bx^m + c)$.

In order to complete the investigation of trinomials I also prove

Theorem 4. *If a, b, c are integers $\neq 0$, $0 < m < n$, $d = (m, n)$, $m = dm_1$, $n = dn_1$, ε, η denote ± 1, then*

$$\frac{ax^n + bx^m + c}{K(ax^n + bx^m + c)} = \begin{cases} x^{2d} + \varepsilon^{m_1}\left(\varepsilon^{n_1}\eta^{m_1}\right)x^d + 1, & \text{if } c = \varepsilon a = \eta b,\ n_1 + m_1 \equiv 0 \pmod 3,\ \varepsilon^{m_1} = \eta^{n_1}, \\ \left(x^d - (-\varepsilon)^{m_1}\varepsilon\eta\right)^2, & \text{if } c = \varepsilon a + \eta b,\ (-\varepsilon)^{m_1} = (-\eta)^{n_1},\ an\varepsilon + bm\eta = 0, \\ x^d - (-\varepsilon)^{m_1}\varepsilon\eta, & \text{if } c = \varepsilon a + \eta b,\ (-\varepsilon)^{m_1} = (-\eta)^{n_1},\ an\varepsilon + bm\eta \neq 0, \\ 1, & \text{otherwise.} \end{cases}$$

Theorems 3 and 4 generalize the results of papers [1], [3] and [2], in which the case $|a| = |c| = 1$ has been considered. The results of those papers could be expressed in the present language in the form $A(1, \pm 1, \pm 1) = 0$, $A(1, \pm 2, \pm 1) = B(1, \pm 2, \pm 1) = 7$, $A(1, \pm p, \pm 1) \leqslant 4^{p^2}$ (p prime > 2), respectively. The ideas of papers [1] and [2] are fundamental for the proof of Theorem 2. The Conjecture formulated above would give a result similar to Theorem 3 but concerning $(k+1)$-nomials.

As a second application of Theorem 2 I prove

Theorem 5. *Let $f(x) \not\equiv \pm 1$ be a polynomial such that $f(0) \neq 0$. There exist two constants $D_0(f)$ and $D_1(f) \neq 0$ such that if $n > D_0(f)$ and $\left(n, D_1(f)\right) = 1$, then $K\left(x^n + f(x)\right)$ is irreducible.*

It seems natural to ask whether the irreducibility of $K\left(x^n + f(x)\right)$ cannot be replaced in Theorem 5 by the irreducibility of $x^n + f(x)$ provided $f(1) \neq -1$. The example

$$f_0(x) = \frac{1}{12}(3x^9 + 8x^8 + 6x^7 + 9x^6 + 8x^4 + 3x^3 + 6x + 5)$$

shows that it is impossible. In fact, $f_0(1) \neq -1$ and $x^n + f_0(x)$ has for every n a factor in common with $x^{12} - 1$. I do not know whether a similar phenomenon can occur for polynomials with integral coefficients.

2.

Lemma 1. *Let Ω be an algebraic number field, and α an element of Ω which is not 0 or a root of unity.*

There exist only finitely many integers e such that $\alpha = w\beta^e$, where w is a root of unity, $\beta \in \Omega$. The greatest of them, $e(\alpha, \Omega)$, satisfies the following relations:

$$e(\alpha, \Omega) \leqslant (\exp 2N^2)\log\left(NH(\alpha)\right), \tag{1}$$

where N is the degree of Ω and $H(\alpha)$ is the height of the irreducible primitive polynomial of α,

$$e(\alpha^n, \Omega) = ne(\alpha, \Omega) \quad (n = 1, 2, \dots). \tag{2}$$

Proof. We note first that if $\gamma \in \Omega$ is an algebraic integer and $\gamma^{(i)}$ $(i = 1, \ldots, n)$ are all its conjugates, then

$$\frac{1}{N} \max_{1 \leqslant i \leqslant N} \left|\gamma^{(i)}\right| \leqslant H(\gamma) \leqslant \left(1 + \max_{1 \leqslant i \leqslant N} \left|\gamma^{(i)}\right|\right)^N. \tag{3}$$

This obvious inequality implies the following one:

$$\max_{1 \leqslant i \leqslant N} \left|\beta^{(i)}\right| > \exp\exp(-2N^2), \tag{4}$$

which holds for all integers $\beta \in \Omega$ which are not 0 or roots of unity. Indeed, assuming the contrary we would clearly have $N > 1$ and for all $k \leqslant \exp 2N^2$

$$\max_{1 \leqslant i \leqslant N} \left|(\beta^k)^{(i)}\right| \leqslant \exp 1.$$

Hence, by (3) applied to $\gamma = \beta^k$,

$$H(\beta^k) \leqslant (1 + \exp 1)^N \quad (1 \leqslant k \leqslant \exp 2N^2).$$

Now there are no more integers of degree $\leqslant N$ and height $\leqslant H$ than $N(2H+1)^N$; thus there are no more integers of degree $\leqslant N$ and height $\leqslant (1 + \exp 1)^N$ than

$$N\left(2(1 + \exp 1)^N + 1\right)^N < 3^N (1 + \exp 1)^{N^2} < \exp 2N^2 \quad (N > 1).$$

It follows that among the numbers β^k $(1 \leqslant k \leqslant \exp 2N^2)$ at least two are equal, whence β is a root of unity. The contradiction obtained proves (4).

Now we show that the equality

$$\alpha = w\beta^e, \tag{5}$$

where w is a root of unity, $\beta \in \Omega$, $e \geqslant 1$, implies

$$e \leqslant (\exp 2N^2) \log\left(N H(\alpha)\right). \tag{6}$$

This will prove the existence of $e(\alpha, \Omega)$ and inequality (1).

Let α be a zero of a primitive irreducible polynomial

$$a_0 x^m + \ldots + a_{m-1} x + a_m,$$

where $m \mid N$, a_i rational integers, $a_0 > 0$, $H(\alpha) = \max\limits_{0 \leqslant i \leqslant m} |a_i|$.

If $a_0 = 1$, α is an integer, and by (5), β is also an integer which is neither 0 nor a root of unity. It follows from (5) that

$$\log\Big(\max_{1 \leqslant i \leqslant N} \left|\alpha^{(i)}\right|\Big) = e \log\Big(\max_{1 \leqslant i \leqslant N} \left|\beta^{(i)}\right|\Big),$$

and hence by (3) applied to $\gamma = \alpha$ and by (4)

$$\log\left(N H(\alpha)\right) \geqslant e \exp(-2N^2),$$

which gives (6).

If $a_0 > 1$, $a_0\alpha$ is an integer but α is not. Therefore, there exists a prime ideal $\mathfrak{p}$ such that $\mathfrak{p}^\lambda \parallel a_0$, $\mathfrak{p}^\mu \parallel a_0\alpha$ and $\mu < \lambda$. Let $\mathfrak{p}^\nu \parallel a_0\beta$. It follows from (5) that $(\lambda - \mu) = (\lambda - \nu)e$, and

since $\lambda - \mu > 0$, we get $\lambda - \nu > 0$ and $e \leqslant \lambda - \mu \leqslant \lambda$. On the other hand, $(\operatorname{norm} \mathfrak{p})^{\lambda} \mid a_0^N$, hence

$$2^{\lambda} \leqslant a_0^N \leqslant H(\alpha)^N.$$

This gives

$$e \leqslant \lambda \leqslant \frac{N}{\log 2} \log H(\alpha) < (\exp 2N^2) \log\bigl(NH(\alpha)\bigr),$$

i.e. again (6).

In order to prove (2) we put $e(\alpha, \Omega) = e$, $e(\alpha^n, \Omega) = f$, $(n, f) = d$ and assume

$$\alpha = w_1 \beta^e, \quad \alpha^n = w_2 \gamma^f, \tag{7}$$

where w_1, w_2 are roots of unity, $\beta, \gamma \in \Omega$. Clearly $\alpha^n = w_1^n \beta^{ne}$, whence $f \geqslant ne$.

On the other hand, there exist integers p, q such that $pn - qf = d$ and it follows from (7) that

$$\bigl(\alpha(\alpha^q \gamma^{-p})^{f/d}\bigr)^d = \alpha^{d+qf} \gamma^{-pf} = \alpha^{pn} (w_2 \alpha^{-n})^p = w_2^p;$$

thus $\alpha(\alpha^q \gamma^{-p})^{f/d}$ is a root of unity, say w_3. We get

$$\alpha = w_3 (\alpha^{-q} \gamma^p)^{f/d}$$

and, by the definition of e, $e \geqslant f/d \geqslant f/n \geqslant e$. This gives $f = ne$ and completes the proof. □

Lemma 2. *Let Ω be an algebraic number field and α an element of Ω which is not 0 or a root of unity. For every positive integer n we put*

$$\nu = \nu(\alpha, \Omega, n) = \bigl(n, 2^{e(\alpha, \Omega) - 1} e(\alpha, \Omega)!\bigr).$$

If $g(x)$ is a monic polynomial irreducible over Ω and $g(x) \mid x^n - \alpha$, then $g(x) = G(x^{n/\nu})$, where $G(x)$ is a polynomial over Ω.

Proof. We proceed by induction with respect to $e(\alpha, \Omega)$. If $e(\alpha, \Omega) = 1$, then neither $\alpha = \beta^p$, $p > 1$, nor $\alpha = -4\beta^4$, $\beta \in \Omega$; thus, in view of a theorem of Capelli (for the proof and references see [5], pp. 288–294), $x^n - \alpha$ is irreducible in Ω and $g(x) = x^n - \alpha$. The lemma holds with $G(x) = x - \alpha$. Assume that the lemma is true for all Ω' and α' with $e(\alpha', \Omega') < m$ $(m > 1)$ and let $e(\alpha, \Omega) = m$, $g(x) \mid x^n - \alpha$.

If $x^n - \alpha$ is irreducible, then the lemma is trivially true with $G(x) = x^{\nu} - \alpha$. If it is reducible, then by the theorem of Capelli

(A) $\alpha = \beta^p$, where $p \mid n$, p prime > 1, $\beta \in \Omega$,

or

(B) $\alpha = -4\beta^4$, where $4 \mid n$, $\beta \in \Omega$.

We consider these cases successively, using the following notation: ζ_q is a primitive qth root of unity, $\Omega_q = \Omega(\zeta_q)$, d_q is the degree of Ω_q over Ω, $N_{\Omega_q/\Omega}$ is the norm of elements of Ω_q or polynomials over Ω_q relative to Ω.

(A) We have here

$$g(x) \mid x^n - \beta^p = (x^{n/p} - \beta) \prod_{r=1}^{p-1} (x^{n/p} - \zeta_p^r \beta). \tag{8}$$

If $g(x) \mid x^{n/p} - \beta$ our inductive assumption applies directly, since by (A) and Lemma 1

$$m = e(\alpha, \Omega) = pe(\beta, \Omega) > e(\beta, \Omega). \tag{9}$$

Putting $\nu_0 = \nu(\beta, \Omega, n/p)$ we have

$$\nu_0 \mid \big(n/p, 2^{m-2}(m-1)!\big), \quad g(x) = G_0(x^{n/p\nu_0}),$$

$G_0(x) \in \Omega[x]$ and it is sufficient to take $G(x) = G_0(x^{\nu/p\nu_0})$.

If $g(x) \nmid x^{n/p} - \beta$, let $h(x)$ be a monic factor of $g(x)$ irreducible over Ω_p. By (8)

$$h(x) \mid g(x) \Big| \prod_{r=1}^{p-1} (x^{n/p} - \zeta_p^r \beta);$$

thus for some positive $r < p$

$$h(x) \mid x^{n/p} - \zeta_p^r \beta. \tag{10}$$

Let $h^{(1)}(x) = h(x), \ldots, h^{(d_p)}(x)$ be all the conjugates of $h(x)$ relative to Ω. It follows from (10) that

$$\big(h^{(i)}(x), h^{(j)}(x)\big) \mid \beta\big(\zeta_p^{(i)r} - \zeta_p^{(j)r}\big) \quad (1 \leqslant i \leqslant j \leqslant d_p);$$

thus $h^{(i)}(x)$ $(i = 1, 2, \ldots, d_p)$ are relatively prime in pairs.

Since $h^{(i)}(x) \mid g(x)$, it follows that

$$g(x) = N_{\Omega_p/\Omega}\big(h(x)\big). \tag{11}$$

On the other hand, we have $e\big(\zeta_p^r \beta, \Omega_p\big) = e_1 < m$. Indeed, if

$$\zeta_p^r \beta = w\gamma^{e_1}, \quad w \text{ a root of unity, } \gamma \in \Omega_p,$$

then

$$\alpha = \beta^p = w^p \gamma^{pe_1} \quad \text{and} \quad \alpha^{d_p} = N_{\Omega_p/\Omega}(w^p)\big(N_{\Omega_p/\Omega}(\gamma)\big)^{pe_1}.$$

It follows by Lemma 1 that

$$d_p m = e(\alpha^{d_p}, \Omega) > pe_1$$

and, since $d_p \leqslant p - 1$, $e_1 < m$.

Applying the inductive assumption to (10) and putting

$$\nu_1 = \nu\big(\zeta_p^r \beta, \Omega_p, n/p\big),$$

we get

$$\nu_1 \mid \big(n/p, 2^{m-2}(m-1)!\big), \quad h(x) = H(x^{n/p\nu_1}), \quad H(x) \in \Omega_p[x]. \tag{12}$$

Since $p \mid m$ by (9), we have $\nu_1 p \mid (n, 2^{m-1}m!) = \nu$ and it is sufficient to put

$$G(x) = N_{\Omega_p/\Omega}\big(H(x^{\nu/p\nu_1})\big).$$

Indeed, by (11) and (12)

$$g(x) = N_{\Omega_p/\Omega}\big(H(x^{n/p\nu_1})\big) = G(x^{n/\nu}).$$

(B) We have here

$$g(x) \mid x^n + 4\beta^4 = \prod_{\varepsilon\eta=\pm 1} \big(x^{n/4} - (\varepsilon + \eta\zeta_4)\beta\big).$$

Let $h(x)$ be a monic factor of $g(x)$ irreducible over Ω_4. There is a pair of integers ε, η such that $\varepsilon\eta = \pm 1$,

$$h(x) \mid x^{n/4} - (\varepsilon + \eta\zeta_4)\beta. \tag{13}$$

It follows, like (11) from (10), that

$$g(x) = N_{\Omega_4/\Omega}\big(h(x)\big). \tag{14}$$

On the other hand, $e\big((\varepsilon + \eta\zeta_4)\beta, \Omega_4\big) = e_2 < m$. Indeed, if

$$(\varepsilon + \eta\zeta_4)\beta = w\gamma^{e_2}, \quad w \text{ a root of unity, } \gamma \in \Omega_4,$$

then

$$\alpha = -4\beta^4 = w^4\gamma^{4e_2} \quad \text{and} \quad \alpha^{d_4} = N_{\Omega_4/\Omega}(w^4)\big(N_{\Omega_4/\Omega}(\gamma)\big)^{4e_2}.$$

It follows by Lemma 1 that

$$d_4 m = e(\alpha^{d_4}, \Omega) > 4e_2$$

and since $d_4 \leqslant 2$, $e_2 < m$.

Applying the inductive assumption to (13) and putting

$$\nu_2 = \nu(\varepsilon + \eta\zeta_4, \Omega_4, n/4)$$

we get

$$\nu_2 \mid \big(n/4, 2^{m-2}(m-1)!\big), \quad h(x) = H(x^{n/4\nu_2}), \quad H(x) \in \Omega_4[x]. \tag{15}$$

By Lemma 1 and (B) $m = e(a, \Omega) = 2e(2\beta^2, \Omega)$. Thus $2 \mid m$ and by (15) $4\nu_2 \mid (n, 2^{m-1}m!) = \nu$. Now put

$$G(x) = N_{\Omega_4/\Omega}\big(H(x)^{\nu/4\nu_2}\big).$$

By (14) and (15)

$$g(x) = N_{\Omega_4/\Omega}\big(H(x)^{n/4\nu_2}\big) = G(x^{n/\nu}),$$

which completes the inductive proof. □

Proof of Theorem 1. Put $C(F) = \exp\big((2N^2 + \log\log NH)(\exp 2N^2)\log NH\big)$, where N is the degree of F and H its height. Let a_0 be the leading coefficient of F, α any of its zeros and $\Omega = \mathbb{Q}(\alpha)$. For any given n, we put $\nu = \big(n, 2^{e(a,\Omega)-1}e(a, \Omega)!\big)$. Clearly

$\nu \leqslant e(a, \Omega)^{e(a,\Omega)}$ and by Lemma 1, $\nu \leqslant C(F)$. Besides, $u = n/\nu$ is an integer; thus parts (i) and (ii) of Theorem 1 are proved. In order to prove (iii) assume that

$$F(x^{\nu}) = F_1(x) \cdots F_r(x) \tag{16}$$

is a standard form of $F(x^{\nu})$ (since $F(x)$ is irreducible, there are no multiple factors). Clearly $F_j(x^u)$ $(1 \leqslant j \leqslant r)$ are relatively prime in pairs and it remains to show that they are all irreducible. Let $f_j(x)$ be a monic irreducible factor of $F_j(x^u)$. Clearly

$$f_j(x) \mid F(x^n). \tag{17}$$

We now use the following Lemma of Capelli (cf. [5], pp. 288–290): if

$$x^n - \alpha = \prod_{i=1}^{l} g_i(x) \tag{18}$$

is a decomposition of $x^n - \alpha$ into monic factors irreducible over $\mathbb{Q}(\alpha) = \Omega$ and $N_{\Omega/\mathbb{Q}}$ denotes the norm relative to $\mathbb{Q}$, then

$$F(x^n) = a_0 \prod_{i=1}^{l} N_{\Omega/\mathbb{Q}}\big(g_i(x)\big) \tag{19}$$

is the decomposition of $F(x^n)$ into monic factors irreducible over $\mathbb{Q}$.

It follows from (17) and (19) that for some $i \leqslant l$

$$f_j(x) = N_{\Omega/\mathbb{Q}} g_i(x). \tag{20}$$

On the other hand, it follows from (18) and Lemma 2 that

$$g_i(x) = G_i(x^u), \tag{21}$$

where $G_i(x)$ is a polynomial over Ω.

By (20), (21) and the choice of $f_j(x)$

$$f_j(x) = N_{\Omega/\mathbb{Q}} G_i(x^u) \mid F_j(x^u); \tag{22}$$

thus

$$N_{\Omega/\mathbb{Q}} G_i(x) \mid F_j(x).$$

Since $F_j(x)$ is irreducible,

$$F_j(x) = \text{const}\, N_{\Omega/\mathbb{Q}} G_i(x);$$

thus by (22)

$$F_j(x^u) = \text{const}\, f_j(x)$$

and by the choice of $f_j(x)$, $F_j(x^u)$ is irreducible. This completes the proof. □

Corollary to Theorem 1. *For every polynomial* $F(x) \neq 0$ *and every positive integer* n *there exists an integer* ν *satisfying the following conditions*:

$$0 \leqslant \nu \leqslant C'(F); \tag{23}$$

$$n = \nu u, \quad u\text{—an integer}; \tag{24}$$

if $KF(x^\nu) = \text{const}\, F_1(x)^{e_1} F_2(x)^{e_2} \cdots F_r(x)^{e_r}$ *is a standard form of* $KF(x^\nu)$, *then*

$$KF(x^n) = \text{const}\, F_1(x^u)^{e_1} F_2(x^u)^{e_2} \cdots F_r(x^u)^{e_r}$$

is a standard form of $KF(x^n)$.

Proof. Let $KF(x) = \text{const}\, \Phi_1^{\varepsilon_1}(x)\Phi_2^{\varepsilon_2}(x) \cdots \Phi_\varrho^{\varepsilon_\varrho}(x)$ be a standard form of $KF(x)$.

Since each polynomial $\Phi_i(x)$ $(1 \leqslant i \leqslant \varrho)$ satisfies the conditions of Theorem 1, there exists for each $i \leqslant \varrho$ a positive integer ν_i satisfying the following conditions:

$0 < \nu_i \leqslant C(\Phi_i)$; $n = \nu_i u_i$, u_i—an integer;

if $\Phi_i(x^{\nu_i}) = \Phi_{i,1}(x)\Phi_{i,2}(x) \cdots \Phi_{i,r_i}(x)$ is a standard form of $\Phi_i(x^{\nu_i})$, then

$$\Phi_i(x^n) = \Phi_{i,1}(x^{u_i})\Phi_{i,2}(x^{u_i}) \cdots \Phi_{i,r_i}(x^{u_i})$$

is a standard form of $\Phi_i(x^n)$.

We put

$$\nu = [\nu_1, \ldots, \nu_\varrho], \quad C'(F) = \Big(\max_{1 \leqslant i \leqslant \varrho} C(\Phi_i)\Big)!.$$

Conditions (23) and (24) are clearly satisfied. Since $\nu_i \mid \nu$ we have $u \mid u_i$ and the irreducibility of $\Phi_{i,j}(x^{u_i})$ implies the irreducibility of $\Phi_{i,j}(x^{u_i/u})$ $(1 \leqslant i \leqslant \varrho,\ 1 \leqslant j \leqslant r_i)$. Since polynomials $\Phi_{i,j}$ are relatively prime in pairs, it follows that

$$KF(x^\nu) = \text{const} \prod_{i=1}^{\varrho} \prod_{j=1}^{r_i} \Phi_{i,j}(x^{u_i/u})^{\varepsilon_i}$$

is a standard form of $KF(x^\nu)$ and

$$KF(x^n) = \text{const} \prod_{i=1}^{\varrho} \prod_{j=1}^{r_i} \Phi_{i,j}(x^{u_i})^{\varepsilon_i}$$

is a standard form of $KF(x^n)$. This completes the proof. □

3.

Lemma 3. *For any two relatively prime polynomials* $G(y, z) \neq 0$, $H(y, z) \neq 0$ *there exist two constants* $B_0(G, H) = B_0 \geqslant 1$ *and* $B_1(G, H)$ *such that if* n, m *are positive integers, then*

$$\left(\frac{JG(x^n, x^m)}{KG(x^n, x^m)}, \frac{JH(x^n, x^m)}{KH(x^n, x^m)}\right) \Bigg| \left(x^{(n,m)B_0} - 1\right)^{B_0}, \tag{25}$$

$$\big(KG(x^n, x^m), KH(x^n, x^m)\big) = 1 \tag{26}$$

unless $\max\{n, m\} \leqslant B_1(G, H)(n, m)$.

Proof. Let $R(z)$ be the resultant of polynomials $G(y, z)$ and $H(y, z)$ with respect to y and $S(y)$ their resultant with respect to z, and $D = \max\{\text{degree } R, \text{degree } S\}$.

Let $e^{2\pi i r_1}$, $e^{2\pi i r_2}$, ..., $e^{2\pi i r_k}$ be all the roots of unity which are zeros of R and $\varrho_1, \varrho_2, \ldots, \varrho_k$ their respective multiplicities, and similarly let

$$e^{2\pi i s_1},\ e^{2\pi i s_2},\ \ldots,\ e^{2\pi i s_l}$$

be all the roots of unity which are zeros of S and $\sigma_1, \sigma_2, \ldots, \sigma_l$ their respective multiplicities. Let d be the least common denominator of $1, r_1, \ldots, r_k, s_1, \ldots, s_l$. We put

$$B_0 = B_0(G, H) = d \max\Big\{1, \max_{1\leqslant i\leqslant k} \varrho_i, \max_{1\leqslant j\leqslant l} \sigma_j\Big\}, \quad B_1(G, H) = DC'(R)C'(S),$$

where C' is a constant from the Corollary to Theorem 1. Clearly

$$\frac{JR(z)}{KR(z)} \,\Big|\, (z^{B_0} - 1)^{B_0}, \quad \frac{JS(y)}{KS(y)} \,\Big|\, (y^{B_0} - 1)^{B_0},$$

whence

$$\frac{JR(x^m)}{KR(x^m)} \,\Big|\, (x^{mB_0} - 1)^{B_0}, \quad \frac{JS(x^n)}{KS(x^n)} \,\Big|\, (x^{nB_0} - 1)^{B_0};$$
$$\left(\frac{JR(x^m)}{KR(x^m)}, \frac{JS(x^n)}{KS(x^n)}\right) \,\Big|\, (x^{(n,m)B_0} - 1)^{B_0}.$$

Since

$$\big(G(x^n, x^m), H(x^n, x^m)\big) \,\big|\, \big(R(x^m), S(x^n)\big), \tag{27}$$

(25) follows. In order to prove (26), assume that $f(x)$ is an irreducible polynomial such that

$$f(x) \,|\, \big(KG(x^n, x^m), KH(x^n, x^m)\big).$$

By (27)

$$f(x) \,|\, KR(x^m) \quad \text{and} \quad f(x) \,|\, KS(x^n).$$

Now by the Corollary to Theorem 1 there exist a $\mu \leqslant C'(R)$ and a polynomial $F_1(x)$ such that

$$f(x) = F_1(x^{m/\mu}) \quad \text{and} \quad F_1(x) \,|\, KR(x^\mu). \tag{28}$$

Similarly there exist a $\nu \leqslant C'(S)$ and a polynomial $F_2(x)$ such that

$$f(x) = F_2(x^{n/\nu}) \quad \text{and} \quad F_2(x) \,|\, KS(x^\nu). \tag{29}$$

Let d_1, d_2 be the degrees of F_1 and F_2 respectively. It follows from (28) and (29) that

$$d_1 \frac{m}{\mu} = d_2 \frac{n}{\nu}, \quad d_1 \leqslant D\mu, \quad d_2 \leqslant D\nu.$$

Hence $\max\{n, m\}/(n, m) \leqslant D\mu\nu \leqslant DC'(R)C'(S) = B_1(G, H)$, which completes the proof. □

Lemma 4. *Let k_i $(0 \leqslant i \leqslant l)$ be an increasing sequence of integers. Let $k_{j_1} - k_{i_1}$, $\ldots, k_{j_P} - k_{i_P}$ $(P \geqslant 0)$ be all the numbers besides $k_l - k_0$ which appear only once in*

the double sequence $k_j - k_i$ $(0 \leqslant i < j \leqslant l)$. *Suppose that for each pair* p, q, *where* $1 \leqslant p < q \leqslant P$

$$c_{p,q}(k_l - k_0) + c'_{p,q}(k_{j_p} - k_{i_p}) + c''_{p,q}(k_{j_q} - k_{i_q}) = 0, \tag{30}$$

where $c_{p,q}$, $c'_{p,q}$, $c''_{p,q}$ *are integers not all zero. Let* $c = 1$ *if* $P < 2$ *and* $c = \max_{1 \leqslant p < q \leqslant P} \max\{|c_{p,q}|, |c'_{p,q}|, |c''_{p,q}|\}$ *if* $P \geqslant 2$. *Then there exist integers* $s, t, \kappa_i, \lambda_i$ $(0 \leqslant i \leqslant l)$ *such that*

$$k_i - k_0 = s\kappa_i + t\lambda_i \quad (0 \leqslant i \leqslant l),$$
$$|\kappa_i| < (5c)^l, \quad |\lambda_i| < (5c)^l \quad (0 \leqslant i \leqslant l).$$

Proof. By the assumption, for each pair $\langle i, j\rangle$, where $0 \leqslant i < j \leqslant l$ and $\langle i, j\rangle \neq \langle 0, l\rangle, \langle i_1, j_1\rangle, \ldots, \langle i_P, j_P\rangle$ there exists a pair $\langle g_{i,j}, h_{i,j}\rangle \neq \langle i, j\rangle$ such that

$$k_j - k_i = k_{h_{i,j}} - k_{g_{i,j}}.$$

Let us consider the system of linear homogeneous equations

$$\begin{aligned} &x_0 = 0, \\ &x_j - x_i = x_{h_{i,j}} - x_{g_{i,j}}, \quad \langle i, j\rangle \neq \langle 0, l\rangle, \langle i_1, j_1\rangle, \ldots, \langle i_P, j_P\rangle, \\ &c_{p,q}x_l + c'_{p,q}(x_{j_p} - x_{i_p}) + c''_{p,q}(x_{j_q} - x_{i_q}) = 0, \quad 1 \leqslant p < q \leqslant P. \end{aligned} \tag{31}$$

$\mathfrak{k} = [0, k_1 - k_0, \ldots, k_l - k_0]$ is a solution of this system. Suppose that there are two other linearly independent solutions, $\mathfrak{a} = [a_0, a_1, \ldots, a_l]$ and $\mathfrak{b} = [b_0, b_1, \ldots, b_l]$. Performing linear transformations on the system $\mathfrak{k}, \mathfrak{a}, \mathfrak{b}$ we shall denote by $\mathfrak{a}^{(\nu)}$, $\mathfrak{b}^{(\nu)}$ the successive images of $\mathfrak{a}$ and $\mathfrak{b}$, and by $a_i^{(\nu)}$, $b_i^{(\nu)}$ the components of $\mathfrak{a}^{(\nu)}$, $\mathfrak{b}^{(\nu)}$ respectively.

Put

$$\mathfrak{a}' = \mathfrak{a} - \frac{a_l}{k_l - k_0}\mathfrak{k}, \quad \mathfrak{b}' = \mathfrak{b} - \frac{b_l}{k_l - k_0}\mathfrak{k},$$

i'—the least i such that $a'_i = \min_{0 \leqslant j \leqslant l} a'_j$ or $\max_{0 \leqslant j \leqslant l} a'_j$,

j'—the greatest i such that $a'_i = \min_{0 \leqslant j \leqslant l} a'_j + \max_{0 \leqslant j \leqslant l} a'_j - a'_{i'}$ (the opposite extremum).

Clearly $j' > i'$. Since $\mathfrak{a}' \neq 0$ and $a'_0 = 0$, it follows from the definition of j' that $a'_{j'} \neq 0$.

Put

$$\mathfrak{b}'' = \mathfrak{b}' - \frac{b'_{j'}}{a'_{j'}}\mathfrak{a}',$$

i''—the least i such that $b''_i = \min_{0 \leqslant j \leqslant l} b''_j$ or $\max_{0 \leqslant j \leqslant l} b''_j$,

j''—the greatest i such that $b''_i = \min_{0 \leqslant j \leqslant l} b''_j + \max_{0 \leqslant j \leqslant l} b''_j - b''_{i''}$.

Clearly $j'' > i''$. $\mathfrak{a}'$ and $\mathfrak{b}''$ are solutions of the system (31) and satisfy the following conditions:

$$a'_{j'} \neq 0 = a'_l, \tag{32}$$

(33) all a'_i are in the interval $\left\langle a'_{i'}, a'_{j'}\right\rangle$, $a'_i \neq a'_{i'}$ for $i < i'$, $a'_i \neq a'_{j'}$ for $i \leqslant i'$ and for $i > j'$,

(34) $b''_{j''} \neq 0 = b''_{j'} = b''_l$,

(35) all b''_i are in the interval $\left\langle b''_{i''}, b''_{j''}\right\rangle$, $b''_i \neq b''_{i''}$ for $i < i''$, $b''_i \neq b''_{j''}$ for $i \leqslant i''$ and for $i > j''$.

Now, (32) and (33) imply that $\langle i', j'\rangle$ is for some $p \leqslant P$ identical with $\langle i_p, j_p\rangle$. Indeed, by (32), $\langle i', j'\rangle \neq \langle 0, l\rangle$, whence we would have in the opposite case

$$a'_{j'} - a'_{i'} = a'_h - a'_g, \quad \text{where} \quad \langle g, h\rangle = \left\langle g_{i',j'}, h_{i',j'}\right\rangle \neq \langle i', j'\rangle.$$

It follows from (33) that $a'_h = a'_{j'}$, $a'_g = a'_{i'}$, whence $g \geqslant i'$, $h \leqslant j'$.

On the other hand,

$$k_{j'} - k_{i'} = k_h - k_g$$

and since k_i are increasing, $g = i'$, $h = j'$, which gives a contradiction. Similarly, (34) and (35) imply that $\langle i'', j''\rangle$ is $\langle i_q, j_q\rangle$, where $1 \leqslant q \leqslant P$.

Moreover, by (34) $\langle i', j'\rangle \neq \langle i'', j''\rangle$. Thus $p \neq q$ and without loss of generality we may assume $p < q$. Putting for brevity $c'_{p,q} = c'$ and $c''_{p,q} = c''$, we get from (30), (32) and (34)

$$c_{p,q}(k_l - k_0) + c'(k_{j'} - k_{i'}) + c''(k_{j''} - k_{i''}) = 0, \tag{36}$$

$$c'(a'_{j'} - a'_{i'}) + c''(a'_{j''} - a'_{i''}) = 0, \tag{37}$$

$$c'(b''_{j'} - b''_{i'}) + c''(b''_{j''} - b''_{i''}) = 0. \tag{38}$$

Since $k_l > k_0$, it follows from (36) that $c' \neq 0$ or $c'' \neq 0$. Now in view of (33) and (37) $|c''| \geqslant |c'|$, and in view of (35) and (38) $|c'| \geqslant |c''|$. Hence $c' = \pm c'' \neq 0$. If $c' = -c''$, (35) and (38) imply that $b''_{j'} = b''_{j''}$, which contradicts (34). If $c' = c''$, (33) and (37) imply that $a'_{i''} = a'_{j'}$, $i'' > i'$. Similarly (35) and (38) imply that $b''_{i'} = b''_{j''}$, $i' > i''$. The contradiction obtained proves that system (31) has at most two linearly independent solutions. Therefore, the rank of the matrix M of system (31) is at least $l - 1$. If this rank is l, solving the system by means of Cramer's formulae we get

$$x_i = x_\mu D_i / D \quad (0 \leqslant i \leqslant l,\ \mu \text{ fixed}),$$

[c] where D and D_i are determinants of order l and, as can easily be seen from the form of matrix M, the sum of the absolute values of integers standing in any line of D_i does not exceed $5c$. Hence $|D_i| < (5c)^l$ and *a fortiori* $|D_i|/(D_0, \ldots, D_l) < (5c)^l$.

Since

$$\frac{(k_\mu - k_0)D_i}{D} = k_i - k_0 \quad (0 \leqslant i \leqslant l),$$

$(k_\mu - k_0)(D_0, \ldots, D_l)/D$ is an integer and the lemma holds with

$$s = (k_\mu - k_0)(D_0, \ldots, D_l)/D, \quad t = 0,$$
$$\kappa_i = D_i/(D_0, \ldots, D_l), \quad \lambda_i = 0 \quad (0 \leqslant i \leqslant l).$$

If the rank of M is $l-1$, we get similarly

$$x_i = (x_\mu D_i' + x_\nu D_i'')/D \quad (0 \leqslant i \leqslant l,\ \mu, \nu \text{ fixed}),$$

where D, D_i' and D_i'' are determinants of order $l-1$,

$$|D_i'| < (5c)^{l-1}, \quad |D_i''| < (5c)^{l-1} \quad (0 \leqslant i \leqslant l). \tag{39}$$

Integral vectors $[x_\mu, x_\nu]$ such that all numbers $(x_\mu D_i' + x_\nu D_i'')/D$ $(0 \leqslant i \leqslant l)$ are integers form a module, say $\mathfrak{M}$. Clearly $[0, |D|] \in \mathfrak{M}$ and $[|D|, 0] \in \mathfrak{M}$. Let ξ_1 be the least positive integer such that for some η_1, $[\xi_1, \eta_1] \in \mathfrak{M}$ and let η_2 be the least positive integer such that $[0, \eta_2] \in \mathfrak{M}$. Clearly $[\xi_1, \eta_1]$ and $[0, \eta_2]$ form a basis for $\mathfrak{M}$ and without loss of generality we may assume $0 \leqslant \eta_1 < \eta_2$. On the other hand, $\eta_2 \leqslant |D|$ and $\xi_1 \leqslant |D|$. Since k_i are integers, $[k_\mu - k_0, k_\nu - k_0] \in \mathfrak{M}$; thus there are integers s, t such that $k_\mu - k_0 = \xi_1 s$, $k_\nu - k_0 = \eta_1 s + \eta_2 t$.

Putting $\kappa_i = (\xi_1 D_i' + \eta_1 D_i'')/D$, $\lambda_i = \eta_2 D_i''/D$, we get for $i \leqslant l$

$$k_i - k_0 = \kappa_i s + \lambda_i t$$

and by (39)

$$|\kappa_i| \leqslant \frac{\xi_1}{|D|}\,|D_i'| + \frac{\eta_1}{|D|}\,|D_i''| \leqslant 2(5c)^{l-1} < (5c)^l,$$

$$|\lambda_i| \leqslant \frac{\eta_2}{|D|}\,|D_i''| < (5c)^{l-1}.$$

This completes the proof. □

Remark. For a given finite linear set, denote by ϱ the number of distances linearly independent over $\mathbb{Q}$ and by ρ_0 the number of linearly independent distances which appear only once. It follows from the lemma that if $\varrho_0 \leqslant 2$, then $\varrho \leqslant 2$. It can easily be found from remark 1 at the end of paper [2] that if $\varrho_0 = 1$ then $\varrho = 1$. The equality $\varrho = \varrho_0$ suggests itself, but I am unable to prove it.

Definition. For a given integral matrix A, $h(A)$ will denote the maximum of absolute values of the elements of A.

Lemma 5. *Let Γ be any given integral matrix 2×2. For arbitrary positive integers d, n, m there exists an integral matrix*

$$M = \begin{bmatrix} \nu_1 & \mu_1 \\ \nu_2 & \mu_2 \end{bmatrix}$$

satisfying the conditions:

$$0 \leqslant \nu_i \leqslant \left((2d^2)!\right)^2, \quad 0 \leqslant \mu_i \leqslant \left((2d^2)!\right)^2 \quad (i = 1, 2), \tag{40}$$

$$|M| > 0, \tag{41}$$

$$[n, m] = [u, v]M, \quad u, v \text{ integers} \geqslant 0, \tag{42}$$

and with the following property. If

$$[n, m]\Gamma = [s, t]\Delta, \tag{43}$$

where s, t are integers, Δ is an integral matrix,

$$|\Delta| \neq 0 \quad \textit{and} \quad h(\Delta) \leqslant d, \tag{44}$$

then

$$M\Gamma = T\Delta \quad \textit{and} \quad [s,t] = [u,v]T, \tag{45}$$

where T is an integral matrix and

$$h(T) \leqslant 4d\big((2d^2)!\big)^2 h(\Gamma). \tag{46}$$

Proof. Let S be the set of all integral matrices Δ satisfying (43) and (44). Integral vectors $[x, y]$ such that for all $\Delta \in S$ and suitable integers s_Δ, t_Δ, $[x, y]\Gamma = [s_\Delta, t_\Delta]\Delta$ form a module, say $\mathfrak{M}$. By (44) $(2d^2) \geqslant |\Delta| \neq 0$, whence $|\Delta|$ divides $(2d^2)!$.

It follows that $[(2d^2)!, 0] \in \mathfrak{M}$ and $[0, (2d^2)!] \in \mathfrak{M}$. Let ξ_1 be the least positive integer such that, for some η_1, $[\xi_1, \eta_1] \in \mathfrak{M}$ and let η_2 be the least positive integer such that $[0, \eta_2] \in \mathfrak{M}$. Clearly $[\xi_1, \eta_1]$ and $[0, \eta_2]$ form a basis for $\mathfrak{M}$ and we may assume without loss of generality that $0 \leqslant \eta_1 < \eta_2$. Hence

$$0 < \xi_1 \leqslant (2d^2)!, \quad 0 \leqslant \eta_1 < \eta_2 \leqslant (2d^2)!. \tag{47}$$

Let

$$\frac{\eta_1}{\eta_2} = \frac{1}{\lfloor b_1} - \frac{1}{\lfloor b_2} - \ldots - \frac{1}{\lfloor b_r}$$

be the expansion of η_1/η_2 into a continued fraction, where b_p are integers > 1 $(1 \leqslant p \leqslant r)$; if $\eta_1 = 0$ let $r = 0$. Put

$$A_{-1} = -1, \quad B_{-1} = 0; \quad A_0 = 0, \quad B_0 = 1;$$

$$A_{p+1} = b_{p+1}A_p - A_{p-1}, \quad B_{p+1} = b_{p+1}B_p - B_{p-1} \quad (0 \leqslant p < r).$$

It follows that the sequences A_p, B_p are increasing and for $0 \leqslant p \leqslant r$

$$A_pB_{p-1} - B_pA_{p-1} = 1, \tag{48}$$

$$0 \leqslant A_p \leqslant \eta_1, \quad 0 < B_p \leqslant \eta_2, \tag{49}$$

$$A_p/B_p < A_r/B_r = \eta_1/\eta_2 \quad (\text{if } p < r). \tag{50}$$

Since $m > 0, n > 0$, we have

$$\frac{\eta_1}{\eta_2} - \frac{m}{n} \cdot \frac{\xi_1}{\eta_2} < \frac{A_r}{B_r}.$$

Let q be the least non-negative integer which can be substituted for r in the last inequality. Assuming $A_{-1}/B_{-1} = -\infty$ we have therefore

$$\frac{A_{q-1}}{B_{q-1}} \leqslant \frac{\eta_1}{\eta_2} - \frac{m}{n} \cdot \frac{\xi_1}{\eta_2} < \frac{A_q}{B_q}. \tag{51}$$

Let us put

$$M = \begin{bmatrix} \nu_1 & \mu_1 \\ \nu_2 & \mu_2 \end{bmatrix} = \begin{bmatrix} B_q & -A_q \\ B_{q-1} & -A_{q-1} \end{bmatrix} \begin{bmatrix} \xi_1 & \eta_1 \\ 0 & \eta_2 \end{bmatrix} = \begin{bmatrix} B_q\xi_1 & B_q\eta_1 - A_q\eta_2 \\ B_{q-1}\xi_1 & B_{q-1}\eta_1 - A_{q-1}\eta_2 \end{bmatrix}.$$

Inequalities (47), (49) and (50) imply (40). By (48)

$$|M| = \begin{vmatrix} \xi_1 & \eta_1 \\ 0 & \eta_2 \end{vmatrix} = \xi_1\eta_2 > 0.$$

Moreover, the vectors $[\nu_1, \mu_1]$, $[\nu_2, \mu_2]$ form a basis for $\mathfrak{M}$. Since $[n, m] \in \mathfrak{M}$, there are integers u, v satisfying (42). We have

$$[u, v] = [n, m]M^{-1} = \frac{1}{\xi_1\eta_2}[n, m]\begin{bmatrix} B_{q-1}\eta_1 - A_{q-1}\eta_2 & -B_q\eta_1 + A_q\eta_2 \\ -B_{q-1}\xi_1 & B_q\xi_1 \end{bmatrix}$$

$$= \frac{1}{\xi_1\eta_2}\big[B_{q-1}(n\eta_1 - m\xi_1) - A_{q-1}\eta_2,\, A_q\eta_2 - B_q(n\eta_1 - m\xi_1)\big].$$

It follows from (51) that $u \geqslant 0$, $v \geqslant 0$. In order to prove the last statement of the lemma suppose that for some integral matrix Δ (43) and (44) hold. Thus $\Delta \in S$ and since $[\nu_i, \mu_i] \in \mathfrak{M}$ $(i = 1, 2)$ there are integers σ_i, τ_i such that $[\nu_i, \mu_i]\Gamma = [\sigma_i, \tau_i]\Delta$ $(i = 1, 2)$. Putting

$$T = \begin{bmatrix} \sigma_1 & \tau_1 \\ \sigma_2 & \tau_2 \end{bmatrix} \tag{52}$$

we get

$$M\Gamma = T\Delta.$$

On the other hand, (42) and (43) imply

$$[u, v]M\Gamma = [s, t]\Delta. \tag{53}$$

Since $|\Delta| \neq 0$ by (44), we get (45) from (52) and (53). Finally, by (52), (40) and (44)

$$h(T) = h(M\Gamma\Delta^{-1}) \leqslant 4h(M)h(\Gamma)h(\Delta) \leqslant 4d\big((2d^2)!\big)^2 h(\Gamma).$$

This completes the proof. □

Lemma 6. *Let $f(x)$ be an irreducible polynomial not dividing $x^\delta - x$ $(\delta > 1)$, α, β integers, $\alpha > 0$ or $\beta > 0$. For arbitrary positive integers n, m such that $\alpha n + \beta m > 0$ there exists an integral matrix*

$$M = \begin{bmatrix} \nu_1 & \mu_1 \\ \nu_2 & \mu_2 \end{bmatrix}$$

satisfying the conditions

$$0 \leqslant \nu_i \leqslant C(f, \alpha, \beta), \quad 0 \leqslant \mu_i \leqslant C(f, \alpha, \beta) \quad (i = 1, 2), \tag{54}$$

$$|M| > 0, \tag{55}$$

$$[n, m] = [u, v]M, \quad u, v \text{ integers} \geqslant 0, \tag{56}$$

$$\alpha\nu_i + \beta\mu_i \geqslant 0 \quad (i = 1, 2), \tag{57}$$

and having the following property: if

$$f\big(y^{\alpha\nu_1+\beta\mu_1}z^{\alpha\nu_2+\beta\mu_2}\big) = f_1(y, z)\cdots f_r(y, z)$$

is a standard form of $f\left(y^{\alpha\nu_1+\beta\mu_1}z^{\alpha\nu_2+\beta\mu_2}\right)$, *then*

$$f(x^{\alpha n+\beta m}) = f_1(x^u, x^v)\cdots f_r(x^u, x^v)$$

is a standard form of $f(x^{\alpha n+\beta m})$.

$C(f, \alpha, \beta)$ *is an effectively computable constant, independent of* n *and* m.

Proof. By Theorem 1, there exists a positive integer $\nu \leqslant C(f)$ such that $\alpha n + \beta m = \nu w$, w integer, and having the following property: if

$$f(x^\nu) = f_1'(x)\cdots f_{r'}'(x) \tag{58}$$

is a standard form of $f(x^\nu)$, then

$$f(x^{\alpha n+\beta m}) = f_1'(x^w)\cdots f_{r'}'(x^w) \tag{59}$$

is a standard form of $f(x^{\alpha n+\beta m})$.

Now we distinguish two cases, $\alpha\beta \geqslant 0$ and $\alpha\beta < 0$.

If $\alpha\beta \geqslant 0$ we put in Lemma 5:

$$\Gamma = \begin{bmatrix}\alpha & \alpha\\ \beta & \beta\end{bmatrix}, \quad d = C(f).$$

Let

$$M = \begin{bmatrix}\nu_1 & \mu_1\\ \nu_2 & \mu_2\end{bmatrix}$$

be an integral matrix whose existence for n, m is asserted in that lemma. It follows from (40) that

$$0 \leqslant \nu_i \leqslant \left(\left(2C^2(f)\right)!\right)^2, \quad 0 \leqslant \mu_i \leqslant \left(\left(2C^2(f)\right)!\right)^2 \quad (i = 1, 2); \tag{60}$$

thus (54) is satisfied with $C(f, \alpha, \beta) = \left(\left(2C^2(f)\right)!\right)^2$ and, in view of $\alpha \geqslant 0$, $\beta \geqslant 0$, (57) holds. Formulae (55) and (56) follow from (41) and (42). We apply the last statement of Lemma 5 with

$$[s, t] = [w, w], \quad \Delta = \begin{bmatrix}\nu & 0\\ 0 & \nu\end{bmatrix}.$$

In virtue of that statement there exists an integral matrix T such that

$$\begin{bmatrix}\nu_1 & \mu_1\\ \nu_2 & \mu_2\end{bmatrix}\begin{bmatrix}\alpha & \alpha\\ \beta & \beta\end{bmatrix} = T\begin{bmatrix}\nu & 0\\ 0 & \nu\end{bmatrix},$$

whence

$$\nu \mid \alpha\nu_i + \beta\mu_i \quad (i = 1, 2). \tag{61}$$

If $\alpha\beta < 0$, we may assume without loss of generality $\alpha > 0$, $\beta < 0$. We put in Lemma 5:

$$\Gamma' = \begin{bmatrix}\nu & \nu\\ -\beta & -\beta\end{bmatrix}, \quad d' = \alpha, \quad n' = \frac{\alpha n + \beta m}{\nu}, \quad m' = m$$

(the "prime" is added to avoid a confusion in notation). In virtue of that lemma there exists an integral matrix

$$M' = \begin{bmatrix} \nu_1' & \mu_1' \\ \nu_2' & \mu_2' \end{bmatrix}$$

such that

$$0 \leqslant \nu_i' \leqslant \big((2\alpha^2)!\big)^2, \quad 0 \leqslant \mu_i' \leqslant \big((2\alpha^2)!\big)^2 \quad (i = 1, 2), \tag{62}$$

$$|M'| > 0, \tag{63}$$

$$[(\alpha n + \beta m)/\nu, m] = [u, v]M', \quad u, v \text{ integers} \geqslant 0. \tag{64}$$

We apply the last statement of Lemma 5 with

$$[s, t] = [w, w], \quad \Delta = \begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix}.$$

In virtue of that statement there exists an integral matrix T such that

$$\begin{bmatrix} \nu_1' & \mu_1' \\ \nu_2' & \mu_2' \end{bmatrix} \begin{bmatrix} \nu & \nu \\ -\beta & -\beta \end{bmatrix} = T \begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix},$$

whence $\alpha \mid \nu\nu_i' - \beta\mu_i'$ $(i = 1, 2)$. We put

$$\nu_i = (\nu\nu_i' - \beta\mu_i')/\alpha, \quad \mu_i = \mu_i' \quad (i = 1, 2).$$

(62) implies (57) and the inequality

$$0 \leqslant \nu_i \leqslant \big((2\alpha^2)!\big)^2\big(C(f) + |\beta|\big), \quad 0 \leqslant \mu_i \leqslant \big((2\alpha^2)!\big)^2 \quad (i = 1, 2);$$

thus (54) is satisfied with $C(f, \alpha, \beta) = \big((2\alpha^2)!\big)^2\big(C(f) + |\beta|\big)$. Formulae (55) and (56) follow from (63) and (64); besides we have (61).

In order to prove the last property of the matrix M postulated in the lemma, we put

$$f_j'(y, z) = f_j'\big(y^{(\alpha\nu_1+\beta\mu_1)/\nu} z^{(\alpha\nu_2+\beta\mu_2)/\nu}\big) \quad (1 \leqslant j \leqslant r'). \tag{65}$$

By (56) $f_j'(x^u, x^v) = f_j'(x^w)$, whence by (59), $f_j'(x^u, x^v)$ is irreducible. We show that $f_j'(y, z)$ is not reducible.

Denote by δ the degree of $f_j'(x)$ and suppose that

$$f_j'(y, z) = g(y, z)h(y, z), \tag{66}$$

where g is of degree γ_1 in y, γ_2 in z; h is of degree χ_1 in y, χ_2 in z and $\gamma_1 + \gamma_2 > 0$, $\chi_1 + \chi_2 > 0$. By (65) we have

$$\delta(\alpha\nu_i + \beta\mu_i)/\nu = \gamma_i + \chi_i \quad (i = 1, 2).$$

On the other hand,

$$f_j'(x^w) = g(x^u, x^v)h(x^u, x^v).$$

The degree of $f_j'(x^w)$ equals

$$\delta(\alpha n + \beta m)/\nu = \delta u(\alpha\nu_1 + \beta\mu_1)/\nu + \delta v(\alpha\nu_2 + \beta\mu_2)/\nu = u(\gamma_1 + \chi_1) + v(\gamma_2 + \chi_2).$$

The degree of $g(x^u, x^v)h(x^u, x^v)$ can be equal to $u\gamma_1 + u\chi_1 + v\gamma_2 + v\chi_2$ only if the degree of $g(x^u, x^v)$ equals $u\gamma_1 + v\gamma_2$ and the degree of $h(x^u, x^v)$ equals $u\chi_1 + v\chi_2$. Since $f'_j(x^w)$ is irreducible we get $u\gamma_1 + v\gamma_2 = 0$ or $u\chi_1 + v\chi_2 = 0$, whence $u = 0$ and $\gamma_2\chi_2 = 0$ or $v = 0$ and $\gamma_1\chi_1 = 0$ or $u = v = 0$. The last case is impossible by (56), and in view of symmetry it is enough to consider $u = 0$, $\gamma_2 = 0$. Thus $g(y, 0) = g(y, z)$ is not constant and, since $f'_j(0) \neq 0$, it follows from (65) and (66) that $\alpha\nu_2 + \beta\mu_2 = 0$. This gives $\alpha n + \beta m = u(\alpha\nu_1 + \beta\mu_1) + v(\alpha\nu_2 + \beta\mu_2) = 0$. The contradiction obtained proves that no $f'_j(y, z)$ $(1 \leqslant j \leqslant r')$ is reducible. Since $f'_j(y, z)$ are also not constant, and by (58)

$$f\left(y^{\alpha\nu_1+\beta\mu_1} z^{\alpha\nu_2+\beta\mu_2}\right) = f'_1(y, z) \cdots f'_{r'}(y, z),$$

it follows that the polynomials $f'_j(y, z)$ $(1 \leqslant j \leqslant r')$ and $f_j(y, z)$ $(1 \leqslant j \leqslant r)$, after a suitable permutation, differ only by constant factors. Since the polynomials $f'_j(x^u, x^v) = f'_j(x^w)$ $(1 \leqslant j \leqslant r')$ are irreducible and coprime, the same applies to $f_j(x^u, x^v)$ $(1 \leqslant j \leqslant r)$, which completes the proof. □

4.

Proof of Theorem 2. It is clear that if $\Phi(x)$ is a polynomial, then $K\Phi(x) = KJ\Phi(x)$. We take this equality as a definition of $K\Phi(x)$, where $\Phi(x)$ is a rational function of the form $\sum_{i=0}^{I} a_i x^{\alpha_i}$ (α_i integers).

Now let

$$F(y, z) = \sum_{i=0}^{I} a_i y^{\alpha_i} z^{\beta_i},$$

where a_i are integers $\neq 0$ and the pairs $\langle \alpha_i, \beta_i \rangle$ $(0 \leqslant i \leqslant I)$ are all different (it is clearly sufficient to prove the theorem for polynomials with integral coefficients). Let ϱ be the rank of the matrix

$$\begin{bmatrix} \alpha_1 - \alpha_0 & \alpha_2 - \alpha_0 & \dots & \alpha_I - \alpha_0 \\ \beta_1 - \beta_0 & \beta_2 - \beta_0 & \dots & \beta_I - \beta_0 \end{bmatrix}.$$

We consider separately two cases, $\varrho = 1$ and $\varrho = 2$.

Case $\varrho = 1$. In this case there exist integers α, β and γ_i $(0 \leqslant i \leqslant I)$ such that $\alpha > 0$ or $\beta > 0$ and

$$\alpha_i - \alpha_0 = \alpha\gamma_i, \quad \beta_i - \beta_0 = \beta\gamma_i \quad (0 \leqslant i \leqslant I).$$

Put

$$f(x) = J \sum_{i=0}^{I} a_i x^{\gamma_i}.$$

Clearly

$$JF(y, z) = Jf(y^\alpha z^\beta). \tag{67}$$

Since $F(y, z)$ is irreducible and is different from ay, az, both $f(x)$ and $Jf(x^{-1}) = J\sum_{i=0}^{I} a_i x^{-\gamma_i}$ are irreducible. If we had for some $\delta > 1$, $f(x) \mid x^{\delta} - x$, this would imply $f(x) = \pm Jf(x^{-1})$, whence $JF(y, z) = \pm JF(y^{-1}, z^{-1})$, against the assumption. Thus both $f(x)$ and $Jf(x^{-1})$ satisfy the conditions of Lemma 6 and constants $C(f, \alpha, \beta)$, $C\big(Jf(x^{-1}), \alpha, \beta\big)$ are well defined. We put

$$C_0(F) = \max\{|\alpha|, |\beta|\}; \quad C_1(F) = \max\big\{C(f, \alpha, \beta), C\big(Jf(x^{-1}), \alpha, \beta\big)\big\}.$$

If $\alpha n + \beta m = 0$, we have $\max\{n, m\} \leqslant C_0(F)(n, m)$.

If $\alpha n + \beta m < 0$, we can replace in (67) f by $Jf(x^{-1})$, α by $-\alpha$, β by $-\beta$, which will not affect the inequality

$$C(f, \alpha, \beta) \leqslant C_1(F). \tag{68}$$

We may therefore assume without loss of generality that $\alpha n + \beta m > 0$ and (68) holds. Let

$$M = \begin{bmatrix} \nu_1 & \mu_1 \\ \nu_2 & \mu_2 \end{bmatrix}$$

be an integral matrix, whose existence for n, m is asserted in Lemma 6. Since by (57) and (67)

$$JF(y^{\nu_1} z^{\nu_2}, y^{\mu_1} z^{\mu_2}) = f(y^{\alpha\nu_1 + \beta\mu_1} z^{\alpha\nu_2 + \beta\mu_2}),$$
$$KF(x^n, x^m) = f(x^{\alpha n + \beta m}),$$

Theorem 2 follows in this case ($\varrho = 1$) from Lemma 6 and (68).

Case $\varrho = 2$. We may assume without loss of generality that

$$\begin{vmatrix} \alpha_1 - \alpha_0 & \alpha_2 - \alpha_0 \\ \beta_1 - \beta_0 & \beta_2 - \beta_0 \end{vmatrix} \neq 0.$$

Let ξ be any irrational number. Clearly the numbers $(\alpha_1 - \alpha_0) + \xi(\beta_1 - \beta_0)$ and $(\alpha_2 - \alpha_0) + \xi(\beta_2 - \beta_0)$ are incommensurable; thus there are incommensurable distances in the set of points $\alpha_i + \xi\beta_i$ $(0 \leqslant i \leqslant I)$. By remark 1 at the end of paper [2] (cf. also the remark after Lemma 4) there are in this set two incommensurable distances which appear only once in the double sequence $\alpha_j - \alpha_i + \xi(\beta_j - \beta_i)$ $(0 \leqslant i < j \leqslant I)$. This means that there exist 4 non-negative integers i', i'', j', j'' such that $\langle \alpha_{j'} - \alpha_{i'}, \beta_{j'} - \beta_{i'} \rangle$ and $\langle \alpha_{j''} - \alpha_{i''}, \beta_{j''} - \beta_{i''} \rangle$ appear only once in the double sequence $\langle \alpha_j - \alpha_i, \beta_j - \beta_i \rangle$ $(0 \leqslant i < j \leqslant I)$ and

$$\begin{vmatrix} \alpha_{j'} - \alpha_{i'} & \alpha_{j''} - \alpha_{i''} \\ \beta_{j'} - \beta_{i'} & \beta_{j''} - \beta_{i''} \end{vmatrix} \neq 0.$$

We put in Lemma 5

$$\Gamma = \begin{bmatrix} \alpha_{j'} - \alpha_{i'} & \alpha_{j''} - \alpha_{i''} \\ \beta_{j'} - \beta_{i'} & \beta_{j''} - \beta_{i''} \end{bmatrix}, \quad d = 2(10N^2)^A, \tag{69}$$

where $N = \max\limits_{0 \leqslant i \leqslant I} \max\{\alpha_i, \beta_i\}$, $A = \sum\limits_{i=0}^{I} a_i^2$.

Let

$$M = \begin{bmatrix} \nu_1 & \mu_1 \\ \nu_2 & \mu_2 \end{bmatrix}$$

be an integral non-singular matrix, whose existence for n, m is asserted in that lemma. Thus we have by (40) and (42)

$$0 \leqslant \nu_i \leqslant \left((8 \cdot 10^{2A} N^{4A})!\right)^2, \quad 0 \leqslant \nu_i \leqslant \left((8 \cdot 10^{2A} N^{4A})!\right)^2 \quad (i = 1, 2), \tag{70}$$

$$[n, m] = [u, v]M, \quad u, v \text{ integers} \geqslant 0. \tag{71}$$

We see that assertions (i) and (ii) of Theorem 2 are satisfied with $C_1(F) = \left((8 \cdot 10^{2A} N^{4A})!\right)^2$.

Moreover, by (70) and (71)

$$\max\{n, m\} \leqslant 2C_1(F) \max\{u, v\}, \quad (n, m) \geqslant (u, v). \tag{72}$$

Let

$$JF(y^{\nu_1} z^{\nu_2}, y^{\mu_1} z^{\mu_2}) = \text{const } F_1(y, z)^{e_1} F_2(y, z)^{e_2} \cdots F_r(y, z)^{e_r} \tag{73}$$

be a standard form of $JF(y^{\nu_1} z^{\nu_2}, y^{\mu_1} z^{\mu_2})$. In order to prove (iii) we have to show that either

$$KF(x^n, x^m) = \text{const } KF_1(x^u, x^v)^{e_1} KF_2(x^u, x^v)^{e_2} \cdots KF_r(x^u, x^v)^{e_r}$$

is a standard form of $KF(x^n, x^m)$ or $\max\{n, m\} \leqslant C_0(F)(n, m)$, where $C_0(F)$ is a constant independent of n, m. In view of (70) it is sufficient to prove the same with $C_0(F)$ replaced by $C_0(F, M)$, a constant depending only on F and M.

In order to define $C_0(F, M)$ we notice that by the assumption $\left(JF(y, z), JF(y^{-1}, z^{-1})\right) = 1$ and by Lemma 3 there exist two constants, $B_{00} = B_0\left(JF(y, z), JF(y^{-1}, z^{-1})\right) \geqslant 1$ and $B_{01} = B_1\left(JF(y, z), JF(y^{-1}, z^{-1})\right)$, such that

$$\left(\frac{JF(x^n, x^m)}{KF(x^n, x^m)}, \frac{JF(x^{-n}, x^{-m})}{KF(x^{-n}, x^{-m})}\right) \Bigg| (x^{(n,m)B_{00}} - 1)^{B_{00}} \tag{74}$$

and

$$\left(KF(x^n, x^m), KF(x^{-n}, x^{-m})\right) = 1 \tag{75}$$

unless

$$\max\{n, m\} \leqslant B_{01}(n, m).$$

Since for an arbitrary polynomial $f(x)$

$$Jf(x)/Kf(x) = Jf(x^{-1})/Kf(x^{-1}), \tag{76}$$

we get from (74)

$$\frac{JF(x^n, x^m)}{KF(x^n, x^m)} \Bigg| (x^{(n,m)B_{00}} - 1)^{B_{00}}. \tag{77}$$

Let S_j $(1 \leqslant j \leqslant r)$ be the set of all the polynomials not divisible by $F_j(y, z)$ which are of the form $J \sum_{i=0}^{l} c_i y^{\sigma_i} z^{\tau_i}$, where c_i are integers $\neq 0$, $\sum_{i=0}^{l} c_i^2 = A$ and

$$\max\{|\sigma_i|, |\tau_i|\} \leqslant 16 \cdot 10^{2A} N^{4A+1} C_1(F) \quad (0 \leqslant i \leqslant l).$$

Clearly the sets S_j $(1 \leqslant j \leqslant r)$ are finite and effectively computable. Moreover, for each $H \in S_j$ there exists by Lemma 3 a constant $B_1(F_j, H)$ such that

$$\big(KF_j(x^u, x^v), KH(x^u, x^v)\big) = 1 \tag{78}$$

unless

$$\max\{u, v\} \leqslant B_1(F_j, H)(u, v).$$

Finally for each pair $\langle i, j\rangle$, where $1 \leqslant i < j \leqslant r$, there exists by Lemma 3 a constant $B_1(F_i, F_j)$ such that

$$\big(KF_i(x^u, x^v), KF_j(x^u, x^v)\big) = 1 \tag{79}$$

unless

$$\max\{u, v\} \leqslant B_1(F_i, F_j)(u, v).$$

We put

$$C_0(F, M) = \max\Big\{8NC_1^2(F)B_{00}^2, B_{01}, \\ 2C_1(F) \max_{1\leqslant j\leqslant r} \max_{H\in S_j} B_1(F_j, H), 2C_1(F) \max_{1\leqslant i<j\leqslant r} B_1(F_i, F_j)\Big\}.$$

If for any pair $\langle i, j\rangle$, where $1 \leqslant i < j \leqslant r$, $\big(KF_i(x^u, x^v), KF_j(x^u, x^v)\big) \neq 1$ we have by (72) and (79)

$$\max\{n, m\}/(n, m) \leqslant 2C_1(F)B_1(F_i, F_j) \leqslant C_0(F, M).$$

It remains to prove that if any polynomial $KF_j(x^u, x^v)$ $(1 \leqslant j \leqslant r)$ is not irreducible, then $\max\{n, m\} \leqslant C_0(F, M)(n, m)$.

We shall do that in two steps assuming first that $KF_1(x^u, x^v)$ is constant and secondly that it is reducible (the treatment of $F_1(x^u, x^v)$ instead of $F_j(x^u, x^v)$ does not affect generality and simplifies a little the notation).

c 1. Assume that $KF_1(x^u, x^v)$ is constant. Let

$$F_1(y, z) = \sum_{j=0}^{k} b_j y^{\gamma_j} z^{\delta_j} \quad (b_j \neq 0,\ \langle \gamma_j, \delta_j\rangle \text{ all different}) \tag{80}$$

and let ϱ_1 be the rank of the matrix

$$\begin{bmatrix} \gamma_1 - \gamma_0 & \dots & \gamma_k - \gamma_0 \\ \delta_1 - \delta_0 & \dots & \delta_k - \delta_0 \end{bmatrix}.$$

It follows from (70) and (73) that

$$\begin{array}{c} 0 \leqslant \gamma_j \leqslant N(\mu_1 + \nu_1) \leqslant 2NC_1(F), \\ 0 \leqslant \delta_j \leqslant N(\mu_2 + \nu_2) \leqslant 2NC_1(F) \end{array} \qquad (0 \leqslant j \leqslant k) \tag{81}$$

and $\varrho_1 = 1$ or 2. If $\varrho_1 = 1$, we have

$$F_1(y, z) = Jf(y^\gamma z^\delta), \tag{82}$$

where f is a polynomial in one variable, γ, δ are integers (cf. p. 319) and by (81)

$$0 < \max\{|\gamma|, |\delta|\} \leqslant 2NC_1(F). \tag{83}$$

$KF_1(x^u, x^v) = \text{const}$ implies $Kf(x^{\gamma u + \delta v}) = \text{const}$; thus $\gamma u + \delta v = 0$ or $Kf(x) = \text{const}$. In the first case, by (83)

$$\max\{u, v\} \leqslant 2NC_1(F)(u, v); \tag{84}$$

in the second case by (76) $Jf(x) = \pm Jf(x^{-1})$ and by (82)

$$Jf(y^\gamma z^\delta) = F_1(y, z) = \pm JF_1(y^{-1}, z^{-1}).$$

The last equality implies by (73)

$$Jf(y^\gamma z^\delta) \,\big|\, \big(JF(y^{\nu_1} z^{\nu_2}, y^{\mu_1} z^{\mu_2}), JF(y^{-\nu_1} z^{-\nu_2}, y^{-\mu_1} z^{-\mu_2})\big).$$

By a substitution $y = \eta^{\mu_2} \zeta^{-\nu_2}$, $z = \eta^{-\mu_1} \zeta^{\nu_1}$ we get

$$Jf(\eta^{\gamma\mu_2 - \delta\mu_1} \zeta^{-\gamma\nu_2 + \delta\nu_1}) \,\big|\, \big(JF(\eta^{|M|}, \zeta^{|M|}), JF(\eta^{-|M|}, \zeta^{-|M|})\big). \tag{85}$$

However $\big(JF(y, z), JF(y^{-1}, z^{-1})\big) = 1$, and thus

$$\big(JF(\eta^{|M|}, \zeta^{|M|}), JF(\eta^{-|M|}, \zeta^{-|M|})\big) = 1$$

and (85) implies

$$Jf(\eta^{\gamma\mu_2 - \delta\mu_1} \zeta^{-\gamma\nu_2 + \delta\nu_1}) = \text{const}.$$

Since by (82) $Jf(x) \neq \text{const}$, we get

$$\begin{aligned} \gamma\mu_2 - \delta\mu_1 &= 0, \\ -\gamma\nu_2 + \delta\nu_1 &= 0. \end{aligned}$$

Since

$$\begin{vmatrix} \mu_2 & -\mu_1 \\ -\nu_2 & \nu_1 \end{vmatrix} = |M| \neq 0,$$

the last system of equations gives $\gamma = \delta = 0$, against (83). The contradiction obtained proves (84).

If $\varrho_1 = 2$ we may assume without loss of generality that

$$\begin{vmatrix} \gamma_1 - \gamma_0 & \gamma_2 - \gamma_0 \\ \delta_1 - \delta_0 & \delta_2 - \delta_0 \end{vmatrix} \neq 0.$$

On the other hand, by (73)

$$\frac{JF_1(x^u, x^v)}{KF_1(x^u, x^v)} \;\Big|\; \frac{JF(x^n, x^m)}{KF(x^n, x^m)}$$

and since $KF_1(x^u, x^v) = \text{const}$, we get from (77)

$$JF_1(x^u, x^v) \;\Big|\; (x^{(n,m)B_{00}} - 1)^{B_{00}}.$$

It follows by (80) that either

$$u\gamma_i + v\delta_i = u\gamma_j + v\delta_j \quad \text{for} \quad i = 1 \text{ or } 2 \text{ and some } j \leqslant k \tag{86}$$

or

$$|u(\gamma_i - \gamma_0) + v(\delta_i - \delta_0)| \leqslant B_{00}^2(n, m) \quad (i = 1, 2). \tag{87}$$

(81) and (86) imply

$$\max\{u, v\} \leqslant 2NC_1(F)(u, v), \tag{88}$$

(81) and (87) imply

$$\max\{u, v\} \leqslant 4NC_1(F)B_{00}^2(n, m). \tag{89}$$

In view of (72) it follows from (84), (88) and (89) that

$$\max\{n, m\} \leqslant C_0(F, M)(n, m).$$

2. Assume that $KF_1(x^u, x^v)$ is reducible. Let $f(x)$ be an irreducible primitive factor of it. Since by (71) and (73) $KF_1(x^u, x^v) \mid F(x^n, x^m)$, we have

$$F(x^n, x^m) = f(x)g(x), \tag{90}$$

where $g(x)$ is a polynomial with integral coefficients. It follows from (75) that

$$\big(KF_1(x^u, x^v), KF(x^{-n}, x^{-m})\big) = 1 \quad \text{unless} \quad \max\{n, m\} \leqslant B_{01}(n, m),$$

whence by (90)

$$f(x) = \text{const}\,\big(KF_1(x^u, x^v), K[f(x)g(x^{-1})]\big) \tag{91}$$

or

$$\max\{n, m\} \leqslant B_{01}(n, m). \tag{92}$$

In order to calculate the right hand side of (91) we put

$$f(x)g(x^{-1}) = \sum_{i=0}^{l} c_i x^{k_i} \quad (c_i \text{ integers} \neq 0,\ k_0 < k_1 < \ldots < k_l) \tag{93}$$

and consider two expressions for $F(x^n, x^m)F(x^{-n}, x^{-m})$:

$$F(x^n, x^m)F(x^{-n}, x^{-m}) = \sum_{i=0}^{I} a_i^2 + \sum_{\substack{0 \leqslant i,j \leqslant I \\ i \neq j}} a_i a_j x^{n\alpha_j + m\beta_j - (n\alpha_i + m\beta_i)},$$

$$\big[f(x)g(x^{-1})\big]\big[f(x^{-1})g(x)\big] = \sum_{i=0}^{l} c_i^2 + \sum_{\substack{0 \leqslant i,j \leqslant l \\ i \neq j}} c_i c_j x^{k_j - k_i}. \tag{94}$$

If for any pair $\langle i, j\rangle$:

$$i \neq j \quad \text{and} \quad n\alpha_j + m\beta_j - (n\alpha_i + m\beta_i) = 0, \tag{95}$$

we get $n(\alpha_j - \alpha_i) + m(\beta_j - \beta_i) = 0$, whence

$$\max\{n, m\} \leqslant N(n, m). \tag{96}$$

Similarly, if for any pair $\langle i, j\rangle$

$$\langle i, j\rangle \neq \langle i', j'\rangle \quad \text{and} \quad n\alpha_j + m\beta_j - (n\alpha_i + m\beta_i) = n\alpha_{j'} + m\beta_{j'} - (n\alpha_{i'} + m\beta_{i'}) \tag{97}$$

or

$$\langle i, j\rangle \neq \langle i'', j''\rangle \quad \text{and} \quad n\alpha_j + m\beta_j - (n\alpha_i + m\beta_i) = n\alpha_{j''} + m\beta_{j''} - (n\alpha_{i''} + m\beta_{i''}), \tag{98}$$

we get by the choice of $\langle i', j'\rangle, \langle i'', j''\rangle$ (p. 320) a linear homogeneous equation on m and n with non-zero coefficients absolutely $\leqslant 2N$, whence

$$\max\{n, m\} \leqslant 2N(n, m). \tag{99}$$

If no pair $\langle i, j\rangle$ satisfies (95), (97) or (98), it follows from (94) that

$$\sum_{i=0}^{l} c_i^2 = \sum_{i=0}^{I} a_i^2 = A, \tag{100}$$

(101) the numbers $n\alpha_{j'} + m\beta_{j'} - (n\alpha_{i'} + m\beta_{i'})$ and $n\alpha_{j''} + m\beta_{j''} - (n\alpha_{i''} + m\beta_{i''})$ appear among the differences $k_j - k_i$ $(0 \leqslant i \leqslant l, 0 \leqslant j \leqslant l)$,

(102) each number $k_j - k_i$ which appears only once in the double sequence $k_j - k_i$ $(0 \leqslant i < j \leqslant l)$ has a value $n\gamma + m\delta$, where $|\gamma| \leqslant N$, $|\delta| \leqslant N$.

Let $k_{j_1} - k_{i_1}, k_{j_2} - k_{i_2}, \ldots, k_{j_P} - k_{i_P}$ $(P \geqslant 0)$ be all the numbers mentioned in (102) besides $k_l - k_0$.

If $P \geqslant 2$, $1 \leqslant p < q \leqslant P$, it follows from

$$\begin{aligned} k_l - k_0 &= \gamma_0 n + \delta_0 m, \\ k_{j_p} - k_{i_p} &= \gamma_p n + \delta_p m, \\ k_{j_q} - k_{i_q} &= \gamma_q n + \delta_q m, \\ \varrho_{p,q} &= \text{rank of } \begin{bmatrix} \gamma_0 & \delta_0 \\ \gamma_p & \delta_p \\ \gamma_q & \delta_q \end{bmatrix}, \end{aligned}$$

that

$$c_{p,q}(k_l - k_0) + c'_{p,q}(k_{j_p} - k_{i_p}) + c''_{p,q}(k_{j_q} - k_{i_q}) = 0,$$

where

$$[c_{p,q}, c'_{p,q}, c''_{p,q}] = \begin{cases} \left[\begin{vmatrix} \gamma_p & \delta_p \\ \gamma_q & \delta_q \end{vmatrix}, \begin{vmatrix} \gamma_q & \delta_q \\ \gamma_0 & \delta_0 \end{vmatrix}, \begin{vmatrix} \gamma_0 & \delta_0 \\ \gamma_p & \delta_p \end{vmatrix} \right] & \text{if } \varrho_{p,q} = 2, \\ [\gamma_p, -\gamma_0, 0] & \text{if } \varrho_{p,q} = 1 \text{ and } \gamma_0 \neq 0, \\ [\delta_p, -\delta_0, 0] & \text{if } \varrho_{p,q} = 1 \text{ and } \delta_0 \neq 0. \end{cases}$$

Clearly

$$0 < \max\{|c_{p,q}|, |c'_{p,q}|, |c''_{p,q}|\} \leqslant 2N^2 \quad (1 \leqslant p < q \leqslant P).$$

Therefore, the assumptions of Lemma 4 are satisfied with $c \leqslant 2N^2$ and we get from that lemma

$$k_i - k_0 = s\kappa_i + t\lambda_i \quad (0 \leqslant i \leqslant l), \tag{103}$$

where $s, t, \kappa_i, \lambda_i$ $(0 \leqslant i \leqslant l)$ are integers, $|\kappa_i| \leqslant (10N^2)^l$, $|\lambda_i| \leqslant (10N^2)^l$.

Since by (93) and (100) $l < A$, we have

$$|\kappa_i| < (10N^2)^A, \quad |\lambda_i| < (10N^2)^A \quad (0 \leqslant i \leqslant l). \tag{104}$$

Now by (101), (103) and (104)

$$\begin{aligned} n\alpha_{j'} + m\beta_{j'} - (n\alpha_{i'} + m\beta_{i'}) &= \kappa' s + \lambda' t, \\ n\alpha_{j''} + m\beta_{j''} - (n\alpha_{i''} + m\beta_{i''}) &= \kappa'' s + \lambda'' t, \end{aligned} \tag{105}$$

where $\kappa', \lambda', \kappa'', \lambda''$ are integers and

$$0 < \max\{|\kappa'|, |\lambda'|\} < 2(10N^2)^A, \quad 0 < \max\{|\kappa''|, |\lambda''|\} < 2(10N^2)^A. \tag{106}$$

($\kappa' = \lambda' = 0$ or $\kappa'' = \lambda'' = 0$ would imply (96).)

We put

$$\Delta = \begin{bmatrix} \kappa' & \kappa'' \\ \lambda' & \lambda'' \end{bmatrix}.$$

It follows from (69), (105) and (106) that

$$[n, m]\Gamma = [s, t]\Delta \quad \text{and} \quad h(\Delta) < 2(10N^2)^A = d. \tag{107}$$

We distinguish two cases, $|\Delta| = 0$ and $|\Delta| \neq 0$.

If $|\Delta| = 0$, let

$$|\Gamma|\Delta\Gamma^{-1} = \begin{bmatrix} \xi_1 & \eta_1 \\ \xi_2 & \eta_2 \end{bmatrix}$$

(by the choice of Γ, Γ^{-1} exists). It follows from (106) that

$$0 < \max\{|\xi_1|, |\eta_1|\} \leqslant 2h(\Delta)h(\Gamma) < 4 \cdot 10^A N^{2A+1}. \tag{108}$$

On the other hand, since $\xi_1\eta_2 - \eta_1\xi_2 = 0$, we get from (107) $\xi_1 m - \eta_1 n = 0$, and thus by (108)

$$\max\{n, m\}/(n, m) < 4 \cdot 10^A N^{2A+1} < C_1(F). \tag{109}$$

If $|\Delta| \neq 0$, we can apply to (107) the last statement of Lemma 5. In virtue of that statement there exists an integral matrix T such that

$$[s, t] = [u, v]T \tag{110}$$

and

$$h(T) \leqslant 8 \cdot 10^A N^{2A+1}\big((8 \cdot 10^{2A} N^{4A})!\big)^2 = 8 \cdot 10^A N^{2A+1} C_1(F). \tag{111}$$

Put

$$T \begin{bmatrix} \kappa_i \\ \lambda_i \end{bmatrix} = \begin{bmatrix} \sigma_i \\ \tau_i \end{bmatrix} \quad (0 \leqslant i \leqslant l), \tag{112}$$

$$H(y, z) = J \sum_{i=0}^{l} c_i y^{\sigma_i} z^{\tau_i}. \tag{113}$$

We have by (103) and (110)

$$k_i - k_0 = u\sigma_i + v\tau_i \quad (0 \leqslant i \leqslant l);$$

thus by (93), (113) and (91)

$$K\big(f(x)g(x^{-1})\big) = K \sum_{i=0}^{l} c_i x^{k_i - k_0} = KH(x^u, x^v),$$

$$f(x) = \text{const}\,\big(KF_1(x^u, x^v), KH(x^u, x^v)\big). \tag{114}$$

If we had $F_1 \mid H$, it would imply $KF_1(x^u, x^v) \mid KH(x^u, x^v)$, whence $KF_1(x^u, x^v) \mid f(x)$, against the choice of $f(x)$. Thus $(F_1, H) = 1$. On the other hand, by (104), (111) and (112)

$$\max\{|\sigma_i|, |\tau_i|\} \leqslant 16 \cdot 10^{2A} N^{4A+1} C_1(F) \quad (0 \leqslant i \leqslant l);$$

thus by (100), (113) and the choice of S_1 (p. 322), $H \in S_1$. It follows by (78) that

$$\big(KF_1(x^u, x^v), KH(x^u, x^v)\big) = 1$$

or

$$\max\{u, v\}/(u, v) \leqslant B_1(F_1, H) \leqslant \max_{H \in S_1} B_1(F_1, H). \tag{115}$$

A comparison with (114) shows that (115) holds. In view of (72) it follows from (92), (96), (99), (109) and (115) that

$$\max\{n, m\} \leqslant C_0(F, M)(n, m).$$

The proof is complete. □

5.

Proof of Theorem 3. Put in Theorem 2 $F(y, z) = ay + bz + c$. Since $c \neq 0$ we have $JF(y, z) \neq \pm JF(y^{-1}, z^{-1})$; thus the assumptions of the theorem are satisfied and the constant $C_0(ay + bz + c)$ exists. Put

$$\begin{aligned} A(a, b, c) &= C_0(ay + bz + c), \\ B(a, b, c) &= A(a, b, c) \max_{(\alpha,\beta)\in S, \alpha>\beta} C'(ax^\alpha + bx^\beta + c), \end{aligned} \tag{116}$$

where C' is a constant from the Corollary to Theorem 1 and S consists of all pairs of relatively prime positive integers $\leqslant A(a, b, c)$.

Now, assume that n, m are positive integers, $n > m$ and $K(ax^n + bx^m + c)$ is reducible. Let

$$M = \begin{bmatrix} \nu_1 & \mu_1 \\ \nu_2 & \mu_2 \end{bmatrix}$$

be an integral non-singular matrix whose existence for F, n, m is asserted in Theorem 2.

Without loss of generality we may assume that $|M| > 0$. It follows from part (iii) of Theorem 2 that if $K(ax^n + bx^m + c)$ is reducible then either $J(ay^{\nu_1}z^{\nu_2} + by^{\mu_1}z^{\mu_2} + c)$ is reducible or

$$n/(n, m) \leqslant C_0(F) = A(a, b, c). \tag{117}$$

We prove that the former eventuality is impossible. Suppose that

$$J(ay^{\nu_1}z^{\nu_2} + by^{\mu_1}z^{\mu_2} + c) = G_1(y, z)G_2(y, z), \tag{118}$$

where G_1, G_2 are polynomials. By a substitution $y = \eta^{\mu_2}\zeta^{-\nu_2}$, $z = \eta^{-\mu_1}\zeta^{\nu_1}$ we get

$$J(a\eta^{|M|} + b\zeta^{|M|} + c) = JG_1(\eta^{\mu_2}\zeta^{-\nu_2}, \eta^{-\mu_1}\zeta^{\nu_1})JG_2(\eta^{\mu_2}\zeta^{-\nu_2}, \eta^{-\mu_1}\zeta^{\nu_1}).$$

However,

$$J(a\eta^{|M|} + b\zeta^{|M|} + c) = a\eta^{|M|} + b\zeta^{|M|} + c = a\eta^{|M|} + D(\zeta)$$

is irreducible by the theorem of Capelli applied to the binomial $a|\eta|^M + D(\zeta)$ in the function field $\mathbb{Q}(\zeta)$; in fact, $\pm D(\zeta)$ is not a power of any element of $\mathbb{Q}(\zeta)$ with exponent > 1. It

follows that

$$JG_i(\eta^{\mu_2}\zeta^{-\nu_2}, \eta^{-\mu_1}\zeta^{\nu_1}) = \text{const}, \quad i = 1 \text{ or } 2,$$

whence by a substitution $\eta = Y^{\nu_1}Z^{\nu_2}$, $\zeta = Y^{\mu_1}Z^{\mu_2}$

$$JG_i(Y^{|M|}, Z^{|M|}) = \text{const}, \quad i = 1 \text{ or } 2.$$

Since $|M| \neq 0$ and by (118) $G_i(0,0) \neq 0$, we get $G_i(y,z) = \text{const}$ $(i = 1 \text{ or } 2)$. This shows that $J(ay^{\nu_1}z^{\nu_2} + by^{\mu_1}z^{\mu_2} + c)$ is irreducible and consequently (117) holds. Part (i) of Theorem 3 is thus proved.

In order to prove part (ii) we notice that by the Corollary to Theorem 1 there exists an integer δ satisfying the following conditions:

$$0 < \delta \leqslant C'\big(ax^{n/(n,m)} + bx^{m/(n,m)} + c\big); \quad (n,m) = \delta u,\ u \text{ integer}; \tag{119}$$

if

$$K\big(ax^{n\delta/(n,m)} + bx^{m\delta/(n,m)} + c\big) = \text{const}\, F_1(x)^{e_1}F_2(x)^{e_2}\cdots F_r(x)^{e_r}$$

is a standard form of $K\big(ax^{n\delta/(n,m)} + bx^{m\delta/(n,m)} + c\big)$, then

$$K(ax^n + bx^m + c) = \text{const}\, F_1(x^u)^{e_1}F_2(x^u)^{e_2}\cdots F_r(x^u)^{e_r}$$

is a standard form of $K(ax^n + bx^m + c)$. We put $\nu = n\delta/(n,m)$, $\mu = m\delta/(n,m)$.

Clearly $n/\nu = m/\mu$ is integral. Further by (117) and the definition of S: $\langle n/(n,m), m/(n,m)\rangle \in S$, and thus by (116) and (119)

$$\nu \leqslant A(a,b,c)\delta \leqslant B(a,b,c).$$

This completes the proof. □

6.

Proof of Theorem 4. Put $(ax^n + bx^m + c)/K(ax^n + bx^m + c) = g(x)$. Clearly $g(x) \mid ax^n + bx^m + c$ and $g(x) \mid cx^n + bx^{n-m} + a$, whence

$$\begin{aligned} g(x) \mid (cx^n + a)(ax^n + bx^m + c) - bx^m(cx^n + bx^{n-m} + a) \\ = ac\Big(x^{2n} + \frac{a^2 + c^2 - b^2}{ac}\,x^n + 1\Big), \\ g(x) \mid (cx^m + b)(ax^n + bx^m + c) - ax^m(cx^n + bx^{n-m} + a) \\ = bc\Big(x^{2m} + \frac{b^2 + c^2 - a^2}{bc}\,x^m + 1\Big). \end{aligned} \tag{120}$$

If $g(x) \neq 1$, it follows that

$$x^2 + \frac{a^2 + c^2 - b^2}{ac}\,x + 1 \neq K\Big(x^2 + \frac{a^2 + c^2 - b^2}{ac}\,x + 1\Big),$$

$$x^2 + \frac{b^2 + c^2 - a^2}{bc}\,x + 1 \neq K\Big(x^2 + \frac{b^2 + c^2 - a^2}{bc}\,x + 1\Big).$$

On the other hand, the only monic reciprocal quadratic polynomials which have roots of unity as zeros are x^2+1, $x^2\pm x+1$, $x^2\pm 2x+1$. It follows that $a^2+c^2-b^2=\varepsilon rac$, $b^2+c^2-a^2=\eta sbc$, where $|\varepsilon|=|\eta|=1$; $r=0$, 1 or 2; $s=0$, 1 or 2. Hence

$$2c^2=\varepsilon rac+\eta sbc, \qquad 2a^2-2b^2=\varepsilon rac-\eta sbc;$$
$$2c=\varepsilon ra+\eta sb, \qquad 4a^2-4b^2=(\varepsilon ra)^2-(\eta sb)^2,$$

and

$$a^2\big(4-(\varepsilon r)^2\big)=b^2\big(4-(\eta s)^2\big).$$

The last inequality implies $(\varepsilon r)^2=(\eta s)^2$, and thus $r=s$. Since $c\neq 0$, it is impossible that $s=r=0$; thus two cases remain:

$$r=s=1, \quad a^2=b^2, \quad c=\varepsilon a=\eta b; \tag{121}$$
$$r=s=2, \quad c=\varepsilon a+\eta b. \tag{122}$$

In the first case, by (120)

$$g(x)\,|\,x^{2n}+\varepsilon x^n+1,$$

and since all zeros of $x^{2n}+\varepsilon x^n+1$ are roots of unity

$$g(x)=(ax^n+bx^m+c,\, x^{2n}+\varepsilon x^n+1).$$

On the other hand, by (121)

$$c(x^{2n}+\varepsilon x^n+1)x^m=\eta(ax^n+bx^m+c)+c(x^{m+n}-\varepsilon\eta)(x^n+\varepsilon)$$

and since $(x^{2n}+\varepsilon x^n+1,\, x^n+\varepsilon)=1$, it follows that

$$g(x)=(ax^n+bx^m+c,\, x^{2n}+\varepsilon x^n+1)=(x^{2n}+\varepsilon x^n+1,\, x^{m+n}-\varepsilon\eta).$$

In the second case, by (120)

$$g(x)\,|\,x^{2n}+2\varepsilon x^n+1=(x^n+\varepsilon)^2,$$

and since all zeros of $x^n+\varepsilon$ are roots of unity,

$$g(x)=\big(ax^n+bx^m+c,\,(x^n+\varepsilon)^2\big).$$

On the other hand, by (122)

$$ax^n+bx^m+c=a(x^n+\varepsilon)+b(x^m+\eta),$$

and every multiple factor of ax^n+bx^m+c divides

$$nax^n+bmx^m=na(x^n+\varepsilon)+mb(x^m+\eta)-(an\varepsilon+mb\eta).$$

It follows that in the second case

$$g(x)=\begin{cases}(x^n+\varepsilon,\,x^m+\eta)^2 & \text{if } an\varepsilon+bm\eta=0,\\ (x^n+\varepsilon,\,x^m+\eta) & \text{if } an\varepsilon+bm\eta\neq 0.\end{cases}$$

In order to complete the proof it remains to calculate

$$(x^{2n}+\varepsilon x^n+1,\, x^{m+n}-\varepsilon\eta) \quad \text{and} \quad (x^n+\varepsilon,\, x^m+\eta).$$

This is easily done by factorization in cyclotomic fields (cf. [1], p. 69, where in Theorem 3 $\varepsilon^m \varepsilon'^n$ should be replaced by $\varepsilon^{m_1} \varepsilon'^{n_1}$). □

7.

Proof of Theorem 5. Put in Theorem 2 $F(y, z) = y + f(z)$. Since $f(z) \not\equiv \pm 1$ and $f(0) \neq 0$, $JF(y, z) \neq \pm JF(y^{-1}, z^{-1})$, and thus the assumptions of the theorem are satisfied and the constants $C_0\big(y + f(z)\big)$, $C_1\big(y + f(z)\big)$ exist. We put

$$D_0(f) = \max\big\{C_0\big(y + f(z)\big), C_1\big(y + f(z)\big)\big\},$$

$D_1(f) =$ the greatest common divisor of multiplicities of all the zeros of $f(z)$.

By Theorem 2 for every n there exists an integral matrix

$$\begin{bmatrix} \nu_1 & \mu_1 \\ \nu_2 & \mu_2 \end{bmatrix}$$

satisfying the following conditions

$$0 \leqslant \nu_i \leqslant C_1\big(y + f(z)\big), \quad 0 \leqslant \mu_i \leqslant C_1\big(y + f(z)\big) \quad (i = 1, 2), \tag{123}$$

$$n = \nu_1 u + \nu_2 v, \quad 1 = \mu_1 u + \mu_2 v, \quad u, v \text{ integers} \geqslant 0; \tag{124}$$

$$\begin{aligned} &\text{if } K\big(x^n + f(x)\big) \text{ is reducible, then} \\ &\text{either } J\big(y^{\nu_1} z^{\nu_2} + f(y^{\mu_1} z^{\mu_2})\big) \text{ is reducible} \\ &\text{or } n = \max\{n, 1\}/(n, 1) \leqslant C_0\big(y + f(z)\big) \leqslant D_0(f). \end{aligned} \tag{125}$$

It follows from (123) and (124) that $\mu_1 u = 0$, $\mu_2 v = 1$ or $\mu_1 u = 1$, $\mu_2 v = 0$. In view of symmetry it is enough to consider the first possibility. We then have $\mu_2 = v = 1$ and $u = 0$ or $\mu_1 = 0$. If $u = 0$, then

$$n = \nu_2 \leqslant C_1\big(y + f(z)\big) \leqslant D_0(f). \tag{126}$$

If $\mu_1 = 0$, then

$$J\big(y^{\nu_1} z^{\nu_2} + f(y^{\mu_1} z^{\mu_2})\big) = y^{\nu_1} z^{\nu_2} + f(z).$$

By the theorem of Capelli applied to the binomial $y^{\nu_1} + z^{-\nu_2} f(z)$ in the function field $\mathbb{Q}(z)$, $y^{\nu_1} z^{\nu_2} + f(z)$ is reducible only if $-z^{-\nu_2} f(z) = g(z)^p$ and $p \mid \nu_1$ or $z^{-\nu_2} f(z) = 4g(z)^4$ and $4 \mid \nu_1$, where $g(z)$ is a rational function and p is a prime. Since $f(0) \neq 0$, it follows that for some prime p

$$p \mid D_1(f), \quad p \mid \nu_1 \quad \text{and} \quad p \mid \nu_2.$$

By (124), this implies

$$\big(n, D_1(f)\big) \neq 1. \tag{127}$$

Therefore, if $K\big(x^n + f(x)\big)$ is reducible, at least one of the inequalities (125), (126) and (127) is satisfied. This completes the proof. □

Note added in proof. 1. H. Zassenhaus and the writer have proved (cf. [4a]) the following improvement of inequality (4): $\max_{1 \leqslant i \leqslant N} |\beta^{(i)}| > 1 + 2^{-N-4}$. Hence inequality (1) can be improved as follows:

$$e(a, \Omega) \leqslant (2^{N+4} + 1) \log(N H(\alpha)).$$

2. E. G. Straus has proved the equality $\varrho = \varrho_0$ conjectured on p. 314. His general proof (to appear in [4b]) specialized to the case $\varrho_0 = 2$ would lead also to a simpler proof of Lemma 4 than that given in the present paper.

References

[1] W. Ljunggren, *On the irreducibility of certain trinomials and quadrinomials*. Math. Scand. 8 (1960), 65–70.

[2] J. Mikusiński, A. Schinzel, *Sur la réductibilité de certains trinômes*. Acta Arith. 9 (1964), 91–95.

[3] A. Schinzel, *Solution d'un problème de K. Zarankiewicz sur les suites de puissances consécutives de nombres irrationnels*. Colloq. Math. 9 (1962), 291–296; *Correction*, ibid. 12 (1964), 289; this collection: D1, 295–300.

[4] —, *Some unsolved problems on polynomials*. In: Neki nerešeni problemi u matematici, Matematička Biblioteka 25, Beograd 1963, 63–70; this collection: E1, 703–708.

[4a] A. Schinzel, H. Zassenhaus, *A refinement of two theorems of Kronecker*. Michigan Math. J. 12 (1965), 81–85; this collection: C1, 175–178.

[4b] E. G. Straus, *Rational dependence in finite sets of numbers*. Acta Arith. 11 (1965), 203–204.

[5] N. Tschebotaröw, *Grundzüge der Galoisschen Theorie*. Übersetzt und bearbeitet von H. Schwerdtfeger, Noordhoff, Groningen–Djakarta 1950.

Originally published in
Acta Arithmetica XIII (1967), 91–101

Reducibility of polynomials and covering systems of congruences

The following problem has been proposed by Professor P. Turán in an oral communication:

Does there exist a constant C such that for every polynomial $f(x) = \sum_{i=0}^{n} a_i x^{n-i}$ (a_i integers, $a_0 \neq 0$), there is a polynomial $g(x) = \sum_{i=0}^{n} b_i x^{n-i}$ (b_i integers) irreducible over the rationals and satisfying $\sum_{i=0}^{n} |b_i - a_i| \leqslant C$?

This problem, apparently very difficult, becomes simpler if one removes the condition that the degree of g should not exceed the degree of f. Then it seems plausible that for polynomials $f(x)$ with $f(0) \neq 0$ the value of C can be taken 1, i.e. for a suitable n and a suitable sign the polynomial $\pm x^n + f(x)$ is irreducible.

I have treated the irreducibility of $x^n + f(x)$ in [3] and I have proved (Theorem 5) that for every polynomial $f(x)$ with rational coefficients such that $f(0) \neq 0$, $f(1) \neq -1$ and $f(x) \not\equiv 1$, there exist infinitely many n's for which $x^n + f(x)$ has exactly one irreducible factor that is not a cyclotomic polynomial (the precise formulation of the theorem says a little more). The example

$$f_0(x) = \frac{1}{12}(3x^9 + 8x^8 + 6x^7 + 9x^6 + 8x^4 + 3x^3 + 6x + 5)$$

shows that $x^n + f(x)$ may have cyclotomic factors for any n. In this example, however, the coefficients of $f(x)$ are not integers. The aim of the present paper is to investigate the irreducibility of $x^n + f(x)$, where $f(x)$ has integer coefficients and to show its connection with the so called covering systems of congruences.

A system of congruences $a_i \bmod m_i$ is called *covering* if every integer satisfies one of the congruences (cf. [1] and the papers quoted there). The precise formulation of the results is given below, but their most striking consequence is that if there are no covering systems with distinct odd moduli > 1 (the conjecture of Selfridge), then for every polynomial $f(x)$ with integer coefficients such that $f(0) \neq 0$, $f(1) \neq -1$, $x^n + f(x)$ is irreducible for infinitely many n.

Theorem 1. *The following two propositions are equivalent.*

A. *For every polynomial $f(x)$ with integer coefficients such that $f(0) \neq 0$, $f(1) \neq -1$ and $f(x) \not\equiv 1$, there exists an arithmetical progression N such that if $v \in N$ then $x^v + f(x)$ is irreducible over the rationals.*

B. *In every finite covering system of congruences $a_i \bmod m_i$ $(m_i > 1)$ at least one of the quotients m_j/m_i equals q^α (q prime, $\alpha \geqslant 0$), $a_j \not\equiv a_i \bmod m_i$ and either $q > 2$ or $m_i \equiv 1 \bmod 2$ or $a_j \not\equiv a_i \bmod (m_i/2)$.*

Theorem 2. *There is an implication* C $\rightarrow$ B $\rightarrow$ D*, where* C *and* D *are the following propositions.*

C. *In every finite covering system of congruences $a_i \bmod m_i$ $(m_i > 1)$ either there are two equal moduli or there is a modulus even.*

D. *In every finite covering system of congruences $a_i \bmod m_i$ $(m_i > 1)$ at least one modulus divides another one.*

Notation. $\mathbb{Z}$ is the ring of integers, $\mathbb{Q}$ the field of rationals, a monic polynomial means a polynomial with the highest coefficient ± 1.

$X_n(x)$ is the nth cyclotomic polynomial, ζ_n is a primitive nth root of unity. For any polynomial $f(x)$, $Kf(x)$ is the factor of $f(x)$ of the greatest possible degree whose no root is 0 or a root of unity and whose leading coefficient is equal to that of $f(x)$.

Lemma 1. *Let $F_i(x)$, $a_i(x) \in \mathbb{Z}[x]$ $(i = 1, 2, \ldots, r)$. If the polynomials $F_i(x)$ $(i = 1, 2, \ldots, r)$ are monic and relatively prime in pairs modulo every prime, then there exists a polynomial $f(x) \in \mathbb{Z}[x]$ such that*

$$f(x) \equiv a_i(x) \bmod F_i(x), \tag{1}$$

$$\text{degree } f(x) < \text{degree} \prod_{i=1}^{r} F_i(x). \tag{2}$$

Proof. For each $i \leqslant r$ consider the polynomials

$$F_i(x) \quad \text{and} \quad G_i(x) = F_i(x)^{-1} \prod_{i=1}^{r} F_i(x).$$

Since they are monic and relatively prime $\bmod 2$ they are relatively prime over $\mathbb{Q}$ and there exist polynomials $U_i(x)$, $V_i(x) \in \mathbb{Z}[x]$ such that

$$\text{degree } U_i < \text{degree } G_i, \quad \text{degree } V_i < \text{degree } F_i$$

and

$$F_i(x)U_i(x) + G_i(x)V_i(x) = R_i \neq 0.$$

Let $U_i(x) = u_i U_i^*(x)$, $V_i(x) = v_i V_i^*(x)$, where u_i, v_i are integers and $U_i^*(x)$, $V_i^*(x)$ are primitive polynomials.

If $R_i/(u_i, v_i)$ has any prime factor p, we have

$$\text{either} \quad p \nmid \frac{u_i}{(u_i, v_i)} \quad \text{or} \quad p \nmid \frac{v_i}{(u_i, v_i)}.$$

Without loss of generality we may assume the former. Since $F_i(x)$ and $G_i(x)$ are relatively prime mod p, it follows from

$$F_i(x)\frac{u_i}{(u_i, v_i)}\, U_i^*(x) + G_i(x)\frac{v_i}{(u_i, v_i)}\, V_i^*(x) = \frac{R_i}{(u_i, v_i)} \tag{3}$$

that

$$\frac{u_i}{(u_i, v_i)}\, U_i^*(x) \equiv 0 \left(\text{mod } p, G_i(x)\right).$$

Since $u_i \neq 0$ and $G_i(x)$ is monic, the degree of $U_i^*(x)$ is less than the degree of $G_i(x)$ also mod p, thus we get a contradiction.

Therefore, $R_i/(u_i, v_i)$ has no prime factors; equals $\varepsilon_i = \pm 1$ and it follows from (3) that

$$\varepsilon_i\, \frac{v_i}{(u_i, v_i)}\, G_i(x) V_i^*(x) \equiv \begin{cases} 1 \bmod F_i(x), \\ 0 \bmod G_i(x). \end{cases} \tag{4}$$

Now, put

$$\sum_{i=1}^{r} \varepsilon_i\, \frac{v_i}{(u_i, v_i)}\, a_i(x) G_i(x) V_i^*(x) = q(x) \prod_{i=1}^{r} F_i(x) + f(x), \tag{5}$$

where $q(x) \in \mathbb{Q}[x]$ and

$$\text{degree } f(x) < \text{degree} \prod_{i=1}^{r} F_i(x).$$

Since $\prod_{i=1}^{r} F_i(x)$ is monic, $f(x) \in \mathbb{Z}[x]$. By (4) and (5) (1) holds. □

Remark. Without the condition (2) the lemma is true also if polynomials $F_i(x)$ are not monic, but the proof is much more complicated.

Lemma 2. *If q is a prime, then $X_m(x)$, $X_n(x)$ $(m \leqslant n)$ are relatively prime* mod q *except if $n/m = q^\alpha$ $(\alpha \geqslant 0)$, in which case*

$$X_n(x) \equiv X_m(x)^{\varphi(n)/\varphi(m)} \bmod q. \tag{6}$$

Proof. Let $m = q^\mu m_1$, $n = q^\nu n_1$, where $q \nmid m_1 n_1$.

We have by the properties of cyclotomic polynomials

$$X_m(x) = \frac{X_{m_1}(x^{q^\mu})}{X_{m_1}(x^{q^{\mu-1}})} \equiv X_{m_1}(x)^{q^\mu - q^{\mu-1}} \bmod q \quad (\mu \geqslant 1) \tag{7}$$

and similarly

$$X_n(x) = \frac{X_{n_1}(x^{q^\nu})}{X_{n_1}(x^{q^{\nu-1}})} \equiv X_{n_1}(x)^{q^\nu - q^{\nu-1}} \bmod q \quad (\nu \geqslant 1). \tag{8}$$

If $n_1 \not\equiv m_1$, the polynomials $X_{m_1}(x)$, $X_{n_1}(x)$ are relatively prime over $\mathbb{Q}$, and both divide $x^{n_1 m_1} - 1$. Thus their resultant R divides the discriminant of $x^{n_1 m_1} - 1$ and since $n_1 m_1 \not\equiv 0 \bmod q$ we get $R \not\equiv 0 \bmod q$. Hence $X_{m_1}(x)$ and $X_{n_1}(x)$ are relatively prime mod q and by (7) and (8) the same is true about $X_m(x)$ and $X_n(x)$. If $n_1 = m_1$, (6) follows from (7) and (8) after taking into account the case $\mu = 0$. □

Lemma 3. *For every odd $c \geqslant 1$ and integer $\alpha \geqslant 1$ the polynomial*

$$D_{2^\alpha c}(x) = \tfrac{1}{2}\big[X_{2^\alpha c}(x) - X_c(x^{2^{\alpha-1}})\big] \tag{9}$$

belongs to $\mathbb{Z}[x]$, is monic and relatively prime mod every prime to $X_{2^\beta c}(x)$, where $\beta < \alpha$.

Proof. We have

$$X_{2^\alpha c}(x) = X_c(-x^{2^{\alpha-1}}), \tag{10}$$

thus $D_{2^\alpha c}(x) \in \mathbb{Z}[x]$. If $c = 1$, $D_{2^\alpha c}(x) = 1$, thus the lemma is true. If $c > 1$ and c^* is the product of all distinct prime factors of c, we have

$$X_c(x) = X_{c^*}(x^{c/c^*}) = x^{\varphi(c)} - \mu(c^*)x^{\varphi(c)-c/c^*} + \dots,$$

whence

$$D_{2^\alpha c}(x) = \mu(c^*)x^{2^{\alpha-1}(\varphi(c)-c/c^*)} + \dots$$

and $D_{2^\alpha c}(x)$ is monic. Since

$$X_c(x^{2^{\alpha-1}}) = \prod_{\beta=0}^{\alpha-1} X_{2^\beta c}(x),$$

it follows from Lemma 2 that $D_{2^\alpha c}(x)$ and $X_{2^\beta c}(x)$ ($\beta < \alpha$) are relatively prime modulo every odd prime. In order to prove that they are relatively prime mod 2 consider their resultant R. We have

$$R = \prod D_{2^\alpha c}(\zeta),$$

where ζ runs through all primitive roots of unity of degree $2^\beta c$. By (9) and (10)

$$R = 2^{-\varphi(2^\beta c)} \prod X_c(-\zeta^{2^{\alpha-1}}).$$

When ζ runs through all primitive roots of unity of degree $2^\beta c$, $\zeta^{2^{\alpha-1}}$ runs $\varphi(2^\beta)$ times through all primitive roots of unity of degree c. Therefore,

$$R = 2^{-\varphi(2^\beta c)}\Big(\prod_{(\gamma,c)=1} X_c(-\zeta_c^\gamma)\Big)^{\varphi(2^\beta)}.$$

Since

$$X_c(x) = \prod_{(\delta,c)=1} (x - \zeta_c^{\delta}),$$

we have

$$\prod_{(\gamma,c)=1} X_c(-\zeta_c^{\gamma}) = \prod_{(\gamma\delta,c)=1} (\zeta_c^{\gamma} + \zeta_c^{\delta}) = 2^{\varphi(c)} \prod_{\substack{(\gamma\delta,c)=1 \\ \gamma\neq\delta}} (\zeta_c^{\gamma} + \zeta_c^{\delta}).$$

Thus

$$R = \prod_{(\gamma\delta,c)=1} (\zeta_c^{\gamma} + \zeta_c^{\delta})^{\varphi(2^\beta)} \equiv \prod_{\substack{(\gamma\delta,c)=1 \\ \gamma\neq\delta}} (\zeta_c^{\gamma} - \zeta_c^{\delta})^{\varphi(2^\beta)} \equiv d^{\varphi(2^\beta)} \bmod 2,$$

where d is the discriminant of $X_c(x)$. Since d is odd, R is also odd and the proof is complete. □

Lemma 4. *Let $f(x)$ be a polynomial satisfying the assumptions of Proposition* A. *Let e_0 be the greatest integer e such that $-f(x) = g(x)^e$, $g(x) \in \mathbb{Z}[x]$.*

There exists a constant $D_0(f)$ such that if $n > D_0(f)$, $(\nu, e_0) = 1$ and $\nu \not\equiv 0 \bmod 4$ in the case $f(x) = 4h(x)^4$, $h(x) \in \mathbb{Z}[x]$, then $K\left(x^\nu + f(x)\right)$ is irreducible over $\mathbb{Q}$.

Proof. Put in Theorem 2 of [3]: $F(y, z) = y + f(z)$, $n = \nu$, $m = 1$. By that theorem there exists an integral matrix $M = \begin{bmatrix} \nu_1 & \mu_1 \\ \nu_2 & \mu_2 \end{bmatrix}$ with the following properties:

$$0 \leqslant \nu_i \leqslant C_1(F), \quad 0 \leqslant \mu_i \leqslant C_1(F) \quad (i = 1, 2), \tag{11}$$

$$[\nu, 1] = [u, v]M, \quad (u, v \text{ integers} \geqslant 0), \tag{12}$$

(13) if $y^{\nu_1} z^{\nu_2} + f(y^{\mu_1} z^{\mu_2}) = \text{const}\, F_1(y, z)^{e_1} F_2(y, z)^{e_2} \cdots F_r(y, z)^{e_r}$ is a decomposition of $y^{\nu_1} z^{\nu_2} + f(y^{\mu_1} z^{\mu_2})$ into factors irreducible over $\mathbb{Q}$, then either

$$K\left(x^\nu + f(x)\right) = \text{const}\, K F_1(x^u, x^v)^{e_1} K F_2(x^u, x^v)^{e_2} \cdots K F_r(x^u, x^v)^{e_r}$$

is a decomposition of $K\left(x^\nu + f(x)\right)$ into factors irreducible over $\mathbb{Q}$ or

$$\nu \leqslant C_0(F).$$

$C_0(F)$ and $C_1(F)$ are constants independent of ν.

We take $D_0(f) = \max\{C_0(F), C_1(F)\}$ and assume $\nu > D_0(f)$, $(\nu, e_0) = 1$ and $\nu \not\equiv 0 \bmod 4$ if $f(x) = 4h(x)^4$, $h(x) \in \mathbb{Z}[x]$.

It follows from (12) that

$$\nu = \nu_1 u + \nu_2 v, \quad 1 = \mu_1 u + \mu_2 v, \tag{14}$$

thus by (11)

$$\mu_1 u = 1,\ \mu_2 v = 0 \quad \text{or} \quad \mu_1 u = 0,\ \mu_2 v = 1.$$

c In view of the symmetry we may assume the latter. Thus $\mu_2 = v = 1$ and either $u = 0$ of $\mu_1 = 0$. If $u = 0$, then $v = \nu_2 \leqslant D_0(f)$ against the assumption. If $\mu_1 = 0$,

$$y^{\nu_1} z^{\nu_2} + f(y^{\mu_1} z^{\mu_2}) = y^{\nu_1} z^{\nu_2} + f(z).$$

By the theorem of Capelli (cf. [3], p. 6 ([1])) the last polynomial can be reducible over $\mathbb{Q}$ only if

$$-f(z)z^{-\nu_2} = k(z)^p, \quad \text{where} \quad p \mid \nu_1 \text{ and } k(z) \in \mathbb{Q}(z) \tag{15}$$

or

$$f(z)z^{-\nu_2} = 4k(z)^4, \quad \text{where} \quad 4 \mid \nu_1 \text{ and } k(z) \in \mathbb{Q}(z). \tag{16}$$

Since $f(0) \neq 0$, (15) implies that $p \mid e_0$ and $p \mid \nu_2$, thus by (14) $(\nu, e_0) \neq 1$ against the assumption. Similarly (16) implies that $f(z) = 4h(z)^4$, $h(z) \in \mathbb{Z}[z]$ and $\nu \equiv 0 \bmod 4$, again contrary to the assumption. Thus $y^{\nu_1} z^{\nu_2} + f(y^{\mu_1} z^{\mu_2})$ is irreducible over $\mathbb{Q}$ and by (13) $K\left(x^{\nu} + f(x)\right)$ is also irreducible. □

Proof of Theorem 1. *Implication* A $\rightarrow$ B. Assume B is false, thus there exists a finite set S of integral pairs (m, a) with $m > 1$ and with the following properties.

(17) For every integer ν there exists a pair $(m, a) \in S$ such that $\nu \equiv a \bmod m$ (the system $a \bmod m$, $(m, a) \in S$ is covering).

(18) If $(m, a) \in S$, $(n, b) \in S$ and $n/m = q^{\alpha}$ (q prime, $\alpha \geqslant 0$), then either $b \equiv a \bmod m$ or $q = 2$, $m \equiv 0 \bmod 2$ and $b \equiv a \bmod \dfrac{m}{2}$.

Let S_0 be a subset of S irreducible with respect to property (17). If $(m, a) \in S_0$, $(n, b) \in S_0$, $(m, a) \neq (n, b)$ and $m \mid n$, then $b \not\equiv a \bmod m$; otherwise, $S_0 \setminus \{(n, b)\}$ would also have property (17). Property (18) is hereditary, but in view of the last remark it takes for S_0 the following simpler form.

> If $(m, a) \in S_0$, $(n, b) \in S_0$, $(m, a) \neq (n, b)$ and $n/m = q^{\alpha}$ (q prime, $\alpha \geqslant 0$), then $q = 2$, $\alpha > 0$, $m \equiv 0 \bmod 2$, $b \equiv a \bmod \dfrac{m}{2}$ and $b \not\equiv a \bmod m$.

Divide the set S_0 into classes assigning two pairs (m, a) and (n, b) to the same class if $n/m = 2^{\alpha}$ ($a \geqslant 0$ or < 0). We obtain the decomposition of S_0

$$S_0 = \bigcup_{i=1}^{r} C_i, \tag{19}$$

and the pairs in any class C_i can be represented in the form $(2^{\alpha_{ij}} c_i, a_{ij})$ $(j = 1, 2, \ldots, k_i)$, c where c_i is odd and either $k_i = 1$, $2^{\alpha_{i1}} c_i > 1$ or

$$\begin{gathered} 0 < \alpha_{i1} < \alpha_{i2} < \ldots < \alpha_{ik_i} = \alpha_i, \\ a_{ij} \equiv a_{ik_i} \bmod 2^{\alpha_{ij}-1} c_i, \quad a_{ij} \not\equiv a_{ik_i} \bmod 2^{\alpha_{ij}} c_i \quad (1 \leqslant j < k_i). \end{gathered} \tag{20}$$

([1]) This collection, page 306.

For each i such that $k_i > 1$ consider the system of congruences

$$g(x) \equiv 0 \bmod \prod_{j=1}^{k_i-1} X_{2^{\alpha_{ij}}c_i}(x), \quad g(x) \equiv -x^{a_{ik_i}} \bmod D_{2^{\alpha_i}c_i}(x). \tag{21}$$

By Lemma 3 for each $j < k_i$, $X_{2^{\alpha_{ij}}c_i}(x)$ is relatively prime to $D_{2^{\alpha_i}c_i}(x)$ mod every prime, thus the same is true about $\prod_{j=1}^{k_i-1} X_{2^{\alpha_{ij}}c_i}(x)$. By Lemma 1 for each i such that $k_i > 1$, there exists a polynomial $g_i(x) \in \mathbb{Z}[x]$ satisfying the system (21).

Now, put for each $i \leqslant r$:

$$f_i(x) = \begin{cases} \dfrac{g_i(x) + x^{a_{ik_i}}}{D_{2^{\alpha_i}c_i}(x)} X_{2^{\alpha_i}c_i}(x) - x^{a_{ik_i}}, & \text{if } k_i > 1, \\ -x^{a_{i1}}, & \text{if } k_i = 1, \end{cases} \tag{22}$$

and consider the system of congruences

$$f(x) \equiv f_i(x) \bmod \prod_{j=1}^{k_i} X_{2^{\alpha_{ij}}c_i}(x) \quad (i = 1, 2, \ldots, r). \tag{23}$$

By Lemma 2 the moduli are relatively prime in pairs mod every prime, thus by Lemma 1 there exists a polynomial $f_{r+1}(x) \in \mathbb{Z}[x]$ satisfying (23) and such that

$$\text{degree } f_{r+1}(x) < \text{degree} \prod_{i=1}^{r} \prod_{j=1}^{k_i} X_{2^{\alpha_{ij}}c_i}(x). \tag{24}$$

We claim that

$$f_{r+1}(x) \equiv -x^{a_{ij}} \bmod X_{2^{\alpha_{ij}}c_i}(x) \quad (1 \leqslant i \leqslant r,\ 1 \leqslant j \leqslant k_i). \tag{25}$$

This is clear by (22), if $k_i = 1$. On the other hand, if $k_i > 1$,

$$X_{c_i}(x^{2^{\alpha_i - 1}}) = \prod_{\beta=0}^{\alpha_i - 1} X_{2^\beta c_i}(x),$$

thus

$$2D_{2^{\alpha_i}c_i}(x) \equiv X_{2^{\alpha_i}c_i}(x) \bmod \prod_{j=1}^{k_i-1} X_{2^{\alpha_{ij}}c_i}(x)$$

and it follows from (21) (with g replaced by g_i), (22) and (23) (with f replaced by f_{r+1}) that

$$\begin{aligned} f_{r+1}(x) &\equiv x^{a_{ik_i}} \bmod \prod_{j=1}^{k_i-1} X_{2^{\alpha_{ij}}c_i}(x), \\ f_{r+1}(x) &\equiv -x^{a_{ik_i}} \bmod X_{2^{\alpha_i}c_i}(x). \end{aligned} \tag{26}$$

By (20) $a_{ik_i} \equiv a_{ij} \bmod 2^{\alpha_{ij}-1}c_i$, but $a_{ik_i} \not\equiv a_{ij} \bmod 2^{\alpha_{ij}}c_i$, hence $x^{2a_{ik_i}} \equiv x^{2a_{ij}} \bmod X_{2^{\alpha_{ij}}c_i}(x)$, $x^{a_{ik_i}} \not\equiv x^{a_{ij}} \bmod X_{2^{\alpha_{ij}}c_i}(x)$, thus

$$x^{a_{ik_i}} \equiv -x^{a_{ij}} \bmod X_{2^{\alpha_{ij}}c_i}(x) \quad (1 \leqslant j < k_i). \tag{27}$$

Now (25) follows from (26) and (27). Put

$$t = \max\{1, 2 - f_{r+1}(0), -f_{r+1}(1)\} \tag{28}$$

and consider the polynomial

$$f_0(x) = f_{r+1}(x) + t\prod_{i=1}^{r}\prod_{j=1}^{k_i} X_{2^{\alpha_{ij}}c_i}(x). \tag{29}$$

By (20) $2^{\alpha_{ij}}c_i > 1$, thus we have

$$f_0(0) = f_{r+1}(0) + t \geqslant 2, \quad f_0(1) \geqslant f_{r+1}(1) + t \geqslant 0$$

and the polynomial $f_0(x)$ satisfies the assumptions of Proposition A. On the other hand, by the choice of S_0 and (19) for every integer $\nu \geqslant 0$ there exist $i \leqslant r$ and $j \leqslant k_i$ such that

$$\nu \equiv a_{ij} \bmod 2^{\alpha_{ij}}c_i.$$

Hence

$$x^{\nu} \equiv x^{a_{ij}} \bmod X_{2^{\alpha_{ij}}c_i}(x)$$

and by (25) and (29)

$$x^{\nu} + f_0(x) \equiv 0 \bmod X_{2^{\alpha_{ij}}c_i}(x). \tag{30}$$

However, by (24) and (28) $f_0(x)$ has the degree equal to that of $\prod_{i=1}^{r}\prod_{j=1}^{k_i} X_{2^{\alpha_{ij}}c_i}(x)$ and the leading coefficient positive. Since $\sum_{i=1}^{r} k_i > 1$, the degree of $x^{\nu} + f_0(x)$ is greater than that of $X_{2^{\alpha_{ij}}c_i}(x)$ and it follows from (30) that $x^{\nu} + f_0(x)$ is reducible. Thus we have proved more than was necessary, namely the existence of a polynomial $f(x)$ satisfying the assumptions of Proposition A and such that $x^{\nu} + f(x)$ is reducible for all $\nu \geqslant 0$.

Implication B $\rightarrow$ A. Let $f(x)$ be a polynomial satisfying the assumptions of A and let e_0 be the greatest integer e such that

$$-f(x) = g(x)^e, \quad g(x) \in \mathbb{Z}[x].$$

Consider first the case, where $f(x) = 4h(x)^4$, $h(x) \in \mathbb{Z}[x]$. Then let r_0 be the least number r such that $(r, 2e_0) = 1$ and $r > D_0(f)$. The arithmetical progression $N: 2e_0t + r_0$ $(t = 0, 1, \dots)$ has the property asserted in A. Indeed, if $\nu \in N$ then $\nu > D_0(f)$, $(\nu, e_0) = 1$ and $\nu \not\equiv 0 \bmod 4$, thus, by Lemma 4, $K\big(x^{\nu} + f(x)\big)$ is irreducible. But no root of unity, ζ_m say, can be a zero of $x^{\nu} + f(x)$, since it would follow that

$$\zeta_m^{\nu} + 4h(\zeta_m)^4 = 0, \quad \zeta_m^{\nu} \equiv 0 \bmod 4,$$

which is impossible.

Assume now that $f(x) \neq 4h(x)^4$, $h(x) \in \mathbb{Z}[x]$. Let P be the set of all pairs $(p, 0)$, where p is a prime and $p \mid e_0$. Let M be the set of all pairs (μ, α), where $0 \leqslant \alpha < \mu$ and

$$\zeta_\mu^\alpha + f(\zeta_\mu) = 0. \tag{31}$$

M is finite. Indeed, it follows from (31) that $f(\zeta_\mu) f(\zeta_\mu^{-1}) = 1$, thus ζ_μ is a root of the equation $x^d f(x) f(x^{-1}) - x^d = 0$, where d is the degree of $f(x)$, and we get $\varphi(\mu) \leqslant 2d$. Since $f(1) \neq -1$ we have $\mu > 1$ for all $(\mu, \alpha) \in M$.

We claim that the system of congruences $a \bmod m$, where $(m, a) \in P \cup M$, does not satisfy the condition for covering system asserted in B. Indeed, suppose that

$$(m, a) \in P \cup M, \quad (n, b) \in P \cup M,$$

$$\frac{n}{m} = q^\alpha \quad (q \text{ prime}, \alpha \geqslant 0), \quad b \not\equiv a \bmod m, \tag{32}$$

$$q > 2 \quad \text{or} \quad m \equiv 1 \bmod 2 \quad \text{or} \quad b \not\equiv a \bmod \frac{m}{2}. \tag{33}$$

$(m, a) \in P$, $(n, b) \in P$ impossible in view of (32).

Consider first the case $(m, a) \in P$, $(n, b) \in M$. By the definition of P, m is a prime and

$$-f(x) = k(x)^m, \quad k(x) \in \mathbb{Z}[x].$$

On the other hand, by the definition of M

$$\zeta_n^b + f(\zeta_n) \equiv 0.$$

Thus, we get $k(\zeta_n)^m = \zeta_n^b$ and

$$k(\zeta_n) = \zeta_{mn}^\beta, \quad \text{where} \quad (\beta, n) = (b, n). \tag{34}$$

$k(\zeta_n)$ is a primitive root of unity of degree $mn/(\beta, mn)$, but $k(\zeta_n) \in \mathbb{Q}(\zeta_n)$, thus by a known theorem (cf. e.g. [2], p. 536)

$$\frac{mn}{(\beta, mn)} \,\Big|\, \frac{2n}{(2, n)}; \quad m \,\Big|\, \frac{2(\beta, mn)}{(2, n)}$$

and

$$m \,\Big|\, \frac{2\beta}{(2, n)}. \tag{35}$$

Since by the first part of (32) $m \mid n$, it follows from (34) and (35) that $b \equiv 0 \bmod m$, which contradicts the second part of (32).

Consider next the case $(m, a) \in M$, $(n, b) \in P$. Then since n is a prime and $m > 1$, it follows from (32) that $n = m$, thus we can interchange the roles of m and n and apply the preceding case.

Consider finally the case $(m, a) \in M$, $(n, b) \in M$. We have

$$\begin{aligned} x^a + f(x) &\equiv 0 \bmod X_m(x), \\ x^b + f(x) &\equiv 0 \bmod X_n(x). \end{aligned} \tag{36}$$

Since by Lemma 2, $X_n(x) \equiv X_m(x)^{\varphi(n)/\varphi(m)} \bmod q$, we get from (36)

$$x^b - x^a \equiv 0 \left(\bmod q, X_m(x)\right).$$

Since x and $X_m(x)$ are relatively prime $\bmod q$, it follows that

$$x^{|b-a|} - 1 \equiv 0 \left(\bmod q, X_m(x)\right). \tag{37}$$

Put $\Delta = |b-a| = q^\delta \Delta_1$, where $q \nmid \Delta_1$. We have

$$x^\Delta - 1 \equiv \left(x^{\Delta_1} - 1\right)^{q^\delta} \equiv \prod_{d \mid \Delta_1} X_d(x)^{q^\delta} \bmod q. \tag{38}$$

It follows from (37), (38) and Lemma 2 that for some $d_1 \mid \Delta_1$ and some $\beta \geqslant 0$,

$$\frac{m}{d_1} = q^\beta, \quad X_m(x) \equiv X_{d_1}(x)^{\varphi(m)/\varphi(d_1)} \bmod q,$$

and

$$X_{d_1}(x)^{q^\delta} \equiv 0 \left(\bmod q, X_{d_1}(x)^{\varphi(m)/\varphi(d_1)}\right).$$

The last congruence implies

$$q^\delta \geqslant \frac{\varphi(m)}{\varphi(d_1)} = \varphi(q^\beta). \tag{39}$$

If $\beta = 0$ or $q > 2$, it follows from (39) that $\delta \geqslant \beta$, thus $\Delta \equiv 0 \bmod m$ and $b \equiv a \bmod m$ contrary to (32). If $\beta > 0$ and $q = 2$ we get from (39) that $\delta \geqslant \beta - 1$, thus $\Delta \equiv 0 \bmod \frac{m}{2}$ and $b \equiv a \bmod \frac{m}{2}$ contrary to (33).

By the proposition B, the system $a \bmod m$, where $(m, a) \in P \cup M$, is not covering, thus there exist numbers D_1 and r_1 such that if $\nu \equiv r_1 \bmod D_1$, then $\nu \not\equiv a \bmod m$ for any $(m, a) \in P \cup M$.

Let r_2 be the least integer r such that $r \equiv r_1 \bmod D_1$ and $r > D_0(f)$. The arithmetical progression $N\colon D_1 t + r_2$ $(t = 0, 1, \dots)$ has the property asserted in A. Indeed, if $\nu \in N$ then $\nu > D_0(f)$ and $(\nu, e_0) = 1$, hence by Lemma 4 $K\left(x^\nu + f(x)\right)$ is irreducible. On the other hand, no root of unity can be a zero of $x^\nu + f(x)$, since this would imply $\left(m, \nu - m\left[\frac{\nu}{m}\right]\right) \in M$ for a suitable m. □

Proof of Theorem 2. The implication B → D being obvious, it is enough to prove C → B. Assume B is false, thus (compare the proof of Theorem 1, implication A → B) there exists a covering system $a_{ij} \bmod 2^{\alpha_{ij}} c_i$ $(1 \leqslant i \leqslant r, 1 \leqslant j \leqslant k_i)$, where c_i are odd and distinct and for $k_i > 1$ (20) holds.

Consider the system of congruences

$$a_{ik_i} \bmod c_i \quad (1 \leqslant i \leqslant r,\ c_i > 1), \tag{40}$$

$$a_{i_0 j} \bmod 2^{\alpha_{i_0 j}} \quad (1 \leqslant j \leqslant k_{i_0}), \quad \text{where } c_{i_0} = 1. \tag{41}$$

If C is true, system (40) is not covering, thus there exists an integer ν_1 such that

$$\nu_1 \not\equiv a_{ik_i} \bmod c_i, \quad \text{for any } i \leqslant r \text{ with } c_i > 1.$$

On the other hand, system (41) is not covering, since by (20) $a_{i_0 j}$ $(1 \leqslant j \leqslant k_{i_0})$ are distinct and $\sum_j \frac{1}{2^{\alpha_{i_0 j}}} < 1$. Thus there exists an integer ν_2 such that

$$\nu_2 \not\equiv a_{i_0 j} \bmod 2^{\alpha_{i_0 j}} \quad \text{for any} \quad j \leqslant k_{i_0}.$$

By the Chinese Remainder Theorem there exists

$$\nu_0 \equiv \begin{cases} \nu_1 \bmod \prod_{i=1}^{r} c_i, \\ \nu_2 \bmod 2^{\alpha_{i_0}}. \end{cases}$$

By the choice of ν_1 and ν_2, ν_0 does not satisfy any of the congruences (40) and (41), thus system (40)–(41) and *a fortiori* the system $a_{ij} \bmod 2^{\alpha_{ij}} c_i$ is not covering and we get a contradiction.

Remark. The implication C $\rightarrow$ D was first proved in a similar way by J. L. Selfridge.

References

[1] P. Erdős, *Some recent advances and current problems in number theory*. In: Lectures on Modern Mathematics, vol. 3, Wiley, New York 1965, 196–244.

[2] H. Hasse, *Zahlentheorie*. Akademie-Verlag, Berlin 1963.

[3] A. Schinzel, *On the reducibility of polynomials and in particular of trinomials*. Acta Arith. 11 (1965), 1–34; *Errata*, ibid., 491; this collection: D2, 301–332.

Originally published in
Acta Arithmetica XVI (1969), 123–159

Reducibility of lacunary polynomials I

To the memory of my teachers
Wacław Sierpiński and Harold Davenport

1.

The present paper is in close connection with [9], the notation of that paper is used and extended (for a result which requires little notation see Corollary to Theorem 2). Reducibility means reducibility over the rational field $\mathbb{Q}$. Constants are considered neither reducible nor irreducible. If $f(x_1, \dots, x_k) \neq 0$ is a polynomial, then

$$f(x_1, \dots, x_k) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} f_\sigma(x_1, \dots, x_k)^{e_\sigma}$$

means that polynomials f_σ are irreducible and relatively prime in pairs.

If $\Phi(x_1, \dots, x_k) = f(x_1, \dots, x_k) \prod_{i=1}^{k} x_i^{\alpha_i}$ where f is a polynomial, α_i are integers and $\big(f(x_1, \dots, x_k), x_1 \cdots x_k\big) = 1$ then

$$J\Phi(x_1, \dots, x_k) = f(x_1, \dots, x_k)$$

(this definition is equivalent to one given in [9]). Let

$$J\Phi(x_1, \dots, x_k) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} f_\sigma(x_1, \dots, x_k)^{e_\sigma}.$$

We set

$$K\Phi(x_1, \dots, x_k) = \text{const} \prod\nolimits_1 f_\sigma(x_1, \dots, x_k)^{e_\sigma},$$
$$L\Phi(x_1, \dots, x_k) = \text{const} \prod\nolimits_2 f_\sigma(x_1, \dots, x_k)^{e_\sigma},$$

where $\prod_1$ is extended over these f_σ which do not divide $J(x_1^{\delta_1} \cdots x_k^{\delta_k} - 1)$ for any $[\delta_1, \dots, \delta_k] \neq 0$, $\prod_2$ is extended over all f_σ such that

$$(*) \qquad Jf_\sigma(x_1^{-1}, \dots, x_k^{-1}) \neq \pm f_\sigma(x_1, \dots, x_k).$$

Corrigenda: *Acta Arithmetica* XIX (1971), 201; ibid. XXXIV (1978), 265.

The leading coefficients of $K\Phi$ and $L\Phi$ are assumed equal to that of $J\Phi$. In particular for $k = 1$, $K\Phi(x)$ equals $J\Phi(x)$ deprived of all its cyclotomic factors and $L\Phi(x)$ equals $J\Phi(x)$ deprived of all its monic irreducible reciprocal factors (a polynomial $f(x)$ is reciprocal if $Jf(x^{-1}) = \pm f(x)$). $J0 = K0 = L0 = 0$. Note that $(*)$ implies $Jf_\sigma(x_1^{-1}, \ldots, x_k^{-1}) \neq \text{const } f_\sigma(x_1, \ldots, x_k)$.

The operations J, K, L are distributive with respect to multiplication, besides for $k = 1$, J and K are commutative with the substitution $x \to x^n$ $(n \geqslant 0)$, L does not share this property and is always performed after the substitution. We have $KJ = JK = K$, $LJ = JL = L$, $LK = KL = L$; the first two formulae follow directly from the definitions, the last one requires a proof (see Lemma 11).

The paper has emerged from unsuccessful efforts to prove the conjecture formulated in [9] concerning the factorization of $KF(x^{n_1}, \ldots, x^{n_k})$ for given F. The operation L has turned out more treatable and the analogue of the conjecture for $LF(x^{n_1}, \ldots, x^{n_k})$ appears below as Lemma 12.

For a polynomial $F(x_1, \ldots, x_k)$ $\|F\|$ is the sum of squares of the absolute values of the coefficients of F; if $F \neq 0$, $|F|$ is the maximum of the degrees of F with respect to x_i $(1 \leqslant i \leqslant k)$,

$$|F|^* = \sqrt{\max\{|F|^2, 2\} + 2},$$

$\exp_1 x = \exp x$, $\exp_j x = \exp(\exp_{j-1} x)$.

From this point onwards all the polynomials considered have integral coefficients unless stated to the contrary. The highest common factor of two polynomials is defined only up to a constant; the formulae involving it should be suitably interpreted; we set $(0, 0) = 0$.

Theorem 1. *For any polynomial $F \neq 0$ and any integer $n \neq 0$ there exist integers v and u such that*

(i) $$0 \leqslant v \leqslant \exp\big(10|F| \log |F|^* \log \|F\|\big)^2,$$

(ii) $$n = uv,$$

(iii) $$KF(x^v) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(x)^{e_\sigma} \text{ implies } KF(x^n) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} JF_\sigma(x^u)^{e_\sigma}.$$

This is a quantitative formulation of Corollary to Theorem 1 [9] and a generalization of that theorem.

Theorem 2. *For any polynomial $F(x_1, \ldots, x_k)$ and any integral vector $\boldsymbol{n} = [n_1, \ldots, n_k] \neq \boldsymbol{0}$ such that $F\big(x^{n_1}, \ldots, x^{n_k}\big) \neq 0$ there exist an integral matrix $\boldsymbol{N} = [v_{ij}]_{\substack{i \leqslant r \\ j \leqslant k}}$ of rank r and an integral vector $\boldsymbol{v} = [v_1, \ldots, v_r]$ such that*

(i) $$\max |v_{ij}| \leqslant c_r(F),$$

(ii) $$\boldsymbol{n} = \boldsymbol{v}\boldsymbol{N},$$

(iii) $LF\Big(\prod_{i=1}^{r} y_i^{v_{i1}}, \dots, \prod_{i=1}^{r} y_i^{v_{ik}}\Big) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(y_1, \dots, y_r)^{e_\sigma}$ *implies*

$$LF\big(x^{n_1}, \dots, x^{n_k}\big) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} LF_\sigma\big(x^{v_1}, \dots, x^{v_r}\big)^{e_\sigma}.$$

Moreover

$$c_r(F) = \begin{cases} \exp 9k \cdot 2^{\|F\|-5} & \text{if } r = k, \\ \exp\big(5 \cdot 2^{\|F\|^2-4} 2\|F\| \log |F|^*\big) & \text{if } r + k = 3, \\ \exp_{(k-r)(k+r-3)}\big(10k|F|^{*\|F\|-1} \log \|F\|\big) & \text{otherwise.} \end{cases}$$

Corollary. *For any polynomial $f(x) \neq 0$ the number of its irreducible non-reciprocal factors except x counted with their multiplicities does not exceed*

$$\exp_{\|f\|^2-5\|f\|+7}\big(\|f\| + 2\big)$$

(*a bound independent of $|f|$*).

Theorem 2 is the main result of the paper. An essential role in the proof is played by a result of Straus [11]. It is an open question equivalent to the conjecture from [9] whether a similar theorem, possibly with greater constants $c_r(F)$, holds for the operation K instead of L.

The case $k = 1$ is settled by Theorem 1, for $k = 2$ a partial result is given by

Theorem 3. *For any polynomial $F(x_1, x_2)$ such that $KF(x_1, x_2) = LF(x_1, x_2)$ and any integral vector $\boldsymbol{n} = [n_1, n_2] \neq \boldsymbol{0}$ such that $F\big(x^{n_1}, x^{n_2}\big) \neq 0$ there exist an integral matrix $\boldsymbol{N} = [v_{ij}]_{\substack{i \leqslant r \\ j \leqslant 2}}$ of rank r and an integral vector $\boldsymbol{v} = [v_1, v_r]$ such that*

(i) $$\max_{i,j} |v_{ij}| \leqslant \begin{cases} \exp 9 \cdot 2^{\|F\|-4} & \text{if } r = 2, \\ \exp\big\{500\|F\|^2\big(2|F|^*\big)^{2\|F\|+1}\big\} & \text{if } r = 1, \end{cases}$$

(ii) $$\boldsymbol{n} = \boldsymbol{v}\boldsymbol{N},$$

(iii) $KF\Big(\prod_{i=1}^{r} y_i^{v_{i1}}, \prod_{i=1}^{r} y_i^{v_{i2}}\Big) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(y_1, y_r)^{e_\sigma}$ *implies*

$$KF\big(x^{n_1}, x^{n_2}\big) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} KF_\sigma\big(x^{v_1}, x^{v_r}\big)^{e_\sigma}.$$

This theorem is closely related to Theorem 2 of [9] but is both quantitative and more general, since it does not assume the irreducibility of F.

Theorem 4. *If $k \geqslant 2$, $a_0 \neq 0$, $a_j \neq 0$ and n_j $(1 \leqslant j \leqslant k)$ are integers then either*

$$L\Big(a_0 + \sum_{j=1}^{k} a_j x^{n_j}\Big)$$

is irreducible or there is an integral vector $[\gamma_1, \dots, \gamma_k]$ *such that*

$$0 < \max_j |\gamma_j| \leqslant \begin{cases} 2^{4\sum_{j=0}^{2} a_j^2+5} \log \sum_{j=0}^{2} a_j^2 & \text{if } k = 2, \\ \exp_{2k-4}\left(k 2^{\sum_{j=0}^{k} a_j^2+3} \log \sum_{j=0}^{k} a_j^2\right) & \text{if } k > 2 \end{cases}$$

c

and

$$\sum_{j=1}^{k} \gamma_j n_j = 0.$$

Theorem 5. *If* a, b, c, n, m *are integers,* $n > m > 0$, $abc \neq 0$ *then either* $K(ax^n+bx^m+c)$ *is irreducible or*

$$n/(n, m) \leqslant 2^{4(a^2+b^2+c^2)+5} \log(a^2 + b^2 + c^2)$$

and there exist integers ν *and* μ *such that* $m/\mu = n/\nu$ *is integral,*

$$0 < \mu < \nu \leqslant \exp(a^2 + b^2 + c^2)^2 2^{4(a^2+b^2+c^2)+11}$$

and

$$K(ax^\nu + bx^\mu + c) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(x)^{e_\sigma}$$

implies

$$K(ax^n + bx^m + c) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(x^{n/\nu})^{e_\sigma}.$$

This is a quantitative formulation of Theorem 3 of [9].

The proofs of Theorems 1, 2, 3, 4, 5 are given in §§ 2, 3, 4, 5, 5 respectively. Some of the proofs could be simplified at the cost of increasing the order of $c_r(F)$ and of other similar constants. Since however simplifications would not be great and the constants already are, I did as much as I could not to increase their order. On the other hand I have refrained from making generalizations to algebraic number fields. The method of proof of Theorem 1 works in any algebraic number field, while the method of proof of Theorems 2 and 3 works only in totally real fields and their totally complex quadratic extensions. The fields of these two types share the property that the trace of a square of the absolute value of any non-zero element is positive. In the case of totally complex fields, the definition of $L\Phi(x_1, \dots, x_k)$ must be modified, namely condition $(*)$ is to be replaced by

$$Jf_\sigma(x_1^{-1}, \dots, x_k^{-1}) \neq \text{const } \overline{f_\sigma(x_1, \dots, x_k)}.$$

c A generalization to function fields over totally real fields is also possible.

The following notation is used through the paper in addition to that introduced already.

1. $|\boldsymbol{\Omega}|$ is the degree of a field $\boldsymbol{\Omega}$.

2. ζ_q is a primitive root of unity of order q.
3. If $\boldsymbol{\Omega}$ is a field and $\alpha \in \boldsymbol{\Omega}$, $\alpha \neq 0$, then

$$e(\alpha, \boldsymbol{\Omega}) = \begin{cases} 0 & \text{if } \alpha = \zeta_q \text{ for some } q, \\ \text{maximal } e \text{ such that } \alpha = \zeta_q \beta^e \text{ with some } q \text{ and } \beta \in \boldsymbol{\Omega}, & \text{otherwise.} \end{cases}$$

4. $h(\boldsymbol{M})$ is the maximum of the absolute values of the elements of a matrix $\boldsymbol{M}$ (the height of $\boldsymbol{M}$).

$\boldsymbol{M}^T$ and $\boldsymbol{M}^A$ are matrices transposed and adjoint to $\boldsymbol{M}$, respectively. The same notation applies to vectors treated as matrices with one row. The elements of a vector denoted by a bold face letter are designated by the same ordinary letter with indices. Bold face capital letters represent matrices except $\boldsymbol{\Omega}$ that is a field.

2.

Lemma 1. *Let $\boldsymbol{\Omega}$ be an algebraic number field and $\alpha \neq 0$ an element of $\boldsymbol{\Omega}$ satisfying an equation $f(\alpha) = 0$, where f is a polynomial. Then*

$$e(\alpha, \boldsymbol{\Omega}) \leqslant \begin{cases} 20|\boldsymbol{\Omega}|^2 \log|\boldsymbol{\Omega}|^* \log\|f\| & \textit{always}, \\ \frac{5}{2}|\boldsymbol{\Omega}| \log\|f\| & \textit{if } \alpha \textit{ is not conjugate to } \alpha^{-1}, \\ (2\log 2)^{-1}|\boldsymbol{\Omega}| \log\|f\| & \textit{if } \alpha \textit{ is not an integer}. \end{cases} \tag{1}$$

Besides, for any algebraic number field $\boldsymbol{\Omega}_1 \supset \boldsymbol{\Omega}$

$$e(\alpha, \boldsymbol{\Omega}_1) \leqslant \frac{|\boldsymbol{\Omega}_1|}{|\boldsymbol{\Omega}|}\, e(\alpha, \boldsymbol{\Omega}). \tag{2}$$

Proof. If α is a root of unity, the lemma follows from the definition of $e(\alpha, \boldsymbol{\Omega})$. Assume that α is not a root of unity and let

$$\alpha = \zeta_q \beta^e, \quad \beta \in \boldsymbol{\Omega}, \quad e = e(\alpha, \boldsymbol{\Omega}). \tag{3}$$

If α is an integer, β is also. It follows that

$$\log\overline{|\alpha|} = e \log\overline{|\beta|}, \tag{4}$$

where $\overline{|\alpha|}$ is the maximal absolute value of the conjugates of α. Now by a recent result of Blanksby and Montgomery [1] and by a slight refinement of a theorem of Cassels [3] (see p. 379 of the present paper)

$$\overline{|\beta|} \geqslant 1 + \begin{cases} \left(40|\boldsymbol{\Omega}|^2 \log|\boldsymbol{\Omega}|^* - 1\right)^{-1} & \text{always}, \\ \left(5|\boldsymbol{\Omega}| - 1\right)^{-1} & \text{if } \alpha \text{ is not conjugate to } \alpha^{-1}. \end{cases}$$

Hence

$$\frac{1}{\log\overline{|\beta|}} \leqslant \begin{cases} 40|\boldsymbol{\Omega}|^2 \log|\boldsymbol{\Omega}|^* & \text{always}, \\ 5|\boldsymbol{\Omega}| & \text{if } \alpha \text{ is not conjugate to } \alpha^{-1}. \end{cases} \tag{5}$$

[The second inequality for $\boxed{\beta}$ and hence the second inequality for $1/\log\boxed{\beta}$ are not justified,
c the inequality (1) is nevertheless true, see the paper D6.] On the other hand $\boxed{\alpha}$ does not exceed the maximal absolute value of the zeros of f and by the inequality of Carmichael–Masson (see [5], p. 125)

$$\boxed{\alpha} \leqslant \|f\|^{1/2},$$

hence

$$\log\boxed{\alpha} \leqslant \tfrac{1}{2}\log\|f\|. \tag{6}$$

The first part of the lemma follows now from (4), (5) and (6). Assume that α is not an integer and let a_0 be the leading coefficient of f. Since $f(\alpha) = 0$, $a_0\alpha$ is an integer. Therefore there exists a prime ideal $\mathfrak{p}$ of $\boldsymbol{\Omega}$ such that

$$-\operatorname{ord}_{\mathfrak{p}} a_0 \leqslant \operatorname{ord}_{\mathfrak{p}} \alpha < 0.$$

It follows from (3) that

$$\operatorname{ord}_{\mathfrak{p}} \alpha = e \operatorname{ord}_{\mathfrak{p}} \beta$$

and

$$e \leqslant -\operatorname{ord}_{\mathfrak{p}} \alpha \leqslant \operatorname{ord}_{\mathfrak{p}} a_0.$$

On the other hand, taking norms N from $\boldsymbol{\Omega}$ to $\mathbb{Q}$ we get

$$N(\mathfrak{p})^{\operatorname{ord}_{\mathfrak{p}} a_0} \mid a_0^{|\boldsymbol{\Omega}|},$$

whence

$$e \leqslant \operatorname{ord}_{\mathfrak{p}} a_0 \leqslant |\boldsymbol{\Omega}|\,\frac{\log|a_0|}{\log 2} \leqslant |\boldsymbol{\Omega}|\,\frac{\log\|f\|}{2\log 2} < \frac{5}{2}\,|\boldsymbol{\Omega}|\log\|f\|,$$

which proves (1).

In order to prove (2), assume that

$$\alpha = \zeta_r \beta_1^{e_1}, \quad \beta_1 \in \boldsymbol{\Omega}_1, \quad e_1 = e(\alpha, \boldsymbol{\Omega}_1)$$

and take norms N_1 from $\boldsymbol{\Omega}_1$ to $\boldsymbol{\Omega}$. We get

$$a^d = N_1(\zeta_r) N_1(\beta_1)^{e_1}; \quad e_1 \leqslant e(\alpha^d, \boldsymbol{\Omega}),$$

where $d = |\boldsymbol{\Omega}_1|/|\boldsymbol{\Omega}|$. Since by Lemma 1 of [9]

$$e(\alpha^d, \boldsymbol{\Omega}) = d e(\alpha, \boldsymbol{\Omega})$$

(2) follows. □

Lemma 2. *If $\Phi(x)$ is any irreducible polynomial not dividing $x^\delta - x$ ($\delta \neq 1$), α is any of its zeros, $\boldsymbol{\Omega} = \mathbb{Q}(\alpha)$, n is an integer $\neq 0$,*

$$\nu = \big(n, 2^{e(\alpha,\boldsymbol{\Omega})-1} e(\alpha, \boldsymbol{\Omega})!\big),$$

then

$$\Phi(x^\nu) \overset{\text{can}}{=} \Phi_1(x) \cdots \Phi_r(x)$$

implies

$$J\Phi(x^n) \overset{\text{can}}{=} J\Phi_1(x^{n/\nu}) \cdots J\Phi_r(x^{n/\nu}).$$

Proof. The proof for $n > 0$ does not differ from the proof of Theorem 1 of [9].

The case $n < 0$ can be reduced to the former in view of the identity $J\Phi(x^n) = \Psi(x^{-n})$, where $\Psi(x) = J\Phi(x^{-1})$. □

Proof of Theorem 1. Let

$$KF(x) \overset{\text{can}}{=} \text{const} \prod_{i=1}^{\varrho} \Phi_i(x)^{\varepsilon_i}.$$

For each Φ_i we denote by α_i, $\boldsymbol{\Omega}_i$, ν_i the relevant parameters from Lemma 2 and set

$$\nu = \Big(n, \max_{1 \leqslant i \leqslant \varrho} 2^{e(\alpha_i, \boldsymbol{\Omega}_i)-1} e(\alpha_i, \boldsymbol{\Omega}_i)!\Big), \quad u = n\nu^{-1}.$$

We may assume that either $\|F\| \geqslant 5$ or $|F| \geqslant 3$, $\|F\| \geqslant 3$ because otherwise $s = 0$.

Since $2^{m-1}m! \leqslant m^m$ and $|\boldsymbol{\Omega}_i| \leqslant |F|$ $(i = 1, \ldots, \varrho)$ we get by Lemma 1

$$\begin{aligned} \nu &\leqslant \exp\big(20|F|^2 \log|F|^* \log\|F\|(\log 20|F|^2 + \log_2|F|^* + \log_2\|F\|)\big) \\ &\leqslant \exp\big(10|F| \log|F|^* \log\|F\|\big)^2, \end{aligned}$$

which proves (i). (ii) is clear. In order to prove (iii) we notice that

$$2^{m_1-1}m_1! \mid 2^{m_2-1}m_2!$$

for $m_1 \leqslant m_2$, thus $\nu_i \mid \nu$ for $i \leqslant \varrho$. By Lemma 2

$$\Phi_i(x^{\nu_i}) \overset{\text{can}}{=} \prod_{j=1}^{r_i} \Phi_{ij}(x)$$

implies

$$\Phi_i(x^{\nu}) \overset{\text{can}}{=} \prod_{j=1}^{r_i} \Phi_{ij}(x^{\nu/\nu_i}),$$

$$J\Phi_i(x^n) \overset{\text{can}}{=} \prod_{j=1}^{r_i} J\Phi_{ij}(x^{n/\nu_i}),$$

whence

$$KF(x^{\nu}) \overset{\text{can}}{=} \prod_{i=1}^{\varrho} \prod_{j=1}^{r_i} \Phi_{ij}(x^{\nu/\nu_i})^{\varepsilon_i},$$

$$KF(x^n) \overset{\text{can}}{=} \prod_{i=1}^{\varrho} \prod_{j=1}^{r_i} J\Phi_{ij}(x^{n/\nu_i})^{\varepsilon_i}.$$

Denoting the polynomials $\Phi_{ij}(x^{\nu/\nu_i})$ $(1 \leqslant i \leqslant \varrho,\ 1 \leqslant j \leqslant r_i)$ by $F_1, \ldots, F_s$ we obtain (iii). □

3.

Lemma 3. *Let $P(x_1, \ldots, x_{k+1}) \neq 0$, $Q(x_1, \ldots, x_{k+1}) \neq 0$ be polynomials with complex coefficients, $(P, Q) = G$ and $P = GT$, $Q = GU$. The resultant of T, U with respect to x_i divides a certain nonvanishing minor of Sylvester's matrix $\boldsymbol{R}$ of P, Q formed with respect to x_i ($|\boldsymbol{R}|$ being the resultant of P, Q).*

Proof. Consider polynomials $A(x), B(x), C(x)$ of degrees $|A| > 0$, $|B| > 0$, $|C|$ with indeterminate coefficients $a_0, \ldots, b_0, \ldots, c_0, \ldots$, the resultant D of A, B and any minor S of order $|A| + |B| + |C|$ of Sylvester's matrix $\boldsymbol{R}$ of AC, BC. Since D is absolutely irreducible and prime to $a_0 b_0$ (see [6], Satz 120), we have either $S = DV$, where V is a polynomial in the coefficients of A, B, C, or there exist complex values of the coefficients such that $D = 0$ and $a_0 b_0 c_0 S \neq 0$ (cf. [6], Satz 136). $A(x)$ and $B(x)$ with these coefficients have a common factor of degree $> |C|$ and by a well known theorem ([6], Satz 114) the rank of $\boldsymbol{R}$ is less than $|A| + |B| + |C|$. The contradiction obtained with $S \neq 0$ proves that

$$S = DV \tag{7}$$

for any minor S of order $|A| + |B| + |C|$ of $\boldsymbol{R}$.

Now, if neither T nor U is constant with respect to x_i we set $A(x_i) = T(x_1, \ldots, x_{k+1})$, $B(x_i) = U(x_1, \ldots, x_{k+1})$, $C(x_i) = G(x_1, \ldots, x_{k+1})$.

Since $(AC, BC) = C$, it follows from the quoted theorem that at least one of the minors of order $|A| + |B| + |C|$ of $\boldsymbol{R}$ does not vanish. By (7) this minor has the property asserted in the lemma.

If T, say, is constant with respect to x_i and the relevant degree of U is u, the principal minor S of order u has the said property (if $u = 0$ we take $S = 1$). □

Lemma 4. *Let $T(x_1, x_2), U(x_1, x_2)$ be polynomials with complex coefficients, $(T, U) = 1$. The number of pairs $\langle \eta, \vartheta \rangle$ such that $T(\eta, \vartheta) = U(\eta, \vartheta) = 0$ does not exceed the degree of the resultant of T, U with respect to x_i $(i = 1, 2)$.*

Remark. The lemma must be notorious but it is not readily found in the literature.

Proof. It suffices to consider $i = 2$. Let t, u be the degrees of T, U with respect to x_2 and for a given η let t_η, u_η be the degrees of $T(\eta, x_2), U(\eta, x_2)$. Let $\boldsymbol{R}(x_1)$ be Sylvester's matrix of T, U formed with respect to x_2, $R(x_1)$ its determinant and $\boldsymbol{R}_\eta$ Sylvester's matrix of $T(\eta, x_2), U(\eta, x_2)$.

If $t_\eta = t$, $u_\eta = u$ then $\boldsymbol{R}_\eta = \boldsymbol{R}(\eta)$, otherwise $\boldsymbol{R}_\eta$ can be obtained from $\boldsymbol{R}(\eta)$ by crossing out step by step row i, column i $(1 \leqslant i \leqslant u - u_\eta)$, row $u + i$, column i $(u - u_\eta < i \leqslant (u - u_\eta) + (t - t_\eta))$. At each step all non-zero elements crossed out are in a row, thus the rank diminishes by at most one. We get

$$\text{rank of } \boldsymbol{R}_\eta \geqslant \text{rank of } \boldsymbol{R}(\eta) - (t - t_\eta) - (u - u_\eta).$$

Now if there are k_η different ϑ such that $T(\eta, \vartheta) = U(\eta, \vartheta) = 0$, $T(\eta, x_2)$, $U(\eta, x_2)$ have a common factor of degree at least k_η, thus ([6], Satz 114)

$$\text{rank of } \boldsymbol{R}_\eta \leqslant t_\eta + u_\eta - k_\eta.$$

It follows that the rank of $\boldsymbol{R}(\eta)$ does not exceed $t + u - k_\eta$, whence by differentiation

$$(x_1 - \eta)^{k_\eta} \mid R(x_1).$$

Giving η all the possible values, we obtain

$$\sum k_\eta \leqslant |R|. \qquad \square$$

Lemma 5. *Let $P(x_1, \ldots, x_{k+1}) \neq 0$, $Q(x_1, \ldots, x_{k+1}) \neq 0$ be polynomials and $S \neq 0$ a minor of their Sylvester's matrix formed with respect to x_i $(1 \leqslant i \leqslant k+1)$. The following inequalities hold*

$$|S| \leqslant 2|P|\,|Q|,$$
$$\|S\| \leqslant \|P\|^{2|Q|} \|Q\|^{2|P|}.$$

Proof. We assume without loss of generality $i = k + 1$ and set

$$P = \sum_{i=0}^{m} P_i(x_1, \ldots, x_k) x_{k+1}^{m-i}, \qquad Q = \sum_{j=0}^{n} Q_j(x_1, \ldots, x_k) x_{k+1}^{n-j}.$$

Since $m \leqslant |P|$, $n \leqslant |Q|$ and Sylvester's matrix of P, Q is

$$\left.\begin{array}{l} \left[\begin{array}{cccccc} P_0 & P_1 & \ldots & P_m & & \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ & & P_0 & P_1 & \ldots & P_m \\ Q_0 & Q_1 & \ldots & Q_n & & \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ & & Q_0 & Q_1 & \ldots & Q_n \end{array}\right] \end{array}\right\} \begin{array}{l} \left.\begin{array}{l} \\ \\ \end{array}\right\} n \text{ times} \\ \left.\begin{array}{l} \\ \\ \end{array}\right\} m \text{ times} \end{array}$$

it follows that

$$|S| \leqslant n \max |P_i| + m \max |Q_j| \leqslant 2|P|\,|Q|.$$

In order to estimate $\|S\|$ we note that

$$\|S\| = (2\pi)^{-k} \int_0^{2\pi} \cdots \int_0^{2\pi} \left|S(e^{i\varphi_1}, \ldots, e^{i\varphi_k})\right|^2 d\varphi_1\, d\varphi_2 \ldots d\varphi_k$$

(cf. [2], Lemma 6 of Chapter VIII), hence

$$\|S\| \leqslant \max_{0 \leqslant \varphi \leqslant 2\pi} \left|S(e^{i\varphi_1}, \ldots, e^{i\varphi_k})\right|^2. \tag{8}$$

On the other hand, for any polynomial R with integral coefficients

$$\max_{0 \leqslant \varphi \leqslant 2\pi} \left|R(e^{i\varphi_1}, \ldots, e^{i\varphi_k})\right|^2 \leqslant \|R\|^2. \tag{9}$$

Using (8), Hadamard's inequality and (9) we obtain

$$\begin{aligned}\|S\| &\leqslant \max_{0\leqslant\varphi\leqslant 2\pi}\left(\sum_{j=0}^{m}\left|P_j(e^{i\varphi_1},\dots,e^{i\varphi_k})\right|^2\right)^n\left(\sum_{j=0}^{n}\left|Q_j(e^{i\varphi_1},\dots,e^{i\varphi_k})\right|^2\right)^m\\ &\leqslant \left(\sum_{j=0}^{m}\max_{0\leqslant\varphi\leqslant 2\pi}\left|P_j(e^{i\varphi_1},\dots,e^{i\varphi_k})\right|^2\right)^n\left(\sum_{j=0}^{n}\max_{0\leqslant\varphi\leqslant 2\pi}\left|Q_j(e^{i\varphi_1},\dots,e^{i\varphi_k})\right|^2\right)^m\\ &\leqslant \left(\sum_{j=0}^{m}\|P_j\|^2\right)^n\left(\sum_{j=0}^{n}\|Q_j\|^2\right)^m \leqslant \left(\sum_{j=0}^{m}\|P_j\|\right)^{2n}\left(\sum_{j=0}^{n}\|Q_j\|\right)^{2m}\\ &\leqslant \|P\|^{2|Q|}\|Q\|^{2|P|}.\end{aligned}$$

□

Lemma 6. *If an m-dimensional sublattice of the n-dimensional integral lattice contains m linearly independent vectors $\boldsymbol{v}_1,\dots,\boldsymbol{v}_m$ then it has a basis of the form*

$$\sum_{j=1}^{m}c_{1j}\boldsymbol{v}_j,\dots,\sum_{j=1}^{m}c_{mj}\boldsymbol{v}_j,$$

where

$$0\leqslant c_{ij}<c_{jj}\leqslant 1\ (i\neq j),\quad c_{ij}=0\ (i<j).$$

Proof. The proof is obtained by a standard method (see [2], Appendix A). For a more precise result see [7]. □

Lemma 7. *Let k_i $(0\leqslant i\leqslant l)$ be an increasing sequence of integers. Let $k_{j_p}-k_{i_p}$ $(1\leqslant p\leqslant p_0)$ be all the numbers which appear only once in the double sequence k_j-k_i $(0\leqslant i\leqslant j\leqslant l)$. Suppose that for each p*

$$k_{j_p}-k_{i_p}=\sum_{q=1}^{k}c_{pq}n_q,$$

where c_{pq} are integers, $|c_{pq}|\leqslant c$, c positive integer. Then either there exist integral matrices

$$\boldsymbol{K}=[\kappa_{qi}]_{\substack{q\leqslant k\\ i\leqslant l}}\quad\text{and}\quad\boldsymbol{\Lambda}=[\lambda_{qt}]_{\substack{q\leqslant k\\ t\leqslant k}}$$

and an integral vector $\boldsymbol{u}$ such that

$$[k_1-k_0,\dots,k_l-k_0]=\boldsymbol{u}\boldsymbol{K},\quad\boldsymbol{n}=[n_1,\dots,n_k]=\boldsymbol{u}\boldsymbol{\Lambda},\tag{10}$$

$$h(\boldsymbol{K})\leqslant k\big(\max\{c^2,2\}+2\big)^{l/2},$$

$$0\leqslant\lambda_{qt}<\lambda_{tt}\leqslant 2^{l-1}\ (q\neq t),\quad\lambda_{qt}=0\ (q<t)\tag{11}$$

or there exists an integral vector $\boldsymbol{\gamma}$ such that

$$\boldsymbol{\gamma}\boldsymbol{n}=0\quad\text{and}\quad 0<h(\boldsymbol{\gamma})\leqslant k^{k-1}\big(\max\{kc^2,2\}+2k\big)^{(l+1)(k-1)/2}.$$

Proof. By the assumption for each pair $\langle i, j\rangle$ where $0 \leqslant i \leqslant j \leqslant l$ and $\langle i, j\rangle \neq \langle i_p, j_p\rangle$ $(1 \leqslant p \leqslant p_0)$ there exists a pair $\langle g_{ij}, h_{ij}\rangle \neq \langle i, j\rangle$ such that

$$k_j - k_i = k_{h_{ij}} - k_{g_{ij}}.$$

Let us consider the system of linear homogeneous equations

$$\begin{aligned} x_0 &= 0, \\ x_j - x_i - x_{h_{ij}} + x_{g_{ij}} &= 0, \qquad \langle i, j\rangle \neq \langle i_1, j_1\rangle, \ldots, \langle i_{p_0}, j_{p_0}\rangle, \\ x_{j_p} - x_{i_p} - \sum_{q=1}^{k} c_{pq} y_q &= 0 \qquad (1 \leqslant p \leqslant p_0) \end{aligned} \tag{12}$$

satisfied by $x_i = k_i - k_0$ $(0 \leqslant i \leqslant l)$, $y_q = n_q$ $(1 \leqslant q \leqslant k)$.

Let $\boldsymbol{A}$ be the matrix of the system obtained from (12) by cancelling the first equation and substituting $x_0 = 0$ in the others, $\boldsymbol{B}$ be the matrix of the coefficients of the x's, $-\boldsymbol{\Gamma}$ the matrix of the coefficients of the y's so that $\boldsymbol{A} = \boldsymbol{B} \mid -\boldsymbol{\Gamma}$ in the sense of juxtaposition (the vertical line is added in order to avoid a confusion with the subtraction).

We assert that (12) has at most k linearly independent solutions. Indeed, if we had $k+1$ such solutions $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{k+1}$ then taking as $\xi_1, \ldots, \xi_{k+1}$ real numbers rationally independent we should find a set of reals $\sum_{m=1}^{k+1} a_{mi}\xi_m$ $(0 \leqslant i \leqslant l)$, where all the differences would span over the rationals a space of dimension $k+1$, while the differences occurring only once

$$\sum_{m=1}^{k+1}(a_{mj_p} - a_{mi_p})\xi_m = \sum_{m=1}^{k+1} \xi_m \sum_{q=1}^{k} c_{pq} a_{m,l+q} = \sum_{q=1}^{k} c_{pq}\Big(\sum_{m=1}^{k+1} a_{m,l+q}\xi_m\Big)$$

would span a space of dimension at most k contrary to the theorem of Straus [11].

It follows that the rank of $\boldsymbol{A}$ is $l + \varrho$, where $0 \leqslant \varrho < k$. If the rank of $\boldsymbol{B}$ is l then since one row of $\boldsymbol{B}$ (corresponding to $\langle i, j\rangle = \langle 0, l\rangle$) is $[0, \ldots, 0, 1]$ there exists a nonsingular submatrix $\boldsymbol{\Delta}$ of $\boldsymbol{B}$ of order l containing this row. Solving the system by means of Cramer formulae we find a system of k linearly independent integral solutions which can be written (horizontally) in the form $\boldsymbol{K}' \mid \boldsymbol{\Lambda}'$, where elements of $\boldsymbol{K}'$ are determinants obtained from $\boldsymbol{\Delta}$ by replacing one column by a column of $\boldsymbol{\Gamma}$ and $\boldsymbol{\Lambda}' = D\boldsymbol{I}_k$, $D = |\boldsymbol{\Delta}|$, $\boldsymbol{I}_k$ is the identity matrix of order k.

By Hadamard's inequality and an inequality for determinants with real entries (see this collection, paper M4)

$$|D| \leqslant 2^{l-1}, \quad h(\boldsymbol{K}') \leqslant \min\{\big(\max\{c^2, 4\} + 2\big)^{l/2}, (c+1)^l\} \leqslant \big(\max\{c^2, 2\} + 2\big)^{l/2}.$$

From $\boldsymbol{K}' \mid \boldsymbol{\Lambda}'$ we obtain by Lemma 6 a fundamental system of integral solutions $\boldsymbol{K} \mid \boldsymbol{\Lambda}$ satisfying (11). Since the system is fundamental there exists an integral vector $\boldsymbol{u}$ satisfying (10).

If the rank of $\boldsymbol{B}$ is less than l, we find a system of $k - \varrho$ linearly independent integral solutions in the form $\boldsymbol{K}' \mid \boldsymbol{\Lambda}'$, where elements of $\boldsymbol{\Lambda}'$ are up to a sign minors of $\boldsymbol{A}$ of order

$l+\varrho$. The rank of $\boldsymbol{\Lambda}'$ is less than k, otherwise the equality $\boldsymbol{B}\boldsymbol{K}'^{T} = \boldsymbol{\Gamma}\boldsymbol{\Lambda}'^{T}$ would imply

$$\boldsymbol{\Gamma} = \boldsymbol{B}\boldsymbol{K}'^{T}(\boldsymbol{\Lambda}'^{T})^{-1}, \quad \boldsymbol{A} = \boldsymbol{B}\,|\,-\boldsymbol{\Gamma} = \boldsymbol{B}\big(\boldsymbol{I}_l\,|\,-\boldsymbol{K}'^{T}(\boldsymbol{\Lambda}'^{T})^{-1}\big)$$

and the rank of $\boldsymbol{A}$ would be less than l, which is impossible. By Hadamard's inequality
c and the inequality for determinants with real entries quoted above

c $$h(\boldsymbol{\Lambda}') \leqslant \min\{\big(\max\{kc^2, 4\}+2\big)^{(l+\varrho)/2}, (kc+1)^{l+\varrho}\} \leqslant \big(\max\{kc^2, 2\}+2k\big)^{(l+\varrho)/2}.$$

By a well known lemma ([2], Lemma 3 of Chapter VI) there exists an integral vector $\boldsymbol{\gamma} \neq \boldsymbol{0}$ such that $\boldsymbol{\Lambda}'\boldsymbol{\gamma}^T = \boldsymbol{0}$ and

c $$h(\boldsymbol{\gamma}) \leqslant \big[h(\boldsymbol{\Lambda}')k\big]^{(k-\max\{\varrho,1\})/\max\{\varrho,1\}} \leqslant k^{k-1}\big(\max\{kc^2, 2\}+2k\big)^{(l+1)(k-1)/2}.$$

Since $\boldsymbol{n} = \boldsymbol{u}'\boldsymbol{\Lambda}'$ ($\boldsymbol{u}'$ not necessarily integral) we get

$$\boldsymbol{\gamma}\boldsymbol{n} = \boldsymbol{n}\boldsymbol{\gamma}^T = \boldsymbol{u}'\boldsymbol{\Lambda}'\boldsymbol{\gamma}^T = 0. \qquad \square$$

Remark. The proof of Straus can be transformed into a proof that (12) has at most k linearly independent solutions, which does not use any irrationalities and is in this respect nearer to the proof of Lemma 4 in [9].

Suppose that $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{k+1}$ are solutions,

$$\boldsymbol{a}_m = [0, a_{m1}, \ldots, a_{ml}, a_{m,l+1}, \ldots, a_{m,l+k}].$$

There exist integers $b_1, \ldots, b_{k+1}$ not all zero such that

$$\sum_{m=1}^{k+1} b_m a_{m,l+q} = 0 \quad (1 \leqslant q \leqslant k).$$

Consider a vector $\boldsymbol{a} = \sum_{m=1}^{k+1} b_m \boldsymbol{a}_m = [0, a_1, \ldots, a_l, 0, \ldots, 0]$. It is also a solution of (12). Set

i' = the least i such that $a_i = \min_{0\leqslant j\leqslant l} a_j$ or $\max_{0\leqslant j\leqslant l} a_j$,

j' = the greatest i such that $a_i = \min_{0\leqslant j\leqslant l} a_j + \max_{0\leqslant j\leqslant l} a_j - a_{i'}$.

The equality $a_{j'} - a_{i'} = a_h - a_g$ implies $a_{i'} = a_g$, $a_{j'} = a_h$, $i' \leqslant g$, $j' \geqslant h$ and either $\langle i', j'\rangle = \langle g, h\rangle$ or $k_{j'} - k_{i'} > k_h - k_g$. It follows that $\langle i', j'\rangle$ is identical with some $\langle i_p, j_p\rangle$ ($1 \leqslant p \leqslant p_0$) and we get

$$a_{j'} - a_{i'} = \sum_{q=1}^{k} c_{pq} a_{l+q} = 0.$$

Hence $a_i = 0$ ($0 \leqslant i \leqslant l+k$) and

$$\sum_{m=1}^{k+1} b_m \boldsymbol{a}_m = \boldsymbol{0}.$$

Lemma 8 (L8$_k$). *Let $P(x_1, \dots, x_k) \neq 0$, $Q(x_1, \dots, x_k) \neq 0$ be polynomials and $(P, Q) = G$. For any integral vector $\boldsymbol{n} = [n_1, \dots, n_k]$ we have either*

$$\big(LP(x^{n_1}, \dots, x^{n_k}), LQ(x^{n_1}, \dots, x^{n_k})\big) = LG(x^{n_1}, \dots, x^{n_k})$$

or $|P|\,|Q| > 0$ and there exists an integral vector $\boldsymbol{\beta}$ such that

$$\boldsymbol{\beta n} = 0, \tag{13}$$

$$0 < h(\boldsymbol{\beta}) < \begin{cases} 5|P|\,|Q| \log \|P\|^{2|Q|} \|Q\|^{2|P|} & \text{if } k = 2, \\ \exp_{2k-5}\big(2\|P\|^{2|Q|}\|Q\|^{2|P|} \log 5|P|\,|Q| + \log 7k\big) & \text{if } k > 2. \end{cases} \tag{14}$$

Lemma 9 (L9$_k$). *For any polynomial $F(x_1, \dots, x_k) \neq 0$, any integral vector $\boldsymbol{n} = [n_1, \dots, n_k]$ and any irreducible factor $f(x)$ of $LF(x^{n_1}, \dots, x^{n_k})$ either there exist an integral matrix $\boldsymbol{\Lambda} = [\lambda_{qt}]$ of degree k, an integral vector $\boldsymbol{u} = [u_1, \dots, u_k]$ and a polynomial $T(z_1, \dots, z_k)$ such that*

$$0 \leqslant \lambda_{qt} < \lambda_{tt} \leqslant 2^{\|F\|-2} \ (q \neq t), \quad \lambda_{qt} = 0 \ (q < t), \tag{15}$$

$$\boldsymbol{n} = \boldsymbol{u\Lambda}, \tag{16}$$

$$T(z_1, \dots, z_k) \mid F\Big(\prod_{q=1}^{k} z_q^{\lambda_{q1}}, \dots, \prod_{q=1}^{k} z_q^{\lambda_{qk}}\Big),$$

$$f(x) = \text{const}\, LT(x^{u_1}, \dots, x^{u_k})$$

or $\|F\| \geqslant 3$ and there exists an integral vector $\boldsymbol{\gamma}$ such that

$$\boldsymbol{\gamma n} = 0, \tag{17}$$

$$0 < h(\boldsymbol{\gamma}) < \begin{cases} 120\big(2|F|^*\big)^{2\|F\|-1} \log \|F\| & \text{if } k = 2, \\ \exp_{2k-4}\big(7k|F|^{*\|F\|-1} \log \|F\|\big) & \text{if } k > 2. \end{cases}$$

We prove these lemmata by induction showing first L8$_2$ and then the implications L8$_k$ $\to$ L9$_k$ ($k \geqslant 1$), L9$_k$ $\to$ L8$_{k+1}$ ($k > 1$). Since L8$_1$ is obvious this argumentation is sufficient.

Proof of L8$_2$. If $P = GT$, $Q = GU$ and

$$\big(LP(x^{n_1}, x^{n_2}), LQ(x^{n_1}, x^{n_2})\big) \neq LG(x^{n_1}, x^{n_2})$$

then for some ξ not conjugate to ξ^{-1}: $T(\xi^{n_1}, \xi^{n_2}) = 0 = U(\xi^{n_1}, \xi^{n_2})$. Let R_i be the resultant of $T(x_1, x_2)$, $U(x_1, x_2)$ with respect to x_i and S_i a nonvanishing minor of Sylvester's matrix of P, Q, divisible by R_i, whose existence is asserted in Lemma 3. Set

$$\alpha_i = \xi^{n_i}, \quad \boldsymbol{\Omega} = \mathbb{Q}(\alpha_1, \alpha_2). \tag{18}$$

$|\boldsymbol{\Omega}|$ does not exceed the number of distinct pairs $\langle \eta, \vartheta \rangle$ satisfying $T(\eta, \vartheta) = U(\eta, \vartheta) = 0$ thus by Lemma 4

$$|\boldsymbol{\Omega}| \leqslant |R_i| \leqslant |S_i| \quad (i = 1, 2).$$

Since $\xi^{(n_1,n_2)} \in \boldsymbol{\Omega}$, it follows

$$|\mathbb{Q}(\xi)| \leqslant (n_1, n_2)|\boldsymbol{\Omega}|.$$

Moreover $R_{3-i}(\alpha_i) = 0$, $S_{3-i}(\alpha_i) = 0$ and if α_i is not an integer or $n_i = 0$ we get from (18) and Lemma 1

$$(19)\quad |n_i| \leqslant e\big(\alpha_i, \mathbb{Q}(\xi)\big) \leqslant (2\log 2)^{-1}|\mathbb{Q}(\xi)| \log \|S_{3-i}\| \leqslant (2\log 2)^{-1}(n_1, n_2)|S_i| \log \|S_{3-i}\|.$$

If α_i is an integer and $n_i \neq 0$, $\xi^{\operatorname{sgn} n_i}$ is also an integer. It is not conjugate to $\xi^{-\operatorname{sgn} n_i}$, thus by the already quoted refinement of Theorem 1 of [3]

$$\boxed{\xi^{\operatorname{sgn} n_i}} > 1 + \frac{1}{5|\mathbb{Q}(\xi)| - 1}; \quad \frac{1}{\log \boxed{\xi^{\operatorname{sgn} n_i}}} < 5|\mathbb{Q}(\xi)|.$$

On the other hand, by the inequality of Carmichael–Masson

$$\boxed{\alpha_i} \leqslant \|S_{3-i}\|^{1/2}; \quad \log \boxed{\alpha_i} \leqslant \tfrac{1}{2} \log \|S_{3-i}\|.$$

It follows from (18) that

$$|n_i| = \frac{\log \boxed{\alpha_i}}{\log \boxed{\xi^{\operatorname{sgn} n_i}}} < \frac{5}{2} |\mathbb{Q}(\xi)| \log \|S_{3-i}\| \leqslant \frac{5}{2} (n_1, n_2)|S_i| \log \|S_{3-i}\|.$$

In view of Lemma 5 this inequality together with (19) implies $\mathrm{L8}_2$ on taking $\boldsymbol{\beta} = \left[\frac{n_2}{(n_1, n_2)}, \frac{-n_1}{(n_1, n_2)}\right]$. □

Proof of the implication $\mathrm{L8}_k \to \mathrm{L9}_k$. Let

$$F(x_1, \ldots, x_k) = \sum_{i=0}^{I} a_i x_1^{\alpha_{i1}} \cdots x_k^{\alpha_{ik}}$$

where a_i are integers $\neq 0$ and the vectors $\boldsymbol{\alpha}_i$ are all different. Let further

$$JF(x^{n_1}, \ldots, x^{n_k}) = f(x)g(x)$$

where f and g have integral coefficients (if necessary we may change $f(x)$ by a constant factor without impairing the assertion of the lemma). We set

$$f(x^{-1})g(x) = \sum_{i=0}^{l} c_i x^{k_i} \quad (c_i \text{ integers} \neq 0,\ k_0 < k_1 < \ldots < k_l)$$

and consider two expressions for $F(x^{n_1}, \ldots, x^{n_k})F(x^{-n_1}, \ldots, x^{-n_k})$:

$$F(x^{n_1}, \ldots, x^{n_k})F(x^{-n_1}, \ldots, x^{-n_k}) = \sum_{i=0}^{I} a_i^2 + \sum_{\substack{0 \leqslant i, j \leqslant I \\ i \neq j}} a_i a_j x^{\boldsymbol{n}\boldsymbol{\alpha}_j - \boldsymbol{n}\boldsymbol{\alpha}_i},$$

$$\big(f(x^{-1})g(x)\big)\big(f(x)g(x^{-1})\big) = \sum_{i=0}^{l} c_i^2 + \sum_{\substack{0 \leqslant i, j \leqslant l \\ i \neq j}} c_i c_j x^{k_j - k_i}.$$

If for any pair $\langle i, j\rangle$

$$i \neq j \quad \text{and} \quad \boldsymbol{n}\boldsymbol{\alpha}_j - \boldsymbol{n}\boldsymbol{\alpha}_i = 0 \tag{20}$$

we have (17) with $h(\boldsymbol{\gamma}) \leqslant |F|$.

If no pair $\langle i, j\rangle$ satisfies (20), it follows that $F(x^{n_1}, \dots, x^{n_k}) \neq 0$

$$\sum_{i=0}^{l} c_i^2 = \sum_{i=0}^{I} a_i^2 = \|F\|, \quad l \leqslant \|F\| - 1, \tag{21}$$

each number $k_j - k_i$ which appears only once in the double sequence $k_j - k_i$ $(0 \leqslant i \leqslant j \leqslant l)$ has a value $\sum_{q=1}^{k} n_q d_q$ with $|d_q| \leqslant |F|$.

Applying Lemma 7 with $c = |F|$ we find either integral matrices $\boldsymbol{K} = [\kappa_{qt}]$, $\boldsymbol{\Lambda} = [\lambda_{qt}]$ and an integral vector $\boldsymbol{u}$ satisfying (15), (16) and

$$k_i - k_0 = \sum_{q=1}^{k} \kappa_{qi} u_q, \quad h(\boldsymbol{K}) < k|F|^{*\|F\|-1}$$

or an integral vector satisfying (17) with

$$h(\boldsymbol{\gamma}) < k^{k-1}\big(k|F|^{*2}\big)^{\|F\|(k-1)/2} < \begin{cases} 120\big(2|F|^*\big)^{2\|F\|-1} \log \|F\| & \text{if } k = 2, \\ \exp_{2k-4}\big(7k|F|^{*\|F\|-1} \log \|F\|\big) & \text{if } k > 2. \end{cases}$$

We notice that $\|F\| \geqslant 3$ since otherwise $LF(x^{n_1}, \dots, x^{n_k}) = \text{const}$. Set

$$P(z_1, \dots, z_k) = \sum_{i=0}^{I} a_i \prod_{q=1}^{k} z_q^{\sum_{t=1}^{k} \lambda_{qt}\alpha_{it}},$$

$$Q(z_1, \dots, z_k) = J \sum_{i=0}^{l} c_i \prod_{q=1}^{k} z_q^{\kappa_{qi}}.$$

Clearly

$$|P| \leqslant k|F|2^{\|F\|-2}, \quad |Q| \leqslant 2k|F|^{*\|F\|-1},$$

whence

$$|P| + |Q| \leqslant 3k|F|^{*\|F\|-1}, \quad |P|\,|Q| \leqslant k^2 2^{\|F\|-1}|F|^{*\|F\|}. \tag{22}$$

The vectors $[\kappa_{1i}, \dots, \kappa_{ki}]$ $(0 \leqslant i \leqslant l)$ are all different since such are the numbers $k_i - k_0$. Similarly, by (16) the vectors $\big[\sum_{t=1}^{n} \lambda_{1t}\alpha_{it}, \dots, \sum_{t=1}^{n} \lambda_{kt}\alpha_{it}\big]$ $(0 \leqslant i \leqslant l)$ are all different since such are the numbers $\sum_{t=1}^{k} \alpha_{it} n_t$. Therefore, by (21)

$$\|P\| = \|Q\| = \|F\|. \tag{23}$$

We get from $\mathrm{L8}_k$ that either

$$\big(LP(x^{u_1},\dots,x^{u_k}),\,LQ(x^{u_1},\dots,x^{u_k})\big) = LG(x^{u_1},\dots,x^{u_k})$$

or $\boldsymbol{\beta u} = 0$ with $\boldsymbol{\beta}$ satisfying (14).

In the former case

$$\begin{aligned} Lg(x) &= \operatorname{const}\big(LF(x^{n_1},\dots,x^{n_k}),\,Lf(x^{-1})g(x)\big)\\ &= \operatorname{const}\big(LP(x^{u_1},\dots,x^{u_k}),\,LQ(x^{u_1},\dots,x^{u_k})\big)\\ &= \operatorname{const} LG(x^{u_1},\dots,x^{u_k}),\end{aligned}$$

$$f(x) = \frac{LF(x^{n_1},\dots,x^{n_k})}{Lg(x)} = \frac{LP(x^{u_1},\dots,x^{u_k})}{\operatorname{const} LG(x^{u_1},\dots,x^{u_k})} = \operatorname{const} LT(x^{u_1},\dots,x^{u_k}),$$

where $T = PG^{-1}$.

In the latter case we have $k \geqslant 2$,

$$\boldsymbol{\gamma n} = 0 \quad \text{with} \quad \boldsymbol{\gamma} = \boldsymbol{\beta}\boldsymbol{\Lambda}^A,$$
$$h(\boldsymbol{\gamma}) \leqslant kh(\boldsymbol{\beta})h(\boldsymbol{\Lambda}^A) \leqslant k(k-1)^{(k-1)/2}h(\boldsymbol{\Lambda})^{k-1}h(\boldsymbol{\beta})$$

and we estimate $h(\boldsymbol{\gamma})$ separately for $k = 2$ and for $k > 2$, using (14), (15), (22), (23) and $|F|^* \geqslant 2$, $\|F\| \geqslant 3$.

For $k = 2$ we obtain

$$\begin{aligned} h(\boldsymbol{\gamma}) &\leqslant 2h(\boldsymbol{\Lambda}) \cdot 5|P|\,|Q| \log \|P\|^{2|Q|}\|Q\|^{2|P|}\\ &\leqslant 5 \cdot 2^{\|F\|-1} \cdot 2^{\|F\|+1}|F|^{*\|F\|} \cdot 12|F|^{*\|F\|-1} \log\|F\|\\ &\leqslant 120\big(2|F|^*\big)^{2\|F\|-1} \log\|F\|.\end{aligned}$$

For $k > 2$ we use the inequality

$$k(k-1)^{(k-1)/2}h(\boldsymbol{\Lambda})^{k-1} < k^{k-1}2^{(k-1)(\|F\|-2)} < \exp_{2k-4}\big(6k|F|^{*\|F\|-1}\log\|F\|\big)$$

and obtain

$$\begin{aligned} h(\boldsymbol{\gamma}) &\leqslant k(k-1)^{(k-1)/2}h(\boldsymbol{\Lambda})^{k-1}\\ &\qquad \times \exp_{2k-4}\big(6k|F|^{*\|F\|-1}\log\|F\| + \log\log 5k^2 2^{\|F\|-1}|F|^{*\|F\|} + \log 3\big)\\ &\leqslant \exp^2_{2k-4}\big(6k|F|^{*\|F\|-1}\log\|F\| + \log\tfrac{5}{2}k^2 + \|F\|\log 2|F|^* + \log 3 - 1\big)\\ &< \exp_{2k-4}\big(7k|F|^{*\|F\|-1}\log\|F\|\big).\end{aligned}$$

□

Proof of the implication $\mathrm{L9}_k \to \mathrm{L8}_{k+1}$ $(k > 1)$. Let $P = GT$, $Q = GU$, let R_j be the resultant of T, U with respect to x_j and let S_j be a nonvanishing minor of Sylvester's matrix of P, Q divisible by R_j, whose existence is asserted in Lemma 3.

If

$$\big(LP(x^{n_1},\dots,x^{n_{k+1}}),\,LQ(x^{n_1},\dots,x^{n_{k+1}})\big) \neq LG(x^{n_1},\dots,x^{n_{k+1}})$$

then $|P|\,|Q| > 0$ and there exists an irreducible polynomial $f(x)$ such that

$$f(x) \mid \big(LT(x^{n_1},\dots,x^{n_{k+1}}),\,LU(x^{n_1},\dots,x^{n_{k+1}})\big).$$

Clearly for each $j \leqslant k+1$

$$f(x) \mid R_j(x^{n_1}, \dots, x^{n_{k+1}}) \mid S_j(x^{n_1}, \dots, x^{n_{k+1}}),$$

where x^{n_j} does not occur among the arguments of R_j and S_j. By L9$_k$ either there exist an integral nonsingular triangular matrix $\boldsymbol{\Lambda}_j$ with nonnegative entries, an integral vector $\boldsymbol{u}_j$ and a polynomial T_j such that

$$h(\boldsymbol{\Lambda}_j) \leqslant 2^{\|S_j\|-2}, \tag{24}$$

$$[n_1, \dots, n_{j-1}, n_{j+1}, \dots, n_{k+1}] = \boldsymbol{\Lambda}_j \boldsymbol{u}_j, \tag{25}$$

$$T_j \mid S_j\Big(\prod_{q=1}^{k} z_q^{\lambda_{q1}}, \dots, \prod_{q=1}^{k} z_q^{\lambda_{qk}}\Big), \quad f(x) = \operatorname{const} T_j(x^{u_{j1}}, \dots, x^{u_{jk}}) \tag{26}$$

or

$$\boldsymbol{\gamma}_j[n_1, \dots, n_{j-1}, n_{j+1}, \dots, n_{k+1}] = 0$$

with

$$0 < h(\boldsymbol{\gamma}_j) < \begin{cases} 120\big(2|S_j|^*\big)^{2\|S_j\|-1} \log \|S_j\| & \text{if } k = 2, \\ \exp_{2k-4}\big(7k|S_j|^{*\|S_j\|-1} \log \|S_j\|\big) & \text{if } k > 2. \end{cases}$$

In the latter case we have $\boldsymbol{\beta}\boldsymbol{n} = 0$, where

$$0 < h(\boldsymbol{\beta}) \leqslant \max_{1 \leqslant j \leqslant k+1} h(\boldsymbol{\gamma}_j).$$

If $k = 2$ we obtain from Lemma 5

$$\begin{aligned} h(\boldsymbol{\beta}) &\leqslant 120\big(2|S_j|^*\big)^{2\|S_j\|-1} \log \|S_j\| \\ &< \exp\big(\log(120 \log \|S_j\|) + (\|S_j\| - \tfrac{1}{2}) \log(16|P|^2|Q|^2 + 8)\big) \\ &< \exp\big(\log\log \|P\|^{2|Q|} \|Q\|^{2|P|} + \|P\|^{2|Q|} \|Q\|^{2|P|} \log\big(16|P|^2|Q|^2 + 8\big) + \log 5\big) \\ &< \exp\big(2\|P\|^{2|Q|} \|Q\|^{2|P|} \log 5|P|\,|Q| + \log 21\big). \end{aligned}$$

If $k > 2$ we have similarly

$$\begin{aligned} h(\boldsymbol{\beta}) &\leqslant \exp_{2k-4}\big(7k|S_j|^{*\|S_j\|-1} \log \|S_j\|\big) \\ &< \exp_{2k-3}\big(\tfrac{1}{2}\|S_j\| \log(4|P|^2|Q|^2 + 2) + \log\log \|S_j\| + \log 7k\big) \\ &< \exp_{2k-3}\big(\|P\|^{2|Q|} \|Q\|^{2|P|} \log 5|P|\,|Q| + \log 7k\big). \end{aligned}$$

In the former case we set $\boldsymbol{u}_{k+1} = \boldsymbol{v} = [v_1, \dots, v_k]$, find

$$\begin{aligned} f(x) &= \operatorname{const} LT_{k+1}(x^{v_1}, \dots, x^{v_k}), \\ Jf(x^{-1}) &= \operatorname{const} LT_{k+1}(x^{-v_1}, \dots, x^{-v_k}) \end{aligned}$$

and

$$\frac{Jf(x^{-1})}{f(x)} = \frac{LT_{k+1}(x^{-v_1}, \dots, x^{-v_k})}{LT_{k+1}(x^{v_1}, \dots, x^{v_k})} = \frac{JT_{k+1}(x^{-v_1}, \dots, x^{-v_k})}{JT_{k+1}(x^{v_1}, \dots, x^{v_k})}. \tag{27}$$

Let

$$T_{k+1}(z_1, \dots, z_k) = \sum_{i=0}^{I} a_i z_1^{\alpha_{i1}} z_2^{\alpha_{i2}} \cdots z_k^{\alpha_{ik}},$$

where $a_i \neq 0$ $(0 \leqslant i \leqslant I)$ and the vectors $\boldsymbol{\alpha}_i$ are all different. Since $S_{k+1} \neq 0$, $|\boldsymbol{\Lambda}_{k+1}| \neq 0$ we get by (26)

$$h(\boldsymbol{\alpha}_i) \leqslant k|S_{k+1}|h(\boldsymbol{\Lambda}_{k+1}) \quad (0 \leqslant i \leqslant I). \tag{28}$$

Let $\boldsymbol{\alpha}_i \boldsymbol{v}$ take its minimum for $i = m$, maximum for $i = M$. We have

$$\begin{aligned} JT_{k+1}(x^{v_1}, \dots, x^{v_k}) &= x^{-\boldsymbol{\alpha}_m \boldsymbol{v}} \sum_{i=0}^{I} a_i x^{\boldsymbol{\alpha}_i \boldsymbol{v}}, \\ JT_{k+1}(x^{-v_1}, \dots, x^{-v_k}) &= x^{\boldsymbol{\alpha}_M \boldsymbol{v}} \sum_{i=0}^{I} a_i x^{-\boldsymbol{\alpha}_i \boldsymbol{v}}. \end{aligned} \tag{29}$$

Since $Jf(x^{-1}) \neq \text{const } f(x)$ we get from (27)

$$d(x) = a_m JT_{k+1}(x^{-v_1}, \dots, x^{-v_k}) - a_M JT_{k+1}(x^{v_1}, \dots, x^{v_k}) \neq 0.$$

By (29) the lowest term in $d(x)$ is of the form $ax^{\boldsymbol{\gamma}\boldsymbol{v}}$, where $\boldsymbol{\gamma} = \boldsymbol{\alpha}_i - \boldsymbol{\alpha}_m$ or $\boldsymbol{\alpha}_M - \boldsymbol{\alpha}_i$ so that

$$a \neq 0; \quad \boldsymbol{\gamma}\boldsymbol{v} > 0 \tag{30}$$

and by (28)

$$h(\boldsymbol{\gamma}) \leqslant k|S_{k+1}|h(\boldsymbol{\Lambda}_{k+1}). \tag{31}$$

It follows that

$$\frac{Jf(x^{-1})}{f(x)} = \frac{JT_{k+1}(x^{-v_1}, \dots, x^{-v_k})}{JT_{k+1}(x^{v_1}, \dots, x^{v_k})} \equiv \frac{a_M}{a_m} + \frac{a}{a_m^2} x^{\boldsymbol{\gamma}\boldsymbol{v}} \bmod x^{\boldsymbol{\gamma}\boldsymbol{v}+1}. \tag{32}$$

By (25) $|\boldsymbol{\Lambda}_{k+1}|\boldsymbol{\gamma}\boldsymbol{v} = (\boldsymbol{\gamma}\boldsymbol{\Lambda}_{k+1}^A)[n_1, \dots, n_k]$ and since

$$\boldsymbol{\gamma}' = \boldsymbol{\gamma}\boldsymbol{\Lambda}_{k+1}^A \neq \boldsymbol{0} \tag{33}$$

we have for some $j \leqslant k$, $\gamma_j' \neq 0$. Applying (25) and (26) we find as above

$$\frac{Jf(x^{-1})}{f(x)} \equiv \frac{b_N}{b_n} + \frac{b}{b_n^2} x^{\boldsymbol{\delta}\boldsymbol{v}_j} \bmod x^{\boldsymbol{\delta}\boldsymbol{v}_j+1} \tag{34}$$

with

$$b \neq 0, \quad \boldsymbol{\delta}\boldsymbol{v}_j > 0, \tag{35}$$

$$h(\boldsymbol{\delta}) \leqslant k|S_{j+1}|h(\boldsymbol{\Lambda}_{j+1}). \tag{36}$$

It follows from (30), (32), (34) and (35) that

$$\boldsymbol{\gamma}\boldsymbol{v} = \boldsymbol{\delta}\boldsymbol{v}_j,$$

which gives

$$|\boldsymbol{\Lambda}_j|\boldsymbol{\gamma}'[n_1,\dots,n_k] = |\boldsymbol{\Lambda}_{k+1}|\boldsymbol{\delta}'[n_1,\dots,n_{j-1},n_{j+1},\dots,n_{k+1}]$$

with

$$\boldsymbol{\delta}' = \boldsymbol{\delta}\boldsymbol{\Lambda}_j^A. \tag{37}$$

Hence

$$\sum_{i=1}^{j-1}\bigl(|\boldsymbol{\Lambda}_j|\gamma_i' - |\boldsymbol{\Lambda}_{k+1}|\delta_i'\bigr)n_i + |\boldsymbol{\Lambda}_j|\gamma_j' n_j + \sum_{i=j+1}^{k}\bigl(|\boldsymbol{\Lambda}_j|\gamma_i' - |\boldsymbol{\Lambda}_{k+1}|\delta_{i-1}'\bigr)n_i + |\boldsymbol{\Lambda}_{k+1}|\gamma_k' n_{k+1} = 0,$$

which is the desired equality (13) with

$$0 < h(\boldsymbol{\beta}) \leqslant |\boldsymbol{\Lambda}_j|h(\boldsymbol{\gamma}') + |\boldsymbol{\Lambda}_{k+1}|h(\boldsymbol{\delta}').$$

It follows from (24), (31), (33), (36), (37) and Lemma 5 that

$$\begin{aligned} h(\boldsymbol{\beta}) &\leqslant h(\boldsymbol{\Lambda}_j)^k k(k-1)^{(k-1)/2}h(\boldsymbol{\Lambda}_{k+1})^{k-1}h(\boldsymbol{\gamma}) \\ &\quad + h(\boldsymbol{\Lambda}_{k+1})^k k(k-1)^{(k-1)/2}h(\boldsymbol{\Lambda}_j)^{k-1}h(\boldsymbol{\delta}) \\ &\leqslant k^2(k-1)^{(k-1)/2}h(\boldsymbol{\Lambda}_j)^k h(\boldsymbol{\Lambda}_{k+1})^k\bigl(|S_j| + |S_{k+1}|\bigr) \\ &< \exp\biggl(\frac{k+3}{2}\log k + k\bigl(\|S_j\| + \|S_{k+1}\|\bigr)\log 2 + \log\bigl(|S_j| + |S_{k+1}|\bigr)\biggr) \\ &< \exp\biggl(\frac{k+3}{2}\log k + 2k\|P\|^{2|Q|}\|Q\|^{2|P|}\log 2 + \log 4|P|\,|Q|\biggr). \end{aligned}$$

For $k = 2$ we get

$$h(\boldsymbol{\beta}) < \exp\bigl(2\|P\|^{2|Q|}\|Q\|^{2|P|}\log 5|P|\,|Q| + \log 21\bigr),$$

for $k > 2$ we use the inequality

$$kx < \exp_{2k-4} x \quad (x \geqslant 0)$$

and obtain

$$\begin{aligned} h(\boldsymbol{\beta}) &\leqslant \exp\bigl(2k\|P\|^{2|Q|}\|Q\|^{2|P|} + k\log 4|P|\,|Q|k\bigr) \\ &< \exp_{2k-3}\bigl(2\|P\|^{2|Q|}\|Q\|^{2|P|}\log 5|P|\,|Q| + \log 7k\bigr). \end{aligned}$$ □

Lemma 10. *If $Q \neq 0$ is a polynomial,*

$$JQ(y_1^{-1},\dots,y_k^{-1}) \neq \pm JQ(y_1,\dots,y_k) \quad \textit{and} \quad LQ(x^{v_1},\dots,x^{v_k}) = \text{const},$$

then

$$\boldsymbol{\beta}\boldsymbol{v} = 0 \quad \textit{with} \quad h(\boldsymbol{\beta}) \leqslant 2|Q|. \tag{38}$$

Proof. Let the degree of JQ with respect to y_j be q_j and

$$JQ(y_1, \dots, y_k) = \sum a_{\boldsymbol{\alpha}} y_1^{\alpha_1} \cdots y_k^{\alpha_k},$$

where the summation is taken over all integral vectors $\boldsymbol{\alpha}$ satisfying $0 \leqslant \alpha_j \leqslant q_j$. Clearly

$$JQ(y_1^{-1}, \dots, y_k^{-1}) = \sum a_{\boldsymbol{q}-\boldsymbol{\alpha}} y_1^{\alpha_1} \cdots y_k^{\alpha_k}$$

and there exist integral vectors $\boldsymbol{\alpha}_j$ and $\boldsymbol{\alpha}_{-j}$ $(1 \leqslant j \leqslant k)$ such that $\alpha_{jj} = q_j$, $a_{\boldsymbol{\alpha}_j} \neq 0$, $\alpha_{-jj} = 0$, $a_{\boldsymbol{\alpha}_{-j}} \neq 0$.

In view of the condition $JQ(y_1^{-1}, \dots, y_k^{-1}) \neq \pm JQ(y_1, \dots, y_k)$ we have for some $\boldsymbol{\alpha}_l, \boldsymbol{\alpha}_{-l}$

$$a_{\boldsymbol{\alpha}_l} \neq a_{\boldsymbol{q}-\boldsymbol{\alpha}_l}, \quad a_{\boldsymbol{\alpha}_{-l}} \neq -a_{\boldsymbol{q}-\boldsymbol{\alpha}_{-l}}. \tag{39}$$

Let the product $\boldsymbol{\alpha}\boldsymbol{v}$ taken over all $\boldsymbol{\alpha}$ for which $a_{\boldsymbol{\alpha}} \neq 0$, attains its minimum for $\boldsymbol{\alpha} = \boldsymbol{\alpha}_m$, maximum for $\boldsymbol{\alpha} = \boldsymbol{\alpha}_n$. We have

$$JQ(x^{v_1}, \dots, x^{v_k}) = x^{-\boldsymbol{\alpha}_m \boldsymbol{v}} \sum a_{\boldsymbol{\alpha}} x^{\boldsymbol{\alpha}\boldsymbol{v}},$$
$$JQ(x^{-v_1}, \dots, x^{-v_k}) = x^{\boldsymbol{\alpha}_n \boldsymbol{v}} \sum a_{\boldsymbol{\alpha}} x^{-\boldsymbol{\alpha}\boldsymbol{v}}.$$

All the exponents $\boldsymbol{\alpha}\boldsymbol{v}$ are different unless (38) holds (even with $h(\boldsymbol{\beta}) \leqslant |Q|$). In particular, $Q(x^{v_1}, \dots, x^{v_k}) \neq 0$.

The equality $LQ(x^{v_1}, \dots, x^{v_k}) = \text{const}$ implies

$$JQ(x^{v_1}, \dots, x^{v_k}) = \text{const}\, JQ(x^{-v_1}, \dots, x^{-v_k})$$

and by the comparison of constant terms

$$a_{\boldsymbol{\alpha}_n} JQ(x^{v_1}, \dots, x^{v_k}) = a_{\boldsymbol{\alpha}_m} JQ(x^{-v_1}, \dots, x^{-v_k}).$$

Comparing the leading coefficients on both sides we get

$$a_{\boldsymbol{\alpha}_n}^2 = a_{\boldsymbol{\alpha}_m}^2, \quad \text{i.e.} \quad a_{\boldsymbol{\alpha}_n} = \pm a_{\boldsymbol{\alpha}_m},$$
$$\sum a_{\boldsymbol{\alpha}} x^{\boldsymbol{\alpha}\boldsymbol{v}} = \pm x^{(\boldsymbol{\alpha}_m + \boldsymbol{\alpha}_n)\boldsymbol{v}} \sum a_{\boldsymbol{\alpha}} x^{-\boldsymbol{\alpha}\boldsymbol{v}}. \tag{40}$$

In particular, we have for each $j \leqslant k$ and a suitable $\boldsymbol{\beta}_j$

$$a_{\boldsymbol{\alpha}_j} x^{\boldsymbol{\alpha}_j \boldsymbol{v}} = \pm a_{\boldsymbol{\beta}_j} x^{(\boldsymbol{\alpha}_m + \boldsymbol{\alpha}_n - \boldsymbol{\beta}_j)\boldsymbol{v}}.$$

If $\boldsymbol{\alpha} + \boldsymbol{\beta}_j - \boldsymbol{\alpha}_m - \boldsymbol{\alpha}_n \neq 0$ we get again (38), otherwise

$$\alpha_{mj} + \alpha_{nj} = \alpha_{jj} + \beta_{jj} \geqslant \alpha_{jj} = q_j. \tag{41}$$

Similarly we have for each $j \leqslant k$ and a suitable $\boldsymbol{\beta}_{-j}$

$$a_{\boldsymbol{\alpha}_{-j}} x^{\boldsymbol{\alpha}_{-j} \boldsymbol{v}} = \pm a_{\boldsymbol{\beta}_{-j}} x^{(\boldsymbol{\alpha}_m + \boldsymbol{\alpha}_n - \boldsymbol{\beta}_{-j})\boldsymbol{v}};$$

thus either (38) holds or

$$\alpha_{mj} + \alpha_{nj} = \alpha_{-jj} + \beta_{-jj} = \beta_{-jj} \leqslant q_j.$$

The last inequality together with (41) implies

$$\boldsymbol{\alpha}_m + \boldsymbol{\alpha}_n = \boldsymbol{q}$$

and

$$x^{(\boldsymbol{\alpha}_m+\boldsymbol{\alpha}_n)\boldsymbol{v}} \sum a_{\boldsymbol{\alpha}} x^{-\boldsymbol{\alpha}\boldsymbol{v}} = \sum a_{\boldsymbol{q}-\boldsymbol{\alpha}} x^{\boldsymbol{\alpha}\boldsymbol{v}}.$$

It follows now from (39) and (40) that with a suitable sign and a suitable integral $\boldsymbol{\alpha}$

$$\boldsymbol{\alpha}_{\pm l}\boldsymbol{v} = \boldsymbol{\alpha}\boldsymbol{v}, \quad \boldsymbol{\alpha} \neq \boldsymbol{a}_{\pm l}$$

which gives (38) again. □

Lemma 11. *For any polynomial* $F(x_1, \ldots, x_k) \neq 0$

$$LKF(x_1, \ldots, x_k) = KLF(x_1, \ldots, x_k) = LF(x_1, \ldots, x_k).$$

Proof. In view of the definition of the operations K and L it is enough to prove that for any integral vector $[\delta_1, \ldots, \delta_k] \neq \mathbf{0}$ and any factor $Q(y_1, \ldots, y_k)$ of $J(y_1^{\delta_1} \cdots y_k^{\delta_k} - 1)$

$$JQ(y_1^{-1}, \ldots, y_k^{-1}) = \pm JQ(y_1, \ldots, y_k).$$

Supposing the contrary we apply Lemma 10 with

$$v_i = \big(4h(\boldsymbol{\delta}) + 1\big)^i \quad (1 \leqslant i \leqslant k).$$

Since the conditions $\boldsymbol{\beta}\boldsymbol{v} = 0$, $h(\boldsymbol{\beta}) \leqslant 2|Q| \leqslant 2h(\boldsymbol{\delta})$ imply $\boldsymbol{\beta} = \mathbf{0}$, it follows from that lemma $LQ(x^{v_1}, \ldots, x^{v_k}) \neq \text{const}$. On the other hand

$$LQ(x^{v_1}, \ldots, x^{v_k}) \mid L(x^{\boldsymbol{v}\boldsymbol{\delta}} - 1)$$

and since all factors of $x^{|\boldsymbol{v}\boldsymbol{\delta}|} - 1$ are reciprocal we get a contradiction. □

Lemma 12. *For any polynomial* $F(x_1, \ldots, x_k)$ *and any integral vector* $\boldsymbol{n} = [n_1, \ldots, n_k]$ *such that* $F(x^{n_1}, \ldots, x^{n_k}) \neq 0$ *there exist an integral matrix* $\boldsymbol{M} = [\mu_{ij}]$ *of order* k *and an integral vector* $\boldsymbol{v} = [v_1, \ldots, v_k]$ *such that*

$$0 \leqslant \mu_{ij} < \mu_{jj} \leqslant \exp 9k \cdot 2^{\|F\|-5} \ (i \neq j), \quad \mu_{ij} = 0 \ (i < j); \tag{42}$$

$$\boldsymbol{n} = \boldsymbol{v}\boldsymbol{M}, \tag{43}$$

and either

$$LF\Big(\prod_{i=1}^{k} y_i^{\mu_{i1}}, \prod_{i=1}^{k} y_i^{\mu_{i2}}, \ldots, \prod_{i=1}^{k} y_i^{\mu_{ik}}\Big) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(y_1, \ldots, y_k)^{e_\sigma} \tag{44}$$

implies

$$LF(x^{n_1}, \ldots, x^{n_k}) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} LF_\sigma(x^{v_1}, \ldots, x^{v_k})^{e_\sigma} \tag{45}$$

or $\|F\| \geqslant 3$ *and there exists an integral vector* $\boldsymbol{\gamma}$ *such that*

$$\boldsymbol{\gamma}\boldsymbol{n} = 0, \tag{46}$$

where

$$0 < h(\boldsymbol{\gamma}) < \begin{cases} \max\{120(2|F|^*)^{2\|F\|-1}\log\|F\|,\ 8|F|\exp 9\cdot 2^{\|F\|-3}\} & \text{if } k=2,\\ \exp_{2k-4}\big(9k|F|^{*\|F\|-1}\log\|F\|\big) & \text{if } k>2. \end{cases} \tag{47}$$

If $k = 2$ and some $LF_\sigma(x^{v_1}, x^{v_2})$ in (45) *are allowed to be constants then* (47) *can be replaced by*

$$0 < h(\boldsymbol{\gamma}) < 120(2|F|^*)^{2\|F\|-1}\log\|F\|.$$

Proof. If $\|F\| \leqslant 2$ then by Lemma 11 $s = 0$, $LF(x_1^{n_1}, \dots, x_k^{n_k}) = \text{const}$ and it suffices to take $\boldsymbol{M} = \boldsymbol{I}_k$ (the identity matrix). Therefore we assume $\|F\| \geqslant 3$.

Let S be the set of all integral matrices $\boldsymbol{\Lambda} = [\lambda_{qt}]$ of order k satisfying

$$0 \leqslant \lambda_{qt} < \lambda_{tt} \leqslant 2^{\|F\|-2}\ (q \neq t), \quad \lambda_{qt} = 0\ (q < t), \tag{48}$$

$$\boldsymbol{n} = \boldsymbol{u}\boldsymbol{\Lambda} \quad \text{with integral } \boldsymbol{u}. \tag{49}$$

Integral vectors $\boldsymbol{m}$ such that for all $\boldsymbol{\Lambda} \in S$ and a suitable integral vector $\boldsymbol{v}_{\boldsymbol{\Lambda}}$

$$\boldsymbol{m} = \boldsymbol{v}_{\boldsymbol{\Lambda}}\boldsymbol{\Lambda}$$

form a module $\mathfrak{M}$, say. By (48) for any $\boldsymbol{\Lambda} \in S$, $|\boldsymbol{\Lambda}|$ divides

$$\exp k\psi(2^{\|F\|-2}) = \mu,$$

where ψ is Chebyshev's function. Clearly vectors $[\mu, 0, \dots, 0]$, $[0, \mu, \dots, 0], \dots,$ $[0, \dots, 0, \mu]$ belong to $\mathfrak{M}$. It follows from Lemma 6 that $\mathfrak{M}$ has a basis $\boldsymbol{\mu}_1, \dots, \boldsymbol{\mu}_k$ such that

$$0 \leqslant \mu_{ij} < \mu_{jj} \leqslant \mu\ (i \neq j), \quad \mu_{ij} = 0\ (i < j).$$

Since by Theorem 12 of [8], $\psi(x) < 1.04x < \frac{9}{8}x$ for all x, the matrix $\boldsymbol{M}$ satisfies (42), since $\boldsymbol{n} \in \mathfrak{M}$ it satisfies also (43).

In order to prove the alternative (45) or (46) and (47) we set

$$\begin{aligned} P(y_1, \dots, y_k) &= F\Big(\prod_{i=1}^{k} y_i^{\mu_{i1}}, \dots, \prod_{i=1}^{k} y_i^{\mu_{ik}}\Big) \\ &\overset{\text{can}}{=} \text{const}\prod_{i=1}^{k} y_i^{\alpha_i}\prod_{\sigma=1}^{s_1} F_\sigma(y_1, \dots, y_k)^{e_\sigma}, \\ H_i(x_1, \dots, x_k) &= \sum_{j=1}^{k} \mu_{ij}x_j\frac{\partial F}{\partial x_j} \end{aligned} \tag{50}$$

(note that $P \neq 0$ since $F(x^{n_1}, \dots, x^{n_k}) \neq 0$). It follows

$$\frac{\partial P}{\partial y_i}\,y_i = H_i\Big(\prod_{i=1}^{k} y_i^{\mu_{i1}}, \dots, \prod_{i=1}^{k} y_i^{\mu_{ik}}\Big) = \Big(y_i\sum_{\sigma=1}^{s_1} e_\sigma F_\sigma^{-1}\frac{\partial F_\sigma}{\partial y_i} + \alpha_i\Big)P \tag{51}$$

and by (43)

$$P(x^{v_1}, \dots, x^{v_k}) = F(x^{n_1}, \dots, x^{n_k}), \tag{52}$$

$$x^{v_i} \frac{\partial P}{\partial y_i}(x^{v_1}, \dots, x^{v_k}) = H_i(x^{n_1}, \dots, x^{n_k}). \tag{53}$$

(44) implies

$$JF_\sigma(y_1^{-1}, \dots, y_k^{-1}) = \pm F_\sigma(y_1, \dots, y_k) \quad (\sigma > s). \tag{54}$$

Assume now that for some distinct $\varrho, \tau \leqslant s_1$

$$D(x) = \big(LF_\varrho(x^{v_1}, \dots, x^{v_k}), LF_\tau(x^{v_1}, \dots, x^{v_k})\big) \neq 1. \tag{55}$$

We consider two cases:

1. for some j: $\dfrac{\partial F_\varrho}{\partial y_j} \neq 0$ and $\dfrac{\partial F_\tau}{\partial y_j} \neq 0$,
2. for each i: $\dfrac{\partial F_\varrho}{\partial y_i} \cdot \dfrac{\partial F_\tau}{\partial y_i} = 0$.

1. Here $H_j \neq 0$ and we set $G = (F, H_j)$. It follows from (50) and (51) that

$$G\Big(\prod_{i=1}^k y_i^{\mu_{i1}}, \dots, \prod_{i=1}^k y_i^{\mu_{ik}}\Big) = \text{const}\Big(P, \frac{\partial P}{\partial y_j} y_j\Big) = \text{const}\, P \prod_{\sigma=1}^{s_1} F_\sigma^{-1}(y_1, \dots, y_k),$$

where the product is taken over all σ satisfying $\dfrac{\partial F_\sigma}{\partial y_j} \neq 0$. On substituting $y_i = x^{v_i}$ $(1 \leqslant i \leqslant k)$ we obtain from (50), (51)

$$D(x) LG\Big(\prod_{i=1}^k x^{\mu_{i1} v_i}, \dots, \prod_{i=1}^k x^{\mu_{ik} v_i}\Big) \;\Big|\; \Big(LP(x^{v_1}, \dots, x^{v_k}), Lx^{v_j} \frac{\partial P}{\partial y_j}(x^{v_1}, \dots, x^{v_k})\Big),$$

which in view of (43), (52) and (53) gives

$$D(x) LG(x^{n_1}, \dots, x^{n_k}) \mid \big(LF(x^{n_1}, \dots, x^{n_k}), LH_j(x^{n_1}, \dots, x^{n_k})\big).$$

By (55) and Lemma 8 we have (46) with

$$0 < h(\boldsymbol{\gamma}) < \begin{cases} 5|F|\,|H_j| \log \|F\|^{2|H_j|} \|H_j\|^{2|F|} & \text{if } k = 2, \\ \exp_{2k-5}\big(2\|F\|^{2|H_j|} \|H_j\|^{2|F|} \log 5|F|\,|H_j| + \log 7k\big) & \text{if } k > 2. \end{cases}$$

2. Here we have for some h, j

$$\frac{\partial F_\varrho}{\partial y_h} \neq 0, \quad \frac{\partial F_\tau}{\partial y_h} = 0; \quad \frac{\partial F_\varrho}{\partial y_j} = 0, \quad \frac{\partial F_\tau}{\partial y_j} \neq 0,$$

thus $H_h \neq 0$, $H_j \neq 0$.

We set $G = (H_h, H_j)$. It follows from (50) and (51) that

$$\begin{aligned} \frac{\partial P}{\partial y_h} y_h &= F_\varrho^{e_\varrho - 1} F_\tau^{e_\tau} U, \quad U \not\equiv 0 \bmod F_\varrho, \\ \frac{\partial P}{\partial y_j} y_j &= F_\varrho^{e_\varrho} F_\tau^{e_\tau - 1} V, \quad V \not\equiv 0 \bmod F_\tau, \end{aligned} \tag{56}$$

hence

$$G\Big(\prod_{i=1}^{k} y_i^{\mu_{i1}}, \dots, \prod_{i=1}^{k} y_i^{\mu_{ik}}\Big) = F_{\varrho}^{e_\varrho - 1} F_{\tau}^{e_\tau - 1}(U, V)(y_1, \dots, y_k).$$

On substituting $y_i = x^{v_i}$ we obtain from (56)

$$D(x) LG\Big(\prod_{i=1}^{k} x^{\mu_{i1} v_i}, \dots, \prod_{i=1}^{k} x^{\mu_{ik} v_i}\Big) \Big| \Big(Lx^{v_h} \frac{\partial P}{\partial y_h}(x^{v_1}, \dots, x^{v_k}), Lx^{v_j} \frac{\partial P}{\partial y_j}(x^{v_1}, \dots, x^{v_k})\Big),$$

which in view of (43) and (53) gives

$$D(x) LG(x^{n_1}, \dots, x^{n_k}) \mid \big(LH_h(x^{n_1}, \dots, x^{n_k}), LH_j(x^{n_1}, \dots, x^{n_k})\big).$$

By (55) and Lemma 8 we have (46) with

$$0 < h(\boldsymbol{\gamma}) < \begin{cases} 5|H_h|\,|H_j| \log \|H_h\|^{2|H_j|} \|H_j\|^{2|H_h|} & \text{if } k = 2, \\ \exp_{2k-5}\big(2\|H_h\|^{2|H_j|} \|H_j\|^{2|H_h|} \log 5|H_h|\,|H_j| + \log 7k\big) & \text{if } k > 2. \end{cases}$$

Since for all i: $|H_i| \leqslant |F|$,

$$\|H_i\| \leqslant k \sum_{j=1}^{k} \Big\| \mu_{ij} x_j \frac{\partial F}{\partial x_j} \Big\| \leqslant k^2 h(\boldsymbol{M})^2 |F|^2 \|F\|,$$

it follows in both cases that if $k = 2$

$$\begin{aligned} 0 < h(\boldsymbol{\gamma}) &< 20|F|^3 \log 4h(\boldsymbol{M})^2 |F|^2 \|F\| \\ &< 20|F|^3 \log 4|F|^2 \|F\| + 20|F|^3 \cdot 9 \cdot 2^{\|F\|-3} < 120\big(2|F|^*\big)^{2\|F\|-1} \log \|F\|, \end{aligned}$$

if $k > 2$

$$\begin{aligned} 0 < h(\boldsymbol{\gamma}) &< \exp_{2k-4}\big(4|F| \log k^2 h(\boldsymbol{M})^2 |F|^2 \|F\| + \log\log 5|F|^2 + \log 3\big) \\ &< \exp_{2k-4}\big(5|F| \log k^2 |F|^2 \|F\| + |F| \cdot 9k \cdot 2^{\|F\|-2}\big) \\ &< \exp_{2k-4}\big(9k|F|^{*\|F\|-1} \log \|F\|\big). \end{aligned}$$

Assume, therefore, that for all distinct $\varrho, \tau \leqslant s_1$

$$\big(LF_\varrho(x^{v_1}, \dots, x^{v_k}), LF_\tau(x^{v_1}, \dots, x^{v_k})\big) = 1 \tag{57}$$

and let $f(x)$ be any irreducible factor of $LF(x^{n_1}, \dots, x^{n_k})$. By Lemma 9 either (46)–(47) hold or there exist an integral matrix $\boldsymbol{\Lambda} = [\lambda_{qt}]$ of order k, an integral vector $\boldsymbol{u} = [u_1, \dots, u_k]$ satisfying (48)–(49) and a polynomial T such that

$$T(z_1, \dots, z_k) \mid F\Big(\prod_{q=1}^{k} z_q^{\lambda_{q1}}, \dots, \prod_{q=1}^{k} z_q^{\lambda_{qk}}\Big), \tag{58}$$

$$f(x) = \text{const}\, LT(x^{u_1}, \dots, x^{u_k}). \tag{59}$$

Since $\boldsymbol{\Lambda} \in S$ and by the choice of $\boldsymbol{M}$: $\boldsymbol{\mu}_1, \ldots, \boldsymbol{\mu}_n \in \mathfrak{M}$ we have for some integral vectors $\boldsymbol{\theta}_1, \ldots, \boldsymbol{\theta}_n$: $\boldsymbol{\mu}_i = \boldsymbol{\theta}_i \boldsymbol{\Lambda}$, thus

$$\left.\begin{aligned} \boldsymbol{M} &= \boldsymbol{\Theta}\boldsymbol{\Lambda} \quad (60)\\ \boldsymbol{u} &= \boldsymbol{v}\boldsymbol{\Theta} \quad (61) \end{aligned}\right\}, \qquad \boldsymbol{\Theta} = \begin{bmatrix} \boldsymbol{\theta}_1 \\ \vdots \\ \boldsymbol{\theta}_n \end{bmatrix}.$$

Set

$$W(y_1, \ldots, y_k) = JT\left(\prod_{i=1}^{k} y_i^{\vartheta_{i1}}, \ldots, \prod_{i=1}^{k} y_i^{\vartheta_{ik}}\right).$$

We have by (58) and (60)

$$W(y_1, \ldots, y_k) \mid F\left(\prod_{i=1}^{k} y_i^{\mu_{i1}}, \ldots, \prod_{i=1}^{k} y_i^{\mu_{ik}}\right),$$

by (59) and (61)

$$f(x) = \text{const}\, LW(x^{v_1}, \ldots, x^{v_k}).$$

Since $f(x)$ is irreducible, the last two formulae imply in view of (50)

$$f(x) = \text{const}\, LF_{\varrho}(x^{v_1}, \ldots, x^{v_k}) \quad \text{for some } \varrho \leqslant s_1 \tag{62}$$

and since $Jf(x^{-1}) \neq \pm Jf(x)$ we have by (54) $\varrho \leqslant s$. By (57)

$$\left(f(x), \prod_{\sigma=s+1}^{s_1} LF_{\sigma}(x^{v_1}, \ldots, x^{v_k})^{e_\sigma}\right) = 1$$

and because of the arbitrariness of $f(x)$

$$\left(LF(x^{n_1}, \ldots, x^{n_k}), \prod_{\sigma=s+1}^{s_1} LF_{\sigma}(x^{v_1}, \ldots, x^{v_k})^{e_\sigma}\right) = 1.$$

Since by (50) and (52)

$$LF(x^{n_1}, \ldots, x^{n_k}) = \text{const} \prod_{\sigma=1}^{s_1} LF_{\sigma}(x^{v_1}, \ldots, x^{v_k})^{e_\sigma},$$

it follows that

$$LF(x^{n_1}, \ldots, x^{n_k}) = \text{const} \prod_{\sigma=1}^{s} LF_{\sigma}(x^{v_1}, \ldots, x^{v_k})^{e_\sigma}.$$

Moreover, none of the $LF_\sigma(x^{v_1}, \ldots, x^{v_k})$ ($\sigma \leqslant s$) is reducible since taking as $f(x)$ any of its reducible factors we would obtain from (62) a contradiction with (57).

It remains to prove that none of $LF_\sigma(x^{v_1}, \ldots, x^{v_k})$ ($\sigma \leqslant s$) is constant unless (46) holds with

$$0 < h(\boldsymbol{\gamma}) < \begin{cases} 8|F| \exp 9 \cdot 2^{\|F\|-3} & \text{if } k = 2, \\ \exp_{2k-4}\left(9k|F|^{*\|F\|-1} \log \|F\|\right) & \text{if } k > 2. \end{cases}$$

This follows from Lemma 10 on taking $Q = F_\sigma$, since (38) implies (46) with $\boldsymbol{\gamma} = \boldsymbol{\beta}\boldsymbol{M}^A$ and

$$0 < h(\boldsymbol{\gamma}) \leqslant kh(\boldsymbol{M}^A)h(\boldsymbol{\beta}) \leqslant k(k-1)^{(k-1)/2}h(\boldsymbol{M})^{k-1}2|P|$$
$$\leqslant 2k^2(k-1)^{(k-1)/2}h(\boldsymbol{M})^k|F| \leqslant 2k^2(k-1)^{(k-1)/2}|F|\exp 9k^2 2^{\|F\|-5}. \quad \square$$

Remark. A comparison of Lemma 12 with the conjecture from [9] shows besides the replacement of K by L the two differences:

it is not assumed that F is irreducible,

it is not assumed that $n_1 > 0, \ldots, n_k > 0$ and it is not asserted that $v_1 \geqslant 0, \ldots, v_k \geqslant 0$ (instead it is asserted that $\boldsymbol{M}$ is triangular).

As to the first difference one may note the fact overlooked in [9] that if F is irreducible all the exponents e_σ in (44) are 1. Indeed, in the notation of the preceding proof $e_\sigma > 1$ implies

$$F_\sigma(y_1, \ldots, y_k) \mid \left(P(y_1, \ldots, y_k), \frac{\partial P}{\partial y_1}, \ldots, \frac{\partial P}{\partial y_k}\right)$$

hence

$$\left(JF(x_1, \ldots, x_k), H_1(x_1, \ldots, x_k), \ldots, H_k(x_1, \ldots, x_k)\right) \neq 1.$$

Since $|\boldsymbol{M}| \neq 0$ it follows by the definition of H_i that

$$\left(JF(x_1, \ldots, x_k), x_1\frac{\partial F}{\partial x_1}, \ldots, x_k\frac{\partial F}{\partial x_k}\right) \neq 1,$$

which for an irreducible F is impossible.

As to the second difference it may be noted that the formulation with the assumption $n_1 \geqslant 0, \ldots, n_k \geqslant 0$ and the assertion $v_1 \geqslant 0, \ldots, v_k \geqslant 0$ (but $\boldsymbol{M}$ not necessarily triangular and $h(\boldsymbol{M})$ possibly greater) is also true its proof however involves the following theorem of Schmidt [10].

If $\mathfrak{M}$ is a full sublattice of the integral k-dimensional lattice and $\mathfrak{M}^+$ consists of all vectors of $\mathfrak{M}$ with nonnegative coordinates then there exists a finite subset $\mathfrak{M}_0$ of $\mathfrak{M}^+$ such that every vector of $\mathfrak{M}^+$ is a linear combination of k vectors of $\mathfrak{M}_0$ with nonnegative integral coefficients.

In the proof of Lemma 5 of [9] the truth of this theorem for $k = 2$ was established together with a bound for the height of the vectors of $\mathfrak{M}_0$ in terms of $\mathfrak{M}$. Such a bound in the general case has been found recently by R. Lee.

Proof of Theorem 2. The theorem is true for $k = 1$ by Lemma 12. Assume that it is true for polynomials in $k-1$ variables and consider $F(x_1, \ldots, x_k)$. By Lemma 12 either there exist a matrix $\boldsymbol{M}$ and a vector $\boldsymbol{v}$ with the properties (42), (43), (45) or we have $\|F\| \geqslant 3$ and there exists a vector $\boldsymbol{\gamma}$ satisfying (46), (47). In the former case the theorem holds with $r = k$, in the latter case $\boldsymbol{n}$ belongs to the module $\mathfrak{N}$ of integral vectors perpendicular to $\boldsymbol{\gamma}$. If $\boldsymbol{\gamma} = [0, \ldots, 0, \gamma_\nu, \ldots, \gamma_k]$ with $\gamma_\nu \neq 0$, $\mathfrak{N}$ contains $k-1$ linearly independent vectors $[1, 0, \ldots, 0], \ldots, [0, \ldots, 1, 0, \ldots, 0], [0, \ldots, \gamma_{\nu+1}, -\gamma_\nu, 0, \ldots, 0]$, $\ldots, [0, \ldots, \gamma_k, 0, \ldots, -\gamma_\nu]$ and by Lemma 6 it has a basis which written in the form of

a matrix $\boldsymbol{\Delta} = [\delta_{tj}]_{\substack{t<k\\ j\leqslant k}}$ satisfies

$$h(\boldsymbol{\Delta}) \leqslant (k-1)h(\boldsymbol{\gamma}), \tag{63}$$

$$\text{rank of } \boldsymbol{\Delta} = k-1, \tag{64}$$

$$\boldsymbol{n} = \boldsymbol{m}\boldsymbol{\Delta}, \quad \boldsymbol{m} \text{ integral} \neq \boldsymbol{0}. \tag{65}$$

Set

$$F'(z_1, \dots, z_{k-1}) = JF\Big(\prod_{t=1}^{k-1} z_t^{\delta_{t1}}, \prod_{t=1}^{k-1} z_t^{\delta_{t2}}, \dots, \prod_{t=1}^{k-1} z_t^{\delta_{tk}}\Big). \tag{66}$$

We have clearly $F'(x^{m_1}, \dots, x^{m_{k-1}}) \neq 0$,

$$|F'|^* \leqslant 2(k-1)|F|^* h(\boldsymbol{\Delta}), \tag{67}$$

and by (8) and (9)

$$\|F'\| \leqslant \max_{0\leqslant\varphi\leqslant 2\pi} \big|F'(e^{i\varphi_1}, \dots, e^{i\varphi_{k-1}})\big|^2 \leqslant \max_{0\leqslant\vartheta\leqslant 2\pi} \big|F(e^{i\vartheta_1}, \dots, e^{i\vartheta_k})\big|^2 \leqslant \|F\|^2. \tag{68}$$

By the inductive assumption there exist an integral matrix $\boldsymbol{N}' = [v'_{it}]_{\substack{i\leqslant r\\ t\leqslant k}}$ and an integral vector $\boldsymbol{v} = [v_1, \dots, v_r]$ such that

$$h(\boldsymbol{N}') \leqslant \begin{cases} \exp 9(k-1)2^{\|F'\|-5} & \text{if } k-1 = r,\\ \exp\big(5\cdot 2^{\|F'\|^2-4} + 2\|F'\| \log |F'|^*\big) & \text{if } k+r-1 = 3,\\ \exp_{(k-r-1)(k+r-4)}\big(8(k-1)|F'|^{*\|F'\|-1} \log \|F'\|\big) & \text{otherwise;}\end{cases} \tag{69}$$

$$\text{rank of } \boldsymbol{N}' = r; \tag{70}$$

$$\boldsymbol{m} = \boldsymbol{v}\boldsymbol{N}'; \tag{71}$$

$$LF'\Big(\prod_{i=1}^{r} y_i^{v'_{i1}}, \dots, \prod_{i=1}^{r} y_i^{v'_{i,k-1}}\Big) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(y_1, \dots, y_r)^{e_\sigma}$$

implies

$$LF'(x^{m_1}, \dots, x^{m_{k-1}}) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s_0} LF_\sigma(x^{v_1}, \dots, x^{v_r})^{e_\sigma}. \tag{72}$$

Set

$$\boldsymbol{N} = \boldsymbol{N}'\boldsymbol{\Delta}. \tag{73}$$

It follows from (64) and (70) that $\boldsymbol{N}$ is of rank r. By (65) and (71) $\boldsymbol{n} = \boldsymbol{v}\boldsymbol{N}$. By (66) and (73)

$$LF'\Big(\prod_{i=1}^{r} y_i^{v'_{i1}}, \dots, \prod_{i=1}^{r} y_i^{v'_{i,k-1}}\Big) = LF\Big(\prod_{i=1}^{r} y_i^{v_{i1}}, \dots, \prod_{i=1}^{r} y_i^{v_{ik}}\Big)$$

and by (65) and (66)

$$JF'(x^{m_1}, \dots, x^{m_{k-1}}) = JF(x^{n_1}, \dots, x^{n_k}).$$

In view of (72) it remains to estimate $h(\boldsymbol{N})$. By (69) and (73)

$$h(\boldsymbol{N}) \leqslant (k-1)^2 h(\boldsymbol{\gamma}) h(\boldsymbol{N}').$$

To proceed further we use the inequalities (47), (67)–(69), $|F|^* \geqslant 2$, $|F|^* \geqslant 3$ and distinguish four cases:

1. $k = 2, r = 1$. Here

$$\begin{aligned} h(\boldsymbol{N}) &\leqslant \max\left\{120(2|F|^*)^{2\|F\|-1} \log \|F\|, 8|F| \exp 9 \cdot 2^{\|F\|-3}\right\} \exp 9 \cdot 2^{\|F\|^2-5} \\ &\leqslant \exp\left(5 \cdot 2^{\|F\|^2-4} + 2\|F\| \log |F|^*\right). \end{aligned}$$

2. $k = 3, r = 1$. Here we use the inequality

$$\log 4 + 5 \cdot 2^{\|F\|^4-4} + 2\|F\|^2 \log 8|F|^* < \left(\|F\|^2 - 1\right) \exp\left(27|F|^{*\|F\|-1} \log \|F\|\right)$$

and obtain

$$\begin{aligned} h(\boldsymbol{N}) &\leqslant 4 \exp_2\left(27|F|^{*\|F\|-1} \log \|F\|\right) \exp\left(5 \cdot 2^{\|F'\|^2-4} + 2\|F'\| \log |F'|^*\right) \\ &< \exp\left(\log 4 + \exp(27|F|^{*\|F\|-1} \log \|F\|)\right) \\ &\quad \times \exp\left(5 \cdot 2^{\|F\|^4-4} + 2\|F\|^2 \log 8|F|^* + 2\|F\|^2 \exp(27|F|^{*\|F\|-1} \log \|F\|)\right) \\ &< \exp\left(3\|F\|^2 \exp(27|F|^{*\|F\|-1} \log \|F\|)\right) < \exp_2\left(30|F|^{*\|F\|-1} \log \|F\|\right). \end{aligned}$$

3. $k - 1 = r > 1$. Here we use the inequality

$$\begin{aligned} (k-1)^2 \exp 9(k-1)2^{\|F\|^2-5} &< \exp 11(k-1)2^{\|F\|^2-5} < \exp_2 9k2^{\|F\|-1} \\ &< \exp_2\left(9k|F|^{*\|F\|-1} \log \|F\|\right) \end{aligned}$$

and obtain

$$\begin{aligned} h(\boldsymbol{N}) &\leqslant (k-1)^2 \exp_{2k-4}\left(9k|F|^{*\|F\|-1} \log \|F\|\right) \cdot \exp 9(k-1)2^{\|F\|^2-5} \\ &\leqslant \exp^2_{2k-4}\left(9k|F|^{*\|F\|-1} \log \|F\|\right) < \exp_{2k-4}\left(10k|F|^{*\|F\|-1} \log \|F\|\right). \end{aligned}$$

4. $k - 1 > \max(r, 2)$. Here we use the inequality

$$\begin{aligned} &20k \log \|F\| \left(2k^2|F|^* \exp_{2k-4}(9k|F|^{*\|F\|-1} \log \|F\|)\right)^{\|F\|^2} \\ &\qquad < \left(\exp_{2k-4}(9k|F|^{*\|F\|-1} \log \|F\|)\right)^{2\|F\|^2} \\ &\qquad = \exp_2\left(\exp_{2k-6}(9k|F|^{*\|F\|-1} \log \|F\|) + \log 2\|F\|^2\right) \\ &\qquad < \exp_{2k-4}(9k|F|^{*\|F\|-1} \log \|F\| + 1) \end{aligned}$$

and obtain

$$
\begin{aligned}
h(\boldsymbol{N}) &\leqslant (k-1)^2 \exp_{2k-4}(9k|F|^{*\|F\|-1}\log\|F\|)\\
&\quad\times \exp_{(k-r-1)(k+r-4)}(10(k-1)|F'|^{*\|F'\|-1}\log\|F'\|)\\
&< \exp_{2k-4}(10k|F|^{*\|F\|-1}\log\|F\|)\\
&\quad\times \exp_{(k-r-1)(k+r-4)}\Big(20k\log\|F\|\big(2k^2|F|^*\exp_{2k-4}(9k|F|^{*\|F\|-1}\log\|F\|)\big)^{\|F\|^2}\Big)\\
&< \exp_{2k-3}(9k|F|^{*\|F\|-1}\log\|F\|+1)\\
&\quad\times \exp_{(k-r-1)(k+r-4)+2k-4}(9k|F|^{*\|F\|-1}\log\|F\|+1)\\
&< \exp^2_{(k-r)(k+r-3)}(9k|F|^{*\|F\|-1}\log\|F\|+1)\\
&< \exp_{(k-r)(k+r-3)}(10k|F|^{*\|F\|-1}\log\|F\|). \qquad \square
\end{aligned}
$$

Proof of Corollary. Let $JF(x) = a_0 + \sum_{j=1}^{k} a_j x^{n_j}$, where $a_j \neq 0$, n_j distinct > 0. Set in Theorem 2

$$F(x_1, \ldots, x_k) = a_0 + \sum_{j=1}^{k} a_j x_j.$$

We have

$$k \leqslant \|F\| - 1 = \|f\| - 1, \quad |F|^* = 2. \tag{74}$$

By Theorem 2, the number l of irreducible factors of $Lf(x)$ equals the number of irreducible factors of

$$LF\Big(\prod_{i=1}^{r} y_i^{\nu_{i1}}, \prod_{i=1}^{r} y_i^{\nu_{i2}}, \ldots, \prod_{i=1}^{r} y_i^{\nu_{ik}}\Big)$$

(in the notation of the theorem), hence $l = 0$ if $\|f\| \leqslant 2$ and $l \leqslant 2rh(\boldsymbol{N})$ otherwise. Thus if $k \neq 2$ we get from (i) and (74)

$$
\begin{aligned}
l &\leqslant \max\big\{2k\exp 9k\cdot 2^{\|F\|-5}, \max_{r<k} 2r\exp_{(k-r)(k+r-3)}(10k|F|^{*\|F\|-1}\log\|F\|)\big\}\\
&\leqslant 2\exp_{k^2-3k+2}(5k\cdot 2^{\|F\|}\log\|F\|) \leqslant 2\exp_{\|f\|^2-5\|f\|+6}\big(5(\|f\|-1)2^{\|f\|}\log\|f\|\big)\\
&< \exp_{\|f\|^2-5\|f\|+7}(\|f\|+2).
\end{aligned}
$$

If $k = 2$ we have

$$l \leqslant \max\big\{4\exp 9\cdot 2^{\|f\|-4}, 2\exp\big(5\cdot 2^{\|f\|^2-4} + 2\|f\|\log 2\big)\big\} < \exp_{\|f\|^2-5\|f\|+7}(\|f\|+2)$$

except when $\|f\| = 3$. However in this case $Jf(x) = \pm x^{n_1} \pm x^{n_2} \pm 1$ has at most one irreducible non-reciprocal factor (see [4] or [13]) and the proof is complete. $\square$

4.

Lemma 13. *If* $KF(x_1, x_2) = LF(x_1, x_2)$ *and* $[n_1, n_2] \neq \mathbf{0}$ *then*

$$\text{either} \quad KF(x^{n_1}, x^{n_2}) = LF(x^{n_1}, x^{n_2}) \quad \text{or} \quad F(x^{n_1}, x^{n_2}) \neq 0$$

and for each zero ξ *of* $\dfrac{KF(x^{n_1}, x^{n_2})}{LF(x^{n_1}, x^{n_2})}$ *the inequality holds*

$$\frac{\max\{|n_1|, |n_2|\}}{(n_1, n_2)}\, e\big(\xi, \mathbb{Q}(\xi)\big) \leqslant 120(2|F|^*)^{2\|F\|-1} \log \|F\|.$$

Proof. We can assume $|F| \geqslant 4$ since otherwise

$$KF(x^{n_1}, x^{n_2}) = LF(x^{n_1}, x^{n_2})$$

holds trivially. Set

$$P = F(x_1, x_2), \quad Q_1 = JF(x_1^{-1}, x_2^{-1}), \quad Q_2 = \frac{\partial P}{\partial x_1}, \quad G_i = (P, Q_i),$$
$$T_i = PG_i^{-1}, \quad U_i = Q_i G_i^{-1}, \quad V = \big(LF(x_1, x_2), LF(x_1^{-1}, x_2^{-1})\big).$$

By the assumption $KF(x_1, x_2) = LF(x_1, x_2)$, we have

$$G_1 = \frac{JF(x_1, x_2)}{KF(x_1, x_2)}\, V(x_1, x_2), \tag{75}$$
$$T_1 = LF(x_1, x_2)V^{-1}, \quad U_1 = LF(x_1^{-1}, x_2^{-1})V^{-1}.$$

If ξ is a zero of $\dfrac{KF(x^{n_1}, x^{n_2})}{LF(x^{n_1}, x^{n_2})}$ then ξ is conjugate to ξ^{-1} thus $P(\xi^{n_1}, \xi^{n_2}) = Q_1(\xi^{n_1}, \xi^{n_2}) = 0$. On the other hand, ξ not being a root of unity is not a zero of $\dfrac{JF(x^{n_1}, x^{n_2})}{KF(x^{n_1}, x^{n_2})}$ and we get from (75) either $T_1(\xi^{n_1}, \xi^{n_2}) = U_1(\xi^{n_1}, \xi^{n_2}) = 0$ or $V(\xi^{n_1}, \xi^{n_2}) = 0$. [This argument needs an amplification. It assumes silently that every zero $\xi \neq 0$ of $\dfrac{JF}{KF}(x^{n_1}, x^{n_2})$ is a zero of $\dfrac{JF(x^{n_1}, x^{n_2})}{KF(x^{n_1}, x^{n_2})}$, which is true but not obvious. When one refers to the definition of KF given of p. 344 one has to show that for an irreducible F the divisibility $F(x_1, x_2) \mid J\big(x_1^{\delta_1} x_2^{\delta_2} - 1\big)$ implies $KF(x^{n_1}, x^{n_2}) = \text{const}$. This is obvious if $n_1\delta_1 + n_2\delta_2 \neq 0$, but if $n_1\delta_1 + n_2\delta_2 = 0$ one needs the fact implied by Lemma 11 of D7 that

$$F(x_1, x_2) = \text{const}\, J\Phi\big(x_1^{\delta_1/(\delta_1,\delta_2)} x_2^{\delta_2/(\delta_1,\delta_2)}\big)$$

for a polynomial $\Phi \mid z^{(\delta_1,\delta_2)} - 1$.]

In the second case (ξ^{n_1}, ξ^{n_2}) is a zero of a certain irreducible factor of $V(x_1, x_2)$, $f(x_1, x_2)$ say. Without loss of generality we may assume $\partial f/\partial x_1 \neq 0$. By the definition of V, it follows that $g(x_1, x_2) = Jf(x_1^{-1}, x_2^{-1})$ divides V and is prime to f. Set

$$P = f^\alpha g^\beta h, \quad \text{where} \quad \alpha\beta > 0, \ (f, g) = (f, h) = (g, h) = 1.$$

We have

$$Q_2 = \frac{\partial P}{\partial x_1} = \Big(\alpha\,\frac{\partial f/\partial x_1}{f} + \beta\,\frac{\partial g/\partial x_1}{g} + \frac{\partial h/\partial x_1}{h}\Big)P \neq 0,$$

$$G_2 = \Big(\frac{\partial h}{\partial x_1}, h\Big)\frac{P}{fgh}, \quad T_2 = \frac{fgh}{(\partial h/\partial x_1, h)},$$

$$U_2 = \alpha\,\frac{\partial f}{\partial x_1}\,g\,\frac{h}{(\partial h/\partial x_1, h)} + \beta f\,\frac{\partial g}{\partial x_1}\cdot\frac{h}{(\partial h/\partial x_1, h)} + fg\,\frac{h}{(\partial h/\partial x_1, h)}.$$

Since $f(\xi^{n_1}, \xi^{n_2}) = g(\xi^{n_1}, \xi^{n_2})$ it follows

$$T_2(\xi^{n_1}, \xi^{n_2}) = U_2(\xi^{n_1}, \xi^{n_2}) = 0.$$

In any case

$$T_i(\xi^{n_1}, \xi^{n_2}) = U_i(\xi^{n_1}, \xi^{n_2}) = 0 \quad \text{with suitable } i. \tag{76}$$

Let R_{ij} be the resultant of T_i, U_i with respect to x_j and S_{ij} a nonvanishing minor of Sylvester's matrix of P, Q_i divisible by R_{ij}. Since

$$|P| = |F|, \quad |Q_i| \leqslant |F|, \quad \|P\| = \|F\|, \quad \|Q_i\| \leqslant |F|^2\|F\|$$

we get from Lemma 5

$$|S_{ij}| \leqslant 2|F|^2, \quad \|S_{ij}\| \leqslant (|F|\,\|F\|)^{4|F|} \quad (1 \leqslant i, j \leqslant 2).$$

Set $\boldsymbol{\Omega} = \mathbb{Q}(\xi^{n_1}, \xi^{n_2})$. By (76) $|\boldsymbol{\Omega}|$ does not exceed the number of distinct pairs $\langle \eta, \vartheta \rangle$ satisfying $T_i(\eta, \vartheta) = U_i(\vartheta, \eta) = 0$ and by Lemma 4

$$|\boldsymbol{\Omega}| \leqslant |R_{ij}| \leqslant |S_{ij}|.$$

Since $\xi^{(n_1,n_2)} \in \boldsymbol{\Omega}$, it follows

$$|\mathbb{Q}(\xi)| \leqslant (n_1, n_2)|\boldsymbol{\Omega}|.$$

Moreover $R_{i,3-j}(\xi^{n_j}) = 0$, $S_{i,3-j}(\xi^{n_j}) = 0$ and we get by Lemma 1 with $\boldsymbol{\Omega}_1 = \mathbb{Q}(\xi)$

$$\begin{aligned} |n_j|e\big(\xi, \mathbb{Q}(\xi)\big) &\leqslant e\big(\xi^{n_j}, \mathbb{Q}(\xi)\big) \leqslant (n_1, n_2)e(\xi^{n_j}, \boldsymbol{\Omega}) \\ &\leqslant (n_1, n_2)20|\boldsymbol{\Omega}|^2 \log|\boldsymbol{\Omega}|^* \log\|S_{i,3-j}\| \\ &\leqslant (n_1, n_2)20|S_{ij}|^2 \log|S_{ij}|^* \cdot 4|F| \log(|F|\,\|F\|) \\ &\leqslant (n_1, n_2)120(2|F|^*)^{2\|F\|-1} \log\|F\|, \end{aligned}$$

which completes the proof. □

Proof of Theorem 3. If $\|F\| \leqslant 2$ then $s = 0$, $KF(x^{n_1}, x^{n_2}) = \text{const}$ and it suffices to take $\boldsymbol{N} = \boldsymbol{I}_2$. Suppose therefore $\|F\| \geqslant 3$ and assume first

$$\frac{\max\{|n_1|, |n_2|\}}{(n_1, n_2)} > 120(2|F|^*)^{2\|F\|-1} \log\|F\|.$$

We apply Lemmata 12 and 13 to polynomial F and vector $[n_1, n_2]$. If $\boldsymbol{M} = [\mu_{ij}]$ is the

matrix of Lemma 12 then $[n_1, n_2] = [v_1, v_2]\boldsymbol{M}$. Moreover

$$KF(y_1^{\mu_{11}} y_2^{\mu_{21}}, y_1^{\mu_{12}} y_2^{\mu_{22}}) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(y_1, y_2)^{e_\sigma} \tag{77}$$

implies by Lemma 11

$$LF(y_1^{\mu_{11}} y_2^{\mu_{21}}, y_1^{\mu_{12}} y_2^{\mu_{22}}) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s_0} F_\sigma(y_1, y_2)^{e_\sigma}$$

where $JF_\sigma(y_1^{-1}, y_2^{-1}) \neq \pm F_\sigma(y_1, y_2)$ for $\sigma \leqslant s_0$ exclusively, and by Lemma 12

$$LF(x^{n_1}, x^{n_2}) = \text{const} \prod_{\sigma=1}^{s_0} LF_\sigma(x^{v_1}, x^{v_2})^{e_\sigma}, \tag{78}$$

the polynomials $LF_\sigma(x^{v_1}, x^{v_2})$ are relatively prime in pairs and either irreducible or constant.

By Lemma 13, $KF(x^{n_1}, x^{n_2}) = LF(x^{n_1}, x^{n_2})$, thus

$$KF_\sigma(x^{v_1}, x^{v_2}) = LF_s(x^{v_1}, x^{v_2}) \quad (\sigma \leqslant s_0)$$

and we get

$$KF(x^{n_1}, x^{n_2}) = \text{const} \prod_{\sigma=1}^{s_0} KF_\sigma(x^{v_1}, x^{v_2})^{e_\sigma}.$$

If none of $LF_\sigma(x^{v_1}, x^{v_2})$ ($\sigma \leqslant s_0$) is constant we set $\boldsymbol{N} = \boldsymbol{M}$. By (42) and (43), (i) and (ii) hold. As to (iii) it remains to prove $s_0 = s$. Supposing contrariwise that

$$F_s(y_1, y_2) = \pm JF_s(y_1^{-1}, y_2^{-1})$$

we obtain

$$D(z_1, z_2) = JF_s(z_1^{\mu_{22}} z_2^{-\mu_{21}}, z_1^{-\mu_{12}} z_2^{\mu_{11}}) = \pm JF_s(z_1^{-\mu_{22}} z_2^{\mu_{21}}, z_1^{\mu_{12}} z_2^{-\mu_{11}}).$$

On the other hand, by (77), $F_s(y_1, y_2)$ divides $f(y_1^{\mu_{11}} y_2^{\mu_{21}}, y_1^{\mu_{12}} y_2^{\mu_{22}})$ where $f(x_1, x_2)$ is a certain irreducible factor of $KF(x_1, x_2)$. By the assumption $KF(x_1, x_2) = LF(x_1, x_2)$ we have

$$\big(f(x_1, x_2), Jf(x_1^{-1}, x_2^{-1})\big) = 1 \quad \text{and} \quad \big(JF(z_1^{|\boldsymbol{M}|}, z_2^{|\boldsymbol{M}|}), JF(z_1^{-|\boldsymbol{M}|}, z_2^{-|\boldsymbol{M}|})\big) = 1.$$

On substituting $y_1 = z_1^{\mu_{22}} z_2^{-\mu_{21}}$, $y_2 = z_1^{-\mu_{12}} z_2^{\mu_{11}}$ we infer that $D(z_1, z_2)$ divides $JF(z_1^{|\boldsymbol{M}|}, z_2^{|\boldsymbol{M}|})$ and $JF(z_1^{-|\boldsymbol{M}|}, z_2^{-|\boldsymbol{M}|})$, thus $D(z_1, z_2) = \text{const}$ and since the substitution is invertible ($|\boldsymbol{M}| \neq 0$), $F_s(y_1, y_2) = \text{const}$, a contradiction.

If some $LF(x^{v_1}, x^{v_2})$ is constant then we have by Lemma 10

$$\frac{\max\{|v_1|, |v_2|\}}{(v_1, v_2)} \leqslant 2|F_\sigma| \leqslant 4|F|\, h(\boldsymbol{M}). \tag{79}$$

In this case we set $r = 1$,

$$\boldsymbol{N} = \left[\frac{n_1}{(v_1, v_2)}, \frac{n_2}{(v_1, v_2)}\right]$$

so that (ii) is clearly satisfied. By (42), (43) and (79)

$$h(\boldsymbol{N}) \leqslant 8|F|\, h(\boldsymbol{M})^2 \leqslant 8|F| \exp(9 \cdot 2^{\|F\|-3}),$$

thus (i) holds. Finally by (78)

$$KF(x^{n_1/(v_1,v_2)}, x^{n_2/(v_1,v_2)}) = \text{const} \prod_{\sigma=1}^{s_0} KF_\sigma(x^{v_1/(v_1,v_2)}, x^{v_2/(v_1,v_2)})^{e_\sigma},$$

where the polynomials $KF_\sigma(x^{v_1/(v_1,v_2)}, x^{v_2/(v_1,v_2)})$ are relatively prime in pairs and irreducible or constant simultaneously with $KF_\sigma(x^{v_1}, x^{v_2})$. This proves (iii).

Assume now that

$$\frac{\max\{|n_1|, |n_2|\}}{(n_1, n_2)} \leqslant 120(2|F|^*)^{2\|F\|-1} \log \|F\| = m \tag{80}$$

and set

$$F'(x) = JF(x^{n_1/(v_1,v_2)}, x^{n_2/(v_1,v_2)}). \tag{81}$$

Clearly

$$|F'| \leqslant 2|F|\, m$$

and by (8) and (9)

$$\|F'\| \leqslant \max_{0\leqslant\varphi\leqslant 2\pi} |F'(e^{i\varphi})|^2 \leqslant \max_{0\leqslant\vartheta\leqslant 2\pi} |F(e^{i\vartheta_1}, e^{i\vartheta_2})|^2 \leqslant \|F\|^2.$$

Let ξ be a zero of $F'(x)$. If ξ^{-1} is not conjugate to ξ, then by Lemma 1

$$e\big(\xi, \mathbb{Q}(\xi)\big) \leqslant \tfrac{5}{2}|F'| \log \|F'\| \leqslant 10|F|\, m \log \|F\|.$$

If ξ^{-1} is conjugate to ξ, then ξ is a zero of

$$\frac{KF(x^{n_1/(n_1,n_2)}, x^{n_2/(n_1,n_2)})}{LF(x^{n_1/(n_1,n_2)}, x^{n_2/(n_1,n_2)})}$$

and by Lemma 13

$$e\big(\xi, \mathbb{Q}(\xi)\big) \leqslant m.$$

In both cases

$$e\big(\xi, \mathbb{Q}(\xi)\big) \leqslant 600(2|F|^*)^{2\|F\|} \log^2 \|F\|, \tag{82}$$

$$\log e\big(\xi, \mathbb{Q}(\xi)\big) \leqslant 3\|F\|\, |F|^*. \tag{83}$$

Put

$$\nu = \Big(n_1, n_2, \max 2^{e(\xi,\mathbb{Q}(\xi))-1} e\big(\xi, \mathbb{Q}(\xi)\big)!\Big), \quad (n_1, n_2) = \nu v, \tag{84}$$

where the maximum is taken over all zeros ξ of $F(x)$.

It follows like in the proof of Theorem 1 that

$$KF'(x^\nu) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(x)^{e_\sigma}$$

implies

$$KF'(x^{(n_1,n_2)}) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(x^v)^{e_\sigma} \tag{85}$$

(since $v > 0$, $KF_\sigma(x^v) = JF_\sigma(x^v) = F_\sigma(x^v)$). Set

$$\boldsymbol{N} = \left[\frac{n_1}{(n_1,n_2)}, \frac{n_2}{(n_1,n_2)}\right]v.$$

We get from (80), (82), (83) and (84)

$$\begin{aligned} h(\boldsymbol{N}) &\leqslant m \max e\big(\xi, \mathbb{Q}(\xi)\big)^{e(\xi,\mathbb{Q}(\xi))} \\ &\leqslant \exp\big\{3\|F\|\,|F|^* + 900(2|F|^*)^{2\|F\|+1}\|F\|\log^2\|F\|\big\} \\ &\leqslant \exp\big\{500(2|F|^*)^{2\|F\|+1}\|F\|^2\big\}, \end{aligned}$$

thus (i) holds. (ii) is clear from (84). Finally by (81)

$$KF(x^{v_{11}}, x^{v_{12}}) = KF'(x^v), \quad KF(x^{n_1}, x^{n_2}) = KF'(x^{(n_1,n_2)})$$

and (iii) follows from (85). □

5.

Lemma 14. *If $k \geqslant 2$, $a_j \neq 0$ $(0 \leqslant j \leqslant k)$ are complex numbers and $\boldsymbol{M} = [\mu_{ij}]$ is an integral nonsingular matrix of degree k then*

$$J\left(a_0 + \sum_{j=1}^{k} a_j \prod_{i=1}^{k} z_i^{\mu_{ij}}\right)$$

is absolutely irreducible.

Proof. We may assume without loss of generality that $|\boldsymbol{M}| > 0$. Suppose that there is a factorization

$$J\left(a_0 + \sum_{j=1}^{k} a_j \prod_{i=1}^{k} z_i^{\mu_{ij}}\right) = T(z_1, \ldots, z_k)U(z_1, \ldots, z_k),$$

where $T \neq \text{const}$, $U \neq \text{const}$.

Setting

$$z_i = \prod_{h=1}^{k} y_h^{\mu'_{hi}}, \quad \text{where} \quad [\mu'_{hi}] = |\boldsymbol{M}| \cdot \boldsymbol{M}^{-1}$$

we obtain

$$a_0 + \sum_{j=1}^{k} a_j y_j^{|\boldsymbol{M}|} = T'(y_1, \ldots, y_k)U'(y_1, \ldots, y_k), \tag{86}$$

where

$$T' = JT\left(\prod_{h=1}^{k} y_h^{\mu'_{h1}}, \ldots, \prod_{h=1}^{k} y_h^{\mu'_{hk}}\right) \neq \text{const},$$

$$U' = JU\left(\prod_{h=1}^{k} y_h^{\mu'_{h1}}, \ldots, \prod_{h=1}^{k} y_h^{\mu'_{hk}}\right) \neq \text{const}.$$

However (86) is impossible since as follows from Capelli's theorem already

$$a_0 + a_1 y_1^{|\boldsymbol{M}|} + a_2 y_2^{|\boldsymbol{M}|}$$

is absolutely irreducible (cf. [14]). □

Remark. The following generalization of the lemma seems plausible.

If $a_j \neq 0\,(0 \leqslant j \leqslant k)$ are complex numbers and the rank of an integral matrix $[\mu_{ij}]_{\substack{i \leqslant l \\ j \leqslant k}}$ exceeds $(k+1)/2$, then

$$J\left(a_0 + \sum_{j=1}^{k} a_j \prod_{i=1}^{l} z_i^{\mu_{ij}}\right)$$

is absolutely irreducible.

Proof of Theorem 4. Set in Lemma 12:

$$F(x_1, \ldots, x_k) = a_0 + \sum_{j=1}^{k} a_j x_j$$

and let $\boldsymbol{M}$ be the matrix of that lemma. Since by Lemma 14

$$JF\left(\prod_{i=1}^{k} y_i^{\mu_{i1}}, \ldots, \prod_{i=1}^{k} y_i^{\mu_{ik}}\right)$$

is irreducible, we conclude that either $LF(x^{n_1}, \ldots, x^{n_k})$ is irreducible or constant or $\boldsymbol{\gamma n} = 0$ with

$$0 < h(\boldsymbol{\gamma}) < \begin{cases} 120(2|F|^*)^{2\|F\|-1} \log \|F\| & \text{if } k = 2, \\ \exp_{2k-4}(9k|F|^{*\|F\|-1} \log \|F\|) & \text{if } k > 2. \end{cases}$$

If however $LF(x^{n_1}, \ldots, x^{n_k})$ is constant we obtain the relation $\boldsymbol{\gamma n} = 0$ from Lemma 10. Taking into account that $|F|^* = 2$, $\|F\| = \sum_{j=0}^{k} a_j^2$, we get the theorem. □

Proof of Theorem 5. It follows from Theorem 4 that $L(ax^n + bx^m + c)$ is irreducible unless

$$\frac{\max\{n, m\}}{(n, m)} \leqslant 2^{4(a^2+b^2+c^2)+5} \log(a^2 + b^2 + c^2).$$

On the other hand, by Lemma 13 (with $F(x_1, x_2) = ax_1 + bx_2 + c$)

$$K(ax^n + bx^m + c) = L(ax^n + bx^m + c)$$

unless

$$\begin{aligned}\frac{\max\{n, m\}}{(n, m)} &\leqslant 120 \cdot 4^{2(a^2+b^2+c^2)-1} \log(a^2 + b^2 + c^2) \\ &\leqslant 2^{4(a^2+b^2+c^2)+5} \log(a^2 + b^2 + c^2).\end{aligned}$$

This proves the first part of the theorem. To obtain the second part we apply Theorem 3 with $F(x_1, x_2) = ax_1 + bx_2 + c$. In view of Lemma 14 and the reducibility of $K(ax^n + bx^m + c)$, the matrix $\boldsymbol{N}$ is of rank 1 and we have

$$h(\boldsymbol{N}) \leqslant \exp\bigl\{500(2|F|^*)^{2\|F\|+1}\|F\|^2\bigr\} \leqslant \exp\bigl(2^{4(a^2+b^2+c^2)+11}(a^2 + b^2 + c^2)^2\bigr). \quad \square$$

Note added in proof. The original result of [1] concerning an algebraic integer α of degree n is

$$\boxed{\alpha} > 1 + (40n^2 \log n)^{-1} \quad (n > 1).$$

This implies the inequality

$$\boxed{\alpha} > 1 + (40n^2 \log n^* - 1)^{-1}$$

used in the proof of Lemma 1 since $40n^2 \log(n^*/n) > 1$ for $n > 1$. For completeness we list below the modifications needed in [3] in order to obtain the inequality

$$\boxed{\alpha} > 1 + (5n - 1)^{-1}$$

used in the same proof.

Inequality (2.4) should be replaced by

$$1 < \varrho \leqslant 1 + \frac{1}{5n - 1}$$

(this is permissible since $\varrho = 5n/(5n - 1)$ satisfies (2.1)). The right hand side of (3.2) should be replaced by $(\delta e^{1/e})^n$ (this is permissible since $t^{1/t} \leqslant e^{1/e}$ for all $t > 0$). Inequality (4.4) and the preceding formula should be replaced by

$$\delta = \Bigl(1 + \frac{1}{5n - 1}\Bigr)^2 - 1 = \frac{10n - 1}{(5n - 1)^2}, \quad \Pi_1 \leqslant (\delta e^{1/e})^n.$$

The two inequalities following (4.5) should be replaced by

$$\begin{aligned}\varrho^{2n(n-1)} &\leqslant \Bigl(1 + \frac{1}{5n - 1}\Bigr)^{2n(n-1)} \leqslant e^{2n/5}, \\ \Pi_1\Pi_2 &< (n\delta e^{1/e+2/5})^n < 1 \quad (n > 2).\end{aligned}$$

For $n = 2$ the lemma is true because then $\boxed{\alpha} \geqslant \sqrt{2}$.

References

[1] P. E. Blanksby, H. L. Montgomery, *Algebraic integers near the unit circle*. Acta Arith. 18 (1971), 355–369.

[2] J. W. S. Cassels, *An Introduction to Diophantine Approximation*. Cambridge Univ. Press, Cambridge 1957.

[3] —, *On a problem of Schinzel and Zassenhaus*. J. Math. Sci. 1 (1966), 1–8.

[4] W. Ljunggren, *On the irreducibility of certain trinomials and quadrinomials*. Math. Scand. 8 (1960), 65–70.

[5] M. Marden, *Geometry of Polynomials*. Amer. Math. Soc., Providence 1966.

[6] O. Perron, *Algebra* I. Walter de Gruyter, Berlin 1951.

[7] R. Remak, *Elementare Abschätzungen von Fundamentaleinheiten und des Regulators eines algebraischen Zahlkörpers*. J. Reine Angew. Math. 165 (1931), 159–179.

[8] J. B. Rosser, L. Schoenfeld, *Approximate formulas for some functions of prime numbers*. Illinois J. Math. 6 (1962), 64–94.

[9] A. Schinzel, *On the reducibility of polynomials and in particular of trinomials*. Acta Arith. 11 (1965), 1–34; *Errata*, ibid., 491; this collection: D2, 301–332.

[10] W. M. Schmidt, *A problem of Schinzel on lattice points*. Acta Arith. 15 (1968), 199–203.

[11] E. G. Straus, *Rational dependence in finite sets of numbers*. Acta Arith. 11 (1965), 203–204.

[12] N. Tschebotaröw, *Grundzüge der Galoisschen Theorie*. Übersetzt und bearbeitet von H. Schwerdtfeger, Noordhoff, Groningen–Djakarta 1950.

[13] H. Tverberg, *On the irreducibility of the trinomials* $x^n \pm x^m \pm 1$. Math. Scand. 8 (1960), 121–126.

[14] —, *A remark on Ehrenfeucht's criterion for irreducibility of polynomials*. Prace Mat. 8 (1964), 117–118.

Originally published in
Acta Arithmetica XVI (1970), 371–392

Reducibility of lacunary polynomials II

To the memory of my teachers
Wacław Sierpiński and Harold Davenport

This paper is based on the results of [6] and the notation of that paper is retained. In particular $|f|$ is the degree of a polynomial $f(x)$ and $\|f\|$ is the sum of squares of the coefficients of f, supposed rational.

The aim of the paper is to prove the following theorem.

Theorem. *For any non-zero integers A, B, and any polynomial $f(x)$ with integral coefficients, such that $f(0) \neq 0$ and $f(1) \neq -A-B$, there exist infinitely many irreducible polynomials $Ax^m + Bx^n + f(x)$ with $m > n > |f|$. One of them satisfies*

$$m < \exp\big((5|f| + 2\log|AB| + 7)(\|f\| + A^2 + B^2)\big).$$

Corollary. *For any polynomial $f(x)$ with integral coefficients there exist infinitely many irreducible polynomials $g(x)$ with integral coefficients such that*

$$\|f - g\| \leqslant \begin{cases} 2 & \text{if } f(0) \neq 0, \\ 3 & \text{always.} \end{cases}$$

One of them, g_0, satisfies $|g_0| < \exp\big((5|f| + 7)(\|f\| + 3)\big)$.

The example $A = 12$, $B = 0$, $f(x) = 3x^9 + 8x^8 + 6x^7 + 9x^6 + 8x^4 + 3x^3 + 6x + 5$ taken from [4], p. 4 ([1]), shows that in the theorem above it would not be enough to assume $A^2 + B^2 > 0$. On the other hand, in the first assertion of Corollary the constant 2 can probably be replaced by 1, but this was deduced in [5] from a hypothetical property of covering systems of congruences. Corollary gives a partial answer to a problem of Turán (see [5]). The complete answer would require $|g_0| \leqslant \max\{|f|, 1\}$.

Lemma 1. *If $\sum_{\nu=1}^{k} a_\nu \zeta_l^{\alpha_\nu} = 0$, where a_ν, α_ν are integers, then either the sum $\sum$ can be divided into two vanishing summands or for all $\mu \leqslant \nu \leqslant k$*

$$l \mid (\alpha_\mu - \alpha_\nu) \exp \vartheta(k).$$

([1]) Page 304 in this collection.

Proof. This is the result of Mann [2] stated in a form more convenient for our applications. If $\sum$ cannot be divided into two vanishing summands, the relation $\sum = 0$ is in Mann's terminology irreducible. Then according to his Theorem 1 there are distinct primes $p_1, p_2, \ldots, p_s$ where $p_1 < p_2 < \ldots < p_s \leqslant k$ and $p_1 p_2 \cdots p_s$th roots of unity η_ν such that

$$\zeta_l^{\alpha_\nu} = \eta_\nu \zeta, \quad 1, \ldots, k.$$

Hence we get

$$l \mid (\alpha_\mu - \alpha_\nu) p_1 p_2 \cdots p_s \quad (1 \leqslant \mu \leqslant \nu \leqslant k)$$

and since $p_1 p_2 \cdots p_s \mid \exp \vartheta(k)$ the lemma follows. □

Lemma 2. *Let A, B, f satisfy the assumptions of the theorem and besides $|f| > 0$, $f(x) \neq \varepsilon A x^q + \eta B x^r$ ($\varepsilon = \pm 1,\ \eta = \pm 1$). Then there exists an integer d such that*

$$d < \exp \tfrac{5}{2}|f| \tag{1}$$

and

$$A\zeta_l^m + B\zeta_l^n + f(\zeta_l) = 0 \tag{2}$$

implies $l \mid d$.

Proof. Set

$$d = \exp \psi(|f|) \exp \vartheta(|f| + 3).$$

By the inequality $\vartheta(x) \leqslant \psi(x) < 1.04x$ (see [3], Theorem 12) it follows that $d \leqslant \exp \frac{5}{2}|f|$ for $|f| > 7$ and for $|f| \leqslant 7$ the same can be verified directly. Assume now (2). Setting $f(x) = \sum_{i=0}^{|f|} a_i x^i$ we get

$$S = A\zeta_l^m + B\zeta_l^n + \sum_{i=0}^{|f|} a_i \zeta_l^i = 0.$$

The sum S can be divided into a certain number $\geqslant 1$ of vanishing summands for which further such division is impossible. If at least one summand with k terms, say, contains at least two terms from $f(\zeta_l), a_q \zeta_l^q$ and $a_r \zeta_l^r$ ($q \neq r$), say, then by Lemma 1 $l \mid (q-r) \exp \vartheta(k)$ and since $q - r \mid \exp \psi(|f|), k \leqslant |f| + 3$, we get $l \mid d$.

If each summand contains at most one term from $f(\zeta_l)$, then since each term is contained in a certain summand the number of terms in $f(\zeta_l)$ is at most two. Since $|f| > 0$, $f(0) \neq 0$ the number of terms is exactly two,

$$f(x) = a_q x^q + a_r x^r, \quad \text{and} \quad A\zeta_l^m + a_q \zeta_l^q = B\zeta_l^n + a_r \zeta_l^r = 0 \quad (q \neq r).$$

It follows hence $a_q = \varepsilon A$, $a_r = \eta B$, $\varepsilon = \pm 1$, $\eta = \pm 1$; $f(x) = \varepsilon A x^q + \eta B x^r$, contrary to the assumption. □

Lemma 3. *If A, B are integers, $0 < |A| \leqslant |B|$, $\varepsilon = \pm 1$, $\eta = \pm 1$ and*

$$A\zeta_l^m + B\zeta_l^n + \varepsilon A\zeta_l^q + \eta B\zeta_l^r = 0, \tag{3}$$

then either

$$\zeta_l^m + \varepsilon\zeta_l^q = \zeta_l^n + \eta\zeta_l^r = 0 \tag{4}$$

or

$$B = 2\theta A \quad (\theta = \pm 1),$$
$$\zeta_l^m = \varepsilon\zeta_l^q, \quad \{\varepsilon\theta\zeta_l^{n-q}, \varepsilon\eta\theta\zeta_l^{r-q}\} = \{\zeta_3, \zeta_3^2\} \tag{5}$$

or

$$B = \theta A \quad (\theta = \pm 1),$$
$$\zeta_l^n = \eta\zeta_l^r, \quad \{\zeta_l^m, \varepsilon\zeta_l^q\} = \{-\theta\zeta_l^n, -\eta\theta\zeta_l^r\}. \tag{6}$$

Proof. Set $A = (A, B)A_1$, $B = (A, B)B_1$. By (3)

$$A_1(\zeta_l^m + \varepsilon\zeta_l^q) = -B_1(\zeta_l^n + \eta\zeta_l^r)$$

and it follows on taking norms that $B_1^{\varphi(l)}$ divides the norm of $\zeta_l^m + \varepsilon\zeta_l^q$. The latter can be divisible by $\varphi(l)$th power of a prime only when it is 0 or $2^{\varphi(l)}$. Hence we get either (4) or $B_1 = \pm 1$ or $B_1 = \pm 2$, $\zeta_l^m = \varepsilon\zeta_l^q$.

Since $|A_1| \leqslant |B_1|$ and $(A_1, B_1) = 1$ we get besides (4) the two possibilities

$$B = 2\theta A \quad (\theta = \pm 1), \qquad \zeta_l^m = \varepsilon\zeta_l^q, \qquad \varepsilon\zeta_l^q + \theta\zeta_l^n + \theta\eta\zeta_l^r = 0$$

or

$$B = \theta A \quad (\theta = \pm 1), \qquad \zeta_l^m + \theta\zeta_l^n + \varepsilon\zeta_l^q + \theta\eta\zeta_l^r = 0, \qquad \zeta_l^m + \varepsilon\zeta_l^q \neq 0.$$

Taking the complex conjugates we get in the former case

$$\varepsilon\zeta_l^{-q} + \theta\zeta_l^{-n} + \theta\eta\zeta_l^{-r} = 0,$$

in the latter case

$$\zeta_l^{-m} + \theta\zeta_l^{-n} + \varepsilon\zeta_l^{-q} + \theta\eta\zeta_l^{-r} = 0.$$

It follows that the elements of both sets occurring in (5) or (6) have the same non-zero sum and the same sum of reciprocals, hence the sets coincide. □

Lemma 4. *Let A, B, f satisfy the assumptions of the theorem and besides $|A| \leqslant |B|$; $|f| = 0$ or $f(x) = \varepsilon Ax^q + \eta Bx^r$, $\varepsilon = \pm 1$, $\eta = \pm 1$. Then there exist integers a, b, d such that*

$$d \leqslant 3|f| + 3 \tag{7}$$

and $m > 0$, $n > 0$, $m \equiv a$, $n \equiv b \bmod d$ implies

$$K\big(Ax^m + Bx^n + f(x)\big) = Ax^m + Bx^n + f(x). \tag{8}$$

Proof. Assume first that $f(x) = \varepsilon Ax^q + \eta Bx^r$, where $qr = 0$. Since $f(1) \neq -A - B$ it follows

$$\varepsilon = 1 \quad \text{or} \quad \eta = 1. \tag{9}$$

(8) holds unless for some l we have (3). Consider separately four cases

$$B \neq \pm A, \pm 2A, \tag{10}$$

$$B = 2\theta A \quad (\theta = \pm 1), \tag{11}$$

$$B = -A, \tag{12}$$

$$B = A. \tag{13}$$

In case (10) by Lemma 3, (3) implies (4) and by (9) $l \equiv 0 \bmod 2$. We set $d = 2$, $a = q + 1$, $b = r + \dfrac{1-\eta}{2}$. If $m \equiv a \bmod d$ we infer from (4) $\varepsilon = 1$, $l \equiv 2 \bmod 4$, $n \equiv r + \dfrac{l}{2} \cdot \dfrac{1+\eta}{2} \bmod l$, $n \equiv r + \dfrac{1+\eta}{2} \bmod 2$, which contradicts $n \equiv b \bmod d$.

In case (11) by Lemma 3, (3) implies (4) or (5). We set $d = 6, a = q+1, b = r + \dfrac{1-\eta}{2}$. By the argument given above, (4) is impossible. (5) is impossible also since it implies $l \equiv 0$, $m \equiv q \bmod 3$. If $q = r = 0$ it is enough to take $d = 2$, thus (7) holds.

In case (12) by Lemma 3, (3) implies (4) or (6). Since $f(1) \neq -A - B = 0$ we have $\varepsilon = -\eta$. In view of symmetry between q and r we assume $r = 0$ and set

$$d = 2, \quad a = q + \frac{1-\varepsilon}{2}, \quad b = q + \frac{1+\varepsilon}{2} \quad \text{if} \quad q \equiv 0 \bmod 2,$$

$$d = 4, \quad a = q\,\frac{3-\varepsilon}{2}, \quad b = q\,\frac{3+\varepsilon}{2} \quad \text{if} \quad q \equiv 1 \bmod 2.$$

(4) implies $l \equiv 0 \bmod 2$ and

$$m \equiv q + \frac{1+\varepsilon}{2} \cdot \frac{l}{2}, \quad n \equiv \frac{1-\varepsilon}{2} \cdot \frac{l}{2} \bmod l,$$

hence if $m \equiv a \bmod 2$, then $\varepsilon = 1, l \equiv 0 \bmod 4$, and $n \equiv 0 \bmod 4$, contrary to $n \equiv b \bmod d$. (6) implies $l \equiv 0 \bmod 2$ and either $m \equiv n \bmod 2$ or

$$m \equiv \frac{1+\varepsilon}{2} \cdot \frac{l}{2}, \quad n \equiv q + \frac{1-\varepsilon}{2} \cdot \frac{l}{2} \bmod l,$$

hence if $n \equiv b \bmod 2$, then either $m \equiv b \bmod 2$ or $\varepsilon = -1, l \equiv 0 \bmod 4$, and $m \equiv 0 \bmod 4$, contrary to $m \equiv a \bmod d$.

In case (13) by Lemma 3, (3) implies (4) or (6). In view of symmetry between q and r we assume $r = 0$ and set

$$d = 2, \quad a = 0,\ b = q + 1 \quad \text{if} \quad \varepsilon = \eta = 1,$$

$$d = 2q, \quad a = b = 1 \quad \text{if} \quad \varepsilon = 1,\ \eta = -1,$$

$$d = 2q, \quad a = b = q + 1 \quad \text{if} \quad \varepsilon = -1,\ \eta = 1$$

(note that if $\varepsilon = -\eta$ we have $q > 0$ since $f(0) \neq 0$).

If $\varepsilon = \eta = 1$, (4) or (6) implies $l \equiv 0 \bmod 2$, $m + n \equiv q \bmod 2$ which is incompatible with $m \equiv 0$, $n \equiv q + 1 \bmod 2$.

If $\varepsilon = 1$, $\eta = -1$, (4) implies $l \equiv 0 \bmod 2$, $n \equiv 0 \bmod 2$ contrary to $n \equiv b \bmod 2$; (6) implies $l \equiv 0 \bmod 2$, $m \equiv 0 \bmod 2$ or $m - n \equiv \frac{l}{2} \bmod l$, $q \equiv 0 \bmod l$ contrary to $m \equiv a \bmod 2$, $m - n \equiv 0 \bmod q$ (q even).

If $\varepsilon = -1$, $\eta = 1$, (4) implies $l \equiv 0 \bmod 2$, $m \equiv q \bmod l$ contrary to $m \equiv a \bmod 2$; (6) implies $l \equiv 0 \bmod 2$, $n \equiv q \bmod 2$ or $m - n \equiv \frac{l}{2} \bmod l$, $q \equiv 0 \bmod l$ contrary to $n \equiv b \bmod 2$, $m - n \equiv 0 \bmod q$ (q even).

Assume now that $|f| = 0$, $f(x) \neq \varepsilon A + \eta B$. Then by Theorem 4 of [4], (8) holds unless

$$f(x) = \varepsilon A = \eta B, \quad m_1 + n_1 \equiv 0 \bmod 3, \quad \varepsilon^{n_1} = \eta^{m_1},$$

where $m_1 = m/(m,n)$, $n_1 = n/(m,n)$. We set $d = 3$, $a = b = 1$. If $m \equiv a$, $n \equiv b \bmod d$ we have $m + n \not\equiv 0 \bmod 3$ and $m_1 + n_1 \not\equiv 0 \bmod 3$. □

Lemma 5. *Let $D = \{\langle m, n\rangle : 0 \leqslant m < d,\ 0 \leqslant n < d\}$ and let $l_1, \dots, l_k$ be divisors of d relatively prime in pairs. Set*

$$D_{l_j} = \{\langle m, n\rangle : 0 \leqslant m < l_j,\ 0 \leqslant n < l_j\} \quad (1 \leqslant j \leqslant k)$$

and let $S(l_j)$ be a subset of D such that

$$\langle m, n\rangle \in S(l_j), \quad \langle m', n'\rangle \in D \quad \text{and} \quad \langle m, n\rangle \equiv \langle m', n'\rangle \bmod l_j \quad \text{imply} \quad \langle m', n'\rangle \in S(l_j). \tag{14}$$

Then

$$d^{-2}|S(l_j)| = l_j^{-2}\big|S(l_j) \cap D_{l_j}\big|,$$

$$d^{-2}\Big|\bigcap_{j=1}^{k} S(l_j)\Big| = \prod_{j=1}^{k} d^{-2}|S(l_j)|,$$

where $|S|$ is the cardinality of S.

Proof. Set

$$L = l_1 l_2 \cdots l_k, \quad D_0 = \big\{\langle m, n\rangle : 0 \leqslant m < dL^{-1},\ 0 \leqslant n < dL^{-1}\big\}.$$

Choose integers a_j such that

$$a_j \equiv 1 \bmod l_j, \quad a_j \equiv 0 \bmod Ll_j^{-1} \quad (1 \leqslant j \leqslant k).$$

The formula

$$\langle m, n\rangle \equiv \langle m_0, n_0\rangle\, L + \sum_{j=1}^{k} \langle m_j, n_j\rangle a_j \bmod d, \quad \langle m_j, n_j\rangle \in D_{l_j}$$

settles one-to-one correspondence between D and the Cartesian product $D_0 \times D_{l_1} \times \dots \times D_{l_k}$ in such a way that

$$\langle m, n\rangle \equiv \langle m_j, n_j\rangle \bmod l_j.$$

If χ_j is the characteristic function of $S(l_j)$ then by (14)

$$\chi_j(m,n) = \chi_j(m_j, n_j).$$

Hence

$$d^{-2}|S(l_j)| = d^{-2}\sum_{\langle m,n\rangle\in D}\chi_j(m,n) = d^{-2}\sum_{\langle m_0,n_0\rangle\in D_0}\sum\nolimits_1\cdots\sum\nolimits_k\chi_j(m_j,n_j),$$

where $\sum_i$ is taken over all $\langle m_i, n_i\rangle \in D_{l_i}$ and

$$d^{-2}|S(l_j)| = d^{-2}|D_0|\prod_{i=1,i\neq j}^{k}|D_{l_i}|\sum\nolimits_j\chi_j(m_j,n_j) = l_j^{-2}\big|S(l_j)\cap D_{l_j}\big|.$$

It follows further

$$\begin{aligned}
&d^{-2}\Big|\bigcap_{j=1}^{k}S(l_j)\Big| \\
&= d^{-2}\sum_{\langle m,n\rangle\in D}\prod_{j=1}^{k}\chi_j(m,n) = d^{-2}\sum_{\langle m_0,n_0\rangle\in D_0}\sum\nolimits_1\cdots\sum\nolimits_k\prod_{j=1}^{k}\chi_j(m_j,n_j) \\
&= d^{-2}|D_0|\prod_{j=1}^{k}\sum\nolimits_j\chi_j(m_j,n_j) = L^{-2}\prod_{j=1}^{k}\big|S(l_j)\cap D_{l_j}\big| = \prod_{j=1}^{k}d^{-2}|S(l_j)|. \qquad \square
\end{aligned}$$

Lemma 6. *The following inequalities hold*

$$\prod_{p=3}^{\infty}\Big(1+\frac{p}{p^3-p^2-2p+1}\Big) < 1.376, \quad \sum_{p=3}^{\infty}\frac{p}{p^3-p^2-2p+1} > 0.3435, \tag{15}$$

$$\prod_{p=3}^{\infty}\Big(1+\frac{p}{p^3-p^2-3p+1}\Big) < 1.459, \quad \sum_{p=3}^{\infty}\frac{p}{p^3-p^2-3p+1} > 0.4165, \tag{16}$$

$$\prod_{p=3}^{\infty}\Big(1-\frac{2(p^2-1)}{p(p^3-p^2-3p+1)}\Big) > 0.3683, \quad \sum_{p=3}^{\infty}\frac{p^2-1}{p(p^3-p^2-3p+1)} > 0.3804, \tag{17}$$

where p runs over primes.

Proof. We have for $p \geqslant 11$ and $c = 2$ or 3

$$\frac{1}{p^2}+\frac{1}{p^3}+\frac{c+1}{p^4} < \frac{p}{p^3-p^2-cp+1} < \frac{1}{p^2}+\frac{1}{p^3}+\frac{c+2}{p^4},$$

hence

$$\sum_{p=11}^{\infty} p^{-2} + \sum_{p=11}^{\infty} p^{-3} + 3\sum_{p=11}^{\infty} p^{-4} < \sum_{p=11}^{\infty} \frac{p}{p^3 - p^2 - 2p + 1}$$
$$< \sum_{p=11}^{\infty} \log\Big(1 + \frac{p}{p^3 - p^2 - 3p + 1}\Big) < \sum_{p=11}^{\infty} \frac{p}{p^3 - p^2 - 3p + 1}$$
$$< \sum_{p=11}^{\infty} p^{-2} + \sum_{p=11}^{\infty} p^{-3} + 5\sum_{p=11}^{\infty} p^{-4}.$$

Now

$$\sum_{p=11}^{\infty} p^{-2} = \sum_{p=2}^{\infty} p^{-2} - \sum_{p=2}^{7} p^{-2} = 0.452247\ldots - 0.421519\ldots = 0.030728 + \varepsilon_2,$$

$$\sum_{p=11}^{\infty} p^{-3} = \sum_{p=2}^{\infty} p^{-3} - \sum_{p=2}^{7} p^{-3} = 0.174762\ldots - 0.172952\ldots = 0.001810 + \varepsilon_3,$$

$$\sum_{p=11}^{\infty} p^{-4} = \sum_{p=2}^{\infty} p^{-4} - \sum_{p=2}^{7} p^{-4} = 0.076993\ldots - 0.076862\ldots = 0.000131 + \varepsilon_4,$$

where the values of $\sum_{p=2}^{\infty} p^{-i}$ $(i = 2, 3, 4)$ are taken from the tables [1], p. 249, and $|\varepsilon_i| < 10^{-6}$. Hence

$$\sum_{p=11}^{\infty} \log\Big(1 + \frac{p}{p^3 - p^2 - 3p + 1}\Big) < 0.033193 + \varepsilon_2 + \varepsilon_3 + 5\varepsilon_4 < 0.0332,$$

$$\sum_{p=11}^{\infty} \frac{p}{p^3 - p^2 - 2p + 1} > 0.032931 + \varepsilon_2 + \varepsilon_3 + 3\varepsilon_4 > 0.0329.$$

On the other hand,

$$\sum_{p=3}^{7} \log\Big(1 + \frac{p}{p^3 - p^2 - 2p + 1}\Big) < 0.2858, \quad \sum_{p=3}^{7} \frac{p}{p^3 - p^2 - 2p + 1} > 0.3106,$$

$$\sum_{p=3}^{7} \log\Big(1 + \frac{p}{p^3 - p^2 - 3p + 1}\Big) < 0.3442, \quad \sum_{p=3}^{7} \frac{p}{p^3 - p^2 - 3p + 1} > 0.3836,$$

hence

$$\sum_{p=3}^{\infty} \log\Big(1 + \frac{p}{p^3 - p^2 - 2p + 1}\Big) < 0.3190, \quad \sum_{p=3}^{\infty} \frac{p}{p^3 - p^2 - 2p + 1} > 0.3435,$$

$$\sum_{p=3}^{\infty} \log\Big(1 + \frac{p}{p^3 - p^2 - 3p + 1}\Big) < 0.3774, \quad \sum_{p=3}^{\infty} \frac{p}{p^3 - p^2 - 3p + 1} > 0.4165,$$

which implies (15) and (16).

In order to prove (17) we notice that for $p \geqslant 11$

$$\log\Big(1 - \frac{2(p^2-1)}{p(p^3 - p^2 - 3p + 1)}\Big) > -\frac{2(p^2-1)}{p(p^3 - p^2 - 3p + 1)} > -\frac{2}{p^2} - \frac{2}{p^3} - \frac{13}{p^4},$$

$$\frac{p^2-1}{p(p^3 - p^2 - 3p + 1)} > \frac{1}{p^2} + \frac{1}{p^3} + \frac{3}{p^4},$$

hence

$$\sum_{p=11}^{\infty} \log\Big(1 - \frac{2(p^2-1)}{p(p^3 - p^2 - 3p + 1)}\Big) > -2\sum_{p=11}^{\infty} p^{-2} - 2\sum_{p=11}^{\infty} p^{-3} - 13\sum_{p=11}^{\infty} p^{-4}$$

$$= -0.066779 - 2\varepsilon_2 - 2\varepsilon_3 - 13\varepsilon_4 > -0.0668,$$

$$\sum_{p=11}^{\infty} \frac{p^2-1}{p(p^3 - p^2 - 3p + 1)} > \sum_{p=11}^{\infty} p^{-2} + \sum_{p=11}^{\infty} p^{-3} + 3\sum_{p=11}^{\infty} p^{-4}$$

$$= 0.032931 + \varepsilon_2 + \varepsilon_3 + 3\varepsilon_4 > 0.0329.$$

On the other hand,

$$\sum_{p=3}^{7} \log\Big(1 - \frac{2(p^2-1)}{p(p^3 - p^2 - 3p + 1)}\Big) > -0.9319,$$

$$\sum_{p=3}^{7} \frac{p^2-1}{p(p^3 - p^2 - 3p + 1)} > 0.3475,$$

whence

$$\sum_{p=3}^{\infty} \log\Big(1 - \frac{2(p^2-1)}{p(p^3 - p^2 - 3p + 1)}\Big) > -0.9987,$$

$$\sum_{p=3}^{\infty} \frac{p^2-1}{p(p^3 - p^2 - 3p + 1)} > 0.3804,$$

which completes the proof. □

Lemma 7. *Let A, B, f satisfy the assumptions of the theorem. Then there exist integers a, b, d such that*

$$d \leqslant 3\exp\tfrac{5}{2}|f| \tag{18}$$

and $m > 0$, $n > 0$, $m \equiv a$, $n \equiv b \bmod d$ implies

$$K\big(Ax^m + Bx^n + f(x)\big) = Ax^m + Bx^n + f(x). \tag{19}$$

Proof. In view of symmetry we can assume $0 < |A| \leqslant |B|$. In virtue of Lemma 4 we can suppose that A, B, f satisfy the assumptions of Lemma 2; set $d = 2d_0$, where d_0 is an integer from that lemma. (18) follows from (1) and (19) holds unless we have (2) for some $l \mid d_0$.

Put

$$D = \big\{\langle m, n\rangle : 0 \leqslant m < d,\ 0 \leqslant n < d\big\},$$
$$D_l = \big\{\langle m, n\rangle : 0 \leqslant m < l,\ 0 \leqslant n < l\big\},$$
$$E_l = \big\{\langle m, n\rangle \in D : A\zeta_l^m + B\zeta_l^n + f(\zeta_l) \neq 0\big\}.$$

If $\langle a, b\rangle \in \bigcap\limits_{l \mid d} E_l$ then $m > 0$, $n > 0$, $m \equiv a$, $n \equiv b \bmod d$ implies (19). Since $f(1) \neq -A - B$ we have $E_1 = D$. We show that $\bigcap\limits_{l \mid d} E \neq \varnothing$ separately in each of the cases (10), (11), (12), (13). In the first two cases we use the inequality

$$\Big|\bigcap_{l \mid d} E_l\Big| \geqslant |D| - \sum_{1 < l \mid d} |D \setminus E_l|,$$

where in virtue of Lemma 5

$$|D \setminus E_l| = d^2 l^{-2}\big|(D \setminus E_l) \cap D_l\big|.$$

In case (10) we have

$$\big|(D \setminus E_l) \cap D_l\big| \leqslant 1.$$

Indeed, if $\langle m, n\rangle \in D \setminus E_l$ and $\langle q, r\rangle \in D \setminus E_l$ we get

$$A\zeta_l^m + B\zeta_l^n - A\zeta_l^q - B\zeta_l^r = 0, \tag{20}$$

hence by Lemma 3 with $\varepsilon = \eta = -1$, $\zeta_l^m - \zeta_l^q = \zeta_l^n - \zeta_l^r = 0$; $\langle m, n\rangle \equiv \langle q, r\rangle \bmod l$. Therefore,

$$d^{-2}\Big|\bigcap_{l \mid d} E_l\Big| \geqslant 1 - \sum_{1 < l \mid d} l^{-2} > 2 - \sum_{l=1}^{\infty} l^{-2} = 2 - \frac{\pi^2}{6} > 0.$$

In case (11) we have

$$\big|(D \setminus E_l) \cap D_l\big| \leqslant \begin{cases} 1 & \text{if } l \not\equiv 0 \bmod 6, \\ 2 & \text{if } l \equiv 0 \bmod 6. \end{cases}$$

Indeed, if $\langle m, n\rangle \in D \setminus E_l$ and $\langle q, r\rangle \in D \setminus E_l$ we get again (20) and hence it follows by Lemma 3 that

$$\zeta_l^m - \zeta_l^q = \zeta_l^n - \zeta_l^r = 0 \quad \text{or} \quad \zeta_l^m = -\zeta_l^q,$$
$$\{-\theta\zeta_l^{n-q}, \theta\zeta_l^{r-q}\} = \{\zeta_3, \zeta_3^2\};$$
$$\langle m, n\rangle \equiv \langle q, r\rangle \bmod l \quad \text{or} \quad l \equiv 0 \bmod 6,$$
$$\langle m, n\rangle \equiv \langle q + l/2, 2q - r + l/2\rangle \bmod l.$$

Therefore,

$$d^{-2}\Big|\bigcap_{l\,|\,d} E_l\Big| \geqslant 1 - \sum_{1<l\,|\,d} l^{-2} - \sum_{\substack{l\,|\,d \\ l\equiv 0 \bmod 6}} l^{-2} > 2 - \frac{37}{36}\sum_{l=1}^{\infty} l^{-2} = 2 - \frac{37\pi^2}{36\cdot 6} > 0.$$

In case (12) let β be the least exponent such that $f(\zeta_{2^\beta}) = 0$ if such equality is possible, otherwise $\beta = \infty$, $2^{-\beta} = 0$. In the former case $2^\beta \,|\, d$, since $A(\zeta_{2^\beta}^0 - \zeta_{2^\beta}^0) + f(\zeta_{2^\beta}) = 0$. Set

$$E_l'' = \big\{\langle m, n\rangle \in D : m \equiv n \bmod l\big\}$$

and

$$E_l' = \begin{cases} E_l \setminus E_l'' & \text{if } l = 2^\beta \text{ or } l \text{ is an odd prime,} \\ E_l \cup E_l'' & \text{otherwise.} \end{cases}$$

If l has an odd prime factor p then

$$E_l' \cap E_p' \setminus E_l \subset E_l'' \cap E_p' \subset E_l'' \setminus E_p'' = \varnothing.$$

If $l = 2^\alpha$, where $\alpha < \beta$, then by the choice of β

$$E_l' \setminus E_l \subset E_l'' \setminus E_l = \varnothing.$$

If $l = 2^\alpha$, where $\alpha \geqslant \beta$, then

$$E_l' \cap E_{2^\beta}' \setminus E_l \subset E_l'' \cap E_{2^\beta}' \subset E_l'' \setminus E_{2^\beta}'' = \varnothing.$$

Hence $\bigcap_{l\,|\,d} E_l' \subset \bigcap_{l\,|\,d} E_l$ and it remains to estimate $\big|\bigcap_{l\,|\,d} E_l'\big|$. With this end we note that

$$\big|(D \setminus E_l \setminus E_l'') \cap D_l\big| \leqslant \begin{cases} 0 & \text{if } l = 2^\beta, \\ 1 & \text{if } l = 2, \\ (2, l) & \text{otherwise.} \end{cases} \tag{21}$$

Indeed, if $\langle m, n\rangle \in D \setminus E_l \setminus E_l''$, $\langle q, r\rangle \in D \setminus E_l \setminus E_l''$ we have

$$A(\zeta_l^m - \zeta_l^n) + f(\zeta_l) = A(\zeta_l^q - \zeta_l^r) + f(\zeta_l) = 0; \quad m \not\equiv n,\ q \not\equiv r \bmod l, \tag{22}$$

thus (20) holds with $B = -A$, $\zeta_l^m - \zeta_l^n \neq 0$. Hence in virtue of Lemma 3

$$\zeta_l^m = \zeta_l^q,\ \zeta_l^n = \zeta_l^r \quad \text{or} \quad \zeta_l^m = -\zeta_l^r,\ \zeta_l^n = -\zeta_l^q$$

and

$$\begin{gathered} \langle m, n\rangle \equiv \langle q, r\rangle \bmod l \quad \text{or} \quad l \equiv 0 \bmod 2, \\ \langle m, n\rangle \equiv \langle r + l/2, q + l/2\rangle \bmod l. \end{gathered} \tag{23}$$

This gives (21) for $l \neq 2^\beta, 2$. If $l = 2^\beta$ then (22) is impossible, thus $D \setminus E_l \setminus E_l'' = \varnothing$. Finally, if $l = 2$ (22) implies $q \equiv r + 1 \bmod 2$, thus (23) is satisfied by only one residue class $\langle m, n\rangle \bmod 2$.

We have further

$$(*) \qquad \left|E_l'' \cap D_l\right| = l.$$

In virtue of Lemma 5 it follows from (21), (∗) and the definition of E_l' that

$$d^{-2}|D \setminus E_l'| \leqslant \begin{cases} l^{-1} + l^{-2} & \text{if } l \text{ is an odd prime,} \\ l^{-1} & \text{if } l = 2^\beta, \\ 4^{-1} & \text{if } l = 2 \neq 2^\beta, \\ (2,l)l^{-2} & \text{otherwise.} \end{cases}$$

Set $\operatorname{ord}_p d = o_p$. We get

$$d^{-2}\sum_{\alpha=1}^{o_2} |D \setminus E_{2^\alpha}'| < \begin{cases} 2^{-1} + \sum_{\alpha=2}^{\infty} 2^{1-2\alpha} = \frac{2}{3} & \text{if } \beta = 1, \\ 4^{-1} + 2^{-\beta} + \sum_{\substack{\alpha=2 \\ \alpha\neq\beta}}^{\infty} 2^{1-2\alpha} = \frac{5}{12} + 2^{-\beta} - 2^{1-2\beta} < \frac{2}{3} & \text{if } \beta > 1; \end{cases}$$

$$e_2 = d^{-2}\Big|\bigcap_{\alpha=1}^{o_2} E_{2^\alpha}'\Big| \geqslant 1 - d^{-2}\sum_{\alpha=1}^{o_2} |D \setminus E_{2^\alpha}'| > \tfrac{1}{3} = c_2,$$

$$e_p = d^{-2}\Big|\bigcap_{\alpha=1}^{o_p} E_{p^\alpha}'\Big| \geqslant 1 - d^2\sum_{\alpha=1}^{o_p} |D \setminus E_{p_\alpha}'| > 1 - p^{-1} - p^{-2} - \sum_{\alpha=2}^{\infty} p^{-2\alpha}$$

$$= \frac{p^3 - p^2 - 2p + 1}{p(p^2-1)} = c_p \quad (p > 2).$$

On the other hand,

$$\bigcap_{l\,|\,d} E_l' = \bigcap_{p^\alpha\,|\,d} E_{p^\alpha}' \setminus \bigcup\nolimits_1\Big((D \setminus E_l') \cap \bigcap_{\substack{p^\alpha\,|\,d \\ p\,\nmid\, l}} E_{p^\alpha}'\Big),$$

$$\Big|\bigcap_{l\,|\,d} E_l'\Big| \geqslant \Big|\bigcap_{p^\alpha\,|\,d} E_{p^\alpha}'\Big| - \sum\nolimits_1\Big|(D \setminus E_l') \cap \bigcap_{\substack{p^\alpha\,|\,d \\ p\,\nmid\, l}} E_{p^\alpha}'\Big|,$$

where $\bigcup_1$ and $\sum_1$ are taken over all divisors l or d except the prime powers.

The families of sets $\{S(p^{o_p})\}_{p\,|\,d} \cup \{S(l)\}$ and $\{S(p^{o_p})\}_{\substack{p\,|\,d \\ p\,\nmid\, l}}$, where $S(p^{o_p}) = \bigcap_{\alpha=1}^{o_p} E_{p^\alpha}'$, $S(l) = D \setminus E_l$, satisfy the assumptions of Lemma 5, hence

$$d^{-2}\Big|\bigcap_{l\,|\,d} E_l'\Big| \geqslant \prod_{p\,|\,d} e_p - \sum\nolimits_1 d^{-2}|D \setminus E_l'| \prod_{\substack{p\,|\,d \\ p\,\nmid\, l}} e_p = \prod_{p\,|\,d} e_p\Big(1 - \sum\nolimits_1 (l,2)l^{-2}\prod_{p\,|\,l} e_p^{-1}\Big)$$

$$> \prod_{p\,|\,d} e_p\Big(1 - \sum_{l=2}^{\infty}(l,2)l^{-2}\prod_{p\,|\,l} c_p^{-1} + \sum_{p^\alpha > 1}(p^\alpha, 2)\,p^{-2\alpha}c_p^{-1}\Big).$$

The function $(l,2)l^{-2}\prod_{p\mid l}c_p^{-1}$ is multiplicative. Therefore

$$\sum_{l=2}^{\infty}(l,2)l^{-2}\prod_{p\mid l}c_p^{-1}=\prod_{p=2}^{\infty}\Big(1+\sum_{\alpha=1}^{\infty}(p^\alpha,2)p^{-2\alpha}c_p^{-1}\Big)-1$$
$$=3\prod_{p=3}^{\infty}\big(1+c_p^{-1}(p^2-1)^{-1}\big)-1=3\prod_{p=3}^{\infty}\Big(1+\frac{p}{p^3-p^2-2p+1}\Big)-1,$$

$$\sum_{p^\alpha>1}(p^\alpha,2)p^{-2\alpha}c_p^{-1}=\sum_{\alpha=1}^{\infty}2^{1-2\alpha}c_2^{-1}+\sum_{p=3}^{\infty}\sum_{\alpha=1}^{\infty}p^{-2\alpha}c_p^{-1}=2+\sum_{p=3}^{\infty}\frac{p}{p^3-p^2-2p+1}\,.$$

In virtue of Lemma 6 we have

$$4-3\prod_{p=3}^{\infty}\Big(1+\frac{p}{p^3-p^2-2p+1}\Big)+\sum_{p=3}^{\infty}\frac{p}{p^3-p^2-2p+1}>0.2,$$

hence

$$d^{-2}\Big|\bigcap_{l\mid d}E_l'\Big|>0.2d^2\prod_{p\mid d}e_p>0$$

and the proof in case (12) is complete.

In case (13) let β be the least positive exponent such that $f(\zeta_{2^\beta})\neq 0$.

Since for $\beta\geqslant 2$

$$A\big(\zeta_{2^{\beta-1}}^{2^{\beta-2}}+\zeta_{2^{\beta-1}}^{0}\big)+f(\zeta_{2^{\beta-1}})=0,$$

we have $2^{\beta-1}\mid d_0$, hence by the choice of d, $2^\beta\mid d$. We set

$$E_l''=\big\{\langle m,n\rangle\in D: m\equiv n \bmod l\big\},\quad E_l'''=\big\{\langle m,n\rangle\in D: m\equiv n+\tfrac{l}{2} \bmod l\big\},$$

$$E_l'=\begin{cases}E_l'' & \text{if } l=2^\alpha,\ \alpha<\beta,\\ E_l''' & \text{if } l=2^\beta,\\ E_l\setminus E_l'' & \text{if } l \text{ is an odd prime},\\ E_l\cup E_l''' & \text{otherwise.}\end{cases}$$

If l has an odd prime factor p then

$$E_l'\cap E_p'\setminus E_l\subset E_l'''\cap E_p'\subset E_l'''\setminus E_p''=\varnothing.$$

If $l=2^\alpha$, $0<\alpha\leqslant\beta$, $\langle m,n\rangle\in E_l'$, then by the choice of β

$$A\big(\zeta_l^m+\zeta_l^n\big)+f(\zeta_l)=\begin{cases}2A\zeta_l^m\neq 0 & \text{if } \alpha<\beta,\\ f(\zeta_l)\neq 0 & \text{if } \alpha=\beta,\end{cases}$$

thus $E_l'\setminus E_l=\varnothing$.

If $l=2^\alpha$, $\alpha>\beta$, then

$$E_l'\cap E_{2^\beta}'\setminus E_l\subset E_l'''\cap E_{2^\beta}'\subset E_{2^\beta}''\cap E_{2^\beta}'=\varnothing.$$

Hence

$$\bigcap_{l\mid d} E'_l \subset \bigcap_{l\mid d} E_l$$

and it remains to estimate $|\bigcap_{l\mid d} E'_l|$. With this end we note that

(24) $$\left|(D \setminus E_l \setminus E'''_l) \cap D_l\right| \leqslant 2.$$

Indeed, if $\langle m, n\rangle \in D \setminus E_l \setminus E'''_l$, $\langle q, r\rangle \in D \setminus E_l \setminus E'''_l$ we have

$$A(\zeta_l^m + \zeta_l^n) + f(\zeta_l) = A(\zeta_l^q + \zeta_l^r) + f(\zeta_l) = 0; \quad m \not\equiv n + \tfrac{l}{2},\ q \not\equiv r + \tfrac{l}{2} \bmod l,$$

thus (20) holds with $A = B$, $\zeta_l^m + \zeta_l^n \neq 0$. Hence in virtue of Lemma 3

$$\zeta_l^m = \zeta_l^q,\ \zeta_l^n = \zeta_l^r \quad \text{or} \quad \zeta_l^m = \zeta_l^r,\ \zeta_l^n = \zeta_l^q$$

and

(25) $$\langle m, n\rangle \equiv \langle q, r\rangle \quad \text{or} \quad \langle r, q\rangle \bmod l.$$

We have further

(26) $$|E'''_l \cap D_l| \leqslant l, \quad |E'_{2^\beta} \cap D_{2^\beta}| = 2^\beta.$$

In virtue of Lemma 5 it follows from (24), (26) and the definition of E'_l that

(27) $$d^{-2}|D \setminus E'_l| \leqslant \begin{cases} 2l^{-2} & \text{if } l \text{ composite} \neq 2^\alpha\ (\alpha \leqslant \beta), \\ l^{-1} + 2l^{-2} & \text{if } l \text{ prime} > 2. \end{cases}$$

On the other hand, since $E'_{2^\beta} \subset E'_{2^\alpha}$ $(\alpha < \beta)$

$$d^{-2}\Big|\bigcap_{\alpha=1}^{\beta} E'_{2^\alpha}\Big| = d^{-2}|E'_{2^\beta}| = 2^{-\beta}.$$

Set $\operatorname{ord}_p d = o_p$. We get

$$2^{-\beta} = d^{-2}|E'_{2^\beta}| \geqslant e_2 = d^{-2}\Big|\bigcap_{\alpha=1}^{o_2} E'_{2^\alpha}\Big| \geqslant d^{-2}|E'_{2^\beta}| - d^{-2}\sum_{\alpha=\beta+1}^{o_2} |D \setminus E'_{2^\alpha}|$$
$$> 2^{-\beta} - \sum_{\alpha=\beta+1}^{\infty} 2^{1-2\alpha} = 2^{-\beta} - \tfrac{1}{3}\cdot 2^{1-2\beta} = c_2,$$

and for prime $p > 2$

$$e_p = d^{-2}\Big|\bigcap_{\alpha=1}^{o_p} E'_{p^\alpha}\Big| \geqslant 1 - d^{-2}\sum_{\alpha=1}^{o_p} |D \setminus E'_{p^\alpha}| > 1 - p^{-1} - 2\sum_{\alpha=1}^{\infty} p^{-2\alpha}$$
$$= \frac{p^3 - p^2 - 3p + 1}{p(p^2-1)} = c_p.$$

If $l = 2^\alpha l_1$, $\alpha > 0$, l_1 odd > 1 then

$$d^{-2}\big|(D \setminus E'_l) \cap E'_{2^\beta}\big| \leqslant 2^{1-\max(\beta-\alpha,0)} l^{-2}. \tag{28}$$

For $\alpha \geqslant \beta$ the inequality follows at once from (27). In order to show it for $\alpha < \beta$ suppose
c that $\langle q, r\rangle \in D \setminus E'_l$ and set

$$E'_{l,l_1} = \big\{\langle m, n\rangle \in D : \langle m, n\rangle \not\equiv \langle q, r\rangle, \langle r, q\rangle \bmod l_1\big\},$$
$$E'_{l,2^\alpha} = \big\{\langle m, n\rangle \in D : \langle m, n\rangle \not\equiv \langle q, r\rangle, \langle r, q\rangle \bmod 2^\alpha\big\}.$$

Since $\langle m, n\rangle \in D \setminus E'_l$ implies (25) we have

$$D \setminus E'_l \subset (D \setminus E'_{l,l_1}) \cap (D \setminus E'_{l,2^\alpha}).$$

The sets

$$S(l_1) = D \setminus E'_{l,l_1}, \quad S(2^\beta) = (D \setminus E'_{l,2^\alpha}) \cap E'_{2^\beta}$$

satisfy the assumptions of Lemma 5, hence

$$d^{-2}|S(l_1)| = l_1^{-2}|S(l_1) \cap D_{l_1}| \leqslant 2l_1^{-2},$$
$$d^{-2}|S(2^\beta)| = 2^{-2\beta}|S(2^\beta) \cap D_{2^\beta}| = \begin{cases} 0 & \text{if } q \not\equiv r \bmod 2^\alpha, \\ 2^{-\alpha-\beta} & \text{if } q \equiv r \bmod 2^\alpha, \end{cases}$$
$$d^{-2}\big|(D \setminus E'_l) \cap E'_{2^\beta}\big| \leqslant d^{-2}\big|S(l_1) \cap S(2^\beta)\big| = d^{-2}|S(l_1)|\, d^{-2}|S(2^\beta)|,$$

c which implies (28).

Now we have

$$\bigcap_{l\,|\,d} E'_l = \Big(\bigcap_{p^\alpha\,|\,d} E'_{p^\alpha} \cap \bigcap_{2p\,|\,d} E'_{2p}\Big) \setminus \bigcup\nolimits_1 \Big((D \setminus E'_l) \cap \bigcap_{\substack{p^\alpha\,|\,d \\ p\,\nmid\, l}} E'_{p^\alpha}\Big)$$
$$\setminus \bigcup\nolimits_2 \Big((D \setminus E'_l) \cap E'_{2^\beta} \cap \bigcap_{\substack{p^\alpha\,|\,d \\ p\,\nmid\, 2l}} E'_{p^\alpha}\Big),$$

$$d^{-2}\Big|\bigcap_{l\,|\,d} E'_l\Big| \geqslant d^{-2}\Big|\bigcap_{p^\alpha\,|\,d} E'_{p^\alpha} \cap \bigcap_{2p\,|\,d} E'_{2p}\Big| - \sum\nolimits_1 d^{-2}\Big|(D \setminus E_l) \cap \bigcap_{\substack{p^\alpha\,|\,d \\ p\,\nmid\, l}} E'_{p^\alpha}\Big| \tag{29}$$
$$- \sum\nolimits_2 d^{-2}\Big|(D \setminus E'_l) \cap E'_{2^\beta} \cap \bigcap_{\substack{p^\alpha\,|\,d \\ p\,\nmid\, 2l}} E'_{p^\alpha}\Big|,$$

where $\bigcup_1$ and $\sum_1$ are taken over all $l \,|\, d$ such that $l \equiv 1 \bmod 2$, $l \neq 1$, p^α, $\bigcup_2$ and $\sum_2$ are taken over all $l \,|\, d$ such that $l \equiv 0 \bmod 2$, $l \neq 2p$ (p is a prime). $\sum_1$ and $\sum_2$ are estimated easily. Indeed, the family of sets

$$\{S(l)\} \cup \{S(p^{o_p})\}_{p\,|\,d,\ p\,\nmid\, l}, \quad \text{where} \quad S(l) = D_l \setminus E'_l,\ S(p^{o_p}) = \bigcap_{\alpha=1}^{o_p} E'_{p^\alpha},$$

satisfies for each l the assumptions of Lemma 5. Hence by (27)

$$\Sigma_1 = \sum\nolimits_1 d^{-2}|D \setminus E'_l| \prod_{\substack{p\mid d\\ p\nmid l}} e_p \leqslant \prod_{p\mid d} e_p \sum\nolimits_1 2l^{-2} \prod_{p\mid l} e_p^{-1} \leqslant \prod_{p\mid d} e_p \sum\nolimits_1 2l^{-2} \prod_{p\mid l} c_p^{-1}$$

$$< \prod_{p\mid d} e_p \Bigg(\sum_{\substack{l=3\\ l \text{ odd}}}^{\infty} 2l^{-2} \prod_{p\mid l} c_p^{-1} - \sum_{\substack{p^\alpha \geqslant 3\\ p \text{ odd}}} 2p^{-2\alpha} c_p^{-1} \Bigg).$$

The function $l^{-2} \prod\limits_{p\mid l} c_p^{-1}$ is multiplicative and in the set of odd numbers there is the uniqueness of factorization, thus

$$\sum_{\substack{l=3\\ l \text{ odd}}} 2l^{-2} \prod_{p\mid l} c_p^{-1} = 2 \prod_{p=3}^{\infty} \Bigg(1 + \sum_{\alpha=1}^{\infty} p^{-2\alpha} c_p^{-1} \Bigg) - 2 \tag{30}$$

$$= 2 \prod_{p=3}^{\infty} \Big(1 + \frac{p}{p^3 - p^2 - 3p + 1} \Big) - 2,$$

$$\sum_{\substack{p^\alpha \geqslant 3\\ p \text{ odd}}} 2p^{-2\alpha} c_p^{-1} = 2 \sum_{p=3}^{\infty} \sum_{\alpha=1}^{\infty} p^{-2\alpha} c_p^{-1} = 2 \sum_{p=3}^{\infty} \frac{p}{p^3 - p^2 - 3p + 1}\,.$$

We get by Lemma 6

$$\Sigma_1 < \prod_{p\mid d} e_p (2 \cdot 1.459 - 2 - 2 \cdot 0.4165) = 0.085 \prod_{p\mid d} e_p. \tag{31}$$

c

Similarly, the family of sets

$$\big\{ S(2^{\max(\beta-\alpha,0)} l) \big\} \cup \big\{ S(p^{o_p}) \big\}_{p\mid d,\ p\nmid 2l},$$

where $S(2^{\max(\beta-\alpha,0)} l) = (D \setminus E'_l) \cap E'_{2^\beta}$, $S(p^{o_p}) = \bigcap\limits_{\alpha=1}^{o_p} E'_{p^\alpha}$, satisfies for each $l = 2^\alpha l_1$,

c $l_1 > 1$ odd, the assumptions of Lemma 5. Hence by (28)

$$\Sigma_2 = \sum\nolimits_2 d^{-2} \big| (D \setminus E'_l) \cap E'_{2^\beta} \big| \prod_{\substack{p\mid d\\ p\nmid 2l}} e_p \leqslant \prod_{\substack{p\mid d\\ p>2}} e_p \sum\nolimits_2 2^{1-\max(\beta-\alpha,0)} l^{-2} \prod_{p\mid l_1} e_p^{-1}$$

$$< \prod_{\substack{p\mid d\\ p>2}} e_p \Bigg(\sum_{\substack{l_1=3\\ l_1 \text{ odd}}}^{\infty} \sum_{\alpha=1}^{\infty} 2^{1-\max(\beta-\alpha,0)-2\alpha} l_1^{-2} \prod_{p\mid l_1} c_p^{-1} - \sum_{p=3}^{\infty} 2^{-\beta} p^{-2} c_p^{-1} \Bigg).$$

Now

$$\sum_{\alpha=1}^{\infty} 2^{1-\max(\beta-\alpha,0)-2\alpha} = \sum_{\alpha=1}^{\beta} 2^{1-\beta-\alpha} + \sum_{\alpha=\beta+1}^{\infty} 2^{1-2\alpha}$$
$$= 2^{1-\beta} - 2^{1-2\beta} + \tfrac{1}{3}\cdot 2^{1-2\beta} = 2c_2 \leqslant 2e_2.$$

On the other hand, by (30) and Lemma 6

$$\sum_{\substack{l_1=3\\ l_1 \text{ odd}}} 2l_1^{-2} \prod_{p\mid l_1} c_p^{-1} = 2\prod_{p=3}^{\infty}\Big(1+\frac{p}{p^3-p^2-3p+1}\Big) - 2 < 2\cdot 1.459 - 2 = 0.918,$$

$$\sum_{p=3}^{\infty} p^{-2}c_p^{-1} = \sum_{p=3}^{\infty} \frac{p^2-1}{p(p^3-p^2-3p+1)} > 0.3804.$$

Hence

$$\Sigma_2 < \prod_{p\mid d} e_p\Big(0.918 - 2^{-\beta}e_2^{-1}\sum_{p=3}^{\infty} p^{-2}c_p^{-1}\Big) < \prod_{p\mid d} e_p\big(0.918 - 2^{-\beta}e_2^{-1}\cdot 0.38\big). \tag{32}$$

It remains to estimate $\big|\bigcap_{p^\alpha\mid d} E'_{p^\alpha} \cap \bigcap_{2p\mid d} E'_{2p}\big|$. Here we distinguish two cases $\beta = 1$ and $\beta > 1$. If $\beta = 1$ we put

$$E_2^1 = \big\{\langle m,n\rangle \in D : \langle m,n\rangle \equiv \langle 0,1\rangle \bmod 2\big\},$$
$$E_2^2 = \big\{\langle m,n\rangle \in D : \langle m,n\rangle \equiv \langle 1,0\rangle \bmod 2\big\},$$

so that

$$E_2^1 \cup E_2^2 = E'_2, \quad E_2^1 \cap E_2^2 = \varnothing. \tag{33}$$

If $E'_2 \setminus E'_{2p} = \varnothing$ we put further $E^1_{2p,p} = E^2_{2p,p} = D$ (p prime $\geqslant 3$). If $E'_2 \setminus E'_{2p} \neq \varnothing$ let $\langle q,r\rangle \in E'_2 \setminus E'_{2p}$. Then also $\langle r,p\rangle \in E'_2 \setminus E'_{2p}$ and in view of symmetry we may assume $\langle q,r\rangle \in E_2^1$. We set

$$E^1_{2p,p} = \big\{\langle m,n\rangle \in D : \langle m,n\rangle \not\equiv \langle q,r\rangle \bmod p\big\},$$
$$E^2_{2p,p} = \big\{\langle m,n\rangle \in D : \langle m,n\rangle \not\equiv \langle r,q\rangle \bmod p\big\}.$$

Since $\langle m,n\rangle \in D \setminus E'_{2p}$ implies (25) with $l = 2p$, we have

$$E'_2 \cap E'_{2p} = \big(E_2^1 \cap E^1_{2p,p}\big) \cup \big(E_2^2 \cap E^2_{2p,p}\big),$$
$$\bigcap_{p^\alpha\mid d} E'_{p^\alpha} \cap \bigcap_{2p\mid d} E'_{2p} = \bigcap_{p\mid d} S_1(p^{o_p}) \cup \bigcap_{p\mid d} S_2(p^{o_p}), \tag{34}$$

where

$$S_i(2^{o_2}) = E_2^i \cap \bigcap_{\alpha=1}^{o_2} E'_{2^\alpha}, \quad S_i(p^{o_p}) = \bigcap_{\alpha=1}^{o_p} E'_{p^\alpha} \cap E^i_{2p,p} \quad (p \geqslant 3).$$

The family of sets $\{S_i(p^{o_p})\}_{p|d}$ satisfies for $i = 1, 2$ the assumptions of Lemma 5, and by (33) the two summands in (34) are disjoint, hence

$$d^{-2}\Big|\bigcap_{p^\alpha|d} E'_{p^\alpha} \cap \bigcap_{2p|d} E'_{2p}\Big| = \prod_{p|d} d^{-2}|S_1(p^{o_p})| + \prod_{p|d} d^{-2}|S_2(p^{o_p})|.$$

However, by (33)

$$|S_1(2^{o_2})| + |S_2(2^{o_2})| = |S_1(2^{o_2}) \cup S_2(2^{o_2})| = \Big|E'_2 \cap \bigcap_{\alpha=1}^{o_2} E'_{2^\alpha}\Big| = d^2 e_2,$$

and for prime $p > 2$

$$\begin{aligned} d^{-2}|S_i(p^{o_p})| &\geqslant d^{-2}\Big|\bigcap_{\alpha=1}^{o_p} E'_{p^\alpha}\Big| - d^{-2}|D \setminus E^i_{2p,p}| \\ &= e_p - p^{-2}\big|(D \setminus E^i_{2p,p}) \cap D_p\big| \geqslant e_p - p^{-2}. \end{aligned}$$

Hence

$$d^{-2}\Big|\bigcap_{p^\alpha|d} E'_{p^\alpha} \cap \bigcap_{2p|d} E'_{2p}\Big| \geqslant d^{-2}\big(|S_1(2^{o_2})| + |S_2(2^{o_2})|\big) \prod_{\substack{p|d \\ p>2}} (e_p - p^{-2})$$

$$= \prod_{p|d} e_p \cdot \prod_{\substack{p|d \\ p>2}} (1 - p^{-2}e_p^{-1}) > \prod_{p|d} e_p \cdot \prod_{p=3}^{\infty} (1 - p^{-2}c_p^{-1})$$

$$> \prod_{p|d} e_p\Big(1 - \sum_{p=3}^{\infty} p^{-2}c_p^{-1} + 3^{-2}\cdot 5^{-2}c_3^{-1}c_5^{-1}\Big) > \prod_{p|d} e_p\Big(1.014 - \sum_{p=3}^{\infty} p^{-2}c_p^{-1}\Big).$$

It follows from (29), (31) and (32) that

$$d^{-2}\Big|\bigcap_{l|d} E'_l\Big| \geqslant \prod_{p|d} e_p\Big(0.011 - \sum_{p=3}^{\infty} p^{-2}c_p^{-1} + 2^{-\beta}e_2^{-1}\sum_{p=3}^{\infty} p^{-2}c_p^{-1}\Big) > 0.011\prod_{p|d} e_p > 0.$$

If $\beta > 1$, we put

$$\begin{aligned} E_2^1 &= \big\{\langle m, n\rangle \in D : \langle m, n\rangle \not\equiv \langle 0, 0\rangle \bmod 2\big\}, \\ E_2^2 &= \big\{\langle m, n\rangle \in D : \langle m, n\rangle \not\equiv \langle 1, 1\rangle \bmod 2\big\} \end{aligned}$$

so that again (33) holds.

If $p > 2$ is a prime, $E'_{2p} \neq D$ and $\langle q, r\rangle \in D \setminus E'_{2p}$ we set

$$E'_{2p,p} = \big\{\langle m, n\rangle \in D : \langle m, n\rangle \not\equiv \langle q, r\rangle, \langle r, q\rangle \bmod p\big\}$$

and we assign p into class P_0, P_1 or P_2 according to whether $\langle q, r\rangle \notin E'_2$, $\langle q, r\rangle \in E_2^1$ or $\langle q, r\rangle \in E_2^2$, respectively.

Since $\langle m, n\rangle \in D \setminus E'_{2p}$ implies (25) with $l = 2p$, the residue classes of $\langle q, r\rangle$, $\langle r, q\rangle$ $\bmod 2p$ are determined uniquely up to a permutation and sets $E'_{2p,p}$, P_1, P_2 are well

defined. We have

$$E_2' \cap E_{2p}' = \begin{cases} E_2^2 \cup \big(E_2^1 \cap E_{2p,p}'\big) & \text{if } p \in P_1, \\ E_2^1 \cup \big(E_2^2 \cap E_{2p,p}'\big) & \text{if } p \in P_2, \\ E_2' & \text{otherwise.} \end{cases}$$

Hence

$$E_2' \cap \bigcap_{2p\,|\,d} E_{2p}' = \Big(E_2^1 \cap \bigcap_{\substack{2p\,|\,d \\ p\in P_1}} E_{2p,p}'\Big) \cup \Big(E_2^2 \cap \bigcap_{\substack{2p\,|\,d \\ p\in P_2}} E_{2p,p}'\Big)$$

and

$$\bigcap_{p^\alpha\,|\,d} E_{p^\alpha}' \cap \bigcap_{2p\,|\,d} E_{2p}' = \bigcap_{p\,|\,d} S_1(p^{o_p}) \cup \bigcap_{p\,|\,d} S_2(p^{o_p}), \tag{35}$$

where

$$S_i(2^{o_2}) = E_2^i \cap \bigcap_{\alpha=1}^{o_2} E_{2^\alpha}',$$

$$S_i(p^{o_p}) = \begin{cases} E_{2p,p}' \cap \bigcap\limits_{\alpha=1}^{o_p} E_{p^\alpha}' & \text{if } p \in P_i, \\ \bigcap\limits_{\alpha=1}^{o_p} E_{p^\alpha}' & \text{if } p \notin P_i,\ p > 2. \end{cases}$$

The family of sets $\{S_i(p^{o_p})\}_{p\,|\,d}$ satisfies for $i = 1, 2$ the assumptions of Lemma 5 and by (33) the two summands in (35) are disjoint. Hence

$$d^{-2}\Big|\bigcap_{p^\alpha\,|\,d} E_{p^\alpha}' \cap \bigcap_{2p\,|\,d} E_{2p}'\Big| = \prod_{p\,|\,d} d^{-2}|S_1(p^{o_p})| + \prod_{p\,|\,d} d^{-2}|S_2(p^{o_p})|.$$

c

On the other hand,

$$S_i(2^{o_2}) = \bigcap_{\alpha=1}^{o_2} E_{2^\alpha}' \setminus (D \setminus E_2^i) \cap E_{2^\beta}',$$

$$\begin{aligned} d^{-2}|S_i(2^{o_2})| &\geqslant e_2 - d^{-2}\big|(D \setminus E_2^i) \cap E_{2^\beta}'\big| \\ &= e_2 - 2^{-2\beta}\big|(D \setminus E_2^i) \cap E_{2^\beta}' \cap D_{2^\beta}\big| = e_2 - 2^{-\beta-1}, \end{aligned}$$

$$d^{-2}|S_1(2^{o_2})| + d^{-2}|S_2(2^{o_2})| = d^{-2}\big|S_1(2^{o_2}) \cup S_2(2^{o_2})\big| = d^{-2}\Big|\bigcap_{\alpha=1}^{o_2} E_{2^\alpha}'\Big| = e_2,$$

whence

$$d^{-2}|S_i(2^{o_2})| = \frac{e_2}{2}\big(1 + (-1)^i\varepsilon\big) \quad \text{where} \quad |\varepsilon| \leqslant 2^{-\beta}e_2^{-1} - 1.$$

Further, for $p > 2$

$$d^{-2}|S_i(p^{o_p})| \geqslant d^{-2}\Big|\bigcap_{\alpha=1}^{o_p} E'_{p^\alpha}\Big| - d^{-2}\big|D \setminus E'_{2p,p}\big|$$
$$= e_p - p^{-2}\big|(D \setminus E'_{2p,p}) \cap D_p\big| = e_p - 2p^{-2} \quad \text{if} \quad p \in P_i,$$
$$d^{-2}|S_i(p^{o_p})| = e_p \quad \text{if} \quad p \notin P_i.$$

Hence

$$d^{-2}\Big|\bigcap_{p^\alpha|d} E'_{p^\alpha} \cap \bigcap_{2p|d} E'_{2p}\Big| \geqslant \prod_{p|d} e_p\big((\tfrac12 - \tfrac12\varepsilon)\Pi_1 + (\tfrac12 + \tfrac12\varepsilon)\Pi_2\big)$$
$$\geqslant \prod_{p|d} e_p\big(\tfrac12\Pi_1 + \tfrac12\Pi_2 - \tfrac12(2^{-\beta}e_2^{-1} - 1)|\Pi_1 - \Pi_2|\big), \tag{36}$$

where

$$\Pi_i = \prod_{p\in P_i}(1 - 2p^{-2}c_p^{-1}) = \prod_{p\in P_i}\Big(1 - \frac{2(p^2-1)}{p(p^3-p^2-3p+1)}\Big).$$

It follows from Lemma 6 that

$$\Pi_1\Pi_2 \geqslant \prod_{p=3}^{\infty}\Big(1 - \frac{2(p^2-1)}{p(p^3-p^2-3p+1)}\Big) = C > 0.3683$$

and, if $3 \in P_1 \cup P_2$, since $1 - 2\cdot 3^{-2}c_3^{-1} = \frac{7}{15} < \sqrt{C}$ we have

$$\tfrac12|\Pi_1 - C\Pi_1^{-1}| \geqslant \tfrac12(\tfrac{15}{7}C - \tfrac{7}{15}),$$
$$\tfrac12\Pi_1 + \tfrac12\Pi_2 \geqslant \tfrac12\Pi_1 + \tfrac12 C\Pi_1^{-1} = \sqrt{C + \tfrac14(\Pi_1 - C\Pi_1^{-1})^2} \geqslant \tfrac12(\tfrac{15}{7}C + \tfrac{7}{15}) > 0.627.$$

If $3 \notin P_1 \cup P_2$, then $\Pi_1\Pi_2 \geqslant \frac{15}{7}C$, hence

$$\tfrac12\Pi_1 + \tfrac12\Pi_2 \geqslant \sqrt{\Pi_1\Pi_2} \geqslant \sqrt{\tfrac{15}{7}C} > 0.627.$$

On the other hand, in both cases

$$|\Pi_1 - \Pi_2| \leqslant 1 - C < 0.632.$$

It follows from (29), (31), (32) and (36) that

$$d^{-2}\Big|\bigcap_{l|d} E'_l\Big| \geqslant \prod_{p|d} e_p\big(0.627 - (2^{-\beta}e_2^{-1} - 1)0.316 - 1.003 + 2^{-\beta}e_2^{-1}\cdot 0.38\big)$$
$$\geqslant \prod_{p|d} e_p\big(0.004 + (2^{-\beta}e_2^{-1} - 1)0.064\big) > 0.004\prod_{p|d} e_p > 0$$

and the proof is complete. □

Lemma 8. *If $A \neq \pm B$ then each rational factor of $Ax^c + B$ is of degree at least $c\,|AB|^{-1}$.*

Proof. Each zero of $Ax^c + B$ has absolute value $|BA^{-1}|^{1/c}$. Hence any monic factor of $Ax^c + B$ of degree γ has constant term with absolute value $|BA^{-1}|^{\gamma/c}$. If this term is rational we have in the notation in Lemma 1 of [6]

$$c \leqslant e\big(B^\gamma A^{-\gamma}, \mathbb{Q}\big) = \gamma e(BA^{-1}, \mathbb{Q}).$$

However, since either BA^{-1} or $B^{-1}A$ is not an integer we get by that lemma

$$e(BA^{-1}, \mathbb{Q}) = e(B^{-1}A, \mathbb{Q}) \leqslant \frac{\log(A^2 + B^2)}{2\log 2} \leqslant |AB|,$$

$$\gamma \geqslant c|AB|^{-1}. \qquad \square$$

Proof of Theorem. Let a, b, d be integers from Lemma 7 and set

(37) $$c = a - b + d + d\big[d^{-1}(b - a + |f|^*|AB|)\big],$$

(38) $$e = b + d + d\big[-bd^{-1} + d^{-1}\log(\|f\| + A^2 + B^2)120(4c^2 + 8)^{\|f\|+A^2+B^2}\big],$$

where as in [6]

$$|f|^* = \sqrt{\max\{|f|^2, 2\} + 2}\,.$$

It follows

(39) $$c > |f|^*|AB| \geqslant \max(|f|, 2)|AB|,$$

(40) $$e > 120(4c^2 + 8)^{\|f\|+A^2+B^2}\log(\|f\| + A^2 + B^2) > |f|.$$

We note that

(41) $$(Ax^c + B)(A + Bx^c) \neq x^c f(x) f(x^{-1}),$$

(42) $$\big(K(Ax^c + B), Kf(x)\big) = \big(L(Ax^c + B), Lf(x)\big) = 1.$$

(41) follows from (39) by comparison of degrees of both sides, (42) is obvious if $A = \pm B$. If $A \neq \pm B$ any rational factor of $Ax^c + B$ is by Lemma 8 and (39) of degree greater than $|f|$, which implies (42). Assume now

(43) $$n = dt + e \quad (t \geqslant 0)$$

and set in Lemmata 12 and 13 of [6]

$$F(x_1, x_2) = (Ax_2^c + B)x_1 + f(x_2), \quad n_1 = n,\ n_2 = 1.$$

The assumption of Lemma 13 is satisfied since by (41), (42)

$$\frac{F(x_1, x_2)}{KF(x_1, x_2)} = \left(\frac{Ax_2^c + B}{K(Ax_2^c + B)}, \frac{f(x_2)}{Kf(x_2)}\right) = \big(Ax_2^c + B, f(x_2)\big)$$
$$= \left(\frac{Ax_2^c + B}{L(Ax_2^c + B)}, \frac{f(x_2)}{Lf(x_2)}\right) = \frac{F(x_1, x_2)}{LF(x_1, x_2)}\,.$$

In view of (39)

$$|F| = c > 2; \quad |F|^* = \sqrt{c^2 + 2}\,, \quad \|F\| = A^2 + B^2.$$

In view of (40) and (43) the numbers n_1, n_2 do not satisfy any relation $\gamma_1 n_1 + \gamma_2 n_2 = 0$ with

$$0 < \max\{|\gamma_1|, |\gamma_2|\} \leqslant 120(2|F|^*)^{2\|F\|} \log \|F\|.$$

c Therefore, by Lemma 12 of [6] there is an integral matrix $\boldsymbol{M} = [\mu_{ij}]$ of order 2 such that

$$0 \leqslant \mu_{21} < \mu_{11}, \quad 0 = \mu_{12} < \mu_{22}, \tag{44}$$

$$[n, 1] = [v_1, v_2]\boldsymbol{M} \tag{45}$$

and

$$L\big((Ay_2^{c\mu_{22}} + B)y_1^{\mu_{11}} y_2^{\mu_{21}} + f(y_2^{\mu_{22}})\big) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(y_1, y_2)^{e_\sigma} \tag{46}$$

c

implies

$$L\big(Ax^{n+c} + Bx^n + f(x)\big) = \text{const} \prod_{\sigma=1}^{s} LF_\sigma(x^{v_1}, x^{v_2})^{e_\sigma},$$

where polynomials $LF_\sigma(x^{v_1}, x^{v_2})$ $(\sigma \leqslant s)$ are either irreducible or constant.

c Now by (44) and (45) $\mu_{22} = 1$ and the left hand side of (46) becomes $L\big((Ay_2^c + B)y_1^{\mu_{11}} y_2^{\mu_{21}} + f(y_2)\big)$ which itself is not reducible.

Indeed, since $c > |f|$ and $Ay_2^c + B$ has no multiple factors

$$\pm\frac{f(y_2)}{y_2^{\mu_{21}}(Ay_2^c + B)}$$

is not a power in the field $\mathbb{Q}(y_2)$ and by Capelli's theorem

$$y_1^{\mu_{11}} + \frac{f(y_2)}{y_2^{\mu_{21}}(Ay_2^c + B)}$$

is irreducible in this field. It follows that

$$\frac{(Ay_2^c + B)y_1^{\mu_{11}} y_2^{\mu_{21}} + f(y_2)}{\big((Ay_2^c + B)y_2^{\mu_{21}}, f(y_2)\big)}$$

is irreducible. Since by (42) and $f(0) \neq 0$

$$\big(L(Ay_2^c + B)y_2^{\mu_{21}}, Lf(y_2)\big) = 1,$$

we have on the right hand side of (46) $s = 0$ or $s = e_1 = 1$. We infer that $L\big(Ax^{n+c} + Bx^n + f(x)\big)$ is not reducible. By Lemma 13 of [6] we have

$$L\big(Ax^{n+c} + Bx^n + f(x)\big) = K\big(Ax^{n+c} + Bx^n + f(x)\big).$$

Finally by (37), (38) and (43) $n + c \equiv a, n \equiv b \bmod d$ and by Lemma 7

$$K\big(Ax^{n+c} + Bx^n + f(x)\big) = Ax^{n+c} + Bx^n + f(x),$$

thus $Ax^m + Bx^n + f(x)$ is irreducible for any $m = n + c, n = dt + e$ $(t \geqslant 0)$. By (40)

we have $n > |f|$. On the other hand, by (18) and (37)

$$c \leqslant |f|^*|AB| + d \leqslant |f|^*|AB| + 3\exp\tfrac{5}{2}|f| \leqslant 5\exp\big(\tfrac{5}{2}|f| + \log|AB|\big)$$

and for $t = 0$ we get by (18) and (38)

$$\begin{aligned} m = c + e &\leqslant c + d + \log\big(\|f\| + A^2 + B^2\big)120(4c^2 + 8)^{\|f\|+A^2+B^2} \\ &\leqslant 8\exp\big(\tfrac{5}{2}|f| + \log|AB|\big) + 6^{\|f\|+A^2+B^2}\big(108\exp(5|f| + 2\log|AB|)^{\|f\|+A^2+B^2}\big) \\ &< \exp\big((5|f| + 2\log|AB| + 7)(\|f\| + A^2 + B^2)\big). \end{aligned}$$

The proof is complete. □

Proof of Corollary. If $f(0) \neq 0$ we set $g(x) = Ax^n + Bx^m + f(x)$ and apply Theorem with $A = B = 1$ if $f(1) \neq -2$, with $A = -B = 1$ if $f(1) = -2$.

The inequality for $|g_0|$ follows, even with $\|f\| + 3$ replaced by $\|f\| + 2$.

If $f(0) = 0$ we set $g(x) = Ax^n + Bx^m + f(x) + 1$ and apply Theorem with $A = B = 1$ if $f(1) \neq -3$, with $A = -B = 1$ if $f(1) = -3$.

If $f(x) \not\equiv 0$ we have $|f(x) + 1| = |f|$, $\|f(x) + 1\| = \|f\| + 1$, which implies the inequality for $|g_0|$. If $f(x) \equiv 0$, $|f| = -\infty$, we set $g_0(x) = x$. □

References

[1] H. T. Davis, *Tables of Higher Mathematical Functions*, vol. II. Principia Press, Bloomington 1935.

[2] H. B. Mann, *On linear relations between roots of unity*. Mathematika 12 (1965), 107–117.

[3] J. B. Rosser, L. Schoenfeld, *Approximate formulas for some functions of prime numbers*. Illinois J. Math. 6 (1962), 64–94.

[4] A. Schinzel, *On the reducibility of polynomials and in particular of trinomials*. Acta Arith. 11 (1965), 1–34; *Errata*, ibid., 491; this collection: D2, 301–332.

[5] —, *Reducibility of polynomials and covering systems of congruences*. Acta Arith. 13 (1967), 91–101; this collection: D3, 333–343.

[6] —, *Reducibility of lacunary polynomials* I. Acta Arith. 16 (1969), 123–159; *Corrigenda*: Acta Arith. 19 (1971), 201; ibid. 24 (1978), 265; this collection: D4, 344–380.

Originally published in
Acta Arithmetica XIX (1971), 195–201

A note on the paper "Reducibility of lacunary polynomials I"

with J. Wójcik (*Warszawa*)

In the paper [1] mentioned in the title the first writer has left a gap in the proof of Lemma 1. The aim of this note is to fill this gap by proving a property of normal number fields which may be of independent interest.

Let $\boldsymbol{\Omega}$ be a number field of degree $|\boldsymbol{\Omega}|$, $\alpha \in \boldsymbol{\Omega}$, $\alpha \neq 0$. We denote by ζ_q a primitive qth root of unity and set following [1]

$$e(\alpha, \boldsymbol{\Omega}) = \begin{cases} 0 \text{ if } \alpha = \zeta_q \text{ for some } q, \\ \text{maximal } e \text{ such that } \alpha = \zeta_q \beta^e \text{ with suitable } q \text{ and } \beta \in \boldsymbol{\Omega}, \text{ otherwise.} \end{cases}$$

It is asserted in Lemma 1 of [1] that if $\alpha \neq 0$, $f(\alpha) = 0$, where $f(x) = \sum_{i=0}^{m} a_i x^i$ is a polynomial with integral coefficients and $\|f\| = \sum_{i=0}^{m} a_i^2$, then

$$e(\alpha, \boldsymbol{\Omega}) \leqslant \tfrac{5}{2} |\boldsymbol{\Omega}| \log \|f\|. \tag{1}$$

The proof for α not being an integer is correct. The proof for α being an integer is based on the following refinement of a result of Cassels ([1], p. 159 ([1])).

If an algebraic integer β of degree n is not conjugate to β^{-1} then

$$\overline{|\beta|} > 1 + \frac{1}{5n-1}, \tag{2}$$

where $\overline{|\beta|}$ is the maximal absolute value of the conjugates of β.

If α is an integer and $\alpha = \zeta_q \beta^e$ then β is also an integer ($e > 0$). However it does not follow that if α is not conjugate to α^{-1} then β is not conjugate to β^{-1}. The example

$$\alpha = -1 - \sqrt{2} = \zeta_4 \left(\zeta_8 \sqrt{1 + \sqrt{2}} \right)^2 = \zeta_4 \beta^2$$

shows that even for all i $\zeta_q^i \beta$ may be conjugate to $\zeta_q^{-i} \beta^{-1}$.

([1]) Page 379 in this volume.

Therefore the inequality (2) does not follow in an obvious way (which is assumed although not asserted in [1]) from the assumption of the lemma in question and we are not able to decide whether it follows at all. However the inequality (1) is a simple consequence (see Corollary below) of the following

Theorem. *If $\alpha = \zeta_q \beta^e$ is not conjugate to α^{-1}, $\beta \in \boldsymbol{K}(\alpha)$ where $\boldsymbol{K}$ is a normal field of degree $|\boldsymbol{K}|$ and $(|\boldsymbol{K}|, q, e) = 1$ then for some i, $\zeta_q^i \beta$ is not conjugate to $\zeta_q^{-i} \beta^{-1}$.*

Lemma 1. *Let p be a prime not dividing $|\boldsymbol{K}|$, $\zeta_p \in \boldsymbol{K}(\alpha)$, $\beta \in \boldsymbol{K}(\alpha)$. If σ_1, σ_2 are two automorphisms of the normal closure of $\boldsymbol{K}(\alpha)$, $\sigma_1(\alpha) = \sigma_2(\alpha)$, $\sigma_1(\zeta_p) = \sigma_2(\zeta_p)$ and $\sigma_1(\beta^p) = \sigma_2(\beta^p)$ then $\sigma_1(\beta) = \sigma_2(\beta)$.*

Proof. Set $\sigma = \sigma_2^{-1}\sigma_1$. Let α be of degree r over $\boldsymbol{K}(\zeta_p)$ and let

$$\beta = a_0 + a_1\alpha + \ldots + a_{r-1}\alpha^{r-1}, \quad a_k \in \boldsymbol{K}(\zeta_p).$$

If $\sigma(\beta) \neq \beta$ we have $\sigma(\beta) = \zeta_p \beta \neq 0$. Therefore,

$$\sigma(\beta) = \zeta_p a_0 + \zeta_p a_1 \alpha + \ldots + \zeta_p a_{r-1}\alpha^{r-1},$$

where at least one coefficient $\zeta_p a_i$, say, is non-zero. On the other hand,

$$\sigma(\beta) = \sigma(a_0) + \sigma(a_1)\alpha + \ldots + \sigma(a_{r-1})\alpha^{r-1}.$$

Since $\boldsymbol{K}$ is normal, $\sigma(a_i) \in \boldsymbol{K}(\zeta_p)$. It follows that

$$\sigma(a_i) = \zeta_p a_i, \quad \sigma(a_i^p) = a_i^p.$$

a_i^p belongs, therefore, to the subfield $\boldsymbol{L}$ of $\boldsymbol{K}(\zeta_p)$ invariant with respect to σ. We have also $\zeta_p \in \boldsymbol{L}, a_i \notin \boldsymbol{L}$ and by Abel's theorem a_i is of degree p over $\boldsymbol{L}$. Since $\boldsymbol{L} \subset \boldsymbol{L}(a_i) \subset \boldsymbol{K}(\zeta_p)$ it follows $|\boldsymbol{K}(\zeta_p)| \equiv 0 \bmod p$ and $|\boldsymbol{K}| \equiv 0 \bmod p$, contrary to the assumption. □

Lemma 2. *The theorem holds for $q = 2^\nu$.*

Proof. Set $\zeta_q = \zeta$. If $e \not\equiv 0 \pmod 2$ we have for suitable i

$$\alpha = \zeta \beta^e = (\zeta^i \beta)^e,$$

hence $\zeta^i \beta$ is not conjugate to $\zeta^{-i}\beta^{-1}$. Assume that $e \equiv 0 \bmod 2$, $|\boldsymbol{K}| \not\equiv 0 \bmod 2$ and that for each i there exists an automorphism σ_i of the normal closure of $\boldsymbol{K}(\alpha)$ such that

$$\sigma_i(\zeta^i \beta) = \zeta^{-i}\beta^{-1}.$$

If $\sigma_i(\zeta) = \zeta^{s_i}$ we have

$$\sigma_i^t(\beta) = \zeta^{-i(s_i^t+1)}\beta^{-1} \quad (t \text{ odd}),$$

$$\sigma_i^t(\alpha) = \begin{cases} \zeta^{s_i^t - ie(s_i^t+1)}\beta^{-e} & \text{for } t \text{ odd}, \\ \zeta^{s_i^t - ie(s_i^t-1)}\beta^{e} & \text{for } t \text{ even}. \end{cases}$$

If $s_i \equiv -1 \bmod q$ then setting $t = 1$ we get $\sigma_i(\alpha) = \alpha^{-1}$, contrary to the assumption. This remark implies the validity of the lemma for $\nu = 1, 2$. Indeed, if $\nu = 1$ then

$s_i \equiv -1 \bmod 2$. If $\nu = 2$ then either $s_0 \equiv -1 \bmod 4$ or $s_1 \equiv -1 \bmod 4$. Otherwise $s_0 \equiv s_1 \equiv 1 \bmod 4$,

$$\sigma_0(\alpha) = \zeta\beta^{-e} = \sigma_1(\alpha), \quad \sigma_0(\beta^2) = \beta^{-2} = \sigma_1(\beta^2)$$

and by Lemma 1

$$\sigma_0(\beta) = \sigma_1(\beta), \quad \beta^{-1} = -\beta^{-1},$$

which is impossible.

In order to prove the lemma for $\nu \geqslant 3$ we prove first the three assertions:

(i) *if* $\nu \geqslant 3$, $2^{\nu-3} \parallel i - j$ *then either* $s_i \equiv -1 \bmod 4$ *or* $s_j \equiv -1 \bmod 4$,

(ii) *if* $\nu \geqslant 4$, $2^{\nu-4} \parallel i - j$, $s_i \equiv 3 \bmod 8$ *then* $s_j \equiv -1 \bmod 4$,

(iii) *if* $1 < l < \nu$, $2^{\nu-1-l} \parallel i - j$, $2^l \parallel s_i + 1$ *then* $2^l \nparallel s_j + 1$.

(i) We have $\sigma_i\sigma_j(\alpha) = \zeta^{s_is_j - je(s_j+1)s_i + ie(s_i+1)}\beta^e$. Since $2(i-j)(s_i+1)(s_j+1) \equiv 0 \bmod 2^\nu$ it follows that $\sigma_i\sigma_j(\alpha) = \sigma_j\sigma_i(\alpha)$ and $\sigma_i\sigma_j(\beta^2) = \sigma_j\sigma_i(\beta^2)$, thus by Lemma 1 $\sigma_i\sigma_j(\beta) = \sigma_j\sigma_i(\beta)$. Hence $(i-j)(s_i+1)(s_j+1) \equiv 0 \bmod 2^\nu$, $(s_i+1)\times(s_j+1) \equiv 0 \bmod 8$ and either $s_i \equiv -1 \bmod 4$ or $s_j \equiv -1 \bmod 4$.

(ii) If $s_i \equiv 3 \bmod 8$ then $2(i-j)(s_i+1)(s_j+1) \equiv 0 \bmod 2^\nu$, $\sigma_i\sigma_j(\alpha) = \sigma_j\sigma_i(\alpha)$, $\sigma_i\sigma_j(\beta^2) = \sigma_j\sigma_i(\beta^2)$ thus by Lemma 1 $\sigma_i\sigma_j(\beta) = \sigma_j\sigma_i(\beta)$, $(i-j)(s_i+1)(s_j+1) \equiv 0 \bmod 2^\nu$, $(s_i+1)(s_j+1) \equiv 0 \bmod 16$, $s_j \equiv -1 \bmod 4$.

(iii) Let $s_i \equiv -5^{\alpha_i}$, $s_j \equiv -5^{\alpha_j} \bmod 2^\nu$. If $2^l \parallel s_i + 1$, $2^l \parallel s_j + 1$ then $5^{\alpha_i} \equiv 2^l + 1 \bmod 2^{l+1}$, $5^{\alpha_j} \equiv 2^l + 1 \bmod 2^{l+1}$, hence $2^{l-2} \parallel \alpha_i$, $2^{l-2} \parallel \alpha_j$, $(\alpha_j, 2^{\nu-2}) \mid \alpha_i$. It follows that the congruence

$$t\alpha_j \equiv \alpha_i \bmod 2^{\nu-2}$$

is soluble. Its root t must be odd since otherwise $l - 1 \leqslant \nu - 2$ implies $\alpha_i \equiv t\alpha_j \equiv 0 \bmod 2^{l-1}$, which is impossible. Thus we have for an odd t

$$s_j^t \equiv s_i \bmod 2^\nu.$$

Since $2(i-j)(s_i+1) \equiv 0 \bmod 2^\nu$ we get $\sigma_j^t(\alpha) = \sigma_i(\alpha)$, $\sigma_j^t(\beta^2) = \sigma_i(\beta^2)$, thus by Lemma 1 $\sigma_j^t(\beta) = \sigma_i(\beta)$, $(i-j)(s_i+1) \equiv 0 \bmod 2^\nu$, which is impossible.

Let l be the greatest integer not exceeding ν such that $s_i \equiv -1 \bmod 2^l$ for suitable i. Since $s_i \not\equiv -1 \bmod 2^\nu$ for all i we have $l < \nu$ and by (i) $l > 1$.

Consider first the case $\nu = 3$. Then $q = 8$, $l = 2$, $s_i \equiv 3 \bmod 8$. Taking in (iii) $l = 2$, $\nu = 3$, $j = i - 1$ or $i + 1$ we get $s_{i-1} \equiv s_{i+1} \equiv 1 \bmod 4$.

If $s_{i-1} \equiv s_{i+1} \bmod 8$ then $2[(i+1) - (i-1)](s_{i-1}+1) \equiv 4(s_{i-1}+1) \equiv 0 \bmod 8$, hence $\sigma_{i-1}(\alpha) = \sigma_{i+1}(\alpha)$, $\sigma_{i-1}(\beta^2) = \sigma_{i+1}(\beta^2)$ and by Lemma 1 $\sigma_{i-1}(\beta) = \sigma_{i+1}(\beta)$, $2(s_{i-1}+1) \equiv 0 \bmod 8$ which is impossible.

In the remaining cases: $s_{i-1} \equiv 1$, $s_i \equiv 3$, $s_{i+1} \equiv 5 \bmod 8$ and $s_{i-1} \equiv 5$, $s_i \equiv 3$, $s_{i+1} \equiv 1$ we have $s_{i-1}s_is_{i+1} \equiv -1$, $s_i \equiv 3 \bmod 8$.

It follows

$$\begin{aligned}\sigma_{i-1}\sigma_i\sigma_{i+1}(\alpha) &= \zeta^{s_{i-1}s_is_{i+1}-e[(i+1)s_{i-1}s_is_{i+1}+s_{i-1}s_i-s_{i-1}+i-1]}\beta^{-e}\\ &= \zeta^{-1-e(-i-1+3s_{i-1}-s_{i-1}+i-1)}\beta^{-e}\\ &= \zeta^{-1-2e(s_{i-1}-1)}\beta^{-e} = \zeta^{-1}\beta^{-e} = \alpha^{-1},\end{aligned}$$

since $2(s_{i-1}-1) \equiv 0 \bmod 8$.

Consider next the case $\nu \geqslant 4$. Let $2^{\nu-1-l} \parallel i-j$, $2^k \parallel s_j + 1$. For suitably chosen j we have $k > 1$. Indeed, if $l > 2$ then $\nu - 1 - l < \nu - 3$, $2^{\nu-1-l} \parallel i - j - 2^{\nu-3}$ and by (i) $s_j \equiv -1 \bmod 4$ or $s_{j+2^{\nu-3}} \equiv -1 \bmod 4$.

If $l = 2$ and $s_j \equiv 1 \bmod 4$ then by (i) $s_{j+2^{\nu-3}} \equiv -1 \bmod 4$, by (ii) $s_{j+2^{\nu-4}} \equiv -1 \bmod 4$, because $s_{j+2^{\nu+3}} \not\equiv -1 \bmod 8$ and again by (ii) $s_j \equiv -1 \bmod 4$, a contradiction.

By the definition of l we have $k \leqslant l$ and by (iii) $k \neq l$. Thus we get $1 < k < l < \nu$. Let

$$s_i \equiv -5^{\alpha_i} \bmod 2^\nu, \quad s_j \equiv -5^{\alpha_j} \bmod 2^\nu.$$

It follows

$$\begin{gathered}5^{\alpha_i} \equiv 1 \bmod 2^l, \quad 5^{\alpha_j} \equiv 2^k + 1 \bmod 2^{k+1};\\ 2^{l-2} \mid \alpha_i, \quad 2^{k-2} \parallel \alpha_j; \quad (\alpha_j, 2^{\nu-2}) \mid \alpha_i\end{gathered}$$

and the congruence

$$t\alpha_j + \alpha_i \equiv 0 \bmod 2^{\nu-2}$$

is soluble. Since $k < l$ its root t must be even. Thus we have for an even t

$$s_i s_j^t \equiv -1 \bmod 2^\nu.$$

Since $2^{\nu-1-l} \mid i-j$, $2^l \mid s_i + 1$ we get

$$j(s_i s_j^t - s_i) + i(s_i+1) \equiv (i-j)(s_i+1) \equiv 0 \bmod 2^{\nu-1}$$

and

$$\sigma_i\sigma_j^t(\alpha) = \zeta^{s_is_j^t - e[j(s_is_j^t - s_i)+i(s_i+1)]}\beta^{-e} = \alpha^{-1},$$

which is impossible. □

Lemma 3. *The theorem holds for $q = p^\nu$, where p is an odd prime.*

Proof. Set $\zeta_q = \zeta$. If $e \not\equiv 0 \bmod p$ we have for suitable i

$$\alpha = \zeta\beta^e = (\zeta^i\beta)^e,$$

hence $\zeta^i\beta$ is not conjugate to $\zeta^{-i}\beta^{-1}$. Assume that $e \equiv 0 \bmod p$, $|\boldsymbol{K}| \not\equiv 0 \bmod p$ and that for each i there exists an automorphism σ_i of the normal closure of $\boldsymbol{K}(\alpha)$ such that

$$\sigma_i(\zeta^i\beta) = \zeta^{-i}\beta^{-1}.$$

If $i \equiv 0 \bmod p^{\nu-1}$, t is odd then

$$\sigma_i^t(\beta) = \zeta^{-i(s_i^t+1)}\beta^{-1}, \quad \sigma_i^t(\alpha) = \zeta^{s_i^t}\beta^{-e}.$$

We have

$$\sigma_0\sigma_{p^{\nu-1}}(\alpha) = \zeta^{s_0 s_{p^{\nu-1}}}\beta^e = \sigma_{p^{\nu-1}}\sigma_0(\alpha),$$
$$\sigma_0\sigma_{p^{\nu-1}}(\zeta_p) = \sigma_{p^{\nu-1}}\sigma_0(\zeta_p), \quad \sigma_0\sigma_{p^{\nu-1}}(\beta^p) = \sigma_{p^{\nu-1}}\sigma_0(\beta^p),$$

thus by Lemma 1

$$\sigma_0\sigma_{p^{\nu-1}}(\beta) = \sigma_{p^{\nu-1}}\sigma_0(\beta); \quad p^{\nu-1}(s_0+1)(s_{p^{\nu-1}}+1) \equiv 0 \bmod p^\nu.$$

Hence either $s_0 \equiv -1 \bmod p$ or $s_{p^{\nu-1}} \equiv -1 \bmod p$ and we assume without loss of generality that the first congruence holds. Then $s_0^{p^{\nu-1}} \equiv -1 \bmod p^\nu$, $\sigma_0^{p^{\nu-1}}(\alpha) = \alpha^{-1}$, which is impossible. □

Proof of the theorem. We proceed by induction with respect to $\omega(q)$ the number of distinct prime factors of q. If $\omega(q) = 0$ the theorem is trivial. If $\omega(q) = 1$ the theorem holds in virtue of Lemmata 2 and 3. Suppose that the theorem holds for $\omega(q) < n$ and consider $\omega(q) = n > 1$. Let p be the least prime factor of q, $q = p^\nu q_1$, $e = p^\mu e_1$, where $p \nmid q_1 e_1$. If $\mu = 0$ then for suitable ζ_{p^ν}, ζ_{q_1} we have

$$\alpha = \zeta_q\beta^e = \zeta_{q_1}(\zeta_{p^\nu}\beta)^e.$$

Since $\zeta_q = \alpha\beta^{-e} \in \boldsymbol{K}(\alpha)$ we have $\zeta_{p^\nu} \in \boldsymbol{K}(\alpha)$, $\zeta_{p^\nu}\beta \in \boldsymbol{K}(\alpha)$ and by the inductive assumption for some i

$$\zeta_{q_1}^i\zeta_{p^\nu}\beta \text{ is not conjugate to } \zeta_{q_1}^{-i}\zeta_{p^\nu}^{-1}\beta^{-1},$$

which was to be proved.

If $\mu > 0$, by the assumption $|\boldsymbol{K}| \not\equiv 0 \bmod p$. We have for suitable ζ_{p^ν}, ζ_{q_1}

$$\alpha = \zeta_q\beta^e = \zeta_{p^\nu}(\zeta_{q_1}\beta^{e_1})^{p^\mu}.$$

Since $\zeta_{q_1}\beta^{e_1} \in \boldsymbol{K}(\alpha)$ it follows by the inductive assumption that for some i

$$\alpha_1 = \zeta_{p^\nu}^i\zeta_{q_1}\beta^{e_1} \text{ is not conjugate to } \alpha_i^{-1}.$$

However we have for suitable j

$$\alpha_1 = \zeta_{q_1}(\zeta_{p^\nu}^j\beta)^{e_1}$$

and $\zeta_{p^\nu}^j\beta \in \boldsymbol{K}(\zeta_{p^\nu}, \alpha_1)$. Indeed, $\beta \in \boldsymbol{K}(\alpha)$ and $\alpha = \zeta_{p^\nu}^{1-ip^\mu}a_1^{p^\mu}$. Moreover since $(|\boldsymbol{K}|, q, e) = 1$ and p is the least prime factor of q

$$\big(|\boldsymbol{K}(\zeta_{p^\nu})|, q_1, e_1\big) \mid \big(p^{\nu-1}(p-1)|\boldsymbol{K}|, q_1, e_1\big) = 1.$$

By the inductive assumption we have for some k:

$$\zeta_{q_1}^k\zeta_{p^\nu}^j\beta \text{ is not conjugate to } \zeta_{q_1}^{-k}\zeta_{p^\nu}^{-j}\beta^{-1},$$

which was to be proved. □

Remark 1. An examination of the proof shows that if $\boldsymbol{K}$ is abelian the assumption $(|\boldsymbol{K}|, q, e) = 1$ can be replaced by $(|\boldsymbol{K}|, q, e) \equiv 1 \bmod 2$.

Corollary. *If $\alpha \in \boldsymbol{\Omega}$ is an integer not conjugate to α^{-1}, $\alpha \neq 0$ and $f(\alpha) = 0$, where f is a polynomial with integer coefficients then*

$$e(\alpha, \boldsymbol{\Omega}) \leqslant \tfrac{5}{2}|\boldsymbol{\Omega}| \log \|f\|.$$

Proof. Suppose first that $\boldsymbol{\Omega} = \mathbb{Q}(\alpha)$, set $e(\alpha, \boldsymbol{\Omega}) = e$ and let β be an integer of $\mathbb{Q}(\alpha)$ such that $\alpha = \zeta_q \beta^e$. It follows that

$$\log \overline{|\alpha|} = e \log \overline{|\beta|}. \tag{3}$$

By the inequality of Carmichael–Masson $\overline{|\alpha|} \leqslant \|f\|^{1/2}$ we have

$$\log \overline{|\alpha|} \leqslant \tfrac{1}{2} \log \|f\|. \tag{4}$$

On the other hand, by the theorem $\zeta_q^i \beta$ is not conjugate to $\zeta_q^{-i} \beta^{-1}$ for some i. Since $\zeta_q^i \beta \in \mathbb{Q}(\alpha)$ we have by the inequality (2)

$$\overline{|\beta|} = \overline{|\zeta_q^i \beta|} > 1 + \frac{1}{5|\mathbb{Q}(\alpha)| - 1},$$

thus

$$\log \overline{|\beta|} > \frac{1}{5|\mathbb{Q}(\alpha)|}$$

and by (3) and (4)

$$e \leqslant \tfrac{5}{2}|\mathbb{Q}(\alpha)| \log \|f\|.$$

In the general case we use the following assertion of Lemma 1 of [1] independent of (1). If $\boldsymbol{\Omega}_1 \supset \boldsymbol{\Omega}$ then

$$e(\alpha, \boldsymbol{\Omega}_1) \leqslant \frac{|\boldsymbol{\Omega}_1|}{|\boldsymbol{\Omega}|} e(\alpha, \boldsymbol{\Omega}).$$

Taking $\boldsymbol{\Omega}_1 = \boldsymbol{\Omega}$, $\boldsymbol{\Omega} = \mathbb{Q}(\alpha)$ we get

$$e(\alpha, \boldsymbol{\Omega}) \leqslant \frac{|\boldsymbol{\Omega}|}{|\mathbb{Q}(\alpha)|} \cdot \tfrac{5}{2}|\mathbb{Q}(\alpha)| \log \|f\| = \tfrac{5}{2}|\boldsymbol{\Omega}| \log \|f\|. \qquad \square$$

Remark 2. The recent unpublished work of C. J. Smyth on the product of conjugates of an algebraic integer lying outside the unit circle allows one to strenghten considerably the Corollary and the relevant results of [1]. This will form an object of another paper (see the paper D7 in this volume).

Reference

[1] A. Schinzel, *Reducibility of lacunary polynomials* I. Acta Arith. 16 (1969), 123–159; *Corrigenda*: Acta Arith. 19 (1971), 201; ibid. 24 (1978), 265; this collection: D4, 344–380.

Andrzej Schinzel
Selecta

Originally published in
Acta Arithmetica XXXIV (1978), 227–265

Reducibility of lacunary polynomials III

1.

The present paper is a sequel to [11] and the notation of that paper is used throughout. All the polynomials considered are supposed to have integral coefficients unless stated to the contrary. Reducibility means reducibility over the rational field $\mathbb{Q}$.

If $f(x_1, \dots, x_k) \neq 0$ is a polynomial then

$$f(x_1, \dots, x_k) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} f_\sigma(x_1, \dots, x_k)^{e_\sigma}$$

means that the polynomials f_σ are irreducible and prime to each other.

If $\Phi(x_1, \dots, x_k) = f(x_1, \dots, x_k) \prod_{i=1}^{k} x_i^{\alpha_i}$, where f is a polynomial prime to $x_1 x_2 \cdots x_k$ and α_i are integers, then we set

$$J\Phi(x_1, \dots, x_k) = f(x_1, \dots, x_k).$$

A polynomial g such that

$$Jg(x_1^{-1}, \dots, x_k^{-1}) = \pm g(x_1, \dots, x_k)$$

is called *reciprocal*. Let

$$J\Phi(x_1, \dots, x_k) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} f_\sigma(x_1, \dots, x_k)^{e_\sigma}.$$

We set

$$K\Phi(x_1, \dots, x_k) = \text{const} \prod\nolimits_1 f_\sigma(x_1, \dots, x_k)^{e_\sigma},$$
$$L\Phi(x_1, \dots, x_k) = \text{const} \prod\nolimits_2 f_\sigma(x_1, \dots, x_k)^{e_\sigma},$$

where $\prod_1$ is extended over all f_σ that do not divide $J(x_1^{\delta_1} \cdots x_k^{\delta_k} - 1)$ for any $[\delta_1, \dots, \delta_k] \neq 0$, $\prod_2$ is extended over all f_σ that are non-reciprocal. The leading coefficients of $K\Phi$ and $L\Phi$ are assumed equal to that of $J\Phi$. In particular for $k = 1$ $K\Phi(x)$ equals $J\Phi(x)$ deprived of all its cyclotomic factors and is called the kernel of Φ.

For a polynomial $F(x_1, \dots, x_k)$, $\|F\|$ is the sum of squares of the coefficients of F; if $F \neq 0$, $|F|$ is the maximum of the degrees of F with respect to x_i $(1 \leqslant i \leqslant k)$, $\Omega(F)$ is the

number of irreducible factors of F counted with multiplicities, $\exp_k$ and $\log_k$ denote the kth iteration of the exponential and the logarithmic function respectively. $\tau(n)$ is the number of divisors and $\Omega_0(n)$ the number of prime divisors of n counted with multiplicities.

The main object of [11] has been to describe the canonical factorization of $LF(x^{n_1}, \dots, x^{n_k})$ for any fixed polynomial F and a variable integral vector $[n_1, \dots, n_k]$. The much more difficult problem of describing the factorization of $KF(x^{n_1}, \dots, x^{n_k})$ has been solved only for $k = 1$ and for $k = 2$ provided $KF(x_1, x_2) = LF(x_1, x_2)$, in particular if $F(x_1, x_2) = a_0 + a_1x_1 + a_2x_2$. For $k > 2$ even the simplest case $F(x_1, x_2, x_3) = a_0 + \sum_{j=1}^{3} a_j x_j$ $(n_1 < n_2 < n_3)$ has been settled only under very restrictive assumption about the a_j's (see [3]).

The aim of the present paper is to improve and to extend the above results in several ways. First, due to the recent progress made by Blanksby and Montgomery [1] and by Smyth [20] in the problem of distribution of the conjugates of an algebraic integer on the plane it has been possible to improve the result on $KF(x^n)$ mentioned above. We have

Theorem 1. *For any polynomial $F(x) \neq 0$ such that $KF(x) \neq \text{const}$, for some positive integer $c(F)$ and for any positive integer n there exist positive integers v and u such that*

(i) $v \mid c(F)$,

(ii) $n = uv$,

(iii) $KF(x^v) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(x)^{e_\sigma}$ *implies* $KF(x^n) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(x^u)^{e_\sigma}$.

Moreover,

$$\log c(F) \ll \big(|KF| \log(2|KF|) \log \|F\|\big)^{1/3} \big(\log 2|KF| + \log_2 \|F\|\big)^{2/3}$$

and if $KF(x) = LF(x)$

$$\log c(F) \leqslant \sqrt{\frac{\log \|F\| \log_2 \|F\|}{2 \log \vartheta_0}} + O\big(\sqrt{\log \|F\| \log_3 \|F\|}\big),$$

where ϑ_0 is the real zero of $x^3 - x - 1$.

In any case

$$\Omega\big(KF(x^n)\big) = \sum_{\sigma=1}^{s} e_\sigma \leqslant \min\left(|KF|\tau(n), |KF|^{1+o(1)} \exp\Big(\frac{\log 2 + o(1)}{\log_3 \|F\|} \log_2 \|F\|\Big)\right).$$

Examples will be given to show that in the first of the estimates for $\log c(F)$ the exponent $1/3$ cannot be lowered, in the second the main term is best possible and the estimate for $\Omega\big(KF(x^n)\big)$ is sharp with respect to all three parameters involved n, $|KF|$ and $\|F\|$.

Corollary 1. *For any polynomial $F(x)$ such that $F(0) \neq 0$ and any n we have*

$$\Omega\big(F(x^n)\big) \leqslant |F|\tau(n).$$

Corollary 2. *For any binomial $b(x)$ we have*

$$\Omega\big(Kb(x)\big) \leqslant \exp\Big(\frac{\log 2 + o(1)}{\log_3 \|b\|} \log_2 \|b\|\Big).$$

Corollary 3. *For any trinomial $t(x)$ we have*

$$\Omega\big(Kt(x)\big) \leqslant \frac{\log \|t\|}{2 \log \vartheta_0 + o(1)}\,.$$

The corollaries are of interest because for a general polynomial $f(x)$ only $\Omega\big(Lf(x)\big)$ is known to be $O\big(\log \|f\|\big)$ and the estimates for $\Omega\big(Kf(x)\big)$ depend upon $|f|$ (see [15] and the Corollary to Lemma 1).

Coming back to [11] it is possible to improve also the estimates given there for the case $k > 1$. The improvements are however not drastic and the new estimates are probably still far from best possible, thus we shall not go into the matter. On the other hand using the result of E. Gourin [4] it is possible to describe the canonical factorization of $KF(x_1^{n_1}, \ldots, x_k^{n_k})$ for any k.

We have

Theorem 2. *For any polynomial $F(x_1, \ldots, x_k) \neq 0$ and any positive integers $n_1, \ldots, n_k$ there exist positive integers $\nu_1, \ldots, \nu_k$ and $v_1, \ldots, v_k$ such that*

(iv) $\nu_j \mid c(F)$ $(1 \leqslant j \leqslant k)$,

(v) $n_j = \nu_j v_j$ $(1 \leqslant j \leqslant k)$,

(vi) $KF(x_1^{\nu_1}, \ldots, x_k^{\nu_k}) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(x_1, \ldots, x_k)^{e_\sigma}$ *implies*

$$KF(x_1^{n_1}, \ldots, x_k^{n_k}) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(x_1^{v_1}, \ldots, x_k^{v_k})^{e_\sigma}.$$

The constant $c(F) \neq 0$ is effectively computable.

This theorem is clearly stronger than its analogue with L in place of K announced in [13]. In the latter case it follows by the method of [11] that

$$\log c(F) \leqslant 9 \cdot 2^{\|F\|-5};$$

it seems however that this estimate is far from the best possible.

Turning again to polynomials in one variable we shall obtain

Theorem 3. *Let $k \geqslant 3$, a_j $(0 \leqslant j \leqslant k)$ be non-zero integers and $n_1 < n_2 < \ldots < n_k$ positive integers. Then either there exist integers γ_j $(1 \leqslant j \leqslant k)$ such that*

(vii) $$\sum_{j=1}^{k} \gamma_j n_j = 0$$

and

(viii) $$0 < \max_{1 \leqslant j \leqslant k} |\gamma_j| < \exp_{2k-4}\Big(k 2^{\sum_{j=0}^{k} a_j^2 + 2} \log \sum_{j=0}^{k} a_j^2\Big)$$

or all primitive irreducible factors of $f(x) = a_0 + \sum_{j=1}^{k} a_j x^{n_j}$ *except a single simple one are reciprocal and monic, moreover if*

$$|a_0| + |a_k| \geqslant \sum_{j=1}^{k-1} |a_j| \tag{ix}$$

they are cyclotomic and if for some $g, h \leqslant k$

$$a_g^2 \not\equiv a_h^2 \bmod \operatorname*{g.c.d.}_{0 \leqslant j \leqslant k} a_j \cdot \operatorname*{g.c.d.}_{j \neq g,h} a_j \tag{x}$$

none whatever.

Besides, (ix) *and* (x) *imply*

$$\Omega\big(Kf(x)/Lf(x)\big) \leqslant \Omega_0\big((a_0, a_k)\big) \quad \text{and} \quad \Omega\big(f(x)/Lf(x)\big) \leqslant \Omega_0\big((a_0, a_k)\big),$$

respectively.

This is a refinement of Theorem 4 of [11]. A refinement in a different direction has been given in [14].

The last part of the paper is concerned with quadrinomials. Improving the results of [3] we shall prove

Theorem 4. *Let* a_j $(0 \leqslant j \leqslant 3)$ *be non-zero integers and*

(xi) *either* $|a_0| + |a_3| \geqslant |a_1| + |a_2|$ *or for some* $g, h \leqslant 3$

$$a_g^2 \not\equiv a_h^2 \bmod \operatorname*{g.c.d.}_{0 \leqslant j \leqslant 3} a_j \cdot \operatorname*{g.c.d.}_{j \neq g,h} a_j$$

or $|a_0| = |a_3|$, $|a_1| = |a_2|$.

Then for any quadrinomial $q(x) = a_0 + \sum_{j=1}^{3} a_j x^{n_j}$ $(0 < n_1 < n_2 < n_3)$ *that is not reciprocal we have one of the following four possibilities.*

(xii) $Kq(x)$ *is irreducible.*

(xiii) $q(x)$ *can be divided into two parts that have the highest common factor* $d(x)$ *being a non-reciprocal binomial.* $K\big(q(x)d^{-1}(x)\big)$ *is then irreducible unless* $q(x)d^{-1}(x)$ *is a binomial.*

(xiv) $q(x)$ *can be represented in one of the forms*

$$\begin{aligned} &k(T^2 - 4TUVW - U^2V^4 - 4U^2W^4) \\ &\quad = k(T - UV^2 - 2UVW - 2UW^2)(T + UV^2 - 2UVW + 2UW^2), \\ &k(U^3 + V^3 + W^3 - 3UVW) \\ &\quad = k(U + V + W)(U^2 + V^2 + W^2 - UV - UW - VW), \\ &k(U^2 + 2UV + V^2 - W^2) = k(U + V + W)(U + V - W), \end{aligned} \tag{1}$$

where $k = \pm(a_0, a_1, a_2, a_3)$ *and* T, U, V, W *are monomials in* $\mathbb{Z}[x]$. *The factors on the right hand side of* (1) *have irreducible kernels.*

(xv) $n_j = \nu\nu_j$ $(1 \leqslant j \leqslant 3)$; *$\nu$ and ν_j are positive integers,*

$$\nu_3 < \exp_2\bigl(12 \cdot 2^{\|q\|} \log \|q\|\bigr)$$

and $K\Bigl(a_0 + \sum_{j=1}^{3} a_j x^{\nu_j}\Bigr)$ *is reducible.*

Moreover

$$K\Bigl(a_0 + \sum_{j=1}^{3} a_j x^{\nu_j}\Bigr) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(x)^{e_\sigma}$$

implies

$$Kq(x) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(x^\nu)^{e_\sigma}.$$

Besides

$$\Omega\bigl(q(x)\bigr) = \sum_{\sigma=1}^{s} e_\sigma \leqslant \Bigl(\frac{1}{2\log\vartheta_0} + \frac{1}{2\log 2}\Bigr)\log\|q\|.$$

The condition (xi) is fulfilled for about 82% of quadruples (a_0, a_1, a_2, a_3) of height $\leqslant H \to \infty$. Since a rule for obtaining the canonical factorization of binomials is contained in Theorem 1 (and a more practical one in Lemma 5 below), Theorem 4 gives a satisfactory description of the canonical factorization of the kernel of $q(x) = a_0 + \sum_{j=1}^{3} a_j x^{n_j}$ $(0 < n_1 < n_2 < n_3)$ for all those quadruples (a_0, a_1, a_2, a_3) provided only $q(x)$ is not reciprocal.

The factorization of $q(x)/Kq(x)$ can be obtained easily by means of the results of Mann [8]. We content ourselves with stating the following

Corollary 4. *A non-reciprocal quadrinomial* $q(x) = a_0 + \sum_{j=1}^{3} a_j x^{n_j}$ $(0 < n_1 < n_2 < n_3)$ *satisfying* (xi) *is reducible if and only if we have one of the conditions* (xii)–(xv) *or* $q(x)$ *can be divided into two parts with the highest common factor equal to* $x^\delta \pm 1$ *or finally*

$$a_0 + \sum_{j=1}^{3} a_j \zeta^{n_j/(n_1,n_2,n_3)} = 0, \quad \textit{where} \quad \zeta^6 = 1.$$

A real enigma is the reducibility of reciprocal quadrinomials. A new idea seems to be needed even to solve the following simple

Problem. *Given a, b with $|a| \neq |b|$ do there exist infinitely many quotients r such that for suitable integers m, n: $m/n = r$ and $K(ax^{m+n} + bx^m + bx^n + a)$ is reducible?*

The proofs of Theorems 1, 2, 3 and 4 are given in Sections 2, 3, 4, 5 respectively. Before proceeding to the proofs we call the attention of the reader to an error in [11] repeated also in [12]. At the bottom of p. 133 in [11] certain inequalities for determinants are said

to follow from Hadamard's inequality. Now the inequalities in question are true but need not follow from Hadamard's inequality ([1]).

2.

In addition to the notation introduced in §1 we shall use the following: ζ_q is a primitive
c root of unity of order q, X_q is the qth cyclotomic polynomial.

If $\boldsymbol{\Omega}$ is a field and $\alpha \in \boldsymbol{\Omega}$, $\alpha \neq 0$, then

$$e(\alpha, \boldsymbol{\Omega}) = \begin{cases} 0 & \text{if } \alpha = \zeta_q \text{ for some } q, \\ \text{maximal } e \text{ such that } \alpha = \zeta_q \beta^e \text{ with some } q \text{ and } \beta \in \boldsymbol{\Omega} & \text{otherwise;} \end{cases}$$

$$E(\alpha, \boldsymbol{\Omega}) = \begin{cases} 0 & \text{if } \alpha = \zeta_q \text{ for some } q, \\ \text{maximal } n \text{ such that } \alpha = \vartheta^n,\ \vartheta \in \boldsymbol{\Omega}(\zeta_n) & \text{otherwise.} \end{cases}$$

For a given polynomial $f = \sum_{j=0}^{k} a_j x^j$

$$l(f) = \sum_{j=0}^{k} |a_j|, \quad C(f) = (a_0, a_1, \ldots, a_k).$$

c

Small bold face letters denote vectors, capital bold face letters denote matrices except $\boldsymbol{\Omega}$ that is a field. N_{Ω_2/Ω_1} is the norm from Ω_2 to Ω_1 or from $\Omega_2(x)$ to $\Omega_1(x)$.

Lemma 1. *Let α_i $(i = 1, \ldots, \varrho)$ be a system of pairwise not conjugate zeros of Kf, where f is a polynomial, and let ε_i be the multiplicity of α_i. Then*

$$\sum_{i=1}^{\varrho} \varepsilon_i \sqrt{e\big(\alpha_i, \mathbb{Q}(\alpha_i)\big)} \leqslant \sqrt{26|Kf| \log(7|Kf|) \log \|f\|}\,, \tag{2}$$

$$\sum{}' \varepsilon_i e\big(\alpha_i, \mathbb{Q}(\alpha_i)\big) \leqslant \frac{\log \|f\|}{2 \log \vartheta_0}\,, \tag{2'}$$

where the sum $\sum'$ is taken over all α_i not conjugate to α_i^{-1} and ϑ_0 is the real zero of $x^3 - x - 1$.

Proof. Let us consider the product

$$P = |a_0| \prod_{f(\alpha)=0,\ |\alpha|>1} |\alpha|,$$

where a_0 is the leading coefficient of f. By the inequality of Landau [6]

$$P < \|f\|^{1/2}. \tag{3}$$

([1]) The explanation is omitted, since in this edition [11] has been corrected.

On the other hand, let

$$Kf(x) \overset{\text{can}}{=} c\prod_{i=1}^{\varrho} f_i^{\varepsilon_i}(x),$$

where $f_i(\alpha_i) = 0$ and f_i is primitive. We have

$$P = c\prod_{i=1}^{\varrho} |a_i|^{\varepsilon_i} \prod_{|\alpha_i^{(j)}|>1} |\alpha_i^{(j)}|^{\varepsilon_i}, \tag{4}$$

where $\alpha_i^{(j)}$ runs over the conjugates of α_i and a_i is the leading coefficient of f_i. We shall show that

$$|a_i| \prod_{|\alpha_i^{(j)}|>1} |\alpha_i^{(j)}| > \begin{cases} \exp \dfrac{e\big(\alpha_i, \mathbb{Q}(\alpha_i)\big)}{52|f_i|\log 7|f_i|} & \text{always,} \\ \vartheta_0^{e(\alpha_i, \mathbb{Q}(\alpha_i))} & \text{if } \alpha_i \text{ is not conjugate to } \alpha_i^{-1}. \end{cases} \tag{5}$$

Since α_i is not a root of unity, we have by the definition of $e\big(\alpha_i, \mathbb{Q}(\alpha_i)\big)$

$$\alpha_i = \zeta_q \beta^e, \quad \beta \in \mathbb{Q}(\alpha_i), \quad e = e\big(\alpha_i, \mathbb{Q}(\alpha_i)\big). \tag{6}$$

If α_i is not an integer we use an argument due to J. Wójcik and set $\alpha_i = \mu/\nu$, $(\mu) = \mathfrak{d}\mathfrak{m}$, $(\nu) = \mathfrak{d}\mathfrak{n}$, where $\mathfrak{d}, \mathfrak{m}, \mathfrak{n}$ are ideals of $\mathbb{Q}(\alpha_i)$ and $(\mathfrak{m}, \mathfrak{n}) = 1$. By Gauss's Lemma the polynomial $N(\mathfrak{d})^{-1} \prod_{j=1}^{|f_i|} \big(\nu^{(j)}x - \mu^{(j)}\big)$ is primitive, N denoting the norm from $\mathbb{Q}(\alpha_i)$ to $\mathbb{Q}$. Since it is also irreducible it coincides with f_i up to a sign.

It follows that

$$a_i = \pm N\mathfrak{d}^{-1} N\nu = \pm N\mathfrak{n}.$$

By (6) $\mathfrak{n} = \mathfrak{r}^e$ and $|a_i| = N\mathfrak{r}^e \geqslant 2^e$ thus (5) holds. If α_i is an integer, β is also. We have

$$\prod_{|\alpha_i^{(j)}|>1} |\alpha_i^{(j)}| = \prod_{|\beta^{(j)}|>1} |\beta^{(j)}|^e. \tag{7}$$

c By the theorem of Blanksby and Montgomery [1]

c $$\prod_{|\beta^{(j)}|>1} |\beta^{(j)}| > 1 + \frac{1}{52|f_i|\log 6|f_i|} > \exp\Big(\frac{1}{52|f_i|\log 6|f_i| + 1}\Big) > \exp\Big(\frac{1}{52|f_i|\log 7|f_i|}\Big),$$

which together with (7) gives the first part of (5).

If α_i is not conjugate to α_i^{-1} then by the result of [18] applied with $\boldsymbol{K} = \mathbb{Q}$, $\zeta_q^r\beta$ is not conjugate to $\zeta_q^{-r}\beta^{-1}$ for a suitable r. By Smyth's theorem [20]

$$\prod_{|\beta^{(j)}|>1} |\beta^{(j)}| = \prod_{|\beta^{(j)}|>1} |(\zeta_q^r\beta)^{(j)}| \geqslant \vartheta_0,$$

which together with (7) gives the second part of (5).

Now (3), (4) and (5) give

$$\sum_{i=1}^{\varrho} \varepsilon_i \frac{e\big(\alpha_i, \mathbb{Q}(\alpha_i)\big)}{52|f_i|\log 7|f_i|} < \tfrac{1}{2}\log\|f\|, \tag{8}$$

$$\sum{}' \varepsilon_i e\big(\alpha_i, \mathbb{Q}(\alpha_i)\big) < \frac{\log\|f\|}{2\log\vartheta_0}.$$

The inequality (2′) follows at once. In order to prove (2) let us notice that

$$\sum_{i=1}^{\varrho} 52|f_i|\log 7|f_i| \leqslant 52|Kf|\log 7|Kf|.$$

Since

$$\varepsilon_i\sqrt{e\big(\alpha_i, \mathbb{Q}(\alpha_i)\big)} = \sqrt{\frac{e\big(\alpha_i, \mathbb{Q}(\alpha_i)\big)\varepsilon_i}{52|f_i|\log 7|f_i|}}\cdot\sqrt{52\varepsilon_i|f_i|\log 7|f_i|}$$

(2) follows from (8) by the Schwarz inequality. □

Corollary. *We have*

$$\Omega(Kf) < \sqrt{26|Kf|\log(7|Kf|)\log\|f\|},$$

$$\Omega(Lf) < \frac{\log\|f\|}{2\log\vartheta_0}.$$

c *Remark.* The bound given in (2′) cannot be improved as it is shown by the example

$$f_m(x) = N_{\mathbb{Q}(\vartheta_0)/\mathbb{Q}}(x-\vartheta_0^m) \tag{9}$$

$$= x^3 - (\vartheta_0^m + \vartheta_1^m + \vartheta_2^m)x^2 + (\vartheta_0^{-m} + \vartheta_1^{-m} + \vartheta_2^{-m})x - 1,$$

where ϑ_1, ϑ_2 are the two conjugates of ϑ_0.

Clearly $e\big(\vartheta_0^m, \mathbb{Q}(\vartheta_0)\big) \geqslant m$. On the other hand, since $|\vartheta_1| = |\vartheta_2| = |\vartheta_0|^{-1/2}$

$$\log\|f_m\| = \log\big(2 + (\vartheta_0^m + \vartheta_1^m + \vartheta_2^m)^2 + (\vartheta_0^{-m} + \vartheta_1^{-m} + \vartheta_2^{-m})^2\big)$$

$$= \log\big(\vartheta_0^{2m} + O(\vartheta_0^m)\big) = 2m\log\vartheta_0 + O(\vartheta_0^{-m}).$$

For further reference note that similarly

$$\log l(f_m) = m\log\vartheta_0 + O(\vartheta_0^{-m/2}). \tag{10}$$

Lemma 2. *For any algebraic number field $\boldsymbol{\Omega}$ and any $\alpha \in \boldsymbol{\Omega}$, $\alpha \neq 0$, we have*

$$E(\alpha, \boldsymbol{\Omega}) \,|\, e(\alpha, \boldsymbol{\Omega})\Big(w(\boldsymbol{\Omega}), 2\operatorname*{l.c.m.}_{\substack{p\,|\,e(\alpha,\boldsymbol{\Omega}) \\ p \text{ prime}}}(p-1)\Big), \tag{11}$$

where $w(\boldsymbol{\Omega})$ is the number of roots of unity contained in $\boldsymbol{\Omega}$. Moreover, if $\alpha = \beta^m$, $\beta \in \boldsymbol{\Omega}_1 \subset \boldsymbol{\Omega}(\zeta_m)$, then

$$mE(\beta, \boldsymbol{\Omega}_1) \,|\, E(\alpha, \boldsymbol{\Omega}). \tag{12}$$

Proof. The equality

$$\alpha = \vartheta^n, \quad \vartheta \in \boldsymbol{\Omega}(\zeta_n) \tag{13}$$

implies by Theorem 3 of [16]

$$\alpha^\sigma = \gamma^n, \quad \gamma \in \boldsymbol{\Omega},$$

where

$$\sigma = \Big(n, w(\boldsymbol{\Omega}), \quad \text{l.c.m.}_{\substack{q \mid n \\ q \text{ prime or } q=4}} [\boldsymbol{\Omega}(\zeta_q) : \boldsymbol{\Omega}]\Big). \tag{14}$$

Hence by Lemma 1 of [10]

$$n \mid e(\alpha, \boldsymbol{\Omega})\sigma \tag{15}$$

and by (14)

$$n \mid e(\alpha, \boldsymbol{\Omega})w(\boldsymbol{\Omega}).$$

It follows that if $e(\alpha, \boldsymbol{\Omega}) \neq 0$, i.e. α is not a root of unity, there are only finitely many n satisfying (13). The greatest of them $E(\alpha, \boldsymbol{\Omega}) = E$ satisfies by (14) and (15)

$$E \mid e(\alpha, \boldsymbol{\Omega})w(\boldsymbol{\Omega}), \tag{16}$$

$$E \mid e(\alpha, \boldsymbol{\Omega}) \text{ l.c.m.}_{\substack{q \mid e(\alpha, \boldsymbol{\Omega})w(\boldsymbol{\Omega}) \\ q \text{ prime or } q=4}} [\boldsymbol{\Omega}(\zeta_q) : \boldsymbol{\Omega}]. \tag{17}$$

However, if $q \mid w(\boldsymbol{\Omega})$ then $[\boldsymbol{\Omega}(\zeta_q) : \boldsymbol{\Omega}] = 1$, thus those factors q contribute nothing to l.c.m.$[\boldsymbol{\Omega}(\zeta_q) : \boldsymbol{\Omega}]$ occurring in (17). It is enough therefore to consider $q \mid 2e(\alpha, \boldsymbol{\Omega})$.

For q being a prime we have

$$[\boldsymbol{\Omega}(\zeta_q) : \boldsymbol{\Omega}] = \frac{[\mathbb{Q}(\zeta_q) : \mathbb{Q}]}{[\boldsymbol{\Omega} \cap \mathbb{Q}(\zeta_q) : \mathbb{Q}]} \;\Big|\; q - 1.$$

For $q = 4$ the degree $[\boldsymbol{\Omega}(\zeta_q) : \boldsymbol{\Omega}]$ divides 2. Thus if $e(\alpha, \boldsymbol{\Omega}) \neq 0$ (11) follows from (16) and (17). If $e(\alpha, \boldsymbol{\Omega}) = 0$ (11) is obvious, as in (12) if $E(\alpha, \boldsymbol{\Omega}) = 0$. If $E(\alpha, \boldsymbol{\Omega}) \neq 0$, α is not a root of unity, hence by Lemma 1 of [10] $0 \neq e(\alpha, \boldsymbol{\Omega}_1) = me(\beta, \boldsymbol{\Omega}_1)$, and by (11) applied to β and $\boldsymbol{\Omega}_1$

$$E_1 = E(\beta, \boldsymbol{\Omega}_1) \neq 0.$$

If

$$\beta = \vartheta_1^{E_1}, \quad \vartheta_1 \in \boldsymbol{\Omega}_1(\zeta_{E_1})$$

and r, s are rational integers satisfying

$$rE + smE_1 = (E, mE_1)$$

we get from (13) with $n = E$ and from $\alpha = \vartheta_1^{mE_1}$ the equality

$$\alpha = (\vartheta^s \vartheta_1^r)^{[E, mE_1]}, \quad \vartheta^s \vartheta_1^r \in \boldsymbol{\Omega}\big(\zeta_{[E, mE_1]}\big).$$

By the definition of E this implies $[E, mE_1] \leqslant E$, hence $E \equiv 0 \bmod mE_1$. □

Lemma 3. *Let $\boldsymbol{\Omega}$ be an algebraic number field and $\alpha \in \boldsymbol{\Omega}$, $\alpha \neq 0$. For every positive integer n we put*

$$\nu = \big(n, E(\alpha, \boldsymbol{\Omega})\big).$$

If $g(x) \in \boldsymbol{\Omega}[x]$ is a monic polynomial irreducible over $\boldsymbol{\Omega}$ and $g(x) \mid x^n - \alpha$, then $g(x) = G(x^{n/\nu})$, where $G(x)$ is a polynomial over $\boldsymbol{\Omega}$.

Proof. We proceed by induction with respect to $E(\alpha, \boldsymbol{\Omega})$. If $E(\alpha, \boldsymbol{\Omega}) = 0$ the assertion is trivial. Assume that the lemma is true for all $\boldsymbol{\Omega}'$ and α' with $E(\alpha', \boldsymbol{\Omega}') < E(\alpha, \boldsymbol{\Omega})$ and let $g(x) \mid x^n - \alpha$.

If $x^n - \alpha$ is irreducible, then the lemma is trivially true with $G(x) = x^\nu - \alpha$. If it is reducible, then by Capelli's theorem either

$$\text{(A)} \qquad \alpha = \beta^p, \quad p \mid n, \quad p \text{ prime}, \quad \beta \in \boldsymbol{\Omega}$$

or

$$\text{(B)} \qquad \alpha = -4\beta^4, \quad 4 \mid n, \quad \beta \in \boldsymbol{\Omega}.$$

We consider these cases successively using the following notation: $\boldsymbol{\Omega}_q = \boldsymbol{\Omega}(\zeta_q)$, $d_q = [\boldsymbol{\Omega}_q : \boldsymbol{\Omega}]$.

(A) We have there

$$g(x) \mid x^n - \beta^p = (x^{n/p} - \beta) \prod_{r=1}^{p-1} \big(x^{n/p} - \zeta_p^r \beta\big). \tag{18}$$

If $g(x) \mid x^{n/p} - \beta$ our inductive assumption applies directly, since by (A) and Lemma 2 $E(\beta, \boldsymbol{\Omega}) \mid \frac{1}{p} E(\alpha, \boldsymbol{\Omega})$.

Putting $\nu_0 = \big(\frac{n}{p}, E(\beta, \boldsymbol{\Omega})\big)$ we have

$$\nu_0 \;\Big|\; \frac{\nu}{p}, \quad g(x) = G_0(x^{n/p\nu_0}),$$

$G_0(x) \in \boldsymbol{\Omega}[x]$ and it is sufficient to take $G(x) = G_0(x^{n/p\nu_0})$.

If $g(x) \nmid x^{n/p} - \beta$, let $h(x)$ be a monic factor of $g(x)$ irreducible over $\boldsymbol{\Omega}_p$. By (18)

$$h(x) \mid g(x) \;\Big|\; \prod_{r=1}^{p-1} \big(x^{n/p} - \zeta_p^r \beta\big),$$

thus for some positive $r < p$

$$h(x) \mid x^{n/p} - \zeta_p^r \beta. \tag{19}$$

Let $h^{(1)}(x) = h(x), \ldots, h^{(d_p)}(x)$ be all the conjugates of $h(x)$ relative to $\boldsymbol{\Omega}(x)$. It follows from (19) that

$$\big(h^{(i)}(x), h^{(j)}(x)\big) \mid \beta\big(\zeta_p^{(i)r} - \zeta_p^{(j)r}\big) \quad (1 \leqslant i < j \leqslant d_p),$$

thus $h^{(i)}(x)$ $(i = 1, 2, \ldots, d_p)$ are relatively prime in pairs. Since $h^{(i)}(x) \mid g(x)$ it follows

that

$$g(x) = N_{\boldsymbol{\Omega}_p/\boldsymbol{\Omega}}\big(h(x)\big). \tag{20}$$

On the other hand, we have by Lemma 2

$$E(\zeta_p^r\beta, \boldsymbol{\Omega}_p) \;\Big|\; \frac{1}{p}\, E(\alpha, \boldsymbol{\Omega}).$$

Applying the inductive assumption to (19) and putting

$$\nu_1 = \Big(\frac{n}{p}\,, E(\zeta_p^r\beta, \boldsymbol{\Omega}_p)\Big)$$

we get

$$\nu_1 \;\Big|\; \frac{\nu}{p}\,, \quad h(x) = H(x^{n/p\nu_1}), \quad H(x) \in \boldsymbol{\Omega}_p[x]. \tag{21}$$

It is sufficient now to take

$$G(x) = N_{\boldsymbol{\Omega}_p/\boldsymbol{\Omega}}\big(H(x^{\nu/p\nu_1})\big).$$

Indeed, by (20) and (21)

$$g(x) = N_{\boldsymbol{\Omega}_p/\boldsymbol{\Omega}}\big(H(x^{n/p\nu_1})\big) = G(x^{n/\nu}).$$

(B) We have here

$$g(x)\,|\,x^n + 4\beta^4 = \prod_{r=0}^{3}\big(x^{n/4} - \zeta_4^r(1+\zeta_4)\beta\big).$$

Let $h(x)$ be a monic factor of $g(x)$ irreducible over $\boldsymbol{\Omega}_4$. We have for an $r \leqslant 3$

$$h(x)\,|\,x^{n/4} - \zeta_4^r(1+\zeta_4)\beta \tag{22}$$

and it follows in the same way as (20) from (19) that

$$g(x) = N_{\boldsymbol{\Omega}_4/\boldsymbol{\Omega}}\big(h(x)\big). \tag{23}$$

On the other hand, by Lemma 2

$$E\big(\zeta_4^r(1+\zeta_4)\beta, \boldsymbol{\Omega}_4\big)\,|\,\tfrac{1}{4}E(\alpha, \boldsymbol{\Omega}).$$

Applying the inductive assumption to (22) and putting

$$\nu_2 = \Big(\frac{n}{4}, E\big(\zeta_4^r(1+\zeta_4)\beta, \boldsymbol{\Omega}_4\big)\Big)$$

we get

$$\nu_2 \;\Big|\; \frac{\nu}{4}\,, \quad h(x) = H(x^{n/4\nu_2}), \quad H(x) \in \boldsymbol{\Omega}_4[x]. \tag{24}$$

It is sufficient now to take

$$G(x) = N_{\boldsymbol{\Omega}_4/\boldsymbol{\Omega}}\big(H(x^{\nu/4\nu_2})\big).$$

Indeed by (23) and (24)

$$g(x) = N_{\boldsymbol{\Omega}_4/\boldsymbol{\Omega}}\big(H(x^{n/4\nu_2})\big) = G(x^{n/\nu}). \qquad \square$$

Remark. One can show by induction with respect to $E(\alpha, \boldsymbol{\Omega})$ that for $n = E(\alpha, \boldsymbol{\Omega})$ there is no $\nu < n$ with the property asserted in the lemma.

Moreover, Lemmata 2 and 3 remain valid for any field $\boldsymbol{\Omega}$, not necessarily algebraic, n not divisible by char $\boldsymbol{\Omega}$ and those $\alpha \in \boldsymbol{\Omega}$ for which $e(\alpha, \boldsymbol{\Omega})$ is defined. $w(\boldsymbol{\Omega})$ is then to be replaced by the number of roots of unity of order $E(\alpha, \boldsymbol{\Omega})$ contained in $\boldsymbol{\Omega}$.

Lemma 4. *If $a \mid b$ then*

$$\sum_{(j,b)=1} (a, j-1) = \tau(a)\varphi(b),$$

where the sum is taken over any reduced system of residues mod b.

Proof. This is a special case of the theorem due to R. Sivaramakrishnan [19]. I owe the reference to Mr. A. Mąkowski. □

Lemma 5. *If $\Phi(x)$ is an irreducible polynomial, $\alpha \neq 0$ is any of its zeros, $n > 0$ is an integer,*

$$\nu = \big(n, E\big(\alpha, \mathbb{Q}(\alpha)\big)\big)$$

then

$$\Phi(x^{\nu}) \overset{\text{can}}{=} \Phi_1(x) \cdots \Phi_r(x)$$

implies

$$\Phi(x^n) \overset{\text{can}}{=} \Phi_1(x^{n/\nu}) \cdots \Phi_r(x^{n/\nu}).$$

Moreover

$$r \leqslant |\Phi|\tau(\nu).$$

Proof. Since Φ is irreducible, $\Phi(x)$ and hence also $\Phi(x^{\nu})$ has no multiple factors. Clearly $\Phi_j(x^{n/\nu})$ $(1 \leqslant j \leqslant r)$ are prime to each other and to prove the first assertion of the lemma we have only to show that they are irreducible. Let $f_j(x)$ be an irreducible factor of $\Phi_j(x^{n/\nu})$. Clearly

$$f_j(x) \mid \Phi(x^n). \tag{25}$$

We now use the following Lemma of Capelli (cf. [21], p. 289): if

$$x^n - \alpha = \prod_{i=1}^{l} g_i(x) \tag{26}$$

is the canonical factorization of $x^n - \alpha$ in $\boldsymbol{\Omega} = \mathbb{Q}(\alpha)$ then

$$\Phi(x^n) \overset{\text{can}}{=} \text{const} \prod_{i=1}^{l} N_{\boldsymbol{\Omega}/\mathbb{Q}} g_i(x). \tag{27}$$

It follows from (25) and (27) that for some $i \leqslant l$

$$\text{const}\, f_j(x) = N_{\boldsymbol{\Omega}/\mathbb{Q}} g_i(x). \tag{28}$$

On the other hand, it follows from (26) and Lemma 3 that

$$g_i(x) = G_i(x^{n/\nu}), \tag{29}$$

where $G_i(x) \in \boldsymbol{\Omega}[x]$. By (28), (29) and the choice of f_j

$$\text{const } f_j(x) = N_{\boldsymbol{\Omega}/\mathbb{Q}} G_i(x^{n/\nu}) \mid \Phi_j(x^{n/\nu}), \tag{30}$$

thus $N_{\boldsymbol{\Omega}/\mathbb{Q}} G_i(x) \mid \Phi_j(x)$.

Since Φ_j is irreducible

$$\Phi_j(x) = \text{const } N_{\boldsymbol{\Omega}/\mathbb{Q}} G_i(x),$$

thus by (30)

$$\Phi_j(x^{n/\nu}) = \text{const } f_j(x)$$

and by the choice of $f_j(x)$, $\Phi_j(x^{n/\nu})$ is irreducible.

To prove the second assertion of the lemma we first remark that by (27)

$$r = l. \tag{31}$$

By the definition of $E(\alpha, \boldsymbol{\Omega}) = E$ we have $E > 0$ or α is a root of unity. In the former case

$$\alpha = \vartheta(\zeta_E)^E, \quad \text{where} \quad \vartheta \in \boldsymbol{\Omega}[x]. \tag{32}$$

Let the Galois group $\mathscr{G}$ of $\boldsymbol{\Omega}(\zeta_E)/\boldsymbol{\Omega}$ be represented as a subgroup $\mathscr{J}$ of the multiplicative group $\mathscr{E}$ of reduced residues mod E, so that

$$\mathscr{J} = \{j \in \mathscr{E} : \exists\, g \in \mathscr{G}\ \zeta_E^j = g(\zeta_E)\}. \tag{33}$$

For any $j \in \mathscr{J}$ we have by (32)

$$\vartheta(\zeta_E^j)^E = \alpha = \vartheta(\zeta_E)^E,$$

hence

$$\vartheta(\zeta_E^j) = \zeta_E^{e(j)} \vartheta(\zeta_E) \tag{34}$$

for a suitable integer $e(j)$.

On the other hand, by (32)

$$x^\nu - \alpha = \prod_{i=1}^{\nu} \big(x - \zeta_\nu^i \vartheta(\zeta_E)^{E/\nu}\big)$$

and taking norms from $\boldsymbol{\Omega}(\zeta_E, x)$ to $\boldsymbol{\Omega}(x)$

$$(x^\nu - \alpha)^{|\mathscr{G}|} = \prod_{i=1}^{\nu} N_{\boldsymbol{\Omega}(\zeta_E)/\boldsymbol{\Omega}} \big(x - \zeta_\nu^i \vartheta(\zeta_E)^{E/\nu}\big), \tag{35}$$

where $|\mathscr{G}|$ is the order of $\mathscr{G}$.

c The ith factor on the right hand side is a power of a polynomial irreducible over $\boldsymbol{\Omega}$ with the exponent equal to the number n_i of those elements of $\mathscr{G}$ that leave $x - \zeta_\nu^i \vartheta(\zeta_E^{E/\nu})$

invariant. By (33) we have

$$n_i = \left|\left\{j \in \mathscr{J} : \zeta_\nu^{ij}\vartheta(\zeta_E^j)^{E/\nu} = \zeta_\nu^i \vartheta(\zeta_E)^{E/\nu}\right\}\right|$$

and by (34)

$$n_i = \left|\left\{j \in \mathscr{J} : ij + e(j) \equiv i \bmod \nu\right\}\right|. \tag{36}$$

Comparing the number of factors irreducible over $\boldsymbol{\Omega}$ on both sides of (35) we get by (26), (31) and (36)

$$r|\mathscr{G}| = \sum_{i=1}^{\nu} n_i = \sum_{i=1}^{\nu}\left|\left\{j \in \mathscr{J} : ij + e(j) \equiv i \bmod \nu\right\}\right|$$

$$= \sum_{j\in\mathscr{J}}\left|\left\{1 \leqslant i \leqslant \nu : ij + e(j) \equiv i \bmod \nu\right\}\right| \leqslant \sum_{j\in\mathscr{J}}(\nu, j-1) \leqslant \sum_{(j,E)=1}(\nu, j-1).$$

Now

$$|\mathscr{G}| = [\boldsymbol{\Omega}(\zeta_E) : \boldsymbol{\Omega}] \geqslant \frac{\varphi(E)}{|\Phi|},$$

by Lemma 4

$$\sum_{(j,E)=1}(\nu, j-1) = \tau(\nu)\varphi(E),$$

and it follows that $r \leqslant |\Phi|\tau(\nu)$.

It remains to consider the case where α is a root of unity. We have then, for a suitable q, $\Phi(x) = \text{const}\, X_q(x)$.

Let now $n = n_1 n_2$, where every prime factor of n_1 divides q and $(n_2, q) = 1$. It follows from the identity

$$X_q(x^n) = \prod_{d|n_2} X_{qn_1 d}(x)$$

and from the irreducibility of cyclotomic polynomials that

$$r \leqslant \tau(n_2) \leqslant \tau(n) = \tau(\nu). \qquad \square$$

In the next three lemmata we use the notation $m(x) = \underset{p|x,\ p\ \text{prime}}{\text{l.c.m.}}(p-1)$ for any positive integer x.

Lemma 6. *For any integer $x > 1$ either there exist three positive integers x_1, x_2, x_3 such that*

$$xm(x) \mid \left[x_1 m(x_1), x_2 m(x_2), x_3 m(x_3)\right] \tag{37}$$

and $\sqrt{x_1} + \sqrt{x_2} + \sqrt{x_3} < \sqrt{x}$ or $x = q^\alpha r^\beta s$, where q, r are primes, s is an integer, $r < 50$, $s < 50$, $\alpha > 0$, $\beta \geqslant 0$.

Proof. Let q be the greatest prime factor of x, $x = q^\alpha y$, $q \nmid y$. If $y \geqslant 50$, but $(q-1, y) = 1$

we set $x_1 = q^\alpha$, $x_2 = y$, $x_3 = 1$ and get

$$\sqrt{x} - \sqrt{x_1} - \sqrt{x_2} - \sqrt{x_3} \geqslant \big(\sqrt{q} - 1\big)\big(\sqrt{y} - 1\big) - 2 > \big(\sqrt{3} - 1\big)\big(\sqrt{50} - 1\big) - 2 > 0.$$

If $(q - 1, y) > 1$ let r be a common prime factor of y and $q - 1$

$$y = r^\beta s, \quad q - 1 = r^\gamma t, \quad r \nmid st.$$

If either $r \geqslant 50$ or $s \geqslant 50$ we set

$$x_1 = q^\alpha, \quad x_2 = r^{\beta+\gamma}, \quad x_3 = r^\beta st,$$

easily verify (37) and get

$$\begin{aligned}\sqrt{x} - \sqrt{x_1} - \sqrt{x_2} - \sqrt{x_3} &\geqslant q^{\alpha/2} r^{\beta/2} s^{1/2} - q^{\alpha/2} - r^{(\beta+\gamma)/2} - r^{\beta/2}(st)^{1/2} \\ &> \sqrt{x}\Big(1 - \frac{1}{r^{\beta/2}s^{1/2}} - \frac{1}{(st)^{1/2}} - \frac{1}{(r^\gamma)^{1/2}}\Big) > \sqrt{x}\Big(1 - \frac{2}{\sqrt{50}} - \frac{1}{\sqrt{2}}\Big) > 0.\end{aligned}$$

The case $st = 1$ is excluded since $q - 1 = r^\gamma$ implies $r = 2 < \sqrt{50}$. □

Lemma 7. *If x_i are positive integers and $\sum_{i=1}^{j} \sqrt{x_i} \leqslant \sqrt{x}$ then*

$$\log \operatorname*{l.c.m.}_{i=1,\dots,j} x_i m(x_i) \ll x^{1/3} (\log x)^{2/3}.$$

Proof. Let $M = \max \operatorname*{l.c.m.}_{i=1,\dots,j} x_i m(x_i)$, where the maximum is taken over (finitely many) integral points $(x_1, \dots, x_j)$ satisfying $x_i > 1$, $\sum_{i=1}^{j} \sqrt{x_i} \leqslant \sqrt{x}$. Let $(x_1^0, \dots, x_k^0)$ be a point in which the maximum is attained with the least value of $\sum_{i=1}^{j} \sqrt{x_i}$. By Lemma 6 we have $x_i^0 = q_i^{\alpha_i} r_i^{\beta_i} s_i$ $(i = 1, \dots, k)$, where q_i, r_i are primes and $\alpha_i > 0$, $r_i < 50$, $s_i < 50$. It follows that

$$\begin{aligned}M = \operatorname*{l.c.m.}_{1\leqslant i\leqslant k} x_i^0 m(x_i^0) &\leqslant \operatorname*{l.c.m.}_{1\leqslant i\leqslant k} q_i^{\alpha_i}(q_i - 1) \operatorname*{l.c.m.}_{1\leqslant i\leqslant k} r_i^{\beta_i} \operatorname*{l.c.m.}_{1\leqslant i\leqslant k} (r_i - 1) s_i m(s_i) \\ &\ll \operatorname*{l.c.m.}_{1\leqslant i\leqslant k} q_i^{\alpha_i}(q_i - 1) \operatorname*{l.c.m.}_{1\leqslant i\leqslant k} r_i^{\beta_i}. \end{aligned} \tag{38}$$

Since $r_i^{\beta_i} \leqslant x$ and $r_i < 50$ we have

$$\log \operatorname*{l.c.m.}_{1\leqslant i\leqslant k} r_i^{\beta_i} \leqslant \pi(50) \log x = 15 \log x. \tag{39}$$

Similarly

$$\log \operatorname*{l.c.m.}_{i=1,\dots,k} q_i^{\alpha_i}(q_i - 1) \leqslant 2n \log x, \tag{40}$$

where n is the number of distinct terms among $q_i^{\alpha_i}$ $(i = 1, \dots, k)$. Let n_1, n_2 be the number of distinct terms with $\alpha_i = 1$ and $\alpha_i \geqslant 2$, respectively. The condition $\sum_{i=1}^{k} q_i^{\alpha_i/2} \leqslant \sqrt{x}$

implies $\sum_{i=1}^{n_1} p_i^{1/2} \leqslant \sqrt{x}$, where p_i is the ith prime and $\sum_{i=1}^{n_2} P_i^{1/2} \leqslant \sqrt{x}$, where P_i is the ith perfect power with an exponent $\geqslant 2$. Using $p_i \gg i \log i$ and $P_i \gg i^2$ we get

$$n_1^{3/2}(\log n_1)^{1/2} \ll \sqrt{x} \quad \text{and} \quad n_2^2 \ll \sqrt{x}.$$

Hence

$$n = n_1 n_2 \ll x^{1/3}(\log x)^{-1/3}, \tag{41}$$

and the lemma follows from (38)–(41). □

Lemma 8. *If x_i are positive integers and $\sum_{i=1}^{j} x_i \leqslant x$ then*

$$\log \operatorname*{l.c.m.}_{i=1,\dots,j} x_i m(x_i) \leqslant \sqrt{x \log x} + O\big(\sqrt{x \log_2 x}\big).$$

Proof. Let $M = \max \operatorname*{l.c.m.}_{1 \leqslant i \leqslant j} x_i m(x_i)$, where the maximum is taken over all integral points $(x_1, \dots, x_j)$ satisfying $x_i > 1$, $\sum_{i=1}^{j} x_i \leqslant x$, and let $(x_1^0, \dots, x_k^0)$ be a point in which the maximum is attained with the least value of $\sum_{i=1}^{k} x_i$. Since $\sqrt{x_1} + \sqrt{x_2} + \sqrt{x_3} < \sqrt{x}$ implies $x_1 + x_2 + x_3 < x$ it follows from Lemma 6 that

$$x_i^0 = q_i^{\alpha_i} r_i^{\beta_i} s_i, \quad \text{where} \quad q_i, r_i \text{ are primes and } r_i < 50,\ s_i < 50,\ \alpha_i > 0$$

and as in the proof of Lemma 7 we find

$$\log M < \log \operatorname*{l.c.m.}_{1 \leqslant i \leqslant k} q_i^{\alpha_i}(q_i - 1) + 15 \log x + O(1). \tag{42}$$

Now by the classical result of Landau ([7], §61) if $\sum_{i=1}^{k} x_i \leqslant x$ then

$$\log \operatorname*{l.c.m.}_{1 \leqslant i \leqslant k} x_i \leqslant \sqrt{x \log x} + O\big(\sqrt{x}\big)$$

hence

$$\log \operatorname*{l.c.m.}_{1 \leqslant i \leqslant k} q_i^{\alpha_i} \leqslant \sqrt{x \log x} + O\big(\sqrt{x}\big). \tag{43}$$

In order to estimate $\operatorname*{l.c.m.}_{i=1,\dots,k}(q_i - 1)$ we divide the primes q_i into two classes C_1 and C_2 assigning q_i to C_1 if $q_i - 1$ has a prime factor t_i between $a = \log x / \log_2 x$ and $b = \sqrt{x \log_2 x}$ and to C_2 otherwise. Since

$$\sum_{q_i \in C_1} \frac{q_i - 1}{t_i} \leqslant \frac{x}{\log x} \log_2 x$$

we have by the quoted Landau's result

$$\log \operatorname*{l.c.m.}_{q_i \in C_1} \frac{q_i - 1}{t_i} \leqslant \sqrt{x \log_2 x} + O\big(\sqrt{x}\big)$$

and

$$\log \operatorname*{l.c.m.}_{q_i \in C_1}(q_i - 1) \leqslant \log \operatorname*{l.c.m.}_{q_i \in C_1} t_i + \log \operatorname*{l.c.m.}_{q_i \in C_1} \frac{q_i - 1}{t_i} \tag{44}$$
$$\leqslant b + O\Big(\frac{b}{\log b}\Big) + \sqrt{x \log_2 x} + O\big(\sqrt{x}\big) = 2\sqrt{x \log_2 x} + O\big(\sqrt{x}\big).$$

In order to estimate $\operatorname*{l.c.m.}_{q_i \in C_2}(q_i - 1)$ we may assume without loss of generality that $C_2 = \{q_1, \ldots, q_n\}$ and $q_1 < q_2 < \ldots < q_n$. By the upper sieve theory (see [5], p. 134, Theorem 4.2) the number $C_2(t)$ of $q_i \in C_2$, $q_i \leqslant t$ satisfies for $t \geqslant b$

$$C_2(t) \ll \frac{t}{\log t} \prod_{a < p < b} \Big(1 - \frac{1}{p}\Big) \ll \frac{t}{\log t} \frac{\log_2 x}{\log x}.$$

For $i > b/\log b$, we have $q_i \gg b$, hence

$$\frac{b}{\log b} < i = C_2(q_i) \ll \frac{q_i}{\log q_i} \frac{\log_2 x}{\log x} \ll \frac{q_i}{\log^2 x} \log_2 x$$

and

$$q_i \gg \frac{b}{\log b} \frac{\log^2 x}{\log_2 x} \gg \sqrt{\frac{x}{\log_2 x}} \log x.$$

The inequality $\sum_{i=1}^{n} q_i \leqslant x$ implies

$$\Big(n - \frac{b}{\log b}\Big)\sqrt{\frac{x}{\log_2 x}} \log x \ll x,$$

hence

$$n \ll \frac{b}{\log b} + \frac{\sqrt{x \log_2 x}}{\log x} \ll \frac{\sqrt{x \log_2 x}}{\log x}.$$

It follows that

$$\log \operatorname*{l.c.m.}_{q_i \in C_2}(q_i - 1) \leqslant n \log x \ll \sqrt{x \log_2 x}, \tag{45}$$

and the lemma results from (42)–(45). □

Proof of Theorem 1. Let

$$K F(x) \overset{\text{can}}{=} \text{const} \prod_{i=1}^{\varrho} \Phi_i(x)^{e_i}. \tag{46}$$

For each Φ_i we denote by α_i, ν_i the relevant parameters from Lemma 5 and set $c(F) = \operatorname*{l.c.m.}_{1 \leqslant i \leqslant \varrho} E\big(\alpha_i, \mathbb{Q}(\alpha_i)\big)$:

$$\nu = \operatorname*{l.c.m.}_{1 \leqslant i \leqslant \varrho} \nu_i = \big(n, c(F)\big), \quad u = n\nu^{-1}.$$

(i) and (ii) follow immediately. By Lemma 2

$$c(F) \mid 2 \underset{1 \leqslant i \leqslant \varrho}{\text{l.c.m.}} e\big(\alpha_i, \mathbb{Q}(\alpha_i)\big) m\Big(e\big(\alpha_i, \mathbb{Q}(\alpha_i)\big)\Big),$$

where $m(x) = \underset{p \mid x}{\text{l.c.m.}}(p-1)$.

On the other hand, by Lemma 1

$$\sum_{i=1}^{\varrho} \sqrt{e\big(\alpha_i, \mathbb{Q}(\alpha_i)\big)} \ll \sqrt{|KF| \log(2|KF|) \log \|F\|}\,,$$

and if $KF(x) = LF(x)$

$$\sum_{i=1}^{\varrho} e\big(\alpha_i, \mathbb{Q}(\alpha_i)\big) \leqslant \frac{\log \|F\|}{2 \log \vartheta_0}\,.$$

Hence by Lemma 7

$$\log c(F) \ll \big(|KF| \log(2|KF|) \log \|F\|\big)^{1/3} \big(\log |KF| + \log_2 \|F\|\big)^{2/3}$$

and if $KF(x) = LF(x)$, by Lemma 8

$$\log c(F) \leqslant \sqrt{\frac{\log \|F\| \log_2 \|F\|}{2 \log \vartheta_0}} + O\big(\sqrt{\log \|F\| \log_3 \|F\|}\big)$$

(note that $|KF| \geqslant 1$ implies $\|F\| \geqslant 3$, $\log_2 \|F\| > 0$).

In order to prove (iii) we note that by Lemma 5

$$\Phi_i(x^{\nu_i}) \overset{\text{can}}{=} \prod_{j=1}^{r_i} \Phi_{ij}(x) \quad \text{implies} \quad \Phi_i(x^n) \overset{\text{can}}{=} \prod_{j=1}^{r_i} \Phi_{ij}(x^{n/\nu_i}),$$

whence by (46)

$$KF(x^{\nu}) \overset{\text{can}}{=} \text{const} \prod_{i=1}^{\varrho} \prod_{j=1}^{r_i} \Phi_{ij}(x^{\nu/\nu_i})^{\varepsilon_i}, \qquad KF(x^n) \overset{\text{can}}{=} \text{const} \prod_{i=1}^{\varrho} \prod_{j=1}^{r_i} \Phi_{ij}(x^{n/\nu_i})^{\varepsilon_i}.$$

Denoting the polynomials $\Phi_{ij}(x^{\nu/\nu_1})$ $(1 \leqslant i \leqslant \varrho, 1 \leqslant j \leqslant r)$ by $F_1, \ldots, F_s$ we obtain (iii).

It remains to estimate $\Omega = \Omega\big(KF(x^n)\big) = \sum_{i=1}^{\varrho} \varepsilon_i r_i$. By Lemma 5 we have $r_i \leqslant |\Phi_i| \tau(\nu_i)$, hence

$$\Omega \leqslant \sum_{i=1}^{\varrho} \varepsilon_i |\Phi_i| \tau(\nu_i). \tag{47}$$

Since $\nu_i \mid n$ and by (46)

$$\sum_{i=1}^{\varrho} \varepsilon_i |\Phi_i| = |KF|, \tag{48}$$

we get $\Omega \leqslant |KF| \tau(n)$. In order to get the other bound for Ω given in the theorem we note

that (the α_i's not being roots of unity) $E\big(\alpha_i, \mathbb{Q}(\alpha_i)\big) \neq 0$ and $v_i \mid E\big(\alpha_i, \mathbb{Q}(\alpha_i)\big)$ implies

$$\tau(v_i) \leqslant \tau\Big(E\big(\alpha_i, \mathbb{Q}(\alpha_i)\big)\Big). \tag{49}$$

By Lemma 2

$$E\big(\alpha_i, \mathbb{Q}(\alpha_i)\big) \leqslant w_i e\big(\alpha_i, \mathbb{Q}(\alpha_i)\big), \tag{50}$$

where w_i is the number of roots of unity contained in $\mathbb{Q}(\alpha_i)$. Clearly $\varphi(w_i) \leqslant |\Phi_i| \leqslant KF$ hence by the classical Landau's result ([7], §59)

$$w_i \ll |KF| \log_2 |KF|, \quad w_i \leqslant 2|KF|^{1+o(1)}.$$

On the other hand, by Lemma 1

$$e\big(\alpha_i, \mathbb{Q}(\alpha_i)\big) \leqslant 26|KF| \log(7|KF|) \log \|F\|,$$

hence by (50)

$$E\big(\alpha_i, \mathbb{Q}(\alpha_i)\big) \leqslant 100|KF|^{2+o(1)} \log \|F\|. \tag{51}$$

Now by the result of Wigert (cf. [7], §60)

$$\tau(x) < \tau_0(x)^{1+o(1)}, \tag{52}$$

where

$$\tau_0(x) = \exp\Big(\frac{\log 2}{\log_2 x} \log x\Big)$$

and $o(1) \to 0$ as $x \to \infty$.

The function $\tau_0(x)$ is increasing to infinity and we easily deduce from (52) the apparently stronger estimate

$$\tau(y) < \tau_0(x)^{1+o(1)} \quad \text{for all} \quad y \leqslant x.$$

Moreover, for $x, y > e$

$$\tau_0(xy) \leqslant \tau_0(x)\tau_0(y) \leqslant x^{o(1)}\tau_0(y).$$

Hence by (51)

$$\begin{aligned}
\tau\Big(E\big(\alpha_i, \mathbb{Q}(\alpha_i)\big)\Big) &\leqslant \tau_0\big(100|KF|^{2+o(1)} \log \|F\|\big)^{1+o(1)} \\
&\leqslant 10|KF|^{o(1)}\tau_0\big(10 \log \|F\|\big)^{1+o(1)} \\
&= |KF|^{o(1)} \exp\Big(\frac{\log 2 + o(1)}{\log_3 \|F\|} \log_2 \|F\|\Big),
\end{aligned}$$

and the desired estimate for $\Omega\big(KF(x^n)\big)$ follows in view of (47), (48) and (49). □

Proof of Corollary 1. Since $F(0) \neq 0$ we have for some q_i, ε_i

$$F(x) = JF(x) = KF(x) \prod_{i=1}^{j} X_{q_i}(x)^{\varepsilon_i}.$$

By the easy case of Lemma 5 ($v = n$) we get

$$\Omega\big(X_{q_i}(x^n)\big) \leqslant |X_{q_i}|\tau(n).$$

Hence

$$\Omega\big(F(x^n)\big) = \Omega\big(KF(x^n)\big) + \sum_{i=1}^{j} \varepsilon_i \Omega\big(X_{q_i}(x^n)\big)$$

$$\leqslant |KF|\tau(n) + \sum_{i=1}^{j} \varepsilon_i |X_{q_i}|\tau(n) = |F|\tau(n). \qquad \square$$

Proof of Corollary 2. If $b(x) = a_0 + a_1 x^n$ it is sufficient to take in the theorem $F(x) = a_0 + a_1 x$. $\square$

Proof of Corollary 3. By Corollary to Lemma 1

$$\Omega\big(Lt(x)\big) < \frac{\log \|t\|}{2 \log \vartheta_0}.$$

On the other hand, if $t(x) = a_0 + a_1 x^{n_1} + a_2 x^{n_2}$ we have

$$\frac{t(x)}{Lt(x)} \;\Big|\; (a_0 x^{n_2} + a_2) t(x) - a_1 x^{n_1+n_2} t(x^{-1}) = a_0 a_2 x^{2n_2} + (a_0^2 + a_2^2 - a_1^2) x^{n_2} + a_0 a_2. \tag{53}$$

Taking in the theorem $F(x) = a_0 a_2 x^2 + (a_0^2 + a_2^2 - a_1^2)x + a_0 a_2$ we get $\|F\| \leqslant 2\|t\|^2$,

$$\Omega\big(KF(x^{n_2})\big) \ll \exp\Big(\frac{\log 2 + o(1)}{\log_3 \|t\|} \log_2 \|t\|\Big) = o(\log \|t\|)$$

and since by (53)

$$\frac{Kt(x)}{Lt(x)} \;\Big|\; KF(x^{n_2})$$

the corollary follows. $\square$

Examples. In order to show that the estimates for $c(F)$ and $\Omega\big(KF(x^n)\big)$ given in Theorem 1 are sharp we consider the following two examples

1. $n = \prod\limits_{p \leqslant t} p, \quad F(x) = \prod\limits_{p \leqslant t} f_p(x);$
2. $n = \prod\limits_{p \leqslant t} p, \quad F(x) = (2^n x - 1)^m,$

where p runs over primes, $f_p(x)$ is given by (9) and t, m are parameters.

In the case 1 we have $F = KF = LF$ since f_p are non-reciprocal,

$$|KF| = 3\pi(t) \ll t/\log t,$$

and by (10)

$$\log \|F\| \leqslant 2 \log l(F) \leqslant 2 \sum_{p \leqslant t} \log l(f_p)$$

$$\leqslant 2 \sum_{p \leqslant t} \big(p \log \nu_0 + O(\vartheta_0^{-p/2})\big) = \log \vartheta_0 \, \frac{t^2}{\log t} + O\Big(\frac{t^2}{(\log t)^2}\Big).$$

Hence

$$\big(|KF| \log(2|KF|) \log \|F\|\big)^{1/3} \big(\log |KF| + \log_2 \|F\|\big)^{2/3} \ll t \, (\log t)^{1/3},$$

$$\sqrt{\frac{\log \|F\| \log_2 \|F\|}{2 \log \vartheta_0}} \leqslant t + O\Big(\frac{t}{\log t}\Big).$$

On the other hand, by Lemma 1

$$e\big(\vartheta_0, \mathbb{Q}(\vartheta_0)\big) \leqslant \frac{\log 3}{2 \log \vartheta_0} < 2,$$

hence $e\big(\vartheta_0, \mathbb{Q}(\vartheta_0)\big) = 1$, $e\big(\vartheta_0^p, \mathbb{Q}(\vartheta_0)\big) = p$. By Capelli's theorem $x^\nu - \vartheta_0^p$ is reducible in $\mathbb{Q}(\vartheta_0)$ if and only if $\nu \equiv 0 \bmod p$. By (9) and Capelli's lemma $\nu \equiv 0 \bmod p$ is also a necessary and sufficient condition for the reducibility of $f_p(x)$. Hence for all proper divisors ν of n

$$\Omega\big(F(x^\nu)\big) < \Omega\big(F(x^n)\big)$$

and if ν satisfies (ii) and (iii) we have $\nu = n$,

$$\log \nu = \sum_{p \leqslant t} \log p = t + O\Big(\frac{t}{\log t}\Big).$$

In the case 2 we have

$$|KF| = |F| = m,$$

$$\log \|F\| \leqslant 2 \log l(F) \leqslant 2m \log(2^n + 1) \leqslant 3mn,$$

$$\frac{\log_2 \|F\|}{\log_3 \|F\|} \leqslant o(\log m) + \frac{\log n}{\log_2 n} = o(\log m) + \frac{t}{\log t} + O\Big(\frac{t}{\log^2 t}\Big)$$

$$= o(\log m) + \pi(t) + o\big(\pi(t)\big).$$

Hence

$$|KF| \tau(n) = m \cdot 2^{\pi(t)},$$

$$|KF|^{1+o(1)} \exp\Big(\frac{\log 2 + o(1)}{\log_3 \|F\|} \log_2 \|F\|\Big) < m^{1+o(1)} \cdot 2^{\pi(t)+o(\pi(t))}.$$

On the other hand

$$KF(x^n) = \prod_{d \mid n} X_d(2x)^m, \quad \Omega\big(KF(x^n)\big) = m\tau(n) = m \cdot 2^{\pi(t)}.$$

3.

Lemma 9. *Let $P(x_1, \dots, x_k)$, $Q(x_1, \dots, x_k)$ be polynomials, $(P, Q) = G$.*
For any positive integers $n_1, \dots, n_k$ we have

$$\big(P(x_1^{n_1}, \dots, x_k^{n_k}), Q(x_1^{n_1}, \dots, x_k^{n_k})\big) = G(x_1^{n_1}, x_2^{n_2}, \dots, x_k^{n_k}).$$

Proof. Let $P = GP_0$, $Q = GQ_0$ and let $R(x_2, \dots, x_k)$ be the resultant of P_0 and Q_0 with respect to x_1. There exist polynomials U and V such that

$$UP_0 + VQ_0 = R.$$

From

$$U(x_1^{n_1}, \dots, x_k^{n_k})P_0(x_1^{n_1}, \dots, x_k^{n_k}) + V(x_1^{n_1}, \dots, x_k^{n_k})Q_0(x_1^{n_1}, \dots, x_k^{n_k}) = R(x_2^{n_2}, \dots, x_k^{n_k})$$

we infer that $\big(P_0(x_1^{n_1}, \dots, x_k^{n_k}), Q_0(x_1^{n_1}, \dots, x_k^{n_k})\big)$ does not depend upon x_1. Since the same argument applies to other variables we have

$$\big(P_0(x_1^{n_1}, \dots, x_k^{n_k}), Q_0(x_1^{n_1}, \dots, x_k^{n_k})\big) = \text{const}$$

and the lemma follows. □

Lemma 10. *If Ψ is an absolutely irreducible polynomial with algebraic coefficients, one of which is rational $\neq 0$, and $\boldsymbol{\Omega}$ is the field generated by these coefficients then $N_{\boldsymbol{\Omega}/\mathbb{Q}}\Psi(X)$ is irreducible ($X = (x_1, \dots, x_k)$).*

Proof. Let Φ be the irreducible factor of $N_{\boldsymbol{\Omega}/\mathbb{Q}}\Psi(X)$ divisible by $\Psi(X)$. For all isomorphic injections σ of $\boldsymbol{\Omega}$ into the complex field $\mathbb{C}$ we have

$$\Psi^\sigma(X) \mid \Phi(X)$$

hence

$$\prod_\sigma \Psi^\sigma(X) = N_{\boldsymbol{\Omega}/\mathbb{Q}}\Psi(X) \mid \Phi(X)^{[\boldsymbol{\Omega}:\mathbb{Q}]}.$$

Since $\Phi(X)$ is irreducible

$$N_{\boldsymbol{\Omega}/\mathbb{Q}}\Psi(X) = \text{const}\,\Phi(X)^a, \quad \Psi(X)^a \mid N_{\boldsymbol{\Omega}/\mathbb{Q}}\Psi(X) \tag{54}$$

and

$$\Psi(X)^{a-1} \mid \prod{}' \Psi^\sigma(X), \tag{55}$$

where $\prod'$ is taken over all injections σ different from the identity e. However for such injections

$$\Psi^\sigma(X) \neq \Psi(X)$$

by the definition of $\boldsymbol{\Omega}$, and since $\Psi^\sigma(X)$, $\Psi(X)$ have a common non-zero coefficient

$$\Psi^\sigma(X) \neq \text{const}\,\Psi(X).$$

Since $\Psi(X)$ is absolutely irreducible and of the same degree as $\Psi^\sigma(X)$ with respect to all the variables it follows that

$$\big(\Psi(X), \Psi^\sigma(X)\big) = 1 \quad (\sigma \neq e).$$

Hence by (55) $a = 1$ and the lemma follows from (54). □

Lemma 11. *If $\Phi(x)$ is irreducible, $\gamma_1, \dots, \gamma_k$ are integers and $(\gamma_1, \dots, \gamma_k) = 1$ then $J\Phi(x_1^{\gamma_1}, \dots, x_k^{\gamma_k})$ is irreducible.*

Proof. Let $\Phi(\alpha) = 0$. If, say, $\gamma_1 \neq 0$ then

$$b(x_1, \dots, x_k) = J(x_1^{\gamma_1} \cdots x_k^{\gamma_k} - \alpha)$$

is a binomial with respect to x_1 over $\mathbb{C}(x_2, \dots, x_k)$. By Capelli's theorem it is irreducible over that field. But b has no factor independent of x_1, hence it is irreducible over $\mathbb{C}$. Since

$$J\Phi(x_1^{\gamma_1}, \dots, x_k^{\gamma_k}) = \text{const}\, N_{\mathbb{Q}(\alpha)/\mathbb{Q}} b(x_1, \dots, x_k)$$

the lemma follows from the preceding one. □

Lemma 12. *Let $\Phi(x_1, \dots, x_k) \neq \text{const}\, x_j$ be irreducible and not of the form $J\Phi_0(x_1^{\delta_1} \cdots x_k^{\delta_k})$, where $\Phi_0 \in \mathbb{Q}[x]$ and $\delta_1, \dots, \delta_k$ are integers. For any positive integers $n_1, \dots, n_k$ there exist positive integers $\mu_1, \dots, \mu_k$, $u_1, \dots, u_k$ such that*

$$\mu_j \leqslant |\Phi|^2, \tag{56}$$

$$n_j = \mu_j u_j, \tag{57}$$

and

$$\Phi(x_1^{\mu_1}, \dots, x_k^{\mu_k}) \overset{\text{can}}{=} \text{const} \prod_{g=1}^{h} \Phi_g(x_1, \dots, x_k)^{e_g} \tag{58}$$

implies $e_g = 1$ $(1 \leqslant g \leqslant h)$ and

$$\Phi(x_1^{n_1}, \dots, x_k^{n_k}) \overset{\text{can}}{=} \text{const} \prod_{g=1}^{h} \Phi_g(x_1^{u_1}, \dots, x_k^{u_k}).$$

Proof. Let Ψ be an absolutely irreducible factor of Φ with the leading coefficient 1. (By the leading coefficient we mean here the coefficient of the first term in the inverse lexicographic order.) By the classical theorem of Kronecker the coefficients of Ψ are algebraic. If $\boldsymbol{\Omega}_0$ is the field generated by them then by Lemma 10

$$N_{\boldsymbol{\Omega}_0/\mathbb{Q}} \Psi(x_1, \dots, x_k)$$

is irreducible, and since it has a factor in common with $\Phi(x_1, \dots, x_k)$

$$\Phi(x_1, \dots, x_k) = \text{const}\, N_{\boldsymbol{\Omega}_0/\mathbb{Q}} \Psi(x_1, \dots, x_k). \tag{59}$$

If Ψ has only two terms then

$$\Psi = J(x_1^{\delta_1} \cdots x_k^{\delta_k} - \alpha)$$

for a suitable α and suitable integers $\delta_1, \dots, \delta_k$. Here $\boldsymbol{\Omega}_0 = \mathbb{Q}(\alpha)$ and if Φ_0 is the minimal polynomial of α

$$N_{\boldsymbol{\Omega}_0/\mathbb{Q}}\Psi(x_1, \dots, x_k) = J\Phi_0(x_1^{\delta_1} \cdots x_k^{\delta_k}),$$

which together with (59) contradicts the assumption. Thus Ψ has more than two terms and by Gourin's theorem there exist positive integers $\mu_1, \dots, \mu_k; u_1, \dots, u_k$ such that

$$\mu_j \leqslant |\Psi|^2, \quad n_j = \mu_j u_j$$

and

(60) every absolutely irreducible factor of $\Psi(x_1^{n_1}, \dots, x_k^{n_k})$ is of the form $T(x_1^{u_1}, \dots, x_k^{u_k})$, where $T \in \mathbb{C}[x_1, \dots, x_k]$.

Since $|\Psi| \leqslant |\Phi|$ the numbers μ_j, u_j satisfy the conditions (56) and (57). Assume now (58). For at least one $j \leqslant k$ we have

$$\frac{\partial \Phi}{\partial x_j}(x_1, \dots, x_k) \neq 0,$$

hence by the irreducibility of Φ

$$\left(\Phi(x_1, \dots, x_k), \frac{\partial \Phi}{\partial x_j}(x_1, \dots, x_k)\right) = 1$$

and by Lemma 9

$$\left(\Phi(x_1^{\mu_1}, \dots, x_k^{\mu_k}), \frac{\partial \Phi}{\partial x_j}(x_1^{\mu_1}, \dots, x_k^{\mu_k})\right) = 1.$$

Since also

$$\left(\Phi(x_1^{\mu_1}, \dots, x_k^{\mu_k}), x_j\right) = 1$$

it follows that

$$\left(\Phi(x_1^{\mu_1}, \dots, x_k^{\mu_k}), \frac{\partial}{\partial x_j}\Phi(x_1^{\mu_1}, \dots, x_k^{\mu_k})\right) = 1,$$

which proves that $e_g = 1$ $(g \leqslant h)$. (Cf. Remark on p. 148 in [11] (2).) The polynomials $\Phi_g(x_1^{u_1}, \dots, x_k^{u_k})$ are clearly non-constant, and by Lemma 9 they are prime to each other. To show that they are irreducible let Ψ_g denote an absolutely irreducible factor of $\Phi_g(x_1^{u_1}, \dots, x_k^{u_k})$ with the leading coefficient 1. By Kronecker's theorem the coefficients of Ψ_g are algebraic. By (57) and (58) we have

$$\Psi_g(x_1, \dots, x_k) \mid \Phi(x_1^{n_1}, \dots, x_k^{n_k})$$

and in view of (59) there exists a conjugate Ψ_g^σ of Ψ_g such that

$$\Psi_g^\sigma(x_1, \dots, x_k) \mid \Psi(x_1, \dots, x_k).$$

Ψ_g^σ is absolutely irreducible and by (60)

$$\Psi_g^\sigma(x_1, \dots, x_k) = T(x_1^{u_1}, \dots, x_k^{u_k}), \tag{61}$$

(2) Page 369 in this volume.

where $T \in \mathbb{C}[x_1, \dots, x_k]$.

The coefficients of Ψ_g^σ generate an algebraic number field $\boldsymbol{\Omega}_g$ and by Lemma 10

$$N = N_{\boldsymbol{\Omega}_g/\mathbb{Q}} \Psi_g^\sigma(x_1, \dots, x_k) \quad \text{is irreducible.} \tag{62}$$

Since N has with $\Phi_g(x_1^{u_1}, \dots, x_k^{u_k})$ the common factor Ψ_g we have

$$N \mid \Phi_g(x_1^{u_1}, \dots, x_k^{u_k})$$

and by (61)

$$N_{\boldsymbol{\Omega}_g/\mathbb{Q}}\big(T(x_1^{u_1}, \dots, x_k^{u_k})\big) \mid \Phi_g(x_1^{u_1}, \dots, x_k^{u_k}).$$

However $T \in \boldsymbol{\Omega}_g[x_1, \dots, x_k]$

$$N_{\boldsymbol{\Omega}_g/\mathbb{Q}}\big(T(x_1^{u_1}, \dots, x_k^{u_k})\big) = \big(N_{\boldsymbol{\Omega}_g/\mathbb{Q}} T\big)(x_1^{u_1}, \dots, x_k^{u_k}).$$

Therefore it follows from Lemma 9 that

$$N_{\boldsymbol{\Omega}_g/\mathbb{Q}} T(x_1, \dots, x_k) \mid \Phi_g(x_1, \dots, x_k)$$

and from the irreducibility of Φ_g that

$$\Phi_g(x_1, \dots, x_k) = \text{const}\, N_{\boldsymbol{\Omega}_g/\mathbb{Q}} T(x_1, \dots, x_k).$$

Thus by (61)

$$\Phi_g(x_1^{u_1}, \dots, x_k^{u_k}) = \text{const}\, N_{\boldsymbol{\Omega}_g/\mathbb{Q}} T(x_1^{u_1}, \dots, x_k^{u_k}) = \text{const}\, N$$

and the missing assertion of the lemma follows from (62). □

Remark. Lemma 12 remains true for polynomials over any field $\boldsymbol{\Omega}$ of characteristic 0. If the characteristic is positive the lemma has to be modified.

Proof of Theorem 2. Let us observe first that

$$K F(x_1^{n_1}, \dots, x_k^{n_k}) = (K F)(x_1^{n_1}, \dots, x_k^{n_k}). \tag{63}$$

Indeed, if $f(x_1, \dots, x_k) \mid J(x_1^{\delta_1} \cdots x_k^{\delta_k} - 1)$ then

$$f(x_1^{n_1}, \dots, x_k^{n_k}) \mid J(x_1^{n_1\delta_1} \cdots x_k^{n_k\delta_k} - 1)$$

hence the left hand side of (63) divides the right hand side. On the other hand for any integral vector $[\delta_1, \dots, \delta_k] \neq \mathbf{0}$

$$\big(K F(x_1, \dots, x_k), J(x_1^{n\delta_1/n_1} \cdots x_k^{n\delta_k/n_k} - 1)\big) = 1, \quad \text{where} \quad n = n_1 \cdots n_k.$$

Hence by Lemma 9

$$\big((K F)(x_1^{n_1}, \dots, x_k^{n_k}), J(x_1^{n\delta_1} \cdots x_k^{n\delta_k} - 1)\big) = 1$$

and since

$$J(x_1^{\delta_1} \cdots x_k^{\delta_k} - 1) \mid J(x_1^{n\delta_1} \cdots x_k^{n\delta_k} - 1)$$

we get

$$\big((K F)(x_1^{n_1}, \dots, x_k^{n_k}), J(x_1^{\delta_1} \cdots x_k^{\delta_k} - 1)\big) = 1.$$

This proves (63). Let now

$$KF(x_1,\dots,x_k) \overset{\text{can}}{=} \text{const}\prod_{i=1}^{r}\Phi_i(x_1,\dots,x_k)^{\varepsilon_i}, \tag{64}$$

where, for $i \leqslant r_0$, Φ_i is of the form $J\Phi_{i0}(x_1^{\delta_{i1}}\cdots x_k^{\delta_{ik}})$ for a suitable Φ_{i0} and suitable integers $\delta_{i1},\dots,\delta_{ik}$ while, for $i > r_0$, Φ_i is not of this form. Clearly, for each $i \leqslant r_0$, Φ_{i0} is irreducible and non-cyclotomic, hence denoting any of its zeros by α_i we have $c_i = E\big(\alpha_i, \mathbb{Q}(\alpha_i)\big) \neq 0$. Let us set

$$c(F) = \text{l.c.m.}\big\{c_1,\dots,c_{r_0},1,2,\dots,\max_{i>r_0}|\Phi_i|^2\big\},$$
$$v_j = \big(c(F),n_j\big), \quad v_j = n_j v_j^{-1} \quad (1\leqslant j\leqslant k),$$
$$\delta_i(\boldsymbol{n}) = (\delta_{i1}n_1,\dots,\delta_{ik}n_k) \quad (1\leqslant i\leqslant r_0),$$
$$\delta_i = \big(\delta_i(\boldsymbol{n}),c_i\big) \quad (1\leqslant i\leqslant r_0).$$

The conditions (iv) and (v) are clearly satisfied.

By Lemma 5 for each $i \leqslant r_0$

$$\Phi_{i0}(x^{\delta_i}) \overset{\text{can}}{=} \prod_{g=1}^{h_i}\Phi_{ig}(x)$$

implies

$$\Phi_{i0}(x^{\delta_i(\boldsymbol{n})}) \overset{\text{can}}{=} \prod_{g=1}^{h_i}\Phi_{ig}(x^{\delta_i(\boldsymbol{n})/\delta_i}).$$

Setting in Lemma 11

$$\gamma_j = \delta_{ij}n_j/\delta_i(\boldsymbol{n}) \quad (1\leqslant j\leqslant k)$$

we infer that for all $g \leqslant h_i$ the polynomials

$$J\Phi_{ig}\Big(\prod_{j=1}^{k}x_j^{\gamma_j\delta_i(\boldsymbol{n})/\delta_i}\Big) = J\Phi_{ig}\Big(\prod_{j=1}^{k}x_j^{\delta_{ij}n_j/\delta_i}\Big)$$

are irreducible. Since

$$J\Phi_{i0}\Big(\prod_{j=1}^{k}x_j^{\gamma_j\delta_i(\boldsymbol{n})}\Big) = J\Phi_{i0}\Big(\prod_{j=1}^{k}x_j^{\delta_{ij}n_j}\Big) = \Phi_i(x_1^{n_1},\dots,x_k^{n_k})$$

we get

$$\Phi_i(x_1^{n_1},\dots,x_k^{n_k}) \overset{\text{can}}{=} \prod_{g=1}^{h_i}J\Phi_{ig}\Big(\prod_{j=1}^{k}x_j^{\delta_{ij}n_j/\delta_i}\Big) \quad (1\leqslant i\leqslant r_0). \tag{65}$$

Since by the definition of $c(F)$ and v_j, $\delta_i \mid \delta_{ij}v_j$ $(1\leqslant j\leqslant k)$ the substitution $x_j \to x_j^{v_j/n_j}$

$(1 \leqslant j \leqslant k)$ gives

$$\Phi_i(x_1^{\nu_1}, \dots, x_k^{\nu_k}) \overset{\text{can}}{=} \prod_{g=1}^{h_i} J\Phi_{ig}\Big(\prod_{j=1}^{k} x_j^{\delta_{ij}\nu_j/\delta_i}\Big) \quad (1 \leqslant i \leqslant r_0). \tag{65'}$$

For $i > r_0$ there exist by Lemma 12 positive integers μ_{ij} and u_{ij} $(1 \leqslant j \leqslant k)$ such that

$$\mu_{ij} \leqslant |\Phi_i|^2, \quad n_j = \mu_{ij} u_{ij},$$

and

$$\Phi_i(x_1^{\mu_{i1}}, \dots, x_k^{\mu_{ik}}) \overset{\text{can}}{=} \prod_{g=1}^{h_i} \Phi_{ig}(x_1, \dots, x_k)$$

implies

$$\Phi_i(x_1^{n_1}, \dots, x_k^{n_k}) \overset{\text{can}}{=} \prod_{g=1}^{h_i} \Phi_{ig}(x_1^{u_{i1}}, \dots, x_k^{u_{ik}}). \tag{66}$$

By the definition of $c(F)$ we have $\mu_{ij} \mid c(F)$, hence

$$\mu_{ij} \mid \nu_j, \quad \nu_j \mid u_{ij} \quad (r_0 < i \leqslant r,\ 1 \leqslant j \leqslant k).$$

The substitution $x_j \to x_j^{1/\nu_j}$ applied to (66) gives

$$\Phi_i(x_1^{\nu_1}, \dots, x_k^{\nu_k}) \overset{\text{can}}{=} \prod_{g=1}^{h_i} \Phi_{ig}(x_1^{\nu_1/\mu_{i1}}, \dots, x_k^{\nu_k/\mu_{ik}}). \tag{66'}$$

From (63), (64), (65), (65′), (66), (66′) and Lemma 9 we infer that

$$KF(x_1^{n_1}, \dots, x_k^{n_k}) \overset{\text{can}}{=} \text{const} \prod_{i=1}^{r_0} \prod_{g=1}^{h_i} J\Phi_{ig}\Big(\prod_{j=1}^{k} x_j^{\delta_{ij} n_j/\delta_i}\Big)^{\varepsilon_i} \times \prod_{i=r_0+1}^{r} \prod_{g=1}^{h_i} \Phi_{ig}(x_1^{u_{i1}}, \dots, x_k^{u_{ik}})^{\varepsilon_i},$$

$$KF(x_1^{\nu_1}, \dots, x_k^{\nu_k}) \overset{\text{can}}{=} \text{const} \prod_{i=1}^{r_0} \prod_{g=1}^{h_i} J\Phi_{ig}\Big(\prod_{j=1}^{k} x_j^{\delta_{ij}\nu_j/\delta_i}\Big)^{\varepsilon_i} \times \prod_{i=r_0+1}^{r} \prod_{g=1}^{h_i} \Phi_{ig}(x_1^{\nu_1/\mu_{i1}}, \dots, x_k^{\nu_k/\mu_{ik}})^{\varepsilon_i}.$$

Denoting the polynomials

$$J\Phi_{ig}\Big(\prod_{j=1}^{k} x_j^{\delta_{ij}\nu_j/\delta_i}\Big) \quad (1 \leqslant i \leqslant r_0,\ 1 \leqslant g \leqslant h_i)$$

and

$$\Phi_{ig}(x_1^{\nu_1/\mu_{i1}}, \ldots, x_k^{\nu_k/\mu_{ik}}) \quad (r_0 < i \leqslant r,\ 1 \leqslant g \leqslant h_i)$$

by $F_1, \ldots, F_s$ we get (vi). □

4.

Lemma 13. *Let a_j $(0 \leqslant j \leqslant k)$ be non-zero integers. If*

$$a_0 + \sum_{j=1}^{k} a_j \lambda^{n_j} = a_0 + \sum_{j=1}^{k} a_j \lambda^{-n_j} = 0 \tag{67}$$

then either λ is an algebraic unit or there exist integers γ_j $(1 \leqslant j \leqslant k)$ such that

$$\sum_{j=1}^{k} \gamma_j n_j = 0 \tag{68}$$

and

$$0 < \max_{1 \leqslant j \leqslant k} |\gamma_j| < \max_{0 \leqslant j \leqslant k} \frac{\log a_j^2}{\log 2}\,. \tag{69}$$

Proof. If λ is not a unit then for a certain prime ideal $\mathfrak{p}$ of $\mathbb{Q}(\lambda)$ we have $\operatorname{ord}_{\mathfrak{p}} \lambda = \xi \neq 0$. Let p be the rational prime divisible by $\mathfrak{p}$ and let $\operatorname{ord}_{\mathfrak{p}} p = e$, $\operatorname{ord}_{\mathfrak{p}} a_j = \alpha_j$ $(0 \leqslant j \leqslant k)$. It follows from (67) that for $\varepsilon = \pm 1$ the minimal term of the sequence $\{e\alpha_j + \varepsilon n_j \xi\}$ $(j = 0, 1, \ldots, k)$ must occur in it at least twice (we take $n_0 = 0$). Thus we have for suitable non-negative indices g, h, i, j

$$\begin{aligned} e\alpha_g - n_g\xi &= e\alpha_h - n_h\xi, \quad g < h, \\ e\alpha_i + n_i\xi &= e\alpha_j + n_j\xi, \quad i < j. \end{aligned} \tag{70}$$

Hence

$$e(\alpha_i - \alpha_j)(n_h - n_g)\xi = e(\alpha_h - \alpha_g)(n_j - n_i)\xi,$$

and since $\xi \neq 0$

$$(\alpha_i - \alpha_j)(n_h - n_g) - (\alpha_h - \alpha_g)(n_j - n_i) = 0. \tag{71}$$

This gives the desired relation (68) unless

$$\alpha_i - \alpha_j = \alpha_h - \alpha_g = 0$$

or

$$\alpha_i - \alpha_j = \alpha_h - \alpha_g \quad \text{and} \quad i = g,\ j = h.$$

The latter possibility however reduces to the former and both give by (70) $n_g = n_h$, $n_i = n_j$. In order to get (69) we notice that the coefficients of n_g, n_h, n_i, n_j in (71) do not

exceed

$$2 \max_{0\leqslant j\leqslant k} \alpha_j \leqslant 2 \max_{0\leqslant j\leqslant k} \frac{\log|a_j|}{\log p} \leqslant \max_{0\leqslant j\leqslant k} \frac{\log a_j^2}{\log 2}. \qquad \square$$

Lemma 14. *If real numbers a_j $(0 \leqslant j \leqslant k)$ and a certain λ satisfy* (67) *and moreover*

$$0 < n_1 < n_2 < \ldots < n_k, \quad |a_0| + |a_k| \geqslant \sum_{j=1}^{k-1} |a_j| > 0 \tag{72}$$

then $|\lambda| = 1$.

Proof. Choose $\varepsilon = \pm 1$ so that $|a_k + \varepsilon a_0| = |a_k| + |a_0|$ and consider the polynomial

$$F(x) = a_0 + \sum_{j=1}^{k} a_j x^{n_j} + \varepsilon x^{n_k}\Big(a_0 + \sum_{j=1}^{k} a_j x^{-n_j}\Big).$$

$F(x)$ is reciprocal of degree n_k. By a theorem of A. Cohn ([2], p. 113) the equations $F(x) = 0$ and $x^{n_k-1}F'(x^{-1}) = 0$ have the same number of zeros inside the unit circle. We have

$$\begin{aligned} G(x) &= x^{n_k-1}F'(x^{-1}) \\ &= x^{n_k-1}\Big(\sum_{j=1}^{k} a_j n_j x^{1-n_j} + \varepsilon a_0 n_k x^{1-n_k} + \varepsilon \sum_{j=1}^{k-1} a_j (n_k - n_j) x^{1+n_j-n_k}\Big) \\ &= (a_k + \varepsilon a_0) n_k + \sum_{j=1}^{k-1} a_j n_j x^{n_k-n_j} + \varepsilon \sum_{j=1}^{k-1} a_j (n_k - n_j) x^{n_j}. \end{aligned}$$

Assuming $G(x) = 0$ for $|x| < 1$ we get

$$|a_k + \varepsilon a_0| n_k < \sum_{j=1}^{k-1} |a_j| n_j + \sum_{j=1}^{k-1} |a_j|(n_k - n_j) = n_k \sum_{j=1}^{k-1} |a_j|,$$

$$|a_k| + |a_0| = |a_k + \varepsilon a_0| < \sum_{j=1}^{k-1} |a_j|,$$

a contradiction. Thus all zeros of $G(x)$ and $F(x)$ are on the unit circle. Since by (67) $F(\lambda) = 0$ we get $|\lambda| = 1$. $\square$

Lemma 15. *If $f(x) = a_0 + \sum_{j=1}^{k} a_j x^{n_j}$ satisfies* (72) *then either $Kf(x) = Lf(x)$ or there exist integers $\gamma_1, \ldots, \gamma_k$ satisfying* (68) *and* (69). *In any case*

$$\Omega\big(Kf(x)/Lf(x)\big) \leqslant \Omega_0\big((a_0, a_k)\big).$$

Proof. Let

$$\frac{Kf(x)}{Lf(x)} \overset{\text{can}}{=} c\prod_{i=1}^{h} f_i(x)^{e_i},$$

where $f_i(x)$ are primitive polynomials with the leading coefficients $c_i > 0$ $(1 \leqslant i \leqslant h)$. Comparing the leading coefficients on both sides we get

$$c = \prod_{i=1}^{h} c_i^{-e_i}.$$

Comparing the contents we get

$$C(Lf) = C(Kf)\prod_{i=1}^{h} c_i^{e_i}.$$

Since Lf has the same leading coefficient as f and the same up to a sign constant term it follows that

$$\prod_{i=1}^{h} c_i^{e_i} \mid (a_0, a_k). \tag{73}$$

If for any $i \leqslant h$ we had $c_i = 1$ the zeros of f_i, which by Lemma 13 lie on the unit circle, by Kronecker's theorem would have to be roots of unity contrary to the definition of Kf. Thus for all $i \leqslant h$ we have $c_i > 1$ and (73) gives the second part of the lemma. To prove the first note that if $h > 0$ we can take for λ in Lemma 13 any zero of f_1. □

Lemma 16. *Let* $0 < n_1 < \ldots < n_k$ *and let* a_j $(0 \leqslant j \leqslant k)$ *be non-zero integers. If* $f(x) = a_0 + \sum_{j=1}^{k} a_j x^{n_j}$ *satisfies for some* $g, h \leqslant k$

$$a_g^2 \not\equiv a_h^2 \bmod \operatorname*{g.c.d.}_{0\leqslant j\leqslant k} a_j \operatorname*{g.c.d.}_{j\neq g,h} a_j \tag{74}$$

then either $Lf(x) = Jf(x)$ *or there exist integers* γ_j $(1 \leqslant j \leqslant k)$ *satisfying* (68) *and* (69). *In any case* $\Omega\big(f(x)/Lf(x)\big) \leqslant \Omega_0\big((a_0, a_k)\big)$.

Proof. Let

$$\frac{f(x)}{Lf(x)} \overset{\text{can}}{=} c\prod_{i=1}^{h} f_i(x)^{e_i},$$

where $f_i(x)$ are primitive polynomials with the leading coefficients $c_i > 0$. By the argument used in the proof of Lemma 15 we deduce again the divisibility (73).

If for $i \leqslant h$ we had $c_i = 1$ any zero λ of f_i would be a unit and would satisfy (67). Setting

$$\operatorname*{g.c.d.}_{0\leqslant j\leqslant k} a_j = \delta, \quad \operatorname*{g.c.d.}_{j\neq g,h} a_j = d$$

we would get from (67)

$$a_g\lambda^{n_g} + a_h\lambda^{n_h} \equiv 0 \bmod d, \quad a_g\lambda^{-n_g} + a_h\lambda^{-n_h} \equiv 0 \bmod d;$$
$$a_g\delta^{-1} \equiv -a_h\delta^{-1}\lambda^{n_h-n_g} \bmod d\delta^{-1}, \quad a_g\delta^{-1} \equiv -a_h\delta^{-1}\lambda^{n_g-n_h} \bmod d\delta^{-1};$$
$$a_g^2\delta^{-2} \equiv a_h^2\delta^{-2} \bmod d\delta^{-1}; \quad a_g^2 \equiv a_h^2 \bmod d\delta$$

contrary to (74). Thus for $i \leqslant h$ we have $c_i > 1$ and (73) gives the second part of the lemma. The first follows from Lemma 13 on taking for λ any hypothetical zero of $f(x)/Lf(x)$.□

Proof of Theorem 3. By Theorem 4 of [11] either $Lf(x)$ is irreducible or there are integers $\gamma_1, \ldots, \gamma_k$ satisfying (vii) and (viii). All zeros of the quotient $f(x)/Lf(x)$ satisfy the assumptions of Lemma 13. Since (69) implies (viii) it follows that unless (vii) and (viii) are satisfied all primitive factors of $f(x)/Lf(x)$ are reciprocal and monic. The remaining part of the theorem follows at once from Lemmata 15 and 16. □

5.

Lemma 17. *If* $|a_0| = |a_3| > 0$, $|a_1| = |a_2| > 0$ *and* $0 < n_1 < n_2 < n_3$ *then either the quadrinomial* $q(x) = a_0 + \sum_{j=1}^{3} a_j x^{n_j}$ *is reciprocal or* $Kq(x) = Lq(x)$.

Proof. $q(\lambda) = q(\lambda^{-1}) = 0$ implies

$$a_0 + a_3\lambda^{n_3} = -a_1\lambda^{n_1} - a_2\lambda^{n_2},$$
$$a_0 + a_3\lambda^{-n_3} = -a_1\lambda^{-n_1} - a_2\lambda^{-n_2}.$$

Dividing the above equalities side by side we get

$$\frac{a_3}{a_0}\lambda^{n_3} = \frac{a_2}{a_1}\lambda^{n_2+n_1},$$

and either λ is a root of unity or $n_3 = n_2 + n_1$ and $a_3/a_0 = a_2/a_1$ in which case $q(x)$ is reciprocal. □

Lemma 18. *If a quadrinomial* $q(x) = a_0 + \sum_{j=1}^{3} a_j x^{n_j}$ *is representable in one of the forms* (1)*, where* k, T, U, V, W *are monomials in* $\mathbb{Q}(x)$ *then it is also representable in the same form where* $\pm k = C(q)$*,* T, U, V, W *are monomials in* $\mathbb{Z}[x]$ *and the factors on the right hand side of* (1) *differ from the original ones by monomial factors.*

Proof. Let $T = \frac{t}{m^3} 2^{\tau_1} x^{\tau}$, $U = \frac{u}{m} 2^{\varphi_1} x^{\varphi}$, $V = \frac{v}{m} 2^{\psi_1} x^{\psi}$, $W = \frac{w}{m} 2^{\omega_1} x^{\omega}$, $k = k' 2^{\kappa_1} x^{\kappa}$, where m, t, u, v, w, k' odd, $m > 0$.

If

$$q(x) = k(T^2 - 4TUVW - U^2V^4 - 4U^2W^4)$$

we have

$$\begin{aligned}\kappa &= -\min(2\tau, \tau+\varphi+\psi+\omega, 2\varphi+4\psi, 2\varphi+4\omega)\\ &= -2\min(\tau, \varphi+2\psi, \varphi+2\omega)\\ C(q) &= |k'|\,\frac{(t^2, tuvw, u^2v^4, u^2w^4)}{m^6}\,2^{\kappa_2} = |k'|\,\frac{(t, uv^2, uw^2)^2}{m^6}\,2^{\kappa_2},\end{aligned} \tag{75}$$

where $\kappa_2 = \min\bigl(\kappa_1+2\tau_1, \kappa_1+2\varphi_1+4\psi_1, \kappa_1+2\varphi_1+4\omega_1+2\bigr) \equiv \kappa_1 \bmod 2$. Since $\kappa_1+2\varphi_1+4\psi_1-\kappa_2, \kappa_1+2\varphi_1+4\omega_1+2-\kappa_2$ are non-negative, even and different mod 4, we have either $\kappa_1+2\varphi_1+4\omega_1+2-\kappa_2 \geqslant 2$ or $\kappa_1+2\varphi_1+4\psi_1-\kappa_2 \geqslant 2$. Taking

$$k_0 = C(q)\operatorname{sgn} k', \quad T_0 = \frac{m^3}{(t, uv^2, uw^2)}\,2^{(\kappa_1-\kappa_2)/2}Tx^{\kappa/2},$$

and, in the former case

$$\begin{aligned}U_0 &= \frac{m(v, w)^2}{(t, uv^2, uw^2)}\,2^{2\psi_1-2\psi_2+(\kappa_1-\kappa_2)/2}Ux^{\kappa/2+2\min(\psi,\omega)},\\ V_0 = \frac{m}{(v, w)}\,2^{\psi_2-\psi_1}Vx^{-\min(\psi,\omega)}, &\quad W_0 = \frac{m}{(v, w)}\,2^{\omega_2-\omega_1}Wx^{-\min(\psi,\omega)},\end{aligned}$$

in the latter case

$$\begin{aligned}U_0 &= \frac{m(v, w)^2}{(t, uv^2, uw^2)}\,2^{2\omega_1-2\psi_2+(\kappa_1-\kappa_2)/2+1}Ux^{\kappa/2+2\min(\psi,\omega)},\\ V_0 = \frac{m}{(v, w)}\,2^{\psi_2-\omega_1}Wx^{-\min(\psi,\omega)}, &\quad W_0 = \frac{m}{(v, w)}\,2^{\omega_2-\psi_1}Vx^{-\min(\psi,\omega)},\end{aligned}$$

we find in view of (75)

$$q(x) = k_0(T_0^2 - 4T_0U_0V_0W_0 - U_0^2V_0^4 - 4U_0^2W_0^4)$$

and

$$T_0, U_0, V_0, W_0 \in \mathbb{Z}[x]. \tag{76}$$

Moreover the factors on the right hand side of (1) differ from the original ones by the factor $cx^{\kappa/2}$, $c \in \mathbb{Q}$.

If

$$q(x) = k(U^3 + V^3 + W^3 - 3UVW)$$

we have

$$\begin{aligned}\kappa &= -\min(3\varphi, 3\psi, 3\omega, \varphi+\psi+\omega) = -3\min(\varphi, \psi, \omega),\\ C(q) &= |k'|\,\frac{(u^3, v^3, w^3, 3uvw)}{m^3} = \frac{|k'|}{m^3}(u, v, w)^3.\end{aligned} \tag{77}$$

Taking

$$k_0 = C(q)\operatorname{sgn} k', \quad U_0 = U\,\frac{m}{(u, v, w)}\,x^{\kappa/3}, \quad V_0 = V\,\frac{m}{(u, v, w)}\,x^{\kappa/3},$$
$$W_0 = W\,\frac{m}{(u, v, w)}\,x^{\kappa/3}$$

we find in view of (77)

$$q(x) = k_0(U_0^3 + V_0^3 + W_0^3 - 3U_0V_0W_0)$$

and again (76). The first and the second factor on the right hand side of (1) differ from the
c original ones by the factor $cx^{\kappa/3}$ and $c^2x^{2\kappa/3}$, respectively, $c \in \mathbb{Q}$.

Finally, if

$$q(x) = k(U^2 + 2UV + V^2 - W^2)$$

we have

$$\kappa = -\min(2\varphi, \varphi + \psi, 2\psi, 2\omega) = -2\min(\varphi, \psi, \omega),$$
$$C(q) = |k'|\,\frac{(u^2, 2uv, v^2, w^2)}{m^2} = |k'|\,\frac{(u, v, w)^2}{m^2}. \tag{78}$$

Taking

$$k_0 = C(q)\operatorname{sgn} k', \quad U_0 = U\,\frac{m}{(u, v, w)}\,x^{\kappa/2}, \quad V_0 = V\,\frac{m}{(u, v, w)}\,x^{\kappa/2},$$
$$W_0 = W\,\frac{m}{(u, v, w)}\,x^{\kappa/2}$$

we find in view of (78)

$$q(x) = k_0(U_0^2 + 2U_0V_0 + V_0^2 - W_0^2)$$

and again (76). The factors on the right hand side of (1) differ now from the original ones
c by the factor $cx^{\kappa/2}$, $c \in \mathbb{Q}$. □

Proof of Theorem 4. With $Kq(x)$ replaced by $Lq(x)$ the theorem has been actually proved in the course of proof of Theorem 2 in [3], see namely formula (20) there and the subsequent argument. We shall have soon to go through the same argument again and then we shall supply a few details missing there or peculiar to the present context (e.g. the application of Lemma 18), taking them now for granted.

By Lemma 15, 16 and 17 we have $Kq(x) = Lq(x)$ unless (68) and (69) hold with $k = 3$. Therefore we shall assume these relations for a certain integral vector $\boldsymbol{\gamma} = [\gamma_1, \gamma_2, \gamma_3]$. In-
c tegral vectors perpendicular to $\boldsymbol{\gamma}$ form a module, say $\mathfrak{N}$. We have $[\gamma_2, -\gamma_1, 0]$, $[\gamma_3, 0, -\gamma_1]$, $[0, \gamma_3, -\gamma_2] \in \mathfrak{N}$ and since $\boldsymbol{\gamma} \neq 0$ two among these three vectors are linearly independent. By Lemma 6 of [11] $\mathfrak{N}$ has a basis which written in the form of a matrix $\boldsymbol{\Delta} = [\delta_{tj}]_{\substack{t\leqslant 2\\ j\leqslant 3}}$ satisfies

$$\max_{t,j}|\delta_{tj}| \leqslant 2\max_j|\gamma_j| \leqslant 4\frac{\log\|q\|}{\log 2}. \tag{79}$$

Moreover,

$$\operatorname{rank}\boldsymbol{\Delta} = 2 \tag{80}$$

and by (67)

$$[n_1, n_2, n_3] = [m_1, m_2]\boldsymbol{\Delta}, \quad [m_1, m_2] \text{ integral} \neq 0. \tag{81}$$

Since $0 < n_1 < n_2 < n_3$ the vectors $[\delta_{1j}, \delta_{2j}]$ $(j = 1, 2, 3)$ are distinct and different from $[0, 0]$. Let us set

$$Q_0(y_1, y_2) = J\Big(a_0 + \sum_{j=1}^{3} a_j y_1^{\delta_{1j}} y_2^{\delta_{2j}}\Big). \tag{82}$$

By (81) we have

$$q(x) = J\,Q_0(x^{m_1}, x^{m_2}). \tag{83}$$

Since $q(x)$ is not reciprocal $Q_0(y_1, y_2)$ is also not reciprocal. Thus by Theorem 1 of [3]

$$L\,Q_0(y_1, y_2) = Q_0(y_1, y_2) \quad \text{or} \quad \frac{Q_0(y_1, y_2)}{D_0(y_1, y_2)}\, L\,D_0(y_1, y_2), \tag{84}$$

where D_0 is a certain binomial defined there. Now, for binomials

$$K\,L\,D_0(y_1, y_2) = K\,D_0(y_1, y_2);$$

on the other hand by Lemma 11 of [11]

$$K\,L\,Q_0(y_1, y_2) = L\,Q_0(y_1, y_2).$$

Applying the operation K to the both sides of (84) we get

$$L\,Q_0(y_1, y_2) = K\,Q_0(y_1, y_2).$$

Now we apply Theorem 3 of [11] setting there $F(x_1, x_2) = Q_0(x_1, x_2)$. By that theorem there exists an integral matrix $\boldsymbol{M} = [\mu_{ij}]_{\substack{i \leqslant r \\ j \leqslant 2}}$ of rank $r \leqslant 2$ and an integral vector $\boldsymbol{v} = [v_1, v_r]$ such that

$$\max_{i,j} |\mu_{ij}| \leqslant \begin{cases} \exp 9 \cdot 2^{\|Q_0\|-4} & \text{if } r = 2, \\ \exp\big(500 \|Q_0\|^2 (2|Q_0|^*)^{2\|Q_0\|+1}\big) & \text{if } r = 1; \end{cases} \tag{85}$$

$$[m_1, m_2] = \boldsymbol{v}\boldsymbol{M}; \tag{86}$$

$$K\,Q_0\Big(\prod_{i=1}^{r} y_i^{\mu_{i1}}, \prod_{i=1}^{r} y_i^{\mu_{i2}}\Big) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(y_1, y_r)^{e_\sigma} \tag{87}$$

implies

$$K\,Q_0(x^{m_1}, x^{m_r}) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} K\,F(x^{v_1}, x^{v_r})^{e_\sigma}. \tag{88}$$

[c] In (85) $|Q_0|^* = \sqrt{\max\{2, |Q_0|^2\} + 2}$.

Let us set

$$\boldsymbol{N} = [v_{ij}]_{\substack{i \leqslant r \\ j \leqslant 3}} = \boldsymbol{M}\boldsymbol{\Delta}. \tag{89}$$

It follows from (80) that $\boldsymbol{N}$ is of rank r and from (81) and (86) that

$$[n_1, n_2, n_3] = \boldsymbol{v}\boldsymbol{N}. \tag{90}$$

Consider first the case $r = 2$ and put

$$Q(y_1, y_2) = JQ_0\Big(\prod_{i=1}^{2} y_i^{\mu_{i1}}, \prod_{i=1}^{2} y_i^{\mu_{i2}}\Big).$$

By (82) and (89)

$$Q(y_1, y_2) = J\Big(a_0 + \sum_{j=1}^{3} a_j y_1^{\nu_{1j}} y_2^{\nu_{2j}}\Big).$$

By (90) the vectors $[\nu_{1j}, \nu_{2j}]$ are distinct and different from $[0, 0]$, moreover

$$q(x) = JQ(x^{\nu_1}, x^{\nu_2}). \tag{91}$$

Now by Theorem 1 of [3] we have the following possibilities.

(92) $Q(y_1, y_2)$ is irreducible.

(93) $Q(y_1, y_2)$ can be divided into two parts with the highest common factor $D(y_1, y_2)$ being a binomial. Then QD^{-1} is either irreducible and non-reciprocal or binomial.

(94) $Q(y_1, y_2)$ can be represented in one of the forms (1), where $k \in \mathbb{Q}$ and T, U, V, W are monomials in $\mathbb{Q}[y_1, y_2]$. The factors on the right hand side of (1) are irreducible and non-reciprocal.

(We have made in comparison to [3] a certain permutation of letters and formulae.)

In the case (92) we have on the right hand side of (87) at most one irreducible factor. By (83) and (88) the same applies to the canonical factorization of $Kq(x)$. Since $q(x)$ is not reciprocal, $Kq(x) \neq \text{const}$ and (xii) follows.

In the case (93) in virtue of (91) $q(x)$ can be divided into two parts that have the common factor $JD(x^{\nu_1}, x^{\nu_2}) = d(x)$ which is either binomial or constant. We get

$$q(x)d^{-1}(x) = JQ(x^{\nu_1}, x^{\nu_2})D^{-1}(x^{\nu_1}, x^{\nu_2}).$$

If qd^{-1} is not a binomial we conclude that QD^{-1} is not a binomial either. Hence QD^{-1} is irreducible and non-reciprocal. From $LQD^{-1} = QD^{-1}$ we infer by Lemma 11 of [11] that $KQD^{-1} = QD^{-1}$. Thus by (88)

$$K\big(Q(x^{\nu_1}, x^{\nu_2})D^{-1}(x^{\nu_1}, x^{\nu_2})\big) = K\big(q(x)d^{-1}(x)\big)$$

is irreducible. If $d(x)$ is reciprocal, $Kd(x) = \text{const}$ and we get (xii); if $d(x)$ is not reciprocal we get (xiii).

In the case (94) we get from Lemma 11 of [11] that $KQ = Q$. The factorization (87) is given by the formulae (1). Taking for F_1, F_2 the two factors occurring on the right hand side of (1) we infer from (88) that $KF_\sigma(x^{\nu_1}, x^{\nu_2})$ $(\sigma = 1, 2)$ are irreducible. Now by (91) to the representation of $Q(y_1, y_2)$ in any one of the forms (1) there corresponds a representation of $q(x)$ in the same form, where k, T, U, V, W are now monomials in $\mathbb{Q}(x)$ and the factors on the right hand side of (1) are $F_\sigma(x^{\nu_1}, x^{\nu_2})$ $(\sigma = 1, 2)$. By Lemma 18 there exists a representation of $q(x)$ in the form in question in which $k = \pm(a_0, a_1, a_2, a_3)$ and T, U, V, W are monomials in $\mathbb{Z}[x]$. Since the relevant factors differ from $F_\sigma(x^{\nu_1}, x^{\nu_2})$ $(\sigma = 1, 2)$ only by monomial factors we infer that their kernels are irreducible. This gives (xiv). It remains to consider the case $r = 1$. The change of signs of μ_{1i} $(1 \leqslant i \leqslant 3)$

in (87) leads to a replacement of $F_\sigma(y_1)$ by $JF_\sigma(y_1^{-1})$ but does not affect the implication (87) $\to$ (88). Therefore, changing the signs of μ_{1i} if necessary we can assume that $v = v_1 > 0$. Hence by (90)

$$0 < \nu_{11} < \nu_{12} < \nu_{13}. \tag{95}$$

By (79), (85) and (95) we have

$$\nu_{13} = \max_{1\leqslant j\leqslant 3} |\nu_{1j}| \leqslant 8\,\frac{\log\|q\|}{\log 2}\exp\bigl(500\|Q_0\|^2(2|Q_0|^*)^{2\|Q_0\|+1}\bigr).$$

Now by (82) and (79)

$$\|Q_0\| = \|q\|,$$

$$|Q_0|^* \leqslant |Q_0| + 1 \leqslant 2\max_{t,j}|\delta_{tj}| + 1 \leqslant 8\,\frac{\log\|q\|}{\log 2} + 1 < 13\log\|q\|$$

and we get

$$\begin{aligned}\nu_{13} &\leqslant 12\log\|q\|\exp\bigl(500\|q\|^2(26\log\|q\|)^{2\|q\|+1}\bigr)\\ &< \exp\bigl(600\|q\|^2(26\log\|q\|)^{2\|q\|+1}\bigr) < \exp_2(12\cdot 2^{\|q\|}\log\|q\|).\end{aligned}$$

Let us set $\nu_{1j} = \nu_j$ $(1 \leqslant j \leqslant 3)$. By (90) we have

$$n_j = v\nu_j \quad (1 \leqslant j \leqslant 3).$$

By (82) and (89)

$$JQ_0(y_1^{\mu_{11}}, y_2^{\mu_{12}}) = J\Bigl(a_0 + \sum_{j=1}^{3} a_j y_1^{\nu_{1j}}\Bigr).$$

The last assertion of (xiv) follows now from the implication (87) $\to$ (88).

To estimate $\Omega\bigl(Kq(x)\bigr)$ we use Corollary to Lemma 1, Theorem 3 and Lemma 17. We get

$$\begin{aligned}\Omega\bigl(Kq(x)\bigr) \leqslant \Omega\bigl(Lq(x)\bigr) + \Omega_0\bigl((a_0,a_3)\bigr) &\leqslant \frac{\log\|q\|}{2\log\vartheta_0} + \frac{\log a_0^2}{2\log 2}\\ &< \Bigl(\frac{1}{2\log\vartheta_0} + \frac{1}{2\log 2}\Bigr)\log\|q\|. \qquad \square\end{aligned}$$

Proof of Corollary 4 does not differ from the proof of Corollary in [3]. We note only that if

$$a_0 + \sum_{i=1}^{3} a_i\zeta^{n_i/(n_1,n_2,n_3)} = 0, \quad \zeta^6 = 1$$

then $q(x)$ is indeed reducible since none of the cyclotomic polynomials of index d $(d \mid 6)$ is a quadrinomial. $\square$

[c] **Note added in proof.** Very recently E. Dobrowolski [2a] has proved the following improvement of Blanksby–Montgomery's theorem.

If $\alpha^{(j)}$ are conjugates of an algebraic integer α different from 0 *and roots of unity then*

$$\prod_{|\alpha^{(j)}|>1} |\alpha^{(j)}| > 1 + c\Big(\frac{\log\log n}{\log n}\Big)^3, \quad c > 0.$$

This result allows one to improve the estimates given in Lemma 1 and Theorem 1 and in particular to obtain

$$\log c(E) \ll (|KF| \log \|F\|)^{1/3} (\log 2|KF| + \log_2 \|F\|)^{2/3}.$$

Here neither the exponent $1/3$ nor the exponent $2/3$ can be lowered.

References

[1] P. E. Blanksby, H. L. Montgomery, *Algebraic integers near the unit circle*. Acta Arith. 18 (1971), 355–369.

[2] A. Cohn, *Über die Anzahl der Wurzeln einer algebraischer Gleichung in einem Kreise*. Math. Z. 14 (1922), 110–148.

[2a] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*. Acta Arith. 34 (1979), 391–401.

[3] M. Fried, A. Schinzel, *Reducibility of quadrinomials*. Acta Arith. 21 (1972), 153–171; *Corrigendum and addendum*, ibid. 99 (2001), 409–410; this collection: E4, 720–738.

[4] E. Gourin, *On irreducible polynomials in several variables which become reducible when the variables are replaced by powers of themselves*. Trans. Amer. Math. Soc. 32 (1931), 485–501.

[5] H. Halberstam, H.-E. Richert, *Sieve Methods*. Academic Press, London–New York 1974.

[6] E. Landau, *Sur quelques théorèmes de M. Petrovitch relatifs aux zéros des fonctions analytiques*. Bull. Soc. Math. France 33 (1905), 1–11.

[7] —, *Handbuch der Lehre von der Verteilung der Primzahlen*. Reprint, Chelsea, New York 1953.

[8] H. B. Mann, *On linear relations between roots of unity*. Mathematika 12 (1965), 107–117.

[9] J. B. Rosser, L. Schoenfeld, *Approximate formulas for some functions of prime numbers*. Illinois J. Math. 6 (1962), 64–94.

[10] A. Schinzel, *On the reducibility of polynomials and in particular of trinomials*. Acta Arith. 11 (1965), 1–34; *Errata*, ibid., 491; this collection: D2, 301–332.

[11] —, *Reducibility of lacunary polynomials* I. Acta Arith. 16 (1969), 123–159; *Corrigenda*: Acta Arith. 19 (1971), 201; ibid. 24 (1978), 265; this collection: D4, 344–380.

[12] —, *Reducibility of lacunary polynomials*. In: 1969 Number Theory Institute, Proc. Sympos. Pure Math. 20, Amer. Math. Soc., Providence 1971, 135–149.

[13] —, *Reducibility of polynomials*. In: Actes du Congrès International des Mathèmaticiens (Nice 1970), t. I, Gauthier–Villars, Paris 1971, 491–496.

[14] —, *A general irreducibility criterion*. J. Indian Math. Soc. (N.S.) 37 (1973), 1–8; this collection: E5, 739–746.

[15] —, *On the number of irreducible factors of a polynomial*. in: Topics in Number Theory, Colloq. Math. Soc. János Bolyai 13, North-Holland, Amsterdam 1976, 305–314.

[16] —, *Abelian binomials, power residues and exponential congruences*. Acta Arith. 32 (1977), 245–274; *Addendum*, ibid. 36 (1980), 101–104; this collection: H5, 939–970.

[17] —, *An inequality for determinants with real entries*. Colloq. Math. 38 (1978), 319–321; this collection: M4, 1347–1349.

[18] A. Schinzel, J. Wójcik, *A note on the paper "Reducibility of lacunary polynomials* I*"*. Acta Arith. 19 (1971), 195–201; this collection: D6, 403–408.

[19] R. Sivaramakrishnan, *Generalization of an arithmetic function*. J. Indian Math. Soc. (N.S.) 33 (1969), 127–132.

[20] C. J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*. Bull. London Math. Soc. 3 (1971), 169–175.

[21] N. Tschebotaröw, *Grundzüge der Galoisschen Theorie*. Übersetzt und bearbeitet von H. Schwerdtfeger, Noordhoff, Groningen–Djakarta 1950.

Andrzej Schinzel
Selecta

Originally published in
Acta Arithmetica XLIII (1984), 313–315

Reducibility of lacunary polynomials IV

The aim of this paper is to make a further contribution to the problem of reducibility of polynomials

$$f(x) = a_0 + \sum_{j=1}^{k} a_j x^{n_j} \quad (0 = n_0 < n_1 < \ldots < n_k,\ a_0 a_k \neq 0) \tag{1}$$

for fixed integral coefficients a_j and variable exponents n_j. The non-reciprocal irreducible factors of $f(x)$ can be found by means of Theorem 2 in [3] and as to reciprocal factors the conjecture proposed in [2] implies the existence of a constant $C(a_0, a_1, \ldots, a_k)$ such that either all reciprocal irreducible factors of f are cyclotomic or $\sum_{j=1}^{k} \gamma_j n_j = 0$ for suitable integers γ_j satisfying

$$0 < \max_{1 \leqslant j \leqslant k} |\gamma_j| \leqslant C(a_0, a_1, \ldots, a_k).$$

We shall prove

Theorem. *If f is given by* (1) *with a_j integral, then either all reciprocal irreducible factors of f are cyclotomic or there exist integers $\gamma_1, \ldots, \gamma_k$ satisfying*

$$\sum_{j=1}^{k} \gamma_j n_j = 0, \tag{2}$$

$$0 < \max_{j=1,\ldots,k} |\gamma_j| \leqslant \max_{0 \leqslant j \leqslant k} \frac{\log a_j^2}{\log 2} \tag{3}$$

and the number of reciprocal non-cyclotomic factors of f does not exceed the total number of prime factors of (a_0, a_k) or finally the following system of inequalities is fulfilled

$$\begin{cases} \displaystyle\sum_{j=0}^{k-1} |a_j|\,|n_j - n_i| > |a_k|(n_k - n_i) & \text{if } n_i < n_k/2, \\ \displaystyle\sum_{j=1}^{k} |a_j|\,|n_j - n_i| > |a_0| n_i & \text{if } n_i > n_k/2, \\ \displaystyle\sum_{j=1}^{k-1} |a_j| \left| n_j - \frac{n_k}{2} \right| > \big||a_k| - |a_0|\big| \frac{n_k}{2}\,. \end{cases} \tag{4}$$

This theorem supersedes Lemma 15 of [3] and implies the following

Corollary. *If* $\sum_{j=0}^{k} \xi^{2^j} = 0$ *and* $|\xi| = 1$ *then* ξ *is a root of unity.*

The corollary answers in the negative Problem 1 of Mahler [1]. The proof of the theorem is based on two lemmata.

Lemma 1. *For every positive real number* $r \neq 1$ *and real numbers* n, m *satisfying* $|n| > |m|$ *we have*

$$h(m,n,r) = \left|\frac{r^m - r^{-m}}{r^n - r^{-n}}\right| < \left|\frac{m}{n}\right|.$$

Proof. Since $h(m,n,r)$ is an even function of m and n and

$$h(m,n,r^{-1}) = h(m,n,r)$$

it is enough to prove the lemma for $n > m \geqslant 0$, $r > 1$. Now, the function $g(r) = m(r^n - r^{-n}) - n(r^m - r^{-m})$ satisfies

$$g'(r) = mnr^{-1}\big[(r^n + r^{-n}) - (r^m + r^{-m})\big] = mnr^{-1}(r^n - r^m)(1 - r^{-n-m}) > 0$$

for all $r > 1$ hence, for such r, $g(r) > g(1) = 0$ and

$$h(m,n,r) = \frac{m}{n} - \frac{g(r)}{n(r^n - r^{-n})} < \frac{m}{n}\,. \qquad \square$$

Lemma 2. *Let* f *be given by* (1) *with* a_j *arbitrary complex numbers. If*

$$f(\xi) = f(\bar{\xi}^{-1}) = 0 \tag{5}$$

then either $|\xi| = 1$ *or the system* (4) *is fulfilled.*

Proof. Let $\xi = re^{i\varphi}$ (r, φ real) and let ϱ be a real number. From (5) we infer that

$$\sum_{j=0}^{k} a_j r^{n_j - \varrho} e^{i\varphi n_j} = 0 = \sum_{j=0}^{k} a_j r^{\varrho - n_j} e^{i\varphi n_j}$$

hence

$$\sum_{j=0}^{k} a_j (r^{n_j - \varrho} - r^{\varrho - n_j}) e^{i\varphi n_j} = 0.$$

Taking

$$\varrho = n_i \quad \text{and} \quad \nu = \begin{cases} k & \text{if } n_i < n_k/2, \\ 0 & \text{if } n_i > n_k/2, \end{cases}$$

we get

$$|n_j - n_i| \leqslant |n_\nu - n_i| \quad (0 \leqslant j \leqslant k),$$

also

$$\sum_{j=0, j\neq\nu}^{k} a_j(r^{n_j-n_i} - r^{n_i-n_j})e^{i\varphi n_j} = -a_\nu(r^{n_\nu-n_i} - r^{n_i-n_\nu})e^{i\varphi n_\nu}$$

hence dividing by $r^{n_\nu-n_i} - r^{n_i-n_\nu}$ and using Lemma 1 we get the first two inequalities of (4). The last inequality is obtained similarly on taking $\varrho = n_k/2$. □

Remark. This lemma supersedes Lemma 14 of [3].

Proof of Theorem. Suppose that f has a reciprocal irreducible factor g that is not cyclotomic. Let η be a zero of g. By Kronecker's theorem either η has a conjugate ξ with $|\xi| \neq 1$ or η is not an algebraic integer. In the former case we use Lemma 2 and get the conditions (4). In the latter case we use Lemma 13 of [3] and get the conditions (2) and (3). Also the product of the leading coefficients of all reciprocal non-cyclotomic factors of f must divide (a_0, a_k). Since all these coefficients are greater than 1 their number does not exceed the total number of prime factors of (a_0, a_k). □

Proof of Corollary. Let g be a minimal polynomial of ξ. Since $g(\xi^{-1}) = g(\overline{\xi}) = 0$, g is reciprocal. We apply the theorem to the polynomial $f(x) = \sum_{j=0}^{k} x^{2^j-1}$. Since this polynomial does not satisfy the conditions (4) (for $i = 0$) and $(a_0, a_k) = 1$ the number of its reciprocal non-cyclotomic factors is 0. Hence g is cyclotomic and ξ is a root of unity. □

References

[1] K. Mahler, *On the zeros of a special sequence of polynomials*. Math. Comp. 39 (1982), 207–212.

[2] A. Schinzel, *On the reducibility of polynomials and in particular of trinomials*. Acta Arith. 11 (1965), 1–34; *Errata*, ibid., 491; this collection: D2, 301–332.

[3] —, *Reducibility of lacunary polynomials* III. Acta Arith. 34 (1978), 227–266; this collection: D7, 409–446.

Originally published in
Acta Arithmetica XLIX (1987), 55–70

On the number of terms of a power of a polynomial

*To Paul Erdős with best wishes
on his 75th birthday*

The conjecture made by Rényi and first published by Erdős [2], who supported it [1], asserts that if Q_k is the least number of non-zero coefficients of the square of a polynomial with exactly k non-zero complex coefficients then

$$\lim_{k=\infty} Q_k = \infty.$$

It has been proved by Erdős in the quoted paper that

$$Q_k < C_1 k^{1-C_2}$$

and the values of the positive constants C_1 and C_2 have been subsequently found by Verdenius [9] (see also Freud [3]). He also established a similar inequality for cubes. It is the principal aim of the present paper to prove an estimate for the number of non-zero coefficients, called the number of terms, of an arbitrary power of a polynomial, which contains as a special case the inequality

$$Q_k > \frac{\log\log k}{\log 2}.$$

Here is the general result.

Theorem 1. *Let* $\boldsymbol{K}$ *be a field,* $f \in \boldsymbol{K}[x]$, $l \in \mathbb{N}$, f *and* f^l *have* $T \geqslant 2$ *and* t *terms, respectively. If either* $\operatorname{char} \boldsymbol{K} = 0$ *or* $\operatorname{char} \boldsymbol{K} > l \deg f$ *then*

$$t \geqslant l + 1 + (\log 2)^{-1} \log\Big(1 + \frac{\log(T-1)}{l \log 4l - \log l}\Big).$$

Already for $l = 2$ there is a big gap between the obtained lower bound and Erdős's upper bound for t. Another open question concerns the number of terms of $F\big(f(x)\big)$, where F is a fixed non-constant polynomial. If $Q_k(F)$ is the minimal number of terms of $F\big(f(x)\big)$, when f runs over all polynomials with exactly k terms then probably $\lim_{k=\infty} Q_k(F) = \infty$, but the method of this paper is insufficient to prove it.

If $\operatorname{char} \boldsymbol{K}$ is positive the number of terms of f_n^l may remain bounded in spite of the fact that the number of terms of $f_n \in \boldsymbol{K}[x]$ tends to infinity with n. The situation is described by the following

[1] Erdős tells me that he arrived at the conjecture independently from Rényi.

Theorem 2. *Let* $\operatorname{char} \boldsymbol{K} > 0$, $f \in \boldsymbol{K}[x]$, $l \in \mathbb{N}$, f *and* f^l *have* $T \geqslant 2$ *and* t *terms, respectively. If*

$$l^{T-1}(T^2 - T + 2) < \operatorname{char} \boldsymbol{K}$$

then

$$t \geqslant l + 1 + (\log 2)^{-1} \log\Big(1 + \frac{\log(T-1)}{l \log 4l - \log l}\Big).$$

On the other hand, if $l \neq (\operatorname{char} \boldsymbol{K})^n$ $(n = 0, 1, 2, \dots)$ *there exist polynomials* $f \in \boldsymbol{K}[x]$ *with* T *arbitrarily large such that* $t \leqslant 2l$.

Finally we have

Theorem 3. *Let* $\boldsymbol{K}$ *be a field and* $f \in \boldsymbol{K}[x]$. *If in the algebraic closure of* $\boldsymbol{K}$ f *has a zero* ξ *of multiplicity exactly* n *then* f *has at least as many terms as* $(x - \xi)^n$.

The algebraic closure of $\boldsymbol{K}$ will be denoted by $\widehat{\boldsymbol{K}}$. The case $\operatorname{char} \boldsymbol{K} = 0$ of Theorem 3 has been proved by G. Hajós [5]. The special case of Theorem 3 for $\boldsymbol{K} = \mathbb{F}_2$ and $\xi = 1$ has been given as a problem in XXVIth International Mathematical Olympiad. A. Mąkowski, the head of the Polish delegation, insisted that there should be a common generalization of this problem and of Hajós's theorem. Hajós's result, slightly extended serves as the first of the three lemmata needed for the proof of Theorem 1.

Lemma 1. *If* $g \in \boldsymbol{K}[x] \setminus \{0\}$ *has in the algebraic closure of* $\boldsymbol{K}$ *a zero* $\xi \neq 0$ *of multiplicity at least* m *and either* $\operatorname{char} \boldsymbol{K} = 0$ *or* $\operatorname{char} \boldsymbol{K} > \deg g$, *then* g *has at least* $m + 1$ *terms.*

Proof. The proof given by Hajós [5] and rediscovered by Montgomery and Schinzel ([6], Lemma 1) for $\boldsymbol{K} = \mathbb{C}$ applies without change to the case $\operatorname{char} \boldsymbol{K} = 0$ or $\operatorname{char} \boldsymbol{K} > \deg g$. □

Lemma 2. *If* $f(x) \in \boldsymbol{K}[x]$, $f(0) \neq 0$, $f(x)^l \in \boldsymbol{K}[x^d]$ *then either* $\operatorname{char} \boldsymbol{K} \mid (l, d)$ *or* $f(x) \in \boldsymbol{K}[x^d]$.

Proof. Let

$$f(x)^l = g(x^d), \quad g(x) = \gamma_0 \prod_{\gamma \in \boldsymbol{\Gamma}} (x - \gamma)^{e(\gamma)},$$

where $\boldsymbol{\Gamma}$ is a subset of $\boldsymbol{K} \setminus \{0\}$. We get

$$f(x)^l = \gamma_0 \prod_{\gamma \in \boldsymbol{\Gamma}} (x^d - \gamma)^{e(\gamma)}.$$

Since for $\gamma \neq 0$ the multiplicity of the zeros of $x^d - \gamma$ is either 1 or equal to the maximal power of $\operatorname{char} \boldsymbol{K}$ dividing d, we get either $\operatorname{char} \boldsymbol{K} \mid (l, d)$ or $l \mid e(\gamma)$ for all $\gamma \in \boldsymbol{\Gamma}$. It follows that

$$f(x) = \gamma_1 \prod_{\gamma \in \boldsymbol{\Gamma}} (x^d - \gamma)^{e(\gamma)/l} \in \widehat{\boldsymbol{K}}[x^d].$$

Since $\boldsymbol{K}[x] \cap \widehat{\boldsymbol{K}}[x^d] = \boldsymbol{K}[x^d]$ we infer that

$$f(x) \in \boldsymbol{K}[x^d]. \qquad \square$$

Lemma 3. *Let $H \in \boldsymbol{K}[y, z]$, $p \in \mathbb{Z}$. Define the sequence $H_n = H_n(y, z; p)$ as follows*

$$H_0 = H, \quad H_{n+1} = \frac{\partial H_n}{\partial y}\, py + \frac{\partial H_n}{\partial z}\, z.$$

Then we have the following

(1) $$\deg_y H_n \leqslant \deg_y H, \quad \deg_z H_n \leqslant \deg_z H;$$

(2) $$H_n(x^p, x; p) = \sum_{k=1}^{n} c(k, n) x^k \frac{d^k H(x^p, x)}{dx^k} \quad (n \geqslant 1)$$

for suitable coefficients $c(k, n) \in \boldsymbol{K}$;

(3) *If* char $\boldsymbol{K} \geqslant l$ *and a polynomial G irreducible over $\boldsymbol{K}$ divides $(H_0, H_1, \ldots, H_{l-1})$, then either $G^l \mid H$ or for each term $gy^\alpha z^\beta$ of G $(g \neq 0)$ $p\alpha + \beta$ is the same* mod char $\boldsymbol{K}$ *if* char $\boldsymbol{K} > 0$*, has the same value if* char $\boldsymbol{K} = 0$*, briefly G is isobaric* mod char $\boldsymbol{K}$ *with respect to the weights $p, 1$.*

Proof. Directly from the definition of H_n we get

$$\deg_y H_{n+1} \leqslant \deg_y H_n, \quad \deg_z H_{n+1} \leqslant \deg_z H_n$$

and formulae (1) follow by induction. The same method is used to prove (2) and (3).

(2) is true for $n = 1$ since

$$H_1(x^p, x; p) = \frac{\partial H}{\partial y}(x^p, x) px^p + \frac{\partial H}{\partial z}(x^p, x) x = x \frac{dH(x^p, x)}{dx}.$$

Assuming the truth of (2) for a fixed n we get

$$\begin{aligned} H_{n+1}(x^p, x; p) &= \frac{\partial H_n}{\partial y}(x^p, x; p) px^p + \frac{\partial H_n}{\partial z}(x^p, x; p) x \\ &= x \frac{dH_n(x^p, x; p)}{dx} \\ &= x \sum_{k=1}^{n} c(k, n) \Big(kx^{k-1} \frac{d^k H(x^p, x)}{dx^k} + x^k \frac{d^{k+1} H(x^p, x)}{dx^{k+1}} \Big), \end{aligned}$$

which implies (2) with n replaced by $n + 1$.

In order to prove (3) let $H = G^m U$, where $U \not\equiv 0 \bmod G$. We shall show by induction on $j \leqslant m$ that

(4) $$H_j(y, z; p) \equiv j! \binom{m}{j} \left(\frac{\partial G}{\partial y}\, py + \frac{\partial G}{\partial z}\, z \right)^j G^{m-j} U \bmod G^{m-j+1}.$$

For $j = 0$ this is obviously true. Assuming it for a fixed j we get upon differentiation

$$\frac{\partial H_j}{\partial y} \equiv j!\binom{m}{j}\left(\frac{\partial G}{\partial y}\,py + \frac{\partial G}{\partial z}\,z\right)^j (m-j)G^{m-j-1}\frac{\partial G}{\partial y}\,U \bmod G^{m-j},$$

$$\frac{\partial H_j}{\partial z} \equiv j!\binom{m}{j}\left(\frac{\partial G}{\partial y}\,py + \frac{\partial G}{\partial z}\,z\right)^j (m-j)G^{m-j-1}\frac{\partial G}{\partial z}\,U \bmod G^{m-j},$$

hence

$$\begin{aligned} H_{j+1}(y,z;p) &= \frac{\partial H_j}{\partial y}\,py + \frac{\partial H_j}{\partial z}\,z \\ &\equiv (j+1)!\binom{m}{j+1}\left(\frac{\partial G}{\partial y}\,py + \frac{\partial G}{\partial z}\,z\right)^{j+1} G^{m-j-1}U \bmod G^{m-j} \end{aligned}$$

and the inductive proof of (4) is complete.

Taking there $j = m$, we get

$$H_m(y,z;p) \equiv m!\left(\frac{\partial G}{\partial y}\,py + \frac{\partial G}{\partial z}\,z\right)^m U \bmod G,$$

hence if $m < l$ the assumption $G \mid (H_0, H_1, \ldots, H_{l-1})$ implies

$$\frac{\partial G}{\partial y}\,py + \frac{\partial G}{\partial z}\,z \equiv 0 \bmod G.$$

However the degree of $\dfrac{\partial G}{\partial y}\,py + \dfrac{\partial G}{\partial z}\,z$ does not exceed the degree of G. Hence

$$\frac{\partial G}{\partial y}\,py + \frac{\partial G}{\partial z}\,z = cG, \quad c \in \boldsymbol{K}$$

and for each term $gy^\alpha z^\beta$ $(g \neq 0)$ of G we have

$$p\alpha + \beta = c,$$

where both sides are viewed as elements of $\boldsymbol{K}$. If $\operatorname{char} \boldsymbol{K} > 0$ this means

$$p\alpha + \beta \equiv c \bmod \operatorname{char} \boldsymbol{K}$$

and if $\operatorname{char} \boldsymbol{K} = 0$

$$p\alpha + \beta = c. \qquad \square$$

Proof of Theorem 1. We shall prove the following equivalent inequality

$$T \leqslant 1 + \left(\frac{(4l)^l}{l}\right)^{2^{t-l-1}-1}. \tag{5}$$

For $T > 1$ we have $t > 1$ hence (5) holds for $t = 1$. For $t > 1$ let

$$f(x)^l = \sum_{j=0}^{t-1} a_j x^{m_j},$$

where

$$a_j \neq 0, \quad m_0 < m_1 < \ldots < m_{t-1}, \quad (m_1 - m_0, m_2 - m_0, \ldots, m_{t-1} - m_0) = d.$$

We have

$$m_0 = l \operatorname{ord}_x f \equiv 0 \bmod l,$$
$$\left(f(x)x^{-m_0/l}\right)^l \in \boldsymbol{K}[x^d], \quad f(x)x^{-m_0/l}\big|_{x=0} \neq 0,$$

hence by Lemma 2

$$f(x)x^{-m_0/l} \in \boldsymbol{K}[x^d], \quad f(x) = f_0(x^d)x^{m_0/l}$$

and

$$f_0(x)^l = a_0 + \sum_{j=1}^{t-1} a_j x^{n_j}, \tag{6}$$

where $n_j = (m_j - m_0)/d$. We get

$$0 = n_0 < n_1 < n_2 < \ldots < n_{t-1} \leqslant l \deg f, \quad (n_1, \ldots, n_{t-1}) = 1 \tag{7}$$

and since f and f_0 have the same number of terms it is enough to prove the inequality (5) for the number of terms of f_0.

If $t \leqslant l + 1$ we apply Lemma 1. Since char $\boldsymbol{K} = 0$ or char $\boldsymbol{K} > n_{t-1}$ the lemma is applicable with $g = f_0^l$, $m = l$ and it gives $t \geqslant l + 1$, hence $t = l + 1$. Every zero ξ of f_0^l is of multiplicity $\geqslant l$, hence on differentiation

$$a_0 + \sum_{j=1}^{l} a_j \xi^{n_j} = 0, \quad \sum_{j=1}^{l} a_j \binom{n_j}{i} \xi^{n_j} = 0 \quad (1 \leqslant i < l).$$

Since char $\boldsymbol{K} = 0$ or char $\boldsymbol{K} > n_{t-1}$ we have

$$\left|\binom{n_j}{i}\right|_{\substack{0 \leqslant i < l \\ 1 \leqslant j \leqslant l}} = \prod_{0 \leqslant q < r < l} \frac{n_r - n_q}{r - q} \neq 0,$$

hence $a_j \xi^{n_j}$ are uniquely determined by a_0. Since $a_j \neq 0$ and $(n_1, \ldots, n_{t-1}) = 1$ there is only one possible value for ξ. Then

$$f_0(x) = c(x - \xi)^{\deg f_0}, \quad c \in \boldsymbol{K}, \ \xi \neq 0$$

and Lemma 1 applies with $g = f_0, m = l \deg f_0$. It gives $l \deg f_0 + 1 \leqslant l + 1, \deg f_0 = 1$, $T = 2$, hence (5).

The further proof proceeds by induction for fields $\boldsymbol{K}$ algebraically closed. Assume that (5) holds for lth powers with less than $t \geqslant l + 2$ terms and consider again the conditions (6) and (7).

By Dirichlet's theorem there exist integers $p_1, p_2, \ldots, p_{t-1}$ such that

$$\left|\frac{n_j}{n_{t-1}} - \frac{p_j}{p_{t-1}}\right| < \frac{1}{4lp_{t-1}} \quad (j = 1, 2, \ldots, t - 2) \tag{8}$$

and

$$0 < p_{t-1} \leqslant (4l)^{t-2}.$$

The inequality $p_i < 0$ or $p_i > p_{t-1}$ would imply

$$\frac{1}{p_{t-1}} < \Big|\frac{n_i}{n_{t-1}} - \frac{p_i}{p_{t-1}}\Big| < \frac{1}{4lp_{t-1}},$$

a contradiction; hence we have

$$0 \leqslant p_j \leqslant p_{t-1} \leqslant (4l)^{t-2} \quad (j = 1, 2, \ldots, t-2). \tag{9}$$

Setting

$$p_{t-1}[n_1, \ldots, n_{t-1}] = n_{t-1}[p_1, \ldots, p_{t-1}] + [r_1, \ldots, r_{t-1}] \tag{10}$$

we get from (8)

$$|r_j| < \frac{n_{t-1}}{4l} \quad (j = 1, 2, \ldots, t-2), \quad r_{t-1} = 0.$$

If $\max\limits_{1 \leqslant i \leqslant t-2} |r_i| = 0$, then by (9), (7) and (10)

$$(4l)^{t-2} \geqslant p_{t-1} = (p_{t-1}n_1, \ldots, p_{t-1}n_{t-1}) \geqslant n_{t-1},$$

hence

$$T \leqslant 1 + \deg f_0 = 1 + \frac{n_{t-1}}{l} \leqslant 1 + \frac{(4l)^{t-2}}{l} \leqslant 1 + \Big(\frac{(4l)^l}{l}\Big)^{2^{t-l-1}-1}.$$

Therefore, assume that

$$0 < \max_{1 \leqslant j \leqslant t-1} |r_j| < \frac{n_{t-1}}{4l}, \quad r_{t-1} = 0 \tag{11}$$

and put

$$r = \min_{1 \leqslant j \leqslant t-1} r_j, \quad F(y, z) = z^{-r}\Big(a_0 + \sum_{j=1}^{t-1} a_j y^{p_j} z^{r_j}\Big).$$

By (9) and the choice of r we have

$$F(y, z) \in \boldsymbol{K}[y, z], \quad \big(F(y, z), yz\big) = 1.$$

(Note that by (7) and (8) no two terms of F are similar.). By (6) and (8) we have

$$f_0(x^{p_{t-1}})^l = x^r F(x^{n_{t-1}}, x). \tag{12}$$

Let

$$F(y, z) = F_0(y, z)^l H(y, z); \quad F_0, H \in \boldsymbol{K}[y, z], \tag{13}$$

where H is not divisible by the lth power of any polynomial in $\boldsymbol{K}[y, z] \setminus \boldsymbol{K}$. It follows from (12) and (13) that every zero of $H(x^{n_{t-1}}, x)$ except possibly $x = 0$ is as least l-tuple.

Hence for any $\xi \in \widehat{\boldsymbol{K}} \setminus \{0\}$

$$\operatorname{ord}_{x-\xi} H(x^{n_{t-1}}, x) \leqslant l \operatorname{ord}_{x-\xi} \frac{d^k}{dx^k} H(x^{n_{t-1}}, x) \quad (k < l)$$

and by (2) with $p = n_{t-1}$

$$\operatorname{ord}_{x-\xi} H(x^{n_{t-1}}, x) \leqslant l \operatorname{ord}_{x-\xi} H_m(x^{n_{t-1}}, x; n_{t-1}) \quad (m < l).$$

Also, by (2)

$$\operatorname{ord}_x H(x^{n_{t-1}}, x) \leqslant \operatorname{ord}_x H_m(x^{n_{t-1}}, x; n_{t-1}).$$

Thus finally

$$H(x^{n_{t-1}}, x) \mid H_m(x^{n_{t-1}}, x; n_{t-1})^l \quad (1 \leqslant m < l)$$

and for indeterminates $u_1, \ldots, u_{l-1}$

$$H(x^{n_{t-1}}, x) \Big| \sum_{m=1}^{l-1} u_m H_m(x^{n_{t-1}}, x; n_{t-1})^l. \tag{14}$$

Suppose first that $(H, H_1, \ldots, H_{l-1}) \neq 1$, where H_m stands for $H_m(y, z; n_{t-1})$. Then by the choice of H and the assertion (3) of Lemma 3 H, hence also F, has a factor $G \notin \boldsymbol{K}$ isobaric mod char $\boldsymbol{K}$ with respect to the weights n_{t-1}, 1. Since $(F, yz) = 1$, G has at least two terms. Let

$$F/G = \sum_{i=1}^{n} G_i,$$

where G_i are polynomials isobaric mod char $\boldsymbol{K}$ with respect to the weights n_{t-1}, 1 and n is minimal. Since G is isobaric mod char $\boldsymbol{K}$ with respect to the weights n_{t-1}, 1,

$$F = \sum_{i=1}^{n} G G_i$$

is the corresponding representation of F. Since G has at least two terms, the same is true for GG_1 hence F has at least two terms with weights congruent mod char $\boldsymbol{K}$, if char $\boldsymbol{K} > 0$, equal if char $\boldsymbol{K} = 0$. However the weights of the terms of F are $p_j n_{t-1} + r_j - r = p_{t-1} n_j - r$ $(0 \leqslant j < t)$. Since n_k are distinct the equality $p_{t-1} n_i - r = p_{t-1} n_j - r$, with $i \neq j$, is impossible. The congruence $p_{t-1} n_i - r \equiv p_{t-1} n_j - r \bmod \text{char } \boldsymbol{K}$ implies $p_{t-1} \equiv 0 \bmod \text{char } \boldsymbol{K}$ or $n_i \equiv n_j \bmod \text{char } \boldsymbol{K}$. Since char $\boldsymbol{K} = 0$ or char $\boldsymbol{K} > n_{t-1}$ the latter case with $i \neq j$ is impossible and we get

$$0 < \text{char } \boldsymbol{K} \leqslant p_{t-1}.$$

Hence by (9)

$$T \leqslant 1 + \deg f < 1 + \frac{\text{char } \boldsymbol{K}}{l} \leqslant 1 + \frac{p_{t-1}}{l} \leqslant 1 + \frac{(4l)^{t-2}}{l} \leqslant 1 + \left(\frac{(4l)^l}{l}\right)^{2^{t-l-1}-1}$$

and (5) holds.

Suppose now that $(H, H_1, \dots, H_{l-1}) = 1$. Then

$$\Big(H, \sum_{m=1}^{l-1} u_m H_m^l\Big) = 1.$$

Therefore the resultant R of H and $\sum_{m=1}^{l-1} u_m H_m^l$ with respect to y is non-zero and in view of (14)

$$H(x^{n_{t-1}}, x) \mid R(x).$$

Now, the degree of R does not exceed

$$\deg_y H \deg_z \sum_{m=1}^{l-1} u_m H_m^l + \deg_z H \deg_y \sum_{m=1}^{l-1} u_m H_m^l.$$

In virtue of (1) we get

$$\deg R \leqslant 2l \deg_y H \deg_z H.$$

On the other hand, if there is no cancellation in $H(x^{n_{t-1}}, x)$ we have

$$\deg H(x^{n_{t-1}}, x) \geqslant \max(n_{t-1} \deg_y H, \deg_z H).$$

It follows that either

$$\deg_y H = \deg_z H = 0 \tag{15}$$

or

$$n_{t-1} \leqslant 2l \deg_z H \leqslant 2l \deg_z F \leqslant 2l(\max r_i - \min r_i) < n_{t-1}$$

by (11), a contradiction.

If there is a cancellation in $H(x^{n_{t-1}}, x)$ then $\deg_y H \neq 0$ and

$$n_{t-1} \leqslant \deg_z H \leqslant \deg_z F < n_{t-1},$$

a contradiction again. Thus we have (15), i.e. $H \in \boldsymbol{K}$ and so by (13)

$$F(y, z) = \text{const}\, F_0(y, z)^l; \tag{16}$$

by (12)

$$f_0(x^{p_{t-1}})^l = \text{const}\, x^r F_0(x^{n_{t-1}}, x)^l;$$
$$F_0(x^{n_{t-1}}, x) = \text{const}\, x^{-r/l} f_0(x^{p_{t-1}}).$$

The number of terms of $F(y, z)$ is t, the number of terms of $F_0(y, z)$ is $T_0 \geqslant T$. Let

$$F_0(y, z) = \sum_{\tau=1}^{T_0} b_\tau y^{\alpha_\tau} z^{\beta_\tau}, \quad \langle \alpha_\tau, \beta_\tau \rangle \text{ all different}, b_\tau \neq 0.$$

By (11) there exists an index $i < t-1$ such that

$$\begin{vmatrix} p_i & p_{t-1} \\ r_i & r_{t-1} \end{vmatrix} = -p_{t-1}r_i \neq 0,$$

hence

$$T_0 = \operatorname{card}\{\langle \alpha_\tau r_i - \beta_\tau p_i, \alpha_\tau r_{t-1} - \beta_\tau p_{t-1}\rangle : \tau \leqslant T_0\}.$$

Now, for $j = i$ or $t-1$ let

$$T_j = \operatorname{card}\{\alpha_\tau r_j - \beta_\tau p_j : \tau \leqslant T_0\}.$$

Clearly $T_i T_{t-1} \geqslant T_0$, hence for a suitable $k \in \{i, t-1\}$

$$T_k^2 \geqslant T_0. \tag{17}$$

Now, let us choose elements η, ζ of $\boldsymbol{K}$ such that all non-empty sums

$$\sum_{\alpha_\tau r_k - \beta_\tau p_k = \text{const}} b_\tau \eta^{\alpha_\tau} \zeta^{\beta_\tau}$$

are non-zero. Then T_k is the number of terms of $F_0(\eta x^{r_k}, \zeta x^{-p_k})$. Let

$$s = \operatorname{ord}_x F_0(\eta x^{r_k}, \zeta x^{-p_k}), \quad G(x) = x^{-s} F_0(\eta x^{r_k}, \zeta x^{-p_k}) \in \boldsymbol{K}[x].$$

We have by (16)

$$\begin{aligned} G(x)^l &= \text{const}\, x^{-ls} F(\eta x^{r_k}, \zeta x^{-p_k}) \\ &= \text{const}\, \zeta^{-r} x^{p_k r - ls}\Big(a_0 + \sum_{j=1}^{t-1} a_j \eta^{p_j} \zeta^{r_j} x^{p_j r_k - r_j p_k}\Big) \end{aligned} \tag{18}$$

and the number of terms of $G(x)^l$ is at most $t-1$ since two terms in the parenthesis on the right hand side of (18), namely a_0 and $a_k \eta^{p_k} \zeta^{r_k} x^{p_k r_k - r_k p_k}$, coalesce. Moreover we have

$$p_j r_k - r_j p_k = p_{t-1}(p_j n_k - n_j p_k) \quad \text{for all } j < t;$$

thus

$$G(x)^l x^{ls - p_k r} \in \boldsymbol{K}(x^{p_{t-1}}).$$

Since $G(0) \neq 0$ we get from (18) and the above

$$\min_{1 \leqslant j < t} (p_j r_k - r_j p_k) \leqslant ls - p_k r \equiv 0 \bmod p_{t-1}, \tag{19}$$

hence

$$G(x)^l \in \boldsymbol{K}[x^{p_{t-1}}].$$

In virtue of Lemma 2

$$G(x) \in \boldsymbol{K}[x^{p_{t-1}}]; \quad G(x) = G_0(x^{p_{t-1}}), \quad G_0 \in \boldsymbol{K}[y].$$

The number of terms of $G_0(x)^l$ is the same as that of G^l, hence at most $t-1$. Moreover by (18), (19), (9) and (11)

$$l \deg G_0 = \frac{l \deg G}{p_{t-1}} \leqslant \frac{1}{p_{t-1}}\Big(\max_{1\leqslant j<t}(p_j r_k - r_j p_k) - \min_{1\leqslant j<t}(p_j r_k - r_j p_k)\Big) < \frac{4n_{t-1}}{4l} \leqslant n_{t-1} < \operatorname{char} \boldsymbol{K},$$

unless $\operatorname{char} \boldsymbol{K} = 0$. The inductive assumption applies and since the number of terms of G_0 is equal to that of G we get

$$T_k \leqslant 1 + \Big(\frac{(4l)^l}{l}\Big)^{2^{t-l-2}-1}.$$

Hence by (17)

$$T \leqslant T_0 \leqslant T_k^2 \leqslant 1 + 2\Big(\frac{(4l)^l}{l}\Big)^{2^{t-l-2}-1} + \Big(\frac{(4l)^l}{l}\Big)^{2^{t-l-1}-2} < 1 + \Big(\frac{(4l)^l}{l}\Big)^{2^{t-l-1}-1}$$

and the inductive proof is complete. The assumption that $\boldsymbol{K}$ is algebraically closed does not diminish the generality. □

Lemma 4. *Let $\boldsymbol{K}$ be any field, $\boldsymbol{U}$ a finite subset of $\boldsymbol{K}$ and $P \in \boldsymbol{K}[t_1, \ldots, t_r] \setminus \{0\}$. The equation $P(t_1, \ldots, t_r) = 0$ has no more than $\deg P(\operatorname{card} \boldsymbol{U})^{r-1}$ solutions $(t_1, \ldots, t_r) \in \boldsymbol{U}^r$.*

Proof. This is Lemma 8 in [8], p. 302 (2). □

Lemma 5. *Let p be a prime, $N = \sum_{\nu=0}^{n} c_\nu p^\nu$, where $0 \leqslant c_\nu < p$. The number of coefficients of $(x+1)^N$ non-divisible by p equals $\prod_{\nu=0}^{n}(c_\nu + 1)$.*

Proof. This is an immediate consequence of a theorem of Lucas about binomial coefficients (see [1], p. 114). □

Proof of Theorem 2. Put

$$f(x) = \sum_{j=1}^{T} A_j x^{N_j}, \quad N_j \text{ all different}, \quad A_j \neq 0 \quad (1 \leqslant j \leqslant T)$$

and let us assign two vectors $[i_1, i_2, \ldots, i_l], [j_1, j_2, \ldots, j_l] \in \{1, 2, \ldots, T\}^l$ to the same class if

$$\sum_{\lambda=1}^{l} N_{i_\lambda} = \sum_{\lambda=1}^{l} N_{j_\lambda}.$$

(2) Page 1171 in this collection.

Let $\boldsymbol{C}_1, \boldsymbol{C}_2, \ldots, \boldsymbol{C}_s$ be all distinct classes, so that

$$\{1, 2, \ldots, T\}^l = \bigcup_{r=1}^{s} \boldsymbol{C}_r.$$

We have

$$f(x)^l = \sum_{r=1}^{s} \sum_{[i_1, i_2, \ldots, i_l] \in \boldsymbol{C}_r} x^{\sum_{\lambda=1}^{l} N_{i_\lambda}} \prod_{\lambda=1}^{l} A_{i_\lambda}.$$

Since $f(x)^l$ has t terms we have for all but t classes $\boldsymbol{C}_r$, say for all $r > t$

$$\sum_{[i_1, i_2, \ldots, i_l] \in \boldsymbol{C}_r} x^{\sum_{\lambda=1}^{l} N_{i_\lambda}} \prod_{\lambda=1}^{l} A_{i_\lambda} = 0. \tag{20}$$

Let us consider the system of linear equations

$$\sum_{\lambda=1}^{l} x_{i_\lambda} = \sum_{\lambda=1}^{l} x_{j_\lambda} \quad \text{for} \quad [i_1, \ldots, i_l], [j_1, \ldots, j_l] \in \boldsymbol{C}_r \text{ and all } r \leqslant s. \tag{21}$$

This system with T unknowns has at least two linearly independent solutions namely $[1, 1, \ldots, 1]$ and $[N_1, \ldots, N_T]$. Hence the matrix $\boldsymbol{M}$ of the system is of rank $\varrho \leqslant T - 2$. The linear space of solutions has a basis consisting of $T - \varrho$ vectors: $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{T-\varrho}$ the components of which are minors of $\boldsymbol{M}$ of order ϱ (see R. Fricke [4], p. 81). Since in each row of the matrix $\boldsymbol{M}$ the sum of the positive elements and the sum of the negative elements is at most l, by the result of [7] the minors in question are in absolute value at most l^ϱ. Hence

$$\boldsymbol{v}_i = [v_{i1}, v_{i2}, \ldots, v_{iT}], \quad \text{where} \quad |v_{ij}| \leqslant l^\varrho \ (1 \leqslant i \leqslant T - \varrho). \tag{22}$$

Since every solution of (21) is a linear combination of $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{T-\varrho}$ we have for suitable $u_i^0 \in \mathbb{Q}\ (1 \leqslant i \leqslant T - \varrho)$

$$N_j = \sum_{i=1}^{T-\varrho} u_i^0 v_{ij} \quad (1 \leqslant j \leqslant T)$$

and since N_j are distinct

$$\prod_{\substack{j,k=1 \\ j<k}}^{T} \sum_{i=1}^{T-\varrho} u_i^0 (v_{ik} - v_{ij}) \neq 0.$$

Since the polynomial

$$\prod_{\substack{j,k=1 \\ j<k}}^{T} \sum_{i=1}^{T-\varrho} u_i (v_{ik} - v_{ij}) \in \mathbb{Q}[u_1, \ldots, u_{T-\varrho}]$$

does not vanish identically and is of degree $\binom{T}{2}$ it follows from Lemma 4 with

$\boldsymbol{U} = \{u \in \mathbb{Z} : |u| \leqslant \frac{1}{2}\binom{T}{2} + \frac{1}{2}\}$ that it does not vanish on the set $\boldsymbol{U}^{T-\varrho}$. Hence there exist integers $u_1^1, \ldots, u_{T-\varrho}^1$ such that

$$|u_i^1| \leqslant \frac{1}{2}\binom{T}{2} + \frac{1}{2} \quad (1 \leqslant i \leqslant T - \varrho) \tag{23}$$

and

$$\prod_{\substack{j,k=1 \\ j<k}}^{T} \sum_{i=1}^{T-\varrho} u_i^1 (v_{ik} - v_{ij}) \neq 0. \tag{24}$$

Let us put

$$N_j^1 = \sum_{i=1}^{T-\varrho} u_i^1 v_{ij} - \min_{1 \leqslant k \leqslant T} \sum_{i=1}^{T-\varrho} u_i^1 v_{ik} \quad (1 \leqslant j \leqslant T).$$

By (23) and (24) we have for all $j \leqslant T$

$$0 \leqslant N_j^1 \leqslant (T - \varrho)\left(\binom{T}{2} + 1\right) l^{\varrho} \leqslant (T^2 - T + 2) l^{T-2}. \tag{25}$$

By (24) N_j^1 are all distinct. Since $[N_1^1, \ldots, N_T^1]$ is a solution of (21) we have for all $r \leqslant s$ and suitable integers $\nu(r)$

$$\sum_{\lambda=1}^{l} N_{i_\lambda}^1 = \nu(r) \tag{26}$$

for all vectors $[i_1, \ldots, i_l] \in \boldsymbol{C}_r$. Let us put

$$f_1(x) = \sum_{j=1}^{T} A_j x^{N_j^1}.$$

The polynomial f_1 has T terms and in virtue of (25)

$$l \deg f_1 \leqslant l^{T-1}(T^2 - T + 2) < \operatorname{char} \boldsymbol{K}.$$

Moreover by (26) and (20)

$$f_1(x)^l = \sum_{r=1}^{s} x^{\nu(r)} \sum_{[i_1, i_2, \ldots, i_l] \in \boldsymbol{C}_r} \prod_{\lambda=1}^{l} A_{i_\lambda} = \sum_{r=1}^{t} x^{\nu(r)} \sum_{[i_1, i_2, \ldots, i_l] \in \boldsymbol{C}_r} \prod_{\lambda=1}^{l} A_{i_\lambda}.$$

Hence $f_1(x)^l$ has at most t terms and by Theorem 1

$$t \geqslant l + 1 + (\log 2)^{-1} \log\left(1 + \frac{\log(T-1)}{l \log 4l - \log l}\right).$$

This shows the first part of the theorem.

In order to prove the second part, let us put char $\boldsymbol{K} = p, l = p^\alpha m$, where $m \not\equiv 0 \bmod p$, $m > 1$. Take

$$f_n(x) = (1+x)^{(p^{\varphi(m)+n}+m-1)/m}$$

and let T_n, t_n be the number of terms of f_n and f_n^l, respectively. We have

$$f_n(x)^l = (1+x)^{(p^{\varphi(m)+n}+m-1)p^\alpha} = (1+x^{p^{\varphi(m)n+\alpha}})(1+x^{p^\alpha})^{m-1}$$

hence

$$t_n \leqslant 2m \leqslant 2l.$$

On the other hand, if

$$\frac{p^{\varphi(m)}+m-1}{m} = \sum_{i=0}^{k} c_i p^i, \quad \frac{p^{\varphi(m)}-1}{m} = \sum_{i=0}^{k} d_i p^i \quad (0 \leqslant c_i, d_i < p,\ c_k \neq 0)$$

then $k < \varphi(m)$; hence

$$\frac{p^{\varphi(m)n}+m-1}{m} = \sum_{i=0}^{k} c_i p^i + \sum_{\nu=1}^{n-1} \sum_{i=0}^{k} d_i p^{\varphi(m)\nu+i}$$

is a reduced representation of $(p^{\varphi(m)n}+m-1)/m$ to the base p and, by Lemma 5

$$T_n = \prod_{i=0}^{k}(c_i+1)\Big(\prod_{i=0}^{k}(d_i+1)\Big)^{n-1} \geqslant 2^n. \qquad \square$$

Lemma 6. *If $\boldsymbol{K}$ is a field of characteristic p, $\xi \in \widehat{\boldsymbol{K}}$,*

$$(x-\xi)^{pm} \Big| \sum_{j=0}^{p-1} x^j f_j(x^p), \quad \textit{where} \quad f_j \in \widehat{\boldsymbol{K}}[y], \tag{27}$$

then

$$(y-\xi^p)^m \mid f_j(y) \quad \textit{for all } j < p.$$

Proof by induction on m. For $m = 1$, we have

$$f_j(x^p) \equiv f_j(\xi^p) \bmod (x-\xi)^p,$$

hence

$$(x-\xi)^p \Big| \sum_{j=0}^{p-1} x^j f_j(\xi^p)$$

and on comparing the degrees we get $f_j(\xi^p) = 0$ for all $j < p$; thus

$$y - \xi^p \mid f_j(y).$$

Assuming that the lemma is true with m replaced by $m-1$ we get first, by applying the case $m=1$, that

$$f_j(y) = (y-\xi^p)g_j(y), \quad g_j \in \widehat{\boldsymbol{K}}[y],$$

hence by (27)

$$(x-\xi)^{p(m-1)} \Big| \sum_{j=0}^{p-1} x^j g_j(x^p)$$

and by inductive assumption

$$(y-\xi^p)^{m-1} \mid g_j(y) \quad (0 \leqslant j < p),$$

which gives the assertion. □

Lemma 7. *Let $\boldsymbol{K}$ be a field of characteristic p,*

$$f(x) = \sum_{j=0}^{p-1} x^j f_j(x^p) \in \boldsymbol{K}[x], \quad n \equiv r \bmod p, \quad 0 \leqslant r < p.$$

If $\xi \in \widehat{\boldsymbol{K}}$ is a zero of f of multiplicity exactly n, then

(28) *for all nonnegative $j \leqslant p$*

$$f_j(x) = (x-\xi^p)^{(n-r)/p} g_j(x), \quad g_j \in \widehat{\boldsymbol{K}}[x];$$

(29) *for all nonnegative $s < r$*

$$\sum_{j=s}^{p-1} \binom{j}{s} \xi^{j-s} g_j(\xi^p) = 0;$$

(30)
$$\sum_{j=r}^{p-1} \binom{j}{r} \xi^{j-r} g_j(\xi^p) \neq 0.$$

Proof. Since $(x-\xi)^{n-r} \mid f(x)$, (28) follows from Lemma 6. Now the condition $(x-\xi)^n \parallel f(x)$ reduces to [3]

$$(x-\xi)^r \parallel g(x), \quad \text{where} \quad g(x) = \sum_{j=0}^{p-1} x^j g_j(x^p).$$

If $r=0$ the condition (29) is void and (30) follows from $g(\xi) \neq 0$. If $r > 0$ we write

$$g(x) = (x-\xi)^r h(x), \quad h(\xi) \neq 0$$

and differentiating $s \leqslant r$ times we find that

$$g^{(s)}(\xi) = 0 \quad \text{for} \quad s < r, \quad g^{(r)}(\xi) = r!\, h(\xi) \neq 0,$$

which gives (29) and (30). □

[3] $a \parallel b$ means that $a \mid b$ and $(a, b/a) = 1$.

Remark. The implication given in Lemma 7 is, in fact, an equivalence.

Proof of Theorem 3. For $\xi = 0$ the theorem is clear. For $\xi \neq 0$ in view of Lemma 1 we may assume char $\boldsymbol{K} = p$. We proceed by induction on n. For $n = 1$ the theorem is obviously true. Assume it is true for all multiplicities less than $n \geqslant 2$ and let f have a zero $\xi \in \boldsymbol{K}$ of multiplicity exactly n. Let

$$f(x) = \sum_{j=0}^{p-1} x^j f_j(x^p), \quad f_j \in \boldsymbol{K}[y] \tag{31}$$

and

$$n = \sum_{i=1}^{k} c_i p^{n_i}, \quad 0 < c_i < p, \quad 0 \leqslant n_1 < n_2 < \ldots < n_k. \tag{32}$$

If $n_1 > 0$, then by Lemma 6

$$(y - \xi^p)^{n/p} \mid f_j(y) \quad (0 \leqslant j < p)$$

and for at least one j

$$(y - \xi)^{n/p} \parallel f_j(y).$$

Hence, by the inductive assumption the number of terms of f_j is at least that of $(y-\xi^p)^{n/p}$, i.e. that of $(x - \xi)^n$.

If $n_1 = 0$ we apply Lemma 7 and infer (28), (29), (30) with $r = c_1$. (30) implies that at least one of the elements $g_j(\xi^p)$ $(c_1 \leqslant j < p)$ is not zero.

We assert that among the numbers $g_j(\xi^p)$ $(0 \leqslant j < p)$ there are at least $c_1 + 1$ different from 0. Indeed, otherwise there would be at least $p - c_1$ indices j with $g_j(\xi^p) = 0$. Let the remaining indices be $j_1, \ldots, j_{c_1}$. The system of equations (29) gives

$$\sum_{t=1}^{c_1} \binom{j_t}{s} \xi^{j_t} g_{j_t}(\xi^p) = 0 \quad (0 \leqslant s < c_1).$$

However

$$\left| \binom{j_t}{s} \right|_{\substack{0 \leqslant s < c_1 \\ 1 \leqslant t \leqslant c_1}} = \prod_{0 \leqslant q < r < c_1} \frac{j_r - j_q}{r - q} \neq 0,$$

hence $g_{j_t}(\xi^p) = 0$ for all t and thus $g_j(\xi^p) = 0$ for all $j < p$, contrary to (30).

Let now $g_j(\xi^p) \neq 0$ for $j \in \boldsymbol{S}$, where $\boldsymbol{S}$ is a set of cardinality $c_1 + 1$. We have for $j \in \boldsymbol{S}$

$$(y - \xi^p)^{(n-c_1)/p} \parallel f_j(y),$$

hence by the inductive assumption $f_j(y)$ has at least as many terms as $(y - \xi^p)^{(n-c_1)/p}$, i.e. by Lemma 5 and by (32) at least $\prod_{i=2}^{k} (c_i + 1)$ terms. It follows that $f(x)$ has at least $\prod_{i=1}^{k} (c_i + 1)$ terms, but this is exactly by Lemma 5 the number of terms of $(x - \xi)^n$.

References

[1] E. R. Berlekamp, *Algebraic Coding Theory*. McGraw–Hill, New York 1968.

[2] P. Erdős, *On the number of terms of the square of a polynomial*. Nieuw Arch. Wiskunde (2) 23 (1949), 63–65.

[3] R. Freud, *On the minimum number of terms in the square of a polynomial*. Mat. Lapok 24 (1973), 95–98 (Hungarian).

[4] R. Fricke, *Lehrbuch der Algebra* I. Braunschweig 1924.

[5] G. Hajós, *Solution of Problem 41*. Mat. Lapok 4 (1953), 40–41 (Hungarian).

[6] H. L. Montgomery, A. Schinzel, *Some arithmetic properties of polynomials in several variables*. In: Transcendence Theory: Advances and Applications (ed. A. Baker and D. Masser), Academic Press, London 1977, 195–203; this collection: E6, 747–754.

[7] A. Schinzel, *An inequality for determinants with real entries*. Colloq. Math. 38 (1978), 319–321; this collection: M4, 1347–1349.

[8] —, *On the relation between two conjectures on polynomials*. Acta Arith. 38 (1980), 285–322; this collection: J5, 1154–1191.

[9] W. Verdenius, *On the number of terms of the square and the cube of polynomials*. Indag. Math. 11 (1949), 546–565.

Originally published in
Dissertationes Mathematicae (*Rozprawy Matematyczne*)
CCCXXIX (1993)

On reducible trinomials

Contents

Introduction and the statement of results

The problem of reducibility of binomials over $\mathbb{Q}$ was settled nearly a hundred years ago by Vahlen [32]. His criterion was soon generalized to all fields of characteristic 0 by Capelli [3] and much later to all fields of positive characteristic by Rédei [18]. It is the aim of the present paper to prove similar results for trinomials at least over algebraic number fields or function fields in one variable. In the latter case, when the field in question is rational, one variable can be replaced by any number of variables, and the results are definitive.

In the sequel n, m denote positive integers, $n > m$,

$$n_1 = \frac{n}{(n,m)}, \qquad m_1 = \frac{m}{(n,m)};$$

K is a field of characteristic $\pi \geqslant 0$ with $\pi \nmid nm(n-m)$, $\overline{K}$ is an algebraic closure of K, $\boldsymbol{y}$ is a variable vector, and ζ_n is a primitive root of unity of order n in K.

Corrected following *Errata*, Acta Arith. 73 (1995), 399–400; *Publ. Math. Debrecen*, 56 (2000), 605–607.

Theorem 1. *Let $n \geqslant 2m$ and $A, B \in K(\mathbf{y})^*$, $A^{-n}B^{n-m} \notin K$. The trinomial $x^n + Ax^m + B$ is reducible over $K(\mathbf{y})$ if and only if either*

(i) *$x^{n_1} + Ax^{m_1} + B$ has a proper linear or quadratic factor over $K(\mathbf{y})$*

or

(ii) *there exists an integer l such that*

$$\left\langle \frac{n}{l}, \frac{m}{l} \right\rangle := \langle \nu, \mu \rangle \in S_0 := \bigcup_{p \text{ prime}} \langle 2p, p \rangle \cup \big\{ \langle 6,1\rangle, \langle 6,2\rangle, \langle 7,1\rangle, \langle 8,2\rangle, \langle 8,4\rangle, \langle 9,3\rangle, \langle 10,2\rangle, \langle 10,4\rangle, \langle 12,2\rangle, \langle 12,3\rangle, \langle 12,4\rangle, \langle 15,5\rangle \big\}$$

and $A = u^{\nu-\mu}A_{\nu,\mu}(v)$, $B = u^{\nu}B_{\nu,\mu}(v)$, where $u, v \in K(\mathbf{y})$ and the polynomials $A_{\nu,\mu}$, $B_{\nu,\mu}$ are given in Table 1.

Table 1

$\nu,\ \mu$	$A_{\nu,\mu}$	$B_{\nu,\mu}$
$2p,\ p$	$-\left(\frac{1+\sqrt{1-4v}}{2}\right)^p - \left(\frac{1-\sqrt{1-4v}}{2}\right)^p$	v^p
c 6, 1	$4v(v^2+3)$	$-(v^2+4v-1)(v^2-4v-1)$
6, 2	$4(v+1)$	$-v^2$
c 7, 1	$-(2v+1)^4(4v^2-3v+1) \times (v^3-2v^2-v+1)$	$v(2v-1)(2v+1)^5(3v-2) \times (v^2-v+1)$
8, 2	$-v^2+8v-8$	$(2v-2)^2$
8, 4	$2v^2-8v+4$	v^4
9, 3	$v^3-81v+243$	$27(v-3)^3$
10, 2	$4v^3-8v+4$	$-(v^2-4v+2)^2$
10, 4	$v^5(-v^3+8v-8)$	$-4v^8(v-1)^4$
12, 2	$1024(v-4)^8(2v-3)(v^2-6v+6) \times (v^2-2v+2)$	$1024(v-4)^{10}(v^3-8v+8)^2$
12, 3	$-729v(v-1)^7(2v-1)(3v^2-6v+2) \times (3v^2-3v+1)$	$729(v-1)^9(3v^3-3v+1)^3$
12, 4	$512(2v-1)(2v^2+2v-1)(2v^2-2v+1)$	$1024(2v^2-4v+1)^4$
c 15, 5	$5(5v-5)^7(5v^4-5v^3-5v^2+5v-1) \times (5v^4-10v^3+10v^2-5v+1)$	$(5v-5)^{10}(5v^2-5v+1)^5$

Theorem 2. *Let $n \geqslant 2m$ and $A, B \in L^*$, where L is a finite separable extension of $K(y_1)$ with $\overline{K}L$ of genus $g > 0$ and $A^{-n}B^{n-m} \notin \overline{K}$.*

For $g = 1$ the trinomial $x^n + Ax^m + B$ is reducible over L if and only if at least one of the following three conditions is satisfied:

(iii) *$x^{n_1} + Ax^{m_1} + B$ has a proper linear or quadratic factor over L ;*

(iv) *there exists an integer l such that*

$$\left\langle \frac{n}{l}, \frac{m}{l} \right\rangle := \langle \nu, \mu \rangle \in S_0 \qquad \text{and} \qquad A = u^{\nu-\mu} A_{\nu,\mu}(v), \quad B = u^{\nu} B_{\nu,\mu}(v),$$

where $u, v \in L$ and $A_{\nu,\mu}$, $B_{\nu,\mu}$ are given in Table 1;

(v) *there exists an integer l such that*

$$\left\langle \frac{n}{l}, \frac{m}{l} \right\rangle := \langle \nu, \mu \rangle \in S_1 := \{\langle 7, 2\rangle, \langle 7, 3\rangle, \langle 8, 1\rangle, \langle 9, 1\rangle, \langle 14, 2\rangle, \langle 21, 7\rangle\}$$

and $A = u^{\nu-\mu} A_{\nu,\mu}(v, w)$, $B = u^{\nu} B_{\nu,\mu}(v, w)$, where $u \in L$, $\langle v, w \rangle \in E_{\nu,\mu}(L)$, and the elliptic curve $E_{\nu,\mu}$ and the polynomials $A_{\nu,\mu}$, $B_{\nu,\mu}$ are given in Table 2. *For $\langle \nu, \mu \rangle = \langle 8, 1 \rangle$ there is a double choice.*

For $g > 1$ the trinomial $x^n + Ax^m + B$ is reducible over L if and only if either (iii) *or* (iv) *holds or there exists an integer l such that*

$$\left\langle \frac{n}{l}, \frac{m}{l} \right\rangle := \langle \nu, \mu \rangle \in \mathbb{Z}^2, \qquad \nu < 24g$$

and $x^{\nu} + Ax^{\mu} + B$ is reducible over L.

Theorem 3. *Let L be a finite separable extension of $K(\boldsymbol{y})$, $L \cap \overline{K} = K_0$, and $A, B \in L^*$, $A^{-n}B^{n-m} \in \overline{K}$. The trinomial $x^n + Ax^m + B$ is reducible over L if and only if there exists a $q \mid (m, n)$, $q = 1, 4$ or a prime and a $C \in L$ such that*

$$A = aC^{(n_1-m_1)q}, \qquad B = bC^{n_1 q}, \qquad a, b \in K_0,$$

and

$$x^{n_1 q} + ax^{m_1 q} + b \qquad \text{is reducible over } K_0.$$

Theorem 1 has the following consequences.

Theorem 4. *Let $a \in K^*$ and $B \in K(\boldsymbol{y}) \setminus K$. The trinomial $x^n + ax^m + B$ is reducible over $K(\boldsymbol{y})$ if and only if for a certain $t \in K(\boldsymbol{y})$ either $B = -t^{n_1} - at^{m_1}$ or $n_1 \geqslant 4$, $m_1 = n_1 - 1$,*

$$B = (-a)^{n_1} t^{n_1-1} \frac{f_{n_1-1}(t)^{n_1-1}}{f_{n_1}(t)^{n_1}}, \qquad f_l(t) = \frac{(1 + \sqrt{1-4t})^l - (1 - \sqrt{1-4t})^l}{2^l \sqrt{1-4t}}$$

or there exists an integer l such that

$$\left\langle \frac{n}{l}, \frac{m}{l} \right\rangle := \langle \nu, \mu \rangle \in \{\langle 4, 1\rangle, \langle 4, 2\rangle, \langle 6, 2\rangle, \langle 6, 3\rangle, \langle 6, 4\rangle, \langle 6, 5\rangle, \langle 7, 6\rangle, \langle 8, 6\rangle\}$$

and $B = B^*_{\nu,\mu}(t)$, where the rational functions $B^*_{\nu,\mu}$ are given in Table 3. *If $\langle \nu, \mu \rangle = \langle 8, 6 \rangle$ we must have $a = \alpha^2 - 2\beta^2$, where $\alpha, \beta \in K$.*

Table 2

$\nu,\ \mu$	$E_{\nu,\mu}$	$A_{\nu,\mu}$	$B_{\nu,\mu}$
7, 2	$w^2 = v^3 + 16v^2 + 64v + 80$	$2v^2 - 8v - 48 + w(2v - 4)$	$-(4v + 12 + w) \times (v^2 + 12v + 32 + 4w)$
7, 3	$w^2 = v^3 - 675v + 13662$	$(-v^3 + 27v^2 + 3753v - 34803 + w(6v - 666)) \times (v - 39)$	$6(v - 39)^2 \times (-v^2 - 12v + 693 + 6w) \times (9v^2 + 162v - 4455 - w(v + 33))$
8, 1	$w^2 = v^3 - 10v + 12$	$-8v^3 + 20v^2 + 8v - 32 + w(3v^2 - 12v - 10)$	$(w - 3v + 5)(-3v^2 + 15v - 17 + w(2v - 5))$
	$w^2 = v^3 - 20v - 16$	$128(w - 2v - 8)^4 \times (v + 2)(v^2 + 12v + 4) \times (2w - v^2 + 4v + 4) \times (4w - v^2 - 12)$	$64(w - 2v - 8)^4(9v^4 + 8v^3 - 8v^2 + 288v + 272 - w(v^3 + 18v^2 + 76v + 24)) \times (v^4 + 24v^3 + 152v^2 + 96v + 16 + w(v^3 - 22v^2 - 52v - 72))$
9, 1	$w^2 = v^3 + 18v - 36$	$81(w - 2v - 9)^4 \times \big((v^7 + 27v^6 + 351v^5 + 639v^4 - 675v^3 - 5589v^2 + 6318v - 7290)w + (-9v^8 - 66v^7 - 936v^6 + 1890v^5 + 4995v^4 - 5670v^3 + 14580v^2 - 72900v + 37179)\big)$	$27(w - 2v - 9)^5\big((5v^7 - 603v^6 - 765v^5 + 5661v^4 + 3213v^3 + 29889v^2 - 28674v + 10206)w + (-v^9 + 63v^8 + 1719v^7 - 4959v^6 - 10611v^5 + 1917v^4 + 111456v^3 - 145800v^2 + 207036v - 61236)\big)$

Theorem 5. *Let $n \geqslant 2m$, $A \in K(\mathbf{y}) \setminus K$, $b \in K^*$. The trinomial $x^n + Ax^m + b$ is reducible over $K(\mathbf{y})$ if and only if for a certain $t \in K(\mathbf{y})^*$ either $A = -t^{n_1 - m_1} - bt^{-m_1}$ or there exists an integer l such that*

$$\left\langle \frac{n}{l}, \frac{m}{l} \right\rangle := \langle \nu, \mu \rangle \in \bigcup_{p \text{ prime}} \{\langle 2p, p \rangle\} \cup \{\langle 6, 2 \rangle, \langle 8, 2 \rangle, \langle 8, 4 \rangle, \langle 9, 3 \rangle\},$$

$A = A^*_{\nu,\mu}(t, b_1)$ and b, $b_1 \in K$ satisfy a suitable equation, which together with the rational function $A^*_{\nu,\mu}$ is given in Table 4.

Table 2 (cont.)

$v,\ \mu$	$E_{v,\mu}$	$A_{v,\mu}$	$B_{v,\mu}$
14, 2	$w^2 = v^3 - 6v + 5$	$4(v-2)^7(4v^4 - v^3 - 34v^2 + 51v - 18 + w(v^3 + 6v^2 - 18v + 8))$	$-(v-2)^8(v^3 - 12v + 14 + w(2v-6))^2$
21, 7	$w^2 = v^3 - 1715v + 33614$	*)	$14^7(w - 7v - 343)^{14} \times (21v^2 - 686v - 7203 - (v+49)w)^7$

*) $A_{v,\mu} = 3764768(w - 7v - 343)^7\big((-70v^{13} - 52822v^{12} + 19467098v^{11} + 3451790790v^{10}$
$- 68568103744v^9 - 7533659832748v^8 + 155066962439572v^7 + 6992189738638860v^6$
$+ 111845300294417242v^5 - 2615541950886590670v^4 - 18520719744403646964 6v^3$
$- 21674061456637587473 14v^2 - 17859482834686233287988v$
$- 18838244084537504480336)w + v^{15} + 2625v^4 + 91584v^{13} - 411648706v^{12}$
$- 8059651761v^{11} + 1191725696763v^{10} + 27401291878562v^9 - 2107086579531888v^8$
$- 82212564592345537v^7 + 2560864878174600039v^6 + 64436612556278953228v^5$
$- 653044731700569035282v^4 - 20619925798094466268271v^3$
$- 3996482589212668949468 83v^2 - 1749201525015966507411086v$
$- 9642297897576373802186512\big)$.

Let us note that Theorems 4 and 5 contain as very special cases Lemmas 2 and 3 of [11], which are crucial for the determination obtained in that paper of all quadrinomials in two variables reducible over K (l.c. Theorem 1). Combining the tools developed for the proof of Theorems 1 and 3 with the Faltings theorem one obtains

Theorem 6. *Let $n \geqslant 2m$, K be an algebraic number field and $a, b \in K^*$. The trinomial $x^n + ax^m + b$ is reducible over K if and only if at least one of the following four conditions is satisfied*:

(vi) *$x^{n_1} + ax^{m_1} + b$ has a proper linear or quadratic factor over K;*

(vii) *there exists an integer l such that $\langle n/l, m/l\rangle := \langle v, \mu\rangle \in S_0$ and $a = u^{v-\mu}A_{v,\mu}(v)$, $b = u^v B_{v,\mu}(v)$, where $u, v \in K$;*

(viii) *there exists an integer l such that $\langle n/l, m/l\rangle := \langle v, \mu\rangle \in S_1$ and $a = u^{v-\mu}A_{v,\mu}(v, w)$, $b = u^v B_{v,\mu}(v, w)$, where $u \in K$, $\langle v, w\rangle \in E_{v,\mu}(K)$;*

(ix) *there exists an integer l such that $\langle n/l, m/l\rangle := \langle v, \mu\rangle \in \mathbb{Z}^2$ and $a = u^{v-\mu}a_0$, $b = u^v b_0$, where $u \in K$, $\langle a_0, b_0\rangle \in F_{v,\mu}(K)$ and $F_{v,\mu}(K)$ is a certain finite set, possibly empty.*

For $\langle v, \mu\rangle \in S_0 \cup S_1 \setminus \{\langle 9, 1\rangle\}$ *we can take*

$$F_{v,\mu}(K) = \begin{cases} \left\{\left\langle 2\cdot 7^{13},\ 7^{14}\left(\frac{7+\sqrt{21}}{2}\right)^7\right\rangle, \left\langle 2\cdot 7^{13},\ 7^{14}\left(\frac{7-\sqrt{21}}{2}\right)^7\right\rangle\right\} \\ \qquad \text{if } \langle v, \mu\rangle = \langle 21, 7\rangle,\ \sqrt{21} \in K, \\ \emptyset \qquad \text{otherwise.} \end{cases}$$

Table 3

$v,\ \mu$	$B^*_{v,\mu}$
4, 1	$\dfrac{1-a^2t^6}{4t^4}$
4, 2	$\left(\dfrac{t^2+a}{2}\right)^2$
6, 2	$-\left(\dfrac{4t^4+a}{4t}\right)^2$
6, 3	$\left(\dfrac{t^3+a}{3t}\right)^2$
6, 4	$-\left(\dfrac{a^2t^4+8at^2+16}{16t^3}\right)^2$
6, 5	$a^6\,\dfrac{B_{6,1}(t)^5}{A_{6,1}(t)^6}$
7, 6	$a^7\,\dfrac{B_{7,1}(t)^6}{A_{7,1}(t)^7}$
8, 6	$\big((2\alpha-2\beta)t^2+(2\alpha-4\beta)t+(\alpha-\beta)\big)^6$ $\times\ \dfrac{\big((2\alpha+2\beta)t^2-(2\alpha+4\beta)t+(\alpha+\beta)\big)^2}{4(2t^2-1)^8}$, where $\alpha^2-2\beta^2=a$

Note that for any $p \in K[x]\setminus K$ there are only finitely many trinomials $x^n+ax^m+b \in K[x]$, $ab\neq 0$, divisible by p and satisfying neither (vi) nor (vii) (see [12]).

Note that for $\langle v, \mu\rangle \in S_1 \setminus \{\langle 7, 2\rangle, \langle 21, 7\rangle\}$ the set $E_{v,\mu}(\mathbb{Q})$ is infinite, but $E_{7,2}(\mathbb{Q}) = \{\langle -4, 4\rangle, \langle -4, -4\rangle\}$, $E_{21,7}(\mathbb{Q}) = \{\langle -49, 0\rangle\}$. Since $B_{7,2}(-4, 4) = 0$ and $x^7 + A_{7,2}(-4, -4)x^2 + B_{7,2}(-4, -4)$ is divisible by $x + 2$ and $A_{21,7}(-49, 0) = B_{21,7}(-49, 0) = 0$, for $K = \mathbb{Q}$ the cases $\langle v, \mu\rangle = \langle 7, 2\rangle, \langle 21, 7\rangle$ can be disregarded.

The sets $F_{v,\mu}(K)$ are not uniquely determined. We propose the following conjecture.

Conjecture. *For every algebraic number field* K *one can choose sets* $F_{v,\mu}(K)$ *such that*

$$\Sigma = \bigcup_{\langle v,\mu\rangle}\ \bigcup_{\langle a,b\rangle\in F_{v,\mu}(K)} \{x^v + ax^\mu + b\} \quad \textit{is finite.}$$

Even in the case $K = \mathbb{Q}$ one cannot choose $F_{v,\mu}(K)$ such that Σ is empty, as Table 5 at the end of the paper shows.

The above conjecture has the following simple consequences.

Consequence 1. *For every algebraic number field K there exists a constant $C_1(K)$ such that if $n_1 > C_1(K)$ and $a, b \in K^*$ then $x^n + ax^m + b$ is reducible over K if and only if* (vi) *holds.*

Consequence 2. *For every algebraic number field K there exists a constant $C_2(K)$ such that if $a, b \in K$ then $x^n + ax^m + b$ has in $K[x]$ an irreducible factor with at most $C_2(K)$ non-zero coefficients.*

Consequence 3. *There are only finitely many integers b such that for some $n \neq 2m$, $x^n + bx^m + 1$ is reducible over $\mathbb{Q}$.*

Table 4

$v,\ \mu$	Condition on b	$A^*_{v,\mu}$
$2p,\ p$	$b = b_1^p$	$-\left(\frac{t+\sqrt{t^2-4b_1}}{2}\right)^p - \left(\frac{t-\sqrt{t^2-4b_1}}{2}\right)^p$
6, 2	$b = -b_1^2$	$4t(t^3 + b_1)$
8, 2	$b = b_1^2$	$\frac{-4t^8 + 12b_1t^4 - b_1^2}{4t^2}$
8, 4	$b = b_1^4$	$4t^4 - 8b_1t^2 + 2b_1^2$
9, 3	$b = b_1^3$	$\frac{t^9 - 18b_1t^6 + 27b_1^2t^3 + 27b_1^3}{27t^3}$

From this point to the end of the introduction reducibility is meant over $\mathbb{Q}$. It is clear from Table 5 that if $C_1(\mathbb{Q})$ exists we have $C_1(\mathbb{Q}) \geqslant 52$.

The problem of existence of $C_2(\mathbb{Q})$ was formulated in [21]. Bremner [1] has shown that if $C_2(\mathbb{Q})$ exists we have $C_2(\mathbb{Q}) \geqslant 8$ (see also [6]) ([1]).

Using Theorem 5 of [22] one can determine an explicit value $c(a, b)$ such that if $a, b \in \mathbb{Q}^*$, $n_1 > c(a, b)$ and $x^n + ax^m + b$ is reducible then $x^{n_1} + ax^{m_1} + b$ has a *cyclotomic* linear or quadratic factor.

The problem of existence of integers b with $|b| > 2$ such that for some $n \neq 2m$ the trinomial $x^n + bx^m + 1$ is reducible was formulated in [23]. First Coray (unpublished) and then Bremner [2] have found an affirmative answer which is clear from Table 5, positions 28, 31, 48.

Here are some arithmetical applications of Theorems 4 and 5.

([1]) The entry 43b in Table 5, due to J. Abbott, shows that if $C_2(\mathbb{Q})$ exists, then $C_2(\mathbb{Q}) \geqslant 9$.

Theorem 7. *For all $a, b \in \mathbb{Z} \setminus \{0\}$ and all n there exist only finitely many reducible trinomials $ax^n + bx^m + c$ where $c \in \mathbb{Z} \setminus \{0\}$ without a factor $x^{(m,n)} - d$ apart from the following*

$$T_1(x^l; t) = ax^{4l} + bx^{2l} + a\left(\frac{at^2 + b}{2a}\right)^2,$$

$$T_2(x^l; t) = ax^{5l} + bx^{4l} - \frac{b^5}{a^5} \cdot \frac{t^2(t-2)^4}{(t^2 - 3t + 1)^5},$$

$$T_3(x^l; t) = ax^{8l} + bx^{6l} + \frac{b^8}{a^7} B^*_{8,6}(t),$$

where $t \in \mathbb{Q}$ and $\langle \alpha, \beta \rangle$ occurring in the definition of $B^*_{8,6}$ is a fixed rational solution of $\alpha^2 - 2\beta^2 = b/a$.

Theorem 8. *For all $a, c \in \mathbb{Z} \setminus \{0\}$ and all n there exist only finitely many reducible trinomials $ax^n + bx^m + c$ where $2m \leqslant n$, $b \in \mathbb{Z} \setminus \{0\}$ apart from the following*

$$T_4(x^l; t) = ax^{2pl} + aA^*_{2p,p}(t, b_1)x^{pl} + c, \qquad b_1^p = c/a,$$

$$T_5(x^l; t) = ax^{6l} + aA^*_{6,2}(t, b_1)x^{2l} + c, \qquad b_1^2 = -c/a,$$

$$T_6(x^l; t) = ax^{8l} + aA^*_{8,4}(t, b_1)x^{4l} + c, \qquad b_1^4 = c/a,$$

where $t, b_1 \in \mathbb{Q}$.

The exceptions given in Theorem 7 and 8 are genuine as it follows from the identities

$$T_1(x; t) = a\left(x^2 + tx + \frac{at^2 + b}{2a}\right)\left(x^2 - tx + \frac{at^2 + b}{2a}\right),$$

$$T_2(x; t) = a\left(x^2 + \frac{b}{a} \cdot \frac{t(t-2)}{t^2 - 3t + 1}\, x + \frac{b^2}{a^2} \cdot \frac{t(t-2)^2}{(t^2 - 3t + 1)^2}\right)$$
$$\times\left(x^3 + \frac{b}{a} \cdot \frac{-t+1}{t^2 - 3t + 1}\, x^2 + \frac{b^2}{a^2} \cdot \frac{t(t-2)}{(t^2 - 3t + 1)^2}\, x + \frac{b^3}{a^3} \cdot \frac{-t(t-2)^2}{(t^2 - 3t + 1)^3}\right),$$

$$T_3(x; t)$$
$$= a\left(x^4 + a_1x^3 + (a_1^2 - b_1^2)x^2 + (a_1 + b_1)(a_1 - b_1)^2 x + \frac{(a_1 + b_1)(a_1 - b_1)^3}{2}\right)$$
$$\times\left(x^4 - a_1x^3 + (a_1^2 - b_1^2)x^2 - (a_1 + b_1)(a_1 - b_1)^2 x + \frac{(a_1 + b_1)(a_1 - b_1)^3}{2}\right),$$

where $a_1 = 2\alpha t^2 - 4\beta t + \alpha$, $b_1 = 2\beta t^2 - 2\alpha t + \beta$,

$$T_5(x^l; t) = a(x^3 + 2tx^2 + 2t^2x + b_1)(x^3 - 2tx^2 + 2t^2x - b_1),$$

$$T_6(x^l; t) = a(x^4 + 2tx^3 + 2t^2x^2 + 2tb_1x + b_1^2)(x^4 + 2tx^3 + 2t^2x^2 - 2tb_1x + b_1^2),$$

from the divisibility

$$x^2 - tx + b_1 \mid T_4(x; t)$$

and from the remark that $T_i(x;t) \in \mathbb{Z}[x]$ for infinitely many $t \in \mathbb{Q}$, at least if $2a \mid b$ $(1 \leqslant i \leqslant 3)$ and $a \mid c$ $(4 \leqslant i \leqslant 6)$. In particular, $T_2(x;t)$ furnishes a counterexample to an assertion of Fried [9] (statement 13), probably the same as mentioned in general terms by Fried himself in [10], p. 600.

Unfortunately, the finite sets of exceptional trinomials occurring in Theorems 7 and 8 cannot be effectively determined from the proofs of the theorems, since the latter use an ineffective theorem of Siegel [28]. In the special case $a = m = 1$ an effective determination has been achieved by Ribenboim [20]. In the case of Theorem 8 it is possible to achieve the same under a less stringent assumption $(m, n) = 1$. This follows from

Theorem 9. *Let $a, b, c \in \mathbb{Z} \setminus \{0\}$, $(a, b, c) = 1$. If $ax^n + bx^m + c$ is reducible then at least one of the following four conditions is satisfied*:

(x) $|b| \leqslant |a|^{m_1}|c|^{n_1-m_1} + 1$;

(xi) $|b| < \dfrac{2m_1(n_1-m_1)}{\log 2m_1(n_1-m_1)}\,|a|^{m/n}|c|^{(n-m)/n}$, $\min\{|a|,|c|\} = 1$, $\sqrt[p]{\max\{|a|,|c|\}}$ *belongs to $\mathbb{Z}$ for some prime $p \mid n_1$*;

(xii) *for some $q \mid (m, n)$, q a prime or $q = 4$, $\sqrt[q]{|a|} \in \mathbb{Z}$, $\sqrt[q]{|c|} \in \mathbb{Z}$ and if $q = 2$ then $(-1)^{n_1}ac > 0$, while if $q = 4$ then $ac > 0$ and $n_1 \equiv 0 \bmod 2$;*

(xiii) $4 \mid (m, n)$, $ac > 0$, $n_1 \equiv 1 \bmod 2$ *and either $\sqrt[4]{|a|} \in \mathbb{Z}$, $\sqrt[4]{4|c|} \in \mathbb{Z}$ or $\sqrt[4]{4|a|} \in \mathbb{Z}$, $\sqrt[4]{|c|} \in \mathbb{Z}$.*

Theorem 9 can be regarded as a refinement of a theorem of Nagell [15], concerning trinomials $T(x; q, r) = x^n + qx^m + r$, $q, r \in \mathbb{Z}$. Nagell proves the following alternative as the necessary condition for reducibility of $T(x; q, r)$:

$$\text{either } |q| \leqslant |r|^{n-1} + 1 \text{ or } \sqrt[p]{|r|} \in \mathbb{Z} \text{ for some prime } p \mid n.$$

It is clear that (x) is stronger than the first term of the alternative and each of (xi), (xii), (xiii) is stronger than the second term. However the proof of Theorem 9 is partly based on Nagell's idea.

Theorem 9 implies

Corollary 1. *For every positive integer d there exist only finitely many trinomials $x^n + bx^m \pm 1$, where $b \in \mathbb{Z}$, $|b| > 2$, $n_1 > d$, with a factor of degree d and all of them can be found effectively. Indeed, they satisfy $n \ll d \log d$, $b \ll d^2 \log d$.*

Corollary 1 gives a partial generalization of results of Bremner [2], who determined all trinomials $x^n + bx^m + 1$, $b \in \mathbb{Z} \setminus \{0\}$, with a cubic factor, and that of H. Tverberg, who did the same for $x^n + bx^m - 1$ [31a]. Another generalization will be given below as Corollary 2 (to Theorem 10). The factorization found by Bremner

$$x^6 + (4\mu^4 - 4\mu)x^2 - 1 = (x^3 + 2\mu x^2 + 2\mu^2 x + 1)(x^3 - 2\mu x^2 + 2\mu^2 x - 1)$$

(a special case of the factorization given above for $T_5(x;t)$) shows that the condition $n_1 > d$ cannot be omitted.

For the case of a, b or a, c fixed we have

Theorem 10. *There exist two effectively computable functions $c_0(d)$ and $c_1(d)$ with the following property. If $a, b, c \in \mathbb{Z} \setminus \{0\}$, $(a, b, c) = 1$,*

$$a\xi^n + b\xi^m + c = 0 \qquad \text{and} \qquad [\mathbb{Q}(\xi) : \mathbb{Q}] \leqslant d$$

then either simultaneously

(xiv) $n < \max\left\{c_0(d),\ c_1(d)\log\dfrac{|ab|}{(a,b)}\right\}$,

(xv) $n < \max\left\{c_0(d),\ c_1(d)\log\dfrac{|bc|}{(b,c)}\right\}$,

(xvi) $n < \max\{c_0(d),\ 3c_1(d)\log|ac|\}$, *provided* $n \neq 2m$

or

(xvii) $\xi^{(n,m)} = q,\ (1 \pm i)q,\ (1 \pm \sqrt{-3})q,\ (3 \pm \sqrt{-3})q,\ q \in \mathbb{Q}$.

Corollary 2. *For every positive integer d there exist only finitely many trinomials $x^n + bx^m + 1$, where $b \in \mathbb{Z}$, $|b| > 2$, $n \neq 2m$ with a proper factor of degree d.*

I conclude the introduction by expressing my thanks to Professor J. Browkin ([2]), Professor J.-L. Nicolas, Dr. A. Pokrzywa ([3]) and Dr. T. Regińska who performed computer calculations used in this or in the previous version of the paper. Professor Nicolas has moreover improved the original Lemma 12 and simplified the proof of Lemma 24. I thank him for the permission to include his proofs. I thank Professor K. Rubin for his contribution to the proof of Lemma 51. I thank also the organizers of the Austrian-Hungarian-Slovak Number-Theory-Colloquium Graz 1992 who let me present the above results there.

PART I
Reducibility over function fields

1. Auxiliary results from the theory of algebraic functions

Let $\overline{K}(t, x)$ be a finite separable extension of $\overline{K}(t)$ and let x be a zero of a polynomial $F(t, u)$ defined and irreducible over $\overline{K}$, of degree d with respect to u.

For every $\tau \in \overline{K}$ let

$$\mathbb{F}(\tau) = \bigcup_{e=1}^{\infty} \overline{K}\big(((t-\tau)^{1/e})\big) \quad \text{and} \quad \mathbb{F}(\infty) = \bigcup_{e=1}^{\infty} \overline{K}\big((t^{-1/e})\big).$$

Lemma 1. (a) *Assume that $F(t, u) = 0$ has exactly d distinct solutions in the field $\mathbb{F}(\tau)$, including e_1 solutions belonging to $\overline{K}\big(((t-\tau)^{1/e_1})\big)$ conjugate over $\overline{K}\big((t-\tau)\big)$, ..., e_r solutions belonging to $\overline{K}\big(((t-\tau)^{1/e_r})\big)$ conjugate over $\overline{K}\big((t-\tau)\big)$, where $e_i \not\equiv 0 \bmod \pi$,*

([2]) He used the programme GP/PARI by C. Batut, D. Bernardi, H. Cohen and M. Olivier.

([3]) He used the programme MATHEMATICA, version 2.0, Wolfram Research, Inc., Champaign, Ill., 1991.

$e_1 + \ldots + e_r = d$. *Then the numerator of* $t - \tau$ *in* $\overline{K}(t, x)$ *has the factorization into prime divisors of the form* $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$.

(b) *Assume that* $F(t, u) = 0$ *has exactly* d *distinct solutions in the field* $\mathbb{F}(\infty)$, *including* f_1 *solutions belonging to* $\overline{K}\big((t^{-1/f_1})\big)$ *conjugate over* $\overline{K}\big((t^{-1})\big)$, ..., f_s *solutions belonging to* $\overline{K}\big((t^{-1/f_s})\big)$ *conjugate over* $\overline{K}\big((t^{-1})\big)$, *where* $f_i \not\equiv 0 \bmod \pi$, $f_1 + \ldots + f_s = d$. *Then the denominator of* t *in* $\overline{K}(t, x)$ *has the factorization into prime divisors of the form* $\mathfrak{q}_1^{f_1} \cdots \mathfrak{q}_s^{f_s}$.

(c) *Under the assumptions of* (a) *and* (b) *the Galois group of the polynomial* F *over* $\overline{K}(t)$ *contains permutations of the type* $(e_1, \ldots, e_r)$ *and* $(f_1, \ldots, f_s)$, *respectively.*

Proof. (a) and (b) are proved in [8], Ch. III, §2 under the assumption that $\operatorname{char} K = 0$ formulated on p. 135. The proof however uses only the assumptions of (a) and (b). One can compare [5], Ch. IV, §6.

To prove (c) we take $e = \underset{1 \leqslant i \leqslant r}{\text{l.c.m.}}\, e_i \not\equiv 0 \bmod \pi$ and consider the automorphism of the field $\overline{K}\big(((t-\tau)^{1/e})\big)$ given by

$$(t - \tau)^{1/e} \to \zeta_e (t - \tau)^{1/e}.$$

The zeros of F belonging to $\overline{K}\big(((t-\tau)^{1/e_i})\big)$ and conjugate over $\overline{K}\big((t-\tau)\big)$ are cyclically permuted. This shows that the Galois group in question contains a permutation of the type $(e_1, \ldots, e_r)$. For the type $(f_1, \ldots, f_s)$ the proof is similar. □

Remark. The proof of (c) is modelled on the proof of a special case given by Turnwald [31].

Lemma 2. *Let* g *be the genus of* $\overline{K}(t, x)$.

(a) *If the assumptions of Lemma* 1(a) *and* (b) *are satisfied for all* $\tau \in \overline{K}$, *we have*

$$g = \frac{1}{2} \sum_{\tau \in \overline{K}} \sum_{i=1}^{r} (e_i - 1) + \frac{1}{2} \sum_{j=1}^{s} (f_j - 1) - d + 1.$$

(b) *If the field* $\overline{K}(t, x)$ *is rational,* $g = 0$.

(c) *If* L *is a field between* $\overline{K}(t)$ *and* $\overline{K}(t, x)$, *the genus of* L *does not exceed* g.

Proof. For (a) see [8], Ch. III, §2, formula (36) and §3, formula (8). For (b) see [5], Ch. II, §2, for (c) see [8], Ch. III, §2, formulae (9) and (10) or [5], Ch. VI, §2, Corollary 2. □

2. Determination of the range of Tables 1 and 2 (Lemmas 3–27)

In all this section except Lemmas 26 and 27 it is assumed that $(m, n) = 1$, $s(n-m) - rn = 1$, $s > 0$, $r \geqslant 0$.

Note that the condition $\pi \nmid nm(n-m)$ implies $\pi \neq 2$.

Lemma 3. *The algebraic function* $x(t)$ *defined by the equation*

$$T(x; t^r, t^s) := x^n + t^r x^m + t^s = 0$$

has just one branch point $t_1 \neq 0, \infty$ *with one two-cycle given by the Puiseux expansions*

$$x(t) = \xi_1 \pm (t - t_1)^{1/2} P_{11}(\pm (t - t_1)^{1/2}), \qquad \xi_1 \neq 0,$$

and the remaining expansions

$$x(t) = P_{1j}(t - t_1) \qquad (2 \leqslant j \leqslant n-1).$$

Moreover, the branch point 0 *has one* m*-cycle given by the Puiseux expansions*

$$x(t) = \zeta_{2m}^{2i+1} t^{(s-r)/m} P_{01}(\zeta_{2m}^{(2i+1)n} t^{1/m}) \qquad (0 \leqslant i < m)$$

and one $(n-m)$*-cycle given by the Puiseux expansions*

$$x(t) = \zeta_{2(n-m)}^{2i+1} t^{r/(n-m)} P_{02}(\zeta_{2(n-m)}^{-(2i+1)n} t^{1/(n-m)}) \qquad (0 \leqslant i < n-m),$$

and the branch point ∞ *with one* n*-cycle given by the Puiseux expansions*

$$x(t) = \zeta_{2n}^{2i+1} t^{s/n} P_{21}(\zeta_{2n}^{(2i+1)m} t^{-1/n}) \qquad (0 \leqslant i < n).$$

Here P_{ij} *are ordinary formal power series with* $P_{ij}(0) \neq 0$.

Proof. The standard argument gives

$$t_1 = \left(-\frac{m}{n}\right)^m \left(-\frac{n-m}{n}\right)^{n-m}, \qquad \xi_1 = \left(-\frac{m}{n}\right)^{s-r} \left(-\frac{n-m}{n}\right)^r,$$

$$P_{11}(0) = \left(\frac{-2\xi_1^2}{nm(n-m)t_1}\right)^{1/2}, \qquad \prod_{j=2}^{n-1} P_{1j}(0) = (-1)^n \frac{t_1^s}{\xi_1^2},$$

$$P_{01}(0) = P_{02}(0) = P_{21}(0) = 1. \qquad \square$$

Lemma 4. *The Galois group of* $T(x; t^r, t^s)$ *over* $\overline{K}(t)$ *is the symmetric group* S_n.

Proof. By Lemmas 1(c) and 3 the Galois group in question contains the following permutations: a transposition, the product of an m-cycle and an $(n-m)$-cycle, and an n-cycle. By Theorem 14 of Chapter I of [30] the group is either S_n or imprimitive. We wish to eliminate the latter possibility.

Assume without loss of generality that $m \leqslant n-m$. By a suitable numbering we can achieve that the product of two cycles is $(1, \ldots, m)(m+1, \ldots, n)$. Further let $\mu, \nu_2, \ldots, \nu_q$ be an imprimitivity system containing $\mu \leqslant m$ with $\nu_i \leqslant m$ for $i \leqslant p$ exclusively. Since $(m, n) = 1$ the group also contains the cycle $(m+1, \ldots, n)^m$. Then according to the definition of imprimitivity $(m+1, \ldots, n)^m$ permutes the numbers $\nu_{p+1}, \ldots, \nu_q$, therefore $\{\nu_{p+1}, \ldots, \nu_q\} = \{m+1, \ldots, n\}$ or $\emptyset$. In the first case, $q \geqslant n - m + p > n/2$ and since $q \mid n$, we have $q = n$. In the second case the imprimitivity system is contained in $\{1, \ldots, m\}$ and since this holds for all $\mu \leqslant m$, we have $q \mid m$. But $(m, n) = 1$ gives $q = 1$. $\square$

Remark. In the course of the proof we have obtained a generalization of Theorem 20 of Chapter V of [30] corresponding to $m = 1$.

Definition 1. Let $T(x; t^r, t^s) = \prod_{i=1}^{n} (x - x_i(t))$. We set

$$L(k, m, n) = K\left(t, \tau_1(x_1, \ldots, x_k), \ldots, \tau_k(x_1, \ldots, x_k)\right),$$

$$L^*(k, m, n) = \overline{K}\left(t, \tau_1(x_1, \ldots, x_k), \ldots, \tau_k(x_1, \ldots, x_k)\right),$$

where τ_j is the jth fundamental symmetric function.

Remark. By Lemma 4 and since

$$T(x; t^{r+n-m}, t^{s+n}) = t^n T\left(\frac{x}{t}; t^r, t^s\right),$$

$L(k, m, n)$ and $L^*(k, m, n)$ are determined by k, m, n up to an isomorphism fixing $K(t)$ and $\overline{K}(t)$, respectively.

Lemma 5. *In $L^*(k, m, n)$, the numerator of $t - t_1$ has $\binom{n-2}{k-1}$ prime divisors in the second power and none in the higher ones.*

Proof. By Lemma 1(a) the prime divisors of the numerator of $t - t_1$ are in one-to-one correspondence with the cycles of Puiseux expansions of a generating element of $L^*(k, m, n)/\overline{K}(t)$ at $t = t_1$, provided the relevant condition is satisfied. For the generating element we take $y(t) = \sum_{j=1}^{k} a^j \tau_j(x_1, \ldots, x_k)$, where $a \in \overline{K}$ is chosen so that $\sum_{j=1}^{k} a^j \tau_j(x_{i_1}, \ldots, x_{i_k}) = \sum_{j=1}^{k} a^j \tau_j(x_1, \ldots, x_k)$ implies $\{i_1, \ldots, i_k\} = \{1, \ldots, k\}$. By Lemma 4 for each set $\{i_1, \ldots, i_k\} \subset \{1, \ldots, n\}$ there is an automorphism of the field $\overline{K}(x_1(t), \ldots, x_n(t))/\overline{K}(t)$ taking $x_1(t), \ldots, x_k(t)$ into $x_{i_1}(t), \ldots, x_{i_k}(t)$, respectively. Then at $t = t_1$ we obtain $\binom{n}{k}$ different expansions for y, including

$$\sum_{j=1}^{k} a^j \big((\xi_1 + (t - t_1)^{1/2} P_{11}((t - t_1)^{1/2}))\tau_{j-1}(P_{1i_1}(t - t_1), \ldots, P_{1i_{k-1}}(t - t_1)) + \tau_j(P_{1i_1}(t - t_1), \ldots, P_{1i_{k-1}}(t - t_1))\big),$$

where $\{i_1, \ldots, i_{k-1}\}$ is any subset of cardinality $k-1$ of $\{2, \ldots, n-1\}$. Since the cofactor of $(t - t_1)^{1/2} P_{11}\big((t - t_1)^{1/2}\big)$ equal to

$$\sum_{j=1}^{k} a^j \tau_{j-1}(P_{1i_1}(t - t_1), \ldots, P_{1i_{k-1}}(t - t_1)) = a \prod_{j=1}^{k-1} (1 + a P_{1i_j}(t - t_1))$$

is non-zero and $\pi \neq 2$, we have indeed $\binom{n-2}{k-1}$ prime divisors in the second power in the numerator of $t - t_1$. All other prime divisors appear in the first power at most. □

Lemma 6. *For every $d \mid n$ the number of subsets $\{i_1, \ldots, i_k\}$ of $\{1, 2, \ldots, n\}$ of cardinality $k > 0$ such that*

$$\{i_1 + d, i_2 + d, \ldots, i_k + d\} \equiv \{i_1, i_2, \ldots, i_k\} \bmod n$$

equals

$$\binom{d}{dk/n} \qquad \text{if } n \mid dk$$

and 0 *otherwise.*

Proof. To every subset S in question we make correspond the set R of all positive integers $r \leqslant d$ such that there exists an $s \in S$ with $s \equiv r \bmod d$. The condition $S + d \equiv S \bmod n$ implies that for every $r \in R$ we have $r + id \in S \bmod n$ for $i = 1, \ldots, n/d$. Since for $r, r' \in R, r \neq r'$ we have $r+id \neq r'+i'd$ it follows that $\frac{n}{d} \mid k$, hence there are no subsets S in question if $n \nmid dk$. If $n \mid dk$ we may choose arbitrarily a subset R of $\{1, \ldots, d\}$ of cardinality dk/n and obtain a set S satisfying $S+d \equiv S \bmod n$ on taking $S \equiv R+\{0, d, \ldots, n-d\}$.□

Lemma 7. *For every $d \mid n$ the number $f(n, k, d)$ of subsets $\{i_1, \ldots, i_k\}$ of $\{1, 2, \ldots, n\}$ of cardinality $k > 0$ such that*

$$\{i_1 + \delta, i_2 + \delta, \ldots, i_k + \delta\} \equiv \{i_1, i_2, \ldots, i_k\} \bmod n$$

holds for $\delta = d$ but for no smaller δ, satisfies

$$f(n, k, d) = \begin{cases} \displaystyle\sum_{\delta \mid (d, dk/n)} \mu(\delta) \binom{d/\delta}{\frac{dk/\delta}{n}} & \text{if } n \mid dk, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. By Lemma 6 we have

$$\sum_{\delta \mid d} f(n, k, \delta) = \begin{cases} \binom{d}{dk/n} & \text{if } n \mid dk, \\ 0 & \text{otherwise,} \end{cases}$$

and Lemma 7 follows by the Möbius inversion formula. □

Lemma 8. *The denominator of t in $L^*(k, m, n)$ has*

$$\frac{1}{n} \sum_{d \mid (n,k)} \varphi(d) \binom{n/d}{k/d}$$

distinct prime divisors.

Proof. The function $y(t)$ has the following Puiseux expansions at $t = \infty$:

$$Q(t; i_1, \ldots, i_k) = \sum_{j=1}^{k} a^j \tau_j \left(\zeta_{2n}^{2i_1+1} t^{s/n} P_{21}(\zeta_{2n}^{(2i_1+1)m} t^{-1/n}), \ldots, \zeta_{2n}^{2i_k+1} t^{s/n} P_{21}(\zeta_{2n}^{(2i_k+1)m} t^{-1/n}) \right),$$

where $\{i_1, \ldots, i_k\}$ runs through all subsets of $\{1, \ldots, n\}$ of cardinality k. The conjugates of $t^{1/n}$ over $\overline{K}\left((t^{-1/d})\right)$, where $d \mid n$ are $\zeta_n^{de} t^{1/n}$, where $0 \leqslant e < n/d$. Therefore if P is an ordinary power series the conjugates of $P(t^{-1/n})$ over $\overline{K}\left((t^{-1/d})\right)$ are $P(\zeta_n^{-de} t^{-1/n})$, where $0 \leqslant e < n/d$. Therefore $Q(t; i_1, \ldots, i_k) \in \overline{K}\left((t^{-1/d})\right)$ if and only if

$$Q(t; i_1, \ldots, i_k) = Q(t; i_1 + ed, \ldots, i_k + ed) \quad (0 \leqslant e < n/d),$$

hence by the choice of a, if and only if

$$\{i_1 + d, \ldots, i_k + d\} \equiv \{i_1, \ldots, i_k\} \bmod n.$$

Thus

$$Q(t; i_1, \dots, i_k) \in \overline{K}\big((t^{-1/d})\big) \setminus \bigcup_{\substack{\delta \mid d \\ \delta < d}} \overline{K}\big((t^{-1/\delta})\big)$$

if and only if

$$\{i_1 + \delta, \dots, i_k + \delta\} \equiv \{i_1, \dots, i_k\} \bmod n$$

for $\delta = d$, but for no smaller $\delta \mid d$. It follows by Lemma 7 that $y(t)$ has, at $t = \infty$, $f(n, k, d)$ expansions belonging to $\overline{K}\big((t^{-1/d})\big) \setminus \bigcup_{\delta \mid d,\, \delta < d} \overline{K}\big((t^{-1/\delta})\big)$. These expansions split into cycles of d conjugate expansions each, where $n \mid dk$, i.e. $d = e\,\frac{n}{(n,k)}$, $e \mid (n, k)$. Hence the number of distinct prime divisors of the denominator of t equals

$$(1)\quad \frac{(n,k)}{n} \sum_{e \mid (n,k)} \frac{1}{e} f\left(n, k, \frac{n}{(n,k)}\, e\right) = \frac{(n,k)}{n} \sum_{e \mid (n,k)} \frac{1}{e} \sum_{\delta \mid e} \mu(\delta) \binom{\frac{n}{(n,k)}\,\frac{e}{\delta}}{\frac{k}{(n,k)}\,\frac{e}{\delta}}$$
$$= \frac{1}{n} \sum_{\delta' \mid (n,k)} \binom{n/\delta'}{k/\delta'} \delta' \sum_{\delta \mid \delta'} \frac{\mu(\delta)}{\delta} = \frac{1}{n} \sum_{\delta' \mid (n,k)} \varphi(\delta') \binom{n/\delta'}{k/\delta'},$$

which proves the lemma. □

Lemma 9. *The numerator of t in $L^*(k, m, n)$ has*

$$\frac{1}{m(n-m)} \sum_{l=0}^{k} \Bigg(\sum_{d \mid (m,l)} \varphi(d) \binom{m/d}{l/d} \Bigg) \Bigg(\sum_{d \mid (n-m, k-l)} \varphi(d) \binom{(n-m)/d}{(k-l)/d} \Bigg)$$

distinct prime divisors.

Proof. The function $y(t)$ has the following Puiseux expansions at $t = 0$:

$$Q(t; l; i_1, \dots, i_k) = \sum_{j=1}^{k} a^j \tau_j \big(\zeta_{2m}^{2i_1+1} t^{(s-r)/m} P_{01}(\zeta_{2m}^{(2i_1+1)n} t^{1/m}),$$
$$\dots,\ \zeta_{2m}^{2i_l+1} t^{(s-r)/m} P_{01}(\zeta_{2m}^{(2i_l+1)n} t^{1/m}),\ \zeta_{2(n-m)}^{2i_{l+1}+1} t^{r/(n-m)} P_{02}(\zeta_{2(n-m)}^{-(2i_{l+1}+1)n} t^{1/(n-m)}),$$
$$\dots,\ \zeta_{2(n-m)}^{2i_k+1} t^{r/(n-m)} P_{02}(\zeta_{2(n-m)}^{-(2i_k+1)n} t^{1/(n-m)}) \big),$$

where l runs from 0 to k, $\{i_1, \dots, i_l\}$ runs through all subsets of $\{0, 1, \dots, m-1\}$ of cardinality l, and $\{i_{l+1}, \dots, i_k\}$ runs through all subsets of $\{0, \dots, n-m-1\}$ of cardinality $k-l$.

If P is an ordinary power series, the conjugates of $P(t^{1/m})$ and $P(t^{1/(n-m)})$ over $\overline{K}\big((t^{1/dd_1})\big)$, where $d \mid m$, $d_1 \mid n-m$ are $P(\zeta_m^{de} t^{1/m})$ $(0 \leqslant e < m/d)$ and $P(\zeta_{n-m}^{d_1 e_1} t^{1/(n-m)})$ $(0 \leqslant e_1 < (n-m)/d_1)$, respectively. Therefore,

$$Q(t; l; i_1, \dots, i_k) \in \overline{K}\big((t^{1/dd_1})\big), \qquad d \mid m,\ \ d_1 \mid n-m$$

if and only if

$$Q(t;l;i_1,\dots,i_k) = Q(t;l;i_1+ed,\dots,i_l+ed,i_{l+1}+e_1d_1,\dots,i_k+e_1d_1) \\ (0\leqslant e<m/d,\ 0\leqslant e_1<(n-m)/d_1),$$

hence by the choice of a, if and only if

$$\{i_1,\dots,i_l\}+d\equiv\{i_1,\dots,i_l\} \bmod m,$$
$$\{i_{l+1},\dots,i_k\}+d_1\equiv\{i_{l+1},\dots,i_k\} \bmod (n-m).$$

It follows from the definition of the function f in Lemma 7 that $y(t)$ has, at $t=0$, $\sum_{l=0}^{k} f(m,l,d)\,f(n-m,k-l,d_1)$ expansions belonging to

$$\overline{K}\big((t^{1/dd_1})\big)\setminus\bigcup_{\substack{\delta\mid dd_1\\ \delta<dd_1}}\overline{K}\big((t^{1/\delta})\big),\qquad \text{where}\quad d\mid m,\ d_1\mid n-m.$$

These expansions split into cycles of dd_1 conjugate expansions each, where $m\mid dl$ and $n-m\mid d_1(k-l)$, i.e.

$$d=e\,\frac{m}{(m,l)},\qquad d_1=e_1\,\frac{n-m}{(n-m,k-l)}.$$

Hence the number of distinct prime divisors of the numerator of t is

$$\sum_{l=0}^{k}\frac{(m,l)}{m}\cdot\frac{(n-m,k-l)}{(n-m)}\Big(\sum_{e\mid(m,l)}\frac{1}{e}\,f\Big(m,l,\frac{m}{(m,l)}\,e\Big)\Big) \\ \times\Big(\sum_{e_1\mid(n-m,k-l)}\frac{1}{e_1}\,f\Big(n-m,k-l,\frac{n-m}{(n-m,k-l)}\,e_1\Big)\Big),$$

which by the formula (1) equals

$$\frac{1}{m(n-m)}\sum_{l=0}^{k}\Big(\sum_{d\mid(m,l)}\varphi(d)\binom{m/d}{l/d}\Big)\Big(\sum_{d\mid(n-m,k-l)}\varphi(d)\binom{(n-m)/d}{(k-l)/d}\Big).\qquad\square$$

Lemma 10. *The genus $g^*(k,m,n)$ of the field $L^*(k,m,n)$ equals*

$$\frac{1}{2}\binom{n-2}{k-1}-\frac{1}{2n}\sum_{d\mid(n,k)}\varphi(d)\binom{n/d}{k/d} \\ -\frac{1}{2m(n-m)}\sum_{l=0}^{k}\Big(\sum_{d\mid(m,l)}\varphi(d)\binom{m/d}{l/d}\Big)\Big(\sum_{d\mid(n-m,k-l)}\varphi(d)\binom{(n-m)/d}{(k-l)/d}\Big)+1.$$

Proof. By Lemma 3 the only ramification points of $y(t)$ may be t_1, 0 and ∞. The lemma follows now from Lemmas 2(a), 5, 8 and 9. $\square$

Lemma 11. *For all positive integers a, b, c with $a > b$ and $c \geqslant 2$ we have*

$$\binom{ac}{bc} \geqslant \frac{a}{4}\binom{a}{b}\binom{2c}{c}.$$

Proof. We assume without loss of generality that $a \geqslant 2b$. We have

$$\binom{ac}{bc}\binom{a}{b}^{-1} = c^{b-1}\,\frac{\prod_{i=a-b}^{a-1}\prod_{j=1}^{c-1}(ic+j)}{\prod_{i=0}^{b-1}\prod_{j=1}^{c-1}(ic+j)}, \qquad \binom{2c}{c} = 2\,\frac{\prod_{j=1}^{c-1}(c+j)}{(c-1)!}.$$

Hence

$$\binom{ac}{bc}\binom{a}{b}^{-1}\binom{2c}{c}^{-1} = \frac{1}{2}\,c^{b-1}\prod_{j=1}^{c-1}\frac{(a-b)c+j}{c+j}\cdot\frac{\prod_{i=a-b+1}^{a-1}\prod_{j=1}^{c-1}(ic+j)}{\prod_{i=1}^{b-1}\prod_{j=1}^{c-1}(ic+j)}$$

$$\geqslant \frac{1}{2}\,c^{b-1}\,\frac{(a-b)c+1}{c+1}.$$

If $b = 1$ the right hand side equals

$$\frac{(a-1)c+1}{2(c+1)} \geqslant \frac{2(a-1)+1}{6} \geqslant \frac{a}{4}.$$

If $b \geqslant 2$ the right hand side is greater than or equal to

$$c\,\frac{ac+2}{4(c+1)} > \frac{a}{4}\cdot\frac{c^2}{c+1} \geqslant \frac{a}{3}.$$

□

Lemma 12. *We have*

$$S = \sum_{c=2}^{\infty} c\varphi(c)\binom{2c}{c}^{-1} < 7/8.$$

Proof (following J.-L. Nicolas). We have

$$S = \sum_{c=2}^{6} c\varphi(c)\binom{2c}{c}^{-1} + \sum_{c=7}^{\infty} c\varphi(c)\binom{2c}{c}^{-1} = S_1 + S_2.$$

Now

$$S_1 = \frac{5821}{6930} < 0.84.$$

Since $\varphi(c) \leqslant c-1$ and for $c \geqslant 7$

$$\frac{c(c-1)\binom{2c}{c}^{-1}}{(c+1)c\binom{2c+2}{c+1}^{-1}} \geqslant \frac{45}{16}$$

we have

$$S_2 \leqslant 7 \cdot 6 \cdot \binom{14}{7}^{-1} \cdot \frac{45}{29} < 0.02$$

and

$$S = S_1 + S_2 < 0.86 < 7/8. \qquad \square$$

Lemma 13. *For all positive integers n and k we have*

$$\sum_{d\,|\,(n,k)} \varphi(d)\binom{n/d}{k/d} \leqslant \left(1 + \frac{3.5}{n}\right)\binom{n}{k}.$$

Proof. By Lemma 11 with $a = n/d$, $b = k/d$, $c = d$, for $d > 1$ we have

$$\binom{n}{k} \geqslant \frac{n}{4d}\binom{n/d}{k/d}\binom{2d}{d},$$

hence

$$\begin{aligned}\binom{n}{k}^{-1} \sum_{d\,|\,(n,k)} \varphi(d)\binom{n/d}{k/d} &\leqslant 1 + \sum_{\substack{d\,|\,(n,k)\\ d>1}} \varphi(d)\,\frac{4d}{n}\binom{2d}{d}^{-1} \\ &< 1 + \frac{4}{n}\sum_{c\geqslant 2} c\varphi(c)\binom{2c}{c}^{-1} < 1 + \frac{3.5}{n},\end{aligned}$$

by virtue of Lemma 12. $\square$

Lemma 14. *We have for $n \geqslant 2k \geqslant 6$*

$$g^*(k,m,n) \geqslant 1 + \frac{1}{2n(n-1)}\binom{n}{k}p(k,m,n), \tag{2}$$

where

$$p(k,m,n) = k(n-k) - \frac{(n-1)(n+3.5)}{n} - \begin{cases} \dfrac{n(n+2.5)}{n-1} & \text{if } m = 1,\ n-1, \\ \dfrac{n(n-1)(n+1.5)}{(n-2)^2} & \text{if } m = 2,\ n-2, \\ \dfrac{(n+7)(m(n-m)+3.5)}{m(n-m)} & \text{if } 2 < m < n-2. \end{cases}$$

Proof. By Lemma 10, $g^*(k,m,n) = g^*(k,n-m,n)$, thus it is enough to consider $m \leqslant n/2$.

If $m = 1$, by Lemmas 10 and 13 we have

$$g^*(k,1,n) \geqslant 1 + \frac{1}{2}\binom{n-2}{k-1} - \frac{1}{2n}\left(1+\frac{3.5}{n}\right)\binom{n}{k} - \frac{1}{2(n-1)}\sum_{l=0}^{1}\left(1+\frac{3.5}{n-1}\right)\binom{n-1}{k-l}$$

and the right hand side equals the right hand side of (2).

If $m = 2$, by Lemmas 10 and 13 we have

$$\begin{aligned} g^*(k,2,n) &\geqslant 1 + \frac{1}{2}\binom{n-2}{k-1} - \frac{1}{2n}\left(1+\frac{3.5}{n}\right)\binom{n}{k} \\ &\quad - \frac{1}{4(n-2)}\sum_{l=0}^{2}\Bigg(\sum_{d\,|\,(2,l)}\binom{2/d}{l/d}\Bigg)\left(1+\frac{3.5}{n-2}\right)\binom{n-2}{k-l} \\ &\geqslant 1 + \frac{1}{2}\binom{n-2}{k-1} - \frac{1}{2n}\left(1+\frac{3.5}{n}\right)\binom{n}{k} \\ &\quad - \frac{1}{2(n-2)}\left(1+\frac{3.5}{n-2}\right)\left(\binom{n-2}{k} + \binom{n-2}{k-1} + \binom{n-2}{k-2}\right) \\ &\geqslant 1 + \frac{1}{2}\binom{n-2}{k-1} - \frac{1}{2n}\left(1+\frac{3.5}{n}\right)\binom{n}{k} - \frac{1}{2(n-2)}\left(1+\frac{3.5}{n-2}\right)\binom{n}{k} \end{aligned}$$

and the right hand side equals the right hand side of (2).

If $m \geqslant 3$, by Lemmas 10 and 13 we have

$$\begin{aligned} g^*(k,m,n) &\geqslant 1 + \frac{1}{2}\binom{n-2}{k-1} - \frac{1}{2n}\left(1+\frac{3.5}{n}\right)\binom{n}{k} - \frac{1}{2m(n-m)} \\ &\quad \times \Bigg\{\left(1+\frac{3.5}{n-m}\right)\binom{n-m}{k}\sum_{d\,|\,m}\varphi(d) \\ &\quad + \sum_{l=1}^{k-1}\left(1+\frac{3.5}{m}\right)\binom{m}{l}\left(1+\frac{3.5}{n-m}\right)\binom{n-m}{k-l} \\ &\quad + \left(1+\frac{3.5}{m}\right)\binom{m}{k}\sum_{d\,|\,n-m}\varphi(d)\Bigg\} \\ &= 1 + \frac{1}{2}\binom{n-2}{k-1} - \frac{1}{2n}\left(1+\frac{3.5}{n}\right)\binom{n}{k} - \frac{1}{2m(n-m)} \\ &\quad \times \Bigg\{\left(m-1-\frac{3.5}{m}\right)\left(1+\frac{3.5}{n-m}\right)\binom{n-m}{k} \\ &\quad + \left(1+\frac{3.5}{m}\right)\left(1+\frac{3.5}{n-m}\right)\sum_{l=0}^{k}\binom{m}{l}\binom{n-m}{k-l} \\ &\quad + \left(n-m-1-\frac{3.5}{n-m}\right)\left(1+\frac{3.5}{m}\right)\binom{m}{k}\Bigg\}. \end{aligned}$$

Now we use the identity

$$\sum_{l=0}^{k} \binom{m}{l}\binom{n-m}{k-l} = \binom{n}{k}$$

and the inequalities

$$m - 1 - \frac{3.5}{m} > 0, \qquad \binom{n-m}{k} \leqslant \frac{(n-m)(n-m-1)}{n(n-1)}\binom{n}{k},$$
$$n - m - 1 - \frac{3.5}{n-m} > 0, \qquad \binom{m}{k} \leqslant \frac{m(m-1)}{n(n-1)}\binom{n}{k}$$

and we obtain

$$\begin{aligned} g^*(k,m,n) \geqslant 1 + \frac{1}{2}\binom{n-2}{k-1} - \frac{1}{2}\binom{n}{k}\Bigg\{ & \frac{1}{n}\left(1 + \frac{3.5}{n}\right) \\ & + \left(m - 1 - \frac{3.5}{m}\right)\left(1 + \frac{3.5}{n-m}\right)\frac{(n-m)(n-m-1)}{n(n-1)} \\ & + \left(1 + \frac{3.5}{m}\right)\left(1 + \frac{3.5}{n-m}\right) \\ & + \left(n - m - 1 - \frac{3.5}{n-m}\right)\left(1 + \frac{3.5}{m}\right)\frac{m(m-1)}{n(n-1)}\Bigg\}. \end{aligned}$$

The right hand side of this inequality coincides with the right hand side of (2). □

Lemma 15. *We have* $g^*(k,m,n) \geqslant n/24$ *for all integers* n, m *and* k *satisfying* $n \geqslant 2m > 0$, $(n,m) = 1$ *and* $n \geqslant 2k \geqslant 6$ *except for* $k = 3$ *and* $\langle n, m\rangle = \langle 6, 1\rangle$ *or* $\langle 7, 1\rangle$. *Moreover,* $g^*(k,m,n) = 1$ *if and only if either* $k = 3$ *and* $\langle n, m\rangle = \langle 7, 2\rangle$, $\langle 7, 3\rangle$, $\langle 8, 1\rangle$ *or* $\langle 9, 1\rangle$, *or* $k = 4$ *and* $\langle n, m\rangle = \langle 8, 1\rangle$.

Proof. For $k = 3$, $n \leqslant 20$, for $k = 4$, $n \leqslant 13$, and for $k = 5$, $n \leqslant 12$ the lemma is proved by direct calculation of $g^*(k,m,n)$ from Lemma 10 kindly performed by J.-L. Nicolas. If $m = 1$ we have

$$p(k,1,n) = (k-2)n - k^2 - 6 - \frac{3.5}{n(n-1)} > (k-2)n - k^2 - 7.$$

We obtain $p(3,1,n) > 5$ for $n \geqslant 21$; $p(4,1,n) > 4$ for $n \geqslant 14$; $p(5,1,n) > 7$ for $n \geqslant 13$. For $k \geqslant 6$, $n \geqslant 2k$ we obtain $p(k,1,n) > k^2 - 4k - 7 \geqslant 5$.

If $m = 2$ we have

$$p(k,2,n) = (k-2)n - k^2 - 7 - \frac{9n^2 - 4n - 14}{n(n-2)^2}.$$

We obtain $p(3,2,n) > 4$ for $n \geqslant 21$; $p(4,2,n) > 4$ for $n \geqslant 14$; $p(5,2,n) > 4$ for $n \geqslant 13$; and $p(k,2,n) > k^2 - 4k - 9 \geqslant 3$ for $k \geqslant 6$, $n \geqslant 2k$.

If $m \geqslant 3$ we have

$$p(k,m,n) \geqslant (k-2)n - k^2 - \frac{32}{3} - \frac{49n + 63}{6n(n-3)}.$$

This gives $p(3, m, n) > 0.8$ for $n \geqslant 21$; $p(4, m, n) > 0.5$ for $n \geqslant 14$; $p(5, m, n) > 2$ for $n \geqslant 13$; and $p(k, m, n) > k^2 - 4k - 11.7 \geqslant 0.3$ for $k \geqslant 6, n \geqslant 2k$.

The lemma follows now from (2). □

Lemma 16. *Let* $T(x; t^r, t^s) = \prod_{i=1}^{n} (x - x_i(t))$. *In the field* $\overline{K}(t, x_1(t), x_2(t))$ *we have the factorizations*

$$t \cong \frac{\prod_{i=1}^{m-1} \mathfrak{p}_i^m \prod_{j=1}^{n-m-1} \mathfrak{q}_j^{n-m} \mathfrak{r}^{m(n-m)} \mathfrak{s}^{m(n-m)}}{\prod_{k=1}^{n-1} \mathfrak{t}_k^n},$$

$$x_1(t) = \frac{\prod_{i=1}^{m-1} \mathfrak{p}_i^{s-r} \prod_{j=1}^{n-m-1} \mathfrak{q}_j^{r} \mathfrak{r}^{(s-r)(n-m)} \mathfrak{s}^{rm}}{\prod_{k=1}^{n-1} \mathfrak{t}_k^s},$$

$$x_2(t) = \frac{\prod_{i=1}^{m-1} \mathfrak{p}_i^{s-r} \prod_{j=1}^{n-m-1} \mathfrak{q}_j^{r} \mathfrak{r}^{rm} \mathfrak{s}^{(s-r)(n-m)}}{\prod_{k=1}^{n-1} \mathfrak{t}_k^s},$$

where $\mathfrak{p}_i$, $\mathfrak{q}_j$, $\mathfrak{r}$, $\mathfrak{s}$, $\mathfrak{t}_k$ $(1 \leqslant i < m,\ 1 < j < n - m,\ 1 \leqslant k < n)$ *are distinct prime divisors. For* t_1 *defined in Lemma* 3 *the numerator of* $t - t_1$ *has* $(n-2)(n-3)$ *prime factors in the first power only, the remaining factors are double.*

Proof. By Lemma 1(a), (b) the prime divisors of the numerator or the denominator of $t - c$ are in one-to-one correspondence with the cycles of the Puiseux expansions of a generating element of $\overline{K}(t, x_1(t), x_2(t))/\overline{K}(t)$ at $t = c$ or at $t = \infty$, respectively provided the relevant conditions are satisfied. For the generating element we take $y(t) = ax_1(t) + bx_2(t)$, where $a, b \in \overline{K}$ are chosen so that for all $i \leqslant n$, $j \leqslant n$, $i \neq j$ we have either $ax_i(t) + bx_j(t) \neq ax_1(t) + bx_2(t)$ or $\langle i, j\rangle = \langle 1, 2\rangle$. By Lemma 4 for each pair $\langle i, j\rangle$ with $i \leqslant n$, $j \leqslant n$, $i \neq j$ there is an automorphism of the extension $\overline{K}(t, x_1(t), \ldots, x_n(t))/\overline{K}(t)$ taking $x_1(t)$, $x_2(t)$ into $x_i(t)$, $x_j(t)$, respectively. At $t = 0$ we obtain for $y(t)$ the expansions

$$a\zeta_{2m}^{2i+1} t^{(s-r)/m} P_{01}(\zeta_{2m}^{(2i+1)n} t^{1/m}) + b\zeta_{2m}^{2j+1} t^{(s-r)/m} P_{01}(\zeta_{2m}^{(2j+1)n} t^{1/m})$$
$$(0 \leqslant i < m,\ 0 \leqslant j < m,\ i \neq j),$$

$$a\zeta_{2m}^{2i+1} t^{(s-r)/m} P_{01}(\zeta_{2m}^{(2i+1)n} t^{1/m}) + b\zeta_{2(n-m)}^{2j+1} t^{r/(n-m)} P_{02}(\zeta_{2(n-m)}^{-(2j+1)n} t^{1/(n-m)})$$
$$(0 \leqslant i < m,\ 0 \leqslant j < n - m),$$

$$a\zeta_{2(n-m)}^{2i+1} t^{r/(n-m)} P_{02}(\zeta_{2(n-m)}^{-(2i+1)n} t^{1/(n-m)}) + b\zeta_{2m}^{2j+1} t^{(s-r)/m} P_{01}(\zeta_{2m}^{-(2j+1)n} t^{1/m})$$
$$(0 \leqslant i < n - m,\ 0 \leqslant j < m),$$

$$a\zeta_{2(n-m)}^{2i+1}t^{r/(n-m)}P_{02}(\zeta_{2(n-m)}^{-(2i+1)n}t^{1/(n-m)}) + b\zeta_{2(n-m)}^{2j+1}t^{r/(n-m)}P_{02}(\zeta_{2(n-m)}^{-(2j+1)n}t^{1/(n-m)}) \qquad (0 \leqslant i < n-m,\ 0 \leqslant j < n-m,\ i \neq j).$$

The $m(m-1)$ expansions of the first set form $m-1$ m-cycles corresponding to the divisors $\mathfrak{p}_1, \ldots, \mathfrak{p}_{m-1}$, which divide the numerators of $x_1(t), x_2(t)$ in exactly the $(s-r)$th power. The $m(n-m)$ expansions of the second set form one $m(n-m)$-cycle corresponding to the divisor $\mathfrak{r}$ which divides $x_1(t)$ in the $(s-r)(n-m)$th power and $x_2(t)$ in the rmth power.

The $m(n-m)$ expansions of the third set form one $m(n-m)$-cycle corresponding to the divisor $\mathfrak{s}$ which divides $x_1(t)$ in the rmth power and $x_2(t)$ in the $(s-r)(n-m)$th power. The $(n-m)(n-m-1)$ expansions of the fourth set form $n-m-1$ $(n-m)$-cycles corresponding to divisors $\mathfrak{q}_1, \ldots, \mathfrak{q}_{n-m-1}$ which divide the numerators of $x_1(t), x_2(t)$ in exactly rth power.

Since $x_1(t) = 0$ implies $t = 0$ we have found all factors of the numerator of $x_1(t)$ and similarly of $x_2(t)$.

At $t = \infty$ we obtain for $y(t)$ the expansions

$$a\zeta_{2n}^{2i+1}t^{s/n}P_{21}(\zeta_{2n}^{(2i+1)m}t^{-1/n}) + b\zeta_{2n}^{2j+1}t^{s/n}P_{21}(\zeta_{2n}^{(2j+1)m}t^{-1/n}) \qquad (0 \leqslant i < n,\ 0 \leqslant j < n,\ i \neq j),$$

which form $n-1$ n-cycles corresponding to the divisors $\mathfrak{t}_1, \ldots, \mathfrak{t}_{n-1}$ dividing the denominator of $x_1(t)$ and of $x_2(t)$ in exactly the sth power.

Since $x_1(t) = \infty$ implies $t = \infty$ we have found all factors of the denominator of $x_1(t)$ and similarly of $x_2(t)$.

At $t = t_1$ we obtain for $y(t)$ among others the expansions

$$aP_{1i}(t-t_1) + bP_{1j}(t-t_1) \qquad (2 \leqslant i < n,\ 2 \leqslant j < n,\ i \neq j)$$

which form $(n-2)(n-3)$ 1-cycles corresponding to $(n-2)(n-3)$ simple factors of the numerator of $t - t_1$. All the remaining expansions contain $(t-t_1)^{1/2}$. □

Lemma 17. *For all primes p,*

$$\sqrt[p]{t} \notin \overline{K}\,(t, x_1(t), \ldots, x_n(t)) = \Omega.$$

Proof. The argument used in the proof of Lemma 16 applied to the field Ω gives that the multiplicity of every prime divisor of the numerator and the denominator of t divides $m(n-m)$ and n, respectively. Since $(m, n) = 1$ we cannot have $t = \gamma^p$, $\gamma \in \Omega$. □

Lemma 18. *For every positive integer q prime to s, $q \not\equiv 0 \bmod \pi$, and every choice of q-th roots we have*

$$\left[\overline{K}\left(t, \sqrt[q]{x_1(t)}, \ldots, \sqrt[q]{x_n(t)}\right) : \overline{K}\left(t, x_1(t), \ldots, x_n(t)\right)\right] = q^n.$$

Proof. By Theorem 1 of [25] it is enough to prove that for every prime $p \mid q$,

$$\prod_{j=1}^{n} x_j^{\alpha_j} = \gamma^p, \qquad \gamma \in \Omega = \overline{K}\big(t, x_1(t), \ldots, x_n(t)\big) \tag{3}$$

implies $\alpha_j \equiv 0 \bmod p$ for all $j \leqslant n$. Assume that (3) holds, but say $\alpha_1 \not\equiv 0 \bmod p$.

If for all j we have $\alpha_j \equiv \alpha_1 \bmod p$ it follows from (3) that

$$\Big(\prod_{j=1}^{n} x_j\Big)^{\alpha_1} = \gamma'^p, \qquad \gamma' \in \Omega,$$

and since $\prod_{j=1}^{n} x_j = (-1)^n t^s$ where $s\alpha_1 \not\equiv 0 \bmod p$ we obtain $\sqrt[p]{t} \in \Omega$, contrary to Lemma 17. Therefore, there exists an $i \leqslant n$ such that $\alpha_i \not\equiv \alpha_1 \bmod p$. If $i \neq 2$, by Lemma 4 there exist automorphisms σ and τ of $\Omega/\overline{K}(t)$ such that $\sigma(x_2) = x_i, \sigma(x_i) = x_2$ and $\tau(x_1) = x_2, \tau(x_2) = x_i, \tau(x_i) = x_1$. Applying σ and τ to (3) we obtain

$$x_1^{\alpha_1} x_2^{\alpha_i} x_i^{\alpha_2} \prod_{j\neq 1,2,i}^{n} x_j^{\alpha_j} = (\gamma^\sigma)^p,$$

$$x_1^{\alpha_i} x_2^{\alpha_1} x_i^{\alpha_2} \prod_{j\neq 1,2,i}^{n} x_j^{\alpha_j} = (\gamma^\tau)^p,$$

hence on division

$$\left(\frac{x_1}{x_2}\right)^{\alpha_1-\alpha_i} = \left(\frac{\gamma^\sigma}{\gamma^\tau}\right)^p = \gamma'^p, \qquad \gamma' \in \Omega^*.$$

If $i = 2$ the same relation follows more simply on taking $\tau(x_1) = x_2, \tau(x_2) = x_1$. Since $\alpha_1 - \alpha_i \not\equiv 0 \bmod p$ we have $1 = a(\alpha_1 - \alpha_i) + bp$, $a, b \in \mathbb{Z}$, hence

$$\left(\frac{x_1}{x_2}\right) = \left(\gamma'^a \left(\frac{x_1}{x_2}\right)^b\right)^p = \delta^p, \qquad \delta \in \Omega^*. \tag{4}$$

c The extension $\overline{K}(t, x_1, x_2, \delta)/\overline{K}(t, x_1, x_2)$ is a normal subextension of $\Omega/\overline{K}(t, x_1, x_2)$ and since the latter has the symmetric Galois group, we have either $\delta \in \overline{K}(t, x_1, x_2)$ or

$$\delta \in \overline{K}\Big(t, x_1, x_2, \prod_{\substack{\mu,\nu=3\\ \nu>\mu}}^{n} (x_\nu - x_\mu)\Big).$$

Since the conjugates of δ with respect to $\overline{K}(t, x_1, x_2)$ are $\zeta_p^j \delta$, we have either $\delta \in \overline{K}(t, x_1, x_2)$ or $p = 2$ and $\delta = \varepsilon \prod_{\substack{\mu,\nu=3\\ \nu>\mu}}^{n} (x_\nu - x_\mu)$, $\varepsilon \in \overline{K}(t, x_1, x_2)$.

In the former case we compare the divisors on both sides of (4) and obtain by Lemma 16

$$\delta^p \cong \frac{\mathfrak{r}}{\mathfrak{s}},$$

a contradiction.

In the latter case we have

$$\delta = \varepsilon \prod_{\substack{\mu,\nu=1\\ \nu>\mu}}^{n} (x_\nu - x_\mu) \cdot \frac{x_1 - x_2}{\prod_{\nu>1}(x_\nu - x_1) \cdot \prod_{\nu\neq 2}(x_\nu - x_2)} = \eta \prod_{\substack{\mu,\nu=1\\ \nu>\mu}}^{n} (x_\nu - x_\mu),$$

$$\eta \in \overline{K}(t, x_1, x_2),$$

hence by (4)

$$\frac{x_1}{x_2} = \eta^2 \operatorname{disc}_x T(x; t^r, t^s) = \text{const}\, \eta^2 t^{s(n-1)-1}(t - t_1).$$

By Lemma 16 $t - t_1$ has at least one simple factor for $n > 3$, which occurs with a non-zero exponent on the right hand side, but not on the left, a contradiction. For $n = 3$ the divisor of the right hand side is a square, while that of the left hand side is not, a contradiction again. □

Lemma 19. *Let $n > 2$, $q \not\equiv 0 \bmod \pi$, $q \geqslant 2$, $y_{iq}^q = x_i(t)$ $(1 \leqslant i \leqslant n)$. Then*

$$\left[\overline{K}\left(t, \left(\sum_{i=1}^{n} y_{iq}\right)^q\right) : \overline{K}(t)\right] = q^{n-1}.$$

Proof. Suppose first that $(q, s) = 1$. By Lemmas 4 and 18 all isomorphic injections of the extension $\overline{K}(t, y_{1q}, \ldots, y_{nq})/\overline{K}(t)$ into $\overline{K(t)}/\overline{K}(t)$ are given by

$$y_{iq} \to \zeta_q^{\alpha_i} y_{\sigma(i)q} \qquad (1 \leqslant i \leqslant n) \tag{5}$$

where σ is a permutation of $\{1, 2, \ldots, n\}$ and

$$[\alpha_1, \ldots, \alpha_n] \in (\mathbb{Z}/q\mathbb{Z})^n. \tag{6}$$

We shall show that there are exactly q^{n-1} distinct images of $\left(\sum_{i=1}^{n} y_{iq}\right)^q$ under transformations (5). Indeed if we apply (5) with $\sigma(i) = i$ to $\left(\sum_{i=1}^{n} y_{iq}\right)^q$ we obtain

$$\left(\sum_{i=1}^{n} \zeta_q^{\alpha_i} y_{iq}\right)^q.$$

If this were equal to $\left(\sum_{i=1}^{n} \zeta_q^{\beta_i} y_{iq}\right)^q$, for a vector $[\beta_1, \ldots, \beta_n] \in (\mathbb{Z}/q\mathbb{Z})^n$ with $\beta_j - \beta_1 \neq \alpha_j - \alpha_1$ for a certain j, we should obtain

$$y_{1q} \in \overline{K}(y_{2q}, \ldots, y_{nq}) \quad \text{or} \quad y_{jq} \in \overline{K}(y_{1q}, \ldots, y_{j-1,q}, y_{j+1,q}, \ldots, y_{nq}),$$

contrary to Lemma 18. Thus the number of distinct images is at least equal to the number of vectors satisfying (6) with $\alpha_1 = 0$, thus to q^{n-1}. On the other hand, $\left(\sum_{i=1}^{n} y_{iq}\right)^q$ is invariant under transformations (5) with $\alpha_1 = \alpha_2 = \ldots = \alpha_n$, which form a group, hence the number in question does not exceed q^{n-1}.

Suppose now that $(q, s) \neq 1$. Taking an integer solution $\sigma = s_1, \varrho = r_1$ of the equation $\sigma(n-m) - \varrho n = 1$ that satisfies $(q, s_1) = 1$ we have

$$T(x; t^r, t^s) = t^{s-s_1} T\left(\frac{x}{t^{(s-s_1)/n}}; t^{r_1}, t^{s_1}\right),$$

hence if $T(x; t^{r_1}, t^{s_1}) = \prod_{i=1}^{n} (x - \overline{x}_i(t))$ one can renumber the $\overline{x}_i(t)$ so that

$$\left(t^{(s_1-s)/nq} y_{iq}\right)^q = \overline{x}_i(t).$$

Therefore, by the already proved case of the lemma

$$\left[\overline{K}\left(t, \left(\sum_{i=1}^{n} t^{(s_1-s)/nq} y_{iq}\right)^q\right) : \overline{K}(t)\right] = q^{n-1}$$

and the lemma follows in full generality. □

Definition 2. Let $q \not\equiv 0 \bmod \pi$ and $y_{iq}^q = x_i(t)$, where $x_i(t)$ are defined in Lemma 16. We set

$$M(m, n, q) = K\left(t, \left(\sum_{i=1}^{n} y_{iq}\right)^q\right), \quad M_*(m, n, q) = \overline{K}\left(t, \left(\sum_{i=1}^{n} y_{iq}\right)^q\right).$$

Remark. By Lemma 19 and the final argument in its proof $M(m, n, q)$ and $M_*(m, n, q)$ are determined by $m,\ n,\ q$ up to an isomorphism which fixes $K(t)$ and $\overline{K}(t)$, respectively.

Lemma 20. *For $n > 2$ and $(q, 2) = 1$ or $(q, s) = 1$ the numerator of $t - t_1$ has in $M_*(m, n, q)$ $(q^{n-1} - q^{n-2})/2$ factors in the second power.*

Proof. Let us fix

$$\overline{y}_{1q} = \left(\xi_1 + (t - t_1)^{1/2} P_{11}((t - t_1)^{1/2})\right)^{1/q},$$
$$\overline{y}_{2q} = \left(\xi_1 - (t - t_1)^{1/2} P_{11}(-(t - t_1)^{1/2})\right)^{1/q},$$

so that

$$\overline{y}_{1q} + \overline{y}_{2q} \in \overline{K}\left((t - t_1)\right), \tag{7}$$

$$(\overline{y}_{1q} - \overline{y}_{2q})(t - t_1)^{1/2} \in \overline{K}\left((t - t_1)\right) \tag{8}$$

and

$$\overline{y}_{jq} = \left(P_{i,j-1}(t - t_1)\right)^{1/q} \in \overline{K}\left((t - t_1)\right) \qquad (2 < j \leqslant n) \tag{9}$$

in an arbitrary way. Using Lemma 3 we obtain for $\left(\sum_{i=1}^{n} y_{iq}\right)^q$ the following Puiseux expansions at $t = t_1$:

$$\left(\overline{y}_{1q} + \zeta_q^{i_2} \overline{y}_{2q} + \sum_{j=3}^{n} \zeta_q^{i_j} \overline{y}_{jq}\right)^q, \qquad [i_2, \ldots, i_n] \in (\mathbb{Z}/q\mathbb{Z})^{n-1}.$$

If such an expansion belongs to $\overline{K}\big((t-t_1)\big)$ then either

$$\overline{y}_{1q} + \zeta_q^{i_2}\overline{y}_{2q} + \sum_{j=3}^{n} \zeta_q^{i_j}\overline{y}_{jq} \in \overline{K}\big((t-t_1)\big)$$

or

$$2 \,|\, q \quad \text{and} \quad \Big(\overline{y}_{1q} + \zeta_q^{i_2}\overline{y}_{2q} + \sum_{j=3}^{n} \zeta_q^{i_j}\overline{y}_{jq}\Big)(t-t_1)^{-1/2} \in \overline{K}\big((t-t_1)\big).$$

In the first case, by (7) and (9),

$$(1-\zeta_q^{i_2})\overline{y}_{1q} \in \overline{K}\big((t-t_1)\big)$$

and since $P_{11}(0) \neq 0$, $i_2 = 0$.

In the second case, by (8),

$$\left(\frac{1+\zeta_q^{i_2}}{2}(\overline{y}_{1q}+\overline{y}_{2q}) + \sum_{j=3}^{n} \zeta_q^{i_j}\overline{y}_{jq}\right)(t-t_1)^{-1/2} \in \overline{K}\big((t-t_1)\big)$$

and since

$$\frac{1+\zeta_q^{i_2}}{2}(\overline{y}_{1q}+\overline{y}_{2q}) + \sum_{j=3}^{n} \zeta_q^{i_j}\overline{y}_{jq} \in \overline{K}\big((t-t_1)\big)$$

by (7) and (9), we obtain

$$\frac{1+\zeta_q^{i_2}}{2}(\overline{y}_{1q}+\overline{y}_{2q}) + \sum_{j=3}^{n} \zeta_q^{i_j}\overline{y}_{jq} = 0,$$

which contradicts Lemma 18 unless $(s,q) > 1$.

Therefore if $(q,2)=1$ or $(q,s)=1$ we obtain $q^{n-1}-q^{n-2}$ expansions for $\big(\sum_{i=1}^{n} y_{iq}\big)^q$ belonging to $\overline{K}\big(((t-t_1)^{1/2})\big)\setminus\overline{K}\big((t-t_1)\big)$, which correspond to $(q^{n-1}-q^{n-2})/2$ distinct prime divisors of the numerator of $t-t_1$ in $M_*(m,n,q)$. □

Lemma 21. *For every positive integer l the number of vectors $[i_1,\dots,i_l] \in (\mathbb{Z}/q\mathbb{Z})^l$ such that*

$$\sum_{j=1}^{l} \zeta_q^{i_j}\zeta_{ql}^{j-1} = 0 \tag{10}$$

does not exceed $q^{l-\varphi(lq)/\varphi(q)}$.

Proof. We have

$$\big[\mathbb{Q}(\zeta_{ql}) : \mathbb{Q}(\zeta_q)\big] = \frac{\varphi(lq)}{\varphi(q)} = \varrho,$$

hence ζ_{lq} has ρ conjugates over $\mathbb{Q}(\zeta_q)$. Let them be $\zeta_{lq}^{r_k}$ $(k \leqslant \rho)$. It follows from (10) that

$$\sum_{j=1}^{l} \zeta_q^{i_j} \zeta_{ql}^{(j-1)r_k} = 0$$

and since

$$\det\left(\zeta_{ql}^{(j-1)r_k}\right)_{j,k\leqslant\rho} = \prod_{\substack{\mu,\nu=1\\ \nu>\mu}}^{\rho} \left(\zeta_{ql}^{r_\nu} - \zeta_{ql}^{r_\mu}\right) \neq 0$$

$\zeta_q^{i_j}$ $(j \leqslant \rho)$ are determined by $\zeta_q^{i_j}$ $(\rho < j \leqslant l)$, which gives the lemma. □

Lemma 22. *The denominator of t in $M_*(m, n, q)$ has at most*

$$q^{n-1}\Big(\frac{1}{n} + \frac{n-1}{nq^{\varphi(nq)/\varphi(q)}}\Big)$$

distinct prime divisors.

Proof. By Lemma 1(b) the prime divisors of the denominator of t correspond to the cycles of the Puiseux expansions of $\big(\sum_{i=1}^{n} y_{iq}\big)^q$ at $t = \infty$, provided the relevant condition is satisfied. By Lemma 3 we obtain for $\big(\sum_{i=1}^{n} y_{iq}\big)^q$ the following expansions at $t = \infty$:

$$\Big(\sum_{j=1}^{n} \zeta_q^{i_j} \zeta_{2qn}^{2j-1} t^{s/qn} P_{21}(\zeta_n^{(2j-1)m} t^{-1/n})^{1/q}\Big)^q \tag{11}$$

where $[i_1, \ldots, i_n] \in (\mathbb{Z}/q\mathbb{Z})^n$, $i_1 = 0$. Note that $qn \not\equiv 0 \bmod \pi$.

Let S be the set of vectors $[i_2, \ldots, i_n] \in (\mathbb{Z}/q\mathbb{Z})^{n-1}$ such that

$$1 + \sum_{j=2}^{n} \zeta_q^{i_j} \zeta_{qn}^{j-1} = 0.$$

By Lemma 21 with $l = n$,

$$\operatorname{card} S \leqslant q^{n-\varphi(qn)/\varphi(q)-1}. \tag{12}$$

If $[i_2, \ldots, i_n] \notin S$ the coefficient of $t^{s/n}$ in the expansion (11) equals

$$\zeta_{2n}\Big(1 + \sum_{j=2}^{n} \zeta_q^{i_j} \zeta_{qn}^{j-1}\Big)^q P_{21}(0) \neq 0,$$

hence we obtain an n-cycle. The number of cycles thus obtained is $\frac{1}{n}(q^{n-1} - \operatorname{card} S)$. The number of the remaining cycles does not exceed card S. Therefore the total number of cycles does not exceed

$$\frac{1}{n}(q^{n-1} - \operatorname{card} S) + \operatorname{card} S = \frac{q^{n-1}}{n} + \left(1 - \frac{1}{n}\right)\operatorname{card} S \leqslant \frac{q^{n-1}}{n}\left(1 + \frac{n-1}{q^{\varphi(qn)/\varphi(q)}}\right)$$

by (12). □

Lemma 23. *The numerator of t in $M_*(m, n, q)$ has at most*

$$\frac{q^{n-2}}{m(n-m)}\left(1+\frac{m-1}{q^{\varphi(mq)/\varphi(q)}}\right)\left(1+\frac{n-m-1}{q^{\varphi((n-m)q)/\varphi(q)}}\right)$$

distinct prime divisors.

Proof. By Lemma 1(a) the prime divisors of the numerator of t correspond to the cycles of the Puiseux expansions of $\big(\sum_{i=1}^{n} y_{iq}\big)^q$ at $t=0$, provided the relevant condition is satisfied. By Lemma 3 we obtain the following expansions

$$\Big(\sum_{j=1}^{m} \zeta_q^{i_j}\zeta_{2mq}^{2j-1} t^{(s-r)/qm} P_{01}(\zeta_{2m}^{(2j-1)n} t^{1/m})^{1/q} + \sum_{j=m+1}^{n} \zeta_q^{i_j}\zeta_{2(n-m)q}^{2j-1} t^{r/q(n-m)} P_{02}(\zeta_{2(n-m)}^{-(2j-1)n} t^{1/n-m})^{1/q}\Big)^q, \tag{13}$$

where $[i_1, \dots, i_n] \in (\mathbb{Z}/q\mathbb{Z})^n$, $i_1 = 0$. Note that $qm(n-m) \not\equiv 0 \bmod \pi$.

Let S be the set of vectors $[i_2, \dots, i_m] \in (\mathbb{Z}/q\mathbb{Z})^{m-1}$ such that

$$1 + \sum_{j=2}^{m} \zeta_q^{i_j}\zeta_{qm}^{j-1} = 0$$

and T the set of vectors $[i_{m+1}, \dots, i_n] \in (\mathbb{Z}/q\mathbb{Z})^{n-m}$ such that

$$\sum_{j=m+1}^{n} \zeta_q^{i_j}\zeta_{q(n-m)}^{j-1} = 0.$$

By Lemma 21,

$$\operatorname{card} S \leqslant q^{m-\varphi(qm)/\varphi(q)-1}, \qquad \operatorname{card} T \leqslant q^{n-m-\varphi(q(n-m))/\varphi(q)}.$$

If $[i_2, \dots, i_m] \notin S$ and $[i_{m+1}, \dots, i_n] \notin T$ the least two powers of t occurring with non-zero coefficients in the (outer) parentheses in (13) are

$$t^{(s-r)/qm} \quad \text{and} \quad t^{r/q(n-m)}.$$

Hence the expansion (13) contains with non-zero coefficients

$$t^{(s-r)/qm+(q-s)r/q(n-m)} \quad \text{and} \quad t^{(q-1)(s-r)/qm+r/q(n-m)}.$$

The least common denominator of the two exponents is $qm(n-m)$, hence we obtain

$$\frac{(q^{m-1} - \operatorname{card} S)(q^{n-m} - \operatorname{card} T)}{qm(n-m)}$$

$qm(n-m)$-cycles.

If $[i_2, \dots, i_m] \notin S$ and $[i_{m+1}, \dots, i_n] \in T$ the least powers of t occurring with non-zero coefficients in the parentheses of (13) are

$$t^{(s-r)/qm}, \quad t^{(s-r)/qm+\mu/m}, \quad \text{and} \quad t^{r/q(n-m)+\nu/(n-m)}$$

for some positive integers $\mu \in M$ (M may be empty) and a positive integer ν satisfying

$$\frac{s-r}{qm} + \frac{\mu}{m} < \frac{r}{q(n-m)} + \frac{\nu}{n-m} \qquad (\mu \in M).$$

Hence the expansion (13) contains with non-zero coefficients

$$t^{(s-r)/m} \quad \text{and} \quad t^{(q-1)(s-r)/qm+r/q(n-m)+\nu/(n-m)}.$$

c Indeed, if we had for some nonnegative integers a_μ ($\mu \in M \cup \{0\}$)

$$\sum_{\mu\in M\cup\{0\}} a_\mu = q, \qquad \sum_{\mu\in M\cup\{0\}} a_\mu\Big(\frac{s-r}{qm} + \frac{\mu}{m}\Big) = \frac{(q-1)(s-r)}{qm} + \frac{r}{q(n-m)} + \frac{\nu}{n-m},$$

it would follow from the second equation

$$(n-m)(s-r)\sum_{\mu\in M\cup\{0\}} a_\mu \equiv -(n-m)(s-r) + rm \equiv -1 \bmod q,$$

contrary to the first equation.

The least common denominator of the two exponents is divisible by

$$\left[m, \frac{mq}{(m, q-1)}\right] = \frac{m^2 q}{(m^2, m(q-1), mq)} = mq,$$

hence we obtain at most

$$\frac{(q^m - \operatorname{card} S)\operatorname{card} T}{qm}$$

qm-cycles.

If $[i_2, \dots, i_m] \in S$ and $[i_{m+1}, \dots, i_n] \notin T$ the least powers of t occurring with non-zero coefficients in the parentheses of (13) are

$$t^{(s-r)/qm+\mu/m}, \quad t^{r/q(n-m)} \quad \text{and} \quad t^{r/q(n-m)+\nu/(n-m)}$$

for a positive integer μ and some positive integers $\nu \in N$ (N may be empty), satisfying

$$\frac{r}{q(n-m)} + \frac{\nu}{n-m} < \frac{s-r}{qm} + \frac{\mu}{m} \qquad (\nu \in N).$$

c By an argument similar to the one above the expansion (13) contains with non-zero coefficients

$$t^{r/(n-m)} \quad \text{and} \quad t^{(q-1)r/q(n-m)+(s-r)/qm}.$$

The least common denominator of the two exponents is divisible by

$$\left[n-m, \frac{(n-m)q}{(n-m, q-1)}\right] = \frac{(n-m)^2 q}{\big((n-m)^2,\ (n-m)(q-1),\ (n-m)q\big)} = (n-m)q,$$

hence we obtain at most

$$\frac{\operatorname{card} S(q^{n-m} - \operatorname{card} T)}{q(n-m)}$$

$q(n-m)$-cycles.

Finally if $[i_2, \dots, i_m] \in S$ and $[i_{m+1}, \dots, i_n] \in T$ the least powers of t occurring in the parentheses in (13) with non-zero coefficients are either

$$t^{(s-r)/qm+\mu/m} \quad (\mu \in M), \qquad t^{r/q(n-m)+\nu/(n-m)}$$

or

$$t^{(s-r)/qm+\mu/m}, \qquad t^{r/q(n-m)+\nu/(n-m)} \quad (\nu \in N),$$

where the sets M and N are non-empty and

$$\frac{s-r}{qm} + \frac{\mu}{m} < \frac{r}{q(n-m)} + \frac{\nu}{n-m} \qquad (\mu \in M)$$

or

$$\frac{r}{q(n-m)} + \frac{\nu}{n-m} < \frac{s-r}{qm} + \frac{\mu}{m} \qquad (\nu \in N),$$

respectively. In view of symmetry it suffices to consider the first case. Then, by an argument
c similar to the one above, the expansion (13) contains with a non-zero coefficient

$$t^{(q-1)(s-r)/qm+(q-1)\mu/m+\nu/q(n-m)+\nu/m}.$$

Since the exponent in its reduced form has q in the denominator we obtain at most

$$\frac{\operatorname{card} S \operatorname{card} T}{q}$$

q-cycles. Therefore the total number of distinct cycles does not exceed

$$\begin{aligned}
&\frac{(q^{m-1} - \operatorname{card} S)(q^{n-m} - \operatorname{card} T)}{qm(n-m)} + \frac{(q^{m-1} - \operatorname{card} S)\operatorname{card} T}{qm} \\
&\qquad + \frac{\operatorname{card} S(q^{n-m} - \operatorname{card} T)}{q(n-m)} + \frac{\operatorname{card} S \cdot \operatorname{card} T}{q} \\
&= \frac{q^{n-1}}{qm(n-m)} + \operatorname{card} S \left(\frac{q^{n-m}}{q(n-m)} - \frac{q^{n-m}}{qm(n-m)} \right) \\
&\qquad + \operatorname{card} T \left(\frac{q^{m-1}}{qm} - \frac{q^{m-1}}{qm(n-m)} \right) \\
&\qquad + \operatorname{card} S \operatorname{card} T \left(\frac{1}{qm(n-m)} - \frac{1}{qm} - \frac{1}{q(n-m)} + \frac{1}{q} \right).
\end{aligned}$$

Since the coefficients are non-negative we can apply Lemma 21 and obtain the desired estimate for the number of distinct cycles. □

Lemma 24. *For all positive integers l and q with $q \geqslant 2$ we have*

$$q^{\varphi(ql)/\varphi(q)} \geqslant q(l-1).$$

Proof (following J.-L. Nicolas). We observe first that

$$\varphi(l) \geqslant \frac{l \log 2}{\log 2l}.$$

Indeed, if l has k distinct prime factors $p_1, \dots, p_k$ we have $l \geqslant 2^k$, and so $k \leqslant \log l / \log 2$. Hence

$$\frac{\varphi(l)}{l} = \prod_{i=1}^{k}\Big(1 - \frac{1}{p_i}\Big) \geqslant \prod_{i=1}^{k}\Big(1 - \frac{1}{i+1}\Big) = \frac{1}{k+1} \geqslant \frac{\log 2}{\log 2l}\,.$$

Suppose now that

$$q^{\varphi(ql)/\varphi(q)} < q(l-1).$$

Since $\varphi(ql) \geqslant \varphi(q)\varphi(l)$ we obtain

$$2^{\varphi(l)-1} \leqslant q^{\varphi(l)-1} < l - 1$$

and thus

$$\frac{l \log 2}{\log 2l} \leqslant \varphi(l) < \frac{\log(l-1)}{\log 2} + 1 < \frac{\log 2l}{\log 2}\,.$$

However, for all $x > 0$, $\log x = 4 \log \sqrt[4]{x} \leqslant (4/e)\sqrt[4]{x}$. Hence

$$l < \Big(\frac{\log 2l}{\log 2}\Big)^2 \leqslant \Big(\frac{4}{e \log 2}\Big)^2 \sqrt{2l},$$

and thus

$$l < 2\Big(\frac{4}{e \log 2}\Big)^4 < 41.$$

Since $l > 2$, $\varphi(l) > 1$ and

$$q < (l-1)^{1/(\varphi(l)-1)}$$

we find that either $l \in \{4, 6, 10, 12\}$, $q = 2$ or $l = 6$, $q \in \{3, 4\}$. In each of the six cases we have

$$q^{\varphi(ql)/\varphi(q)} \geqslant q(l-1),$$

which proves the lemma. □

Lemma 25. *For all positive integers m, n and q where $n > 2m$, $(m, n) = 1$, $qnm(n-m) \not\equiv 0 \bmod \pi$ and $q \geqslant 2$ the genus $g_*(m, n, q)$ of $M_*(m, n, q)$ is greater than $nq/24$ unless*

$$\langle q, n, m\rangle \in \{\langle 2,3,1\rangle,\ \langle 2,4,1\rangle,\ \langle 2,5,1\rangle,\ \langle 2,5,2\rangle,\ \langle 2,6,1\rangle,\ \langle 3,3,1\rangle,\ \langle 3,4,1\rangle,\ \langle 4,3,1\rangle,\ \langle 5,3,1\rangle\}, \tag{14}$$

and is greater than 1 *unless* (14) *holds or*

$$\langle q, n, m\rangle \in \{\langle 2,7,1\rangle,\ \langle 6,3,1\rangle,\ \langle 7,3,1\rangle\}. \tag{15}$$

If (14) *or* (15) *holds and $\langle q, n, m\rangle \neq \langle 6, 3, 1\rangle$ we have $g_*(m, n, q) = 0$ or* 1, *respectively.*

Proof. By Lemma 2(a) and by Lemmas 21–23 together with Remark after Definition 2 we

have

$$(16)\quad g_*(m,n,q) \geqslant 1 + \frac{q^{n-2}}{2}\Bigg(\frac{q-1}{2} - \frac{q}{n}\Big(1 + \frac{n-1}{q^{\varphi(qn)/\varphi(q)}}\Big) - \frac{1}{m(n-m)}\Big(1 + \frac{m-1}{q^{\varphi(qm)/\varphi(q)}}\Big)\Big(1 + \frac{n-m-1}{q^{\varphi(q(n-m))/\varphi(q)}}\Big)\Bigg).$$

Hence by Lemma 24,

$$g_*(m,n,q) \geqslant 1 + \frac{q^{n-2}}{2}\,\gamma(q,n,m),$$

where

$$\gamma(q,n,m) = \begin{cases} \dfrac{q-1}{2} - \dfrac{q+1}{n} - \dfrac{1}{n-1}\left(1 + \dfrac{1}{q}\right) & \text{if } m = 1, \\ \dfrac{q-1}{2} - \dfrac{q+1}{n} - \dfrac{1}{m(n-m)}\left(1 + \dfrac{1}{q}\right)^2 & \text{otherwise.} \end{cases}$$

It is easy to check using (16) that the lemma holds if

$$(17)\quad \langle q,n,m\rangle \in \{\langle 2,7,2\rangle,\ \langle 2,7,3\rangle,\ \langle 2,8,1\rangle,\ \langle 2,8,3\rangle,\ \langle 2,9,1\rangle,\ \langle 3,5,1\rangle, \langle 3,5,2\rangle,\ \langle 4,4,1\rangle,\ \langle 5,4,1\rangle,\ \langle 8,3,1\rangle\}.$$

If $\langle q,n,m\rangle$ satisfies neither (14) nor (15) nor (17) we have one of the following cases:

$$q = 2,\ m = 1,\ n \geqslant 10,\ \gamma(q,n,m) \geqslant 1/30,\quad g_*(m,n,q) \geqslant 1 + \frac{2^{n-2}}{60} > \frac{n}{12};$$

$$q = 2,\ m \geqslant 2,\ n \geqslant 9,\ \gamma(q,n,m) \geqslant 1/168,\quad g_*(m,n,q) \geqslant 1 + \frac{2^{n-2}}{336} > \frac{n}{12};$$

$$q = 3,\ m = 1,\ n \geqslant 6,\ \gamma(q,n,m) \geqslant 1/15,\quad g_*(m,n,q) \geqslant 1 + \frac{2^{n-2}}{30} > \frac{n}{8};$$

$$q = 3,\ m \neq 2,\ n \geqslant 7,\ \gamma(q,n,m) \geqslant 1/4,\quad g_*(m,n,q) \geqslant 1 + \frac{2^{n-2}}{8} > \frac{n}{8};$$

$$q \in \{4,5\},\ n \geqslant 5,\ \gamma(q,n,m) \geqslant 1/5,\quad g_*(m,n,q) \geqslant 1 + \frac{2^{n-2}}{10} > \frac{5n}{24};$$

$$q \in \{6, 7, 8\},\ n \geqslant 4,\ \gamma(q, n, m) \geqslant 1/3\,,$$
$$g_*(m, n, q) \geqslant 1 + \frac{2^{n-2}}{6} > \frac{n}{3}\,;$$
$$q \geqslant 9,\ n \geqslant 3,\ \gamma(q, n, m) = (q^2 - 8q - 3)/6q\,,$$
$$g_*(m, n, q) \geqslant 1 + \frac{q^{n-3}}{12}(q^2 - 8q - 3) > \frac{qn}{24}\,.$$

The last assertion of the lemma is proved by a direct use of the Lemma 2(a). □

Lemma 26. *Let $n \geqslant 2m$ and $A, B \in K(\boldsymbol{y})^*$, $A^{-n}B^{n-m} \notin K$. Then $x^n + Ax^m + B$ is reducible over $K(\boldsymbol{y})$ if and only if one of the following cases holds*:

(18) *$x^{n_1} + Ax^{m_1} + B$ has a proper linear or quadratic factor over $K(\boldsymbol{y})$.*

(19) *There exists an integer l such that*

$$\left\langle \frac{n}{l}, \frac{m}{l} \right\rangle := \langle \nu, \mu \rangle \in S_0 := \bigcup_{p \text{ prime}} \{\langle 2p, p\rangle\} \cup \{\langle 6, 1\rangle,\ \langle 6, 2\rangle,\ \langle 7, 1\rangle,$$
$$\langle 8, 2\rangle,\ \langle 8, 4\rangle,\ \langle 9, 3\rangle,\ \langle 10, 2\rangle,\ \langle 10, 4\rangle,\ \langle 12, 2\rangle,\ \langle 12, 3\rangle,\ \langle 12, 4\rangle,\ \langle 15, 5\rangle\}$$

and $x^\nu + Ax^\mu + B$ is reducible over $K(\boldsymbol{y})$.

Proof. The sufficiency is obvious. We proceed to prove the necessity.

If $x^n + Ax^m + B$ is reducible over $K(\boldsymbol{y})$ then by Capelli's lemma (see e.g. [18], p. 662, or [26], p. 89) either

(20) $$x^{n_1} + Ax^{m_1} + B \text{ is reducible over } K(\boldsymbol{y})$$

or

(21) $x^{(m,n)} - \xi$ is reducible over $K(\boldsymbol{y}, \xi)$, where ξ is a zero of $x^{n_1} + Ax^{m_1} + B$.

In the former case either (18) holds or $x^{n_1} + Ax^{m_1} + B$ has a factor of degree k, where $n \geqslant 2k \geqslant 6$. In this case let us choose non-negative integers r and s such that

$$s(n_1 - m_1) - rn_1 = 1.$$

We have

(22) $$A^{-n_1 s}B^{n_1 r}(x^{n_1} + Ax^{m_1} + B)$$
$$= (A^{-s}B^r x)^{n_1} + (A^{-n_1}B^{n_1 - m_1})^r (A^{-s}B^r x)^{m_1} + (A^{-n_1}B^{n_1-m_1})^s,$$

hence $x^{n_1} + (A^{-n_1}B^{n_1-m_1})^r x^{m_1} + (A^{-n_1}B^{n_1-m_1})^s$ also has a factor of degree k over $K(\boldsymbol{y})$.

Therefore the field $L^*(k, m_1, n_1)$ defined in Definition 1 is a rational function field and by Lemma 2(b), $g^*(k, m_1, n_1) = 0$. It follows by Lemma 15 that $k = 3$ and $\langle n_1, m_1\rangle = \langle 6, 1\rangle$ or $\langle 7, 1\rangle$, hence (19) holds with $l = (m, n)$ and $\langle \nu, \mu\rangle = \langle 6, 1\rangle$ or $\langle 7, 1\rangle$.

Assume now that we have (21), but not (20). It follows by Capelli's theorem that either

(23) $$\xi = \eta^p, \qquad \text{where } p \text{ is a prime, } p \mid (m, n),\ \eta \in K(\boldsymbol{y}, \xi)$$

or

(24) $$\xi = -4\eta^4, \qquad \text{where } 4 \mid (m, n),\ \eta \in K(\boldsymbol{y}, \xi).$$

If (23) or (24) holds then $x^{pn_1} + Ax^{pm_1} + B$ or $x^{4n_1} + Ax^{4m_1} + B$, respectively, is reducible over $K(\boldsymbol{y})$. Let

$$x^{n_1} + t^r x^{m_1} + t^s = \prod_{i=1}^{n_1}(x - x_i), \qquad y_{iq}^q = x_i.$$

It follows from (22) that if $t = A^{-n_1}B^{n_1-m_1}$ one can take

$$\begin{aligned} &q = p, && y_{iq} = (A^{-s}B^r)^{1/p}\eta_i && \text{if (23) holds,}\\ &q = 4, && y_{iq} = (A^{-s}B^r)^{1/4}(1+\zeta_4)\eta_i && \text{if (24) holds,}\end{aligned}$$

where η_i are the conjugates of η over $K(\boldsymbol{y})$. Hence the field $M_*(m_1, n_1, q) = \overline{K}(t, (y_{1q} + \ldots + y_{n_1q})^q)$ is parameterized as follows:

$$t = A^{-n_1}B^{n_1-m_1},$$

$$(y_{1q} + \ldots + y_{n_1q})^q = \begin{cases} A^{-s}B^r(\eta_1 + \ldots + \eta_{n_1})^p & \text{if (23) holds,}\\ -4A^{-s}B^r(\eta_1 + \ldots + \eta_{n_1})^4 & \text{if (24) holds.}\end{cases}$$

It follows by Lemma 2(b) that $g_*(m_1, n_1, q) = 0$ and by Lemma 25 either $\langle n_1, m_1\rangle = \langle 2, 1\rangle$ or

$$\langle q, n_1, m_1\rangle \in \{\langle 2,3,1\rangle,\ \langle 2,4,1\rangle,\ \langle 2,5,1\rangle,\ \langle 2,5,2\rangle,\ \langle 2,6,1\rangle,\ \langle 3,3,1\rangle,\ \langle 3,4,1\rangle,\ \langle 4,3,1\rangle,\ \langle 5,3,1\rangle\}.$$

In the former case (19) holds, with $\langle \nu, \mu\rangle = \langle 2p, p\rangle$, $l = (m, n)/p$ or $\langle \nu, \mu\rangle = \langle 8, 4\rangle$, $l = (m, n)/4$. In the latter case (19) holds with $\langle \nu, \mu\rangle = \langle n_1 q, m_1 q\rangle$, $l = (m, n)/q$. □

Lemma 27. *Let $n > 2m$, L be a finite separable extension of $K(y_1)$ with $\overline{K}L$ of genus $g > 0$, and $A,\ B \in L^*$, $A^{-n}B^{n-m} \notin \overline{K}$. The trinomial $x^n + Ax^m + B$ is reducible over L if and only if either*

(25) *$x^{n_1} + Ax^{m_1} + B$ has a proper linear or quadratic factor over L*

or there exists an integer l such that

(26) $$\left\langle \frac{n}{l}, \frac{m}{l}\right\rangle := \langle \nu, \mu\rangle \in \mathbb{Z}^2,\ \ \nu < 24g \ \text{ and } x^\nu + Ax^\mu + B \text{ is reducible over } L.$$

If $g = 1$ the latter condition can be made more precise as follows: there exists an integer l such that

(27) $$\left\langle \frac{n}{l}, \frac{m}{l}\right\rangle := \langle \nu, \mu\rangle \in S_0 \cup S_1,$$

$x^\nu + Ax^\mu + B$ is reducible over L and for $\langle \nu, \mu\rangle = \langle 9, 1\rangle$ it has a cubic factor over L.

Proof. The sufficiency of the condition is obvious. The proof of the necessity is similar to that of Lemma 26.

If $x^n + Ax^m + B$ is reducible over L then either

(28) $$x^{n_1} + Ax^{m_1} + B \text{ is reducible over } L$$

or

(29) $x^{(m,n)} - \xi$ is reducible over $L(\xi)$, where ξ is a zero of $x^{n_1} + Ax^{m_1} + B$.

In the former case either (25) holds or $x^{n_1}+Ax^{m_1}+B$ has a factor of degree k, where $n \geqslant 2k \geqslant 6$. In this case we infer from (22) that $x^{n_1} + (A^{-n_1}B^{n_1-m_1})^r x^{m_1} + (A^{-n_1}B^{n_1-m_1})^s$ has a factor of degree k over L. Therefore the field $L^*(k, m_1, n_1)$ defined in Definition 1 is isomorphic to a subfield of $\overline{K}L$ and by Lemma 2(c), $g^*(k, m_1, n_1) \leqslant g$.

It follows by Lemma 15 that $n_1 < 24g$ and if $g = 1$ then $\langle n_1, m_1\rangle \in S_0 \cup S_1$ with the proviso that for $\langle n_1, m_1\rangle = \langle 9, 1\rangle$ we have $k = 3$, hence (26) and (27) hold with $l = (m, n)$ and $\langle \nu, \mu\rangle = \langle 6, 1\rangle$, $\langle 7, 1\rangle$, $\langle 8, 1\rangle$ or $\langle 9, 1\rangle$.

Assume now that we have (29), but not (28).

Then in the same way as in the proof of Lemma 26 we infer that for a suitable $q \mid (m, n)$, $q = 4$ or a prime, $x^{n_1 q} + Ax^{m_1 q} + B$ is reducible over L and the field $M_*(m_1, n_1, q)$ is isomorphic to a subfield of $\overline{K}L$. Hence by Lemma 2(c) we have $g_*(m_1, n_1, q) \leqslant g$. Since $\langle n_1, m_1\rangle \neq \langle 2, 1\rangle$ it follows by Lemma 25 that either $\langle q, n_1, m_1\rangle \in \{\langle 2, 3, 1\rangle, \langle 2, 4, 1\rangle, \langle 2, 5, 1\rangle, \langle 2, 6, 1\rangle, \langle 3, 3, 1\rangle, \langle 3, 4, 1\rangle, \langle 4, 3, 1\rangle, \langle 5, 3, 1\rangle\}$ or $n_1 q < 24g$. Moreover if $g = 1$ the last inequality can be replaced by $\langle q, n_1, m_1\rangle \in \{\langle 2, 7, 1\rangle, \langle 6, 3, 1\rangle, \langle 7, 3, 1\rangle\}$ and the case $\langle q, n_1, m_1\rangle = \langle 6, 3, 1\rangle$ is impossible because of the restriction on q. Thus (26) and (27) follow with $l = (m, n)/q$, $\langle \nu, \mu\rangle = \langle n_1 q, m_1 q\rangle$. □

3. Determination of the content of Table 1 (Lemmas 28 to 40)

Lemma 28. *Let K be any field of characteristic different from 2, and $A, B \in K^*$. The trinomial $x^{2m} + Ax^m + B$ is reducible over K if and only if either $\sqrt{A^2 - 4B}$ belongs to K or for some prime $p \mid m$,*

(30) $$A = u^p A_{2p,p}(v), \qquad B = u^{2p} B_{2p,p}(v), \qquad u, v \in K,$$

or $4 \mid m$ and

(31) $$A = u^4 A_{8,4}(v), \qquad B = u^8 B_{8,4}(v), \qquad u, v \in K.$$

Proof. The condition is necessary. Indeed, if $x^2 + Ax + B$ is reducible over K then $\sqrt{A^2 - 4B} \in K$. If $x^2 + Ax + B$ is irreducible over K, but $x^{2m} + Ax^m + B$ is reducible it follows by Capelli's lemma that $x^m - \left(-A + \sqrt{A^2 - 4B}\right)/2$ is reducible over $K\left(\sqrt{A^2 - 4B}\right)$, hence by Capelli's theorem either there is a prime $p \mid m$ such that

(32) $$\frac{-A + \sqrt{A^2 - 4B}}{2} = \vartheta^p, \qquad \vartheta \in K\left(\sqrt{A^2 - 4B}\right),$$

or $4 \mid m$ and

(33) $$\frac{-A + \sqrt{A^2 - 4B}}{2} = -4\vartheta^4, \qquad \vartheta \in K\left(\sqrt{A^2 - 4B}\right).$$

Since ϑ is of degree 2 over K it can be written in the form

(34) $$\vartheta = \frac{A_1 + \sqrt{A_1^2 - 4B_1}}{2}, \qquad A_1, B_1 \in K.$$

Substituting (34) into (32) and taking traces and norms of both sides we obtain (30) with $u = A_1, v = B_1/A_1^2$. Substituting (34) into (33) and taking traces and norms of both sides we obtain (31) with $u = A_1, v = 2B_1/A_1^2$.

The condition is sufficient. If $\sqrt{A^2 - 4B} \in K$ this is obvious. If (30) holds $x^{2m} + Ax^m + B$ is divisible by $x^{2m/p} - ux^{m/p} + u^2v$, while if (31) holds it is equal to

$$\left(x^m + 2ux^{3m/4} + 2u^2x^{m/2} + 2u^3vx^{m/4} + u^4v^2\right) \times \left(x^m - 2ux^{3m/4} + 2u^2x^{m/2} - 2u^3vx^{m/4} + u^4v^2\right). \quad \square$$

Lemma 29. *Let K be any field, $f \in K[x]$, f irreducible and separable over K, and n a positive integer. Then $f(x^n)$ is reducible over K if and only if either for a prime $p \mid n$,*

$$f(x^p) = c \prod_{j=0}^{p-1} g\left(\zeta_p^j x\right),$$

or $4 \mid n$, char $K \neq 2$, *and*

$$f(-4x^4) = c \prod_{j=0}^{3} g(\zeta_4^j x),$$

where $g \in K[x]$ is monic and $\zeta_p = 1$ if $p =$ char K.

Proof. The condition is necessary. Indeed, let $f(\eta) = 0$. By Capelli's lemma $x^n - \eta$ is reducible over $K(\eta)$. By Capelli's theorem we have $\eta = \vartheta^p$, $\vartheta \in K(\eta)$ or char $K \neq 2$, $\eta = -4\vartheta^4$, $\vartheta \in K(\eta)$. Let $\vartheta_1, \ldots, \vartheta_d$ be all the conjugates of ϑ with respect to K. We take

$$g(x) = \prod_{i=1}^{d} (x - \vartheta_i) \in K[x]$$

and find in the first case

$$f(x^p) = a \prod_{i=1}^{d} (x^p - \vartheta_i^p) = a \prod_{i=1}^{d} \prod_{j=0}^{p-1} (x - \zeta_p^{-j} \vartheta_i)$$

$$= a(-1)^{(p-1)d} \prod_{j=0}^{p-1} \prod_{i=1}^{d} (\zeta_p^j x - \vartheta_i) = c \prod_{j=0}^{p-1} g(\zeta_p^j x),$$

in the second case

$$f(-4x^4) = a \prod_{i=1}^{d} (-4x^4 + 4\vartheta_i^4) = a(-4)^d \prod_{i=1}^{d} \prod_{j=0}^{3} (x - \zeta_4^{-j} \vartheta_i)$$

$$= a \cdot 4^d \prod_{j=0}^{3} \prod_{i=1}^{d} (\zeta_4^j x - \vartheta_i) = c \prod_{j=0}^{3} g(\zeta_4^j x).$$

c The condition is sufficient, since in the first case it gives $g(x^{n/p})$ as a proper factor of $f(x^n)$ in $K[x]$.

In the second case we have

$$f(x^4) = c\prod_{j=0}^{3} g\big(\tfrac{1}{2}\zeta_4^j(1-\zeta_4)x\big).$$

If $\zeta_4 \notin K$ then $\zeta_4^j(1-\zeta_4)$ for $j = 0$ and 1 are conjugate to each other over K, hence

$$h(x) = \prod_{j=0}^{1} g\big(\tfrac{1}{2}\zeta_4^j(1-\zeta_4)x\big) \in K[x],$$

and $h(x^{n/4})$ is a proper factor of $f(x^n)$ in $K[x]$. □

Remark. For $n = 2$ the lemma was proved by Selmer [27].

Lemma 30. *Let K be a field of characteristic different from 2, and $A, B \in K^*$. The trinomial $x^6 + Ax + B$ has a cubic factor in $K[x]$ if and only if*

$$A = u^5 A_{6,1}(v), \qquad B = u^6 B_{6,1}(v), \tag{35}$$

where $u, v \in K$.

Proof. The condition (35) is sufficient, since it implies

$$\begin{aligned} x^6 + Ax + B = \big(&x^3 + 2ux^2 + 2u^2(1+v)x + u^3(-v^2+4v+1)\big)\\ &\times\big(x^3 - 2ux^2 + 2u^2(1-v)x + u^3(v^2+4v-1)\big). \end{aligned}$$

On the other hand, if

$$x^6 + Ax + B = (x^3 + a_1x^2 + b_1x + c_1)(x^3 + a_2x^2 + b_2x + c_2)$$

we have

$$\begin{gathered} a_2 + a_1 = 0,\\ b_2 + a_1a_2 + b_1 = 0, \qquad c_2 + a_1b_2 + b_1a_2 + c_1 = 0,\\ a_1c_2 + b_1b_2 + c_1a_2 = 0, \qquad b_1c_2 + c_1b_2 = A, \qquad c_1c_2 = B. \end{gathered}$$

If $a_1 = 0$ we obtain $a_2 = 0$, $b_1 + b_2 = b_1b_2 = 0$, hence $b_1 = b_2 = 0$ and $A = 0$, contrary to $A \in K^*$. If $a_1 \neq 0$, we take $a_1 = 2u$, $b_1 = 2u^2(1+v)$ and find $a_2 = -2u$, $b_2 = 2u^2(1-v)$, $c_1 = u^3(-v^2+4v+1)$, $c_2 = u^3(v^2+4v-1)$, which gives (35). □

Lemma 31. *Let K be a field of characteristic different from 2, and $A, B \in K^*$. The trinomial $x^6 + Ax^2 + B$ is reducible over K if and only if either $x^3 + Ax + B$ is reducible over K or*

$$A = u^4 A_{6,2}(v), \qquad B = u^6 B_{6,2}(v), \tag{36}$$

where $u, v \in K$.

Proof. The condition (36) is sufficient, since it implies

$$x^6 + Ax^2 + B = (x^3 + 2ux^2 + 2u^2x - u^3v)(x^3 - 2ux^2 + 2u^2x + u^3v).$$

On the other hand, if $x^6 + Ax^2 + B$ is reducible and $x^3 + Ax + B$ is irreducible over K we have, by Lemma 29,

$$x^6 + Ax^2 + B = (x^3 + ax^2 + bx + c)(x^3 - ax^2 + bx - c),$$

hence

$$2b - a^2 = 0, \qquad b^2 - 2ac = A, \qquad -c^2 = B.$$

If $a = 0$ we obtain $b = 0$, hence $A = 0$, contrary to $A \in K^*$. If $a \neq 0$ we take $a = 2u$, $c = -u^3v$ and obtain (36). □

Lemma 32. *Let K be a field of characteristic different from 2, 7, and $A, B \in K^*$. The trinomial $x^7 + Ax + B$ has a cubic factor in $K[x]$ if and only if*

$$A = u^6 A_{7,1}(v), \qquad B = u^7 B_{7,1}(v), \tag{37}$$

where $u, v \in K$.

Proof. The condition (37) is sufficient, since it implies

$$\begin{aligned} x^7 + Ax + B = \big(&x^4 + u(2v+1)x^3 + u^2(2v+1)^2vx^2 \\ &+ u^3(2v+1)^2(v^2+2v-1)x + u^4(2v-1)(2v+1)^3(v^2-v+1)\big) \\ &\times (x^3 - u(2v+1)x^2 + u^2(1-v)(2v+1)^2x + u^3v(2v+1)^2(3v-2)). \end{aligned}$$

On the other hand, if

$$x^7 + Ax + B = (x^4 + a_1x^3 + b_1x^2 + c_1x + d_1)(x^3 + a_2x^2 + b_2x + c_2)$$

we have

$$\begin{gathered} a_2 + a_1 = 0, \qquad b_2 + a_1a_2 + b_1 = 0, \qquad c_2 + a_1b_2 + b_1a_2 + c_1 = 0, \\ a_1c_2 + b_1b_2 + c_1a_2 + d_1 = 0, \qquad b_1c_2 + c_1b_2 + d_1a_2 = 0, \\ c_1c_2 + d_1b_2 = A, \qquad d_1c_2 = B. \end{gathered}$$

If $a_1 = 0$ we obtain $b_2 = -b_1$, $c_2 = -c_1$, $d_1 = b_1^2$, $2b_1c_1 = 0$, hence $B = 0$, contrary to $B \in K^*$. If $a_1 \neq 0$ and $b_1 = -\frac{1}{2}a_1^2$ we obtain $b_2 = \frac{3}{2}a_1^2$, $c_2 + c_1 = -2a_1^3$, $a_1^2(c_2 + c_1) = \frac{3}{2}a_1^5$, a contradiction. If $a_1 \neq 0$ and $b_1 \neq -\frac{1}{2}a_1^2$ we take $v = b_1/a_1^2$, $u = a_1/(2v+1)$ and obtain (37) by a simple elimination. □

Lemma 33. *Let K be a field of characteristic different from 2, and $A, B \in K^*$. The trinomial $x^8 + Ax^2 + B$ is reducible over K if and only if either $x^4 + Ax + B$ is reducible over K or*

$$A = u^6 A_{8,2}(v), \qquad B = u^8 B_{8,2}(v), \tag{38}$$

where $u, v \in K$.

Proof. The condition (38) is sufficient, since it implies

$$x^8 + Ax^2 + B = \big(x^4 + 2ux^3 + 2u^2x^2 + u^3vx + u^4(2v - 2)\big) \times \big(x^4 - 2ux^3 + 2u^2x^2 - u^3vx + u^4(2v - 2)\big).$$

On the other hand, if $x^8 + Ax^2 + B$ is reducible and $x^4 + Ax + B$ irreducible over K we have, by Lemma 29,

$$x^8 + Ax^2 + B = (x^4 + ax^3 + bx^2 + cx + d)(x^4 - ax^3 + bx^2 - cx + d),$$

hence

$$2b - a^2 = 0, \qquad 2d + b^2 - 2ac = 0, \qquad bd - c^2 = A, \qquad d_2 = B.$$

If $a = 0$ we obtain $b = 0$, $d = 0$, $B = 0$, contrary to $B \in K^*$. If $a \neq 0$ we take $a = 2u$, $c = u^3v$ and obtain (38). □

Lemma 34. *Let K be a field of characteristic different from 3, and $A, B \in K^*$. The trinomial $x^9 + Ax^3 + B$ is reducible over K if and only if either $x^3 + Ax + B$ is reducible over K or*

$$A = u^6 A_{9,3}(v), \qquad B = u^9 B_{9,3}(v), \tag{39}$$

where $u, v \in K$.

Proof. The condition (39) is sufficient, since it implies

$$\begin{aligned} x^9 + Ax^3 + B &= \big(x^3 + 3ux^2 + u^2vx + u^3(3v - 9)\big)\big(x^3 + 3u\zeta_3^2x^2 + u^2v\zeta_3x + u^3(3v - 9)\big) \\ &\quad \times \big(x^3 + 3u\zeta_3x^2 + u^2v\zeta_3^2x + u^3(3v - 9)\big). \end{aligned}$$

On the other hand, if $x^9 + Ax^3 + B$ is reducible and $x^3 + Ax + B$ irreducible over K we have, by Lemma 29,

$$\begin{aligned} x^9 + Ax^3 + B &= (x^3 + ax^2 + bx + c)(x^3 + a\zeta_3^2x^2 + b\zeta_3x + c) \\ &\quad \times (x^3 + a\zeta_3x^2 + b\zeta_3^2x + c) \\ &= (x^3 + c)^3 + a^3x^6 + b^3x^3 - 3(x^3 + c)abx^3, \end{aligned}$$

hence

$$3c + a^3 - 3ab = 0, \qquad 3c^2 + b^3 - 3abc = A, \qquad c^3 = B.$$

If $a = 0$ we obtain $c = 0$, $B = 0$, contrary to $B \in K^*$. If $a \neq 0$ we take $a = 3u$, $b = u^2v$ and obtain (39). □

Lemma 35. *Let K be a field of characteristic different from 2, and $A, B \in K^*$. The trinomial $x^{10} + Ax^2 + B$ is reducible over K if and only if either $x^5 + Ax + B$ is reducible over K or*

$$A = u^8 A_{10,2}(v), \qquad B = u^{10} B_{10,2}(v), \tag{40}$$

where $u, v \in K$.

Proof. The condition (40) is sufficient, since it implies

$$\begin{aligned} &x^{10} + Ax^2 + B \\ &= \left(x^5 + 2ux^4 + 2u^2x^3 + 2u^3vx^2 + u^4(4v-2)x + u^5(-v^2+4v-2)\right) \\ &\qquad \times \left(x^5 - 2ux^4 + 2u^2x^3 - 2u^3vx^2 + u^4(4v-2)x - u^5(-v^2+4v-2)\right). \end{aligned}$$

On the other hand, if $x^{10} + Ax^2 + B$ is reducible and $x^5 + Ax + B$ irreducible over K we have, by Lemma 29,

$$x^{10} + Ax^2 + B = (x^5 + ax^4 + bx^3 + cx^2 + dx + e)(x^5 - ax^4 + bx^3 - cx^2 + dx - e),$$

hence

$$\begin{gathered} 2b - a^2 = 0, \qquad 2d + b^2 - 2ac = 0, \qquad 2bd - 2ae - c^2 = 0, \\ d^2 - 2ce = A, \qquad -e^2 = B. \end{gathered}$$

If $a = 0$, we obtain $b = c = d = 0$, $A = 0$, contrary to $A \in K^*$. If $a \neq 0$ we take $a = 2u$, $c = 2u^3 v$ and obtain (40). □

Lemma 36. *Let K be a field of characteristic different from 2, and $A, B \in K^*$. The trinomial $x^{10} + Ax^4 + B$ is reducible over K if and only if either $x^5 + Ax^2 + B$ is reducible over K or*

$$A = u^8 A_{10,4}(v), \qquad B = u^{10} B_{10,4}(v), \tag{41}$$

where $u, v \in K$.

Proof. The condition (41) is sufficient, since it implies

$$\begin{aligned} &x^{10} + Ax^4 + B \\ &= \left(x^5 + 2uvx^4 + 2u^2v^2x^3 + u^3v^4x^2 + u^4v^4(2v-2)x + 2u^5v^4(v-1)^2\right) \\ &\qquad \times \left(x^5 - 2uvx^4 + 2u^2v^2x^3 - u^3v^4x^2 + u^4v^4(2v-2)x - 2u^5v^4(v-1)^2\right). \end{aligned}$$

On the other hand, if $x^{10} + Ax^4 + B$ is reducible and $x^5 + Ax^2 + B$ irreducible over K we have, by Lemma 29,

$$x^{10} + Ax^4 + B = (x^5 + ax^4 + bx^3 + cx^2 + dx + e)(x^5 - ax^4 + bx^3 - cx^2 + dx - e),$$

hence

$$\begin{gathered} 2b - a^2 = 0, \qquad 2d + b^2 - 2ac = 0, \qquad 2bd - 2ae - c^2 = A, \\ d^2 - 2ce = 0, \qquad -e^2 = B. \end{gathered}$$

If $a = 0$, we obtain $b = d = 0$, $ce = 0$ and $AB = 0$, contrary to $A, B \in K^*$. If $a \neq 0$, $c = 0$ we obtain $d = 0, b = 0, a^2 = 0$, a contradiction. If $a \neq 0, c \neq 0$ we take $v = 8c/a^3$, $u = a/2v$ and obtain (41). □

Lemma 37. *Let K be a field of characteristic different from 2, and $A, B \in K^*$. The trinomial $x^{12} + Ax^2 + B$ is reducible over K if and only if either $x^6 + Ax + B$ is reducible over K or*

$$A = u^{10}A_{12,2}(v), \qquad B = u^{12}B_{12,2}(v), \tag{42}$$

where $u, v \in K$.

Proof. The condition (42) is sufficient, since it implies

$$\begin{aligned} x^{12} + Ax^2 + B = \big(&x^6 + 4u(v-4)x^5 + 8u^2(v-4)^2x^4 + 8u^3v(v-4)^3x^3 \\ &+ 32u^4(v-1)(v-4)^4x^2 + 32u^5(v-4)^4(3v^2 - 12v + 10)x \\ &+ 32u^6(v-4)^5(v^3 - 8v + 8)\big)\big(x^6 - 4u(v-4)x^5 + 8u^2(v-4)^2x^4 \\ &- 8u^3v(v-4)^3x^3 + 32u^4(v-1)(v-4)^4x^2 \\ &- 32u^5(v-4)^4(3v^2 - 12v + 10)x + 32u^6(v-4)^5(v^3 - 8v + 8)\big). \end{aligned}$$

On the other hand, if $x^{12} + Ax^2 + B$ is reducible, but $x^6 + Ax + B$ irreducible over K we have, by Lemma 29,

$$x^{12}+Ax^2+B = (x^6+ax^5+bx^4+cx^3+dx^2+ex+f)(x^6-ax^5+bx^4-cx^3+dx^2-ex+f),$$

hence

$$\begin{gathered} 2b - a^2 = 0, \quad 2d + b^2 - 2ac = 0, \quad 2f - 2bd - 2ae - c^2 = 0, \\ 2bf + d^2 - 2ce = 0, \quad 2df - e^2 = A, \quad f^2 = B. \end{gathered}$$

If $a = 0$, we obtain $b = 0$, $d = 0$, $ce = 0$, $AB = 0$, contrary to $A, B \in K^*$. If $a \neq 0$, $c = \frac{1}{2}a^3$ we obtain $b = \frac{1}{2}a^2$, $d = \frac{3}{8}a^4$, $f - ae = -\frac{1}{16}a^6$, $a^2f - a^3e = -\frac{9}{64}a^8$, a contradiction. If $a \neq 0$, $c \neq \frac{1}{2}a^3$ we take $v = 8c/a^3$, $u = a/4(v-4)$ and obtain (42).□

Lemma 38. *Let K be a field of characteristic different from 3, and $A, B \in K^*$. The trinomial $x^{12} + Ax^3 + B$ is reducible over K if and only if either $x^4 + Ax + B$ is reducible over K or*

$$A = u^9A_{12,3}(v), \qquad B = u^{12}B_{12,3}(v), \tag{43}$$

where $u, v \in K$.

Proof. The condition (43) is sufficient, since it implies

$$x^{12}+Ax^3+B = \prod_{i=0}^{2}\big(\zeta_3^i x^4+3u(v-1)x^3+9u^2v(v-1)^2\zeta_3^{2i}x^2+9u^3(v-1)^3(3v-1)\zeta_3^i x + 9u^4(v-1)^3(3v^3-3v+1)\big).$$

On the other hand, if $x^{12}+Ax^3+B$ is reducible and x^4+Ax+B irreducible over K we have, by Lemma 29,

$$\begin{aligned} x^{12}+Ax^3+B &= \prod_{i=0}^{2}\big(\zeta_3^i x^4+ax^3+b\zeta_3^{2i}x^2+c\zeta_3^i x+d\big)\\ &= (x^4+cx)^3+(ax^3+d)^3b^3x^6-3bx^2(x^4+cx)(ax^3+d). \end{aligned}$$

Hence

$$3c+a^3-3ab=0,\qquad 3c^2+3a^2d+b^3-3abc-3bd=0,$$
$$c^3+3ad^2-3bcd=A,\qquad B=d^3.$$

If $a=0$, we obtain $c=0$, $A=0$, contrary to $A\in K^*$. If $a\neq 0$, $b=a^2$ we obtain $c=\frac{2}{3}a^3$, $\frac{1}{3}a^6=0$, a contradiction. If $a\neq 0$, $b\neq a^2$ we take $v=b/a^2$, $u=a/3(v-1)$ and obtain (43). □

Lemma 39. *Let K be a field of characteristic different from 2, and $A, B\in K^*$. The trinomial $x^{12}+Ax^4+B$ is reducible over K if and only if either x^6+Ax^2+B is reducible over K or*

$$A=u^8A_{12,4}(v),\qquad B=u^{12}B_{12,4}(v), \tag{44}$$

where $u, v\in K$.

Proof. The condition (44) is sufficient, since it implies

$$\begin{aligned} x^{12}+Ax^4+B = &\big(x^6+4ux^5+8u^2x^4+8u^3(2v^2+1)x^3+64u^4v^2x^2\\ &+64u^5v(-2v^2+4v-1)x+32u^6(-2v^2+4v-1)^2\big)\\ &\times\big(x^6-4ux^5+8u^2x^4-8u^3(2v^2+1)x^3+64u^4v^2x^2\\ &-64u^5v(-2v^2+4v-1)x+32u^6(-2v^2+4v-1)^2\big). \end{aligned}$$

On the other hand, if $x^{12}+Ax^4+B$ is reducible and x^6+Ax^2+B irreducible over K we have, by Lemma 29,

$$\begin{aligned} -64x^{12}+Ax^4+B &= -64\prod_{i=0}^{3}(\zeta_4^i x^3+a\zeta_4^{2i}x^2+b\zeta_4^i x+c)\\ &= -64\left((x^3+bx)^2-(ax^2+c)^2\right)\left((-x^3+bx)^2+(-ax^2+c)^2\right). \end{aligned}$$

Hence

$$2b^2 - 4ac - (2b - a^2)^2 = 0, \quad 16\left((b^2 - 2ac)^2 + 2(2b - a^2)c^2\right) = A, \quad 64c^4 = B.$$

If $a = 0$, we obtain $b = 0$, $A = 0$, contrary to $A \in K^*$. If $a \neq 0$ we take $a = 2u, b = 4u^2v$ and obtain (44). □

Lemma 40. *Let K be a field of characteristic different from 5, and $A, B \in K^*$. The trinomial $x^{15} + Ax^5 + B$ is reducible over K if and only if either $x^3 + Ax + B$ is reducible over K or*

$$A = u^{10}A_{15,5}(v), \qquad B = u^{15}B_{15,5}(v), \tag{45}$$

where $u, v \in K$.

Proof. The condition (45) is sufficient, since it implies

$$x^{15} + Ax^5 + B = \prod_{i=0}^{4}\big(\zeta_5^{3i}x^3 + u(5v - 5)\zeta_5^{2i}x^2 + u^2v(5v - 5)^2\zeta_5^i x + u^3(5v - 5)^2(5v^2 - 5v + 1)\big).$$

On the other hand, if $x^{15} + Ax^5 + B$ is reducible and $x^3 + Ax + B$ irreducible over K we have, by Lemma 29,

$$x^{15} + Ax^5 + B = \prod_{i=0}^{4}\big(\zeta_5^{3i}x^3 + a\zeta_5^{2i}x^2 + b\zeta_5^i x + c\big).$$

Hence

$$-5bc + 5a^2c + 5ab^2 - 5a^3b + a^5 = 0,$$
$$-5ac^3 - 5ab^3c + 5a^2bc^2 + 5b^2c^2 + b^5 = A, \qquad c^5 = B.$$

If $a = 0$, we obtain $bc = 0$, $AB = 0$, contrary to $A, B \in K^*$. If $a \neq 0$, $b = a^2$ we obtain $a^5 = 0$, a contradiction. If $a \neq 0$, $b \neq a^2$ we take $v = b/a^2$, $u = a/(5v - 5)$ and obtain (45). □

4. Determination of the content of Table 2 (Lemmas 41 to 48)

Lemma 41. *Let K be a field of characteristic different from 2. The curve*

$$y^2 = x^4 + a_1x^3 + 3a_2x^2 + a_3x + a_4 = R(x), \tag{46}$$

where $R \in K[x]$ is not a square over $\overline{K}$, is equivalent to the curve

$$w^2 = v^3 - (4a_4 - a_1a_3 + 3a_2^2)v - (8a_2a_4 + a_1a_2a_3 - a_4a_1^2 - a_3^2 - 2a_2^3) \tag{47}$$

under the following birational transformation over K:

$$
\begin{aligned}
v &= 2y + 2x^2 + a_1 x + a_2,\\
w &= 4xy + a_1 y + 4x^3 + 3a_1 x^2 + 6a_2 x + a_3;\\
x &= \frac{(v-a_2)^2 - 4a_4}{2w + a_1(v-a_2) + 2a_3},\\
y &= \frac{1}{2}\,v - x^2 - \frac{a_1}{2}\,x - \frac{a_2}{2}.
\end{aligned}
\tag{48a}
$$

The zeros of the denominator in the above formula for x, lying on (47)*, correspond to the point at infinity on* (46) *and to the points $\langle x, y\rangle$, where*

$$
x = \frac{4(a_3 + a_1\sqrt{a_4})}{a_1^2 - 12a_2 - 8\sqrt{a_4}}, \qquad y = \frac{1}{2}\,v - x^2 - \frac{a_1}{2}\,x - \frac{a_2}{2}
$$

with any choice of the square root.

Moreover, if $R(x_0) = 0$, $R'(x_0) \neq 0$ for an $x_0 \in K$ there is a simpler birational transformation over K:

$$
\begin{aligned}
v &= \frac{\frac{1}{3}R''(x_0)x + \left(2R'(x_0) - \frac{1}{3}R''(x_0)x_0\right)}{2(x - x_0)},\\
w &= \frac{R'(x_0)y}{(x-x_0)^2};\\
x &= \frac{2x_0 v + \left(2R'(x_0) - \frac{1}{3}R''(x_0)x_0\right)}{2v - \frac{1}{3}R''(x_0)},\\
y &= \frac{4R'(x_0)w}{\left(2v - \frac{1}{3}R''(x_0)\right)^2},
\end{aligned}
\tag{48b}
$$

where $\frac{1}{3}R''(x_0) = 4x_0^2 + 2a_1x_0 + 2a_2$.The two zeros of the denominator in the above formula for x, lying on (47)*, correspond to the double point at infinity on* (46).

Remark. Note that $4(a_3 + a_1\sqrt{a_4})$ and $a_1^2 - 12a_2 - 8\sqrt{a_4}$ are not simultaneously 0 since otherwise $R(x) = (x^2 + \frac{1}{2}a_1x - \sqrt{a_4})^2$.

Proof. The curve (46) is equivalent to the curve

$$
y_1^2 = a_4x_1^4 + a_3x_1^3 + 3a_2x_1^2 + a_1x_1 + 1 = R(x_1) \tag{49}
$$

via the involution I:

$$
x_1 = \frac{1}{x}, \qquad y_1 = \frac{y}{x^2}.
$$

On the other hand, the curve (49) has the rational point $\langle 0, 1\rangle$. Applying to (49) the transformation of Weierstrass as described in Theorem 3 of [16] with $x_0 = 0$, $y_0 = 1$ we find that it is equivalent to the curve

$$
Y^2 = 4X^3 - g_2X - g_3, \tag{50}
$$

where

$$g_2 = \frac{1}{4}(4a_4 - a_1a_3 + 3a_2^2), \qquad g_3 = \frac{1}{16}(8a_2a_4 + a_1a_2a_3 - a_4a_1^2 - a_3^2 - 2a_2^3),$$

via the birational transformation T:

$$\begin{aligned} X &= \frac{y_1 + 1 + \frac{1}{2}a_1x_1 + 3a_2}{2x_1^2}, \\ Y &= \frac{y_1^2}{x_1^3} - \frac{1}{4}\frac{R'(x_1)}{x_1^2} + \left(\frac{1}{x_1^3} + \frac{1}{4}\frac{a_1}{x_1^2}\right) y_1; \\ x_1 &= \frac{Y + \frac{1}{2}a_1(X - \frac{3}{2}a_2) + \frac{1}{4}a_3}{2\left(X - \frac{3}{2}a_2\right)^2 - \frac{1}{2}a_4}, \\ y_1 &= 2Xx_1^2 - 1 - \frac{1}{2}a_1x_1 - 3a_2x_1^2. \end{aligned}$$

Finally, the curve (50) is equivalent to the curve (47) via the linear transformation L:

$$v = 4X, \qquad w = 4Y.$$

The birational transformation (48a) given in the lemma is a composition of I, T and L.

The birational transformation (48b) is obtained directly from Theorem 3 in [16] by setting $y_0 = 0$. □

Lemma 42. *Let K be a field of characteristic different from 2, and $A, B \in K^*$. The trinomial $x^7 + ax^2 + B$ has a cubic factor in $K[x]$ if and only if either*

$$A = -2u^5, \qquad B = u^7, \qquad u \in K \tag{51}$$

or

$$A = u^5A_{7,2}(v, w), \qquad B = u^7B_{7,2}(v, w), \tag{52}$$

where $u \in K$ and

$$\langle v, w\rangle \in E_{7,2}(K). \tag{53}$$

Proof. The condition is sufficient, since if (51) holds we have

$$x^7 + Ax^2 + B = (x^4 - u^2x^2 - u^3x + u^4)(x^3 + ux^2 + u^3)$$

and if (52) and (53) hold we have

$$\begin{aligned} x^7 + Ax^2 + B &= \left(x^4 + 2ux^3 - u^2vx^2 + u^3(w + 4)x + u^4(v^2 + 12v + 4w + 32)\right) \\ &\quad \times \left(x^3 - 2ux^2 + u^2(v + 4)x + u^3(-4v - w - 12)\right). \end{aligned}$$

On the other hand, if $x^7 + Ax^2 + B$ has a cubic factor we have

$$x^7 + Ax^2 + B = (x^4 + a_1x^3 + b_1x^2 + c_1x + d_1)(x^3 + a_2x^2 + b_2x + c_2),$$

hence

$$a_2 + a_1 = 0, \qquad b_2 + a_1a_2 + b_1 = 0, \qquad c_2 + a_1b_2 + b_1a_2 + c_1 = 0,$$
$$a_1c_2 + b_1b_2 + c_1a_2 + d_1 = 0, \qquad b_1c_2 + c_1b_2 + d_1a_2 = A,$$
$$c_1c_2 + d_1b_2 = 0, \qquad d_1c_2 = B.$$

If $a_1 = 0$ we obtain $a_2 = 0, b_2 = -b_1, c_2 = -c_1, d_1 = b_1^2, c_1^2 + b_1^3 = 0$ and on taking $b_1 = -u^2$ we obtain (51).

If $a_1 \neq 0$ we take $a_1 = 2u, b_1 = -u^2v, c_1 = u^3(w + 4)$ and obtain (52)–(53). □

Lemma 43. *Let K be a field of characteristic different from 2, 3, and $A, B \in K^*$. The trinomial $x^7 + Ax^3 + B$ has a cubic factor in $K[x]$ if and only if*

$$A = u^4A_{7,3}(v), \qquad B = u^7B_{7,3}(v), \tag{54}$$

where $u \in K$ and

$$\langle v, w\rangle \in E_{7,3}(K). \tag{55}$$

Proof. The condition is sufficient, since if it is satisfied we have

$$\begin{aligned} &x^7 + Ax^3 + B \\ &= \big(x^4 + u(v - 39)x^3 - 36u^2(v - 39)x^2 + 6u^3(v - 39)(-w + 3v + 99)x \\ &\quad + 6u^4(v - 39)(-w(v + 33) + 9v^2 + 162v - 4455)\big) \\ &\quad \times \big(x^3 - u(v - 39)x^2 + u^2(v - 3)(v - 39)x + u^3(6w - v^2 - 12v + 693)\big). \end{aligned}$$

On the other hand, if

$$x^7 + Ax^3 + B = (x^4 + a_1x^3 + b_1x^2 + c_1x + d_1)(x^3 + a_2x^2 + b_2x + c_2)$$

we have

$$a_2 + a_1 = 0, \qquad b_2 + a_1a_2 + b_1 = 0, \qquad c_2 + a_1b_2 + b_1a_2 + c_1 = 0,$$
$$a_1c_2 + b_1b_2 + c_1a_2 + d_1 = A, \qquad b_1c_2 + c_1b_2 + d_1a_2 = 0,$$
$$c_1c_2 + d_1b_2 = 0, \qquad d_1c_2 = B.$$

If $a_1 = 0$ we obtain $a_2 = 0, b_2 = -b_1, c_2 = -c_1, b_1c_1 = 0, B = 0$, contrary to $B \in K^*$.

If $a_1 \neq 0$ we take $x = 2b_2/a_1^2, y = 4c_2a_1^{-3} + 4b_2^2a_1^{-4} + 2b_2a_1^{-2} - 2$ and obtain

$$y^2 = x^4 - 2x^3 + x^2 - 4x + 4 = R(x).$$

If $x = 2$ we obtain $b_2 = a_1^2, b_1 = 0, c_2 = -a_1^3, c_1 = 0, d_1 = 0, B = 0$, contrary to $B \in K^*$. Since $R(2) = 0$, if $x \neq 2$ we put

$$v = \frac{39x - 6}{x - 2}, \qquad w = \frac{216y}{(x - 2)^2}.$$

By Lemma 41 we have (55) and $v \neq 39$. On taking $u = a_1/(v - 39)$ we obtain (54). □

Lemma 44. *Let K be a field and $A, B \in K^*$. The trinomial $x^8 + Ax + B$ has a cubic factor in $K[x]$ if and only if either*

$$A = -3u^7, \qquad B = 2u^8, \qquad u \in K \tag{56}$$

or

$$\begin{aligned} A &= \big((3v^2 - 12v - 10)w - 8v^3 + 20v^2 + 8v - 32\big)u^7, \\ B &= (w - 3v + 5)\big((2v - 5)w - 3v^2 + 15v - 17\big)u^8, \end{aligned} \tag{57}$$

where $u, v, w \in K$ and

$$w^2 = v^3 - 10v + 12. \tag{58}$$

Proof. The condition is sufficient, since if (56) holds then

$$x^8 + Ax + B = (x^5 - u^2x^3 + u^3x^2 + u^4x + 2u^5)(x^3 + u^2x + u^3)$$

and if (57) and (58) hold then

$$\begin{aligned} &x^8 + Ax + B \\ &\quad = \big(x^5 - ux^4 + u^2(2 - v)x^3 + u^3(-w + v - 2)x^2 + u^4(-2w + v^2 + v - 5)x \\ &\qquad + u^5((2v - 5)w - 3v^2 + 15v - 17)\big)\big(x^3 - ux^2 + (v - 1)x + (w - 3v + 5)\big). \end{aligned}$$

On the other hand, if

$$x^8 + Ax + B = (x^5 + a_1x^4 + b_1x^3 + c_1x^2 + d_1x + e_1)(x^3 + a_2x^2 + b_2x + c_2)$$

we have

$$\begin{gathered} a_2 + a_1 = 0, \qquad b_2 + a_1a_2 + b_1 = 0, \qquad c_2 + a_1b_2 + b_1a_2 + c_1 = 0, \\ a_1c_2 + b_1b_2 + c_1a_2 + d_1 = 0, \qquad b_1c_2 + c_1b_2 + d_1a_2 + e_1 = 0, \\ c_1c_2 + d_1b_2 + e_1a_2 = 0, \qquad d_1c_2 + e_1b_2 = A, \qquad e_1c_2 = B. \end{gathered}$$

If $a_1 = 0$ we obtain $a_2 = 0, b_2 = -b_1, c_2 = -c_1, d_1 = b_1^2, e_1 = 2b_1c_1, c_1^2 + b_1^3 = 0$, and (56) follows on taking $u = c_1/b_1$. If $a_1 \neq 0$, (57) and (58) follow on taking

$$u = a_1, \qquad v = 2 - \frac{b_1}{a_1^2}, \qquad w = -\frac{b_1}{a_1^2} - \frac{c_1}{a_1^3}. \qquad \square$$

Lemma 45. *Let K be a field of characteristic different from 2, and $A, B \in K^*$. The trinomial $x^8 + Ax + B$ has a quartic factor in $K[x]$ if and only if either*

$$A = 3u^7, \qquad B = 2u^8, \qquad u \in K \tag{59}$$

or

$$\begin{aligned} A &= 128(w - 2v - 8)^4(v + 2)(v^2 + 12v + 4) \\ &\quad \times (2w - v^2 + 4v + 4)(4w - v^2 - 12), \\ B &= 64(w - 2v - 8)^4 \\ &\quad \times \big(9v^4 + 8v^3 - 8v^2 + 288v + 272 - w(v^3 + 18v^2 + 76v + 24)\big) \\ &\quad \times \big(v^4 + 24v^3 + 152v^2 + 96v + 16 + w(v^3 - 22v^2 - 52v - 72)\big), \end{aligned} \tag{60}$$

where $u, v, w \in K$ *and*

$$w^2 = v^3 - 20v - 16. \tag{61}$$

Proof. The condition is sufficient, since if (59) holds we have

$$x^8 + Ax + B = (x^4 + ux^3 + u^2x^2 + 2u^3x + u^4)(x^4 - ux^3 - u^3x + 2u^4).$$

If (60) and (61) hold we have

$$\begin{aligned} x^8 + Ax + B = \big(&x^4 + 4(w - 2v - 8)x^3 + 4(w - 2v - 8)(v^2 - 8v - 20)x^2 \\ &+ 8(w - 2v - 8)^2(-20v - 24 + w(v - 2))x \\ &+ 8(w - 2v - 8)^2(9v^4 + 8v^3 - 8v^2 + 288v + 272 \\ &- w(v^3 + 18v^2 + 76v + 24))\big) \\ &\times \big(x^4 - 4(w - 2v - 8)x^3 + 4(w - 2v - 8)(4w - v^2 - 12)x^2 \\ &+ 8(w - 2v - 8)^2(4v^2 + 4v + 8 - w(v + 6))x \\ &+ 8(w - 2v - 8)^2(v^4 + 24v^3 + 152v^2 + 96v + 16 \\ &+ w(v^3 - 22v^2 - 52v - 72))\big). \end{aligned}$$

On the other hand, if

$$x^8 + Ax + B = (x^4 + a_1x^3 + b_1x^2 + c_1x + d_1)(x^4 + a_2x^3 + b_2x^2 + c_2x + d_2)$$

we have

$$\begin{gathered} a_2 + a_1 = 0, \qquad b_2 + a_1a_2 + b_1 = 0, \qquad c_2 + a_1b_2 + b_1a_2 + c_1 = 0, \\ d_2 + a_1c_2 + b_1b_2 + c_1a_2 + d_1 = 0, \qquad a_1d_2 + b_1c_2 + c_1b_2 + d_1a_2 = 0, \\ b_1d_2 + c_1c_2 + d_1b_2 = 0, \qquad c_1d_2 + d_1c_2 = A, \qquad d_1d_2 = B. \end{gathered}$$

If $a_1 = 0$ we obtain $a_2 = 0$, $b_2 = -b_1$, $c_2 = -c_1$, $d_2 = b_1^2 - d_1$, $2b_1c_1 = 0$, $b_1^3 - 2b_1d_1 - c_1^2 = 0$, $A = 0$, contrary to $A \in K^*$.

If $a_1 \neq 0$ we take $x_1 = 2b_1/a_1^2$, $y_1 = 4c_1/a_1^3 - 4b_1^2/a_1^4 - 1$ and obtain

$$y_1^2 = x_1^4 - 4x_1^3 + 12x_1^2 - 16x_1 + 9 = R(x_1).$$

If $x_1 = 2$ we obtain $y_1 = \pm 3$ hence either $b_1 = a_1^2$, $c_1 = 2a_1^3$, $b_2 = 0$, $c_2 = -a_1^3$, $d_1 = a_1^4$, $d_2 = 2a_1^4$ and (59) holds with $u = -a_1$ or $b_1 = a_1^2$, $c_1 = \frac{1}{2}a_1^3$, $b_2 = 0$, $c_2 = \frac{1}{2}a_1^3$, $d_1 = \frac{1}{4}a_1^4$, $d_2 = -\frac{1}{4}a_1^4$, $A = 0$, contrary to $A \in K^*$.

If $x_1 \neq 2$ we put

$$\begin{aligned} v &= 2y_1 + 2x_1^2 - 4x_1 + 4, \\ w &= 4x_1y_1 - 4y_1 + 4x_1^3 - 12x_1^2 + 24x_1 - 16 \end{aligned}$$

and using Lemma 41 we obtain (61) with $w - 2v - 8 \neq 0$. Now (60) follows on taking

$$u = \frac{a_1}{4(w - 2v - 8)}. \qquad \square$$

Lemma 46. *Let K be a field of characteristic different from* 2 *and* 3*, and $A, B \in K^*$. The trinomial $x^9 + Ax + B$ has a cubic factor in $K[x]$ if and only if either $\sqrt{13} \in K$ and*

$$\begin{aligned} A &= (-480053919711226727 \pm 66936076602084894\sqrt{13})u^8, \\ B &= \tfrac{1}{2}(-57126858783170637 25 \pm 66644985243629014605\sqrt{13})u^9, \\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \textit{where } u \in K, \end{aligned} \tag{62}$$

or

$$A = u^8 A_{9,1}(v, w), \qquad B = u^9 B_{9,1}(v, w), \tag{63}$$

where $u \in K$ and

$$\langle v, w \rangle \in E_{9,1}(K). \tag{64}$$

Proof. The condition is sufficient, since if (62) is satisfied we have with the suitable value of $\sqrt{13}$

$$\begin{aligned} &x^9 + Ax + B \\ &= \left(x^3 + 183ux^2 + (41175 + 549\sqrt{13})u^2x + \frac{9879255 - 1774917\sqrt{13}}{2}\,u^3\right) \\ &\quad \times \left(x^6 - 183ux^5 - (7686 + 549\sqrt{13})u^2x^4 + \frac{8003871 + 2176785\sqrt{13}}{2}\,u^3x^3\right. \\ &\quad + (491986899 - 334756044\sqrt{13})u^4x^2 \\ &\quad + \frac{-461897936703 + 20279163483\sqrt{13}}{2}\,u^5x \\ &\quad \left. + \frac{34367850319995 + 19666467995175\sqrt{13}}{2}\,u^6\right) \end{aligned}$$

and if (63) and (64) hold we have

$$\begin{aligned} x^9 + Ax + B = {} & \big(x^3 + 3(w - 2v - 9)ux^2 + 3(w - 2v - 9)(v^2 - 9v - 9)u^2x \\ & + 3(w - 2v - 9)^2(6v^2 - 21v - 9 - w(v + 3))u^3\big) \\ & \times \big(x^6 - 3(w - 2v - 9)ux^5 \\ & + 3(w - 2v - 9)(-v^2 + 3v - 18 + 3w)u^2x^4 \\ & + 3(w - 2v - 9)^2(-15v + 36 + w(v - 6))u^3x^3 + 9(w - 2v - 9)^2 \\ & \times \big(-v^4 - 21v^3 + 30v^2 - 117v + 351 + w(7v^2 + 33v - 45)\big)u^4x^2 \\ & + 9(w - 2v - 9)^3\big(12v^4 + 48v^3 - 153v^2 + 135v - 567 \\ & + w(-2v^3 - 24v^2 - 90v + 54)\big)u^5x + 9(w - 2v - 9)^3 \\ & \times \big(v^6 + 219v^5 - 9v^4 - 792v^3 - 2916v^2 + 6804v - 6804 \\ & + w(v^5 - 60v^4 - 228v^3 - 81v^2 - 972v + 1134)\big)u^6\big) \end{aligned}$$

On the other hand, if

$$x^9 + Ax + B = (x^6 + a_1x^5 + b_1x^4 + c_1x^3 + d_1x^2 + e_1x + f_1)(x^3 + a_2x^2 + b_2x + c_2)$$

we find

$$a_2 + a_1 = 0, \qquad b_2 + a_1a_2 + b_1 = 0, \qquad c_2 + a_1b_2 + b_1a_2 + c_1 = 0,$$
$$a_1c_2 + b_1b_2 + c_1a_2 = 0, \qquad b_1c_2 + c_1b_2 + d_1a_2 + e_1 = 0,$$
$$c_1c_2 + d_1b_2 + e_1a_2 + f_1 = 0, \qquad d_1c_2 + e_1b_2 + f_1a_2 = 0,$$
$$e_1c_2 + f_1b_2 = A, \qquad f_1c_2 = B.$$

If $a_1 = 0$ we obtain $a_2 = 0, b_2 = -b_1, c_2 = -c_1, d_1 = b_1^2, e_1 = 2b_1c_1, f_1 - b_1^3 - c_1^2 = 0$, $3b_1e_1 = 0$ and either $b_1 = 0$, which gives $A = 0$, or $c_1 = 0$, which gives $B = 0$, contrary to the assumption.

If $a_1 \neq 0$ we take

$$x_1 = 3b_2/a_2^2, \qquad y_1 = -18c_2/a_2^3 - 15 + 36b_2/a_2^2 - 9b_2^2/a_2^4$$

and obtain

$$y_1^2 = x_1^4 - 8x_1^3 + 54x_1^2 - 144x_1 + 117.$$

If

$$\langle x_1, y_1\rangle = \left\langle \frac{225 \pm 3\sqrt{13}}{61}, \frac{11478 \pm 10545\sqrt{13}}{61^2} \right\rangle$$

(62) follows on taking $u = a_2/183$.

If

$$\langle x_1, y_1\rangle \neq \left\langle \frac{225 \pm 3\sqrt{13}}{61}, \frac{11478 \pm 10545\sqrt{13}}{61^2} \right\rangle$$

we put

$$v = \frac{y_1}{2} + \frac{x_1^2}{2} - 2x_1 + \frac{9}{2}, \qquad w = \frac{x_1y_1}{2} - y_1 + \frac{x_1^3}{2} - 3x_1^2 + \frac{27}{2}x_1 - 18.$$

By Lemma 41 we obtain (64) and $w - 2v - 9 \neq 0$. Hence (63) follows on taking $u = a_2/183(w - 2v - 9)$. □

Lemma 47. *Let K be a field of characteristic different from 2, and $A, B \in K^*$. The trinomial $x^{14} + Ax^2 + B$ is reducible over K if and only if either $x^7 + Ax + B$ is reducible over K or*

$$A = u^{12}A_{14,2}(v, w), \qquad B = u^{14}B_{14,2}(v, w), \tag{65}$$

where $u \in K$ and

$$\langle v, w\rangle \in E_{14,2}(K). \tag{66}$$

Proof. The condition is sufficient, since it yields

$$\begin{aligned} x^{14}+Ax^2+B = \prod_{\varepsilon=\pm1} \big(&x^7+2\varepsilon u(v-2)x^6+2u^2(v-2)^2x^5\\ &+2\varepsilon u^3(v-2)^2(v-1)x^4+2u^4(v-2)^3vx^3\\ &+2\varepsilon u^5(v-2)^3(w+v^2-3)x^2\\ &+2u^6(v-2)^4(2w+v^2+2v-5)x\\ &+\varepsilon u^7(v-2)^4((2v-6)w+v^3-12v+14)\big). \end{aligned}$$

On the other hand, if $x^{14}+Ax^2+B$ is reducible, but x^7+Ax+B irreducible over K we have, by Lemma 29,

$$\begin{aligned} x^{14}+Ax^2+B &= \prod_{\varepsilon=\pm1}\big(x^7+\varepsilon ax^6+bx^5+\varepsilon cx^4+dx^3+\varepsilon ex^2+fx+\varepsilon g\big)\\ &= (x^7+bx^5+dx^3+fx)^2-(ax^6+cx^4+ex^2+g)^2. \end{aligned}$$

Hence (cf. [1])

$$\begin{gathered} 2b-a^2=0,\qquad 2d+b^2-2ac=0,\qquad 2f+2bd-2ae-c^2=0,\\ 2bf+d^2-2ag-2ce=0,\qquad 2df-2cg-e^2=0,\\ f^2-2eg=A,\qquad -g^2=B. \end{gathered}$$

If $a=0$ we obtain $b=0$, $d=0$, $2f-c^2=0$, $2ce=0$, $2cg+e^2=0$, $e=0$, $AB=0$, contrary to $A, B\in K^*$.

If $a\neq 0$ we put $x_1=4c/a^3$, $y_1=16e/a^5-8c/a^3-16c^2/a^6+2$ and obtain

$$y_1^2=x_1^4+2x_1^3-6x_1^2+3x_1.$$

If $x_1=1$ we obtain $y_1=0$, $c=a^3/4$, $e=a^5/16$, $b=a^2/2$, $d=a^4/8$, $f=a^6/32$, $g=a^7/128$, $A=0$, contrary to $A\in K^*$.

If $x_1\neq 1$ we put

$$v=\frac{2x_1-1}{x_1-1},\qquad w=\frac{y_1}{(x_1-1)^2}$$

and using Lemma 41 obtain (66) with $v\neq 2$. Now (65) follows on taking $u=a/2(v-2)$.□

Lemma 48. *Let K be a field of characteristic different from 2, 7 and $A, B\in K^*$. The trinomial $x^{21}+Ax^7+B$ is reducible over K if and only if either x^3+Ax+B is reducible over K or*

$$A=2\cdot 7^{13}u^{14},\qquad B=7^{14}\left(\frac{7\pm\sqrt{21}}{2}\right)^7u^{21},\qquad u\in K \tag{67}$$

or

$$A=u^{14}A_{21,7}(v,w),\qquad B=u^{21}B_{21,7}(v,w), \tag{68}$$

where $u \in K$ and

$$\langle v, w\rangle \in E_{21,7}(K). \tag{69}$$

Proof. The conditions are sufficient since if (67) holds we have

$$x^{21} + Ax^7 + B = \prod_{i=0}^{6}\left(\zeta_7^{3i}x^3 + 7\zeta_7^{2i}ux^2 + 49\zeta_7^i u^2 x + 49u^3\left(\frac{7 \pm \sqrt{21}}{2}\right)\right).$$

If (68) and (69) hold, we have

$$\begin{aligned} x^{21} + Ax^7 + B = \prod_{i=0}^{6}\big(&\zeta_7^{3i}x^3 + 14\zeta_7^{2i}u(w - 7v - 343)x^2 \\ &+ 14\zeta_7^i u^2(w - 7v - 343)(v^2 - 98v - 1715)x \\ &+ 14u^3(w - 7v - 343)^2(-(49 + v)w + 21v^2 - 686v - 7203)\big). \end{aligned}$$

On the other hand, if $x^{21} + Ax^7 + B$ is reducible and $x^3 + Ax + B$ irreducible over K we have, by Lemma 29,

$$\begin{aligned} x^{21} + Ax^7 + B &= \prod_{i=0}^{6}(\zeta_7^{3i}x^3 + a\zeta_7^{2i}x^2 + b\zeta_7^i x + c) \\ &= x^{21} + (a^7 - 7a^5b + 7a^4c + 14a^3b^2 - 21a^2bc - 7ab^3 + 7ac^2 + 7b^2c)x^{14} \\ &\quad + (b^7 - 7b^5ac + 7b^4c^2 + 14b^3a^2c^2 - 21b^2ac^3 - 7ba^3c^3 + 7bc^4 + 7a^2c^4)x^7 + c^7. \end{aligned}$$

Hence

$$a^7 - 7a^5b + 7a^4c + 14a^3b^2 - 21a^2bc - 7ab^3 + 7ac^2 + 7b^2c = 0.$$

If $a = 0$, we have $bc = 0$ and $AB = 0$, contrary to $A, B \in K^*$.

If $a \neq 0$ we put

$$x_1 = 7\,\frac{b}{a^2}\,, \qquad y_1 = -98\,\frac{c}{a^3} - 49\,\frac{b^2}{a^4} + 147\,\frac{b}{a^2} - 49$$

and obtain

$$y_1^2 = x_1^4 - 14x_1^3 + 147x_1^2 - 686x_1 + 1029.$$

If $x_1 = 7$ we obtain $y_1 = \pm 7\sqrt{21}$, $b = a^2$, $c = \frac{7 \pm \sqrt{21}}{14}a^3$ and (67) follows on taking $u = a/7$.

If $x_1 \neq 1$ we put

$$\begin{aligned} v &= 2y_1 + 2x_1^2 - 14x_1 + 49, \\ w &= 4x_1y_1 - 14y_1 + 4x_1^3 - 42x_1^2 + 294x_1 - 686. \end{aligned}$$

By Lemma 41 we obtain (69) and $w - 7v - 343 \neq 0$. Hence (68) follows on taking $u = a/14(w - 7v - 343)$. □

5. Proof of Theorems 1, 2 and 3

Proof of Theorem 1. The theorem follows from Lemmas 26, 28 and 30–40. □

Proof of Theorem 2. For $n > 2m$ the theorem follows from Lemmas 27, 30–40 and 42–48. For $n = 2m$ it follows from Lemma 28. □

For the proof of Theorem 3 we need two lemmas.

Lemma 49. *Let L be a finite separable extension of $K(\boldsymbol{y})$ and let $L \cap \overline{K} = K_0$. Then* $[L : \overline{K}(\boldsymbol{y})] = [L : K_0(\boldsymbol{y})]$.

Proof. Let $L = K_0(\boldsymbol{y}, z)$ and let F be the minimal polynomial of z over $K_0(\boldsymbol{y})$, of degree d. Suppose that $[L : \overline{K}(\boldsymbol{y})] < [L : K_0(\boldsymbol{y})]$. Then F is reducible over $\overline{K}(\boldsymbol{y})$, hence over $K_1(\boldsymbol{y})$, where $[K_1 : K_0] < \infty$. Since the coefficients of any monic factor of F belong to the normal closure of L over $\overline{K}(\boldsymbol{y})$, which is separable over $\overline{K}(\boldsymbol{y})$, we may assume without loss of generality that K_1/K_0 is separable.

c [Here the following inclusion has been used

$$(*) \qquad K_0(\boldsymbol{y})^{\mathrm{sep}} \cap K_1(\boldsymbol{y}) \subset (K_0^{\mathrm{sep}} \cap K_1)(\boldsymbol{y}),$$

where K_0 is a subfield of K_1, $\boldsymbol{y} = \langle y_1, \ldots, y_r \rangle$ is a variable vector, K_0^{sep} and $K_0(\boldsymbol{y})^{\mathrm{sep}}$ is the separable closure of K_0 and $K_0(\boldsymbol{y})$, respectively.

Here is a proof of $(*)$ by induction on r. For $r = 0$ $(*)$ is obvious. Assume $(*)$ is true for $\boldsymbol{y}$ of $r-1$ coordinates and let

$$t \in K_0(\boldsymbol{y})^{\mathrm{sep}} \cap K_1(\boldsymbol{y}).$$

We have $F(\boldsymbol{y}, t) = 0$, where $F \in K_0[\boldsymbol{y}, T]$ and the discriminant $D(y)$ of $F(y, T)$ with respect to T is not zero. Let $a \in K_0[\boldsymbol{y}]$ be the leading coefficient of F with respect to T, so that

$$(**) \qquad G(\boldsymbol{y}, at) = 0,$$

where $G(\boldsymbol{y}, T) := a^{\deg_T F - 1} F(\boldsymbol{y}, T/a)$ is monic with respect to T. We have $at \in K_1[\boldsymbol{y}]$, hence

$$\binom{*}{**} \qquad at = \sum_{\nu=0}^{n} a_\nu y_r^{n-\nu}, \ a_\nu \in K_1[y_1, \ldots, y_{r-1}] \quad (0 \leqslant \nu \leqslant n).$$

Choose $n+1$ distinct elements $\eta_0, \ldots, \eta_n$ of K_0^{sep} such that

$$\binom{**}{**} \qquad a(y_1, \ldots, y_{r-1}, \eta_i) D(y_1, \ldots, y_{r-1}, \eta_i) \neq 0 \quad (0 \leqslant i \leqslant n).$$

Since by $(**)$ and $\binom{*}{**}$

$$G\Big(y_1, \ldots, y_{r-1}, \eta_i, \sum_{\nu=0}^{n} a_\nu \eta_i^{n-\nu}\Big) = 0$$

and, by $\binom{**}{**}$, the discriminant of $G(y_1, \dots, y_{r-1}, \eta_i, T)$ with respect to T is not zero, we have

$$\sum_{\nu=0}^{n} a_\nu \eta_i^{n-\nu} \in K_0(y_1, \dots, y_{r-1})^{\mathrm{sep}}.$$

Since $\det(\eta_i^{n-\nu}) \neq 0$ we have $a_\nu \in K_0(y_1, \dots, y_{r-1})^{\mathrm{sep}}$ $(0 \leqslant \nu \leqslant n)$. By the inductive assumption $a_\nu \in (K_0^{\mathrm{sep}} \cap K_1)(y_1, \dots, y_{r-1})$ $(0 \leqslant \nu \leqslant n)$ and by $(**)$

$$t \in \left(K_0^{\mathrm{sep}} \cap K_1\right)(\boldsymbol{y}). \,]$$

Then $K_1 = K_0(\vartheta)$. Let f be the minimal polynomial of ϑ over K_0. Then f is irreducible over L; indeed, the coefficients of its problematic monic factors over L would have to belong to $L \cap \overline{K} = K_0$. Hence

$$[L(\vartheta) : L] = [K_1 : K_0]$$

and since $L(\vartheta) = K_1(\boldsymbol{y}, z)$ we have

$$[K_1(\boldsymbol{y}, z) : K_0(\boldsymbol{y})] = [K_1(\boldsymbol{y}, z) : K_0(\boldsymbol{y}, z)][K_0(\boldsymbol{y}, z) : K_0(\boldsymbol{y})] = d[K_1 : K_0].$$

On the other hand, $[K_1(\boldsymbol{y}) : K_0(\boldsymbol{y})] = [K_1 : K_0]$, hence

$$\begin{aligned}[K_1(\boldsymbol{y}, z) : K_0(\boldsymbol{y})] &= [K_1(\boldsymbol{y}, z) : K_1(\boldsymbol{y})][K_1(\boldsymbol{y}) : K_0(\boldsymbol{y})] \\ &= [K_1(\boldsymbol{y}, z) : K_1(\boldsymbol{y})][K_1 : K_0].\end{aligned}$$

By comparison of the two above formulae,

$$[K_1(\boldsymbol{y}, z) : K_1(\boldsymbol{y})] = d,$$

hence F is irreducible over K_1. The obtained contradiction completes the proof. □

Lemma 50. *Under the assumptions of Theorem* 3, *if* $C_0 \in L^*$, $C_0 = c_1 C_1^q$, *where* $c_1 \in \overline{K}$, $C_1 \in \overline{K}L$, $q \not\equiv 0 \bmod \pi$ *then there exist* $c \in K_0$ *and* $C \in L^*$ *such that* $C_0 = cC^q$.

Proof. Let K_1 be the separable closure of K_0 in $\overline{K}$ and consider first the case where $c_1 \in K_1$ and $C_1 \in K_1 L$.

Since $K_0 = L \cap \overline{K}$ we have, by Lemma 49,

$$L = K_0(\boldsymbol{y}, z),$$

where z is a zero of a polynomial over $K_0(\boldsymbol{y})$ irreducible over $\overline{K}(\boldsymbol{y})$, of degree d, say.

Let $G = \mathrm{Gal}(K_1/K_0)$. We extend the action of G to $K_1 L$ by putting $\boldsymbol{y}^\sigma = \boldsymbol{y}$, $z^\sigma = z$ for all $\sigma \in G$.

We have

$$C_1 = \sum_{j=0}^{d-1} f_j z^j, \qquad f_j \in K_1(\boldsymbol{y}),$$

hence

$$C_1^\sigma = \sum_{j=0}^{d-1} f_j^\sigma z^j \qquad \text{for all } \sigma \in G.$$

On the other hand,

$$c_1^\sigma (C_1^\sigma)^q = C_0^\sigma = C_0 = c_1 C_1^q,$$

hence

$$C_1^\sigma = e_\sigma C_1, \qquad e_\sigma \in K_1.$$

Since z is of degree d over $K_1(\boldsymbol{y})$ we obtain

$$f_j^\sigma = e_\sigma f_j \qquad (0 \leqslant j < d).$$

Let i be the least index such that $f_i \neq 0$,

$$f_i = \frac{g}{h}, \qquad \text{where } g, h \in K_1[\boldsymbol{y}],$$

and let γ, χ be the coefficients of the first term in the inverse lexicographic order of g and h, respectively.

We have

$$\left(\frac{\gamma}{\chi}\right)^\sigma = e_\sigma \frac{\gamma}{\chi},$$

hence

$$\left(C_1 \frac{\chi}{\gamma}\right)^\sigma = C_1 \frac{\chi}{\gamma} \qquad \text{for all } \sigma \in G.$$

It follows that

$$C := C_1 \frac{\chi}{\gamma} \in L$$

and the assertion holds with $c = c_1(\gamma/\chi)^q$.

Consider now the general case. Since the extension $\overline{K}/K_1$ is purely inseparable there exists an exponent e such that $c_1^{\pi^e} \in K_1$ and $C_1^{\pi^e} \in K_1 L$.

Since $\pi \nmid q$ there exist integers r and s such that $\pi^e r - qs = 1$ and we obtain

$$C_0 = c_1^{\pi^e r} \left(\frac{C_1^{\pi^e r}}{C_0^s}\right)^q = c_2 C_2^q, \qquad \text{where } c_2 \in K_1,\ C_2 \in K_1 L.$$

The assertion follows by the already proved part of the lemma. □

Proof of Theorem 3. The condition given in the theorem is sufficient, since if

$$x^{n_1 q} + a x^{m_1 q} + b = f(x) g(x), \qquad f, g \in K_0[x] \setminus K_0,$$

we have

$$x^n + A x^m + B = C^{n_1 q} f\left(\frac{x^{(m,n)/q}}{C}\right) g\left(\frac{x^{(m,n)/q}}{C}\right).$$

On the other hand, $A^{-n} B^{n-m} \in \overline{K}$ implies $A^{-n} B^{n-m} \in K_0$,

$$A = a_0 C_0^{n_1 - m_1}, \qquad B = b_0 C_0^{n_1}, \qquad a_0, b_0 \in K_0, \qquad C_0 \in L,$$

and

$$C_0^{-n_1}(x^n + Ax^m + B) = \left(\frac{x^{(m,n)}}{C_0}\right)^{n_1} + a_0\left(\frac{x^{(m,n)}}{C_0}\right)^{m_1} + b_0.$$

Thus if $x^n + Ax^m + B$ is reducible over L we infer by Capelli's lemma that either $x^{n_1} + a_0x^{m_1} + b_0$ is reducible over L or else

$$\frac{x^{(m,n)}}{C_0} - \xi$$

is reducible over $L(\xi)$, where ξ is a zero of $x^{n_1} + a_0x^{m_1} + b_0$. In the former case the condition is satisfied with $a = a_0$, $b = b_0$, $C = C_0$, $q = 1$. In the latter case by Capelli's theorem there exists a $q \mid (m, n)$, $q = 4$ or a prime, such that

$$C_0 = c_1C_1^q, \qquad c_1 \in \{\xi^{-1}, -4\xi^{-1}\}, \qquad C_1 \in L(\xi),$$

and

$$\frac{x^q}{C_0} - \xi \quad \text{is reducible over } L(\xi).$$

By Lemma 50 we have $C_0 = cC^q$, $c \in K_0$, $C \in L$ and $x^q - c\xi$ is reducible over $L(\xi)$. This implies, again by Capelli's lemma, that $x^{n_1q} + a_0c^{n_1-m_1}x^{m_1q} + b_0c^{n_1}$ is reducible over L, hence over K_0 and the condition follows with $a = a_0c^{n_1-m_1}$, $b = b_0c^{n_1}$. □

6. Proof of Theorems 4 and 5

Proof of Theorem 4. According to Theorem 1, if $n \geqslant 2m$, $a \in K^*$, $B \in K(\boldsymbol{y}) \setminus K$ and $x^n + ax^m + B(\boldsymbol{y})$ is reducible over $K(\boldsymbol{y})$ we have either (i) or (ii). In case (i), no matter whether $n \geqslant 2m$ or $n < 2m$, if $x^{n_1} + ax^{m_1} + B(\boldsymbol{y})$ has a linear factor over $K(\boldsymbol{y})$, say $x - t$, $t \in K(\boldsymbol{y})$, we have $B(\boldsymbol{y}) = -t^{n_1} - at^{m_1}$. If $n_1 \geqslant 4$ and the factor is quadratic of the form $x^2 - t$, we find $t^{n_1/2} + at^{m_1/2} + B(\boldsymbol{y}) = 0 = (-1)^{n_1}t^{n_1/2} + (-1)^{m_1}t^{m_1/2} + B(\boldsymbol{y})$ and since at least one of the numbers n_1, m_1 is odd, we have $t^{1/2} \in K(\boldsymbol{y})$, hence $x^{n_1} + ax^{m_1} + B(\boldsymbol{y})$ has a linear factor over $K(\boldsymbol{y})$.

If $n_1 \geqslant 4$ and the quadratic factor has the middle coefficient different from zero we can write the factor in the form

$$x^2 - ux + u^2v = \left(x - u\,\frac{1 + \sqrt{1 - 4v}}{2}\right)\left(x - u\,\frac{1 - \sqrt{1 - 4v}}{2}\right), \qquad u, v \in K(\boldsymbol{y}),$$

and thus we obtain

$$u^{n_1}\left(\frac{1 \pm \sqrt{1 - 4v}}{2}\right)^{n_1} + au^{m_1}\left(\frac{1 \pm \sqrt{1 - 4v}}{2}\right)^{m_1} + B(\boldsymbol{y}) = 0,$$

whence

$$a = -u^{n_1-m_1}\,\frac{f_{n_1}(v)}{f_{m_1}(v)}, \qquad B(\boldsymbol{y}) = u^{n_1}v^{m_1}\,\frac{f_{n_1-m_1}(v)}{f_{m_1}(v)}.$$

The first of the above equations implies that the irreducible curve it describes is of genus 0. We have

$$f_k(v) = \text{const} \prod_{j=1}^{[(k-1)/2]} \left(v - \frac{1}{2 + 2\cos(2j\pi/k)} \right) \tag{70}$$

hence $(f_{m_1}, f_{n_1}) = 1$ and the condition on the genus implies that either $n_1 - m_1 = 1$ or

$$\left[\frac{n_1 - 1}{2} \right] = 1 \tag{71}$$

or $n_1 - m_1 = 2$ and $\left[\frac{n_1-1}{2}\right] + \left[\frac{m_1-1}{2}\right] = 2$. The last condition gives $2\left[\frac{n_1-1}{2}\right] = 3$, which is impossible, hence we have either $n_1 - m_1 = 1$ or, from (71), $n_1 = 4$, $m_1 = 1$. In the first case we take $t = v$ and obtain

$$u = -a \frac{f_{n_1-1}(t)}{f_{n_1}(t)}, \qquad B = \frac{u^{n_1} t^{n_1-1}}{f_{n_1-1}(t)} = (-a)^{n_1} t^{n_1-1} \frac{f_{n_1-1}(t)^{n_1-1}}{f_{n_1}(t)^{n_1}}.$$

In the second case we take $t = u^{-1}$ and find $B = B^*_{4,1}(t)$.

In case (ii) we infer that the curve $a = u^{\nu-\mu} A_{\nu,\mu}(v)$ must have at least one irreducible component of genus 0. Examining all the 13 cases we find that this condition is satisfied if and only if $\langle \nu, \mu \rangle = \langle 4, 2 \rangle$, $\langle 6, 2 \rangle$ or $\langle 6, 3 \rangle$.

In each case we take $t = u$ and obtain

- for $\langle \nu, \mu \rangle = \langle 4, 2 \rangle$,

$$v = \frac{t^2 + a}{2t^2}, \qquad B = u^4 v^2 = B^*_{4,2}(t);$$

- for $\langle \nu, \mu \rangle = \langle 6, 2 \rangle$,

$$v = \frac{-4t^4 + a}{4t^4}, \qquad B = -u^6 v^2 = B^*_{6,2}(t);$$

- for $\langle \nu, \mu \rangle = \langle 6, 3 \rangle$,

$$v = \frac{t^3 + a}{3t^3}, \qquad B = u^6 v^3 = B^*_{6,3}(t).$$

It remains to consider the case where $n < 2m$ and $x^{n_1} + ax^{m_1} + B(\boldsymbol{y})$ has no proper linear or quadratic factor. Then

$$x^{n_1} + \frac{a}{B(\boldsymbol{y})} x^{n_1-m_1} + \frac{1}{B(\boldsymbol{y})}$$

satisfies (ii), hence there exists an integer l and $\langle \nu, \mu \rangle \in S_0$ such that $n = \nu l$, $n - m = \mu l$ and

$$\frac{a}{B(\boldsymbol{y})} = u^{\nu-\mu} A_{\nu,\mu}(v), \qquad \frac{1}{B(\boldsymbol{y})} = u^{\nu} B_{\nu,\mu}(v), \qquad u, v \in K(\boldsymbol{y}).$$

It follows that $au^\mu = A_{\nu,\mu}(v)/B_{\nu,\mu}(v)$ and thus the curve in question has at least one irreducible component of genus 0. Examining all the 13 cases we find that this holds if and only if $\langle \nu, \mu\rangle = \langle 6, 1\rangle,\ \langle 6, 2\rangle,\ \langle 7, 1\rangle$ or $\langle 8, 2\rangle$.

If $\langle \nu, \mu\rangle = \langle 6, 1\rangle$ or $\langle 7, 1\rangle$ we take $t = v$ and obtain

$$u = \frac{A_{\nu,\mu}(t)}{aB_{\nu,\mu}(t)}, \qquad B = u^{-\nu}B_{\nu,\mu}(v)^{-1} = B^*_{\nu,\nu-\mu}(t).$$

If $\langle \nu, \mu\rangle = \langle 6, 2\rangle$ we take $t = uv$ and obtain

$$v = -\frac{at^2+4}{4}, \qquad u = \frac{-4t}{at^2+4}, \qquad B = -u^{-6}v^{-2} = B^*_{6,4}(t).$$

Finally, if $\langle \nu, \mu\rangle = \langle 8, 2\rangle$ and

$$au^2 = \frac{-v^2+8v-8}{(2v-2)^2}$$

we have

$$a = \Big(\frac{v}{u(2v-2)}\Big)^2 - 2\Big(\frac{v-2}{u(2v-2)}\Big)^2,$$

hence

$$a = \alpha^2 - 2\beta^2, \qquad \alpha, \beta \in K.$$

Taking

$$t = \frac{(v-2) - \beta u(2v-2)}{v - \alpha u(2v-2)}$$

we find

$$\frac{v}{u(2v-2)} = \alpha + \frac{2\alpha - 4\beta t}{2t^2-1}, \qquad \frac{v-2}{u(2v-2)} = \beta + t\,\frac{2\alpha - 4\beta t}{2t^2-1},$$

hence

$$u^{-1} = \alpha + \beta + (t+1)\frac{2\alpha - 4\beta t}{2t^2-1}, \qquad v^{-1} = \Big(2\Big(\alpha + \frac{2\alpha - 4\beta t}{2t^2-1}\Big)u - 1\Big)^{-1},$$

$$B = u^{-8}(2v-2)^{-2} = B^*_{8,6}(t). \qquad \square$$

Proof of Theorem 5. According to Theorem 1, if $n \geqslant 2m$, $A \in K(\boldsymbol{y}) \setminus K$, $b \in K^*$ and $x^n + A(\boldsymbol{y})x^m + b$ is reducible over $K(\boldsymbol{y})$ we have either (i) or (ii). In case (i) if $x^{n_1} + A(\boldsymbol{y})x^{m_1} + b$ has a linear factor over $K(\boldsymbol{y})$, say $x - t$, $t \in K(\boldsymbol{y})^*$, we have $A(\boldsymbol{y}) = -t^{n_1-m_1} - bt^{-m_1}$. If $n_1 \geqslant 4$ and the factor in question is quadratic of the form $x^2 - t$ we find

$$t^{n_1/2} + A(\boldsymbol{y})t^{m_1/2} + b = 0 = (-1)^{n_1}t^{n_1/2} + A(\boldsymbol{y})(-1)^{m_1}t^{m_1/2} + b$$

and since at least one of the numbers n_1, m_1 is odd, we have $t^{1/2} \in K(\boldsymbol{y})$, hence $x^{n_1} + A(\boldsymbol{y})x^{m_1} + b$ has a linear factor over $K(\boldsymbol{y})$.

If $n_1 \geqslant 4$ and the quadratic factor has the middle coefficient different from zero we can write the factor in the form $x^2 - ux + u^2 v$ and thus we obtain

$$u^{n_1}\left(\frac{1 \pm \sqrt{1-4v}}{2}\right)^{n_1} + A(\boldsymbol{y})u^{m_1}\left(\frac{1 \pm \sqrt{1-4v}}{2}\right)^{m_1} + b = 0,$$

whence

$$A(\boldsymbol{y}) = -u^{n_1-m_1}\,\frac{f_{n_1}(v)}{f_{m_1}(v)}\,, \qquad b = u^{n_1}v^{m_1}\,\frac{f_{n_1-m_1}(v)}{f_{m_1}(v)}\,.$$

The second of the above equations implies that the irreducible curve it describes is of genus 0. In view of the formula (70) we have $\big(f_{m_1}(v),\, v f_{n_1-m_1}(v)\big) = 1$ and the condition on the genus implies that

$$m_1 + \left[\frac{n_1 - m_1}{2}\right] = 1,$$

which is impossible for $n_1 \geqslant 4$.

In the case (ii) we infer that the curve $b = u^{\nu} B_{\nu,\mu}(v)$ must have at least one irreducible component of genus 0. Examining all the 13 cases we find that this condition is fulfilled if and only if $\langle \nu, \mu\rangle = \langle 2p,\, p\rangle$ (p a prime), $\langle 6, 2\rangle$, $\langle 8, 2\rangle$, $\langle 8, 4\rangle$, $\langle 9, 3\rangle$.

- If $\langle \nu, \mu\rangle = \langle 2p,\, p\rangle$ we have $b = (u^2 v)^p$, hence
$$b_1 := u^2 v \in K(\boldsymbol{y}) \cap \overline{K} = K, \qquad v = b_1 u^{-2}.$$
- If $\langle \nu, \mu\rangle = \langle 6, 2\rangle$ we have $b = -(u^3 v)^2$, hence
$$b_1 := u^3 v \in K(\boldsymbol{y}) \cap \overline{K} = K, \qquad v = b_1 u^{-3}.$$
- If $\langle \nu, \mu\rangle = \langle 8, 2\rangle$ we have $b = (u^4(2v-2))^2$, hence
$$b_1 := u^4(2v-2) \in K(\boldsymbol{y}) \cap \overline{K} = K, \qquad v = 1 + \frac{b_1}{2u^4}\,.$$
- If $\langle \nu, \mu\rangle = \langle 8, 4\rangle$ we have $b = (u^2 v)^4$, hence
$$b_1 := u^2 v \in K(\boldsymbol{y}) \cap \overline{K} = K, \qquad v = b_1 u^{-2}.$$
- If $\langle \nu, \mu\rangle = \langle 9, 3\rangle$ we have $b = (3u^2(v-3))^3$, hence
$$b_1 := 3u^3(v-3) \in K(\boldsymbol{y}) \cap \overline{K} = K, \qquad v = 3 + \frac{b_1}{3u^3}\,.$$

In every case we take $t = u$ and obtain

$$A(\boldsymbol{y}) = u^{\nu-\mu} A_{\nu,\mu}(v) = A^*_{\nu,\mu}(t, b_1). \qquad \square$$

PART II

Reducibility over algebraic number fields and, in particular, over $\mathbb{Q}$

7. Proof of Theorem 6 and of the subsequent remarks

Proof of Theorem 6. We begin by defining the sets $F_{\nu,\mu}(K)$ for $\nu \geqslant 2\mu$. This is done in several steps. First we put $q = (\mu, \nu)$, $\nu_1 = \nu/q$, $\mu_1 = \mu/q$, choose the least non-negative integers ϱ, σ satisfying the equation $\sigma(\nu_1 - \mu_1) - \varrho\nu_1 = 1$ and introduce fields $L(k, \mu_1, \nu_1)$ and $M(\mu_1, \nu_1, q)$. Let $L(k, \mu_1, \nu_1) = K(t, y)$, where y is integral over $K[t]$ with the discriminant $D(t)$. By Lemma 19 the function $(y_{1q} + \ldots + y_{\nu_1 q})^q$ generating $M(\mu_1, \nu_1, q)$ over $K(t)$ is determined up to a conjugacy. Let ϕ be its minimal polynomial over $K[t]$. We put

$$S_{\nu,\mu}(K) = \begin{cases} \bigcup\limits_{2<k\leqslant\nu_1/2, g^*(k,\mu_1,\nu_1)>1} \{t_0 \in K : \\ D(t_0) = 0 \text{ or } t - t_0 \text{ has in } L(k, \mu_1, \nu_1) \\ \text{a prime divisor of degree 1}\} & \text{if } q = 1, \\ \{\langle t_0, u_0\rangle \in K^2 : \text{there exists} \\ \text{a prime divisor } \mathfrak{p} \text{ of } M(\mu_1, \nu_1, q) \\ \text{such that } t \equiv t_0 \bmod \mathfrak{p}, \\ (y_{1q} + \ldots + y_{\nu_1 q})^q \equiv u_0 \bmod \mathfrak{p}\}, & \text{if } q > 1,\ g_*(\mu_1, \nu_1, q) > 1, \\ \emptyset & \text{otherwise.} \end{cases}$$

It follows from Lemmas 4 and 19 that $[L(k, \mu_1, \nu_1) : K(t)] = [L^*(k, \mu_1, \nu_1) : \overline{K}(t)]$ and $[M(\mu_1, \nu_1, q) : K(t)] = [M_*(\mu_1, \nu_1, q) : \overline{K}(t)]$, hence K is the exact constant field of $L(k, \mu_1, \nu_1)$ and $M(\mu_1, \nu_1, q)$. Therefore the conditions $t \equiv t_0$, $(y_{1q} + \ldots + y_{\nu_1 q})^q \equiv u_0 \bmod \mathfrak{p}$, $\langle t_0, u_0\rangle \in K^2$ imply that either $\mathfrak{p}$ is of degree 1 or $\langle t_0, u_0\rangle$ is a singular point of $\phi = 0$. By the Faltings theorem there are only finitely many prime divisors of degree 1 in $L(k, \mu_1, \nu_1)$ or $M(\mu_1, \nu_1, q)$ if $g^*(k, \mu_1, \nu_1) > 1$ or $g_*(\mu_1, \nu_1, q) > 1$, respectively. Hence the sets $S_{\nu,\mu}(K)$ are finite.

Now we introduce auxiliary sets

$$T_{\nu,\mu}(K) = \begin{cases} \bigcup\limits_{t_0\in S_{\nu,\mu}(K)} \{\langle t_0^{\varrho}, t_0^{\sigma}\rangle\} & \text{if } q = 1, \\ \bigcup\limits_{\langle t_0,u_0\rangle\in S_{\nu,\mu}(K)} \{\langle t_0^{\varrho} u_0^{(\mu-\nu)/q}, t_0^{\sigma} u_0^{-\nu/q}\rangle\} & \text{if } q \text{ is a prime}, \\ \bigcup\limits_{\langle t_0,u_0\rangle\in S_{\nu,\mu}(K)} \{\langle t_0^{\varrho} (-u_0/4)^{(\mu-\nu)/4}, t_0^{\sigma} (-u_0/4)^{-\nu/4}\rangle\} & \text{if } q = 4, \\ \emptyset & \text{otherwise.} \end{cases}$$

[The formulae make sense only for $u_0 \neq 0$. The argument for $u_0 = 0$ is given at the end of D13 (page 604 in this volume).]

Finally, we put

$$F_{\nu,\mu}(K) = \begin{cases} \{\langle a,b\rangle \in T_{\nu,\mu}(K) : x^\nu + ax^\mu + b \text{ is reducible over } K\} \\ \qquad\qquad \text{if } \langle \nu,\mu\rangle \notin S_0 \cup S_1, \text{ or } \langle \nu,\mu\rangle = \langle 9,1\rangle,\ \sqrt{13} \notin K, \\ \{\langle a,b\rangle \in T_{9,1}(K) : x^9 + ax + b \text{ is reducible over } K\} \cup \\ \bigcup\limits_{\varepsilon=\pm 1} \big\{\big\langle -480053919711226727 + \varepsilon 66936076602084894\sqrt{13}, \\ \qquad \tfrac{1}{2}(-57126885878317063725 + \varepsilon 66644985243629014605\sqrt{13})\big\rangle\big\}, \\ \qquad\qquad \text{if } \langle \nu,\mu\rangle = \langle 9,1\rangle,\ \sqrt{13} \in K, \\ \left\{\left\langle 2\cdot 7^{13},\ 7^{14}\left(\frac{7+\sqrt{21}}{2}\right)^7\right\rangle, \left\langle 2\cdot 7^{13},\ 7^{14}\left(\frac{7-\sqrt{21}}{2}\right)^7\right\rangle\right\}, \\ \qquad\qquad \text{if } \langle \nu,\mu\rangle = \langle 21,7\rangle,\ \sqrt{21} \in K, \\ \emptyset \qquad\qquad \text{otherwise.} \end{cases}$$

Since the sets $S_{\nu,\mu}(K)$ are finite, so are the sets $F_{\nu,\mu}(K)$. We proceed to prove that they have all the other properties asserted in the theorem.

Assume that $x^n + ax^m + b$ is reducible over K. There are two possibilities:

$$x^{n_1} + ax^{m_1} + b \quad \text{is reducible over } K \tag{72}$$

and

$$x^{n_1} + ax^{m_1} + b \quad \text{is irreducible over } K. \tag{73}$$

In the case (72), $x^{n_1} + ax^{m_1} + b$ has a proper factor over K of degree $k \leqslant n_1/2$. If $k \leqslant 2$ we have (vi). If $k > 2$ and $g^*(k, m_1, n_1) \leqslant 1$, by Lemmas 15 and 30, 31, 42–46 we have (vii) or (viii) with $l = (m,n)$, $\nu = n_1$, $\mu = m_1$ or one of the exceptional cases (51), (56), (59), (62) with $A = a$, $B = b$. In the cases (51), (56), (59), $x^{n_1} + ax^{m_1} + b$ has the linear factor $x - u \in K[x]$, hence (vi) holds. In the case (62) we obtain (ix) with $l = (m,n)$, $\nu = 9$, $\mu = 1$ by the definition of $F_{\nu,\mu}(K)$.

Now, suppose that $k > 2$ and $g^*(k, m_1, n_1) > 1$. Then by Lemma 15, $\langle n_1, m_1\rangle \notin S_0 \cup S_1 \setminus \{\langle 9,1\rangle\}$. Put

$$t_0 = a^{-n_1} b^{n_1 - m_1}. \tag{74}$$

If r, s are the least non-negative integers satisfying $s(n_1 - m_1) - rn_1 = 1$, by the identity (22) the trinomial $x^{n_1} + t_0^r x^{m_1} + t_0^s$ has a factor of degree k over K. Hence there exists a prime divisor $\mathfrak{P}$ of $L^*(k, m_1, n_1)$ such that $t \equiv t_0$, $y \equiv y_0 \bmod \mathfrak{P}$, where $L^*(k, m_1, n_1) = \overline{K}(t, y)$ and $y_0 \in K$. Let $\mathfrak{p}$ be a prime divisor of $L(k, m_1, n_1)$ divisible by $\mathfrak{P}$. Since $t_0, y_0 \in K$, either $\mathfrak{p}$ is of degree 1 or $D(t_0) = 0$. Thus $t_0 \in S_{n_1,m_1}(K)$, $\langle t_0^r, t_0^s\rangle \in F_{n_1,m_1}(K)$ and (ix) holds with $l = (m,n)$, $\nu = n_1$, $\mu = m_1$, $a_0 = t_0^r$, $b_0 = t_0^s$, $u = a^s b^{-r}$.

In the case (73) by Capelli's lemma

$$x^{(m,n)} - \xi \quad \text{is reducible over } K(\xi),$$

where $\xi^{n_1} + a\xi^{m_1} + b = 0$.

Further, by Capelli's theorem, there exists a $q \mid (m,n)$ such that either q is a prime and $\xi = \eta^q$, $\eta \in K(\xi)$ or $q = 4$ and $\xi = -4\eta^4$, $\eta \in K(\xi)$. In both cases

$$x^{n_1 q} + ax^{m_1 q} + b \quad \text{is reducible over } K. \tag{75}$$

If $g_*(m_1, n_1, q) \leqslant 1$, by Lemmas 25 and 31, 33–40, 47, 48 we have either (vii) or (viii) with $l = (m,n)/q$, $\nu = n_1 q$, $\mu = m_1 q$ or (67) with $A = a$, $B = b$. In the last case we have (ix) with $l = (m,n)/7$, $\nu = 21$, $\mu = 7$, by the definition of $F_{\nu,\mu}(K)$.

Now, suppose that $g_*(m_1, n_1, q) \geqslant 2$ and (74) holds. Then by Lemma 25, $\langle n_1 q, m_1 q\rangle \notin S_0 \cup S_1$. If $\eta_1, \ldots, \eta_{n_1}$ are all the conjugates of η over K we have

$$x^{n_1} + ax^{m_1} + b = \begin{cases} \prod_{i=1}^{n_1} (x - \eta_i^q) & \text{if } q \text{ is a prime,} \\ \prod_{i=1}^{n_1} (x + 4\eta_i^4) & \text{if } q = 4, \end{cases}$$

and by (22),

$$x^{n_1} + t_0^r x^{m_1} + t_0^s = \begin{cases} \prod_{i=1}^{n_1} (x - a^{-s} b^r \eta_i^q) & \text{if } q \text{ is a prime,} \\ \prod_{i=1}^{n_1} (x + 4a^{-s} b^r \eta_i^4) & \text{if } q = 4. \end{cases}$$

Hence there exists a prime divisor $\mathfrak{P}$ of $M_*(m_1, n_1, q)$ such that

$$t \equiv t_0, \qquad (y_{1q} + \ldots + y_{n_1 q})^q \equiv u_0 \bmod \mathfrak{P},$$

where

$$u_0 = \begin{cases} a^{-s} b^r (\eta_1 + \ldots + \eta_{n_1})^q & \text{if } q \text{ is a prime,} \\ -4a^{-s} b^r (\eta_1 + \ldots + \eta_{n_1})^4 & \text{if } q = 4. \end{cases} \tag{76}$$

Let $\mathfrak{p}$ be a prime divisor of $M(m_1, n_1, q)$ divisible by $\mathfrak{P}$. Since $t_0, u_0 \in K$ we have

$$t \equiv t_0, \qquad (y_{1q} + \ldots + y_{n_1 q})^q \equiv u_0 \bmod \mathfrak{p}.$$

Hence $\langle t_0, u_0\rangle \in S_{n_1 q, m_1 q}$ and

$$\begin{aligned} &\langle t_0^r u_0^{m_1 - n_1}, t_0^s u_0^{-n_1}\rangle \in T_{\nu,\mu}(K) \qquad \text{if } q \text{ is a prime,} \\ &\left\langle t_0^r \left(\frac{-u_0}{4}\right)^{m_1 - n_1}, t_0^s \left(\frac{-u_0}{4}\right)^{-n_1} \right\rangle \in T_{\nu,\mu}(K) \qquad \text{if } q = 4. \end{aligned} \tag{77}$$

By (74) and (76) the above pairs equal

$$\langle a(\eta_1 + \ldots + \eta_{n_1})^{qm_1 - qn_1}, b(\eta_1 + \ldots + \eta_{n_1})^{-qn_1}\rangle$$

and since

$$\begin{aligned} &x^{qn_1} + a(\eta_1 + \ldots + \eta_{n_1})^{qm_1 - qn_1} x^{m_1 q} + b(\eta_1 + \ldots + \eta_{n_1})^{-qn_1} \\ &\quad = (\eta_1 + \ldots + \eta_{n_1})^{-qn_1} \big((x(\eta_1 + \ldots + \eta_{n_1}))^{qn_1} + a(x(\eta_1 + \ldots + \eta_{n_1}))^{qm_1} + b\big) \end{aligned}$$

$T_{\nu,\mu}(K)$ can be replaced in (77) by $F_{\nu,\mu}(K)$, by virtue of (75). Thus (ix) holds with

$$l = \frac{(m,n)}{q}, \qquad \nu = n_1 q, \qquad \mu = m_1 q, \qquad u = \eta_1 + \ldots + \eta_{n_1}.$$

Assume now that one of the cases (vi)–(ix) holds. (vi) and (ix) imply the reducibility of $x^n + ax^m + b$ in an obvious way, and so do (vii) and (viii) by Lemmas 30–40 and 42–48, respectively.

The proof of Theorem 6 is complete. □

The remark following Theorem 6 can be summarized as

Lemma 51. *For $\langle \nu, \mu \rangle \in S_1$ the sets $E_{\nu,\mu}(\mathbb{Q})$ are infinite, except that*

$$E_{7,2}(\mathbb{Q}) = \{\langle -4, 4\rangle, \langle -4, -4\rangle\}, \qquad E_{21,7}(\mathbb{Q}) = \{\langle -49, 0\rangle\}.$$

Proof. The curve $E_{7,2}$ is equivalent via an affine transformation to a curve listed in the tables [17a] as curve 35A (I owe this information to Professor Karl Rubin). The curves $E_{7,3}$, $E_{9,1}$ and $E_{14,2}$ have rational points of infinite order $\langle 3, 108\rangle$, $\langle 16, 62\rangle$ and $\langle 5, 10\rangle$, respectively. Also the two curves to be taken as $E_{8,1}$, namely $w^2 = v^3 - 10v + 12$ and $w^2 = v^3 - 20v - 16$ have rational points of infinite order $\langle 3, 3\rangle$ and $\langle 5, 3\rangle$, respectively. It remains to find all rational points on the curve

$$E_{21,7} : w^2 = v^3 - 1715v + 33614.$$

The discriminant of the cubic on the right hand side is $-2^8 \cdot 7^9$ and using Nagell's theorem (see [4], Theorem 22.1) we easily find that the only rational point of finite order is $\langle -49, 0\rangle$. In order to show that there are no rational points of infinite order we notice that by Lemma 41 the curve $E_{21,7}$ is birationally equivalent over $\mathbb{Q}$ to the curve

$$y^2 = x^4 + 294x^2 - 343.$$

By Theorem 8 of [19] the number of generators of infinite order of the group of rational points on the above curve equals $\varrho_1 + \varrho_2 - 2$ where 2^{ϱ_1} is the number of solvable equations

$$s(x^4 - 588sx^2y^2 + s^2 \cdot 87808y^4) = z^2 \tag{78}$$

and 2^{ϱ_2} the number of solvable equations

$$t(t^2x^4 + 294tx^2y^2 - 343y^4) = z^2 \tag{79}$$

where s and t run through the square-free divisors of 87808 and of 343 respectively. The left hand side of (78) is negative for negative s, hence the only relevant values of s are 1, 2, 7 and 14, while the relevant values of t are ± 1, ± 7. For $s = 1$ and 7 the equation (78) has solutions $\langle x, y, z\rangle = \langle 1, 0, 1\rangle$ and $\langle 0, 1, 5488\rangle$, respectively. For $t = 1$ and -7 the equation (79) has solutions $\langle 1, 0, 1\rangle$ and $\langle 0, 1, 49\rangle$, respectively. However, (78) for $s = 2$ and (79) for $t = -1$ are insoluble in $\mathbb{Z}_2$ hence $\varrho_1 = \varrho_2 = 1$ and $\varrho_1 + \varrho_2 - 2 = 0$. □

8. Deduction of Consequences 1–3 from Conjecture

Consequence 1 is immediate. In order to deduce Consequence 2 we prove

Lemma 52. *For every field K and every polynomial $f \in K[x]$ of degree d, $f(x^n)$ has over K an irreducible factor with at most $2d+1$ non-zero coefficients.*

Remark. A special case of this lemma with $K = \mathbb{Q}$ and $d = 1$ was proved in [21].

Proof. Let $h(x)$ be a factor of $f(x)$ irreducible over $K(\zeta_4)$, let $h(\xi) = 0$ and let e be the maximal exponent dividing n such that $\xi = \eta^e$, $\eta \in K(\zeta_4, \xi)$. By Capelli's theorem $x^{n/e} - \eta$ is irreducible over $K(\zeta_4, \xi)$, hence by Capelli's lemma

$$g(x) = N_{K(\zeta_4,\xi)/K(\zeta_4)}(x^{n/e} - \eta)$$

is irreducible over $K(\zeta_4)$, divides $f(x^n)$ and has at most $[K(\zeta_4, \xi) : K(\zeta_4)] + 1 \leqslant d + 1$ non-zero coefficients. If $g \in K[x]$ we have more than asserted. If $g(x) \notin K[x]$, g and its conjugate $\overline{g}$ over K are coprime and $f_1 = g\overline{g} \in K[x]$ is irreducible over K. Moreover, the number of non-zero coefficients of f_1 does not exceed $2d + 1$. □

Deduction of Consequence 2. Suppose that $x^n + ax^m + b$ is reducible over K. Then by Consequence 1, $n_1 \leqslant C_1(K)$ or $x^{n_1} + ax^{m_1} + b$ has a factor of degree $\leqslant 2$. Hence by Lemma 52, $x^n + ax^m + b = (x^{(m,n)})^{n_1} + a(x^{(m,n)})^{m_1} + b$ has an irreducible factor with at most $2C_1(K) + 1$ non-zero coefficients. Hence one can take $C_2(K) = 2C_1(K) + 1$. □

From this point onwards reducibility means reducibility over $\mathbb{Q}$. In order to deduce Consequence 3 we show

Lemma 53. *The trinomial $x^n + bx^m \pm 1$, where $(n, m) = 1$, $n > 2$, $b \in \mathbb{Z}$, $|b| > 2$, has no linear or quadratic factor.*

Proof. In view of symmetry we may assume $n < 2m, m > 1$. Linear factors being excluded by $|b| > 2$ we write a supposed quadratic factor as $(x-\alpha)(x-\beta)$, where α, β are conjugate units. It follows that

$$b = \frac{\alpha^n - \beta^n}{\beta^m - \alpha^m}$$

and since $(\alpha^n - \beta^n, \alpha^m - \beta^m) = (\alpha^{(m,n)} - \beta^{(m,n)}) = \alpha - \beta$ and $b \in \mathbb{Z}$ we obtain

$$\frac{\alpha^m - \beta^m}{\alpha - \beta} = \pm 1. \tag{80}$$

Since $|b| > 2$, α and β cannot be roots of unity, thus they are real and

$$\max\{|\alpha|, |\beta|\} \geqslant \frac{1+\sqrt{5}}{2}, \qquad \min\{|\alpha|, |\beta|\} \leqslant \frac{\sqrt{5}-1}{2}.$$

Hence (80) implies $m = 2$, $n = 3$ and the existence of a quadratic factor would imply the existence of a linear factor, a contradiction. □

Deduction of Consequence 3. By Theorem 6, Lemma 53 and Conjecture the existence of infinitely many integers b with $x^n + bx^m \pm 1$ reducible for some $n \neq 2m$ would imply the existence of fixed $n \neq 2m$ and infinitely many integers b with $x^n + bx^m + 1$ reducible. This, however, is impossible by Theorem 8, since for $a = c = 1$ the condition $b_1^2 = -c/a$ is not satisfied by any rational b_1. □

Remark. The proof of Theorem 8 to be given in §9 is independent of the present section, thus there is no danger of a vicious circle.

9. Proof of Theorems 7 and 8

Lemma 54. *If $g(t) \in \mathbb{Q}(t)$ takes infinitely many integer values for rational values of t, then*

$$\text{either } g \in \mathbb{Q}[t] \quad \text{or} \quad g(t) = \frac{P(t)}{Q(t)}, \ P, Q \in \mathbb{Q}[t], \ \deg P \leqslant \deg Q, \tag{81}$$

where Q is a power of a linear polynomial or of an irreducible quadratic polynomial with a positive discriminant.

Proof. This is the result of [13]. □

Lemma 55. *Let $F \in \mathbb{Q}[x, y] \setminus \mathbb{Q}$. There exists a finite (possibly empty) subset $S(F)$ of $\mathbb{Q}(t)$ with the following properties*:

(82) *If $g \in S(F)$ then $F(x, g(t))$ has a zero in $\mathbb{Q}(t)$ and* (81) *holds.*

(83) *The set of integers $y^* \notin \bigcup_{g \in S(F)} g(\mathbb{Q})$ such that $F(x, y^*)$ has an integer zero is finite.*

Proof. Assume first that F is irreducible over $\mathbb{C}$. If the genus of the curve $F(x, y) = 0$ is positive we take $S(F) = \emptyset$ and (83) follows from Siegel's theorem. If the genus is zero, by the Hilbert–Hurwitz theorem all but finitely many rational points on the curve are given by $x^* = f(t^*)$, $y^* = g(t^*)$, $f, g \in \mathbb{Q}(t)$, where $t^* \in \mathbb{Q}$. We take $S(F) = \{g(t)\}$ if g satisfies (81), $S(F) = \emptyset$ otherwise and (83) follows from Lemma 54.

Assume now that F is reducible over $\mathbb{C}$, but irreducible over $\mathbb{Q}$. Then the number of rational points on $F(x, y)$ is finite (see [4], p. 196), hence it suffices to take $S = \emptyset$.

Assume finally that $F = \prod_{i=1}^{k} F_i$, where F_i are irreducible over $\mathbb{Q}$. Then we take $S(F) = \bigcup_{i=1}^{k} S(F_i)$. □

Lemma 56. *Let $F \in \mathbb{Q}[x, y]$ be irreducible over $\mathbb{Q}$. Then there exists a finite (possibly empty) subset $R(F)$ of $\mathbb{Q}(t)$ with the following properties*:

(84) *If $g \in R(F)$ then $F(x, g(t))$ is reducible over $\mathbb{Q}(t)$ and* (81) *holds.*

(85) *The set of integers $y^* \notin \bigcup_{g \in R(F)} g(\mathbb{Q})$ such that $F(x, y^*)$ is reducible over $\mathbb{Q}$ is finite.*

c *Proof.* This follows from Lemma 55 in the same way as Theorem 33 of [26] follows from Lemma 1 there for $K = \mathbb{Q}$, $r = s = 1$. □

Remark. Similar results are stated without proof by M. Fried: in [9] in the special case $F(x, y) = f(x)-y$, in [10] in general. In the former case the possibility $g \notin \mathbb{Q}[t]$ is omitted by mistake (acknowledged in [10], p. 600), in the latter case the condition $\deg P \leqslant \deg Q$ in (81) is replaced by $\deg P = \deg Q$, the possibility of Q being a power of a linear form is omitted and there is no restriction on the discriminant of Q. These changes are permissible, since if Q is a power of a linear form, we may replace g by $g(a + t^{-1})$, where $Q(a) = 0$; if Q is a power of an irreducible quadratic form and $\deg P \leqslant \deg Q$, we may replace g by $g(a + t^{-1})$, where $P(a) \neq 0$.

Proof of Theorem 7. Applying Lemma 56 with $F(x, y) = ax^n + bx^m + y$ we infer from (84) and Theorem 4 that if $n_1 = 5$, $m_1 = 4$ then

$$R(F) = \left\{-at^5 - bt^4,\ a\Big(\frac{b}{a}\Big)^5 \frac{t^2(t-2)^4}{(t^2-3t+1)^5}\right\};$$

if $n_1 = 2$, $m_1 = 1$ and $2 \mid (m, n)$ then

$$R(F) = \left\{-at^2 - bt,\ a\Big(\frac{at^2+b}{2a}\Big)^2\right\};$$

if $n_1 = 4$, $m_1 = 3$ and $2 \mid (m, n)$ then

$$R(F) = \Bigg\{-at^4 - bt^3,$$
$$a\,\frac{\big((2\alpha-2\beta)t^2+(2\alpha-4\beta)t+(\alpha-\beta)\big)^6\big((2\alpha+2\beta)t^2-(2\alpha+4\beta)t+(\alpha+\beta)\big)^2}{4(2t^2-1)^8}\Bigg\},$$

where $\alpha^2 - 2\beta^2 = b/a$, $\alpha, \beta \in \mathbb{Q}$ fixed; otherwise

$$R(F) = \left\{-at^{n_1} - bt^{m_1}\right\}$$

and (85) implies the theorem. The only point which requires a proof is that the function

$$g(t) = \left(-\frac{b}{a}\right)^{n_1} t^{n_1-1}\,\frac{f_{n_1-1}(t)^{n_1-1}}{f_{n_1}(t)^{n_1}}$$

occurring in Theorem 4 satisfies the condition (81) only for $n_1 = 5$. To see this let us
c observe that by (70),

$$(tf_{n-1}(t),\ f_{n_1}(t)) = 1,$$

hence $g(t)$ in a reduced form has the denominator

$$f_{n_1}(t)^{n_1} = \prod_{j=1}^{[(n_1-1)/2]} \left(t - \frac{1}{2+2\cos(2j\pi/n_1)}\right)^{n_1}.$$

c Therefore for $n_1 > 6$, $g(t)$ has at least three different poles, and for $n_1 = 4$ or 6 its numerator is of greater degree than the denominator. □

Proof of Theorem 8. Applying Lemma 56 with $F(x, y) = ax^n + yx^m + c$ we infer from (84) and Theorem 5 that if $n = 2m$ then

$$R(F) = \bigcup_{\substack{p\,|\,m \\ p \text{ prime} \\ b_1 = \sqrt[p]{c/a} \in \mathbb{Q}}} \left\{ -a\left(\frac{t+\sqrt{t^2-4b_1}}{2}\right)^p - a\left(\frac{t-\sqrt{t^2-4b_1}}{2}\right)^p \right\}$$

$$\cup \left\{ a(4t^4 - 8t^2 b_1 + 2b_1^2) \right\},$$

where the last summand occurs only if $4\,|\,m$ and $b_1 = \sqrt[4]{c/a} \in \mathbb{Q}$; if $n_1 = 3$, $m_1 = 1$, $2\,|\,(m, n)$ and $\sqrt{-ac} \in \mathbb{Q}$ then

$$R(F) = \{4at^4 - 4t\sqrt{-ac}\};$$

otherwise, $R(F) = \emptyset$ and (85) implies the theorem. □

10. Proof of Theorem 9 and of Corollary 1

Lemma 57. *Let $A \in \mathbb{C}$ and $T(x) = x^n + Ax^m + 1$. If $|A| > 2$, exactly m zeros of $T(x)$ (counting the multiplicities) satisfy the inequality*

$$\left| \log|x| + \frac{1}{m}\log|A| \right| < \frac{1}{m}\log\frac{|A|}{|A|-1} \tag{86}$$

and the remaining $n - m$ zeros satisfy the inequality

$$\left| \log|x| - \frac{1}{n-m}\log|A| \right| < \frac{1}{n-m}\log\frac{|A|}{|A|-1}\,. \tag{87}$$

Remark. Under the conditions of the lemma all zeros of $T(x)$ are simple, but we do not need this in the sequel.

Proof. Since $|Ax^m + 1| \geqslant |A| - 1 > 1 = |x|^n$ for $|x| = 1$, by Rouché's theorem $T(x)$ has as many zeros inside the unit circle as $Ax^m + 1$, hence m. For each of these zeros we have

$$\pm\left|Ax^m\right| \leqslant |x|^n \pm 1 \leqslant |x|^m \pm 1,$$

hence

$$\frac{1}{|A|+1} \leqslant |x|^m \leqslant \frac{1}{|A|-1}\,,$$

and

$$\log\frac{|A|}{|A|+1} \leqslant m\log|x| + \log|A| \leqslant \log\frac{|A|}{|A|-1}\,,$$

which gives (86). The remaining $n - m$ zeros of $T(x)$ are outside the unit circle and satisfy

$$\pm\left|x^n\right| \leqslant \pm\left|Ax^m\right| + 1 < \pm\left|Ax^m\right| + |x|^m\,,$$

hence

$$|A| - 1 \leqslant |x|^{n-m} \leqslant |A| + 1,$$

$$\log \frac{|A| - 1}{|A|} \leqslant (n - m) \log |x| - \log |A| \leqslant \log \frac{|A| + 1}{|A|},$$

which gives (87). □

Lemma 58. *In the notation of Lemma* 57*, if* $(m, n) = 1$ *and*

$$|A| \geqslant \frac{2m(n-m)}{\log 2m(n-m)}, \tag{88}$$

then the trinomial $T(x)$ *has no proper monic factor* $f \in \mathbb{C}[x] \setminus \mathbb{C}$ *with* $|f(0)| = 1$.

Proof. The condition (88) implies $|A| \geqslant e$, hence $T(x)$ has no zero on the unit circle, which settles the case $n < 4$. Since $|f(0)| = 1$ implies $\left|T(0) f^{-1}(0)\right| = 1$ it is enough to consider the case where $n \geqslant 4$, $\deg f \leqslant n/2$. Let

$$f(x) = \prod_{j=1}^{r} (x - \xi_j) \prod_{k=1}^{s} (x - \eta_k),$$

where ξ_j satisfy (86) and η_k satisfy (87). The condition $|f(0)| = 1$ gives

$$\sum_{j=1}^{r} \log \left|\xi_j\right| + \sum_{k=1}^{s} \log |\eta_k| = 0,$$

hence by (86) and (87)

$$\left| \frac{r}{m} - \frac{s}{n-m} \right| \log |A| \leqslant \left(\frac{r}{m} + \frac{s}{n-m} \right) \log \frac{|A|}{|A| - 1}. \tag{89}$$

Since $(m, n) = 1$ we have $(m, n - m) = 1$ and $r(n - m) - sm = 0$ would imply $r \equiv 0 \bmod m$, $s \equiv 0 \bmod (n - m)$, hence either $r = s = 0$ or $r = m$, $s = n - m$, $\deg f = n$ contrary to the assumption. Hence

$$|r(n-m) - sm| \geqslant 1. \tag{90}$$

Moreover, if $r \geqslant (m + 1)/2$ we have

$$r(n-m) - sm = rn - (r+s)m \geqslant \frac{m+1}{2} n - \frac{mn}{2} = \frac{n}{2} \geqslant 2,$$

similarly if $s \geqslant (n - m + 1)/2$ we have

$$r(n-m) - sm = (r+s)(n-m) - sn \leqslant \frac{n(n-m)}{2} - \frac{n(n-m+1)}{2} = -\frac{n}{2} \leqslant -2.$$

Thus

$$|r(n-m) - sm)| \geqslant 2, \quad \text{unless } r \leqslant m/2 \text{ and } s \leqslant (n-m)/2. \tag{91}$$

The inequalities (89)–(91) give

$$\frac{\log|A|}{m(n-m)} \leqslant \log\frac{|A|}{|A|-1}\,. \tag{92}$$

However, $t\log\frac{t}{t-1}$ is a decreasing function of $t>1$, hence

$$|A|\log\frac{|A|}{|A|-1} \leqslant e\log\frac{e}{e-1}$$

and (92) gives

$$\frac{|A|\log|A|}{m(n-m)} \leqslant e\log\frac{e}{e-1}\,.$$

Thus, by (91),

$$2\Big(1-\frac{\log\log 2m(n-m)}{\log 2m(n-m)}\Big) \leqslant e\log\frac{e}{e-1}$$

and

$$2(1-e^{-1}) \leqslant e\log\frac{e}{e-1}\,,$$

which is false. □

Lemma 59. *If $a,b,c\in\mathbb{Z}\setminus\{0\}$, $n>m$ are positive integers and $|b|>|a|^m\,|c|^{n-m}+1$ then every monic factor $f\in\mathbb{Q}[x]\setminus\mathbb{Q}$ of ax^n+bx^m+c satisfies $|f(0)|=|c/a|^{(\deg f)/n}$.*

Proof. Assume first that $2m\leqslant n$. Let $f(x)=\prod_{j=1}^{d}(x-\vartheta_j)$. For every j we have

$$a\vartheta_j^{n-m} = -b-c\vartheta_j^{-m}$$

and both sides are algebraic integers since the left hand side may have in the denominator only those prime ideals $\mathfrak{p}$ of $\mathbb{Q}(\vartheta_j)$ for which $\operatorname{ord}_{\mathfrak{p}}\vartheta_j<0$, and the right hand side only those $\mathfrak{p}$ for which $\operatorname{ord}_{\mathfrak{p}}\vartheta_j>0$. Hence

$$a\vartheta_j^{n-m} \equiv -c\vartheta_j^{-m} \bmod b \quad (1\leqslant j\leqslant d),$$

where the congruence is taken in the ring of algebraic integers. Multiplying the obtained congruences we obtain

$$a^d\big((-1)^d f(0)\big)^{n-m} \equiv (-1)^d c^d\big((-1)^d f(0)\big)^{-m} \bmod b.$$

If both sides of the congruence are equal then

$$|f(0)| = \Big|\frac{c}{a}\Big|^{d/n}\,, \tag{93}$$

otherwise

$$|a|^d\,|f(0)|^{n-m} + |c|^d\,|f(0)|^{-m} \geqslant |b|\,. \tag{94}$$

By the same argument applied to the polynomial

$$g(x) = \frac{ax^n + bx^m + c}{af(x)}$$

we infer that either

$$\left|\frac{c}{af(0)}\right| = \left|\frac{c}{a}\right|^{(n-d)/n} \tag{95}$$

or

$$|a|^{n-d}\left|\frac{c}{af(0)}\right|^{n-m} + |c|^{n-d}\left|\frac{c}{af(0)}\right|^{-m} \geqslant |b|\,. \tag{96}$$

However (95) implies (93), hence we have either (93), i.e. the assertion of the lemma, or simultaneously (94) and (96). Let us put, for $t > 0$,

$$\varphi_d(t) = |a|^d\, t^{n-m} + |c|^d\, t^{-m}.$$

The conjunction of (94) and (96) can be written as

$$\min\left\{\varphi_d(|f(0)|),\ \varphi_{n-d}\left(\left|\frac{c}{f(0)}\right|\right)\right\} \geqslant |b|\,. \tag{97}$$

On the other hand, we have $af(0) \in \mathbb{Z}$ and $cf(0)^{-1} \in \mathbb{Z}$, hence $|a|^{-1} \leqslant |f(0)| \leqslant |c|$ and we infer from (97) that

$$M := \max_{|a|^{-1} \leqslant t \leqslant |c|} \min\{\varphi_d(t),\ \varphi_{n-d}(|c/a|\, t^{-1})\} \geqslant |b|\,. \tag{98}$$

Now, the function $\varphi_d(t)$ has no local maximum in $(0, \infty)$, and the same applies to $\varphi_{n-d}(|c/a|\, t^{-1})$.

Consider first the case $d \leqslant m$. The inequality (98) with the above remark implies that

$$\max\{\varphi_d(|a|^{-1}), \varphi_d(|c|)\} \geqslant M \geqslant |b|\,.$$

In view of $d \leqslant m \leqslant n - m$ we have

$$\begin{aligned} \varphi_d(|a|^{-1}) &= |a|^{d+m-n} + |c|^d\, |a|^m \leqslant 1 + |c|^{n-m}\, |a|^m\,, \\ \varphi_d(|c|) &= |a|^d\, |c|^{n-m} + |c|^{d-m} \leqslant |a|^m\, |c|^{n-m} + 1, \end{aligned} \tag{99}$$

hence

$$|a|^m\, |c|^{n-m} + 1 \geqslant |b|\,, \tag{100}$$

contrary to the assumption.

Consider now the case $m < d < n - m$. The equation

$$\varphi_d(t) = \varphi_{n-d}(|c/a|\, t^{-1})$$

implies

$$t^{n-2m} = |c|^{n-m-d}\, |a|^{m-d}\,;$$

moreover, denoting the positive root of the latter equation by t_0, we have

$$|a|^{-1} \leqslant t_0 \leqslant |c|\,,$$
$$\varphi_d(t) < \varphi_{n-d}(|c/a|\,t^{-1}) \quad \text{for } t < t_0,$$
$$\varphi_d(t) > \varphi_{n-d}(|c/a|\,t^{-1}) \quad \text{for } t > t_0.$$

Hence, by (98) and the subsequent remark

$$M = \max\{\varphi_d(|a|^{-1}),\ \varphi_d(t_0),\ \varphi_{n-d}(|a|^{-1})\} \geqslant |b|\,.$$

Now

$$\begin{aligned}
\varphi_d(|a|^{-1}) &= |a|^{d+m-n} + |c|^d\,|a|^m \leqslant 1 + |c|^{n-m}\,|a|^m\,,\\
\varphi_d(t_0) &= (|a|^m\,|c|^{n-m})^{(n-m-d)/(n-2m)} + (|a|^m\,|c|^{n-m})^{(d-m)/(n-2m)}\\
&\leqslant |a|^m\,|c|^{n-m} + 1,\\
\varphi_{n-d}(|a|^{-1}) &= |a|^{m-d} + |c|^{n-d}\,|a|^m \leqslant 1 + |c|^{n-m}\,|a|^m
\end{aligned}$$

hence (100), contrary to the assumption.

Consider next the case $d \geqslant n - m$. Then

$$\max\{\varphi_{n-d}(|c|),\ \varphi_{n-d}(|a|^{-1})\} \geqslant M \geqslant |b|$$

and since $n - d \leqslant m$, by (99) we have again (100), contrary to the assumption.

Finally, assume that $2m > n$. Then $2(n - m) < n$ and since $f(0)^{-1}x^d f(x^{-1})$ is a monic factor of $cx^n + bx^{n-m} + a$ we infer from the already proved case of the lemma that

$$\left|f(0)^{-1}\right| = \left|\frac{a}{c}\right|^{d/n},$$

which gives the assertion. □

Lemma 60. *If $a, b, c \in \mathbb{Z}\setminus\{0\}$, $n > m$ are positive integers, $(m, n) = 1$ and $ax^n + bx^m + c$ is reducible then either*

$$|b| \leqslant |a|^m\,|c|^{n-m} + 1 \tag{101}$$

or simultaneously

$$\min\{|a|\,,|c|\} = 1, \qquad |b| \leqslant \frac{2m(n-m)}{\log 2m(n-m)}\,|a|^{m/n}\,|c|^{(n-m)/n}$$

and

$$\sqrt[p]{\max\{|a|\,,|c|\}} \in \mathbb{Z} \quad \textit{for some prime } p\,|\,n,$$

Proof. Suppose that

$$ax^n + bx^m + c = f(x)g(x), \quad \text{where } f, g \in \mathbb{Q}[x]\setminus\mathbb{Q} \text{ and } f \text{ is monic.} \tag{102}$$

If (101) does not hold we have, by Lemma 59,

$$|f(0)| = \left|\frac{c}{a}\right|^{(\deg f)/n}, \qquad \text{hence } \left|\frac{c}{a}\right|^{1/p} \in \mathbb{Q} \text{ for some prime } p\,|\,n. \tag{103}$$

Choose any value of $(c/a)^{1/n}$ and put

$$A = bc^{-1}\left(\frac{c}{a}\right)^{m/n}. \tag{104}$$

By (102) we have

$$c(x^n + Ax^m + 1) = f\left(\left(\frac{c}{a}\right)^{1/n} x\right) g\left(\left(\frac{c}{a}\right)^{1/n} x\right).$$

The polynomial

$$f_1(x) = \left(\frac{c}{a}\right)^{-(\deg f)/n} f\left(\left(\frac{c}{a}\right)^{1/n} x\right)$$

is a proper monic factor of $x^n + Ax^m + 1$ and, by (103),

$$|f_1(0)| = \left|\left(\frac{c}{a}\right)^{-(\deg f)/n} f(0)\right| = 1.$$

Hence by Lemma 58,

$$|A| \leqslant \frac{2m(n-m)}{\log 2m(n-m)}$$

and by (104),

$$|b| \leqslant \frac{2m(n-m)}{\log 2m(n-m)} |a|^{m/n} |c|^{(n-m)/n}.$$

If $\min\{|a|, |c|\} \geqslant 2$, then

$$\frac{|a|^m |c|^{n-m} + 2}{|a|^{m/n} |c|^{(n-m)/n}} \geqslant \frac{2^n + 2}{2} > \frac{n^2/2}{\log n^2/2} \geqslant \frac{2m(n-m)}{\log 2m(n-m)},$$

thus $|b| < |a|^n |c|^{n-m} + 2$ and (101) holds. If $\min\{|a|, |c|\} = 1$, (103) gives $\sqrt[p]{\max\{|a|, |c|\}} \in \mathbb{Z}$ for some prime $p \mid n$. □

Lemma 61. *If $f \in \mathbb{Z}[x]$ is a primitive irreducible polynomial with leading coefficient l,*

$$f(\xi) = 0 \quad \textit{and} \quad \xi = \eta^p,\ \eta \in \mathbb{Q}(\xi),$$

then $\sqrt[p]{|l|} \in \mathbb{Z}$, $\sqrt[p]{|f(0)|} \in \mathbb{Z}$; moreover, if $p = 2$ then

$$(-1)^{\deg f} l f(0) > 0. \tag{105}$$

Proof. Let $(\eta) = \mathfrak{a}/\mathfrak{b}$, where $\mathfrak{a}, \mathfrak{b}$ are integral ideals of $\mathbb{Q}(\xi)$, $(\mathfrak{a}, \mathfrak{b}) = 1$. We have $(\xi) = \mathfrak{a}^p/\mathfrak{b}^p$ and $\mathfrak{b}^{-p}$ is the content of $x - \xi$, hence $|l|\,(N\mathfrak{b})^{-p}$ is the content of f and since f is primitive, $|l| = (N\mathfrak{b})^p$, $\sqrt[p]{|l|} = N\mathfrak{b} \in \mathbb{Z}$, N denoting the absolute norm in $\mathbb{Q}(\xi)$. Now

$$(-1)^{\deg f} \frac{f(0)}{l} = N\xi = (N\eta)^p, \tag{106}$$

hence $\sqrt[p]{|f(0)|} = |N\eta|\ \sqrt[p]{|l|} \in \mathbb{Q}$. Moreover, if $p = 2$ then (106) implies (105). □

Lemma 62. *In the notation of Lemma* 61*, if*

$$f(\xi)=0 \quad \textit{and} \quad \xi=-4\eta^4, \quad \eta\in\mathbb{Q}(\xi), \quad \deg f\equiv 1 \bmod 2 \tag{107}$$

then $lf(0)>0$ *and either* $\sqrt[4]{|l|}\in\mathbb{Z}$, $\sqrt[4]{4\,|f(0)|}\in\mathbb{Z}$ *or* $\sqrt[4]{4\,|l|}\in\mathbb{Z}$, $\sqrt[4]{|f(0)|}\in\mathbb{Z}$.

Proof. Let

$$(2)=\prod_{j=1}^{k}\mathfrak{p}_j^{e_j}, \qquad N\mathfrak{p}_j=2^{f_j},$$

be the factorization of (2) into prime ideals of $\mathbb{Q}(\xi)$.

The equality $(\xi)=(4\eta^4)$ implies that

$$(\xi)=\prod_{j=1}^{k}\mathfrak{p}_j^{a_j}\,\frac{\mathfrak{a}}{\mathfrak{b}}, \qquad a_j\equiv 2e_j \bmod 4 \quad (1\leqslant j\leqslant k),$$

where $\mathfrak{a}$, $\mathfrak{b}$ are integral ideals of $\mathbb{Q}(\xi)$, $(\mathfrak{a},\mathfrak{b})=1$ and $(2,\mathfrak{ab})=1$. Arguing as in the proof of Lemma 61 we infer that

$$|l|=2^{\sum' |a_j| f_j}(N\mathfrak{b})^4$$

where the sum $\sum'$ is taken over all j with $a_j<0$, and

$$\frac{f(0)}{l}=(-1)^{\deg f}N\xi=4^{\deg f}(N\eta)^4.$$

Hence $lf(0)>0$ and if $\sum' a_j f_j\equiv 0 \bmod 4$ we have

$$\sqrt[4]{|l|}\in\mathbb{Z}, \qquad \sqrt[4]{4\,|f(0)|}=2^{(\deg f+1)/2}\,|N\eta|\,\sqrt[4]{|l|}\in\mathbb{Q}.$$

If $\sum' a_j f_j\equiv 2 \bmod 4$ we have

$$\sqrt[4]{4\,|l|}\in\mathbb{Z}, \qquad \sqrt[4]{|f(0)|}=2^{(\deg f-1)/2}\,|N\eta|\,\sqrt[4]{4\,|l|}\in\mathbb{Q}. \qquad \square$$

Proof of Theorem 9. If $t(x):=ax^{n_1}+bx^{m_1}+c$ is reducible then by Lemma 60 we have either (x) or (xi). If $t(x)$ is irreducible we apply Capelli's lemma to $t(x^{(m,n)})=ax^m+bx^n+c$ and we infer that it is reducible if and only if

$$x^{(m,n)}-\xi \ \text{ is reducible over } \ \mathbb{Q}(\xi),$$

where $t(\xi)=0$. However, by Capelli's theorem the last binomial is reducible if and only if either

$$\xi=\eta^p, \quad \text{where} \quad \eta\in\mathbb{Q}(\xi), \ p \text{ a prime}, \ p\,|\,(m,n),$$

or

$$\xi=-4\eta^4, \quad \text{where} \ \ \eta\in\mathbb{Q}(\xi), \ \ 4\,|\,n.$$

These conditions give (xii) and (xiii) in virtue of Lemmas 61 and 62. $\square$

Proof of Corollary 1. Replacing x by x^{-1}, if necessary, we may assume $n\geqslant 2m$. Since $n_1>d$ and $x^n+bx^m\pm 1$ has a factor of degree d, by Capelli's lemma $x^{n_1}+bx^{m_1}\pm 1$ is

reducible. Hence by Theorem 9,

$$|b| < \frac{2m_1(n_1-m_1)}{\log 2m_1(n_1-m_1)} \leqslant \frac{2(n-m)^2}{\log 2(n-m)^2}\,. \tag{108}$$

On the other hand, since $|b| > 2$, $x^n + bx^m \pm 1$ has no cyclotomic factors, and also no reciprocal factors since $x^n + bx^m \pm 1 - (x^n \pm bx^{n-m} \pm 1) = b(x^m \pm x^{n-m})$. Therefore by Smyth's result [29] at least one zero ϑ of the factor of degree d satisfies the inequality

$$\log|\vartheta| \geqslant \frac{\log\vartheta_0}{d}\,, \quad \text{where } \vartheta_0^3 - \vartheta_0 - 1 = 0.$$

c

c Hence by Lemma 57,

$$\frac{\log\vartheta_0}{d} \leqslant \frac{1}{n-m}\log\frac{|b|^2}{|b|-1}\,,$$

and by (108),

$$\frac{\log\vartheta_0}{d} \ll \frac{\log(n-m)}{n-m}\,.$$

This gives $n \leqslant 2(n-m) \ll d\log d$ and by (108), $|b| \ll d^2\log d$. The constants in the Vinogradov symbols are effective. □

11. Proof of Theorem 10 and of Corollary 2

Lemma 63. *Let K be an algebraic number field, $\xi, \eta \in K^*$ and $(\xi,\eta) = \mathfrak{c}/\mathfrak{d}$, where $\mathfrak{c}$, $\mathfrak{d}$ are integral ideals of K. Then*

$$(\xi^n - \eta^n, \xi^m - \eta^m) \;\Big|\; \frac{\mathfrak{c}^{n-(m,n)}}{\mathfrak{d}^{m-(m,n)}}\big(\xi^{(m,n)} - \eta^{(m,n)}\big).$$

Proof. Let K_1 be an extension of K such that $\mathfrak{c} = (\gamma)$ and $\mathfrak{d} = (\delta)$ are principal ideals of K_1. We have then

$$\xi = \frac{\gamma}{\delta}\,\xi_1, \qquad \eta = \frac{\gamma}{\delta}\,\eta_1,$$

where ξ_1, η_1 are integers of K_1 and $(\xi_1, \eta_1) = 1$. Clearly

$$(\xi^n - \eta^n, \xi^m - \eta^m) \;\Big|\; \frac{\gamma^n}{\delta^m}(\xi_1^n - \eta_1^n,\ \xi_1^m - \eta_1^m). \tag{109}$$

Let $(m,n) = rn - sm$, where r, s are positive integers. We have

$$\xi_1^n - \eta_1^n \,|\, \xi_1^{rn} - \eta_1^{rn}, \quad \xi_1^m - \eta_1^m \,|\, \xi_1^{sm} - \eta_1^{sm},$$

hence

$$(\xi_1^n - \eta_1^n,\ \xi_1^m - \eta_1^m) \;\Big|\; \xi_1^{rn} - \eta_1^{rn} - \xi_1^{(m,n)}(\xi_1^{sm} - \eta_1^{sm}) = \eta_1^{sm}(\xi_1^{(m,n)} - \eta_1^{(m,n)})$$

and by symmetry

$$(\xi_1^n - \eta_1^n,\ \xi_1^m - \eta_1^m) \,|\, \xi_1^{sm}\big(\xi_1^{(m,n)} - \eta_1^{(m,n)}\big).$$

Since $(\xi_1, \eta_1) = 1$ it follows that

$$(\xi_1^n - \eta_1^n,\ \xi_1^m - \eta_1^m) \mid \xi_1^{(m,n)} - \eta_1^{(m,n)} = \frac{\delta^{(m,n)}}{\gamma^{(m,n)}}\big(\xi^{(m,n)} - \eta^{(m,n)}\big),$$

and the lemma follows from (109). □

Lemma 64. *In the notation of Lemma* 63 *let* $l = [K : \mathbb{Q}]$, $l_0 = [\mathbb{Q}(\xi/\eta) : \mathbb{Q}]$. *If* ξ/η *is not a root of unity we have*

$$\log|N(\xi^n - \eta^n)| = n \log \frac{N\mathfrak{c}}{N\mathfrak{d}} + n\,\frac{l}{l_0} \log M(\xi/\eta) + O\Big(\frac{l}{l_0} \log M(\xi/\eta) + l\Big) \log n$$

where N *is the absolute norm in* K, $M(\xi/\eta)$ *is the Mahler measure of* ξ/η *and the constant in the* O *symbol depends only on* l_0.

Proof. Let $\xi/\eta = \alpha/\beta$, where $\alpha, \beta \in \mathbb{Q}(\xi/\eta) = K_0$, α, β are integers and $(\alpha, \beta) = \mathfrak{d}_0$. Let S be the set of all isomorphic injections of K_0 into $\mathbb{C}$ and N_0 be the absolute norm in K_0.

In the notation of [24] we have

$$\begin{aligned} w(\alpha/\beta) &:= \log \prod_{\sigma\in S} \max\big\{|\alpha^\sigma|, |\beta^\sigma|\big\} - \log N_0\mathfrak{d}_0 \\ &= \log M(\alpha/\beta) = \log M(\xi/\eta), \end{aligned} \tag{110}$$

since $N_0\mathfrak{d}_0^{-1} \prod_{\sigma\in S} \beta^\sigma$ is the leading coefficient of the primitive irreducible polynomial $N_0\mathfrak{d}_0^{-1} \prod_{\sigma\in S} (\beta^\sigma x - \alpha^\sigma)$ which has α/β as a zero. Therefore, by Lemmas 1 and 2 from [24], for all $\sigma \in S$ we have

$$\log\big|(\alpha^\sigma)^n - (\beta^\sigma)^n\big| = n \log \max\big\{|\alpha^\sigma|,\ |\beta^\sigma|\big\} + O(l_0 + \log M(\xi/\eta)) \log n,$$

where the constant in the O symbol depends only on l_0 and is effectively computable. This gives

$$\log|N_0(\alpha^n - \beta^n)| = n \log \prod_{\sigma\in S} \max\big\{|\alpha^\sigma|,\ |\beta^\sigma|\big\} + O(l_0 + \log M(\xi/\eta)) \log n$$

and by (110),

$$\log|N_0(\alpha^n - \beta^n)| = n \log N_0\mathfrak{d}_0 + n \log M(\xi/\eta) + O(l_0 + \log M(\xi/\eta)) \log n,$$

which gives at once

$$\log|N(\alpha^n - \beta^n)| = n \log N\mathfrak{d}_0 + n\,\frac{l}{l_0} \log M(\xi/\eta) + O\Big(l + \frac{l}{l_0} \log M(\xi/\eta)\Big) \log n.$$

On the other hand,

$$\left(\frac{\xi^n - \eta^n}{\alpha^n - \beta^n}\right) = \frac{(\xi, \eta)^n}{(\alpha, \beta)^n} = \frac{\mathfrak{c}^n}{\mathfrak{d}^n\mathfrak{d}_0^n},$$

hence

$$\log|N(\xi^n-\eta^n)| = n\log\frac{N\mathfrak{c}}{N\mathfrak{d}} + n\,\frac{l}{l_0}\log M(\xi/\eta) + O\Big(l+\frac{l}{l_0}\log M(\xi/\eta)\Big)\log n. \quad \square$$

Proof of Theorem 10. Suppose that the minimal polynomial of ξ, say $f(x)$, is of degree $e \leqslant d$. If for every zero η of f we have ξ/η equal to a root of unity then $\xi^e/N\xi$ is a root of unity and

$$\xi^{(m,n)} = \sqrt[r]{g}\,\zeta_s,$$

where g is a positive integer, not a power with exponent greater than 1 and dividing r. If $\xi^{(m,n)} \in \mathbb{Q}$ we have the case (xvii); otherwise $\xi^{(m,n)}$ has a conjugate

$$\eta^{(m,n)} = \xi^{(m,n)}\zeta_t^j, \qquad j \not\equiv 0 \bmod t.$$

Since

$$a\xi^n + b\xi^m + c = a\eta^n + b\eta^m + c = 0 \tag{111}$$

and $\zeta_t^{jn/(m,n)} = \zeta_t^{jm/(m,n)} = 1$ is impossible we obtain

$$\xi^{(m,n)} \in \mathbb{Q}(\zeta_t), \quad \text{hence} \quad \sqrt[r]{g} \in \mathbb{Q}(\zeta_s, \zeta_t).$$

It follows (see [17]) that $r = 1$ or 2. If $r = 1$ then by Mann's theorem [14], $s \mid 6$ and we have (xvii). If $r = 2$ the equation

$$a\big(\sqrt{g}\,\zeta_s\big)^{n/(m,n)} + b\big(\sqrt{g}\,\zeta_s\big)^{m/(m,n)} + c = 0$$

gives a representation of $\sqrt{g}$ as a linear combination of two roots of unity. Hence squaring and using Mann's theorem again we obtain $s = 8$, $g = 2q^2$ or $s = 12$, $g = 3q^2$, $q \in \mathbb{Q}$, which gives (xvii).

It remains to consider the case where for a certain zero η of f we have ξ/η different from roots of unity. Let $K = \mathbb{Q}(\xi, \eta)$ be of degree l and let $(\xi, \eta) = \mathfrak{c}/\mathfrak{d}$, where $\mathfrak{c}$, $\mathfrak{d}$ are integral ideals of K, $(\mathfrak{c}, \mathfrak{d}) = 1$. We infer from (111) that

$$\mathfrak{c}^m \mid c, \qquad \mathfrak{d}^{n-m} \mid a,$$

hence

$$m\log N\mathfrak{c} \leqslant l\log|c|, \qquad (n-m)\log N\mathfrak{d} \leqslant l\log|a|. \tag{112}$$

On the other hand,

$$a(\xi^n - \eta^n) = b(\eta^m - \xi^m), \tag{113}$$

hence

$$\xi^n - \eta^n \;\Big|\; \frac{b}{(a,b)}(\eta^m - \xi^m)$$

and

$$\xi^n - \eta^n \;\Big|\; \frac{b}{(a,b)}(\xi^n - \eta^n,\ \xi^m - \eta^m).$$

By Lemma 63 this gives

$$(\xi^n - \eta^n) \;\Big|\; \frac{b}{(a,b)} \frac{\mathfrak{c}^{n-(m,n)}}{\mathfrak{d}^{m-(m,n)}} \big(\xi^{(m,n)} - \eta^{(m,n)}\big),$$

hence

$$\log |N(\xi^n - \eta^n)| \leqslant l \log \frac{|b|}{(a,b)} + (n - (m,n)) \log N\mathfrak{c} - (m - (m,n)) \log N\mathfrak{d} + \log |N(\xi^{(m,n)} - \eta^{(m,n)})|.$$

Now we apply Lemma 64 and obtain

$$\begin{aligned} n(\log N\mathfrak{c} - \log N\mathfrak{d}) + n \frac{l}{l_0} \log M(\xi/\eta) + O\Big(\frac{l}{l_0} \log M(\xi/\eta) + l\Big) \log n \\ \leqslant l \log \frac{|b|}{(a,b)} + (n - (m,n)) \log N\mathfrak{c} - (m - (m,n)) \log N\mathfrak{d} \\ + (m,n)(\log N\mathfrak{c} - \log N\mathfrak{d}) + (m,n) \frac{l}{l_0} \log M(\xi/\eta) \\ + \Big(\frac{l}{l_0} \log M(\xi/\eta) + l\Big) \log (m,n) \end{aligned}$$

and thus by (112),

$$\begin{aligned} (n - (m,n)) \log M(\xi/\eta) &\leqslant l_0 \log \frac{|b|}{(a,b)} + (n-m) \frac{l_0}{l} \log N\mathfrak{d} \\ &\quad + O(\log M(\xi/\eta) + l_0) \log n \\ &\leqslant l_0 \log \frac{|ab|}{(a,b)} + O(\log M(\xi/\eta) + l_0) \log n. \end{aligned} \tag{114}$$

Let $B_0(l_0)$ be the constant in the O symbol,

$$B_1(l_0) = \inf \log M(\theta),$$

where the infimum is taken over all algebraic numbers θ of degree l_0 different from roots of unity. By Dobrowolski's theorem [7] or by earlier results $B_1(l_0) > 0$. Let $c_0(d)$ be a unique solution of the equation

$$\frac{n}{\log n} = 4 \sup_{l_0 \leqslant d(d-1)} B_0(l_0) \left(1 + \frac{l_0}{B_1(l_0)}\right).$$

Since $(m,n) \leqslant \frac{1}{2}n$, $l_0 \leqslant d(d-1)$ for $n > c_0(d)$ the inequality (114) implies

$$\frac{1}{2} n \log M(\xi/\eta) \leqslant l_0 \log \frac{|ab|}{(a,b)} + \frac{1}{4} n \log M(\xi/\eta),$$

hence (xiv) holds with

$$c_1(d) = \sup_{l_0 \leqslant d(d-1)} \frac{4l_0}{B_1(l_0)}.$$

(xv) is obtained from (xiv) on replacing ξ by ξ^{-1}, with c taking the role of a.

In order to obtain (xvi) we assume without loss of generality that $n < 2m$. (If $n > 2m$ we replace ξ by ξ^{-1}, then m is replaced by $n - m$.) We infer from (113) that

$$\xi^m - \eta^m \mid a(\xi^n - \eta^n)$$

and since $\xi^m - \eta^m \mid a(\xi^m - \eta^m)$ we have

$$\xi^m - \eta^m \mid a(\xi^n - \eta^n,\ \xi^m - \eta^m).$$

By Lemma 63 this gives

$$(\xi^m - \eta^m) \;\Big|\; (a)\frac{\mathfrak{c}^{n-(m,n)}}{\mathfrak{d}^{m-(m,n)}}\big(\xi^{(m,n)} - \eta^{(m,n)}\big),$$

hence

$$\begin{aligned}\log|N(\xi^m - \eta^m)| \leqslant{}& l\log|a| + (n-(m,n))\log N\mathfrak{c}\\ &- (m-(m,n))\log N\mathfrak{d} + \log\big|N\big(\xi^{(m,n)} - \eta^{(m,n)}\big)\big|.\end{aligned}$$

Now we apply Lemma 64 and obtain

$$\begin{aligned}m\log N\mathfrak{c} - m\log N\mathfrak{d} + m\frac{l}{l_0}\log M(\xi/\eta) + O\Big(\frac{l}{l_0}\log M(\xi/\eta) + l\Big)\log m&\\ \leqslant l\log|a| + (n-(m,n))\log N\mathfrak{c} - (m-(m,n))\log N\mathfrak{d}&\\ + (m,n)\log N\mathfrak{c} - (m,n)\log N\mathfrak{d} + (m,n)\frac{l}{l_0}\log M(\xi/\eta)&\\ + O\left(\frac{l}{l_0}\log M(\xi/\eta) + l\right)\log(m,n),&\end{aligned}$$

thus by (112)

$$\begin{aligned}(m-(m,n))\log M(\xi/\eta) &\leqslant l_0\log|a| + (n-m)\frac{l_0}{l}\log N\mathfrak{c}\\ &\quad + O(\log M(\xi/\eta) + l_0)\log m\\ &\leqslant l_0\log|ac| + O(\log M(\xi/\eta) + l_0)\log n.\end{aligned}$$

Since $n < 2m$, by considering a few cases we find $m - (m,n) \geqslant n/3$, hence for $n > c_0(d)$ we obtain

$$\frac{1}{3}\log M(\xi/\eta) \leqslant l_0\log|ac| + \frac{1}{4}n\log M(\xi/\eta),$$

which implies (xvi) by the definition of $c_1(d)$. □

Proof of Corollary 2. If ξ is a zero of the factor in question, then ξ is an algebraic unit, hence (xvii) would imply that ξ is a root of unity, impossible for $|b| > 2$. Therefore by Theorem 10 we have (xvi), which for $a = c = 1$ gives $n < c_0(d)$. However, by Theorem 8, for every n there exist only finitely many reducible trinomials $x^n + bx^m + 1$ with $n \neq 2m$.□

Table 5. Sporadic trinomials over $\mathbb{Q}$

The table contains all reducible trinomials $x^n + Ax^m + B, n \geqslant 2m, A, B \in \mathbb{Z} \setminus \{0\}$ known to the author, which satisfy neither (vi) nor (vii) nor (viii) and have the following properties: 1) for every divisor $d > 1$ of (n, m), $x^{n/d} + Ax^{m/d} + B$ is irreducible, 2) (A^n, B^{n-m}) is free from $n(n-m)$th powers, 3) if $n - m$ is odd then $A > 0$, if n, m are both odd, then $B > 0$.

Number	Trinomial	Factor	Discoverer
1	$x^8 + 3x^3 - 1$	$x^3 + x - 1$	Łutczyk
2	$x^8 + 2^3 \cdot 3x^3 + 2^5$	$x^3 - 2x^2 + 4$	Nicolas
3	$x^8 + 2^2 \cdot 3^3 x^3 + 3^5$	$x^3 + 3x^2 + 9x + 9$	Nicolas
4	$x^8 + 3 \cdot 5 \cdot 7^3 \cdot 59x^3 - 2^3 \cdot 7^5 \cdot 11^3$	$x^3 - 7x^2 - 98x + 2156$	Schinzel
5	$x^9 - 2^2 \cdot 19x + 2^5 \cdot 3$	$x^4 - 2x^2 - 4x + 6$	Schinzel
6	$x^9 + 2^5 x^2 - 2^6$	$x^3 - 2x^2 + 4x - 4$	Nicolas
7	$x^9 + 3^4 x^2 - 2 \cdot 3^3$	$x^3 + 3x + 3$	Nicolas
8	$x^9 + 3^6 x^2 - 2 \cdot 3^6$	$x^3 - 3x^2 + 9$	Browkin
9	$x^9 + 3^5 x^4 - 2^2 \cdot 3^6$	$x^3 - 3x^2 + 18$	Browkin
10	$x^9 + 2^4 \cdot 3^5 x^4 - 2^8 \cdot 3^6$	$x^3 + 6x^2 + 36x + 72$	Nicolas
11	$x^{10} + 3^3 \cdot 11x - 3^5$	$x^3 + 3x - 3$	Schinzel
11a	$x^{10} + 3^6 \cdot 11x + 2 \cdot 3^8$	$x^3 + 3x^2 + 9x + 18$	Cisłowska
12	$x^{10} + 2^6 \cdot 3^3 \cdot 5^6 \cdot 11x - 2^7 \cdot 3^5 \cdot 5^5 \cdot 19$	$x^4 - 60x^2 - 300x + 5400$	Browkin
12a	$x^{10} + 2^6 \cdot 5 \cdot 7^6 \cdot 11 \cdot 631x + 2^7 \cdot 7^7 \cdot 17 \cdot 19 \cdot 73$	$x^3 + 14x^2 + 392x + 3332$	Cisłowska
13	$x^{10} + 3x^3 - 2^3$	$x^4 + x^3 - x - 2$	Morain
14	$x^{10} + 2^5 x^3 - 2^6$	$x^5 - 2x^4 + 8x - 8$	Morain
15	$x^{10} + 3^2 \cdot 11x^3 + 2 \cdot 3^3$	$x^3 + 3x + 3$	Nicolas
16	$x^{11} + 2^2 \cdot 3x + 2^3$	$x^5 - 2x^4 + 2x^3 - 2x^2 + 2$	Nicolas
17	$x^{11} + 2^3 \cdot 3^3 \cdot 23x^2 - 2^4 \cdot 3^5$	$x^3 + 6x - 6$	Browkin
18	$x^{11} + 2^2 \cdot 23x^3 + 2^3 \cdot 3$	$x^3 + 2x^2 + 4x + 2$	Morain

Table 5 (cont.)

Number	Trinomial	Factor	Discoverer
19	$x^{11} + x^4 + 2^2$	$x^5 - x^3 - x^2 + 2$	Jonassen
20	$x^{11} - 3^3 \cdot 5^2 \cdot 23x^5 + 3^8 \cdot 5^4$	$x^3 - 15x - 45$	Browkin
21	$x^{12} + 2^6 \cdot 3^2x + 2^4 \cdot 23$	$x^3 + 2x^2 + 4x + 2$	Browkin–Schinzel
22	$x^{12} + 2^5 \cdot 3^4 \cdot 13x + 2^4 \cdot 3^4 \cdot 23$	$x^3 + 6x + 6$	Browkin
23	$x^{12} + 2^6x^5 - 2^8$	$x^3 - 2x^2 + 4x - 4$	Morain
23a	$x^{12} + 5 \cdot 3^6x^5 - 2 \cdot 3^9$	$x^4 + 3x^3 + 9x^2 + 27$	Browkin
24	$x^{13} + 2^8 \cdot 3x + 2^{10}$	$x^3 + 2x^2 + 4x + 4$	Browkin
25	$x^{13} + 2^8 \cdot 3 \cdot 53x - 2^{12} \cdot 7$	$x^3 - 4x^2 + 8x - 4$	Browkin–Schinzel
26	$x^{13} + 2^8 \cdot 3 \cdot 5^6 \cdot 53x + 2^{11} \cdot 5^7 \cdot 13$	$x^3 + 20x + 100$	Browkin
27	$x^{13} - 2^6 \cdot 3 \cdot 5^5 \cdot 53x^3 + 2^8 \cdot 5^8 \cdot 11$	$x^3 + 20x - 100$	Browkin
28	$x^{13} + 3x^4 - 1$	$x^3 + x^2 - 1$	Coray
29	$x^{13} + 2^6 \cdot 3x^4 - 2^9$	$x^3 + 2x^2 + 4x + 4$	Browkin
30	$x^{13} + 3^3 \cdot 53x^4 - 2^2 \cdot 3^6$	$x^3 - 3x^2 + 6$	Browkin
31	$x^{13} + 3x^6 + 1$	$x^4 - x + 1$	Coray
32	$x^{13} + 2^4 \cdot 3x^6 - 2^8$	$x^3 - 2x^2 + 4x - 4$	Browkin
34	$x^{14} + 2^2x^5 - 1$	$x^3 + x^2 - 1$	Bremner
35	$x^{14} + 2^2 \cdot 3^6x^5 + 3^{11}$	$x^4 - 3x^3 + 9x^2 - 18x + 27$	Morain
36	$x^{15} - 3^7 \cdot 5^6 \cdot 31x + 2^2 \cdot 3^8 \cdot 5^5 \cdot 29$	$x^3 + 15x - 45$	Browkin
36a	$x^{15} - 3^6x^6 + 3^9$	$x^5 + 3x^4 + 9x^3 + 18x^2 + 27x + 27$	Chaładus
37	$x^{15} - 2^4 \cdot 7^3 \cdot 31x^7 + 2^{11} \cdot 3 \cdot 7^5$	$x^3 - 14x - 28$	Browkin
38	$x^{16} + 7x^3 + 3$	$x^3 - x^2 + 1$	Bremner

Table 5 (cont.)

Number	Trinomial	Factor	Discoverer
39	$x^{16} + 2^3 \cdot 7x^3 - 3^2$	$x^3 + x^2 + x - 1$	Bremner
40	$x^{16} + 2^8 x^7 + 2^{12}$	$x^4 - 2x^3 + 4x^2 - 8x + 8$	Morain
41	$x^{16} + 2^8 \cdot 7x^7 - 2^{15}$	$x^3 + 2x^2 - 8$	Bremner
42	$x^{17} + 103x + 2^3 \cdot 7$	$x^3 - x^2 + x + 1$	Bremner
43	$x^{17} + 2^{12} \cdot 103x^4 - 2^{16} \cdot 3^2$	$x^3 + 2x^2 + 4x - 8$	Browkin
43a	$x^{19} + 7 \cdot 2^8 x^7 - 2^{15}$	$x^4 - 2x^3 + 4x^2 - 4x + 8$	John Abbott
43b	$x^{20} + 7 \cdot 2^{12} x^2 + 2^{16}$	$x^{10} + 4x^9 + 8x^8 + 8x^7 + 32x^4 + 128x^3 + 256x^2 + 320x + 256$	John Abbott
44	$x^{21} + 2^{11} \cdot 13x^5 + 2^{14} \cdot 3$	$x^3 - 2x^2 + 4$	Browkin
45	$x^{22} + 2^{14} \cdot 23x - 2^{15} \cdot 13$	$x^3 + 2x^2 - 4$	Browkin
46	$x^{24} + 2^{11} \cdot 7x + 2^8 \cdot 47$	$x^3 - 2x^2 + 2$	Browkin–Schinzel
47	$x^{26} + 2^7 \cdot 3 \cdot 53x^3 + 2^8 \cdot 47$	$x^3 - 2x^2 + 2$	Browkin–Schinzel
48	$x^{33} + 67x^{11} + 1$	$x^3 + x + 1$	Bremner
49	$x^{39} + 2^9 \cdot 3 \cdot 157x^{13} + 2^{13}$	$x^3 + 2x + 2$	Browkin
50	$x^{46} + 2^{26} \cdot 47x^7 - 2^{31} \cdot 3^2$	$x^3 - 2x^2 + 4x - 4$	Browkin
51	$x^{51} - 2^{31} \cdot 103x^5 + 2^{34} \cdot 47$	$x^3 - 2x^2 + 4x - 4$	Browkin
52	$x^{52} + 2^{34} \cdot 3 \cdot 53x + 2^{35} \cdot 103$	$x^3 + 2x^2 + 4x + 4$	Browkin

c

References

[1] A. Bremner, *On reducibility of trinomials*. Glasgow Math. J. 22 (1981), 155–156.

[2] —, *On trinomials of type* $x^n + Ax^m + 1$. Math. Scand. 49 (1981), 145–155.

[3] A. Capelli, *Sulla riduttibilità delle equazioni algebriche, Nota prima*. Rend. Accad. Sci. Fis. Mat. Soc. Napoli (3) 3 (1897), 243–252.

[4] J. W. S. Cassels, *Diophantine equations with special reference to elliptic curves*. J. London Math. Soc. 41 (1966), 193–291.

[5] C. Chevalley, *Introduction to the Theory of Algebraic Functions of One Variable*. Amer. Math. Soc., New York 1951.

[6] A. Choudhry, A. Schinzel, *On the number of terms in the irreducible factors of a polynomial over* $\mathbb{Q}$. Glasgow Math. J. 34 (1992), 11–15.

[7] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*. Acta Arith. 34 (1979), 391–401.

[8] M. Eichler, *Einführung in die Theorie der algebraischen Zahlen und Funktionen*. Birkhäuser, Basel–Stuttgart 1963.

[9] M. Fried, *On the Diophantine equation* $f(y) - x = 0$. Acta Arith. 19 (1971), 79–87.

[10] —, *Exposition on an arithmetic-group theoretic connection via Riemann's existence theorem*. In: The Santa Cruz Conference on Finite Groups, Proc. Sympos. Pure Math. 37 (1980), 571–602.

[11] M. Fried, A. Schinzel, *Reducibility of quadrinomials*. Acta Arith. 21 (1972), 153–171; *Corrigendum and addendum*, ibid. 99 (2001), 409–410; this collection: E4, 720–738.

[12] K. Győry, A. Schinzel, *On a conjecture of Posner and Rumsey*. J. Number Theory 47 (1994), 63–78; this collection: D11, 549–562.

[13] E. Maillet, *Détermination des points entiers des courbes algébriques unicursales à coefficients entiers*. C. R. Acad. Sci. Paris 168 (1919), 217–220; J. École Polytechn. (2) 20 (1920), 115–156.

[14] H. B. Mann, *On linear relations between roots of unity*. Mathematika 12 (1965), 107–117.

[15] T. Nagell, *Sur la réductibilité des trinômes*. In: Comptes rendus du 8. congrès des mathématiciens scandinaves, Stockholm 1934, 273–275.

[16] —, *Sur la classification des cubiques planes du premier genre par des transformations birationelles dans un domaine de rationalité quelconque*. Nova Acta Soc. Sci. Upsaliensis (4) 12 (1941), No. 8.

[17] —, *Contributions à la théorie des corps et des polynômes cyclotomiques*. Ark. Mat. 5 (1964), 153–192.

[17a] Numerical tables on elliptic curves. In: *Modular Functions of One Variable* IV, Lecture Notes in Math. 476, Springer, Berlin 1975, 81–144.

[18] L. Rédei, *Algebra* I. Akademische Verlagsgesellschaft, Geest & Portig, Leipzig 1959.

[19] H. Reichardt, *Über die Diophantische Gleichung* $ax^4 + bx^2y^2 + cy^4 = ez^2$. Math. Ann. 117 (1940), 235–276.

[20] P. Ribenboim, *On the factorization of* $x^n - Bx - A$. Enseign. Math. (2) 37 (1991), 191–200.

[21] A. Schinzel, *Some unsolved problems on polynomials*. In: Neki nerešeni problemi u matematici, Matematička Biblioteka 25, Beograd 1963, 63–70; this collection: E1, 703–708.

[22] —, *Reducibility of lacunary polynomials* I. Acta Arith. 16 (1969), 123–159; *Corrigenda*: Acta Arith. 19 (1971), 201; ibid. 24 (1978), 265; this collection: D4, 344–380.

[23] —, *Reducibility of polynomials*. In: Computers in Number Theory, Academic Press, London 1971, 73–75.

[24] —, *Primitive divisors of the expression* $A^n - B^n$ *in algebraic number fields*. J. Reine Angew. Math. 268/269 (1974), 27–33; this collection: I5, 1090–1097.

[25] A. Schinzel, *On linear dependence of roots*. Acta Arith. 28 (1975), 161–175; this collection: C7, 238–252.

[26] —, *Selected Topics on Polynomials*. University of Michigan Press, Ann Arbor 1982.

[27] E. S. Selmer, *On the irreducibility of certain trinomials*. Math. Scand. 4 (1956), 287–302.

[28] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*. Abh. Preuss. Akad. Wiss. Phys.-math. Kl. Nr. 1 (1929); Ges. Abhandlungen I, Springer, Berlin 1966, 209–266.

[29] C. J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*. Bull. London Math. Soc. 3 (1971), 169–175.

[30] N. Tschebotaröw, *Grundzüge der Galoisschen Theorie*. Übersetzt und bearbeitet von H. Schwerdtfeger, Noordhoff, Groningen–Djakarta 1950.

[31] G. Turnwald, *On Schur's conjecture*. J. Austral. Math. Soc. Ser. A 58 (1995), 312–357.

[31a] H. Tverberg, *On cubic factors of certain trinomials*. Math. Scand. 53 (1983), 178–184.

[32] K. Th. Vahlen, *Über reductible Binome*. Acta Math. 19 (1895), 195–198.

Originally published in
Journal of Number Theory 47 (1994), 63–78

On a conjecture of Posner and Rumsey

with K. Győry (Debrecen)*

Dedicated to the memory of Professor Hans Zassenhaus

Abstract. In 1965 Posner and Rumsey made a conjecture concerning common divisors of infinitely many monic polynomials over $\mathbb{Q}$ having fewer than i non-constant terms. The conjecture is proved here for $i = 3$ and disproved for $i \geqslant 4$.

1. Introduction

In 1965 C. Posner and H. Rumsey, Jr. [13] considered polynomials that divide infinitely many trinomials and, more generally, i-nomials. In the introduction to their paper they defined a trinomial as a polynomial $ax^m - bx^n - c$, with distinct positive integers m, n and a, b, c not all zero; in the concluding remarks they defined an i-nomial as a polynomial with i or fewer non-zero coefficients. The two definitions are incompatible since $x^3 + x^2 + x$ is a trinomial according to the second definition, but not according to the first. The generalization of trinomials according to the first definition is polynomials of the form

$$\sum_{j=1}^{i-1} a_j x^{m_j} + a_i, \qquad \text{with } m_1 > m_2 > \ldots > m_{i-1} > 0, \, a_j \text{ not all zero.}$$

We call monic polynomials of the above form *standard i-nomials*. We can now state the general conjecture of Posner and Rumsey, formulated in the last paragraph of [13]: *If a polynomial with rational coefficients divides infinitely many standard i-nomials over $\mathbb{Q}$, it divides a non-zero polynomial of degree less than i in x^r over $\mathbb{Q}$, for some $r \geqslant 1$.* For $i = 2$ the conjecture is obvious. The paper [13] is devoted almost exclusively to the case $i = 3$. The authors succeed in proving the following. If $p \in \mathbb{Q}[x]$ divides infinitely many standard trinomials over $\mathbb{Q}$, then $p(x)$ divides an at most cubic polynomial in x^r and the cubic polynomial divides infinitely many standard trinomials over $\mathbb{Q}$. (The result is phrased a little differently since instead of fixing the leading coefficient the authors do not

Communicated by D. J. Lewis.

* Research supported in part by Grant 1641 from the Hungarian National Foundation for Scientific Research.

distinguish polynomials differing by a constant multiple.) We shall prove that the Posner and Rumsey conjecture is true in a rather strong sense for $i = 3$ and false for $i \geqslant 4$. More precisely we shall prove the following theorem:

Theorem 1. *Let $p \in \mathbb{Q}[x] \setminus \mathbb{Q}$, k be the number of distinct roots of $p(x)$, K the splitting field of $p(x)$ over $\mathbb{Q}$, $d = [K : \mathbb{Q}]$, S the set of places of K consisting of all infinite places and all valuations induced by the prime ideal factors of the non-zero roots of $p(x)$, and $s = \operatorname{card} S$. If $p(x)$ divides more than*

$$(4sd)^{s^6 \cdot 2^{180d} + 8sk} \tag{1}$$

standard trinomials over $\mathbb{Q}$, then it divides a linear or quadratic polynomial in x^r over $\mathbb{Q}$ for some integer $r \geqslant 1$.

It should be observed that the bound in (1) depends only on d, k and s, but not on the size of the coefficients of $p(x)$. We note that following our proof of Theorem 1, Theorem 1 can be easily generalized to the case where the ground field is not necessarily $\mathbb{Q}$, but an arbitrary algebraic number field. We do not work out this generalization in the present paper.

The following more general qualitative result provides a criterion for a polynomial to divide infinitely many standard trinomials over a field of characteristic 0.

Theorem 2A. *Let K be a field of characteristic 0. A polynomial $p \in K[x]$ divides infinitely many standard trinomials over K if and only if it divides a linear or quadratic polynomial in x^r over K for some integer $r \geqslant 1$.*

Theorem 2A can be refined as follows:

Theorem 2B. *Let K be a field of characteristic 0. For each polynomial $p \in K[x]$ there exists a finite set F of standard trinomials over K such that if $T(x) = x^m + ax^n + b \in K[x] \setminus F$, $ab \neq 0$ and $p \mid T$, then*

$$p \mid q\left(x^{(m,n)}\right) \mid T(x),$$

where $q \in K[x]$, $\deg q \leqslant 2$.

The following theorem disproves the conjecture of Posner and Rumsey for every $i \geqslant 4$.

Theorem 3A. *For every $i \geqslant 2$ there exists a polynomial $p \in \mathbb{Q}[x]$ that divides infinitely many standard quadrinomials over $\mathbb{Q}$, but that does not divide any non-zero polynomial of degree less than i in x^r over $\mathbb{Q}$ for any integer $r \geqslant 1$.*

The quadrinomials of the form constructed in the proof of Theorem 3A have the constant term zero. For polynomials with the constant term non-zero the relevant problem is harder and we can only prove

Theorem 3B. *For every $i \geqslant 2$ there exists a polynomial $p \in \mathbb{Q}[x]$ that divides infinitely many standard quintinomials over $\mathbb{Q}$ with the constant term non-zero, but does not divide any non-zero polynomial of degree less than i in x^r over $\mathbb{Q}$ for any integer $r \geqslant 1$.*

The proofs of Theorem 1 and Theorems 2A and 2B are based on known results on S-unit equations, while the proof of Theorems 3A and 3B is quite elementary. The following problem remains open.

Problem. Let K be a field of characteristic 0. Is it true that a polynomial $p \in K[x]$ with $p(0) \neq 0$ divides infinitely many standard k-nomials with the constant term non-zero if and only if either p divides a non-zero polynomial of degree less than k in x^r over K for any integer $r \geqslant 1$ or divides a standard $\left[\frac{k+1}{2}\right]$-nomial?

2. Proofs

To prove Theorem 1, we need some results on S-unit equations.

Let K be an algebraic number field of degree d over $\mathbb{Q}$, M_K the set of places on K, S a finite subset of M_K containing all infinite places, s the cardinality of S, and U_S the multiplicative group of S-units in K. For $n \geqslant 2$, consider the S-unit equation

$$\alpha_1 u_1 + \ldots + \alpha_n u_n = 1 \quad \text{in} \quad u_1, \ldots, u_n \in U_S, \tag{2}$$

where $\alpha_1, \ldots, \alpha_n$ are elements of K^*, the set of non-zero elements of K. A solution $u_1, \ldots, u_n$ is called non-degenerate if $\alpha_1 u_1 + \ldots + \alpha_n u_n$ has no non-empty vanishing subsum. For $n = 2$, all solutions are non-degenerate. Denote by $v_s(\alpha_1, \ldots, \alpha_n)$ the number of non-degenerate solutions of (2). Evertse [4] proved the following

Lemma 1. *We have*

$$v_S(\alpha_1, \alpha_2) \leqslant 3 \times 7^{d+2s} \quad \textit{for all} \quad (\alpha_1, \alpha_2) \in (K^*)^2.$$

In the general case, Schlickewei [14] showed

Lemma 2. *For $n \geqslant 2$ we have*

$$v_S(\alpha_1, \ldots, \alpha_n) \leqslant (4sd!)^{2^{36nd!} \cdot s^6} \quad \textit{for all} \quad (\alpha_1, \ldots \alpha_n) \in (K^*)^n.$$

Further, if $K/\mathbb{Q}$ is a normal extension then $d!$ can be replaced by d.

We call two n-tuples $(\alpha_1, \ldots, \alpha_n)$ and $(\beta_1, \ldots, \beta_n)$ in $(K^*)^n$ (and the corresponding S-unit equations) S-equivalent if there are S-units $\varepsilon_1, \ldots, \varepsilon_n$ such that $\beta_i = \varepsilon_i \alpha_i$ for $i = 1, \ldots, n$. If $(\alpha_1, \ldots, \alpha_n)$ and $(\beta_1, \ldots, \beta_n)$ are S-equivalent then $v_S(\alpha_1, \ldots, \alpha_n) = v_S(\beta_1, \ldots, \beta_n)$. Evertse *et al.* [7, Theorem 1] proved that in case $n = 2$, Eq. (2) has at most two solutions for all but finitely many S-equivalence classes of pairs $(\alpha_1, \alpha_2) \in (K^*)^2$. The proof of this result depends among other things on the fact that

$$v_{S,n} := v_S(\underbrace{1, \ldots, 1}_{n \text{ times}}) < \infty \text{ for all } n \leqslant 5.$$

Following the proof of Theorem 1 of [7], it is easy to show that apart from at most

$$v_{S,5} + 12 v_{S,3} + 30 v_{S,2}^2 \tag{3}$$

S-equivalence classes of pairs $(\alpha_1, \alpha_2) \in (K^*)^2$, the equation

$$\alpha_1 u_1 + \alpha_2 u_2 = 1 \qquad \text{in } u_1, u_2 \in U_S \tag{4}$$

has at most two solutions (see, e.g., Győry [8]; some generalizations to the case $n \geqslant 2$ are given in a paper of Győry and Tijdeman (in preparation)). Together with Lemma 2, this gives immediately the following

Lemma 3. *Apart from at most*

$$2(4sd!)^{2^{180d!}s^6}$$

S-equivalence classes of pairs $(\alpha_1, \alpha_2) \in (K^*)^2$, Eq. (4) has at most two solutions. Further, if $K/\mathbb{Q}$ is a normal extension then $d!$ can be replaced by d.

Proof of Theorem 1. Let $p(x) \in \mathbb{Q}[x] \setminus \mathbb{Q}$ be a polynomial satisfying the assumptions of Theorem 1. We may assume without loss of generality that $p(x)$ is monic. Let $T(x)$ be an arbitrary but fixed standard trinomial over $\mathbb{Q}$ which is divisible by $p(x)$. Then $T(x)$ can be written in the form

$$T(x) = x^m + ax^n + b \qquad \text{with some } m > n \text{ and } a, b \in \mathbb{Q}. \tag{5}$$

First consider the case when $p(x)$ is divisible by x. Then we have $p(x) = x^t p_1(x)$ with some integer $t \geqslant 1$ and some monic polynomial $p_1(x) \in \mathbb{Q}[x]$ which is not divisible by x. This implies that $b = 0$. If $p_1(x)$ is not constant then $a \neq 0$, $n \geqslant t$, and $p_1(x) \mid x^{m-n} + a$ over $\mathbb{Q}$. In this case $p(x) \mid q(x^r)$ over $\mathbb{Q}$ for $q(x) = (x - (-a)^n)x$ and $r = n(m-n)$. If $p_1(x)$ is constant then $p(x) \mid q(x^r)$ for $q(x) = x$ and $r = t$, and our theorem is proved.

Next consider the case when $p(x)$ is not divisible by x. By the result of Hajós [9]; see also [10, Lemma 1], $T(x)$ cannot have a zero of multiplicity $\geqslant 3$ except 0. Consequently, we may write

$$p(x) = p_1(x)p_2^2(x),$$

where p_1, p_2 are relatively prime square-free monic polynomials in $\mathbb{Q}[x]$.

If, in $T(x)$, $a = 0$ or $b = 0$ then the assertion of Theorem 1 easily follows. Hence, in what follows, we assume that $ab \neq 0$. Let $\xi_1, \ldots, \xi_k$ be the roots of $p_1(x) \cdot p_2(x)$. These roots are all distinct and different from 0. Further, they are all S-units in K. It follows from $p(x) \mid T(x)$ that

$$\xi_j^m + a\xi_j^n + b = 0 \qquad \text{for } j = 1, \ldots, k. \tag{6}$$

This implies that for $j = 1, \ldots, k$, (ξ_j^m, ξ_j^n) is a solution of the S-unit equation

$$(-1/b)u + (-a/b)v = 1 \qquad \text{in } u, v \in U_S. \tag{7}$$

(A) First consider those trinomials $T(x) = x^m + ax^n + b$ $(ab \neq 0)$ over $\mathbb{Q}$ for which $p(x) \mid T(x)$ and for which the corresponding Eq. (7) has at most two solutions in U_S. Fix such a trinomial $T(x) = x^m + ax^n + b$. Then among the pairs $\langle \xi_j^m, \xi_j^n \rangle$, $j = 1, \ldots, k$, there are at most two different ones, say $\langle u_1, v_1 \rangle$, and $\langle u_2, v_2 \rangle$. These pairs are conjugate or both rational, and they may be identical. Hence we obtain that

$$p_1(x)p_2(x) \mid q(x^m) \text{ over } \mathbb{Q},$$

where

$$q(x) = \begin{cases} (x-u_1)(x-u_2) & \text{if } u_1/u_2 \text{ is not a root of unity,} \\ (x^N - u_1^N)^2 & \text{if } u_1/u_2 \text{ is a root of unity of order } N, \end{cases}$$

and $q(x) \in \mathbb{Q}[x]$. This proves our theorem in the case when $p(x)$ has no multiple root or when u_1/u_2 is a root of unity.

There remains the case when $p(x)$ has multiple root and u_1/u_2 is not a root of unity. Then $p_2^2(x) \mid T(x)$, whence $p_2(x) \mid T'(x)$ and so

$$p_2(x) \;\Big|\; a\,\frac{m-n}{m}\,x^n + b \quad \text{over } \mathbb{Q}.$$

Consequently, for each root ξ_j of $p_2(x)$, we have $\xi_j^n \in \mathbb{Q}$. This implies that $\xi_j^m \in \mathbb{Q}$. Since ξ_j^m is equal to u_1 or u_2 for each j, $1 \leqslant j \leqslant k$, it follows that u_1 and u_2 are rational numbers. Further, this implies that ξ_j^m and ξ_j^n are rational numbers for $j = 1, \ldots, k$. If ξ_j^m assume the same value, say u_1, for $j = 1, \ldots, k$, then $p(x) \mid (x^m - u_1)^2$ and Theorem 1 is proved. Hence assume that there are i and j for which $\xi_i^m \neq \xi_j^m$.

We use now a refinement of an argument of Posner and Rumsey [13]. Denote by t the least positive integer for which $\xi_j^t \in \mathbb{Q}$ for $j = 1, \ldots, k$. Then t depends only on $p(x)$. Further, t divides both m and n. Put $m = tm_1$, $n = tn_1$ with $m_1, n_1 \in \mathbb{N}$. Let ξ_i be one of the multiple roots of $p(x)$, and let ξ_j be any other root of $p(x)$ for which $\xi_j^m \neq \xi_i^m$. Since u_1/u_2 is not a root of unity, it follows that ξ_j/ξ_i also is not a root of unity. Further, $T(\xi_j) = T(\xi_i) = T'(\xi_i) = 0$, whence

$$\begin{vmatrix} \xi_j^m & \xi_j^n & 1 \\ \xi_i^m & \xi_i^n & 1 \\ m\xi_i^{m-1} & n\xi_i^{n-1} & 0 \end{vmatrix} = 0. \tag{8}$$

Putting $\vartheta = (\xi_j/\xi_i)^t$, ϑ is a non-zero rational number which is not a root of unity; i.e., ϑ is different from ± 1. Further, we get from (8) that

$$m_1(\vartheta^{n_1} - 1) = n_1(\vartheta^{m_1} - 1). \tag{9}$$

We can write $\vartheta = e/f$ with coprime rational integers e, f such that $e \neq \pm f$. Then it follows from (9) that

$$m_1 f^{m_1 - n_1}(e^{n_1} - f^{n_1}) = n_1(e^{m_1} - f^{m_1}). \tag{10}$$

A prime factor p of $e^{m_1} - f^{m_1}$ is called primitive if $p \nmid e^h - f^h$ for each integer h with $0 < h < m_1$. Suppose that $m_1 > 6$. Then, by a theorem of Zsigmondy [15] and Birkhoff and Vandiver [1], $e^{m_1} - f^{m_1}$ has a primitive prime factor p. It follows from (10) that $p \mid m_1$; i.e., $m_1 = pm_2$ with some positive integer m_2. But

$$0 \equiv e^{m_1} - f^{m_1} \equiv e^{m_2} - f^{m_2} \pmod{p},$$

which is a contradiction. Hence $m_1 \leqslant 6$, and $1 \leqslant n_1 < m_1$. The number of pairs $\langle m_1, n_1 \rangle$ having this property is $\binom{6}{2} = 15$ ([1]). Hence, if $p(x)$ divides more than 15 trinomials of

([1]) Using a more explicit version of the theorem of Zsigmondy and Birkhoff and Vandiver, this bound of 15 could be still further improved.

the form $x^m + ax^n + b$ $(ab \neq 0)$ over $\mathbb{Q}$ for which the corresponding Eq. (7) has at most two solutions and for which the roots u_1, u_2 of the corresponding polynomial $q(x)$ have the property that u_1/u_2 is not a root of unity, then among these trinomials there are two different ones, say $x^m + a_1x^n + b_1$ and $x^m + a_2x^n + b_2$, in which the exponents m, n are the same. But then $p(x) \mid x^n + c$ for some $c \in \mathbb{Q}$ which proves our theorem.

Thus we have proved that if $p(x)$ divides more than 15 trinomials of the form $x^m + ax^n + b$ $(ab \neq 0)$ over $\mathbb{Q}$ for which the corresponding Eq. (7) has at most two solutions then the assertion of the theorem follows.

(B) Next consider those trinomials $T(x) = x^m + ax^n + b$ $(ab \neq 0)$ over $\mathbb{Q}$ for which $p(x) \mid T(x)$ and for which the corresponding Eq. (7) has at least three solutions in U_S. If $x^m + ax^n + b$ and $x^{m'} + a'x^{n'} + b'$ are such trinomials and if the corresponding equations of the form (7) are S-equivalent then $a' = a\varepsilon$, $b' = b\eta$ with some $\varepsilon, \eta \in U_S^0 := U_S \cap \mathbb{Q}^*$. Hence it follows from Lemma 3 that there is a subset $\mathscr{A}$ of $(\mathbb{Q}^*)^2$ with cardinality at most

$$C_1 := 2(4sd)^{2^{180d}\cdot s^6}$$

such that for each trinomial $x^m + ax^n + b$ under consideration, $a = \varepsilon a_0$, $b = \eta b_0$ with some $\varepsilon, \eta \in U_S^0$ and some $\langle a_0, b_0\rangle \in \mathscr{A}$. Fix such a pair $\langle a_0, b_0\rangle \in \mathscr{A}$, and consider all the trinomials of the form $x^m + \varepsilon a_0 x^n + \eta b_0$ with $\varepsilon, \eta \in U_S^0$, which are divisible by $p(x)$ over $\mathbb{Q}$. If $x^m + \varepsilon a_0 x^n + \eta b_0$ and $x^m + \varepsilon' a_0 x^n + \eta' b_0$ are such trinomials then $p(x) \mid x^n + c$ with some $c \in \mathbb{Q}^*$ and the assertion follows. Hence it is enough to deal with those trinomials for which the pairs $\langle m, n\rangle$ are pairwise distinct. Put

$$C_2 := 3 \times 7^{d+2s},$$

and assume that the maximal number of such trinomials is greater than C_2^{2k}. Then among the pairs $\langle m, n\rangle$ associated with these trinomials there are more than C_2^k distinct m or distinct n. We may assume without loss of generality that in the pairs $\langle m, n\rangle$ in question, $m_1, \ldots, m_u$ are pairwise distinct for $u > C_2^k$. (One can proceed in a similar way if there are more than C_2^k distinct values for n.) Then

$$p(x) \mid T_i(x) = x^{m_i} + \varepsilon_i a_0 x^{n_i} + \eta_i b_0 \text{ over } \mathbb{Q} \text{ for } i = 1, \ldots, u,$$

and hence, for each i,

$$(-1/b_0)(\xi_j^{m_i}/\eta_i) + (-a_0/b_0)(\varepsilon_i \xi_j^{n_i}/\eta_i) = 1 \qquad \text{for } j = 1, \ldots, k,$$

where $\varepsilon_i, \eta_i \in U_S^0$ for $i = 1, \ldots, u$. It follows from Lemma 1 that for each j with $1 \leqslant j \leqslant k$, $\xi_j^{m_i}/\eta_i$ can assume at most C_2 values. Hence, by the assumption $u > C_2^k$, there are distinct i_1 and i_2 with $1 \leqslant i_1, i_2 \leqslant u$ such that

$$\xi_j^{m_{i_1}}/\eta_{i_1} = \xi_j^{m_{i_2}}/\eta_{i_2} \qquad \text{for } j = 1, \ldots, k.$$

We may assume that $m_{i_1} > m_{i_2}$. Putting $r = m_{i_1} - m_{i_2}$ and $\eta = \eta_{i_1}/\eta_{i_2}$, we get

$$\xi_j^r = \eta \qquad \text{for } j = 1, \ldots, k.$$

Consequently, $p_1(x)p_2(x) \mid x^r - \eta$ and so $p(x) \mid (x^r - \eta)^2$ over $\mathbb{Q}$, which proves the assertion of our theorem.

Thus we have proved that if there are more than $C_1 \cdot C_2^{2k}$ standard trinomials $T(x) = x^m + ax^n + b$ $(ab \neq 0)$ with $p(x) \mid T(x)$ for which the corresponding Eq. (7) has more than two solutions then the assertion of Theorem 1 follows.

Finally, we obtain that if $p(x)$ divides more than

$$15 + C_1 \cdot C_2^{2k}$$

standard trinomials over $\mathbb{Q}$ then the assertion follows. Since $d/2 \leqslant s$, our theorem is proved. □

To prove Theorem 2A, we need some further lemmas. Now let K be a finitely generated extension field of $\mathbb{Q}$, Γ a finitely generated subgroup of the multiplicative group K^* of non-zero elements of K, and $\alpha_1, \ldots, \alpha_n \in K^*$ $(n \geqslant 2)$. As a generalization of Eq. (2), consider the generalized unit equation

$$\alpha_1 u_1 + \ldots + \alpha_n u_n = 1 \qquad \text{in } u_1, \ldots, u_n \in \Gamma. \tag{11}$$

The degeneracy of a solution $u_1, \ldots, u_n$ can be defined in the same way as in case of Eq. (2). The following lemma is a generalization of non-explicit character of Lemmas 1 and 2.

Lemma 4. *The number of non-degenerate solutions of* (11) *is at most* $C_1 = C_1(n, \Gamma)$, *where* C_1 *is a number depending only on* n *and* Γ.

For a proof, see Evertse and Győry [6]. In this generality, the finiteness of the number of non-degenerate solutions of (11) was earlier claimed by van der Poorten and Schlickewei [11]; see also their recent paper [12]. We note that for $n = 2$ an explicit expression for C_1 was given in [5].

Consider now the case $n = 2$; i.e., the equations of the form

$$\alpha_1 u_1 + \alpha_2 u_2 = 1 \qquad \text{in } u_1, u_2 \in \Gamma. \tag{12}$$

Equivalence of pairs and generalized unit equations can be defined in the same way as in the number field case.

The next lemma is a qualitative generalization of Lemma 3.

Lemma 5. *Apart from finitely many equivalence classes of pairs* $(\alpha_1, \alpha_2) \in (K^*)^2$, *Eq.* (12) *has at most two solutions.*

This result is due to Evertse *et al.* [7]. In fact, this was explicitly stated in [7] only for the case when K is an algebraic number field, but it was indicated at p. 464 in [7] how to prove this general version.

Lemma 6. *Let* ϑ *be a non-zero element of* K *which is not a root of unity. Then there are only finitely many pairs* $\langle m, n \rangle$ *of positive integers with* $m > n$ *such that*

$$\frac{\vartheta^m - 1}{m} = \frac{\vartheta^n - 1}{n}. \tag{13}$$

c It is enough to prove Lemma 6 in the number field case since (13) implies that ϑ is algebraic. The following lemma will be established in a quantitative form for two reasons. On one hand, this explicit version is interesting in itself. Further, together with Lemmas 1 to 3, it makes it possible to generalize Theorem 1 to the case of polynomials considered over an arbitrary but fixed algebraic number field.

In what follows, $c_1, c_2, \ldots, c_8$ denote effectively computable positive absolute constants.

Lemma 7. *If ϑ is an algebraic number of degree $d > 1$, different from zero and roots of unity, $m > n \geqslant 1$ are integers and* (13) *holds, then*

$$m \leqslant c_1 d \frac{(\log d)^4}{(\log\log ed)^3}. \tag{14}$$

For $d = 1$, a more explicit version of Lemma 7 was implicitly proved in the proof of our Theorem 1.

To prove Lemma 7, we need the following:

Lemma 8. *If $x \in \mathbb{C}$ satisfies $|x| \geqslant x_0 > 1$ and $x^m/m - x^n/n = a \in \mathbb{C}$ where $x_0 < 2$, $|a| \leqslant 1$, then*

$$m \leqslant -c_2 \frac{\log\log x_0}{\log x_0}.$$

Proof of Lemma 8. The equation $x^m/m - x^n/n = a$ gives $|x|^m/m - |x|^n/n \leqslant |x^m/m - x^n/n| = |a| \leqslant 1$. Now $|x|^n/n$ as a function of n is decreasing for $n \leqslant 1/\log|x|$ and increasing for $n > 1/\log|x|$. Hence we obtain

$$\frac{|x|^m}{m} \leqslant \max\left\{|x| + 1,\ \frac{|x|^{m-1}}{m-1} + 1\right\} \leqslant \max\left\{2|x|,\ \frac{|x|^{m-1}}{m-1} + 1\right\}.$$

Thus either

$$|x|^{m-1} \leqslant 2m$$

or

$$|x|^{m-1}\left(\frac{|x|}{m} - \frac{1}{m-1}\right) \leqslant 1.$$

The first inequality gives

$$(m-1)\log x_0 \leqslant \log 2m,$$

whence

$$\frac{m-1}{\log 2m} \leqslant (\log x_0)^{-1}, \quad \text{and so} \quad m \leqslant -c_3 \frac{\log\log x_0}{\log x_0}.$$

The second inequality gives either

$$\frac{|x|}{m} - \frac{1}{m-1} \leqslant \frac{1}{m(m-1)}, \quad \text{i.e.,} \quad m \leqslant \frac{|x|+1}{|x|-1} \leqslant \frac{x_0+1}{x_0-1} \leqslant -c_4 \frac{\log\log x_0}{\log x_0},$$

or

$$|x|^{m-1} \leqslant m(m-1), \quad \text{whence} \quad (m-1)\log x_0 \leqslant \log m(m-1),$$

i.e.,

$$m \leqslant -c_5 \frac{\log\log x_0}{\log x_0}. \qquad \square$$

Proof of Lemma 7. We shall consider three cases: (1) ϑ is an algebraic integer, (2) ϑ^{-1} is an algebraic integer, (3) neither ϑ nor ϑ^{-1} is an algebraic integer.

In the Case 1, we choose a conjugate ϑ' of ϑ such that

$$\log|\vartheta'| > \frac{c_6}{d}\left(\frac{\log\log ed}{\log d}\right)^3.$$

It exists by Dobrowolski's theorem [3] and it also satisfies (13). Using Lemma 8 with

$$x = \vartheta', \quad x_0 = \exp\left\{\frac{c_7}{d}\left(\frac{\log\log ed}{\log d}\right)^3\right\},$$

where c_7 is a suitable positive absolute constant, we obtain (14).

In the Case 2, we choose a conjugate θ of ϑ^{-1} such that

$$\log|\theta| > \frac{c_6}{d}\left(\frac{\log\log ed}{\log d}\right)^3.$$

It exists by Dobrowolski's theorem and it satisfies (13) with n replaced by $m-n$. Using Lemma 8 with

$$x = \theta, \quad x_0 = \exp\left\{\frac{c_7}{d}\left(\frac{\log\log ed}{\log d}\right)^3\right\}$$

we obtain (14).

In the Case 3, there exist prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ of $\mathbb{Q}(\vartheta)$ such that $\operatorname{ord}_{\mathfrak{p}}\vartheta > 0, \operatorname{ord}_{\mathfrak{q}}\vartheta < 0$. Then Eq. (13) gives

$$\operatorname{ord}_{\mathfrak{p}}(m-n) \geqslant n, \qquad \operatorname{ord}_{\mathfrak{q}} n \geqslant m-n,$$

hence

$$(m-n)^d \geqslant 2^n, \qquad n^d \geqslant 2^{m-n}, \qquad \left(\frac{m^2}{4}\right)^d \geqslant 2^m,$$

and so $m \leqslant c_8 d\log d$. $\square$

Proof of Theorem 2A. Let K be a field of characteristic 0. For constant polynomials $p \in K[X]$, the assertion is trivial. Hence we deal only with the case when $p(x)$ is not constant.

Using an argument of Posner and Rumsey [13] applied in the case $K = \mathbb{Q}$, we prove first that if a non-constant polynomial $p \in K[X]$ divides a polynomial of the form $s(x^r)$ for some integer $r \geqslant 1$, where $s(x)$ is linear or quadratic, then $p(x)$ divides infinitely many standard trinomials over K. Indeed, the space of polynomials over K modulo $s(x)$ is at

most two-dimensional. Hence for every pair of positive integers m, n with $m > n$ there are $a, b, c \in K$ such that at least one of a and b is different from 0 and that $s(x)$ divides the trinomial $T(x) = ax^m + bx^n + c$ over K. This implies that $s(x^r)$ divides $T(x^r)$. Since $p(x)$ divides $s(x^r)$, our claim is proved.

Conversely, suppose that $p(x)$ divides infinitely many standard trinomials $T_k(x)$ over K for $k = 1, 2, \ldots$. We show that then $p(x)$ divides a polynomial of the form $s(x^r)$ for some $r \geqslant 1$, where $s(x)$ is linear or quadratic. First we prove this in the particular case when K is a finitely generated extension field of $\mathbb{Q}$. For this purpose, it suffices to repeat the proof of our Theorem 1 in this generality, without giving quantitative estimates and with the following changes. Replace $\mathbb{Q}$ by K; replace U_S by Γ, the multiplicative group generated by the non-zero roots of $p(x)$ in the splitting field of $p(x)$ over K; and apply Lemmas 4 to 6 in place of Lemmas 2 to 3 and the theorem of Zsigmondy or Birkhoff and Vandiver, respectively.

Next consider the general case (when K is an arbitrary field of characteristic 0). Denote by $a_0, a_1, \ldots, a_n$ the coefficients of $p(x)$, and by K_0 the subfield of K generated by $a_0, \ldots, a_n$ over $\mathbb{Q}$. Then K_0 is finitely generated over $\mathbb{Q}$. Since the standard trinomials $T_k(x)$ are divisible by $p(x)$, they can be written in the form

$$T_k(x) = x^{m_k} + x^{n_k}\Big(b_{k,0} + \sum_{i=1}^{N_k} b_{k,i} w_{k,i}\Big) + \Big(c_{k,0} + \sum_{i=1}^{N_k} c_{k,i} w_{k,i}\Big),$$

where $b_{k,i}, c_{k,i} \in K_0$ $(i = 0, 1, \ldots, N_k)$ and 1, $w_{k,i}$ $(i = 1, \ldots, N_k)$ are linearly independent elements of K over K_0, $N_k \leqslant 2$. Let

$$x^{m_k} + b_{k,0}x^{n_k} + c_{k,0} = p(x)q_{k,0}(x) + r_{k,0}(x)$$

and

$$b_{k,i}x^{n_k} + c_{k,i} = p(x)q_{k,i}(x) + r_{k,i}(x)$$

over K_0, where $\deg r_{k,i} < \deg p$ for $i = 0, 1, \ldots, N_k$. The divisibility $p(x) \mid T_k(x)$ gives

$$r_{k,0}(x) + \sum_{i=1}^{N_k} r_{k,i}(x) w_{k,i} \equiv 0 \pmod{p(x)},$$

whence $r_{k,i}(x) = 0$ $(i = 0, \ldots, N_k)$ and thus $p(x) \mid b_{k,i}x^{n_k} + c_{k,i}$ over K_0 for $i = 1, \ldots, N_k$. This implies the required assertion unless $b_{k,i} = c_{k,i} = 0$ for $i = 1, \ldots, N_k$ and for all k. But in this case the trinomials $T_k(x) = x^{m_k} + b_{k,0}x^{n_k} + c_{k,0}$ have their coefficients in K_0, and we can use the truth of the assertion for the ground field K_0. This completes the proof of Theorem 2A. □

For the proof of Theorem 2B we need two lemmas.

Lemma 9. *Let x_1, x_2, y_1, y_2 be roots of unity. If*

$$D = \begin{vmatrix} 1 & 1 & 1 \\ x_1 & x_2 & 1 \\ y_1 & y_2 & 1 \end{vmatrix} = 0$$

then either two rows or two columns of the determinant are identical.

Proof. D is the sum of six roots of unity. By Theorem 6 of [2] there are three possibilities:

(a) the sum can be split into three parts each consisting of two terms and each equal to 0;
(b) the sum can be split into two parts each consisting of three terms, proportional in some order to $1, \zeta_3, \zeta_3^2$, where ζ_3 is a primitive root of unity of order 3;
(c) the six terms are proportional in some order to $-\zeta_3, -\zeta_3^2, \zeta_5, \zeta_5^2, \zeta_5^3, \zeta_5^4$.

The lemma follows by a tedious but straightforward consideration of cases [2]. □

Lemma 10. *Let $p(x)$ be a common factor of $(x^M - c)^2 \in K[x]$ and of $T(x) = x^m + ax^n + b \in K[x]$, where $ab \neq 0$. Then*

$$p(x) \mid q\left(x^{(m,n)}\right) \mid T(x),$$

where $q \in K[x]$, $\deg q \leqslant 2$.

Proof. Since $p(x) \mid (x^M - c)^2$ and $p(0) \neq 0$, p has no zero of multiplicity greater than 2. Assume first that p has a double zero ξ. Then $T(\xi) = T'(\xi) = 0$, which gives

$$\xi^m = \frac{bn}{m-n}, \quad \xi^n = -\frac{bm}{a(m-n)}.$$

For every other zero ζ of p, ζ/ξ is a root of unity, hence

$$\zeta^m = \frac{bnx}{m-n}, \quad \zeta^n = -\frac{bmy}{a(m-n)},$$

where x, y are roots of unity. The equation $T(\zeta) = 0$ gives

$$nx - my + m - n = 0.$$

By taking complex conjugates we obtain $n/x - m/y + m - n = 0$. These two equations in x and y imply $x = y = 1$; $\zeta^m = \xi^m$, $\zeta^n = \xi^n$,

$$\zeta^{(m,n)} = \xi^{(m,n)} \in K.$$

It follows that $p(x) \mid q\left(x^{(m,n)}\right)$, where $q = (x - \xi^{(m,n)})^2$.

If $p(x)$ has no multiple zeros it suffices to show that for $S = \{\xi^{(m,n)} : p(\xi) = 0\}$ we have $\#S \leqslant 2$. Indeed, we then take $q(x) = \prod_{u \in S} (x - u)$.

Suppose that $\#S \geqslant 3$. Then there exists a zero ξ of p and two distinct roots of unity $\zeta_M^{e_1}$, $\zeta_M^{e_2}$ different from 1 such that

$$\xi^m \zeta_M^{e_i(m/(m,n))} + a\xi^n \zeta_M^{e_i(n/(m,n))} + b = 0 \qquad (i = 0, 1, 2), \tag{15}$$

where we have put $e_0 = 0$. Since $ab \neq 0$ we have

$$\begin{vmatrix} 1 & 1 & 1 \\ \zeta_M^{e_1(m/(m,n))} & \zeta_M^{e_1(n/(m,n))} & 1 \\ \zeta_M^{e_2(m/(m,n))} & \zeta_M^{e_2(n/(m,n))} & 1 \end{vmatrix} = 0.$$

[2] For a simpler proof, due to J. Browkin, see this collection, D15, proof of Lemma 1, p. 633.

By Lemma 9 we have either for some distinct $i, j \in \{0, 1, 2\}$

$$\zeta_M^{e_i(m/(m,n))} = \zeta_M^{e_j(m/(m,n))}, \qquad \zeta_M^{e_i(n/(m,n))} = \zeta_M^{e_j(n/(m,n))} \tag{16}$$

or

$$\zeta_M^{e_1(m/(m,n))} = 1, \quad \text{or} \quad \zeta_M^{e_1(n/(m,n))} = 1, \quad \text{or} \quad \zeta_M^{e_1(m/(m,n))} = \zeta_M^{e_1(n/(m,n))}. \tag{17}$$

Now (16) gives $\zeta_M^{e_i} = \zeta_M^{e_j}$, a contradiction; (17) gives, in view of (15),

$$\zeta_M^{e_1(m/(m,n))} = \zeta_M^{e_1(n/(m,n))} = 1,$$

hence $\zeta_M^{e_1} = 1$, a contradiction. □

Proof of Theorem 2B. To prove Theorem 2B we follow the proof of Theorem 2A and at a crucial point we use Lemma 10. □

Proof of Theorems 3A *and* 3B. Let $i \geqslant 2$ be an arbitrary integer, and consider the polynomial

$$p(x) = x^p + 2x + 2 \tag{18}$$

for some fixed prime $p \geqslant i$. As is known, $p(x)$ is irreducible over $\mathbb{Q}$. Further, $p(x)$ divides infinitely many standard quadrinomials over $\mathbb{Q}$ and infinitely many standard quintinomials over $\mathbb{Q}$ with the constant term different from 0; namely, we have

$$p(x) \mid (x^p + 2x + 2)x^q = x^{p+q} + 2x^{q+1} + 2x^q,$$
$$p(x) \mid (x^p + 2x + 2)(x^p + q) = x^{2p} + 2x^{p+1} + (2 + q)x^p + 2qx + 2q$$

for any integer $q \geqslant 1$.

Suppose now that there are a non-zero polynomial $s(x)$ in $\mathbb{Q}[x]$ with degree less than i and an integer $r \geqslant 1$ such that

$$p(x) \text{ divides } s(x^r) \text{ over } \mathbb{Q}. \tag{19}$$

Since $p(x)$ is irreducible, we may assume that $s(x)$ is also irreducible over $\mathbb{Q}$. Further, its degree, denoted by t, is positive. Denote by $\xi_1, \ldots, \xi_p$ the roots of $p(x)$, and by $\gamma_1, \ldots, \gamma_t$ the roots of $s(x)$. Then (19) implies that $(x - \xi_1)$ divides $x^r - \gamma_j$ for some j $(1 \leqslant j \leqslant t)$ over $\overline{\mathbb{Q}}$. Thus we have

$$\xi_1^r = \gamma_j. \tag{20}$$

Hence $\gamma_j \in \mathbb{Q}(\xi_1)$. But the field $\mathbb{Q}(\xi_1)$ is of degree p over $\mathbb{Q}$, where p is a prime. This implies that either $\gamma_j \in \mathbb{Q}$ or γ_j is of degree p over $\mathbb{Q}$. But the latter case cannot hold because γ_j is of degree at most $i - 1$ and $p \geqslant i$. Hence $\gamma_j \in \mathbb{Q}$ and so $t = 1$. Consequently, it follows from (20) that

$$\xi_j^r = \xi_1^r \qquad \text{for } j = 1, \ldots, p.$$

There are rth roots of unity ζ_j such that $\xi_j = \zeta_j \xi_1$ for $j = 1, \ldots, p$. Comparing the

coefficients of x^{p-1} in the representation (18) and $\prod_{j=1}^{p}(x-\xi_j)$ of $p(x)$, we get

$$0 = \xi_1 + \ldots + \xi_p = \xi_1(\zeta_1 + \ldots + \zeta_p),$$

whence

$$\zeta_1 + \ldots + \zeta_p = 0.$$

Hence the coefficient of x in $p(x) = \prod_{j=1}^{p}(x-\xi_j)$ is

$$\frac{\xi_1\cdots\xi_p}{\xi_1} + \ldots + \frac{\xi_1\cdots\xi_p}{\xi_p} = \frac{\xi_1\cdots\xi_p}{\xi_1}(\zeta_1^{-1} + \ldots + \zeta_p^{-1})$$
$$= \frac{\xi_1\cdots\xi_p}{\xi_1}(\overline{\zeta_1 + \ldots + \zeta_p}) = 0,$$

which contradicts the fact that in (18), the coefficient of x in $p(x)$ is equal to 2. This completes the proof of Theorems 3A and 3B. □

References

[1] G. D. Birkhoff, H. S. Vandiver, *On the integral divisors of $a^n - b^n$*. Ann. of Math. (2) 5 (1904), 173–180.

[2] J. H. Conway, A. J. Jones, *Trigonometric Diophantine equations* (*On vanishing sums of roots of unity*). Acta Arith. 30 (1976), 229–240.

[3] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*. Acta Arith. 34 (1979), 391–401.

[4] J. H. Evertse, *On equations in S-units and the Thue–Mahler equation*. Invent. Math. 75 (1984), 561–584.

[5] J. H. Evertse, K. Győry, *On unit equations and decomposable form equations*. J. Reine Angew. Math. 358 (1985), 6–19.

[6] —, —, *On the numbers of solutions of weighted unit equations*. Compositio Math. 66 (1988), 329–354.

[7] J. H. Evertse, K. Győry, C. L. Stewart, R. Tijdeman, *On S-unit equations in two unknowns*. Invent. Math. 92 (1988), 461–477.

[8] K. Győry, *Upper bounds for the numbers of solutions of unit equations in two unknowns*. Liet. Mat. Rink. 32 (1992), 53–58; Lithuanian Math. J. 32 (1992), 40–44.

[9] G. Hajós, *Solution of Problem 41*. Mat. Lapok 4 (1953), 40–41 (Hungarian).

[10] H. L. Montgomery, A. Schinzel, *Some arithmetic properties of polynomials in several variables*. In: Transcendence Theory: Advances and Applications (ed. A. Baker and D. Masser), Academic Press, London 1977, 195–203; this collection: E6, 747–754.

[11] A. J. van der Poorten, H. P. Schlickewei, *The growth condition for recurrence sequences*. Macquarie Univ. Math. Rep. 82–0041, North Ryde 1982.

[12] —, —, *Additive relations in fields*. J. Austral. Math. Soc. Ser. A 51 (1991), 154–170.

[13] E. C. Posner, H. Rumsey, Jr., *Polynomials that divide infinitely many trinomials*. Michigan Math. J. 12 (1965), 339–348.

[14] H. P. Schlickewei, *S-unit equations over number fields*. Invent. Math. 102 (1990), 95–107.

[15] K. Zsigmondy, *Zur Theorie der Potenzreste*. Monatsh. Math. 3 (1892), 265–284.

Andrzej Schinzel
Selecta

Originally published in
Acta Arithmetica XC (1999), 273–289

Reducibility of lacunary polynomials XII

In memory of Paul Erdős

E. Bombieri and U. Zannier [1] have recently proved an important theorem, which permits improving most of the results of papers VII, VIII, X and XI of this series. In order to state the results I shall use the same notation as in those papers, explained below, together with a new usage of the matrix notation.

$\mathbb{N}$ and $\mathbb{N}_0$ are the sets of positive and non-negative integers, respectively, $\overline{\mathbb{Q}}$ is the field of algebraic numbers.

Bold face letters denote vectors written horizontally, $\boldsymbol{x} = [x_1, \dots, x_k]$, $\boldsymbol{x}^{-1} = [x_1^{-1}, \dots, x_k^{-1}]$ and similarly for $\boldsymbol{z}$; $\boldsymbol{ab}$ is the scalar product of $\boldsymbol{a}$ and $\boldsymbol{b}$.

The set of $k \times l$ integral matrices is denoted by $\mathfrak{M}_{k,l}(\mathbb{Z})$, and the identity matrix of order k by $\boldsymbol{I}_k$. For a matrix $\boldsymbol{A} = (a_{ij}) \in \mathfrak{M}_{k,l}(\mathbb{Z})$ we put

$$h(\boldsymbol{A}) = \max_{i,j} |a_{ij}|, \quad \boldsymbol{x}^{\boldsymbol{A}} = \Big[\prod_{i=1}^{k} x_i^{a_{i1}}, \dots, \prod_{i=1}^{k} x_i^{a_{il}} \Big].$$

For a Laurent polynomial $F \in \boldsymbol{K}[\boldsymbol{x}, \boldsymbol{x}^{-1}]$, where $\boldsymbol{K}$ is any field, if $F = \prod_{i=1}^{k} x_i^{\alpha_i} F_0(\boldsymbol{x})$, where $F_0 \in \boldsymbol{K}[\boldsymbol{x}]$ and $(F_0, \prod_{i=1}^{k} x_i) = 1$ we put

$$JF = F_0.$$

A polynomial F is *reciprocal* if $JF(\boldsymbol{x}^{-1}) = \pm F(\boldsymbol{x})$.

A polynomial is *irreducible* over $\boldsymbol{K}$ if it is not reducible over $\boldsymbol{K}$ and not a constant. For $\boldsymbol{K} = \mathbb{Q}$ we omit the words "over $\mathbb{Q}$". If $F = c \prod_{\sigma=1}^{s} F_\sigma^{e_\sigma}$, where $c \in \boldsymbol{K}^*$, F_σ are irreducible over $\boldsymbol{K}$ and pairwise coprime, and $e_\sigma \geqslant 1$ $(1 \leqslant \sigma \leqslant s)$, we write

$$F \overset{\text{can}}{\underset{\boldsymbol{K}}{=}} \text{const} \prod_{\sigma=1}^{s} F_\sigma^{e_\sigma}$$

and call this a *canonical factorization* of F over $\boldsymbol{K}$. If $\boldsymbol{K} = \mathbb{Q}$, then $\overset{\text{can}}{\underset{\boldsymbol{K}}{=}}$ is replaced by $\overset{\text{can}}{=}$. If

$$JF \overset{\text{can}}{\underset{\boldsymbol{K}}{=}} \text{const} \prod_{\sigma=1}^{s} F_\sigma^{e_\sigma}$$

we put

$$KF = \text{const} \prod\nolimits^{*} F_\sigma^{e_\sigma},$$

and if $\boldsymbol{K} = \mathbb{Q}$

$$LF = \text{const} \prod\nolimits^{**} F_\sigma^{e_\sigma},$$

where $\prod^*$ is taken over all F_σ that do not divide $J(\boldsymbol{x}^{t\boldsymbol{\alpha}} - 1)$ for any $\boldsymbol{\alpha} \in \mathbb{Z}^k \setminus \{\boldsymbol{0}\}$ and $\prod^{**}$ is taken over all F_σ that are not reciprocal. The leading coefficients (i.e. the coefficients of the first term in the inverse lexicographic order) of KF and LF are equal to that of F. Note that KF depends only on F and the prime field of $\boldsymbol{K}$, which in this paper is always $\mathbb{Q}$.

If T is any transformation of $\boldsymbol{K}[\boldsymbol{x}, \boldsymbol{x}^{-1}]$ into itself and $F \in \boldsymbol{K}[\boldsymbol{x}, \boldsymbol{x}^{-1}]$ then

$$KF(T\boldsymbol{x}) = K\big(F(T\boldsymbol{x})\big),$$

and if $\boldsymbol{K} = \mathbb{Q}$

$$LF(T\boldsymbol{x}) = L\big(F(T\boldsymbol{x})\big).$$

The Bombieri–Zannier theorem can be stated as follows.

Theorem BZ. *Assume that* $P, Q \in \overline{\mathbb{Q}}[\boldsymbol{x}]$ *and* $\boldsymbol{n} \in \mathbb{Z}^k$. *If* $(P, Q) = 1$, *but* $\big(KP(x^{\boldsymbol{n}}), KQ(x^{\boldsymbol{n}})\big) \neq 1$, *then there exists a* $\boldsymbol{\gamma} \in \mathbb{Z}^k$ *such that*

$$\boldsymbol{\gamma n} = 0 \quad \textit{and} \quad 0 < h(\boldsymbol{\gamma}) \leqslant c_1(P, Q),$$

where $c_1(P, Q)$ *depends only on* P *and* Q.

In the sequel $c_i(\dots)$ denote effectively computable positive numbers depending only on the parameters displayed in parentheses. Theorem BZ extends Theorem 1 of [7] from $k \leqslant 3$ to arbitrary k in the crucial case $[\boldsymbol{K} : \mathbb{Q}] < \infty$ and immediately implies that in Theorem 2 of [7],

$$c_2(P, Q) N^{k - \min\{k,6\}/(2k-2)} \frac{(\log N)^{10}}{(\log\log N)^9}$$

can be replaced by

$$c_2(P, Q) N^{k-1}.$$

Theorems 3 and 5 of [7] can now be extended in the following manner.

Theorem 1. *Let* $F \in \mathbb{Z}[\boldsymbol{x}] \setminus \{0\}$, k_0 *be the number of variables with respect to which* F *is of positive degree, and* $||F||$ *be the sum of squares of the coefficients of* F. *Assume* $KF = LF$. *For every vector* $\boldsymbol{n} \in \mathbb{Z}^k$ *such that* $F(x^{\boldsymbol{n}}) \neq 0$ *there exist a matrix* $\boldsymbol{M} = (\mu_{ij}) \in \mathfrak{M}_{k,k}(\mathbb{Z})$ *and a vector* $\boldsymbol{v} \in \mathbb{Z}^k$ *such that*

$$0 \leqslant \mu_{ij} < \mu_{jj} \leqslant \exp(9k_0 \cdot 2^{||F||-5}) \ (i \neq j), \quad \mu_{ij} = 0 \ (i < j), \tag{1}$$

$$\boldsymbol{n} = \boldsymbol{v}\boldsymbol{M}, \tag{2}$$

and either

$$KF(z^{\boldsymbol{M}}) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(z)^{e_\sigma} \tag{3}$$

implies

$$KF(x^{\boldsymbol{n}}) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(x^{\boldsymbol{v}})^{e_\sigma} \tag{4}$$

or there exists a $\boldsymbol{\gamma} \in \mathbb{Z}^k$ *such that*

$$\boldsymbol{\gamma n} = 0 \quad \textit{and} \quad 0 < h(\boldsymbol{\gamma}) \leqslant c_3(F, \boldsymbol{M}). \tag{5}$$

Theorem 4 of [7] is extended as follows.

Theorem 2. *Let* $F \in \mathbb{Q}[\boldsymbol{x}] \setminus \{0\}$, $\boldsymbol{n} \in \mathbb{Z}^{\boldsymbol{k}} \setminus \{\boldsymbol{0}\}$. *If* $JF(x^{\boldsymbol{n}})$ *is not reciprocal, then* $KF(x^{\boldsymbol{n}})$ *is reducible if and only if there exist a matrix* $\boldsymbol{N} \in \mathfrak{M}_{r,k}(\mathbb{Z})$ *of rank* r *and a vector* $\boldsymbol{v} \in \mathbb{Z}^r$ *such that*

$$h(\boldsymbol{N}) \leqslant c_4(F), \tag{6}$$

$$\boldsymbol{n} = \boldsymbol{vN}, \tag{7}$$

$$KF(\boldsymbol{y}^{\boldsymbol{N}}) = F_1 F_2, \quad \boldsymbol{y} = [y_1, \ldots, y_r], \quad F_i \in \mathbb{Q}[\boldsymbol{y}] \ (i = 1, 2), \tag{8}$$

$$KF_i(x^{\boldsymbol{v}}) \notin \mathbb{Q} \ (i = 1, 2). \tag{9}$$

Further we have

Theorem 3. *Let* $F \in \overline{\mathbb{Q}}[\boldsymbol{x}] \setminus \{0\}$, $\boldsymbol{n} \in \mathbb{Z}^{\boldsymbol{k}} \setminus \{\boldsymbol{0}\}$, $\boldsymbol{K}$ *be the field generated over* $\mathbb{Q}$ *by the ratios of the coefficients of* $F(x^{\boldsymbol{n}})$ *and* $\widehat{\boldsymbol{K}}$ *be its normal closure. Assume that* $F \in \boldsymbol{K}[\boldsymbol{x}]$, $F(x^{\boldsymbol{n}}) \neq 0$ *and for all embeddings* τ *of* $\boldsymbol{K}$ *into* $\widehat{\boldsymbol{K}}$,

$$\frac{JF(x^{-\boldsymbol{n}})}{JF^{\tau}(x^{\boldsymbol{n}})} \notin \widehat{\boldsymbol{K}}. \tag{10}$$

If $KF(x^{\boldsymbol{n}})$ *is reducible over* $\boldsymbol{K}$ *there exist a matrix* $\boldsymbol{N} \in \mathfrak{M}_{r,k}(\mathbb{Z})$ *of rank* r *and a vector* $\boldsymbol{v} \in \mathbb{Z}^r$ *such that*

$$h(\boldsymbol{N}) \leqslant c_5(F) \tag{11}$$

$$\boldsymbol{n} = \boldsymbol{vN} \tag{12}$$

and $JF(\boldsymbol{y}^{\boldsymbol{N}})$ *is reducible over* $\widehat{\boldsymbol{K}}$, *where* $\boldsymbol{y} = [y_1, \ldots, y_r]$.

This theorem implies

Corollary 1. *Let* $\boldsymbol{a} = [a_0, \ldots, a_k] \in \overline{\mathbb{Q}}^{*k+1}$, $\boldsymbol{n} = [n_1, \ldots, n_k] \in \mathbb{N}^k$, $0 < n_1 < n_2 < \ldots$ $\ldots < n_k$ *and let* $\boldsymbol{K} = \mathbb{Q}(a_1/a_0, \ldots, a_k/a_0)$. *If* $a_0 \in \boldsymbol{K}$ *and* $K(a_0 + \sum_{j=1}^{k} a_j x^{n_j})$ *is reducible*

over $\boldsymbol{K}$, *then there exist a matrix* $\boldsymbol{N}_0 \in \mathfrak{M}_{[(k+1)/2],k}(\mathbb{Z})$ *and a vector* $\boldsymbol{v}_0$ *in* $\mathbb{Z}^{[(k+1)/2]}$ *such that*

$$h(\boldsymbol{N}_0) \leqslant c_6(\boldsymbol{a}) \tag{13}$$

and

$$\boldsymbol{n} = \boldsymbol{v}_0 \boldsymbol{N}_0 \tag{14}$$

Corollary 2. *Under the assumptions of Corollary* 1 *the number of vectors* $\boldsymbol{n}$ *such that* $n_k \leqslant N$ *and* $K\big(a_0 + \sum_{j=1}^{k} a_j x^{n_j}\big)$ *is reducible over* $\boldsymbol{K}$ *is less than* $c_7(\boldsymbol{a}) N^{[(k+1)/2]}$.

Corollary 3. *Let* $\boldsymbol{a} = [a_0, \ldots, a_k] \in \mathbb{C}^{*k+1}$ *be such that* $a_0 \in \boldsymbol{K} = \mathbb{Q}(a_1/a_0, \ldots, \ldots, a_k/a_0)$. *The number of integer vectors* $\boldsymbol{n} = [n_1, \ldots, n_k]$ *such that* $0 < n_1 < \ldots \ldots < n_k \leq N$ *and* $K(a_0 + \sum_{j=1}^{k} a_j x^{n_j})$ *is reducible over* $\boldsymbol{K}$ *is less than* $c_8(\boldsymbol{a}) N^{k-1}$.

Corollary 1 improves in the case $\boldsymbol{K} = \mathbb{Q}$ and extends Theorem 2 of [3], Corollary 2 drastically improves Theorem 1 of [5]. The exponent $[(k+1)/2]$ cannot be further improved, as will be shown by an example, the gist of which is in [3]. Corollary 3 improves Theorem 2 of [6] and the Theorem of [8].

Further we have

Theorem 4. *Let* $F \in \mathbb{Q}[\boldsymbol{x}] \setminus \{0\}$. *There exist two finite subsets* R *and* S *of* $\bigcup_{r=1}^{k} \mathfrak{M}_{r,k}(\mathbb{Z})$ *with the following property. If* $\boldsymbol{n} \in \mathbb{Z}^k \setminus \{\boldsymbol{0}\}$ *and* $JF(x^{\boldsymbol{n}})$ *is not reciprocal, then* $KF(x^{\boldsymbol{n}})$ *is reducible if and only if the equation* $\boldsymbol{n} = \boldsymbol{v}\boldsymbol{N}$ *is soluble in* $\boldsymbol{v} \in \mathbb{Z}^r$ *and* $\boldsymbol{N} \in R \cap \mathfrak{M}_{r,k}(\mathbb{Z})$ *but insoluble in* $\boldsymbol{v} \in \mathbb{Z}^s$ *and* $\boldsymbol{N} \in S \cap \mathfrak{M}_{s,k}(\mathbb{Z})$ *for each* $s < r$.

The reducibility condition given in Theorem 4 is more readily verifiable than that of Theorem 2, because of the relation (9) occurring in the latter. It is conjectured that a similar reducibility condition holds without the assumption that $JF(x^{\boldsymbol{n}})$ is not reciprocal and over any finite extension of $\mathbb{Q}$.

The proofs of Theorems 1–4 are based on several lemmas.

Lemma 1. *For every polynomial* $P \in \mathbb{Q}[\boldsymbol{x}] \setminus \{0\}$,

$$LKP = LP.$$

Proof. See [2], Lemma 11. □

Lemma 2. *For every polynomial* $F \in \mathbb{Z}[\boldsymbol{x}]$ *and every vector* $\boldsymbol{n} \in \mathbb{Z}^k$ *such that* $F(x^{\boldsymbol{n}}) \neq 0$ *there exist a matrix* $\boldsymbol{M} = (\mu_{ij}) \in \mathfrak{M}_{k,k}(\mathbb{Z})$ *and a vector* $\boldsymbol{v} \in \mathbb{Z}^k$ *such that*

$$0 \leqslant \mu_{ij} < \mu_{jj} \leqslant \exp(9k \cdot 2^{\|F\|-5}) \ (i \neq j), \quad \mu_{ij} = 0 \ (i < j), \tag{15}$$

$$\boldsymbol{n} = \boldsymbol{v}\boldsymbol{M}, \tag{16}$$

and either

$$LF(\boldsymbol{z}^{\boldsymbol{M}}) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma^{e_\sigma}$$

implies

$$LF(x^{\boldsymbol{n}}) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(x^{\boldsymbol{v}})^{e_\sigma},$$

or there exists a vector $\boldsymbol{\gamma} \in \mathbb{Z}^k$ *such that*

$$\boldsymbol{\gamma n} = 0 \quad \textit{and} \quad 0 < h(\boldsymbol{\gamma}) \leqslant c_9(k, F).$$

Proof. See [2], Lemma 12, where $c_9(k, F)$ is given explicitly. □

Lemma 3. *If* $F \in \mathbb{Q}[\boldsymbol{x}]$ *is irreducible and non-reciprocal and a matrix* $\boldsymbol{M} \in \mathfrak{M}_{k,k}(\mathbb{Z})$ *is non-singular, then*

$$LF(\boldsymbol{z}^{\boldsymbol{M}}) = JF(\boldsymbol{z}^{\boldsymbol{M}}).$$

Proof. See [7], Lemma 17. □

Lemma 4. *If* $F \in \mathbb{Q}[\boldsymbol{x}] \setminus \{0\}$, $KF = LF$, $\boldsymbol{M} \in \mathfrak{M}_{k,k}(\mathbb{Z})$ *and* $\det \boldsymbol{M} \neq 0$, *then*

$$KF(\boldsymbol{z}^{\boldsymbol{M}}) = LF(\boldsymbol{z}^{\boldsymbol{M}}). \tag{17}$$

Proof. By Lemma 1 we have, for every polynomial $P \in \mathbb{Q}[\boldsymbol{x}] \setminus \{0\}$,

$$LP \mid KP \mid JP. \tag{18}$$

Assume first that F is irreducible. If $F = cx_i$, $c \in \mathbb{Q}$, then $JF(\boldsymbol{z}^{\boldsymbol{M}}) = c$, hence $KF(\boldsymbol{z}^{\boldsymbol{M}}) = LF(\boldsymbol{z}^{\boldsymbol{M}}) = c$. If $F \mid J(\boldsymbol{x}^{{}^t\boldsymbol{\alpha}} - 1)$ for an $\boldsymbol{\alpha} \in \mathbb{Z}^k \setminus \{\boldsymbol{0}\}$, then $F(z^{\boldsymbol{M}}) \mid J(\boldsymbol{z}^{\boldsymbol{M}^t\boldsymbol{\alpha}} - 1)$, hence $KF(\boldsymbol{z}^{\boldsymbol{M}}) \in \mathbb{Q}$ and (18) implies (17). If $F \neq cx_i$ for all $c \in \mathbb{Q}$ and all $i \leqslant k$, and $F \nmid J(\boldsymbol{x}^{{}^t\boldsymbol{\alpha}} - 1)$ for all $\boldsymbol{\alpha} \in \mathbb{Z}^k \setminus \{\boldsymbol{0}\}$, then $KF = F$, hence $KF = LF$ implies that F is not reciprocal. By Lemma 3 we have $LF(\boldsymbol{z}^{\boldsymbol{M}}) = JF(\boldsymbol{z}^{\boldsymbol{M}})$ and (18) implies (17).

Assume now that

$$F \overset{\text{can}}{=} c \prod_{\sigma=1}^{s} F_\sigma^{e_\sigma}, \quad c \in \mathbb{Q}^*.$$

Then

$$KF = c \prod_{\sigma=1}^{s} KF_\sigma^{e_\sigma}, \quad LF = c \prod_{\sigma=1}^{s} LF_\sigma^{e_\sigma},$$

which together with $KF = LF$ and (18) implies

$$KF_\sigma = LF_\sigma \quad (1 \leqslant \sigma \leqslant s).$$

By the part of the lemma already proved, $KF_\sigma(z^{\boldsymbol{M}}) = LF_\sigma(z^{\boldsymbol{M}})$, hence

$$KF(z^{\boldsymbol{M}}) = c\prod_{\sigma=1}^{s} KF_\sigma(z^{\boldsymbol{M}})^{e_\sigma} = c\prod_{\sigma=1}^{s} LF_\sigma(z^{\boldsymbol{M}})^{e_\sigma} = LF(z^{\boldsymbol{M}}). \qquad \square$$

Lemma 5. *Let $\Phi \in \mathbb{Q}[x]$ be irreducible, $\boldsymbol{\gamma} = (\gamma_1, \dots, \gamma_k) \in \mathbb{Z}^k$, $(\gamma_1, \dots, \gamma_k) = 1$. Then $J\Phi(x^{{}^t\boldsymbol{\gamma}})$ is irreducible.*

Proof. See [4], Lemma 11. $\square$

Lemma 6. *If $F \in \mathbb{Q}[\boldsymbol{x}]$ and $KF \in \mathbb{Q}$, then for every vector $\boldsymbol{v} \in \mathbb{Z}^k$ we have $KF(x^{\boldsymbol{v}}) \in \mathbb{Q}$.*

Proof. It is enough to prove the lemma for F irreducible and different from cx_i $(1 \leqslant i \leqslant k)$, $c \in \mathbb{Q}^*$. The condition $KF \in \mathbb{Q}$ gives

$$F \mid J(x^{{}^t\boldsymbol{\alpha}} - 1), \text{ where } \boldsymbol{\alpha} \in \mathbb{Z}^{\boldsymbol{k}} \setminus \{\boldsymbol{0}\}.$$

If $\boldsymbol{\alpha v} \neq 0$ the conclusion follows at once, but the case $\boldsymbol{\alpha v} = 0$ remains to be considered.

Let $\boldsymbol{\alpha} = a\boldsymbol{\gamma}$, where $a \in \mathbb{N}$, $\boldsymbol{\gamma} \in \mathbb{Z}^k$ and the coordinates of $\boldsymbol{\gamma}$ are relatively prime. We have

$$J(x^{{}^t\boldsymbol{\alpha}} - 1) = \prod_{d \mid a} J\phi_d(x^{{}^t\boldsymbol{\gamma}}),$$

where ϕ_d is the cyclotomic polynomial of order d. By Lemma 5, $J\phi_d(x^{{}^t\boldsymbol{\gamma}})$ is irreducible. Hence $F = cJ\phi_d(x^{{}^t\boldsymbol{\gamma}})$ for a $c \in \mathbb{Q}^*$ and a divisor d of a. The equality $\boldsymbol{\alpha v} = 0$ gives $\boldsymbol{v}^t\boldsymbol{\gamma} = (0)$, hence $JF(x^{\boldsymbol{v}}) = c\phi_d(1) \in \mathbb{Q}$. $\square$

Proof of Theorem 1. Let c_1 have the meaning of Theorem BZ and c_9 the meaning of Lemma 2. We may assume without loss of generality that $F \in \mathbb{Q}[x_1, \dots, x_{k_0}]$ and apply Lemma 2 with k replaced by k_0, $\boldsymbol{n}$ replaced by $\boldsymbol{n}_0 = [n_1, \dots, n_{k_0}]$, and $\boldsymbol{z}$ replaced by $\boldsymbol{z}_0 = [z_1, \dots, z_{k_0}]$. Let $\boldsymbol{M}_0$ and $\boldsymbol{v}_0$ be the matrix and the vector the existence of which is asserted in Lemma 2. We put

$$(\mu_{ij})_{i,j \leqslant k_0} = \boldsymbol{M}_0, \quad \mu_{ii} = 1 \text{ if } i > k_0, \quad \mu_{ij} = 0 \text{ if } i > k_0 \text{ or } j > k_0 \text{ and } i \neq j;$$
$$[v_1, \dots, v_{k_0}] = \boldsymbol{v}_0, \quad v_i = n_i \text{ if } i > k_0.$$

This together with (15) and (16) gives (1) and (2). Moreover, by Lemma 2, either

$$LF(z^{\boldsymbol{M}}) = LF(z_0^{\boldsymbol{M}_0}) \overset{\text{can}}{=} \text{const}\prod_{\sigma=1}^{s_0} F_\sigma^0(z_0)^{e_\sigma^0} \tag{19}$$

implies

$$LF(x^{\boldsymbol{n}}) = LF(x^{\boldsymbol{n}_0}) \overset{\text{can}}{=} \text{const}\prod_{\sigma=1}^{s_0} F_\sigma^0(x^{\boldsymbol{v}_0})^{e_\sigma^0}, \tag{20}$$

or there exists a $\boldsymbol{\gamma}_0 \in \mathbb{Z}^{k_0}$ such that

$$\boldsymbol{\gamma}_0\boldsymbol{n}_0 = 0 \quad \text{and} \quad 0 < h(\boldsymbol{\gamma}_0) \leqslant c_9(k_0, F). \tag{21}$$

By Lemma 4 the left hand sides of (3) and (19) coincide. Since the canonical factorization is essentially unique we have $s = s_0$ and we may assume that $F_\sigma = F_\sigma^0$, $e_\sigma = e_\sigma^0$ $(1 \leqslant \sigma \leqslant s)$. Therefore $\big(JF_\sigma(z^{-1}), F_\sigma(z)\big) = 1$ for all $\sigma \leqslant s$ and the number

$$c_3(F, \boldsymbol{M}) = \max\Big\{c_9(k_0, F), \max_{1 \leqslant \sigma \leqslant s} c_1\big(JF_\sigma(z^{-1}), F_\sigma(z)\big)\Big\} \tag{22}$$

is well defined. We now show that it has the property claimed in the theorem.

By (3) we have

$$F(z^{\boldsymbol{M}}) = F_0(z) \prod_{\sigma=1}^{s} F_\sigma(z)^{e_\sigma}, \tag{23}$$

where $KF_0 \in \mathbb{Q}$. Hence on substitution $z = x^{\boldsymbol{v}}$ we obtain, by (2),

$$F(x^{\boldsymbol{n}}) = F_0(x^{\boldsymbol{v}}) \prod_{\sigma=1}^{s} F_\sigma(x^{\boldsymbol{v}})^{e_\sigma},$$

and, on applying K to both sides, by Lemma 6 we infer that

$$KF(x^{\boldsymbol{n}}) = \text{const} \prod_{\sigma=1}^{s} KF_\sigma(x^{\boldsymbol{v}})^{e_\sigma}.$$

If $KF_\sigma(x^{\boldsymbol{v}}) = LF_\sigma(x^{\boldsymbol{v}})$ for all $\sigma \leqslant s$, then since $F_\sigma(x^{\boldsymbol{v}}) = F_\sigma^0(x^{\boldsymbol{v}_0})$, (20) implies (4), while (21) and (22) imply (5) with $\boldsymbol{\gamma} = [\boldsymbol{\gamma}_0, 0, \ldots, 0]$. If $KF_\sigma(x^{\boldsymbol{v}}) \neq LF_\sigma(x^{\boldsymbol{v}})$ for at least one $\sigma \leqslant s$, then $KF_\sigma(x^{\boldsymbol{v}})$ has an irreducible reciprocal factor. Hence

$$\big(KF_\sigma(x^{-\boldsymbol{v}}),\ KF_\sigma(x^{\boldsymbol{v}})\big) \neq 1$$

and by Theorem BZ there is a $\boldsymbol{\gamma} \in \mathbb{Z}^k$ such that

$$\boldsymbol{\gamma}\boldsymbol{n} = 0 \quad \text{and} \quad 0 < h(\boldsymbol{\gamma}) \leqslant c_1\big(JF_\sigma(z^{-1}),\ F_\sigma(z)\big),$$

which gives (5) by virtue of (22). □

Lemma 7. *Let $F \in \mathbb{Q}[\boldsymbol{x}]$ with $KF \notin \mathbb{Q}$. If $\boldsymbol{n} \in \mathbb{Z}^k$ and $KF(x^{\boldsymbol{n}}) \in \mathbb{Q}$, then there exists a vector $\boldsymbol{\gamma} \in \mathbb{Z}^k$ such that*

$$\boldsymbol{\gamma}\boldsymbol{n} = 0 \quad \textit{and} \quad 0 < h(\boldsymbol{\gamma}) \leqslant c_{10}(F). \tag{24}$$

Proof. See [7], Lemma 18. □

Lemma 8. *Let $G \in \overline{\mathbb{Q}}[\boldsymbol{x}] \setminus \{0\}$, $\boldsymbol{n} \in \mathbb{Z}^k \setminus \{\boldsymbol{0}\}$, $\boldsymbol{K}$ be the field generated over $\mathbb{Q}$ by the ratios of the coefficients of $G(x^{\boldsymbol{n}})$ and $\widehat{\boldsymbol{K}}$ be its normal closure. Assume that $G \in \boldsymbol{K}[\boldsymbol{x}]$, $G(x^{\boldsymbol{n}}) \neq 0$ and*

$$JG(x^{-\boldsymbol{n}})/JG^\tau(x^{\boldsymbol{n}}) \notin \widehat{\boldsymbol{K}} \text{ for all embeddings } \tau \text{ of } \boldsymbol{K} \text{ into } \widehat{\boldsymbol{K}}. \tag{25}$$

There exist a matrix $\boldsymbol{M} \in \mathfrak{M}_{k,k}(\mathbb{Z})$ and a vector $\boldsymbol{v} \in \mathbb{Z}^k$ such that

$$\det \boldsymbol{M} \neq 0, \quad h(\boldsymbol{M}) \leqslant c_{11}(G), \tag{26}$$

$$\boldsymbol{n} = \boldsymbol{v}\boldsymbol{M}, \tag{27}$$

and either

$$KG(x^{\boldsymbol{n}}) \text{ is irreducible over } \boldsymbol{K}, \tag{28}$$

or there exists a vector $\boldsymbol{\gamma} \in \mathbb{Z}^k$ *such that*

$$\boldsymbol{\gamma n} = 0 \quad \text{and} \quad 0 < h(\boldsymbol{\gamma}) \leqslant c_{12}(G), \tag{29}$$

or

$$JG(z^{\boldsymbol{M}}) = G_1 G_2, \quad G_i \in \widehat{\boldsymbol{K}}[z] \setminus \widehat{\boldsymbol{K}} \tag{30}$$

and if $\boldsymbol{K} = \mathbb{Q}$

$$KG_i(x^{\boldsymbol{v}}) \notin \mathbb{Q} \quad (i = 1, 2). \tag{31}$$

Proof. Let T be the set of all embeddings of $\boldsymbol{K}$ into $\widehat{\boldsymbol{K}}$. The assumption (25) implies

$$\frac{JG(\boldsymbol{x}^{-1})}{JG^{\tau}(\boldsymbol{x})} \notin \widehat{\boldsymbol{K}} \quad \text{for all } \tau \in T, \tag{32}$$

hence, in particular, $JG \notin \widehat{\boldsymbol{K}}$. If JG is reducible over $\widehat{\boldsymbol{K}}$ or $\boldsymbol{K} = \mathbb{Q}$ and KG is reducible we have (26), (27) and (30) with $\boldsymbol{M} = \boldsymbol{I}_k$, $\boldsymbol{v} = \boldsymbol{n}$ (provided $c_{11}(G) \geqslant 1$) and for $\boldsymbol{K} = \mathbb{Q}$ we may additionally assume that

$$KG_i \notin \mathbb{Q} \quad (i = 1, 2). \tag{33}$$

In this last case we have either (31) or, denoting by l_i the leading coefficient of G,

$$Kl_i^{-1} G_i(x^{\boldsymbol{n}}) \in \mathbb{Q} \quad \text{for an } i \leqslant 2.$$

However, $l_i^{-1} G_i$ belongs to a finite set S of monic non-constant divisors D of JG in $\mathbb{Q}[z]$ satisfying $KD \notin \mathbb{Q}$ by virtue of (33). Hence, by Lemma 7, (29) holds provided

$$c_{12}(G) \geqslant \max_{D \in S} c_{10}(D).$$

It remains to consider the case where JG is irreducible over $\widehat{\boldsymbol{K}}$, or $\boldsymbol{K} = \mathbb{Q}$ and KG is irreducible.

If JG is irreducible over $\widehat{\boldsymbol{K}}$, let l be the leading coefficient of $JG(x^{\boldsymbol{n}})$. Since $JG(x^{\boldsymbol{n}})$ has the same coefficients as $G(x^{\boldsymbol{n}})$, by the definition of $\boldsymbol{K}$, $\tau_1 \neq \tau_2$ implies for all $\tau_1, \tau_2 \in T$,

$$\left(l^{-1} JG(x^{\boldsymbol{n}})\right)^{\tau_1} \neq \left(l^{-1} JG(x^{\boldsymbol{n}})\right)^{\tau_2}$$

and since both sides are monic,

$$\frac{\left(l^{-1} JG(x^{\boldsymbol{n}})\right)^{\tau_2}}{\left(l^{-1} JG(x^{\boldsymbol{n}})\right)^{\tau_1}} \notin \widehat{\boldsymbol{K}}. \tag{34}$$

It follows that $JG^{\tau_2}/JG^{\tau_1} \notin \widehat{\boldsymbol{K}}$, and since JG^{τ_1}, JG^{τ_2} are both irreducible over $\widehat{\boldsymbol{K}}$, $(JG^{\tau_1}, JG^{\tau_2}) = 1$. If F is the polynomial over $\mathbb{Z}$ with the least positive leading coefficient divisible by JG and irreducible over $\mathbb{Q}$ we find that

$$JN_{\boldsymbol{K}/\mathbb{Q}} G = \prod_{\tau \in T} JG^{\tau} \mid F$$

and, since $JN_{\boldsymbol{K}/\mathbb{Q}}G \in \mathbb{Q}[\boldsymbol{x}] \setminus \mathbb{Q}$, we infer that

$$JN_{\boldsymbol{K}/\mathbb{Q}}G/F \in \mathbb{Q}^*. \tag{35}$$

Moreover, by (32),

$$\left(JF(\boldsymbol{x}^{-1}), F\right) = 1,$$

which implies $LF = F$ and, by (18), $KF = LF$.

If $\boldsymbol{K} = \mathbb{Q}$ and KG is irreducible we define F as the polynomial over $\mathbb{Z}$ which is a scalar multiple of G with the least positive leading coefficient. Thus we have (34) and infer, by (32) and (18), that $KF = LF$.

Hence in any case Theorem 1 applies to F. By virtue of that theorem and of (34) there exist a matrix $\boldsymbol{M} \in \mathfrak{M}_{k,k}(\mathbb{Z})$ and a vector $\boldsymbol{v} \in \mathbb{Z}^k$ such that (26), with $c_{11}(G) = 9k_0 \cdot 2^{||F||-5}$, and (27) hold and either

$$KN_{\boldsymbol{K}/\mathbb{Q}}G(\boldsymbol{z}^{\boldsymbol{M}}) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(\boldsymbol{z})^{e_\sigma} \tag{36}$$

implies

$$KN_{\boldsymbol{K}/\mathbb{Q}}G(x^{\boldsymbol{n}}) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(x^{\boldsymbol{v}})^{e_\sigma}, \tag{37}$$

or there exists a $\boldsymbol{\gamma}_1 \in \mathbb{Z}^k$ such that

$$\boldsymbol{\gamma}_1 \boldsymbol{n} = 0 \quad \text{and} \quad 0 < h(\boldsymbol{\gamma}_1) \leqslant c_3(F, \boldsymbol{M}) = c_{13}(G, \boldsymbol{M}).$$

In the latter case we have (29) provided

$$c_{12}(G) \geqslant \max c_{13}(G, \boldsymbol{M}),$$

where maximum is taken over all matrices $\boldsymbol{M} \in \mathfrak{M}_{k,k}(\mathbb{Z})$ satisfying (26). In the former case on the right hand side of (36) we have $\sum_{\sigma=1}^{s} e_\sigma \geqslant 1$. Indeed, if $\boldsymbol{K} \neq \mathbb{Q}$, then by Lemma 3,

$$LF(\boldsymbol{z}^{\boldsymbol{M}}) = JF(z^{\boldsymbol{M}}),$$

hence by (18),

$$KF(\boldsymbol{z}^{\boldsymbol{M}}) = JF(\boldsymbol{z}^{\boldsymbol{M}}) \notin \mathbb{Q}.$$

If $\boldsymbol{K} = \mathbb{Q}$ the same argument works with F replaced by KG.

If $\sum_{\sigma=1}^{s} e_\sigma = 1$, then by (37), $KN_{\boldsymbol{K}/\mathbb{Q}}G(x^{\boldsymbol{n}})$ is irreducible, hence we have (28). If $\sum_{\sigma=1}^{s} e_\sigma \geqslant 2$, then we have (30). Indeed, otherwise $JG(\boldsymbol{z}^{\boldsymbol{M}})$ would be irreducible over $\widehat{\boldsymbol{K}}$ and would satisfy

$$JG(\boldsymbol{z}^{\boldsymbol{M}}) \mid F_\sigma(\boldsymbol{z}) \tag{38}$$

for a $\sigma \leqslant s$. Since

$$JG(x^{\boldsymbol{n}}) = JG\big((x^{\boldsymbol{v}})^{\boldsymbol{M}}\big)$$

(34) implies that $JG(z^{\boldsymbol{M}})^{\tau_2}/JG(z^{\boldsymbol{M}})^{\tau_1} \notin \widehat{\boldsymbol{K}}$ for any two distinct elements τ_1, τ_2 of T. Since $JG(z^{\boldsymbol{M}})^{\tau_1}$, $JG(z^{\boldsymbol{M}})^{\tau_2}$ are both irreducible over $\widehat{\boldsymbol{K}}$,

$$\big(JG(z^{\boldsymbol{M}})^{\tau_1},\ JG(z^{\boldsymbol{M}})^{\tau_2}\big) = 1$$

and by (38),

$$JN_{\boldsymbol{K}/\mathbb{Q}}G(z^{\boldsymbol{M}}) = \prod_{\tau\in T} JG(z^{\boldsymbol{M}})^{\tau} \mid F_{\sigma}(z),$$

contrary to (36) under the assumption $\sum_{\sigma=1}^{s} e_{\sigma} \geqslant 2$. The contradiction obtained shows (30). If $K = \mathbb{Q}$ the same assumption together with (37) shows the existence of a factorization (30) satisfying (31). Indeed, according to the definition of canonical factorization, $F_{\sigma}(x^{\boldsymbol{v}}) \notin \mathbb{Q}$ for all $\sigma \leqslant s$. □

Proof of Theorem 2. The reducibility condition given in the theorem is clearly sufficient. We proceed to prove that it is necessary. Assume that the condition is necessary for $\mathbb{Q}[x_1, \ldots, x_{k-1}]$, $c_4(F)$ being defined for all polynomials in less than k variables for which it is needed (for $k = 1$ this is an empty statement); assume that $F \in \mathbb{Q}[\boldsymbol{x}]$, $JF(x^{\boldsymbol{n}})$ is not reciprocal and $KF(x^{\boldsymbol{n}})$ is reducible.

Consider first the case where F is of positive degree with respect to all k variables, so that k is determined by F. For $k = 1$ this is the only case.

If the matrix $\boldsymbol{M}$ and the vector $\boldsymbol{v}$ appearing in Lemma 8 for $G = F$ have the properties (30) and (31) we take $\boldsymbol{N} = \boldsymbol{M}$, $r = k$, $F_i = (KF, G_i)$ $(i = 1, 2)$ and obtain $h(\boldsymbol{N}) \leqslant c_{11}(F)$. Otherwise, by Lemma 8, there exists a vector $\boldsymbol{\gamma} \in \mathbb{Z}^k$ such that $\boldsymbol{\gamma n} = 0$ and $0 < h(\boldsymbol{\gamma}) \leqslant c_{12}(F)$. For $k = 1$ this completes the proof, since $\boldsymbol{\gamma n} = 0$ implies $\boldsymbol{n} = \boldsymbol{0}$.

For $k > 1$ the integer vectors perpendicular to $\boldsymbol{\gamma}$ form a lattice, say $\boldsymbol{\Lambda}$. It is easily seen (cf. for instance Lemma 6 in [2]) that $\boldsymbol{\Lambda}$ has a basis that written in the form of a matrix $\boldsymbol{B} \in \mathfrak{M}_{k-1,k}(\mathbb{Z})$ satisfies

$$h(\boldsymbol{B}) \leqslant \frac{k}{2}\, c_{12}(F). \tag{39}$$

Let us put

$$\widetilde{F} = JF(\widetilde{\boldsymbol{x}}^{\boldsymbol{B}}),\ \text{where } \widetilde{\boldsymbol{x}} = [x_1, \ldots, x_{k-1}]. \tag{40}$$

Since $\boldsymbol{n} \in \boldsymbol{\Lambda}$ we have $\boldsymbol{n} = \boldsymbol{mB}$ for an $\boldsymbol{m} \in \mathbb{Z}^{k-1}$. Clearly

$$JF(x^{\boldsymbol{n}}) = J\widetilde{F}(x^{\boldsymbol{m}}), \tag{41}$$

thus, by assumption, $J\widetilde{F}(x^{\boldsymbol{m}})$ is not reciprocal and $K\widetilde{F}(x^{\boldsymbol{m}})$ is reducible. By the inductive assumption there exist a matrix $\widetilde{\boldsymbol{N}} \in \mathfrak{M}_{r,k-1}(\mathbb{Z})$ of rank $r \leqslant k-1$ and a vector $\boldsymbol{v} \in \mathbb{Z}^r$

such that

$$h(\widetilde{\boldsymbol{N}}) \leqslant c_4(\widetilde{F}), \tag{42}$$

$$\boldsymbol{m} = \boldsymbol{v}\widetilde{\boldsymbol{N}}; \tag{43}$$

$$K\widetilde{F}(\boldsymbol{y}^{\widetilde{\boldsymbol{N}}}) = F_1F_2, \quad F_i \in \mathbb{Q}[\boldsymbol{y}],\ K F_i(x^{\boldsymbol{v}}) \notin \mathbb{Q} \quad (i = 1, 2).$$

Let us take $\boldsymbol{N} = \widetilde{\boldsymbol{N}}\boldsymbol{B}$. It follows from (40) that $J\widetilde{F}(\boldsymbol{y}^{\widetilde{\boldsymbol{N}}}) = JF(\boldsymbol{y}^{\boldsymbol{N}})$ and from (43) that $\boldsymbol{n} = \boldsymbol{v}\boldsymbol{N}$; moreover, since $\operatorname{rank}\boldsymbol{B} = k-1$, $\operatorname{rank}\boldsymbol{N} = r$. Thus $\boldsymbol{N}$ and $\boldsymbol{v}$ have all the properties required in the theorem apart from (6); it remains to establish (6) by an appropriate choice of $c_4(F)$. We have, by (39) and (42),

$$h(\boldsymbol{N}) \leqslant (k-1)h(\widetilde{\boldsymbol{N}})h(\boldsymbol{B}) \leqslant \binom{k}{2} c_4(\widetilde{F})c_{12}(F).$$

However, $\widetilde{F}$ is determined by F and $\boldsymbol{B}$ via (40) and, by virtue of (39), $\boldsymbol{B}$ runs through a finite set of matrices depending only on F. Hence $c_4(\widetilde{F}) \leqslant c_{14}(F)$ and the theorem holds with

$$c_4(F) = \max\left\{c_{11}(F), \binom{k}{2} c_{12}(F)c_{14}(F)\right\}.$$

Consider now the case where F is of positive degree with respect to less than k variables. We may assume that $F \in \mathbb{Q}[\widetilde{\boldsymbol{x}}]$. By the inductive assumption there exist a matrix $\boldsymbol{N}_0 \in \mathfrak{M}_{k-1,r_0}(\mathbb{Z})$ of rank r_0 and a vector $\boldsymbol{v}_0 \in \mathbb{Z}^{r_0}$ such that

$$h(\boldsymbol{N}_0) \leqslant c_4(F), \quad [n_1, \ldots, n_k] = \boldsymbol{v}_0\boldsymbol{N}_0,$$

$$KF(\boldsymbol{y}_0^{\boldsymbol{N}_0}) = F_1F_2, \quad \boldsymbol{y}_0 = [y_1, \ldots, y_{r_0}],$$

$$F_i \in \mathbb{Q}[\boldsymbol{y}_0], \quad KF_i(x^{\boldsymbol{v}_0}) \notin \mathbb{Q} \quad (i = 1, 2).$$

We put $r = r_0 + 1$, $\boldsymbol{N} = \begin{pmatrix} \boldsymbol{N}_0 & 0 \\ 0 & 1 \end{pmatrix}$, $\boldsymbol{v} = [\boldsymbol{v}_0, n_k]$ and easily verify that conditions (6)–(9) are satisfied. □

Proof of Theorem 3. We proceed in the same way as in the proof of the necessity part of Theorem 2, with $\boldsymbol{K}$ instead of $\mathbb{Q}$, using Lemma 8 without the formula (31). Therefore we point out only the argument not needed in the proof of Theorem 2. Before applying the inductive assumption to $\widetilde{F}(x^{\boldsymbol{m}})$ we have to check that $\widetilde{F} \in \boldsymbol{K}[\widetilde{\boldsymbol{x}}]$ and that

$$\frac{J\widetilde{F}(\widetilde{\boldsymbol{x}}^{-\boldsymbol{m}})}{J\widetilde{F}^{\tau}(\widetilde{\boldsymbol{x}}^{\boldsymbol{m}})} \notin \widehat{\boldsymbol{K}} \tag{44}$$

for all embeddings τ of $\boldsymbol{K}$ into $\widehat{\boldsymbol{K}}$.

Now $\widetilde{F} \in \boldsymbol{K}[\widetilde{\boldsymbol{x}}]$ follows from $F \in \boldsymbol{K}[x]$ and from the definition of $\widetilde{F}$ by the formula (40), while (44) follows from (10) and (41). □

Lemma 9. *If $a_j \neq 0$ $(0 \leqslant j \leqslant k)$ are complex numbers and the rank of a matrix $(v_{ij}) \in \mathfrak{M}_{r,k}(\mathbb{Z})$ is greater than $(k+1)/2$, then*

$$J\Big(a_0 + \sum_{j=1}^{k} a_j \prod_{i=1}^{r} x_i^{v_{ij}}\Big)$$

is absolutely irreducible.

Proof. See [3], Corollary to Theorem 1. The proof of Theorem 1 given there shows less than stated in the theorem, but only in the case of positive characteristic of the ground field, so the Corollary is fully justified. □

Proof of Corollary 1. We apply Theorem 3 with $F = a_0 + \sum_{j=1}^{k} a_j x_j$ and infer that if $K\big(a_0 + \sum_{j=1}^{k} a_j x^{n_j}\big)$ is irreducible over $\boldsymbol{K}$, then either

$$\frac{J\big(a_0 + \sum_{j=1}^{k} a_j x^{-n_j}\big)}{a_0^{\tau} + \sum_{j=1}^{k} a_j^{\tau} x^{n_j}} \in \widehat{\boldsymbol{K}} \tag{45}$$

for an embedding τ of $\boldsymbol{K}$ into $\widehat{\boldsymbol{K}}$, or there exist a matrix $\boldsymbol{N} = (v_{ij}) \in \mathfrak{M}_{r,k}(\mathbb{Z})$ of rank r and a vector $\boldsymbol{v} \in \mathbb{Z}^r$ such that $h(\boldsymbol{N}) \leqslant c_4(F)$, $\boldsymbol{n} = \boldsymbol{v}\boldsymbol{N}$ and

$$J\Big(a_0 + \sum_{j=1}^{k} a_j \prod_{i=1}^{r} y_i^{v_{ij}}\Big) \quad \text{is reducible over } \widehat{\boldsymbol{K}}. \tag{46}$$

Let us put $c_6(\boldsymbol{a}) = \max\{2, c_4(F)\}$.

If (45) holds, then $n_j + n_{k-j} = n_k$ $(1 \leqslant j < k)$ and we satisfy (13) and (14) by taking

$$\boldsymbol{v}_0 = \begin{cases} [n_1, \ldots, n_{k/2}] & \text{if } k \text{ is even,} \\ [n_1, \ldots, n_{(k-1)/2}, n_k] & \text{if } k \text{ is odd;} \end{cases}$$

$$\boldsymbol{N}_0 = \begin{pmatrix} 1 & & & & & & & -1 \\ & 1 & & & & & \iddots & \\ & & \ddots & & & -1 & & \\ & & & 1 & -1 & & & \\ & & & & 1 & 2 & 2 \ \ldots \ 2 & 2 \end{pmatrix} \qquad \text{if } k \text{ is even,}$$

$$\boldsymbol{N}_0 = \begin{pmatrix} 1 & & & & & & -1 & \\ & 1 & & & & \iddots & & \\ & & \ddots & & -1 & & & \\ & & & 1 & 1 & & & \\ & & & & 1 & 1 & \ldots \ 1 & 1 \end{pmatrix} \qquad \text{if } k \text{ is odd,}$$

where the empty places (but not the dots) denote zeros.

If (46) holds, then by Lemma 9 $r \leqslant (k+1)/2$. If $r = [(k+1)/2]$ we take $\boldsymbol{N}_0 = \boldsymbol{N}$, $\boldsymbol{v}_0 = \boldsymbol{v}$; if $r < (k+1)/2$ we amplify $\boldsymbol{N}$ and $\boldsymbol{v}$ by inserting zeros. □

Proof of Corollary 2. For each matrix $\boldsymbol{N}_0 \in \mathfrak{M}_{[(k+1)/2],k}(\mathbb{Z})$ the number of vectors $\boldsymbol{n} \in \mathbb{Z}^k$ with $h(\boldsymbol{n}) \leqslant N$ for which there exists a $\boldsymbol{v}_0 \in \mathbb{Z}^{[(k+1)/2]}$ satisfying (14) is less than $c_{15}(\boldsymbol{N}_0)N^{[(k+1)/2]}$. Hence Corollary 2 follows from Corollary 1 with

$$c_7(\boldsymbol{a}) = \sum c_{15}(\boldsymbol{N}_0),$$

where the sum is taken over all matrices $\boldsymbol{N}_0 \in \mathfrak{M}_{[(k+1)/2],k}$ satisfying (13). □

Remark 1. If $k > 1$ and $\sum_{j=0}^{k} a_j = 0$, then the polynomial $a_0 + \sum_{j=1}^{k} a_j x^{n_j}$ is reducible for all vectors $\boldsymbol{n}$ in question. This shows that replacing $a_0 + \sum_{j=1}^{k} a_j x^{n_j}$ by $K\big(a_0 + \sum_{j=1}^{k} a_j x^{n_j}\big)$ is really needed in order to obtain a non-trivial result.

Example. Here is the example announced in the introduction showing that the exponent $[(k+1)/2]$ is best possible in Corollary 2, and hence also in Corollary 1.

If $k = 2l-1$ we take $a_0 = 4, a_j = 2\ (1 \leqslant j \leqslant l), a_j = 1\ (l < j < 2l), n_j = n_l + n_{j-l}$ $(l < j < 2l)$. It follows that

$$a_0 + \sum_{j=1}^{k} a_j x^{n_j} = \Big(2 + \sum_{j=1}^{l-1} x^{n_j}\Big)(2 + x^{n_l}).$$

The two factors on the right hand side are not reciprocal, hence $K\big(a_0 + \sum_{j=1}^{k} a_j x^{n_j}\big)$ is reducible. The number X of relevant vectors $\boldsymbol{n}$ with $n_k \leqslant N$ is at least equal to the number of increasing sequences $n_1 < n_2 < \ldots < n_l$ with $n_l \leqslant [N/2]$, hence

$$X \geqslant \binom{[N/2]}{l} \geqslant c_{16}(l)N^l \quad \text{for } N \geqslant 2l,$$

where $c_{16}(l) > 0$.

If $k = 2l$ we take $a_0 = 4$, $a_j = 2\ (1 \leqslant j \leqslant l)$, $a_{l+1} = 3$, $a_j = 1\ (l+1 < j \leqslant 2l)$, $n_j = n_l + n_{j-l}\ (l < j < 2l)$, $n_{2l} = 2n_l + n_1$. It follows that

$$a_0 + \sum_{j=1}^{k} a_j x^{n_j} = \Big(2 + \sum_{j=1}^{l-1} x^{n_j} + x^{n_l+n_1}\Big)(2 + x^{n_l}).$$

The two factors on the right hand side are not reciprocal, hence $K\big(a_0 + \sum_{j=1}^{k} a_j x^{n_j}\big)$ is reducible. The number X of relevant vectors $\boldsymbol{n}$ with $n_k \leqslant N$ is at least equal to the number of increasing sequences $n_1 < n_2 < \ldots < n_l$ with $n_l \leqslant [N/3]$, hence

$$X \geqslant \binom{[N/3]}{l} \geqslant c_{17}(l)N^l \quad \text{for } N \geqslant 3l,$$

where $c_{17}(l) > 0$.

Lemma 10. *For every $k+1$ non-zero complex numbers $a_0, \dots, a_k$ such that $a_0 \in \boldsymbol{K} = \mathbb{Q}(a_1/a_0, \dots, a_k/a_0)$ there exist $k+1$ algebraic numbers $\alpha_0, \dots, \alpha_{k-1}, \alpha_k = 1$ such that if $0 = n_0 < n_1 < \dots < n_k$ and $K\big(\sum_{j=0}^{l} a_j x^{n_j}\big)$ is reducible over $\boldsymbol{K}$ then either $K\big(\sum_{j=0}^{l} \alpha_j x^{n_j}\big)$ is reducible over $\boldsymbol{K}_0 = \mathbb{Q}(\alpha_0, \dots, \alpha_{k-1})$, or there is a vector $\boldsymbol{\gamma} \in \mathbb{Z}^k$ such that $\boldsymbol{\gamma n} = 0$ and*

$$0 < h(\boldsymbol{\gamma}) \leqslant c_{18}(\boldsymbol{a}). \tag{47}$$

Proof. See [6], Lemma 5. □

Proof of Corollary 3. Let α_i have the meaning of Lemma 10. By Corollary 2 the number of relevant vectors $\boldsymbol{n}$ for which $n_k \leqslant N$ and $K\big(\sum_{j=0}^{k} \alpha_j x^{n_j}\big)$ is reducible over $\mathbb{Q}(\alpha_0, \dots, \alpha_{k-1})$ is less than $c_7(\boldsymbol{\alpha}) N^{[(k+1)/2]}$. For a fixed $\boldsymbol{\alpha} \in \mathbb{Z}^k \setminus \{\boldsymbol{0}\}$ the number of relevant vectors $\boldsymbol{n} \in \mathbb{Z}^k$ with $n_k \leqslant N$ such that $\boldsymbol{\gamma n} = 0$ is less than $c_{19}(\boldsymbol{\gamma}) N^{k-1}$. Hence Corollary 3 holds with

$$c_8(\boldsymbol{a}) = c_7(\boldsymbol{\alpha}) + \sum c_{19}(\boldsymbol{\gamma}),$$

where the sum is taken over all vectors $\boldsymbol{\gamma} \in \mathbb{Z}^k$ satisfying (47). □

Remark 2. It seems likely that by improving Lemma 10 one can replace the exponent $k-1$ in Corollary 3 by $[(k+1)/2]$.

Proof of Theorem 4. We begin by defining subsets S_i and R_i of $\mathfrak{M}_{k-i,k}(\mathbb{Z})$ $(0 \leqslant i < k)$ inductively, as follows:

$$S_0 = \{\boldsymbol{I}_k\}, \tag{48}$$

and supposing that S_i is already defined, $\boldsymbol{y} = [y_1, \dots, y_{k-1}]$,

$$R_i = \big\{\boldsymbol{MN} : \boldsymbol{N} \in S_i,\ \boldsymbol{M} \in \mathfrak{M}_{k-i,k-i}(\mathbb{Z}),\ \det \boldsymbol{M} \neq 0,\ h(\boldsymbol{M}) \leqslant c_{11}\big(F(\boldsymbol{y}^{\boldsymbol{N}})\big),\ KF(\boldsymbol{y}^{\boldsymbol{MN}}) \text{ is reducible}\big\}, \tag{49}$$

and for $i < k-1$

$$S_{i+1} = \Big\{\boldsymbol{N} \in \mathfrak{M}_{k-i-1,k}(\mathbb{Z}) : \operatorname{rank} \boldsymbol{N} = k-i-1,\ h(\boldsymbol{N}) \leqslant \tfrac{1}{2}(k-i)^2 \max_{\boldsymbol{N}_1 \in S_i} \big\{h(\boldsymbol{N}_1) \max\{\max c_{12}\big(F(\boldsymbol{y}^{\boldsymbol{N}_1})\big), \max{}^*(k-1)c_{10}(D)h(\boldsymbol{M})\}\big\}\Big\} \tag{50}$$

where $\max^*$ is taken over all $\boldsymbol{M} \in \mathfrak{M}_{k-i,k-i}(\mathbb{Z})$ with $\det \boldsymbol{M} \neq 0$, $h(\boldsymbol{M}) \leqslant c_{11}\big(F(\boldsymbol{y}^{\boldsymbol{N}_1})\big)$ and all monic irreducible divisors D of $KF(\boldsymbol{y}^{\boldsymbol{MN}_1})$. (If $KF(\boldsymbol{y}^{\boldsymbol{MN}_1})$ belongs to $\mathbb{Q}$ we take $\max^* = 0$.)

In this way R_i and S_i are defined for all $i < k$ and we put

$$R = \bigcup_{i=0}^{k-1} R_i, \quad S = \bigcup_{i=1}^{k-1} S_i.$$

We first prove that the condition given in the theorem is necessary. By (48) there exist indices i such that

$$\boldsymbol{n} = \boldsymbol{u}\boldsymbol{U}, \quad \boldsymbol{U} \in S_{k-i}, \quad \boldsymbol{u} \in \mathbb{Z}^i.$$

Let r be the least such index and

$$\boldsymbol{n} = \boldsymbol{v}\boldsymbol{N}, \quad \boldsymbol{N} \in S_{k-r}, \quad \boldsymbol{v} \in \mathbb{Z}^r. \tag{51}$$

By Lemma 8 if $KF(x^{\boldsymbol{n}}) = KF(x^{\boldsymbol{vN}})$ is reducible, then there exists a matrix $\boldsymbol{M} \in \mathfrak{M}_{r,r}(\mathbb{Z})$ such that

$$\det \boldsymbol{M} \neq 0, \quad h(\boldsymbol{M}) \leqslant c_{11}\big(F(\boldsymbol{y}^{\boldsymbol{N}})\big), \quad \boldsymbol{y} = [y_1, \ldots, y_r], \tag{52}$$

$$\boldsymbol{v} = \boldsymbol{v}_1\boldsymbol{M}, \quad \boldsymbol{v}_1 \in \mathbb{Z}^r \tag{53}$$

and either $KF(\boldsymbol{y}^{\boldsymbol{MN}})$ is reducible, or there exists a vector $\boldsymbol{\gamma} \in \mathbb{Z}^r$ such that

$$\boldsymbol{\gamma}\boldsymbol{v} = 0 \quad \text{and} \quad 0 < h(\boldsymbol{\gamma}) \leqslant c_{12}\big(F(\boldsymbol{y}^{\boldsymbol{N}})\big).$$

The second possibility can only hold for $r > 1$ since for $r = 1$ it gives $\boldsymbol{v} = \boldsymbol{0}$ and by (51), $\boldsymbol{n} = \boldsymbol{0}$. For $r > 1$ the vectors $\boldsymbol{v}$ perpendicular to $\boldsymbol{\gamma}$ form a lattice $\boldsymbol{\Lambda}$ in $\mathbb{Z}^r$. This lattice has a basis that written in the form of a matrix $\boldsymbol{B} \in \mathfrak{M}_{r-1,r}(\mathbb{Z})$ satisfies

$$\operatorname{rank} \boldsymbol{B} = r - 1, \tag{54}$$

$$h(\boldsymbol{B}) \leqslant \frac{r}{2}\, h(\boldsymbol{\gamma}) \leqslant \frac{r}{2}\, c_{12}\big(F(\boldsymbol{y}^{\boldsymbol{N}})\big) \tag{55}$$

(cf. Lemma 6 in [2]). Since $\boldsymbol{v} \in \boldsymbol{\Lambda}$ we have

$$\boldsymbol{v} = \boldsymbol{w}\boldsymbol{B}, \quad \boldsymbol{w} \in \mathbb{Z}^{r-1},$$

hence, by (51),

$$\boldsymbol{n} = \boldsymbol{w}\boldsymbol{B}\boldsymbol{N}, \quad \boldsymbol{B}\boldsymbol{N} \in \mathfrak{M}_{r-1,k}(\mathbb{Z}). \tag{56}$$

Since, by (50) and (51), $\operatorname{rank} \boldsymbol{N} = r$, it follows from (54), by linear algebra, that

$$\operatorname{rank} \boldsymbol{B}\boldsymbol{N} = r - 1.$$

Moreover, by (55),

$$h(\boldsymbol{B}\boldsymbol{N}) \leqslant r h(\boldsymbol{B}) h(\boldsymbol{N}) \leqslant \frac{r^2}{2}\, h(\boldsymbol{N}) c_{12}\big(F(\boldsymbol{y}^{\boldsymbol{N}})\big)$$

and, by (50), $\boldsymbol{B}\boldsymbol{N} \in S_{k-r+1}$, contrary, in view of (56), to the definition of r. The contradiction obtained proves that $KF(\boldsymbol{y}^{\boldsymbol{MN}})$ is reducible, hence $\boldsymbol{M}\boldsymbol{N} \in R_{k-r}$ by (49). By (51) and (53) we have

$$\boldsymbol{n} = \boldsymbol{v}_1\boldsymbol{M}\boldsymbol{N},$$

while by the definition of r the equation $\boldsymbol{n} = \boldsymbol{u}\boldsymbol{U}$ is insoluble in $\boldsymbol{u} \in \mathbb{Z}^i$, $\boldsymbol{U} \in S_{k-i}$ for $i < r$. Thus the condition given in the theorem is necessary.

Now we prove that it is sufficient. Assume that for a certain matrix $\boldsymbol{N} \in R_{k-r}$ $(1 \leqslant r \leqslant k)$,

$$\boldsymbol{n} = \boldsymbol{v}\boldsymbol{N}, \quad \boldsymbol{v} \in \mathbb{Z}^r, \tag{57}$$

but

$$\boldsymbol{n} \neq \boldsymbol{u}\boldsymbol{U} \quad \text{for all } s < r, \quad \boldsymbol{u} \in \mathbb{Z}^s, \quad \boldsymbol{U} \in S_{k-s}. \tag{58}$$

Then by (49)

$$\boldsymbol{n} = \boldsymbol{v}\boldsymbol{M}\boldsymbol{N}_1, \quad \boldsymbol{N}_1 \in S_{k-r}, \quad \boldsymbol{M} \in \mathfrak{M}_{r,r}(\mathbb{Z}), \quad \det \boldsymbol{M} \neq 0,$$
$$h(\boldsymbol{M}) \leqslant c_{11}\big(F(\boldsymbol{y}^{\boldsymbol{N}_1})\big), \quad \boldsymbol{y} = [y_1, \ldots, y_r]$$

and

$$KF(\boldsymbol{y}^{\boldsymbol{M}\boldsymbol{N}_1}) = F_1 F_2, \quad F_1, F_2 \in \mathbb{Q}[\boldsymbol{y}] \setminus \mathbb{Q}.$$

Hence

$$KF(x^{\boldsymbol{n}}) = KF_1(x^{\boldsymbol{v}})KF_2(x^{\boldsymbol{v}}). \tag{59}$$

Suppose that for an $i \leqslant 2$ we have $KF_i(x^{\boldsymbol{v}}) \in \mathbb{Q}$. Then $KD(x^{\boldsymbol{v}}) \in \mathbb{Q}$ for an irreducible monic factor D of KF, hence by Lemma 7 there exists a vector $\boldsymbol{\gamma} \in \mathbb{Z}^r$ such that

$$\boldsymbol{\gamma}\boldsymbol{v} = 0, \quad 0 < h(\boldsymbol{\gamma}) \leqslant c_{10}(D).$$

Again this can occur only for $r > 1$ and, repeating the argument about the lattice given above, we find a matrix $\boldsymbol{B} \in \mathfrak{M}_{r-1,r}(\mathbb{Z})$ such that

$$\operatorname{rank} \boldsymbol{B} = r - 1, \quad h(\boldsymbol{B}) \leqslant \frac{r}{2}\, h(\boldsymbol{\gamma}) \leqslant \frac{r}{2}\, c_{10}(D);$$
$$\boldsymbol{v} = \boldsymbol{w}\boldsymbol{B}, \quad \boldsymbol{w} \in \mathbb{Z}^{r-1}.$$

It follows that

$$\boldsymbol{n} = \boldsymbol{w}\boldsymbol{B}\boldsymbol{M}\boldsymbol{N}_1, \quad \boldsymbol{B}\boldsymbol{M}\boldsymbol{N}_1 \in \mathfrak{M}_{r-1,k}(\mathbb{Z}), \tag{60}$$
$$\operatorname{rank} \boldsymbol{B}\boldsymbol{M}\boldsymbol{N}_1 = r - 1,$$
$$h(\boldsymbol{B}\boldsymbol{M}\boldsymbol{N}_1) \leqslant r^2 h(\boldsymbol{B})h(\boldsymbol{M})h(\boldsymbol{N}_1) \leqslant \frac{r^3}{2}\, c_{10}(D)h(\boldsymbol{M})h(\boldsymbol{N}_1),$$

hence by (50),

$$\boldsymbol{B}\boldsymbol{M}\boldsymbol{N}_1 \in S_{k-r+1},$$

which together with (59) contradicts (58). The contradiction obtained shows that $KF_i(x^{\boldsymbol{v}}) \notin \mathbb{Q}$ $(i = 1, 2)$, hence by (59), $KF(x^{\boldsymbol{n}})$ is reducible. □

References

[1] E. Bombieri, U. Zannier, *Intersections of varieties with* 1*-dimensional tori and a conjecture of Schinzel*. Preprint. See also: U. Zannier, *Proof of Conjecture* 1. Appendix in the book by A. Schinzel, *Polynomials with Special Regard to Reducibility*. Encyclopedia of Mathematics and its Applications 77, Cambridge Univ. Press, Cambridge 2000.

[2] A. Schinzel, *Reducibility of lacunary polynomials* I. Acta Arith. 16 (1969), 123–159; *Corrigenda*: Acta Arith. 19 (1971), 201; ibid. 24 (1978), 265; this collection: D4, 344–380.

[3] —, *A general irreducibility criterion*. J. Indian Math. Soc. (N.S.) 37 (1973), 1–8; this collection: E5, 739–746.

[4] —, *Reducibility of lacunary polynomials* III. Acta Arith. 34 (1978), 227–266; this collection: D7, 409–446.

[5] —, *Reducibility of lacunary polynomials* VII. Monatsh. Math. 102 (1986), 309–337; *Errata*, Acta Arith. 53 (1989), 95.

[6] —, *Reducibility of lacunary polynomials* VIII. Acta Arith. 50 (1988), 91–106.

[7] —, *Reducibility of lacunary polynomials* X. Acta Arith. 53 (1989), 47–97.

[8] —, *Reducibility of lacunary polynomials* XI. Acta Arith. 57 (1991), 165–175.

Andrzej Schinzel
Selecta

Originally published in
Publicationes Mathematicae Debrecen
56 (2000), 575–608

On reducible trinomials II

To Professor Kálmán Győry on his 60th birthday

Abstract. It is shown that if a trinomial has a binomial factor then under certain conditions the cofactor is irreducible.

1. Introduction

This paper is a sequel to [5]. In that paper we considered an arbitrary field K of characteristic π, the rational function field $K(\boldsymbol{y})$, where $\boldsymbol{y}$ is a variable vector, a finite algebraic extension L of $K(y_1)$ and a trinomial

$$\text{(i)} \qquad T(x; A, B) = x^n + Ax^m + B, \quad \text{where } n > m > 0,\ \pi \nmid mn(n-m)$$

and either $A, B \in K(\boldsymbol{y})^*$, $A^{-n}B^{n-m} \notin K$ or $A, B \in L$, $A^{-n}B^{n-m} \notin \overline{K}$.

A necessary and sufficient condition was given for reducibility of $T(x; A, B)$ over $K(\boldsymbol{y})$ or L respectively, provided in the latter case that L is separable. (This proviso was only made in the errata [6] ([1]).) As a consequence a criterion was derived for reducibility of $T(x; a, b)$ over an algebraic number field containing a, b. In each case it was assumed that $n \geqslant 2m$, but this involved no loss of generality, since $x^n + Ax^m + B$ and $x^n + AB^{-1}x^{n-m} + B^{-1}$ are reducible simultaneously. Let

$$\text{(ii)} \qquad n_1 = n/(n, m),\ m_1 = m/(n, m).$$

One case of reducibility of $T(x; A, B)$ over the field $\Omega = K(\boldsymbol{y})$ or L is that $x^{n_1} + Ax^{m_1} + B$ has in $\Omega[x]$ a linear factor. The aim of this paper is to prove that if n_1 is sufficiently large and $x^{n_1} + Ax^{m_1} + B$ has in $\Omega[x]$ a linear factor $F(x)$, but not a quadratic factor, then $T(x; A, B)F(x^{(m,n)})^{-1}$ is irreducible over Ω. More precisely, we shall prove using the notation introduced in (i) and (ii) the following three theorems.

Theorem 1. *Let $n_1 > 5$ and $A, B \in K(\boldsymbol{y})^*$, $A^{-n}B^{n-m} \notin K$. If $x^{n_1} + Ax^{m_1} + B$ has in $K(\boldsymbol{y})[x]$ a linear factor, $F(x)$, but not a quadratic factor, then $T(x; A, B)F(x^{(m,n)})^{-1}$ is irreducible over $K(\boldsymbol{y})$.*

Theorem 2. *Let $n_1 > 3$ and $A, B \in L^*$, where L is a finite separable extension of $K(y_1)$ with $\overline{K}L$ of genus g and $A^{-n}B^{n-m} \notin \overline{K}$. If $x^{n_1} + Ax^{m_1} + B$ has in $L[x]$ a linear factor*

([1]) In this volume it is added to Theorem 2 and Lemma 27.

$F(x)$, but not a quadratic factor, then

(iii) $$T(x; A, B)F(x^{(m,n)})^{-1} \text{ is reducible over } L$$

if and only if there exists an integer l such that

$$\left\langle \frac{n}{l}, \frac{m}{l} \right\rangle =: \langle \nu, \mu \rangle \in \mathbb{N}^2 : \nu < \max\{17, 8g\}$$

and $\dfrac{x^\nu + Ax^\mu + B}{F(x^{(\mu,\nu)})}$ *is reducible over L. Moreover, if $g = 1$, then* (iii) *implies $n_1 \leqslant 6$.*

Theorem 3. *Let $n_1 > 6$, K be an algebraic number field and $a, b \in K^*$. If the trinomial $x^{n_1} + ax^{m_1} + b$ has in $K[x]$ a monic linear factor $F(x)$, but not a quadratic factor, then $T(x; a, b)F(x^{(m,n)})^{-1}$ is reducible over K if and only if there exists an integer l such that* c $\langle n/l, m/l \rangle =: \langle \nu, \mu \rangle \in \mathbb{N}^2$ *and $a = u^{\nu-\mu}a_0$, $b = u^\nu b_0$, $F = u^{(\mu,\nu)}F_0\left(x/u^{(\mu,\nu)}\right)$, where $u \in K^*$, $\langle a_0, b_0, F_0 \rangle \in F^1_{\nu,\mu}(K)$ and $F^1_{\nu,\mu}(K)$ is a certain finite set, possibly empty.*

There is no principal difficulty in determining in Theorems 1, 2 for $g = 1$, and 3 all cases of reducibility when $n_1 \leqslant 6$ in much the same way as it was done in [5] for $T(x; A, B)$ or $T(x; a, b)$, however this seems of secondary interest. On the other hand, it is natural to ask what happens when $x^{n_1} + Ax^{m_1} + B$ has a quadratic factor. We intend to return to this question in the next paper of this series.

In analogy with a conjecture proposed in [5] we formulate

c **Conjecture.** For every algebraic number field K one can choose sets $F^1_{\nu,\mu}(K)$ such that the set

$$\sum{}^1 = \bigcup_{\nu,\mu,F} \bigcup_{\langle a,b,F\rangle \in F^1_{\nu,\mu}} \{x^\nu + ax^\mu + b\} \text{ is finite.}$$

2. 16 lemmas to Theorems 1–2

Lemma 1. *If in a transitive permutation group G the length of a cycle $C \in G$ is at least equal to the length of a block of imprimitivity, then it is divisible by the latter.*

Proof. Let $C = (a_1, \dots, a_\nu)$, $a_{\nu+i} := a_i$ $(i = 1, 2, \dots)$ and let $B_1, B_2, \dots$ be conjugate blocks of imprimitivity. Let μ be the least positive integer such that for some i, a_i and $a_{i+\mu}$ belong to the same block B. If $\mu = 1$, then by induction $a_i \in B$ for all i, hence $\nu \leqslant |B|$ and, since $\nu \geqslant |B|$ by the assumption, we have $\nu = |B|$.

If $\mu > 1$ we may assume, changing if necessary the numeration of the a_i and of the blocks, that

$$a_i \in B_i \ (1 \leqslant i \leqslant \mu), \quad a_{\mu+1} \in B_1.$$

It follows by induction on i that

(1) $$a_{k\mu+i} \in B_i \quad (1 \leqslant i \leqslant \mu,\ k = 0, 1, \dots),$$

hence, in particular, $i \equiv j \bmod \nu$ implies $i \equiv j \bmod \mu$, thus $\mu \mid \nu$.

If $a \in B_1$ then $C(a) \in B_2$, hence $C(a) \neq a$ and there exists a_j such that $a = a_j$. By (1) we have

$$j \equiv 1 \bmod \mu.$$

Thus among a_j $(1 \leqslant j \leqslant \nu,\ j \equiv 1 \bmod \mu)$ occur all elements of B_1 and only such elements. However a_j in question are distinct, hence

$$\frac{\nu}{\mu} = |B_1| \quad \text{and} \quad |B_1| \,\Big|\, \nu. \qquad \square$$

Lemma 2. *If $(m, n) = 1$ the polynomial $R_1(x, t) = (x^n + tx^m - (1 + t))/(x - 1)$ is absolutely irreducible. The algebraic function $x(t)$ defined by the equation $R_1(x, t) = 0$ has just $n - 2$ branch points $t_i \neq -1, \infty$ with one 2-cycle given by the Puiseux expansions*

$$x(t) = \xi_i \pm (t - t_i)^{1/2} P_{i1}\big(\pm(t - t_i)^{1/2}\big), \quad \xi_i \neq 0 \quad (1 \leqslant i \leqslant n - 2)$$

and the remaining expansions

$$x(t) = P_{ij}(t - t_i) \quad (2 \leqslant j \leqslant n - 2).$$

At the branch point -1, $x(t)$ has one m-cycle given by the Puiseux expansions

$$x(t) = \zeta_{2m}^{2i+1}(t + 1)^{1/m} P_{n-1,1}\big(\zeta_{2m}^{2i+1}(t + 1)^{1/m}\big) \quad (0 \leqslant i \leqslant m)$$

and the remaining expansions at this point are

$$x(t) = P_{n-1,j}(t + 1) \quad (2 \leqslant j \leqslant n - m).$$

At the branch point ∞, $x(t)$ has one $(n - m)$-cycle given by the Puiseux expansions

$$x(t) = \zeta_{2(n-m)}^{2i+1} t^{1/(n-m)} P_{n1}\big(\zeta_{2(n-m)}^{2i+1} t^{1/(n-m)}\big),$$

and the remaining expansions at this point are

$$x(t) = P_{nj}(t^{-1}) \quad (2 \leqslant j \leqslant m).$$

Here P_{ij} are ordinary formal power series with $P_{ij}(0) \neq 0$ and ζ_q is a primitive root of unity of order q. For a fixed i the values ξ_i (if $i \leqslant n - 2$) and $P_{ij}(0)$ $(j > 1)$ are distinct.

Proof. The polynomial $R_1(x, t)$ is absolutely irreducible since it can be written as

$$\frac{x^n - 1}{x - 1} + t\,\frac{x^m - 1}{x - 1}$$

and, since $(m, n) = 1$, we have $\big((x^n - 1)/(x - 1), (x^m - 1)/(x - 1)\big) = 1$.

If τ is a finite branch point of the algebraic function $x(t)$ we have for some ξ

$$R_1(\xi, \tau) = R'_{1x}(\xi, \tau) = 0, \tag{2}$$

hence also $T(\xi; \tau, -\tau - 1) = T'_x(\xi; \tau, -\tau - 1) = 0$, which gives either $\xi = 0$, $\tau = -1$ or

$$\tau \neq 0, \quad \xi^{n-m} = -\frac{m}{n}\,\tau, \quad \xi^m = \frac{n}{n - m}\,\frac{\tau + 1}{\tau}.$$

If $\tau = -n/m$, then $\xi^{n-m} = 1$, $\xi^m = 1$ and, since $(m, n) = 1$, $\xi = 1$. However $R'_{1x}(1, -n/m) = n(n-1)/2 - (n/m) \cdot m(m-1)/2 = n(n-m)/2 \neq 0$ thus for $\tau \neq -1$ (2) implies $(-(m/n)\tau)^m = \big((n/(n-m))(\tau+1)/\tau\big)^{n-m}$, $\tau \neq -n/m$, which gives

$$(-m)^m (n-m)^{n-m} \tau^n - n^n (\tau+1)^{n-m} = 0.$$

The only multiple root of this equation is $\tau = -n/m$ and it has multiplicity 2. Denoting the remaining roots by t_i $(1 \leqslant i \leqslant n-2)$ we find $t_i \neq 0, -1$,

$$\left(-\frac{m}{n}\, t_i\right)^m = \left(\frac{n}{n-m}\, \frac{t_i+1}{t_i}\right)^{n-m},$$

hence for a uniquely determined $\xi_i \neq 0, 1$

$$\xi_i^{n-m} = -\frac{m}{n}\, t_i, \quad \xi_i^m = \frac{n}{n-m}\, \frac{t_i+1}{t_i}$$

and $R_1(\xi_i, t_i) = R'_{1x}(\xi_i, t_i) = 0$.

Further,

$$R''_{1x}(\xi_i, t_i) = \frac{n(n-1)\xi_i^{n-1} - n(n-1)\xi_i^{n-2} + m(m-1)t_i\xi_i^{m-1} - m(m-1)t_i\xi_i^{m-2}}{(\xi_i - 1)^2}$$
$$= \frac{n(n-1)\xi_i^{n-2} + m(m-1)t_i\xi_i^{m-2}}{\xi_i - 1} = \xi_i^{m-2}\, \frac{m(m-n)t_i}{\xi_i - 1} \neq 0$$

and

$$R'_{1t}(\xi_i, t_i) = \frac{\xi_i^m - 1}{\xi_i - 1} = \frac{mt_i + n}{(\xi_i - 1)(n-m)} \neq 0.$$

c It follows that the Taylor expansion of $R_1(x, t)$ at $\langle \xi_i, t_i \rangle$ has the lowest terms

$$\frac{1}{2}\, R''_{1x}(\xi_i, t_i)(x - \xi_i)^2 \quad \text{and} \quad R'_{1t}(\xi_i, t_i)(t - t_i),$$

which implies the existence at the point t_i of the two-cycle with the expansions given in the lemma. The remaining expansions are obtained using the fact that $R_1(x, t_i)$ has $n-3$ distinct zeros, different from 0 and ξ_i. These zeros are $P_{ij}(0)$ $(2 \leqslant j \leqslant n-2)$. The assertions concerning branch points -1 and ∞ are proved in a standard way. □

Lemma 3. *If $(m, n) = 1$, the discriminant $D_1(t)$ of $R_1(x, t)$ with respect to x equals*

$$c(t+1)^{m-1} \prod_{i=1}^{n-2} (t - t_i), \quad c \in K^*.$$

c

Proof. Since R_1 is monic with respect to x we have

$$D_1(t) = \prod_{i<j} (x_i - x_j)^2,$$

where $R_1(x, t) = \prod_{j=1}^{n-1} (x - x_j)$. Using Lemma 2 we find that the only possible zeros of

$D_1(t)$ are t_i $(1 \leqslant i \leqslant n-2)$ and -1. Taking for x_j the Puiseux expansion of $x(t)$ at these points we find the exponents with which $t - t_i$ and $t + 1$ divide $D_1(t)$. □

Lemma 4. *If $(m, n) = 1$ the Galois group of the polynomial $R_1(x, t)$ over $\overline{K}(t)$ is the symmetric group S_{n-1}.*

Proof. Since, by Lemma 2, $R_1(x, t)$ is absolutely irreducible, the group G in question is transitive. By Lemma 1(c) of [5] and Lemma 2 G contains a transposition (for $n > 2$), an m-cycle and an $(n-m)$-cycle, where we may assume $m \leqslant n - m$. If G were imprimitive with blocks of imprimitivity of length b, $1 < b < n - 1$ we should have $2b \leqslant n - 1$, $b \leqslant n - m$ and by Lemma 1, $b \mid m$ and $b \mid (n, m)$, $b = 1$, a contradiction. Thus G is primitive and since it contains a transposition it must be symmetric by Theorem 14 in Chapter 1 of [7]. □

Definition 1. Let $(m, n) = 1$, $R_1(x, t) = \prod_{i=1}^{n-1} \big(x - x_i(t)\big)$. We set

$$L_1(k, m, n) = K\big(t, \tau_1(x_1, \ldots, x_k), \ldots, \tau_k(x_1, \ldots, x_k)\big)$$
$$L_1^*(k, m, n) = \overline{K}\big(t, \tau_1(x_1, \ldots, x_k), \ldots, \tau_k(x_1, \ldots, x_k)\big),$$

where τ_j is the j-th fundamental symmetric function.

Remark. By Lemma 4 the fields $L_1(k, m, n)$ and $L_1^*(k, m, n)$ are determined by k, m, n up to an isomorphism fixing $K(t)$ and $\overline{K}(t)$, respectively.

Lemma 5. *The numerator of $t - t_i$ in $L_1^*(k, m, n)$ has $\binom{n-3}{k-1}$ prime divisors in the second power and none in the higher ones.*

Proof. The proof is analogous to the proof of Lemma 5 in [5]. □

Lemma 6. *The numerator of $t + 1$ in $L_1^*(k, m, n)$ has*

$$\frac{1}{m} \sum_{l=0}^{k} \binom{n-m-1}{k-l} \sum_{d \mid (m,l)} \varphi(d) \binom{m/d}{l/d}$$

distinct prime divisors.

Proof. By Lemma 1(a) of [5] the prime divisors of the numerator of $t + 1$ are in one-to-one correspondence with the cycles of the Puiseux expansions of a generating element of $L_1^*(k, m, n)$ at $t = -1$ provided the lengths of these cycles are not divisible by π. For the generating element we take $y(t) = \sum_{j=1}^{k} a^j \tau_j(x_1, \ldots, x_k)$, where $a \in \overline{K}$ if K is finite and $a \in K$ otherwise, is chosen so that $\sum_{j=1}^{k} a^j \tau_j(x_{i_1}, \ldots, x_{i_k}) = \sum_{j=1}^{k} a^j \tau_j(x_1, \ldots, x_k)$ implies

$\{i_1, \dots, i_k\} = \{1, \dots, k\}$. By Lemma 4 for each set $\{i_1, \dots, i_k\} \subset \{1, \dots, n-1\}$ there is an automorphism of the extension

$$\overline{K}(t, x_1(t), \dots, x_{n-1}(t))/\overline{K}(t)$$

taking $x_1(t), \dots, x_k(t)$ into $x_{i_1}(t), \dots, x_{i_k}(t)$, respectively. Thus at $t = -1$ we obtain the following Puiseux expansions for $y(t)$

$$Q(t, l, i_1, \dots, i_k) = \sum_{j=1}^{k} a^j \tau_j \Big(\zeta_{2m}^{2i_1+1} (t+1)^{1/m} P_{n-1,1}\big(\zeta_{2m}^{2i_1+1}(t+1)^{1/m}\big), \dots, \zeta_{2m}^{2i_l+1}(t+1)^{1/m} P_{n-1,1}\big(\zeta_{2m}^{2i_l+1}(t+1)^{1/m}\big), P_{n-1,i_{l+1}}(t+1), \dots, P_{n-1,i_k}(t+1) \Big)$$

where l runs from 0 to k, $\{i_1, \dots, i_l\}$ runs through all subsets of $\{0, 1, \dots, m-1\}$ of cardinality l and $\{i_{l+1}, \dots, i_k\}$ runs through all subsets of $\{2, 3, \dots, n-m\}$ of cardinality $k - l$.

To see this note that the fundamental symmetric functions of $Q(t, l, i_1, \dots, i_k)$ coincide with the fundamental symmetric functions of the conjugates of $y(t)$ over $\overline{K}(t)$.

If P is an ordinary formal power series, the conjugates of $P\big((t+1)^{1/m}\big)$ over $\overline{K}\big(((t+1)^{1/d})\big)$, where $d \mid m$, are $P\big(\zeta_m^{de}(t+1)^{1/m}\big)$ $(0 \leqslant e < m/d)$. Therefore

$$Q(t, l, i_1, \dots, i_k) \in \overline{K}\big(((t+1)^{1/d})\big), \quad \text{where } d \mid m,$$

if and only if

$$Q(t, l, i_1, \dots, i_k) = Q(t, l, i_1 + ed, \dots, i_l + ed, i_{l+1}, \dots, i_k) \quad (0 \leqslant e < m/d),$$

hence by the choice of a if and only if

$$\{i_1, \dots, i_l\} + d \equiv \{i_1, \dots, i_l\} \bmod m.$$

It follows by Lemma 7 of [5] that $y(t)$ has at $t = -1$ exactly

$$\sum_{l=0}^{k} f(m, l, d) \binom{n-m-1}{k-l}$$

expansions belonging to $\overline{K}\big(((t+1)^{1/d})\big) \setminus \bigcup_{\delta < d} \overline{K}\big(((t+1)^{1/\delta})\big)$, where $d \mid m$ and

$$f(m, l, d) = \begin{cases} \displaystyle\sum_{\delta \mid (d, dl/m)} \mu(\delta) \binom{d/\delta}{\frac{dl/\delta}{m}} & \text{if } m \mid dl, \\ 0 & \text{otherwise.} \end{cases}$$

These expansions split into cycles of d conjugate expansions each, where $m \mid dl$, i.e.

$$d = e \frac{m}{(m, l)}, \quad e \mid (m, l).$$

Hence the number of distinct prime divisors of the numerator of $t+1$ is

$$\sum_{l=0}^{k} \frac{m}{(m,l)} \sum_{e\,|\,(m,l)} \frac{1}{e} f\Big(m, l, \frac{em}{(m,l)}\Big)\binom{n-m-1}{k-l},$$

which, by the formula (1) of [5], equals

$$\frac{1}{m}\sum_{l=0}^{k}\binom{n-m-1}{k-l}\sum_{d\,|\,(m,l)}\varphi(d)\binom{m/d}{l/d}. \qquad \square$$

Lemma 7. *The denominator of t in $L_1^*(k,m,n)$ has*

$$\frac{1}{n-m}\sum_{l=0}^{k}\binom{m-1}{k-l}\sum_{d\,|\,(n-m,l)}\varphi(d)\binom{(n-m)/d}{l/d}$$

distinct prime divisors.

Proof. The proof is analogous to the proof of Lemma 6. $\square$

Lemma 8. *If $n \geqslant 6$, $(m,n)=1$, $n-1 \geqslant 2k \geqslant 4$, the genus $g_1^*(k,m,n)$ of $L_1^*(k,m,n)$ satisfies $g_1^*(k,m,n) \geqslant n/6$.*

Proof. By Lemma 2 the only branch points of $y(t)$ may be t_i $(1 \leqslant i \leqslant n-2)$, -1 and ∞.
c It follows now from Lemma 2(a) of [5], and Lemmas 5, 6 and 7 that

$$g_1^*(k,m,n) = \frac{1}{2}\binom{n-3}{k-1}(n-2) - \frac{1}{2m}\sum_{l=0}^{k}\binom{n-m-1}{k-l}\sum_{d\,|\,(m,l)}\varphi(d)\binom{m/d}{l/d}$$
$$- \frac{1}{2(n-m)}\sum_{l=0}^{k}\binom{m-1}{k-l}\sum_{d\,|\,(n-m,l)}\varphi(d)\binom{(n-m)/d}{l/d} + 1.$$

Using this formula we verify the lemma by direct calculation for $n=6,7,8$. To proceed further we first establish the inequality

$$g_1^*(k,m,n) \geqslant 1 + \frac{1}{2(n-1)}\binom{n-1}{k} p_1(k,m,n), \tag{3}$$

where

$$p_1(k,m,n) = k(n-k-1) - \begin{cases} \dfrac{n^2-n+3.5}{n-1} & \text{if } m=1, n-1, \\ \dfrac{(n-1)(n^2-3n+5.5)}{(n-2)^2} & \text{if } m=2, n-2, \\ n\Big(1+\dfrac{3.5}{m(n-m)}\Big) & \text{if } 2<m<n-2. \end{cases}$$

Indeed, by Lemma 13 of [5] we have for $l > 0$

$$\sum_{d\,|\,(m,l)} \varphi(d)\binom{m/d}{l/d} \leqslant \left(1+\frac{3.5}{m}\right)\binom{m}{l}$$

and trivially for $l \geqslant 0$

$$\sum_{d\,|\,(m,l)} \varphi(d)\binom{m/d}{l/d} \leqslant m\binom{m}{l}.$$

Similar inequalities hold with m replaced by $n-m$. Hence, for $m=1$

$$\begin{aligned} g_1^*(k,m,n) &= \frac{1}{2}\binom{n-3}{k-1}(n-2) - \frac{1}{2}\sum_{l=0}^{1}\binom{n-2}{k-l} \\ &\qquad - \frac{1}{2(n-1)}\sum_{d\,|\,(n-1,k)}\varphi(d)\binom{(n-1)/d}{k/d} + 1 \\ &\geqslant 1 + \frac{k(n-k-1)}{2(n-1)}\binom{n-1}{k} - \frac{1}{2}\binom{n-1}{k} - \frac{1}{2(n-1)}\left(1+\frac{3.5}{n-1}\right)\binom{n-1}{k}, \end{aligned}$$

for $m=2$

$$\begin{aligned} g_1^*(k,m,n) &\geqslant \frac{1}{2}\binom{n-3}{k-1}(n-2) - \frac{1}{2}\sum_{l=0}^{2}\binom{n-3}{k-l}\binom{2}{l} \\ &\qquad - \frac{1}{2(n-1)}\sum_{l=k-1}^{k}\left(1+\frac{3.5}{n-2}\right)\binom{n-2}{l} + 1 \\ &= 1 + \frac{k(n-k-1)}{2(n-1)}\binom{n-1}{k} - \frac{1}{2}\binom{n-1}{k} - \frac{1}{2(n-1)}\left(1+\frac{3.5}{n-2}\right)\binom{n-1}{k}, \end{aligned}$$

for m between 2 and $n-2$

$$m-1-\frac{3.5}{m} > 0, \quad n-m-1-\frac{3.5}{n-m} > 0,$$

$$\binom{n-m-1}{k} \leqslant \frac{n-m-1}{n-1}\binom{n-1}{k}, \quad \binom{m-1}{k} \leqslant \frac{m-1}{n-1}\binom{n-1}{k};$$

$$\begin{aligned} g_1^*(k,m,n) &\geqslant \frac{1}{2}\binom{n-3}{k-1}(n-2) - \frac{1}{2m}\binom{n-m-1}{k}m \\ &\quad - \frac{1}{2m}\sum_{l=1}^{k}\binom{n-m-1}{k-l}\left(1+\frac{3.5}{m}\right)\binom{m}{l} - \frac{1}{2(n-m)}\binom{m-1}{k}(n-m) \\ &\quad - \frac{1}{2(n-m)}\sum_{l=1}^{k}\binom{m-1}{k-l}\left(1+\frac{3.5}{n-m}\right)\binom{n-m}{l} + 1 \\ &= \frac{1}{2}\binom{n-3}{k-1}(n-2) - \frac{1}{2m}\binom{n-m-1}{k}\left(m-1-\frac{3.5}{m}\right) - \end{aligned}$$

$$
\begin{aligned}
&- \frac{1}{2m}\left(1+\frac{3.5}{m}\right)\sum_{l=0}^{k}\binom{n-m-1}{k-l}\binom{m}{l}\\
&- \frac{1}{2(n-m)}\binom{m-1}{k}\left(n-m-1-\frac{3.5}{n-m}\right)\\
&- \frac{1}{2(n-m)}\left(1+\frac{3.5}{n-m}\right)\sum_{l=0}^{k}\binom{m-1}{k-l}\binom{n-m}{l}+1\\
\geqslant\ & 1+\frac{k(n-k-1)}{2(n-1)}\binom{n-1}{k}-\frac{n-m-1}{2m(n-1)}\binom{n-1}{k}\left(m-1-\frac{3.5}{m}\right)\\
&- \frac{1}{2m}\left(1+\frac{3.5}{m}\right)\binom{n-1}{k}-\frac{m-1}{2(n-m)(n-1)}\binom{n-1}{k}\left(n-m-1-\frac{3.5}{n-m}\right)\\
&- \frac{1}{2(n-m)}\left(1+\frac{3.5}{n-m}\right)\binom{n-1}{k}.
\end{aligned}
$$

In each case the right hand side of the obtained inequality coincides with the right hand side of (3). Now for $n \geqslant 9$,

$$p_1(k,m,n) \geqslant p_1(2,\min\{m,3\},n) \geqslant \min_{m\leqslant 3} p_1(2,m,9) = 1.25,$$

hence by (3)

$$g_1^*(k,m,n) \geqslant 1+\frac{1.25}{2(n-1)}\binom{n-1}{2} > \frac{n}{4}. \qquad \square$$

Lemma 9. *Let $n \geqslant 3$, $(m,n)=1$, $R_1(x,t)=\prod_{i=1}^{n-1}(x-x_i(t))$. In the field $\overline{K}(t,x_1(t),x_2(t))$ we have the factorizations*

$$
\begin{aligned}
t+1 &\cong \frac{\prod_{i=1}^{m-1}\mathfrak{p}_i^m \prod_{j=1}^{n-m-1}\mathfrak{q}_j^m \prod_{j=1}^{n-m-1}\mathfrak{r}_j^m \prod_{k=1}^{(n-m-1)(n-m-2)}\mathfrak{s}_k}{\prod_{j=1}^{n-m-1}\mathfrak{t}_j^{n-m}\prod_{i=1}^{m-1}\mathfrak{u}_i^{n-m}\prod_{i=1}^{m-1}\mathfrak{v}_i^{n-m}\prod_{l=1}^{(m-1)(m-2)}\mathfrak{w}_l},\\
x_1(t) &\cong \frac{\prod_{i=1}^{m-1}\mathfrak{p}_i \prod_{j=1}^{n-m-1}\mathfrak{q}_j}{\prod_{j=1}^{n-m-1}\mathfrak{t}_j \prod_{i=1}^{m-1}\mathfrak{u}_i},\\
x_2(t) &\cong \frac{\prod_{i=1}^{m-1}\mathfrak{p}_i \prod_{j=1}^{n-m-1}\mathfrak{r}_j}{\prod_{j=1}^{n-m-1}\mathfrak{t}_j \prod_{i=1}^{m-1}\mathfrak{v}_i}
\end{aligned}
$$

where $\mathfrak{p}_i$, $\mathfrak{q}_j$, $\mathfrak{r}_j$, $\mathfrak{s}_k$, $\mathfrak{t}_j$, $\mathfrak{u}_i$, $\mathfrak{v}_i$, $\mathfrak{w}_l$ are distinct prime divisors. For t_i defined in Lemma 2 the numerator of $t-t_i$ has $(n-3)(n-4)$ factors in the first power only, the remaining factors are double.

Proof. By Lemma 1(a)(b) of [5] the prime divisors of the numerator or the denominator of $t - c$ are in one-to-one correspondence with the cycles of the Puiseux expansions of a generating element of $\overline{K}(t, x_1(t), x_2(t))/\overline{K}(t)$ at $t = c$ or $t = \infty$, respectively, provided the lenghts of the cycles are not divisible by π. For the generating element we take $y(t) = ax_1(t) + bx_2(t)$, where $a, b \in \overline{K}$ are chosen so that for all $i < n$, $j < n$, $i \neq j$ we have either $ax_i(t) + bx_j(t) \neq ax_1(t) + bx_2(t)$ or $\langle i, j\rangle = \langle 1, 2\rangle$. By Lemma 4 for each pair $\langle i, j\rangle$ with $i < n$, $j < n$ there is an automorphism of the extension $\overline{K}(t, x_1(t), \ldots, x_n(t))/\overline{K}(t)$ taking $x_1(t), x_2(t)$ into $x_i(t), x_j(t)$, respectively. At $t = -1$ we obtain for $y(t)$ the expansions

$$a\zeta_{2m}^{2i+1}(1+t)^{1/m}P_{n-1,1}\big(\zeta_{2m}^{2i+1}(1+t)^{1/m}\big) + b\zeta_{2m}^{2j+1}(1+t)^{1/m}P_{n-1,1}\big(\zeta_{2m}^{2j+1}(1+t)^{1/m}\big)$$
$$(0 \leqslant i < m,\ 0 \leqslant j < m,\ i \neq j),$$

$$a\zeta_{2m}^{2i+1}(1+t)^{1/m}P_{n-1,1}\big(\zeta_{2m}^{2i+1}(1+t)^{1/m}\big) + bP_{n-1,j}(1+t)$$
$$(0 \leqslant i < m,\ 2 \leqslant j \leqslant n-m),$$

$$aP_{n-1,j}(1+t) + b\zeta_{2m}^{2i+1}(1+t)^{1/m}P_{n-1,1}\big(\zeta_{2m}^{2i+1}(1+t)^{1/m}\big)$$
$$(0 \leqslant i < m,\ 2 \leqslant j \leqslant n-m),$$

$$aP_{n-1,i}(1+t) + bP_{n-1,j}(1+t) \quad (2 \leqslant i \leqslant n-m,\ 2 \leqslant j \leqslant n-m,\ i \neq j).$$

The $m(m-1)$ expansions of the first set form $m-1$ m-cycles corresponding to the divisors $\mathfrak{p}_1, \ldots, \mathfrak{p}_{m-1}$, that divide the numerators of $x_1(t), x_2(t)$ in exactly first power. (Note that $\operatorname{ord}_{\mathfrak{p}_\mu} x_1 = m \operatorname{ord}_{t+1}(1+t)^{1/m}P_{n-1,1}(\zeta_{2m}^{2i+1}(1+t)^{1/m})$ for $\mu < m$ and similarly for x_2.) The $m(n-m-1)$ expansions of the second set form $n-m-1$ m-cycles corresponding to the divisors $\mathfrak{q}_1, \ldots, \mathfrak{q}_{n-m-1}$, that divide the numerator of $x_1(t)$ in exactly first power and do not divide the numerator of $x_2(t)$.

The $m(n-m-1)$ expansions of the third set form $n-m-1$ m-cycles corresponding to the divisors $\mathfrak{r}_1, \ldots, \mathfrak{r}_{n-m-1}$ that divide the numerator of $x_2(t)$ in exactly first power and do not divide the numerator of $x_1(t)$. The $(n-m-1)(n-m-2)$ expansions of the fourth set form as many 1-cycles corresponding to the divisors that divide the numerator of $1+t$ in exactly first power and divide the numerator of neither $x_1(t)$ nor $x_2(t)$.

Since $x_1(t) = 0$ implies $t = -1$ we have found all factors of the numerator of $x_1(t)$ and similarly of $x_2(t)$.

At $t = \infty$ we obtain for $y(t)$ again four sets of expansions that correspond to the four sets of divisors: $\mathfrak{t}_j$ $(1 \leqslant j \leqslant n-m-1)$, $\mathfrak{u}_i, \mathfrak{v}_i$ $(1 \leqslant i \leqslant m-1)$ and $\mathfrak{w}_l$ $(1 \leqslant l \leqslant (m-1)(m-2))$ occurring in the denominator of $1+t$, $x_1(t)$ and $x_2(t)$.

Since $x_1(t) = \infty$ implies $t = \infty$ no other divisor occurs in the denominator of $x_1(t)$, or of $x_2(t)$.

At $t = t_i$ we obtain for $y(t)$ among others the expansions

$$aP_{ij} + bP_{ik} \quad (1 \leqslant i \leqslant n-2,\ 2 \leqslant j \leqslant n-2,\ 2 \leqslant k \leqslant n-2,\ j \neq k)$$

which form $(n-3)(n-4)$ 1-cycles corresponding to $(n-3)(n-4)$ simple factors of the numerator of $t - t_i$. All the remaining expansions contain $(t-t_i)^{1/2}$. □

Lemma 10. *If* $(m, n) = 1$, *for all primes* p

$$\sqrt[p]{t+1} \notin \overline{K}\big(t, x_1(t), \ldots, x_{n-1}(t)\big) =: \Omega.$$

Proof. The argument used in the proof of Lemma 9 applied to the field Ω gives that the multiplicity of every prime divisor of the numerator and the denominator of $t+1$ divides m and $n-m$, respectively. Since $(m, n) = 1$ we cannot have $1 + t = \gamma^p$, $\gamma \in \Omega$. □

Lemma 11. *Let* $(m, n) = 1$, $n \geqslant 3$. *For every positive integer* $q \not\equiv 0 \bmod \pi$ *and for every choice of* q*-th roots we have*

$$\left[\overline{K}\left(\sqrt[q]{x_1(t)}, \ldots, \sqrt[q]{x_{n-1}(t)}\right) : \overline{K}\big(t, x_1(t), \ldots, x_{n-1}(t)\big)\right] = q^{n-1}.$$

Proof. By Theorem 1 of [4] it is enough to prove that for every prime $p \mid q$

$$\prod_{j=1}^{n-1} x_j^{\alpha_j} = \gamma^p, \quad \gamma \in \Omega = \overline{K}\big(t, x_1(t), \ldots, x_{n-1}(t)\big) \tag{4}$$

implies $\alpha_j \equiv 0 \bmod p$ for all $j < n$. Assume that (4) holds, but say $\alpha_1 \not\equiv 0 \bmod p$.

If for all j we have $\alpha_j \equiv \alpha_1 \bmod p$ it follows from (4) that

$$\left(\prod_{j=1}^{n-1} x_j\right)^{\alpha_1} = \gamma'^p, \quad \gamma \in \Omega,$$

and since

$$\prod_{j=1}^{n-1} x_j = (-1)^{n-1}(t+1)$$

we obtain $\sqrt[p]{t+1} \in \Omega$, contrary to Lemma 10. Therefore, there exists an $i \leqslant n-1$ such that $\alpha_i \not\equiv \alpha_1 \bmod p$, and in particular $n \geqslant 3$. Changing, if necessary, the numeration of x_i we may assume that $i = 2$. By Lemma 4 there exists an automorphism τ of $\Omega/\overline{K}(t)$ such that $\tau(x_1) = x_2$, $\tau(x_2) = x_1$, $\tau(x_i) = x_i$ $(i \neq 1, 2)$. Applying τ to (4) we obtain

$$x_1^{\alpha_2} x_2^{\alpha_1} \prod_{j=1}^{n-1} x_j^{\alpha_j} = \big(\gamma^\tau\big)^p,$$

hence on division

$$\left(\frac{x_1}{x_2}\right)^{\alpha_1 - \alpha_2} = \left(\frac{\gamma}{\gamma^\tau}\right)^p.$$

Since $\alpha_1 - \alpha_2 \not\equiv 0 \bmod p$ it follows that

$$\frac{x_1}{x_2} = \delta^p, \quad \delta \in \Omega. \tag{5}$$

The extension $\overline{K}(t, x_1, x_2, \delta)/\overline{K}(t, x_1, x_2)$ is a normal subextension of $\Omega/\overline{K}(t, x_1, x_2)$ of degree 1 or p and, since by Lemma 4 the latter has the symmetric Galois group, we have

either $\delta \in \overline{K}(t, x_1, x_2)$, or $p = 2$,

$$\delta \in \overline{K}\left(t, x_1, x_2 \prod_{\substack{\mu,\nu=3 \\ \nu>\mu}}^{n-1} (x_\nu - x_\mu)\right) \setminus \overline{K}(t, x_1, x_2).$$

In the former case we compare the divisors on both sides of (5) and obtain

$$\delta^p \cong \frac{\prod_{j=1}^{n-m-1} \mathfrak{q}_j \prod_{i=1}^{m-1} \mathfrak{v}_i}{\prod_{j=1}^{n-m-1} \mathfrak{r}_j \prod_{i=1}^{m-1} \mathfrak{u}_i},$$

a contradiction.

In the latter case, since the conjugates of δ with respect to $\overline{K}(t, x_1, x_2)$ are $\pm\delta$ we have

$$\delta = \varepsilon \prod_{\substack{\mu,\nu=3 \\ \nu>\mu}}^{n-1} (x_\nu - x_\mu), \quad \varepsilon \in \overline{K}(t, x_1, x_2),$$

hence

$$\delta = \varepsilon \prod_{\substack{\mu,\nu=1 \\ \nu>\mu}}^{n-1} (x_\nu - x_\mu) \cdot \frac{x_1 - x_2}{\prod_{\nu>1} (x_\nu - x_1) \cdot \prod_{\nu\neq 2} (x_\nu - x_2)}$$
$$= \eta \prod_{\substack{\mu,\nu=1 \\ \nu>\mu}}^{n-1} (x_\nu - x_\mu), \qquad \eta \in K(t, x_1, x_2).$$

It follows by (5) and Lemma 3 that

$$\frac{x_1}{x_2} = \eta^2 \operatorname{disc}_x R_1(x, t) = \text{const}\, \eta^2 (t+1)^{m-1} \prod_{i=1}^{n-2} (t - t_i).$$

For $n \geqslant 5$, by Lemma 9, $t - t_1$ has at least one simple factor, which occurs with a non-zero exponent on the right hand side, but not on the left, a contradiction. On the other hand for $n = 3$ or 4 the divisor of the right hand side is a square, of the left hand side is not. □

Lemma 12. *Let $n \geqslant 3$, $(n, m) = 1$, $q \not\equiv 0 \bmod \pi$, $q \geqslant 2$ and $y_{iq}^q = x_i(t)$ $(1 \leqslant i < n)$. Then*

$$\left[\overline{K}\left(t, \left(\sum_{i=1}^{n-1} y_{iq}\right)^q\right) : \overline{K}(t)\right] = q^{n-2}.$$

Proof. By Lemmas 4 and 11 all embeddings of $\overline{K}(t, y_{1q}, \ldots, y_{n-1,q})/\overline{K}(t)$ into $\overline{K(t)}/\overline{K}(t)$ are given by

$$y_{iq} \to \zeta_q^{\alpha_i} y_{\sigma(i)q} \quad (1 \leqslant i < n), \tag{6}$$

where σ is a permutation of $\{1, 2, \ldots, n-1\}$ and

$$\langle \alpha_1, \ldots, \alpha_{n-1} \rangle \in (\mathbb{Z}/q\mathbb{Z})^{n-1}. \tag{7}$$

We shall show that there are exactly q^{n-2} distinct images of $\big(\sum_{i=1}^{n-1} y_{iq}\big)^q$ under transformations (6). Indeed, if we apply (7) with $\sigma(i) = i$ to $\big(\sum_{i=1}^{n-1} y_{iq}\big)^q$ we obtain

$$\Big(\sum_{i=1}^{n-1} \zeta_q^{\alpha_i} y_{iq}\Big)^q.$$

If this were equal to $\big(\sum_{i=1}^{n-1} \zeta_q^{\beta_i} y_{iq}\big)^q$ for a vector $\langle \beta_1, \ldots, \beta_{n-1} \rangle \in (\mathbb{Z}/q\mathbb{Z})^{n-1}$ with $\beta_j - \beta_1 \neq \alpha_j - \alpha_1$ for a certain j we should obtain

$$y_{1q} \in \overline{K}(y_{2q}, \ldots, y_{n-1,q}), \quad \text{or} \quad y_{jq} \in \overline{K}(y_{1q}, \ldots, y_{j-1,q}, y_{j+1,q}, \ldots, y_{n-1,q}),$$

contrary to Lemma 11. Thus the number of distinct images is at least equal to the number of vectors satisfying (7) with $\alpha_1 = 0$, thus to q^{n-2}. On the other hand, $\big(\sum_{i=1}^{n-1} y_{iq}\big)^q$ is invariant under transformations (6) with $\alpha_1 = \alpha_2 = \ldots = \alpha_{n-1}$, which form a group, hence the number in question does not exceed q^{n-2}. □

Definition 2. Let $(m, n) = 1$, $q \not\equiv 0 \bmod \pi$ and $y_{iq}^q = x_i(t)$, where $x_i(t)$ are defined in Definition 1. We set

$$M_1(m, n, q) = K\Big(t, \Big(\sum_{i=1}^{n-1} y_{iq}\Big)^q\Big), \quad M_{1*}(m, n, q) = \overline{K}\Big(t, \Big(\sum_{i=1}^{n-1} y_{iq}\Big)^q\Big)$$

Remark. By Lemma 12, for $n \geqslant 3$, $M_1(m, n, q)$ and $M_{1*}(m, n, q)$ are determined by m, n, q up to an isomorphism which fixes $K(t)$ and $\overline{K}(t)$, respectively.

Lemma 13. *For $n > 3$ the numerator of $t - t_i$ has $(q^{n-2} - q^{n-3})/2$ factors in the second power in $M_{1*}(m, n, q)$.*

Proof. Let us put for each $i \leqslant n - 2$

$$y_{i1q} = \xi_i^{1/q} \sum_{k=0}^{\infty} \binom{1/q}{k} \xi^{-k/q} (t - t_i)^{k/2} P_{i1}\big((t - t_i)^{1/2}\big)^k,$$

$$y_{i2q} = \xi_i^{1/q} \sum_{k=0}^{\infty} (-1)^k \binom{1/q}{k} \xi^{-k/q} (t - t_i)^{k/2} P_{i1}\big(-(t - t_i)^{1/2}\big)^k,$$

so that for $j = 1, 2$

$$y_{ijq}^q = \xi_i + (-1)^{j-1}(t-t_i)^{1/2} P_{i1}\big((-1)^{j-1}(t-t_i)\big),$$

$$y_{i1q} + y_{i2q} \in \overline{K}\big((t-t_i)\big), \tag{8}$$

$$(y_{i1q} - y_{i2q})(t-t_i)^{1/2} \in \overline{K}\big((t-t_i)\big) \tag{9}$$

and choose in an arbitrary way

$$y_{ijq} = \big(P_{i,j-1}(t-t_i)\big)^{1/q} \in \overline{K}\big((t-t_i)\big) \quad (2 < j < n). \tag{10}$$

It follows from Lemma 2 that over the field $\overline{K}\big((t-t_i)\big)$

$$\prod_{j=1}^{n-1}\prod_{\alpha=0}^{q-1}\Big(x - \zeta_q^\alpha y_{jq}\Big) = R_1(x^q, t) = \prod_{j=1}^{n-1}\prod_{\alpha=0}^{q-1}\Big(x - \zeta_q^\alpha y_{ijq}\Big),$$

thus the corresponding fundamental symmetric functions of $\zeta_q^\alpha y_{jq}$ $(1 \leqslant j < n, 0 \leqslant \alpha < q)$ and of $\zeta_q^\alpha y_{ijq}$ coincide. Hence

$$\prod_{\alpha_2=0}^{q-1}\cdots\prod_{\alpha_{n-1}=0}^{q-1}\Big(x - \Big(y_{1q} + \sum_{j=2}^{n-1}\zeta_q^{\alpha_j} y_{jq}\Big)^q\Big) = \prod_{\alpha_2=0}^{q-1}\cdots\prod_{\alpha_{n-1}=0}^{q-1}\Big(x - \Big(y_{i1q} + \sum_{j=2}^{n-1}\zeta_q^{\alpha_j} y_{ijq}\Big)^q\Big),$$

which means that $\big(\sum_{i=1}^{n-1} y_{jq}\big)^q$ has the following Puiseux expansions at $t = t_i$

$$\Big(y_{i1q} + \zeta_q^{\alpha_2} y_{i2q} + \sum_{j=3}^{n-1}\zeta_q^{\alpha_j} y_{ijq}\Big)^q, \quad \langle\alpha_2, \ldots, \alpha_{n-1}\rangle \in (\mathbb{Z}/q\mathbb{Z})^{n-2}.$$

If such an expansion belongs to $\overline{K}\big((t-t_i)\big)$, then either

$$y_{i1q} + \zeta_q^{\alpha_2} y_{i2q} + \sum_{j=3}^{n-1}\zeta_q^{\alpha_j} y_{ijq} \in \overline{K}\big((t-t_i)\big)$$

or $2 \mid q$ and

$$\Big(y_{i1q} + \zeta_q^{\alpha_2} y_{i2q} + \sum_{j=3}^{n-1}\zeta_q^{\alpha_j} y_{ijq}\Big)(t-t_i)^{1/2} \in \overline{K}\big((t-t_i)\big).$$

In the former case, by (8) and (10)

$$(1 - \zeta_q^{\alpha_2}) y_{i1q} \in \overline{K}\big((t-t_i)\big)$$

and since $P_{i1}(0) \neq 0$, $\alpha_2 = 0$.

In the latter case, by (9), on multiplying it by $(\zeta_q^{\alpha_i} - 1)/2$ and adding

$$\left(\frac{1+\zeta_q^{\alpha_2}}{2}(y_{i1q} + y_{i2q}) + \sum_{j=3}^{n-1} \zeta_q^{\alpha_j} y_{ijq}\right)(t-t_i)^{1/2} \in \overline{K}\big((t-t_i)\big)$$

and, since

$$\frac{1+\zeta_q^{\alpha_2}}{2}(y_{i1q} + y_{i2q}) + \sum_{j=3}^{n-1} \zeta_q^{\alpha_j} y_{ijq} \in \overline{K}\big((t-t_i)\big)$$

by (8) and (10), we obtain

$$\frac{1+\zeta_q^{\alpha_2}}{2}(y_{i1q} + y_{i2q}) + \sum_{j=3}^{n-1} \zeta_q^{\alpha_j} y_{ijq} = 0. \tag{11}$$

However the left hand side is an expansion at $t = t_i$ of

$$\frac{1+\zeta_q^{\alpha_2}}{2}(y_{iq} + y_{2q}) + \sum_{j=3}^{n-1} \zeta_q^{\alpha_j} y_{jq},$$

hence (11) contradicts for $n > 3$ the linear independence of y_{jq} $(1 \leqslant j < n)$ over $\overline{K}$ resulting from Lemma 11.

Therefore for $n > 3$ we obtain $q^{n-2} - q^{n-3}$ expansions for $\big(\sum_{j=3}^{n-1} y_{jq}\big)^q$ belonging to $\overline{K}\big((t-t_i)^{1/2}\big) \setminus \overline{K}\big((t-t_i)\big)$, which correspond to $(q^{n-2}-q^{n-3})/2$ distinct prime divisors of the numerator of $t - t_i$ in $M_{1*}(m, n, q)$. □

Lemma 14. *The numerator of $t + 1$ in $M_{1*}(m, n, q)$ has at most*

$$\frac{q^{\max\{n-3,m-1\}}}{m}\left(1 + \frac{m-1}{q^{\varphi(mq)/\varphi(q)}}\right)$$

distinct prime divisors.

Proof. By Lemma 1(a) in [5] the prime divisors of the numerator of $t + 1$ correspond to the cycles of the Puiseux expansions of $\big(\sum_{j=1}^{n-1} y_{jq}\big)^q$ at $t = -1$ provided the lengths of these cycles are not divisible by π. By Lemma 2 and the argument about symmetric functions used in the proof of Lemma 13 we obtain the expansions

$$\left(\sum_{j=1}^{m} \zeta_q^{\alpha_j} \zeta_{2mq}^{2j-1}(t+1)^{1/qm} P_{n-1,1}\big(\zeta_{2m}^{2j-1}(t+1)^{1/m}\big)^{1/q} + \sum_{j=m+1}^{n-1} \zeta_q^{\alpha_j} P_{n-1,j-m+1}(t+1)^{1/q}\right)^q, \tag{12}$$

where $\langle \alpha_1, \dots, \alpha_{n-1} \rangle \in (\mathbb{Z}/q\mathbb{Z})^{n-1}$, $\alpha_1 = 0$. Note that $qm \not\equiv 0 \bmod \pi$. Let S be the set of vectors $\langle \alpha_2, \dots, \alpha_m \rangle \in (\mathbb{Z}/q\mathbb{Z})^{m-1}$ such that

$$1 + \sum_{j=2}^{m} \zeta_q^{\alpha_j} \zeta_{qm}^{j-1} = 0.$$

By Lemma 21 of [5]

$$\text{card } S \leqslant q^{m-\varphi(qm)/\varphi(q)-1}. \tag{13}$$

If $n \geqslant m+2$ and $\langle \alpha_2, \dots, \alpha_m \rangle \notin S$ the least power of $t+1$ occurring in the first or the second sum in (12) is $(t+1)^{1/qm}$ and $(t+1)^{\nu_0}$, respectively, where ν_0 is a nonnegative integer. Hence the expansion (12) contains with a non-zero coefficient

$$(t+1)^{1/m} \quad \text{and} \quad (t+1)^{(q-1)/qm+\nu_0}. \tag{14}$$

Indeed, if we had for some nonnegative integers a_μ ($\mu = 0, 1, \dots$)

$$\sum_{\mu=0}^{\infty} a_\mu = q \quad \text{and} \quad \sum_{\mu=0}^{\infty} a_\mu \left(\frac{1}{qm} + \frac{\mu}{m} \right) = \frac{q-1}{qm} + \nu_0$$

it would follow from the second formula that $\sum_{\mu=0}^{\infty} a_\mu \equiv q - 1 \bmod q$, contrary to the first formula.

The least common denominator of the two exponents in (14) is

$$\left[m, \frac{qm}{(qm, q-1)} \right] = \frac{qm^2}{(qm^2, (q-1)m, qm)} = qm,$$

hence we obtain at most

$$\frac{(q^{m-1} - \text{card } S) q^{n-m-1}}{qm}$$

qm-cycles.

If $n \geqslant m+2$ and $\langle \alpha_2, \dots, \alpha_m \rangle \in S$ the least power of $t+1$ occurring in the first or the second sum in (12) is $(t+1)^{1/qm+\mu_0/m}$ and $(t+1)^{\nu_0}$, respectively, where $\mu_0 \in \mathbb{N}$ and $\nu_0 \in \mathbb{N}$. Hence the expansion (12) contains with a non-zero coefficient

$$(t+1)^{(q-1)/qm+(q-1)\mu_0/m+\nu_0} \quad \text{if } \frac{1}{qm} + \frac{\mu_0}{m} < \nu_0$$

and

$$(t+1)^{1/qm+\mu_0/m+(q-1)\nu_0} \quad \text{otherwise.}$$

Since both exponents in the reduced form have q in the denominator we obtain at most

$$\frac{\text{card } S \cdot q^{n-m-1}}{q}$$

q-cycles.

If $n = m+1$ and $\langle \alpha_2, \dots, \alpha_m \rangle \notin S$ the least power of $t+1$ occurring in the parentheses in (12) is $(t+1)^{1/qm}$, thus the expansion (12) contains with a non-zero exponent $(t+1)^{1/m}$ and we obtain at most $(q^{m-1} - \operatorname{card} S)/m$ m-cycles.

Finally if $n = m+1$ and $\langle \alpha_2, \dots, \alpha_m \rangle$ runs through S we bound the number of cycles by card S. Therefore by (13), if $n \geqslant m+2$ the total number of cycles does not exceed

$$\frac{(q^{m-1} - \operatorname{card} S)q^{n-m-1}}{qm} + \frac{\operatorname{card} S \cdot q^{n-m-1}}{q}$$
$$= \frac{q^{n-3}}{m}\left(1 + \frac{(m-1)\operatorname{card} S}{q^{m-1}}\right) \leqslant \frac{q^{n-3}}{m}\left(1 + \frac{(m-1)}{q^{\varphi(qm)/\varphi(q)}}\right),$$

if $n = m+1$ the total number of cycles does not exceed

$$\frac{(q^{m-1} - \operatorname{card} S)}{m} + \operatorname{card} S = \frac{q^{m-1}}{m}\left(1 + \frac{(m-1)\operatorname{card} S}{q^{m-1}}\right)$$
$$= \frac{q^{m-1}}{m}\left(1 + \frac{(m-1)}{q^{\varphi(qm)/\varphi(q)}}\right). \quad \square$$

Lemma 15. *The denominator of t has in $M_{1*}(m, n, q)$ at most*

$$\frac{q^{\max\{n-3, n-m-1\}}}{n-m}\left(1 + \frac{n-m-1}{q^{\varphi(q(n-m))/\varphi(q)}}\right)$$

distinct prime divisors.

Proof. Proof is analogous to the proof of Lemma 14. $\square$

Lemma 16. *For all positive integers m, n and q where $n > 3$, $n > m$, $(n, m) = 1$, $qnm(n-m) \not\equiv 0 \bmod \pi$ and $q \geqslant 2$, the genus $g_{1*}(m, n, q)$ of $M_{1*}(m, n, q)$ is greater than $nq/8$ unless $nq \leqslant 16$. Moreover $g_{1*}(m, n, q) > 1$ unless $n < 6$.*

Proof. By Lemma 2(a) of [5] and by Lemmas 13–15 we have

$$g_{1*}(m, n, q) \geqslant 1 + \frac{q^{n-3}}{2}\left(\frac{q-1}{2}(n-2) - \frac{q^{\max\{0, m-n+2\}}}{m}\left(1 + \frac{m-1}{q^{\varphi(qm)/\varphi(q)}}\right)\right.$$
$$\left. - \frac{q^{\max\{0, 2-m\}}}{n-m}\left(1 + \frac{n-m-1}{q^{\varphi(q(n-m))/\varphi(q)}}\right)\right).$$

Hence, by Lemma 24 of [5]

$$g_{1*}(m, n, q) \geqslant 1 + \frac{q^{n-3}}{2}\gamma_1(q, n, m),$$

where

$$\gamma_1(q, n, m) = \begin{cases} \dfrac{q-1}{2}(n-2) - 1 - \dfrac{q+1}{n-1} & \text{if } m = 1 \text{ or } m = n-1, \\ \dfrac{q-1}{2}(n-2) - \left(\dfrac{1}{m} + \dfrac{1}{n-m}\right)\left(1 + \dfrac{1}{q}\right) & \text{otherwise.} \end{cases}$$

For $n \geqslant 6$ we have $q^{n-3} \geqslant \frac{2}{3}nq$, $\gamma_1(q,n,m) \geqslant \frac{2}{5}$, hence $g_{1*}(m,n,q) > 2nq/15 > nq/8 > 1$; for $6 > n > 3$ $g_1^*(m,n,q) \leqslant nq/8$ implies $nq \leqslant 16$. □

3. Proof of Theorems 1 and 2

Proof of Theorem 1. Let $F(x) = x - C$, where $C \in K(\boldsymbol{y})$. Since $F(x) \mid x^{n_1} + Ax^{m_1} + B$ we obtain $B = -C^{n_1} - AC^{m_1}$, $C \neq 0$. From $A^{-n}B^{n-m} \notin K$ we infer that $t := AC^{m_1-n_1} \notin K$. We have the identity

$$Q(x) := \frac{x^{n_1} + Ax^{m_1} + B}{F(x)} = C^{n_1-1}\,\frac{(C^{-1}x)^{n_1} + t(C^{-1}x)^{m_1} - (t+1)}{C^{-1}x - 1}. \tag{15}$$

If $T(x; A, B)F(x^{(m,n)})^{-1}$ is reducible over $K(\boldsymbol{y})$, then by Capelli's Lemma (see e.g. [1], p. 662) either

$$Q(x) \text{ is reducible over } K(\boldsymbol{y}), \tag{16}$$

or

$$x^{(m,n)} - \xi \text{ is reducible over } K(\boldsymbol{y}, \xi), \text{ where } \xi \text{ is a zero of } Q(x). \tag{17}$$

In the former case $Q(x)$ has in $K(\boldsymbol{y})[x]$ a factor $x^k + \sum_{i=1}^{k} a_i x^{k-i}$, where, by the assumption, $2 \leqslant k \leqslant (n_1 - 1)/2$. The identity (15) implies that the field $L_1^*(k, m_1, n_1)$ defined in Definition 1 is a rational function field parametrized as follows:

$$t = AC^{m_1-n_1},\ \tau_i(x_1, \ldots, x_k) = (-1)^i a_i C^{-i} \quad (1 \leqslant i \leqslant k).$$

By Lemma 2(b) of [5] $g_1^*(k, m_1, n_1) = 0$.

Assume now that we have (17) but not (16). It follows by Capelli's theorem that either

$$\xi = \eta^p, \quad \text{where } p \text{ is a prime, } p \mid (m,n),\ \eta \in K(\boldsymbol{y}, \xi), \tag{18}$$

or

$$\xi = -4\eta^4, \quad \text{where } 4 \mid (m,n),\ \eta \in K(\boldsymbol{y}, \xi). \tag{19}$$

Let

$$\frac{x^{n_1} + tx^{m_1} - (t+1)}{x - 1} = \prod_{j=1}^{n_1-1}(x - x_j), \quad y_{jq}^q = x_j.$$

It follows from (15) that if $t = AC^{m_1-n_1}$ one can take

$$\begin{aligned} &q = p, \quad y_{jq} = C^{-1/p}\eta_j && \text{if (18) holds,}\\ &q = 4, \quad y_{jq} = (1 + \zeta_4)C^{-1/4}\eta_j && \text{if (19) holds,} \end{aligned}$$

where η_j are conjugates of η over $K(\boldsymbol{y})$. Hence the field

$$M_{1*}(m_1, n_1, q) = \overline{K}\big(t, (y_{1q} + \ldots + y_{n_1-1,q})^q\big)$$

is parametrized by rational functions as follows

$$t = AC^{m_1-n_1},$$

$$(y_{1q} + \ldots + y_{n_1-1,q})^q = \begin{cases} C^{-1}(\eta_1 + \ldots + \eta_{n_1-1})^p & \text{if (18) holds,} \\ -4C^{-1}(\eta_1 + \ldots + \eta_{n_1-1})^4 & \text{if (19) holds,} \end{cases}$$

and, by Lemma 2(b) of [5], $g_{1*}(m_1, n_1, q) = 0$, contrary to Lemma 16. □

Proof of Theorem 2. The sufficiency of the condition is obvious. The proof of the necessity is similar to that of Theorem 1.

Let $F(x) = x - C$, where $C \in L$,

$$Q(x; A, B) = \frac{x^{n_1} + Ax^{m_1} + B}{F(x)}.$$

Since $F(x) \mid x^{n_1} + Ax^{m_1} + B$ and $B \neq 0$ we have $C \neq 0$, $B = -C^{n_1} - AC^{m_1}$. Since $A^{-n}B^{n-m} \notin \overline{K}$, we have $t := AC^{m_1-n_1} \notin \overline{K}$.

If $T(x; A, B)F(x^{(m,n)})^{-1} = Q(x^{(m,n)}; A, B)$ is reducible over L then either

$$Q(x) := Q(x; A, B) \text{ is reducible over } L \tag{20}$$

or

$$x^{(m,n)} - \xi \text{ is reducible over } L(\xi) \text{ where } \xi \text{ is a zero of } Q. \tag{21}$$

In the former case Q has in $L[x]$ a factor of degree k, where by the assumption $2 \leqslant k \leqslant (n_1 - 1)/2$ and it follows from the identity (15) that the field $L_1^*(k, m_1, n_1)$ is isomorphic to a subfield of $\overline{K}L$. Hence, by Lemma 2(c) of [5], $g_1^*(k, m_1, n_1) \leqslant g$ and, by Lemma 8, $n_1 \leqslant 6 \max\{1, g\}$. In particular, for $g = 1$ we have $n_1 \leqslant 6$. The condition given in the theorem holds with $l = (m, n)$, $\langle \nu, \mu \rangle = \langle n_1, m_1 \rangle$.

Assume now that we have (21), but not (20). Then in the same way as in the proof of Theorem 1 we infer that for a certain $q \mid (m, n)$, $q = 4$ or a prime

$$x^q - \xi \text{ is reducible over } L(\xi) \tag{22}$$

and the field $M_{1*}(m_1, n_1, q)$ is isomorphic to a subfield of $\overline{K}L$. Hence, by Lemma 2(c) of [5], we have $g_{1*}(m_1, n_1, q) \leqslant g$, thus by Lemma 16 for $n_1 > 3$ we have $n_1 q < \max\{17, 8g\}$ and $g > 1$ for $n_1 \geqslant 6$. On the other hand, by (22), $Q(x^q)$ is reducible over L. Hence the condition given in the theorem holds with $l = (m, n)/q$, $\langle \nu, \mu \rangle = \langle n_1 q, m_1 q \rangle$. □

4. Two lemmas to Theorem 3

Lemma 17. *Let L be a finite extension of a field K, q a prime different from* char K. *There exists a finite subset $F = F(q, L/K)$ of K^* of cardinality at most $q^{\mathrm{ord}_q[L:K]}$ such that if*

$$c \in K^*,\ \gamma \in L,\ c = \gamma^q, \tag{23}$$

then there exist $f \in F$ and $e \in K^*$ such that

$$c = fe^q. \tag{24}$$

Proof. Let

$$A = \{a \in K^* : a = \alpha^q,\ \alpha \in L\} \tag{25}$$

and let B be a finite subset of A with the property that for all functions $x : B \to \mathbb{Z}$

$$\prod_{a \in B} a^{x(a)} = b^q, \quad b \in K \text{ implies } x(a) \equiv 0 \bmod q \text{ for all } a \in B. \tag{26}$$

It follows from Theorem 1 of [4] that for every choice of q-th roots

$$\left[K\left(\sqrt[q]{a} : a \in B\right) : K\right] = q^{\operatorname{card} B},$$

hence by (25), in view of $B \subset A$,

$$q^{\operatorname{card} B} \mid [L : K]$$

and $\operatorname{card} B \leqslant \operatorname{ord}_q[L : K]$. Among all subsets B of A with the property (26) let us choose one of maximal cardinality and denote it by A_0. We assert that the set

$$F = \left\{ \prod_{a \in A_0} a^{x(a)} : x(A_0) \subset \{0, 1, \ldots, q-1\} \right\}$$

has the property asserted in the lemma. Indeed

$$\operatorname{card} F = q^{\operatorname{card} A_0} \leqslant q^{\operatorname{ord}_q[L:K]}.$$

c On the other hand, if $c \in A_0$, (24) holds with $f = c, e = 1$. If $c \notin A_0$ the set $B = A_0 \cup \{c\}$ has more elements than A_0. By definition of A_0 it has not the property (26). Hence there exist integers $x(a)$ $(a \in A_0)$ and $x(c)$ such that $c^{x(c)} \prod_{a \in A_0} a^{x(a)} = b^q$, $b \in K$ and either

$$x(c) \equiv 0 \bmod q \text{ and for at least one } a \in A_0 : x(a) \not\equiv 0 \bmod q \tag{27}$$

or

$$x(c) \not\equiv 0 \bmod q. \tag{28}$$

The case (27) is impossible, since it implies

$$\prod_{a \in A_0} a^{x(a)} = \left(bc^{-x(c)/q}\right)^q,$$

contrary to the choice of A_0.

In the case (28) there exist integers y and z such that

$$-x(c)y = 1 + qz$$

and we obtain (24) with

$$f = \prod_{a \in A_0} a^{q\{-x(a)y/q\}}, \quad e = b^{-y} c^{-z} \prod_{a \in A_0} a^{-[x(a)y/q]},$$

where $\{\cdot\}$ and $[\cdot]$ denote the fractional and the integral part, respectively. □

Lemma 18. *Let q be a prime or $q = 4$. For every finite extension $K(\xi)$ of a field K there exists a finite subset $S(q, K, \xi)$ of K such that if $c \in K^*$ and*

$$\begin{aligned} &c\xi = \eta^q, \qquad \eta \in K(\xi)^* \quad \text{if } q \text{ is a prime,} \\ &c\xi = -4\eta^4, \quad \eta \in K(\xi)^* \quad \text{if } q = 4, \end{aligned} \tag{29}$$

then

$$c = de^q, \quad \text{where} \quad d \in S(q, K, \xi),\ e \in K^*. \tag{30}$$

Proof. Assume first that q is a prime. If there is no $c \in K^*$ such that (29) holds we put $S(q, K, \xi) = \emptyset$. Otherwise we have

$$c_0\xi = \eta_0^q, \quad \eta_0 \in K(\xi)^*, \quad c_0 \in K^* \tag{31}$$

and the equations (29) and (31) give

$$c/c_0 = (\eta/\eta_0)^q.$$

Hence, by Lemma 17

$$c/c_0 = fe^q, \quad \text{where} \quad f \in F(q, K(\xi)/K),\ e \in K^*,$$

and in order to satisfy (30) it is enough to put

$$S(q, K, \xi) = \{c_0 f :\ f \in F(q, K(\xi)/K)\}.$$

Assume now that $q = 4$. Again if there is no c such that (29) holds we put $S(q, K, \xi) = \emptyset$. Otherwise, we have

$$c_0\xi = -4\eta_0^4, \quad \eta_0 \in K(\xi)^*,\ c_0 \in K^* \tag{32}$$

and the equations (29) and (32) give

$$c/c_0 = (\eta/\eta_0)^4. \tag{33}$$

By Lemma 17 applied with $q = 2$

$$c/c_0 = fe^2, \quad f \in F\big(2, K(\xi)/K\big), \quad e \in K^*. \tag{34}$$

If for a given $f \in F\big(2, K(\xi)/K\big)$ there exists $e_f \in K^*$ such that

$$fe_f^2 = \vartheta^4, \quad \vartheta \in K(\xi) \tag{35}$$

the equations (33)–(35) give

$$\big(e/e_f\big)^2 = (\eta/\eta_0\vartheta)^4, \quad \text{hence } e/e_f = \pm(\eta/\eta_0\vartheta)^2$$

and another application of Lemma 17 gives

$$e/e_f = \pm f_1 e_1^2, \quad f_1 \in F(2, K(\xi)/K), \quad e_1 \in K^*.$$

Hence, by (34)

$$c/c_0 = fe_f^2 f_1^2 e_1^4$$

and in order to satisfy (30) it is enough to put

$$S(q, K, \xi) = \bigcup_{\substack{f \in F(2, K(\xi)/K) \\ e_f \text{ exists}}} \{c_0 f e_f^2 f_1^2 : f_1 \in F(2, K(\xi)/K)\}. \qquad \square$$

5. Proof of Theorem 3

We begin by defining the sets $F^1_{\nu,\mu}(K)$. This is done in three steps. First we put $q = (\mu, \nu), \nu_1 = \nu/q, \mu_1 = \mu/q$ and introduce the fields $L_1(k, \mu_1, \nu_1)$ and $M_1(\mu_1, \nu_1, q)$ as defined in Definitions 1, 2. Since K is infinite we have $L_1(k, \mu_1, \nu_1) = K(t, y(t))$, where $y(t)$ is defined up to a conjugacy over $K(t)$ in the proof of Lemma 6. Let Φ^1_k be the minimal polynomial of $y(t)$ over $K(t)$. It follows from the definition of $y(t)$ that $\Phi^1_k \in K[t, z]$. By Lemma 12 the function $(y_{1q} + \ldots + y_{\nu_1-1,q})^q$ generating $M_1(\mu_1, \nu_1, q)$ over $K(t)$ is determined up to a conjugacy. Let Ψ^1_q be its minimal polynomial over $K(t)$. Since y_{iq} are integral over $K[t]$ we have $\Psi^1_q \in K[t, z]$. If $\nu_1 > 6$ we put

$$S^1_{\nu,\mu}(K) = \begin{cases} \bigcup_{2<2k<\nu_1} \{t_0 \in K : \Phi^1_k(t_0, z) \text{ has a zero in } K\} & \text{if } q = 1, \\ \{t_0 \in K : \Psi^1_q(t_0, z) \text{ has a zero in } K\} & \text{if } q > 1. \end{cases}$$

Since for $\nu_1 > 6$ and $k > 1$ or $q > 1$ we have $g^*_1(k, \mu_1, \nu_1) > 1$ or $g_{1*}(\mu_1, \nu_1, q) > 1$, respectively, it follows by the Faltings theorem that the sets $S^1_{\nu,\mu}(K)$ are finite. Now we put

$$T^1_{\nu,\mu}(K) = \begin{cases} \bigcup_{t_0 \in S^1_{\nu,\mu}(K)} \{\langle t_0, -t_0 - 1, 1\rangle\} & \text{if } q = 1, \\ \bigcup_{t_0 \in S^1_{\nu,\mu}(K)} \{\langle t_0 d^{\nu_1-\mu_1}, -(t_0+1)d^{\nu_1}, d\rangle : \exists \xi_0\, d \in S(q, K, \xi_0), \\ \qquad \xi_0^{\nu_1} + t_0 \xi_0^{\mu_1} - (t_0 + 1) = 0\} & \text{if } q \text{ is a prime or } q = 4, \\ \emptyset & \text{otherwise} \end{cases}$$

($S(q, K, \xi)$ is defined in Lemma 18);

$$F^1_{\nu,\mu}(K) = \Big\{\langle a, b, x - d\rangle : \langle a, b, d\rangle \in T^1_{\nu,\mu}(K) \text{ and } \frac{x^\nu + ax^\mu + b}{x^q - d} \text{ is a polynomial reducible over } K\Big\}.$$

Since the sets $S^1_{\nu,\mu}(K)$ and the sets $S(q, K, \xi_0)$ are finite, so are the sets $F^1_{\nu,\mu}(K)$. We proceed to prove that they have all the other properties asserted in the theorem.

By the assumption $n_1 > 6$ and $x^{n_1} + ax^{m_1} + b$ has in $K[x]$ a linear factor $F(x)$ but not a quadratic factor. Let $F(x) = x - c$, where $c \in K^*$, so that $b = -c^{n_1} - ac^{m_1}$. Put

$$t_0 = ac^{m_1-n_1}, \quad Q(x; a, b) = \frac{x^{n_1} + ax^{m_1} + b}{F(x)}. \tag{36}$$

Assume that

$$\frac{x^n + ax^m + b}{F(x^{(m,n)})} = Q\big(x^{(m,n)}; a, b\big) \text{ is reducible over } K.$$

By Capelli's lemma either

$$Q(x; a, b) \text{ is reducible over } K \tag{37}$$

or

$$x^{(n,m)} - \xi \text{ is reducible over } K, \text{ where } Q(\xi; a, b) = 0. \tag{38}$$

In the case (37) $Q(x; a, b)$ has a factor in $K[x]$ of degree k such that $1 < k \leqslant (n_1 - 1)/2$, say $\prod_{i=1}^{k}(x - \xi_i)$. It follows from the identity

$$\frac{x^{n_1} + t_0 x^{m_1} - (t_0 + 1)}{x - 1} = c^{1-n_1} Q(cx; a, b) \tag{39}$$

that the left hand side has the factor $\prod_{i=1}^{k}(x - c^{-1}\xi_i)$, thus $\tau_i(c^{-1}\xi_1, \ldots, c^{-1}\xi_k) \in K$ $(1 \leqslant i \leqslant k)$ and at least one value of the algebraic function $y(t)$ at $t = t_0$ lies in K, hence $t_0 \in S^1_{n_1,m_1}(K)$. It follows that $\langle t_0, -t_0 - 1, 1\rangle \in T^1_{n_1,m_1}(K)$, $\langle t_0, -t_0 - 1, x - 1\rangle \in F^1_{n_1,m_1}(K)$ and the condition given in the theorem holds with $l = (m, n)$, $\nu = n_1$, $\mu = m_1$, $a_0 = t_0$, $b_0 = -t_0 - 1$, $F_0 = x - 1$, $u = c$.

In the case (38) note that

$$Q(\xi; a, b) = 0 \quad \text{implies} \quad \xi \neq 0. \tag{40}$$

Further, by Capelli's theorem, there exists a $q \mid (m, n)$ such that

$$\begin{gathered} \text{either } q \text{ is a prime and } \xi = \eta^q,\ \eta \in K(\xi)^* \\ \text{or } q = 4 \text{ and } \xi = -4\eta^4,\ \eta \in K(\xi)^*. \end{gathered} \tag{41}$$

If $\eta_1, \ldots, \eta_{n_1-1}$ are all the conjugates of η over K we have

$$Q(x; a, b) = \begin{cases} \prod_{i=1}^{n_1-1}(x - \eta_i^q) & \text{if } q \text{ is a prime,} \\ \prod_{i=1}^{n_1-1}(x + 4\eta_i^4) & \text{if } q = 4, \end{cases}$$

hence

$$Q(x^q; a, b) \text{ is reducible over } K. \tag{42}$$

By the identity (39) it follows that

$$\frac{x^{n_1}+t_0x^{m_1}-(t_0+1)}{x-1}=\begin{cases}\prod_{i=1}^{n_1-1}(x-c^{-1}\eta_i^q) & \text{if } q \text{ is a prime,}\\ \prod_{i=1}^{n_1-1}(x+4c^{-1}\eta_i^4) & \text{if } q=4.\end{cases}$$

Hence $\Psi_q^1(t_0,u_0)=0$, where

$$u_0=\begin{cases}c^{-1}(\eta_1+\ldots+\eta_{n_1-1})^q & \text{if } q \text{ is a prime,}\\ -4c^{-1}\left(\eta_1+\ldots+\eta_{n_1-1}\right)^4 & \text{if } q=4,\end{cases}$$

and, since $\eta_1+\ldots+\eta_{n_1-1}\in K$, we have $u_0\in K$, $t_0\in S_{n_1,m_1}(K)$.

Further, it follows from (39) and (40) that $\xi_0=c^{-1}\xi$ is a zero of the polynomial $\big(x^{n_1}+t_0x^m-(t_0+1)\big)/(x-1)$ and, by (41), $c\xi_0=\eta^q$ or $-4\eta^4$, where $\eta\in K(\xi_0)^*$ and q is a prime or $q=4$, respectively.

By Lemma 18 $c=de^q$, where $d\in S(q,K,\xi_0)$, $e\in K$, hence

$$\langle t_0d^{n_1-m_1},-(t_0+1)d^{n_1},d\rangle\in T^1_{n_1q,m_1q}(K).$$

By (39)

$$\frac{x^{n_1q}+t_0d^{n_1-m_1}x^{m_1q}-(t_0+1)d^{n_1}}{x^q-d}=(cd^{-1})^{1-n_1}Q\big((ex)^q;a,b\big),$$

hence, by (42)

$$\frac{x^{n_1q}+t_0d^{n_1-m_1}x^{m_1q}-(t_0+1)d^{n_1}}{x^q-d}\text{ is reducible over }K$$

and $\langle t_0d^{n_1-m_1},-(t_0+1)d^{n_1},x-d\rangle\in F^1_{n_1q,m_1q}(K)$. Thus the condition given in the theorem holds with $l=(m,n)/q$, $\nu=n_1q$, $\mu=m_1q$, $a_0=t_0d^{n_1-m_1}$, $b_0=-(t_0+1)d^{n_1}$, $F_0=x-d$, $u=e$.

Assume now that for an integer $l: n/l=\nu$, $m/l=\mu$ and $a=u^{\nu-\mu}a_0$, $b=u^\nu b_0$, $F(x)=u^{(\nu,\mu)}F_0(x/u^{(\nu,\mu)})$, where $u\in K^*$, $\langle a,b,F_0\rangle\in F^1_{\nu,\mu}(K)$. Then by the definition of $F^1_{\nu,\mu}(K)$

$$\frac{x^\nu+ax^\mu+b}{F_0(x^{(\mu,\nu)})}\text{ is a polynomial reducible over }K,$$

and by the substitution $x\mapsto x^l/u$ we obtain reducibility of $T(x;a,b)F(x^{(n,m)})^{-1}$ over K.

The proof of Theorem 3 is complete. □

6. Addendum to the paper [5] ([2])

The formulae for $T_{\nu,\mu}(K)$ in [5], p. 62 (p. 525 in this volume) make sense only for $u_0 \neq 0$. If $u_0 = 0$ one should write instead, both for q prime and $q = 4$, $\langle t_0^{\rho} d^{(\nu-\mu)/q}, t_0^{\sigma} d^{\nu/q} \rangle$, where $d \in S(q, K, \xi_0)$ and $\xi_0^{\nu/q} + t_0^{\rho} \xi_0^{\mu/q} + t_0^{\sigma} = 0$. $S(q, K, \xi)$ is the set defined in Lemma 18 above.

If $x^n + ax^m + b$ is reducible over K and $x^{n_1} + ax^{m_1} + b$ is irreducible over K, then retaining the notation of [5] and putting $\xi_0 = a^{-s} b^r \xi$ we argue as follows.

Since $a^s b^{-r} \xi_0 = \xi = \eta^q$ or $-4\eta^4$, where $\eta \in K(\xi)^*$ and q is a prime or $q = 4$, respectively, we have by Lemma 18 above

$$a^s b^{-r} = d e^q, \ d \in S(q, K, \xi_0), \ e \in K.$$

Since, by (74) $t_0 = a^{-n_1} b^{n_1 - m_1}$ we obtain

$$a = a^{s(n_1-m_1)-rn_1} = t_0^r (de^q)^{n_1-m_1} = t_0^r d^{n_1-m_1} e^{n_1 q - m_1 q},$$
$$b = b^{s(n_1-m_1)-rn_1} = t_0^s (de^q)^{n_1} = t_0^r d^{n_1} e^{qn_1}.$$

By (75) $x^{n_1 q} + t_0^r d^{n_1-m_1} x^{m_1 q} + t_0^s d^{n_1}$ is reducible over K, hence $\langle t_0^r d^{n_1-m_1}, t_0^s d^{n_1} \rangle \in F_{n_1 q, m_1 q}$ and (ix) holds with $l = (m, n)/q$, $\nu = n_1 q$, $\mu = m_1 q$, $u = e$.

References

[3] L. Rédei, *Algebra* I. Akademische Verlagsgesellschaft, Geest & Portig, Leipzig 1959. ([3]).

[4] A. Schinzel, *On linear dependence of roots*. Acta Arith. 28 (1975), 161–175; this collection: C7, 238–252.

[5] —, *On reducible trinomials*. Dissert. Math. (Rozprawy Mat.) 329 (1993); this collection: D10, 466–548.

[6] —, *Errata* to [5]. Acta Arith. 73 (1995), 399–400.

[7] N. Tschebotaröw, *Grundzüge der Galoisschen Theorie*. Übersetzt und bearbeitet von H. Schwerdtfeger, Noordhoff, Groningen–Djakarta 1950.

([2]) The corrections listed in the original paper are put in this volume directly to the text of D10.

([3]) [1] and [2] are moved to D10 since they concern the items added to Table 5 there.

Originally published in
Periodica Mathematica Hungarica 43 (2001), 43–69

On reducible trinomials III

Dedicated to Professor András Sárközy
on the occasion of his 60th birthday

Abstract. It is shown that if a trinomial has a trinomial factor then under certain conditions the cofactor is irreducible.

1.

This paper is a sequel to [7] and [8]. We considered in these papers an arbitrary field K of characteristic π, the rational function field $K(\boldsymbol{y})$, where $\boldsymbol{y}$ is a variable vector, a finite separable extension L of $K(y_1)$ and a trinomial

$$T(x; A, B) = x^n + Ax^m + B, \text{ where } n > m > 0, \ \pi \nmid mn(n-m) \tag{i}$$

and either $A, B \in K(\boldsymbol{y})^*$, $A^{-n}B^{n-m} \notin K$ or $A, B \in L^*$, $A^{-n}B^{n-m} \notin \overline{K}$.

Let

$$n_1 = n/(n,m), \ m_1 = m/(n,m) \tag{ii}$$

and let $F(x)$ be a monic factor $x^{n_1} + Ax^{m_1} + B$ of maximal possible degree $d \leqslant 2$. The reducibility of $T(x; A, B)F(x^{(m,n)})^{-1}$ over $K(\boldsymbol{y})$ or L was studied in [7] for $d = 0$ and in [8] for $d = 1$. Here we study the reducibility of the above quotient for $d = 2$ and in this way complete the proof of the following theorems (the notation introduced in (i) and (ii) being retained).

Theorem 1. *Let $A, B \in K(\boldsymbol{y})^*$, $A^{-n}B^{n-m} \notin K$, F be a monic factor of $x^{n_1} + Ax^{m_1} + B$ in $K(\boldsymbol{y})[x]$ of maximal possible degree $d \leqslant 2$. If $n_1 > \max\{5, 7 - 2d\}$ then $T(x; A, B)F(x^{(m,n)})^{-1}$ is irreducible over $K(\boldsymbol{y})$.*

Theorem 2. *Let L be a finite separable extension of $K(y_1)$ with $\overline{K}L$ of genus g and $A^{-n}B^{n-m} \notin \overline{K}$ and let F be a monic factor of $x^{n_1} + Ax^{m_1} + B$ in $K(\boldsymbol{y})[x]$ of maximal possible degree $d \leqslant 2$. If $n_1 > d + 2$, then*

$$T(x; A, B)F(x^{(n,m)})^{-1} \text{ is reducible over } L \tag{iii}$$

if and only if there exists an integer l such that $\langle n/l, m/l\rangle =: \langle \nu, \mu\rangle \in \mathbb{N}^2$, $\nu < \max\left\{9d^2 - 8d + 16, 24g/(2d+1)\right\}$ and $(x^\nu + Ax^\mu + B)/F(x^{(\nu,\mu)})$ is reducible over L.

Moreover, if $g = 1$, then (iii) *implies $n_1 \leqslant \max\{6, 9 - 3d\}$.*

Theorem 3. *Let K be an algebraic number field and $a, b \in K^*$. If F is a monic factor of $x^{n_1} + ax^{m_1} + b$ in $K[x]$ of maximal possible degree $d \leqslant 2$ and $n_1 > \max\{6, 9-3d\}$, then $T(x; a, b)F(x^{(n,m)})^{-1}$ is reducible over K if and only if there exists an integer l such that $\langle n/l, m/l\rangle =: \langle \nu, \mu\rangle \in \mathbb{N}^2$ and $a = u^{\nu-\mu}a_0$, $b = u^{\nu}b_0$, $F = u^{d(\mu,\nu)}F_0\big(x/u^{(\mu,\nu)}\big)$, where $u \in K^*$, $\langle a_0, b_0, F_0\rangle \in F^d_{\nu,\mu}(K)$ and $F^d_{\nu,\mu}(K)$ is a certain finite set, possibly empty.*

In analogy with a conjecture proposed in [7] we formulate

Conjecture. *For every algebraic number field K and each $d \leqslant 2$ one can choose sets $F^d_{\nu,\mu}(K)$ such that the set*

$$\sum{}^{d} = \bigcup_{\nu,\mu,F} \bigcup_{\langle a,b,F\rangle \in F^d_{\nu,\mu}} \{x^{\nu} + ax^{\mu} + b\} \quad \textit{is finite.}$$

For $d = 0$ or 1 Theorems 1–3 have been proved in [7] or [8], respectively. Proofs for $d = 2$ given in Section 3 are preceded in Section 2 by 23 lemmas.

2.

Lemma 1. *Let polynomials f_n be given by the formulae*

$$f_n = \frac{1}{\sqrt{t-4}}\left(\left(\frac{\sqrt{t}+\sqrt{t-4}}{2}\right)^n - \left(\frac{\sqrt{t}-\sqrt{t-4}}{2}\right)^n\right) \quad \textit{if } n \textit{ is odd},$$

$$f_n = \frac{1}{\sqrt{t(t-4)}}\left(\left(\frac{\sqrt{t}+\sqrt{t-4}}{2}\right)^n - \left(\frac{\sqrt{t}-\sqrt{t-4}}{2}\right)^n\right) \quad \textit{if } n \textit{ is even}.$$

The polynomial f_n is monic separable of degree $[(n-1)/2]$ with

$$f_n(0) = \begin{cases} (-1)^{(n-1)/2} & \textit{if } n \textit{ is odd}, \\ (-1)^{n/2-1}n/2 & \textit{if } n \textit{ is even}; \end{cases} \qquad f_n(4) = \begin{cases} n & \textit{if } n \textit{ is odd}, \\ n/2 & \textit{if } n \textit{ is even} \end{cases}$$

and $(n, m) = 1$ implies $(f_n, f_m) = 1$.

Moreover

$$T_k\left(\frac{\sqrt{t}}{2}\right)^2 \equiv 1 \bmod f_k$$

and

$$f_n \equiv t^{\{n/2\}-\{m/2\}}T_{n-m}\left(\frac{\sqrt{t}}{2}\right) f_m \bmod f_{n-m}, \tag{1}$$

where T_k is the Chebyshev polynomial of the first kind, defined by

$$\cos kx = T_k(\cos x).$$

Proof. We have (see [5], Exercise 1.2.20)

$$f_n = t^{-\{(n-1)/2\}} U_{n-1}\left(\frac{\sqrt{t}}{2}\right),$$

where U_k is the Chebyshev polynomial of the second kind, defined by the equation

$$\frac{\sin(k+1)x}{\sin x} = U_k(\cos x).$$

Now the properties of f_n except formula (1) follow from the well known properties of Chebyshev polynomials (see [5], Exercise 1.2.15 (i) and Remark 1 on p. 233). Formula (1) follows from the identity

$$U_{n-1}(x) = T_{n-m}(x)U_{m-1}(x) + T_m(x)U_{n-m-1}(x). \qquad \square$$

Lemma 2. *The discriminant of a trinomial $ax^n + bx^m + c$, where $n > m > 0$, $(n, m) = 1$, $a \neq 0$, equals*

$$(-1)^{n(n-1)/2} a^{n-m-1} c^{m-1} \left(m^m (n-m)^{n-m} b^n - n^n a^m c^{n-m}\right).$$

Proof. See [3]. $\square$

Lemma 3. *Let $(n, m) = 1$, $\alpha = [n/2] - [m/2]$, $\beta = [(n+m)/2] - [m/2]$, i.e.*

$$\langle \alpha, \beta \rangle = \begin{cases} \left\langle \dfrac{n-m}{2}, \dfrac{n+1}{2} \right\rangle & \text{if } n \equiv m \equiv 1 \bmod 2, \\ \left\langle \dfrac{n-m-1}{2}, \dfrac{n-1}{2} \right\rangle & \text{if } n \equiv 1,\ m \equiv 0 \bmod 2, \\ \left\langle \dfrac{n-m+1}{2}, \dfrac{n}{2} \right\rangle & \text{if } n \equiv 0,\ m \equiv 1 \bmod 2, \end{cases}$$

$$T(x,t) = f_m x^n - t^\alpha f_n x^m + t^\beta f_{n-m},$$

$$R_2(x,t) = \frac{T(x,t)}{x^2 - xt + t}.$$

$R_2(x,t)$ is a polynomial and its discriminant with respect to x equals

(2) $$\operatorname{disc}_x R_2(x,t) = \frac{(-1)^{n(n-1)/2} t^\gamma (t-4) f_m^{n-m-1} f_{n-m}^{m-1} \left(m^m (n-m)^{n-m} t^\delta f_n^n - n^n t^\varepsilon f_m^m f_{n-m}^{n-m}\right)}{E(t)^2},$$

where

$$E(t) = 2mnt^{\{(n-m)/2\}} T_{n-m}\left(\frac{\sqrt{t}}{2}\right) f_m f_n - m^2 t^{2\{(n-1)/2\}} f_n^2 - n^2 t^{2\{(m-1)/2\}} f_m^2$$

and

$$\langle \gamma, \delta, \varepsilon \rangle = \begin{cases} \left\langle \dfrac{n^2-5n+m+5}{2}, 0, \dfrac{n-m}{2} \right\rangle & \text{if } n \equiv m \equiv 1 \bmod 2, \\ \left\langle \dfrac{n^2-6n-m+11}{2}, 0, \dfrac{m}{2} \right\rangle & \text{if } n \equiv 1,\ m \equiv 0 \bmod 2, \\ \left\langle \dfrac{n^2-5n+6}{2}, \dfrac{n}{2}, 0 \right\rangle & \text{if } n \equiv 0,\ m \equiv 1 \bmod 2. \end{cases}$$

Proof. We have

$$x^2 - tx + t = \big(x - u(u+v)\big)\big(x - v(u+v)\big),$$

where

$$u = \frac{\sqrt{t} + \sqrt{t-4}}{2}, \quad v = \frac{\sqrt{t} - \sqrt{t-4}}{2}$$

and using the definition of f_k we easily find

$$T\big(u(u+v), t\big) = T\big(v(u+v), t\big) = 0,$$

hence $R_2(x,t)$ is a polynomial.

From the well known properties of discriminants and resultants it follows that

$$\begin{aligned} &\operatorname{disc}_x T(x,t) \\ &\quad = \operatorname{disc}_x R_2(x,t) \cdot \operatorname{disc}_x(x^2 - tx + t) \cdot \operatorname{res}_x\big(R_2(x,t), x^2 - tx + t\big)^2 \\ &\quad = \operatorname{disc}_x R_2(x,t)(t^2 - 4t) R_2\big(u(u+v), t\big)^2 R_2\big(v(u+v), t\big)^2. \end{aligned} \tag{3_1}$$

We have by Lemma 2

$$\begin{aligned} &\operatorname{disc}_x T(x,t) \\ &\quad = (-1)^{n(n-1)/2} f_m^{n-m-1} t^{(m-1)\beta} f_{n-m}^{m-1} \\ &\qquad\qquad \times \big(m^m (n-m)^{n-m} t^{n\alpha} f_n^n - n^n f_m^m t^{(n-m)\beta} f_{n-m}^{n-m}\big) \\ &\quad = (-1)^{n(n-1)/2} t^{(m-1)\beta + \min\{n\alpha, (n-m)\beta\}} f_m^{n-m-1} f_{n-m}^{m-1} \\ &\qquad\qquad \times \big(m^m (n-m)^{n-m} t^{\delta} f_n^n - n^n t^{\varepsilon} f_m^m f_{n-m}^{n-m}\big). \end{aligned} \tag{3_2}$$

In order to compute $R_2(u(u+v), t)$ we differentiate the equality

$$T(x,t) = (x^2 - tx + t) R_2(x,t)$$

at $x = u(u+v)$ and obtain

$$T_x'\big(u(u+v), t\big) = \big(2u(u+v) - t\big) R_2\big(u(u+v), t\big).$$

Similarly

$$T_x'\big(v(u+v), t\big) = \big(2v(u+v) - t\big) R_2\big(v(u+v), t\big),$$

hence

$$
\begin{aligned}
&R_2\big(u(u+v),t\big)R_2\big(v(u+v),t\big)\\
&\quad=(4t-t^2)^{-1}T_x'\big(u(u+v),t\big)T_x'\big(v(u+v),t\big)\\
&\quad=(4t-t^2)^{-1}\left(nf_mu^{n-1}(u+v)^{n-1}-mt^\alpha f_nu^{m-1}(u+v)^{m-1}\right)\\
&\qquad\times\left(nf_mv^{n-1}(u+v)^{n-1}-mt^\alpha f_nv^{m-1}(u+v)^{m-1}\right)\\
&\quad=(t^2-4t)^{-1}\big(mnt^\alpha f_mf_n\left(u^{n-m}+v^{n-m}\right)(u+v)^{n+m-2}\\
&\qquad-n^2f_m^2(u+v)^{2n-2}-m^2t^{2\alpha}f_n(u+v)^{2m-2}\big)\\
&\quad=(t^2-4t)^{-1}\left(2mnt^{\alpha+(n+m-2)/2}T_{n-m}\left(\frac{\sqrt{t}}{2}\right)f_mf_n\right.\\
&\qquad\left.-n^2t^{n-1}f_m^2-m^2t^{2\alpha+m-1}f_n^2\right)\\
&\quad=(t^2-4t)^{-1}\,t^{\min\{\alpha+(n+m-2)/2+\{(n-m)/2\},\,n-1,\,2\alpha+m-1\}}\\
&\qquad\times\left(2mnt^{\{(n-m)/2\}}T_{n-m}\left(\frac{\sqrt{t}}{2}\right)f_mf_n\right.\\
&\qquad\left.-m^2t^{2\{(n-1)/2\}}f_n^2-n^2t^{2\{(m-1)/2\}}f_m^2\right).
\end{aligned}
\tag{4}
$$

Since

$$
\begin{aligned}
&(m-1)\beta+\min\{n\alpha,\ (n-m)\beta\}\\
&\qquad-2\min\left\{\alpha+\frac{n+m-2}{2}+\left\{\frac{n-m}{2}\right\},\ n-1,\ 2\alpha+m-1\right\}+1=\gamma
\end{aligned}
$$

(2) follows from (3)–(4). □

Lemma 4. *If* $(m,n)=1$,

$$D(t):=(t-4)\big(m^m(n-m)^{n-m}t^\delta f_n^n-n^nt^\varepsilon f_m^mf_{n-m}^{n-m}\big)E(t)^{-2}$$

is a separable polynomial of degree $\binom{n-2}{2}$.

Proof. We easily check that $E(t)$ is a polynomial of degree $n-1$ with the leading coefficient $m(n-m)$ and that $E(4)=0$. Moreover

$$E(t)\equiv -m^2t^{2\{(m-1)/2\}}f_n(t)^2 \bmod f_m$$

and, by Lemma 1,

$$
\begin{aligned}
E(t)&\equiv 2mnt^{\{(n-m)/2\}+\{n/2\}-\{m/2\}}T_{n-m}\left(\frac{\sqrt{t}}{2}\right)^2f_m^2\\
&\quad-m^2t^{2\{(n-1)/2\}+2\{n/2\}-2\{m/2\}}T_{n-m}\left(\frac{\sqrt{t}}{2}\right)^2f_m^2-n^2t^{2\{(m-1)/2\}}f_m^2\\
&\equiv t^{2\{(m-1)/2\}}f_m^2(2mn-m^2-n^2)\equiv-(n-m)^2t^{2\{(m-1)/2\}}f_m^2 \bmod f_{n-m}.
\end{aligned}
$$

Hence, by Lemma 1,

$$(f_m f_{n-m},\ E) = 1$$

and, by Lemma 3,

$$D \in K[t].$$

Moreover,

$$\deg D = 1 + \deg\bigl(m^m (n-m)^{n-m} t^\delta f_n^n - n^n t^\varepsilon f_m^m f_{n-m}^{n-m}\bigr) - 2\deg E$$
$$= 1 + \binom{n}{2} - 2(n-1) = \binom{n-2}{2}.$$

In order to prove that D is separable, assume that $(t-a)^2 \mid D(t)$. Then

$$(t-a)^2 \left(\frac{E(t)}{t-4}\right)^2 \Bigm| m^m (n-m)^{n-m} t^\delta f_n^n - n^n t^\varepsilon f_m^m f_{n-m}^{n-m}$$

and

$$(t-a)\frac{E(t)}{t-4} \Bigm| m^m (n-m)^{n-m} f_n^{n-1} \left(\delta t^{\delta-1} f_n + n t^\delta f_n'\right)$$
$$- n^n f_m^{m-1} f_{n-m}^{n-m-1} \left(\varepsilon t^{\varepsilon-1} f_m f_{n-m} + t^\varepsilon m f_m' f_{n-m} + t^\varepsilon (n-m) f_m f_{n-m}'\right).$$

Since $(f_n,\ f_m f_{n-m}) = 1$ and $\varepsilon\delta = 0$ it follows that either

$$(5_1) \qquad (t-a)\frac{E(t)}{t-4} \Bigm| \begin{vmatrix} f_n & t f_m f_{n-m} \\ n f_n' & \varepsilon f_m f_{n-m} + t m f_m' f_{n-m} + t(n-m) f_m f_{n-m}' \end{vmatrix}$$

if $\delta = 0$, or

$$(5_2) \qquad (t-a)\frac{E(t)}{t-4} \Bigm| \begin{vmatrix} t f_n & f_m f_{n-m} \\ \delta f_n + t n f_n' & m f_m' f_{n-m} + (n-m) f_m f_{n-m}' \end{vmatrix}$$

if $\varepsilon = 0$.

However, the degree of the determinants on the right hand side in each case does not exceed

$$\deg f_n + \deg f_m + \deg f_{n-m} = n-2 < n-1 = \deg E(t).$$

Hence each divisibility (5) would imply that the relevant determinant is zero, hence either

$$D_1 := \varepsilon f_m f_{n-m} f_n + t m f_m' f_{n-m} f_n + t(n-m) f_m f_{n-m}' f_n - t n f_n' f_m f_{n-m} = 0$$
$$\text{if } \delta = 0,$$

or

$$D_2 := m t f_m' f_{n-m} f_n + (n-m) t f_m f_{n-m}' f_n - \delta f_m f_{n-m} f_n - n t f_m f_{n-m} f_n' = 0$$
$$\text{if } \varepsilon = 0.$$

We calculate the coefficients of t^{n-2} in D_1 and D_2. The coefficient of t^{n-2} in D_1 is

$$\frac{n-m}{2}+\frac{m(m-1)}{2}+\frac{(n-m)(n-m-2)}{2}-\frac{n(n-1)}{2}=m(n-m)$$

if $m \equiv 1 \bmod 2$,

$$\frac{m}{2}+\frac{m(m-2)}{2}+\frac{(n-m)(n-m-1)}{2}-\frac{n(n-1)}{2}=m(n-m)$$

if $m \equiv 0 \bmod 2$.

The coefficient of t^{n-2} in D_2 is

$$\frac{m(m-1)}{2}+\frac{(n-m)(n-m-1)}{2}-\frac{n}{2}-\frac{n(n-2)}{2}=m(n-m).$$

Since $\pi \nmid m(n-m)$, our assumption has led to a contradiction. □

Lemma 5. *If $(n,m)=1$ the polynomial $R_2(x,t)$ is absolutely irreducible.*

Proof. The polynomials $R_2(x,t)$ and $t^{1-\beta}x^{n-2}R_2(tx^{-1},t)$ are simultaneously reducible and since the latter is obtained from the former on replacing m by $n-m$, it is enough to prove the lemma for $2m \leqslant n$.

We note first that the highest homogeneous part of $R_2(x,t)$ equals the ratio of the highest homogeneous part of $T(x,t)$ and of x^2-xt+t, hence equals

$$\frac{t^{[(m-1)/2]}x^n - t^{[n/2]-[m/2]+[(n-1)/2]}x^m}{x^2-tx} = t^{[(m-1)/2]}x^{m-1}\,\frac{x^{n-m}-t^{n-m}}{x-t}.$$

It follows that for $m \leqslant 2$ every factor of $R_2(x,t)$ of degree at most 2 with respect to x is a scalar multiple of

$$\varphi(x,t)=x+a_1t+b_1 \quad \text{or} \quad x^2+(a_2t+b_2)x+(ct^2+dt+e),$$

where if $m=1$, ζ_q is a primitive root of unity of order q

$$a_1=-\zeta_{n-1}^{j} \quad (0<j<n-1) \tag{6}$$

$$a_2=-\zeta_{n-1}^{j_1}-\zeta_{n-1}^{j_2} \quad (0<j_1<j_2<n-1), \quad c=\zeta_{n-1}^{j_1+j_2}. \tag{7}$$

However $\varphi(x,0) \mid R_2(x,0)=x^{n-2}$, hence

$$x+b_1 \mid x^{n-2}, \quad \text{or} \quad x^2+b_2x+e \mid x^{n-2},$$

thus $b_1=b_2=e=0$.

If $x+a_1t \mid R_2(x,t)$ we have $R_2(-a_1t,t)=0$, hence

$$f_m(t)(-a_1t)^n - t^{\alpha}f_n(t)(-a_1t)^m + t^{\beta}f_{n-m}(t)=0 \tag{8}$$

and since $n>\beta$, $f_{n-m}(0)\neq 0$ we have $\alpha+m=\beta$,

$$\left[\frac{n}{2}\right]-\left[\frac{m}{2}\right]+m=\left[\frac{n+m}{2}\right]-\left[\frac{m}{2}\right]; \quad \left[\frac{n}{2}\right]=\left[\frac{n-m}{2}\right];$$

$m=1$, n odd, the coefficient of t^{n-1} on the left hand side of (8) is $-(n-2)a_1+1$, hence $-(n-2)a_1+1=0$, which contradicts (6) for $n>3$.

Consider first the case $2m \leqslant n \leqslant 6$. Since $(m, n) = 1$ we have $m \leqslant 2$. By the above argument $R_2(x, t)$, of degree $n-2$, has no linear factor, hence if it is reducible, $n = 6$, $m = 1$ and $R_2(x, t)$ has a quadratic factor $\varphi = x^2 + a_2 t x + (ct^2 + dt)$. Substituting $t = 1$ we get

$$x^2 + a_2 x + c + d \;\Big|\; \frac{x^6 - 1}{x^2 - x + 1},$$

hence

$$a_2 = 0, 1, 1 - \zeta_3, 1 - \zeta_3^2, \zeta_3, \zeta_3^2,$$

contrary to (7).

Consider now the case $n \geqslant 7$. If $R_2(x, t)$ is the product of two factors of degree r and s with respect to x, where $1 \leqslant r \leqslant s$, then $T(x, t)$ is the product of two factors of degree $r + 2$ and s. If $r \leqslant [n/2] - 2$, we have $2 < r + 2 \leqslant n/2$ and by Lemma 26 of [7], $n = 7$, $m = 1$, $r = 1$, which we already know to be impossible.

If $r = [n/2] - 1$, then $s = n - 2 - r = [(n-1)/2]$ satisfies $2 < s \leqslant n/2$, hence again by Lemma 26 of [7], $n = 7, m = 1, s = 3, r = 2$. Therefore $R_2(x, t)$ has a quadratic factor $\varphi(x, t) = x^2 + a_2 t x + ct^2 + dt$. Substituting $x = 0$ we obtain $ct^2 + dt \mid t^3(t^2 - 4t + 3)$, hence either $d = 0$, or $d = -c$, or $d = -3c$. The case $d = 0$ is excluded, since then $R_2(x, t)$ would have a linear factor $x + t(a_2 + \sqrt{a_2^2 - 4c})/2$. Substituting $t = 3$ we obtain

$$x^2 + 3a_2 x + 9c + 3d \;\Big|\; \frac{x^7 + 3^3 x}{x^2 - 3x + 3} = x \prod_{j=0}^{3} \left(x - \zeta_6^j \sqrt{-3}\right), \quad \zeta_6 = \frac{1 + \sqrt{-3}}{2}.$$

$d = -c$ gives $6c = -3\zeta_6^{j+k}$ $(0 \leqslant j < k \leqslant 3)$, $d = -3c$ gives $3a_2 = -\zeta_6^j \sqrt{-3}$, which both are impossible, since by (7) a_2 and c are algebraic integers. □

Lemma 6. *If $(m, n) = 1$ and t_i $(1 \leqslant i \leqslant [(m-1)/2])$ is a zero of $f_m(t)$, then the algebraic function $x(t)$ given by the equation $R_2(x, t) = 0$ has at $t = t_i$ one $(n-m)$-cycle given by the Puiseux expansions*

$$x(t) = \zeta_{n-m}^j (t - t_i)^{-1/(n-m)} P_{i1}\left(\zeta_{n-m}^{-j} (t - t_i)^{1/(n-m)}\right)$$

and the remaining expansions

$$x(t) = P_{ij}(t - t_i) \quad (j = 2, \ldots, m-1),$$

where P_{ij} are ordinary formal power series with $P_{ij}(0) \neq 0$ $(j = 1, \ldots, m-1)$.

Proof is standard. One uses the fact that $(f_m, t f_m' f_n f_{n-m}) = 1$. □

Lemma 7. *If $(m, n) = 1$ and t_i $([(m-1)/2] < i \leqslant [(m-1)/2] + [(n-m-1)/2])$ is a zero of $f_{n-m}(t)$, then the algebraic function $x(t)$ has at $t = t_i$ one m-cycle given by the Puiseux expansions*

$$x(t) = \zeta_m^j (t - t_i)^{1/m} P_{i1}\left(\zeta_m^j (t - t_i)^{1/m}\right)$$

and the remaining expansions

$$x(t) = P_{ij}(t - t_i) \quad (j = 2, \dots, n - m - 1),$$

where P_{ij} are ordinary formal power series with $P_{ij}(0) \neq 0$.

Proof is standard. One uses the fact that $(f_{n-m}, tf'_{n-m} f_m f_n) = 1$. □

Lemma 8. *If $(m, n) = 1$, the algebraic function $x(t)$ has at $t = 0$*

one m-cycle and $(n - m - 2)/2$ two-cycles,	*if $n \equiv m \equiv 1 \bmod 2$,*
one $(n - m)$-cycle and $(m - 2)/2$ two-cycles,	*if $n \equiv 1$, $m \equiv 0 \bmod 2$,*
$(n/2) - 1$ two-cycles,	*if $n \equiv 0$, $m \equiv 1 \bmod 2$.*

They are given by the following Puiseux expansions.

If $n \equiv m \equiv 1 \bmod 2$

$$x(t) = \zeta_m^j t^{(m+1)/2m} P_{01}^{1,1}(\zeta_m^{2j} t^{1/m}) \quad (0 \leqslant j < m),$$
$$x(t) = \pm t^{1/2} P_{0j}^{1,1}(\pm t^{1/2}) \quad (1 < j \leqslant (n - m)/2);$$

if $n \equiv 1$, $m \equiv 0 \bmod 2$

$$x(t) = \zeta_{n-m}^j t^{(n-m-1)/2(n-m)} P_{01}^{1,0}(\zeta_{n-m}^{-2j} t^{1/(n-m)}) \quad (0 \leqslant j < n - m),$$
$$x(t) = \pm t^{1/2} P_{0j}^{1,0}(\pm t^{1/2}) \quad (1 < j \leqslant m/2);$$

if $n \equiv 0$, $m \equiv 1 \bmod 2$

$$x(t) = \pm t^{1/2} P_{0j}^{0,1}(\pm t^{1/2}) \quad (1 \leqslant j \leqslant n/2 - 1),$$

where $P_{0j}^{\rho,\sigma}$ are ordinary formal power series with $P_{0j}^{\rho,\sigma}(0) \neq 0$.

Proof is standard using the fact that $f_m(0) f_n(0) f_{n-m}(0) \neq 0$. □

Lemma 9. *If $(n, m) = 1$ the algebraic function $x(t)$ has at $t = \infty$ no branching and the Puiseux expansions are given by*

$$x(t) = t P_{\infty j}(t^{-1}) \quad (1 \leqslant j < n - m),$$
$$x(t) = P_{\infty j}(t^{-1}) \quad (n - m \leqslant j \leqslant n - 2),$$

where $P_{\infty j}$ are ordinary formal power series with $P_{\infty j}(0) \neq 0$.

Proof is standard. □

Lemma 10. *If $(n, m) = 1$ the discriminant d of the field $\overline{K}(t, x(t))$ equals the numerator of*

$$t^{\zeta} f_m^{n-m-1} f_{n-m}^{m-1} D(t),$$

where

$$\zeta = \begin{cases} (n+m-4)/2 & \text{if } n \equiv m \equiv 1 \bmod 2, \\ (2n-m-4)/2 & \text{if } n \equiv 1,\ m \equiv 0 \bmod 2, \\ (n-2)/2 & \text{if } n \equiv 0,\ m \equiv 1 \bmod 2. \end{cases} \tag{9}$$

Proof. Let $\theta = f_m x(t)$. The element θ of $K(t, x(t))$ is a zero of the polynomial $f_m^{n-1} T(x/f_m, t)$ monic with respect to x, hence θ is t-integral.

The discriminant of θ,

$$d(\theta) = f_m^{(n-3)(n-4)} \operatorname{disc}_x R_2(x, t)$$

and by a well known theorem (see [2], p. 464).

t-discriminant of $\overline{K}(x(t), t)$ differs from $d(\theta)$ by a square factor. In view of Lemma 4 we have

t-discriminant of $\overline{K}(x(t), t) = t^{\zeta} f_m^{\vartheta} f_{n-m}^{\iota} D(t)$.

The exponents ζ, ϑ, ι can be read off from Lemmas 6, 7, 8 together with Dedekind's theorem for discriminants (see [2], p. 463). By the same theorem and Lemma 9 the denominator of t does not contribute anything to the discriminant of $\overline{K}(t, x(t))$. □

Lemma 11. *If $(m, n) = 1$ for each zero τ of $D(t)$ the algebraic function $x(t)$ has at $t = \tau$ one two-cycle given by the Puiseux expansion*

$$x(t) = \xi_{\tau 1} + \left(\pm(t-\tau)^{1/2}\right)^{p_\tau} P_{\tau 1}\left(\pm(t-\tau)^{1/2}\right)$$

and the remaining expansions

$$x(t) = P_{ij}(t-\tau) \qquad (1 < j \leqslant n-3),$$

where $\xi_{\tau 1} \neq 0$, p_τ is a positive integer and $P_{\tau 1}$ are ordinary formal power series with $P_{\tau 1}(0) \neq 0$. Moreover, $(t-\tau)^{p_\tau/2} P_{\tau 1}\left((t-\tau)^{1/2}\right) \notin \overline{K}\left((t-\tau)\right)$.

Proof. Since $(f_n,\ f_m f_{n-m}) = 1$ we have $(D,\ f_m f_{n-m} f_n) = 1$ hence, by Lemmas 4 and 10, each factor $t - \tau$, where $D(\tau) = 0$, occurs exactly once in the discriminant d of the field $\overline{K}(t, x(t))$. It follows by Dedekind's theorem that $t - \tau$ has in the above field exactly one factor in the second power and all the other factors are simple. Therefore by Lemma 1(a) of [7] the algebraic function $x(t)$ has at $t = \tau$ one two-cycle given by the Puiseux expansion

$$x(t) = L_{\tau 1}\left((t-\tau)^{1/2}\right)$$

and the remaining expansions

$$x(t) = L_{\tau j}(t-\tau) \qquad (1 < j \leqslant n-3),$$

where $L_{\tau j}$ are ordinary formal Laurent series with

$$L_{\tau 1}\left((t-\tau)^{1/2}\right) \notin \overline{K}\left((t-\tau)\right).$$

However

$$\tau f_m(\tau) f_{n-m}(\tau) \neq 0 \quad \text{and} \quad T\left(x(t), t\right) = 0,$$

hence $L_{\tau j}$ do not contain negative powers of the variable and their constant term is non-zero. □

Lemma 12. *If* $(m, n) = 1$ *and* $\min\{m, n-m\} \leqslant 2$ *the extension* $\overline{K}\big(t, x(t)\big)/\overline{K}(t)$ *is primitive.*

Proof. Suppose that there exists a field L such that $\overline{K}(t) \subset L \subset \overline{K}(t, x(t))$ and $\big[\overline{K}(t, x(t)) : L\big] = r$ satisfies $1 < r < n-2$. Let d_L be the discriminant of L. By the composition theorem for discriminants ([2], p. 443) we have $d_L \mid d$. However, by Lemma 10, if $(m, n) = 1$ and $\min\{m, n-m\} \leqslant 2$ the only non-separable unitary divisor of d is t^{ζ}, hence

$$d_L^r \mid t^{\zeta} \text{ and } r \deg d_L \leqslant \zeta.$$

On the other hand,

$$\deg d_L \geqslant 2\Big(\frac{n-2}{r} - 1\Big) \quad \text{(see [2], p. 627),}$$

hence

$$2(n-2-r) \leqslant \zeta.$$

Since $r \mid n-2$ we have $r \leqslant (n-2)/2$ and we obtain

$$n - 2 \leqslant \zeta$$

which contradicts (9). □

Lemma 13. *If* $(m, n) = 1$ *the monodromy group of* $R_2(x, t) = 0$ *is the symmetric group* S_{n-2}.

Proof. By Lemma 5 group G in question is transitive hence it is S_{n-2} for $n \leqslant 4$. If $n > 4$ by Lemma 2(c) of [7] G contains a transposition, since, by Lemma 4, D has at least one zero and Lemma 11 applies.

Therefore (see [9], Ch. I, Theorem 14) G is symmetric if and only if it is primitive. If $\min\{m, n-m\} \leqslant 2$ primitivity follows from Lemma 12. If $\min\{m, n-m\} > 2$ assume that G is imprimitive with blocks of imprimitivity of length b. Then by Lemma 1 of [8] and by Lemmas 6, 7 we have $b \mid \max\{m, n-m\}$, but $b \mid n-2$, hence $b \mid \min\{m, n-m\} - 2$, $b < \min\{m, n-m\}$ and, again by the same argument, $b \mid \min\{m, n-m\}$. Thus $b \mid (m, n-m)$ and since $(m, n-m) = 1$, $b = 1$. □

Definition 1. Let $(m, n) = 1$, $R_2(x, t) = \prod_{i=1}^{n-2} \big(x - x_i(t)\big)$. We set

$$L_2(k, m, n) = K\big(t, \tau_1(x_1, \ldots, x_k), \ldots, \tau_k(x_1, \ldots, x_k)\big),$$
$$L_2^*(k, m, n) = \overline{K}\big(t, \tau_1(x_1, \ldots, x_k), \ldots, \tau_k(x_1, \ldots, x_k)\big),$$

where τ_j is the j-th fundamental symmetric function.

Remark. By Lemma 13 the fields $L_2(k,m,n)$ and $L_2^*(k,m,n)$ are determined by k,m,n up to an isomorphism fixing $K(t)$ and $\overline{K}(t)$, respectively.

Lemma 14. *If* $(n,m)=1$, $D(\tau)=0$ *the numerator of* $t-\tau$ *in* $L_2^*(k,m,n)$ *has* $\binom{n-4}{k-1}$ *prime divisors in the second power and none in the higher ones.*

Proof. Given Lemma 11 the proof is analogous to the proof of Lemma 5 in [7]. □

Lemma 15. *If* $n \geqslant 5$, $(m,n)=1$, $n-2 \geqslant 2k$ *then either the genus* $g_2^*(k,m,n)$ *of* $L_2^*(k,m,n)$ *satisfies*

$$g_2^*(k,m,n) > \frac{5n}{24}, \quad \text{or} \quad n \leqslant 6.$$

Moreover, $g_2^*(k,m,n)=0$ *implies* $n=5$.

Proof. It follows from Lemma 2(a) of [7] and from Lemmas 4 and 14 that

$$g_2^*(k,m,n) \geqslant \frac{1}{2}\binom{n-4}{k-1}\binom{n-2}{2} - \binom{n-2}{k} + 1 = \binom{n-2}{k}\left(\frac{k(n-k-2)}{4} - 1\right) + 1.$$

For $k \geqslant 2$ and $n \geqslant 2k+2$ we obtain

$$g_2^*(k,m,n) \geqslant \binom{2k}{k}\left(\frac{k(n-2)}{8} - 1\right) + 1 \geqslant 6 \cdot \frac{n-6}{4} + 1 > \frac{5n}{24}, \quad \text{or} \quad n \leqslant 6.$$

For $k=1$ we find from Lemma 2(a) of [7] and Lemmas 4, 8 and 11 that

$$\begin{aligned} g_2^*(k,m,n) &\geqslant \frac{1}{2}\binom{n-2}{2} + \frac{1}{2}\zeta - (n-2) + 1 \\ &\geqslant \frac{1}{2}\binom{n-2}{2} + \frac{[n/2]-1}{2} - (n-2) + 1 > \frac{5n}{24}, \quad \text{or} \quad n \leqslant 6. \end{aligned}$$

For $n=6$ we obtain from the above inequalities $g_2^*(k,m,n) \geqslant 1$, which proves the last statement of the lemma. □

Lemma 16. *Let* $(m,n)=1$,

$$R_2(x,t) = \prod_{i=1}^{n-2}\bigl(x - x_i(t)\bigr).$$

In the field $\overline{K}\bigl(t, x_1(t), x_2(t)\bigr)$ *for each zero* t_i *of* f_m *we have the factorization*

$$t - t_i \cong \frac{\prod_{h=1}^{n-m-1} \mathfrak{p}_{ih}^{n-m} \prod_{j=1}^{m-2} \mathfrak{q}_{ij}^{n-m} \prod_{j=1}^{m-2} \mathfrak{r}_{ij}^{n-m} \prod_{k=1}^{(m-2)(m-3)} \mathfrak{s}_{ik}}{\prod_{h=1}^{(n-m-1)(n-m-2)} \mathfrak{t}_h \cdot \prod_{j=1}^{(n-m-1)(m-1)} \mathfrak{u}_j \cdot \prod_{j=1}^{(n-m-1)(m-1)} \mathfrak{v}_j \cdot \prod_{k=1}^{(m-1)(m-2)} \mathfrak{w}_k}$$

$$\left(i \leqslant \left[\frac{m-1}{2}\right]\right)$$

and for each zero t_i of f_{n-m} we have the factorization

$$t - t_i \cong \frac{\prod_{h=1}^{m-1} \mathfrak{p}_{ih}^{m} \prod_{j=1}^{n-m-2} \mathfrak{q}_{ij}^{m} \prod_{j=1}^{n-m-2} \mathfrak{r}_{ij}^{m} \prod_{k=1}^{(n-m-2)(n-m-3)} \mathfrak{s}_{ik}}{\prod_{h=1}^{(n-m-1)(n-m-2)} \mathfrak{t}_h \cdot \prod_{j=1}^{(n-m-1)(m-1)} \mathfrak{u}_j \cdot \prod_{j=1}^{(n-m-1)(m-1)} \mathfrak{v}_j \cdot \prod_{k=1}^{(m-1)(m-2)} \mathfrak{w}_k}$$
$$\left(\left[\frac{m-1}{2}\right] < i \leqslant \left[\frac{m-1}{2}\right] + \left[\frac{n-m-1}{2}\right]\right).$$

Besides

$$t \cong \frac{\prod_{\mathfrak{p}\,|\,t} \mathfrak{p}^{\nu(\mathfrak{p})}}{\prod_{h=1}^{(n-m-1)(n-m-2)} \mathfrak{t}_h \cdot \prod_{j=1}^{(n-m-1)(m-1)} \mathfrak{u}_j \cdot \prod_{j=1}^{(n-m-1)(m-1)} \mathfrak{v}_j \cdot \prod_{k=1}^{(m-1)(m-2)} \mathfrak{w}_k},$$

$$x_1(t) \cong \frac{\prod_{i=[(m-1)/2]+1}^{[(m-1)/2]+[(n-m-1)/2]} \left(\prod_{h=1}^{m-1} \mathfrak{p}_{ih} \cdot \prod_{j=1}^{n-m-2} \mathfrak{q}_{ij}\right) \prod_{\mathfrak{p}\,|\,t} \mathfrak{p}^{\nu_1(\mathfrak{p})}}{\prod_{i=1}^{[(m-1)/2]} \left(\prod_{h=1}^{n-m-1} \mathfrak{p}_{ih} \cdot \prod_{j=1}^{m-2} \mathfrak{q}_{ij}\right) \prod_{h=1}^{(n-m-1)(n-m-2)} \mathfrak{t}_h \cdot \prod_{j=1}^{(n-m-1)(m-1)} \mathfrak{u}_j},$$

$$x_2(t) \cong \frac{\prod_{i=[(m-1)/2]+1}^{[(m-1)/2]+[(n-m-1)/2]} \left(\prod_{h=1}^{m-1} \mathfrak{p}_{ih} \cdot \prod_{j=1}^{n-m-2} \mathfrak{r}_{ij}\right) \prod_{\mathfrak{p}\,|\,t} \mathfrak{p}^{\nu_2(\mathfrak{p})}}{\prod_{i=1}^{[(m-1)/2]} \left(\prod_{h=1}^{n-m-1} \mathfrak{p}_{ih} \cdot \prod_{j=1}^{m-2} \mathfrak{r}_{ij}\right) \prod_{h=1}^{(n-m-1)(n-m-2)} \mathfrak{t}_h \cdot \prod_{j=1}^{(n-m-1)(m-1)} \mathfrak{v}_j}.$$

Here $\mathfrak{p}$, $\mathfrak{p}_{ih}$, $\mathfrak{q}_{ij}$, $\mathfrak{r}_{ij}$, $\mathfrak{s}_{ik}$, $\mathfrak{t}_h$, $\mathfrak{u}_j$, $\mathfrak{w}_k$ are prime divisors, $\nu(\mathfrak{p}) = \operatorname{ord}_{\mathfrak{p}} t$, $\nu_1(\mathfrak{p}) = \operatorname{ord}_{\mathfrak{p}} x_1(t)$, $\nu_2(\mathfrak{p}) = \operatorname{ord}_{\mathfrak{p}} x_2(t)$ are nonnegative integers.

If $D(\tau) = 0$, $t - \tau$ has in the field $\overline{K}\big(t, x_1(t), x_2(t)\big)$ exactly $(n-4)(n-5)$ simple factors, the remaining factors are double.

Proof is analogous to the proof of Lemma 10 in [8]. □

Lemma 17. *If $(m, n) = 1$, $\kappa = \begin{cases} \beta + n - 3 & \text{if } m = 2, \\ \beta - 1 & \text{otherwise,} \end{cases}$ then for all primes p*

$$\sqrt[p]{\frac{t^{\kappa} f_{n-m}(t)}{f_m(t)}} \notin \overline{K}\big(t, x_1(t), \ldots, x_{n-2}(t)\big) =: \Omega.$$

Proof. By Lemma 1(a)(b) of [7] the prime divisors of the numerator or the denominator of $t - c$ in Ω are in one-to-one corespondence with the cycles of the Puiseux expansions of a generating element of $\Omega/\overline{K}(t)$ at $t = c$ or $t = \infty$, respectively, provided the lengths of

the cycles are not divisible by π. For the generating element we take $y(t) = \sum_{i=1}^{n-2} a^i x_i(t)$, where a is chosen in $\overline{K}$ so that for every permutation $\sigma(i)$ of $\{1, \dots, n-2\}$ different from the identity we have $y(t) \neq \sum_{i=1}^{n-2} a^i x_{\sigma(i)}(t)$. By Lemma 13 for each permutation σ there is an automorphism of the extension $\Omega/\overline{K}(t)$ taking x_i in $x_{\sigma(i)}$ $(1 \leqslant i \leqslant n-2)$. By Lemma 6 at $t = t_i$ $(1 \leqslant i \leqslant [(m-1)/2])$ we obtain for $y(t)$ the expansions

$$\sum_{j=1}^{n-m} a^{\sigma(j)} \zeta_{n-m}^{j-1} (t-t_i)^{-1/(n-m)} P_{i1}\big(\zeta_{n-m}^{1-j}(t-t_i)^{1/(n-m)}\big) + \sum_{j=n-m+1}^{n-2} a^{\sigma(j)} P_{i,\,j-n+m+1}(t-t_i),$$

where σ runs through all permutations of $\{1, \dots, n-2\}$. They split into $H = (n-2)!/(n-m)$ cycles of length $n-m$.

By Lemma 9 at $t = \infty$ we obtain for $y(t)$ the $(n-2)!$ expansions

$$\sum_{j=1}^{n-m-1} a^{\sigma(j)} \zeta_{n-m}^{j} P_{\infty 1}\big(\zeta_{n-m}^{-j} t^{-1}\big) + \sum_{j=n-m}^{n-2} a^{\sigma(j)} P_{\infty,\,j-n+m+2}(t^{-1}),$$

which do not split into any cycles of length greater than 1. Therefore,

$$t - t_i \cong \frac{\prod_{h=1}^{H} \mathfrak{P}_{ih}^{n-m}}{\prod_{k=1}^{(n-2)!} \mathfrak{Q}_k} \qquad \left(1 \leqslant i \leqslant \left[\frac{m-1}{2}\right]\right),$$

where $\mathfrak{P}_{ih}, \mathfrak{Q}_k$ are prime divisors of Ω.

Similarly, if $[(m-1)/2] < i \leqslant [(m-1)/2] + [(n-m-1)/2]$ we obtain in Ω the factorization

$$t - t_i \cong \frac{\prod_{j=1}^{J} \mathfrak{P}_{ij}^{m}}{\prod_{k=1}^{(n-2)!} \mathfrak{Q}_k} \qquad \left(\left[\frac{m-1}{2}\right] < i \leqslant \left[\frac{m-1}{2}\right] + \left[\frac{n+m-1}{2}\right]\right),$$

where $\mathfrak{P}_{ij}$ are prime divisors of Ω and $J = (n-2)!/m$.

Finally,

$$t \cong \frac{\prod_{\mathfrak{P}\,|\,t} \mathfrak{P}^{\nu(\mathfrak{P})}}{\prod_{k=1}^{(n-2)!} \mathfrak{Q}_k},$$

where $\nu(\mathfrak{P}) = \operatorname{ord}_{\mathfrak{P}} t$ is a positive integer.

It follows hence that

$$\frac{t^{\kappa} f_{n-m}(t)}{f_m(t)} \cong \frac{\prod\limits_{\mathfrak{P}\mid t} \mathfrak{P}^{\kappa \nu(\mathfrak{P})} \prod\limits_{i=[(m-1)/2]+1}^{[(m-1)/2]+[(n-m-1)/2]} \prod\limits_{j=1}^{J} \mathfrak{P}_{ij}^{m}}{\prod\limits_{k=1}^{(n-2)!} \Omega_k^{\kappa+[(n-m-1)/2]-[(m-1)/2]} \prod\limits_{i=1}^{[(m-1)/2]} \prod\limits_{h=1}^{H} \mathfrak{P}_{ih}^{n-m}}.$$

Now $\kappa+[(n-m-1)/2]-[(m-1)/2] = 2n-5$, if $m = 2$ and $n-m-1$, otherwise. Since $(n-m-1, n-m) = 1$, if $[(m-1)/2] \geqslant 1$ the denominator of the fraction in question is not a p-th power. If $[(m-1)/2] = 0$ and $m = 1$, $n \geqslant 4$ we have $[(n-m-1)/2] \geqslant 1$, the numerator contains simple factors and the fraction again is not a p-th power. There remain the cases $n = 3$ and $m = 2$, n odd > 3. In the former case

$$\frac{t^{\kappa} f_{n-m}(t)}{f_m(t)} = t$$

clearly is not a p-th power in $\Omega = \overline{K}(t)$.

In the latter case the numerator of the fraction in question contains prime divisors in the second power, while the denominator in the odd power $2n-5$, hence the fraction is not a p-th power. □

Lemma 18. *Let $(m, n) = 1$, $n \geqslant 4$. For every positive integer $q \not\equiv 0 \bmod \pi$ and for every choice of q-th roots we have*

$$\left[\overline{K}\left(t, \sqrt[q]{t^{\lambda} x_1(t)}, \ldots, \sqrt[q]{t^{\lambda} x_{n-2}(t)}\right) : \overline{K}\left(t, x_1(t), \ldots, x_{n-2}(t)\right)\right] = q^{n-2},$$

where

$$\lambda = \begin{cases} 1 & \text{if } m = 2, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. By Theorem 1 of [6] it is enough to prove that for every prime $p \mid q$

$$\prod_{j=1}^{n-2} \left(t^{\lambda} x_j\right)^{\alpha_j} = \omega^p, \quad \omega \in \Omega = \overline{K}\left(t, x_1(t), \ldots, x_{n-2}(t)\right) \tag{10}$$

implies $\alpha_j \equiv 0 \bmod p$ for all $j \leqslant n-2$. Assume that (10) holds, but say, $\alpha_1 \not\equiv 0 \bmod p$.

If for all j we have $\alpha_j \equiv \alpha_1 \bmod p$, it follows from (10) that

$$\left(\prod_{j=1}^{n-2} t^{\lambda} x_j\right)^{\alpha_1} = \omega_1^p, \quad \omega_1 \in \Omega$$

and since $\alpha_1 \not\equiv 0 \bmod p$

$$\prod_{j=1}^{n-2} t^{\lambda} x_j = (-1)^{n-2} t^{\lambda(n-2)} \frac{t^{\beta-1} f_{n-m}(t)}{f_m(t)} = (-1)^{n-2} \frac{t^{\kappa} f_{n-m}(t)}{f_m(t)}$$

we obtain

$$\sqrt[p]{\frac{t^{\kappa} f_{n-m}(t)}{f_m(t)}} \in \Omega,$$

contrary to Lemma 17.

Therefore, there exists an $i \leqslant n-2$ such that $\alpha_i \not\equiv \alpha_1 \bmod p$. Changing, if necessary, the numeration of the x_j we may assume that $i = 2$. By Lemma 13 there exists an automorphism σ of Ω stable on $\overline{K}(t)$ such that

$$\sigma(x_1) = x_2,\ \sigma(x_2) = x_1,\ \sigma(x_i) = x_i \quad (i \neq 1, 2).$$

Applying σ to both sides of (10) we obtain

$$\left(t^{\lambda} x_1\right)^{\alpha_2} \left(t^{\lambda} x_2\right)^{\alpha_1} \prod_{j=3}^{n-2} \left(t^{\lambda} x_j\right)^{\alpha_j} = (\omega^{\sigma})^p,$$

hence on division

$$\left(\frac{x_1}{x_2}\right)^{\alpha_1 - \alpha_2} = \left(\frac{\omega}{\omega^{\sigma}}\right)^p.$$

Since $\alpha_1 - \alpha_2 \not\equiv 0 \bmod p$ it follows that

$$\frac{x_1}{x_2} = \omega_2^p, \quad \omega_2 \in \Omega. \tag{11}$$

The extension $\overline{K}(t, x_1, x_2, \omega_2)/\overline{K}(t, x_1, x_2)$ is a normal subextension of $\Omega/\overline{K}(t, x_1, x_2)$ of degree 1 or p and since, by Lemma 13, the latter has the symmetric Galois group, we have either

$$\omega_2 \in \overline{K}(t, x_1, x_2)$$

or $p = 2$ and

$$\omega_2 \in \overline{K}\Big(t, x_1, x_2, \prod_{\substack{\mu,\nu=3 \\ \nu>\mu}}^{n-2} (x_\nu - x_\mu)\Big) \setminus \overline{K}(t, x_1, x_2).$$

In the former case we compare the divisors on both sides of (11) and obtain by Lemma 16,

$$(\omega_2)^p = \frac{\left(\prod_{i=1}^{\left[\frac{m-1}{2}\right]} \prod_{j=1}^{m-2} \mathfrak{r}_{ij}\right) \left(\prod_{i=\left[\frac{m-1}{2}\right]+1}^{\left[\frac{m-1}{2}\right]+\left[\frac{n-m-1}{2}\right]} \prod_{j=1}^{n-m-2} \mathfrak{q}_{ij}\right)^{(n-m-1)(m-1)} \prod_{j=1} \mathfrak{v}_j}{\left(\prod_{i=1}^{\left[\frac{m-1}{2}\right]} \prod_{j=1}^{m-2} \mathfrak{q}_{ij}\right) \left(\prod_{i=\left[\frac{m-1}{2}\right]+1}^{\left[\frac{m-1}{2}\right]+\left[\frac{n-m-1}{2}\right]} \prod_{j=1}^{n-m-2} \mathfrak{r}_{ij}\right)^{(n-m-1)(n-m-2)} \prod_{j=1} \mathfrak{u}_j} \times \prod_{\mathfrak{p} \mid t} \mathfrak{p}^{\nu_1(\mathfrak{p}) - \nu_2(\mathfrak{p})},$$

a contradiction, since for $n \geqslant 4$, $(m, n) = 1$ we have

$$\text{either} \quad \left[\frac{m-1}{2}\right](m-2) > 0 \quad \text{or} \quad \left[\frac{n-m-1}{2}\right](n-m-2) > 0.$$

In the latter case, since the conjugates of ω_2 with respect to $\overline{K}(t, x_1, x_2)$ are $\pm\omega_2$ we have

$$\omega_2 = \omega_3 \prod_{\substack{\mu,\nu=3 \\ \nu>\mu}}^{n-2} (x_\nu - x_\mu), \quad \omega_3 \in \overline{K}(t, x_1, x_2),$$

hence

$$\omega_2 = \omega_3 \prod_{\substack{\mu,\nu=1 \\ \nu>\mu}}^{n-2} (x_\nu - x_\mu) \cdot \frac{x_1 - x_2}{\prod_{\nu\neq 1}(x_\nu - x_1) \cdot \prod_{\nu\neq 2}(x_\nu - x_2)} = \omega_4 \prod_{\substack{\mu,\nu=1 \\ \nu>\mu}}^{n-2} (x_\nu - x_\mu),$$

where $\omega_4 \in \overline{K}(t, x_1, x_2)$. It follows by (11) and by Lemma 3 that

$$\frac{x_1}{x_2} = \omega_4^2 \operatorname{disc}_x R_2(x, t) = (-1)^{n(n-1)/2} \omega_4^2 t^\gamma f_m^{n-m-1} f_{n-m}^{m-1} D(t).$$

For $n \geqslant 6$ the polynomial $D(t)$ has at least one zero τ and, by Lemma 16, $t - \tau$ has at least one simple factor in $\overline{K}(t, x_1, x_2)$, hence we have on the right hand side a factor which does not occur on the left, a contradiction. On the other hand, for $n = 4$ or 5 the prime divisor $\mathfrak{q}_{11}$ enters the left hand side with the exponent ± 1, while the right hand side with an even exponent. □

Lemma 19. *Let $n \geqslant 4$, $(m, n) = 1$, $q \not\equiv 0 \bmod \pi$, $q \geqslant 2$ and $y_{iq}^q = x_i(t)$ $(1 \leqslant i \leqslant n-2)$. Then*

$$\left[K\left(t, \left(\sum_{i=1}^{n-2} y_{iq}\right)^q\right) : K(t)\right] = q^{n-3}.$$

Proof. By Lemma 13 and 18 all embeddings of $K\left(t, t^{\lambda/q} y_{1q}, \ldots, t^{\lambda/q} y_{n-2,q}\right)$ into $\overline{K(t)}$ stable on $\overline{K}(t)$ are given by

$$t^{\lambda/q} y_{iq} \mapsto \zeta_q^{\alpha_i} t^{\lambda/q} y_{\sigma(i)q} \quad (1 \leqslant i \leqslant n-2), \tag{12}$$

where σ is a permutation of $\{1, 2, \ldots, n-2\}$ and

$$\langle \alpha_1, \ldots, \alpha_{n-2} \rangle \in (\mathbb{Z}/q\mathbb{Z})^{n-2}. \tag{13}$$

We shall show that there are exactly q^{n-3} distinct images of $\left(\sum_{i=1}^{n-2} y_{iq}\right)^q$ under transformations (12). Indeed, if we apply (12) with $\sigma(i) = i$ to

$$\left(\sum_{i=1}^{n-2} y_{iq}\right)^q = t^{-\lambda}\left(\sum_{i=1}^{n-2} t^{\lambda/q} y_{iq}\right)^q \tag{14}$$

we obtain

$$t^{-\lambda}\Big(\sum_{i=1}^{n-2}\zeta_q^{\alpha_i}t^{\lambda/q}y_{iq}\Big)^q.$$

If this were equal to $t^{-\lambda}\Big(\sum\limits_{i=1}^{n-2}\zeta_q^{\beta_i}t^{\lambda/q}y_{iq}\Big)^q$ for a vector $\langle\beta_1,\dots,\beta_{n-2}\rangle\in(\mathbb{Z}/q\mathbb{Z})^{n-2}$ with $\beta_j-\beta_1\neq\alpha_j-\alpha_1$ for a certain j we should obtain

$$t^{\lambda/q}y_{1q}\in\overline{K}\big(t^{\lambda/q}y_{2q},\dots,t^{\lambda/q}y_{n-2,q}\big),$$

or

$$t^{\lambda/q}y_{jq}\in\overline{K}\big(t^{\lambda/q}y_{1q},\dots,t^{\lambda/q}y_{j-1,q},t^{\lambda/q}y_{j+1,q},\dots,t^{\lambda/q}y_{n-2,q}\big).$$

The obtained contradiction with Lemma 18 shows that the number of distinct images is at least equal to the number of vectors satisfying (13) with $\alpha_1=0$, thus to q^{n-3}. On the other hand by (14) $\Big(\sum\limits_{i=1}^{n-2}y_{iq}\Big)^q$ is invariant under transformations (12) with $\alpha_1=\alpha_2=\dots$ $\dots=\alpha_{n-2}$, which form a group of order $q(n-2)!$, hence the number in question does not exceed q^{n-3}. Therefore

$$\Big[\overline{K}\Big(t,\Big(\sum_{i=1}^{n-2}y_{iq}\Big)^q\Big):\overline{K}(t)\Big]=q^{n-3}. \qquad \square$$

Definition 2. Let $(m,n)=1$, $q\not\equiv 0 \bmod \pi$ and $y_{iq}^q=x_i(t)$, where $x_i(t)$ are defined in Definition 1. We set

$$M_2(m,n,q)=K\Big(t,\Big(\sum_{i=1}^{n-2}y_{iq}\Big)^q\Big),\quad M_{2*}(m,n,q)=\overline{K}\Big(t,\Big(\sum_{i=1}^{n-2}y_{iq}\Big)^q\Big).$$

Remark. By Lemma 19 for $n\geqslant 4$, $(m,n)=1$, $M_2(m,n,q)$ and $M_{2*}(m,n,q)$ are determined by m,n,q up to an isomorphism which fixes $K(t)$ and $\overline{K}(t)$, respectively.

Lemma 20. *For $n>4$, $(m,n)=1$ and $D(\tau)=0$ the numerator of $t-\tau$ in $M_{2*}(m,n,q)$ has $(q^{n-3}-q^{n-4})/2$ factors in the second power.*

Proof. Let us put for each zero τ of D in the notation of Lemma 11

$$y_{\tau 1q}=\xi_\tau^{1/q}\sum_{k=0}^{\infty}\binom{1/q}{k}\xi^{-k/q}(t-\tau)^{p_\tau k/2}P_{\tau 1}\big((t-\tau)^{1/2}\big)^k$$

$$y_{\tau 2q}=\xi_\tau^{1/q}\sum_{k=0}^{\infty}(-1)^{p_\tau k}\binom{1/q}{k}\xi^{-k/q}(t-\tau)^{p_\tau k/2}P_{\tau 1}\big(-(t-\tau)^{1/2}\big)^k,$$

so that for $j = 1, 2$

$$y_{\tau jq}^{q} = \xi_\tau (-1)^{p_\tau (j-1)} (t-\tau)^{p_\tau /2} P_{\tau 1}\big((-1)^{j-1}(t-\tau)^{1/2}\big),$$

$$y_{\tau jq} \notin \overline{K}\big((t-\tau)\big), \tag{15}$$

$$y_{\tau 1q} + y_{\tau 2q} \in \overline{K}\big((t-\tau)\big), \tag{16}$$

$$(y_{\tau 1q} - y_{\tau 2q})(t-\tau)^{1/2} \in \overline{K}\big((t-\tau)\big) \tag{17}$$

and choose in an arbitrary way

$$y_{\tau jq} = \big(P_{\tau, j-1}(t-\tau)\big)^{1/q} \in \overline{K}\big((t-\tau)\big) \quad (2 < j \leqslant n-2). \tag{18}$$

It follows from Lemma 11 that over the field $\overline{K}\big((t-\tau)\big)$

$$\prod_{j=1}^{n-2}\prod_{\alpha=0}^{n-1}\Big(x - \zeta_q^\alpha y_{jq}\Big) = R_2(x^q, t)\prod_{j=1}^{n-2}\prod_{\alpha=0}^{n-1}\Big(x - \zeta_q^\alpha y_{\tau jq}\Big),$$

thus the symmetric polynomials of $\zeta_q^\alpha y_{jq}$ $(1 \leqslant j \leqslant n-2, 0 \leqslant \alpha < q)$ and of $\zeta_q^\alpha y_{\tau jq}$ are the same. Hence

$$\prod_{\alpha_2=0}^{q-1}\cdots\prod_{\alpha_{n-2}=0}^{q-1}\Big(x - \Big(y_{1q} + \sum_{j=2}^{n-2}\zeta_q^{\alpha_j} y_{jq}\Big)^q\Big) = \prod_{\alpha_2=0}^{q-1}\cdots\prod_{\alpha_{n-2}=0}^{q-1}\Big(x - \Big(y_{\tau 1q} + \sum_{j=2}^{n-2}\zeta_q^{\alpha_j} y_{\tau jq}\Big)^q\Big),$$

which means that $\Big(\sum\limits_{j=1}^{n-2} y_{jq}\Big)^q$ has the following Puiseux expansions at $t = \tau$

$$\Big(y_{\tau 1q} + \zeta_q^{\alpha_2} y_{\tau 2q} + \sum_{j=3}^{n-2}\zeta_q^{\alpha_j} y_{\tau jq}\Big)^q, \quad \langle \alpha_2, \ldots, \alpha_{n-2}\rangle \in (\mathbb{Z}/q\mathbb{Z})^{n-3}.$$

If such an expansion belongs to $\overline{K}\big((t-\tau)\big)$, then either

$$y_{\tau 1q} + \zeta_q^{\alpha_2} y_{\tau 2q} + \sum_{j=3}^{n-2}\zeta_q^{\alpha_j} y_{\tau jq} \in \overline{K}\big((t-\tau)\big),$$

or $2 \,|\, q$ and

$$\Big(y_{\tau 1q} + \zeta_q^{\alpha_2} y_{\tau 2q} + \sum_{j=3}^{n-2}\zeta_q^{\alpha_j} y_{\tau jq}\Big)(t-\tau)^{1/2} \in \overline{K}\big((t-\tau)\big).$$

In the former case, by (16) and (18),

$$(1 - \zeta_q^{\alpha_2}) y_{\tau 1q} \in \overline{K}\big((t-\tau)\big),$$

[c] and, by (15), $1 - \zeta_q^{\alpha_2} = 0$, $\alpha_2 = 0$.

In the latter case, by (17), on multiplying it by $(\zeta_q^{\alpha_2}-1)/2$ and adding

$$\left(\frac{1+\zeta_q^{\alpha_2}}{2}(y_{\tau 1q}+y_{\tau 2q})+\sum_{j=3}^{n-2}\zeta_q^{\alpha_j}y_{\tau jq}\right)(t-\tau)^{1/2}\in\overline{K}\big((t-\tau)\big)$$

and since, by (16) and (18),

$$\frac{1+\zeta_q^{\alpha_2}}{2}(y_{\tau 1q}+y_{\tau 2q})+\sum_{j=3}^{n-2}\zeta_q^{\alpha_j}y_{\tau jq}\in\overline{K}\big((t-\tau)\big),$$

we obtain

$$\frac{1+\zeta_q^{\alpha_2}}{2}\big(y_{\tau 1q}+y_{\tau 2q}\big)+\sum_{j=3}^{n-2}\zeta_q^{\alpha_j}y_{\tau jq}=0. \tag{19}$$

However, the left hand side is an expansion at $t=\tau$ of

$$\frac{1+\zeta_q^{\alpha_2}}{2}\big(y_{1q}+y_{2q}\big)+\sum_{j=3}^{n-2}\zeta_q^{\alpha_j}y_{jq},$$

hence (19) contradicts for $n>4$ the linear independence of y_{jq} $(1\leqslant j\leqslant n-2)$ over $\overline{K}$ resulting from Lemma 18.

Therefore, for $n>4$ we obtain $q^{n-3}-q^{n-4}$ expansions for $\Big(\sum\limits_{j=1}^{n-2}y_{jq}\Big)^q$ belonging to $\overline{K}\big((t-\tau)^{1/2}\big)\setminus\overline{K}\big((t-\tau)\big)$, which correspond to $(q^{n-3}-q^{n-4})/2$ distinct prime divisors of the numerator of $t-\tau$ in $M_{2*}(m,n,q)$ each occurring in the second power. □

Lemma 21. *For every zero t_i of f_m $(1\leqslant i\leqslant[(m-1)/2])$ the numerator of $t-t_i$ in $M_{2*}(m,n,q)$ has at most*

$$\frac{q^{n-4}}{n-m}\left(1+\frac{n-m-1}{q^{\varphi((n-m)q)/\varphi(q)}}\right)$$

distinct prime divisors.

Proof. Given Lemma 6 the proof is similar to the proof of Lemma 14 in [8]. □

Lemma 22. *For every zero t_i of f_{n-m} $([(m-1)/2]<i\leqslant[(m-1)/2]+[(n-m-1)/2])$ the numerator of $t-t_i$ in $M_{2*}(m,n,q)$ has at most*

$$\frac{q^{n-4}}{m}\left(1+\frac{m-1}{q^{\varphi((n-m)q)/\varphi(q)}}\right)$$

distinct prime divisors.

Proof. Given Lemma 7 the proof is similar to the proof of Lemma 14 in [8]. □

Lemma 23. *For all positive integers m,n, where $m<n$, $n\geqslant 5$, $(n,m)=1$ and all q being 4 or a prime such that $qmn(n-m)\not\equiv 0 \bmod \pi$, either the genus $g_{2*}(m,n,q)$ of*

$M_{2*}(m, n, q)$ is greater than $5nq/24$ or $nq < 36$. Moreover, if $g_{2*}(m, n, q) \leqslant 1$, then $n = 5$.

Proof. By Lemma 2(a) of [7] and by Lemmas 20–22 we have

$$\begin{aligned} &g_{2*}(m, n, q) \\ &\geqslant 1 + \frac{q^{n-4}}{2}\left(\frac{q-1}{2}\binom{n-2}{2} + \left[\frac{m-1}{2}\right]\left(q - \frac{1}{n-m}\left(1 + \frac{n-m-1}{q^{\varphi((n-m)q)/\varphi(q)}}\right)\right)\right. \\ &\quad \left. + \left[\frac{n-m-1}{2}\right]\left(q - \frac{1}{m}\left(1 + \frac{m-1}{q^{\varphi(neq)/\varphi(q)}}\right)\right) - 2q\right). \end{aligned}$$

For $n = 5$ we obtain

$$g_{2*}(m, n, q) \geqslant 1 + \frac{q}{2}\left(\frac{3}{2}q - \frac{3}{2} + q - 1 - 2q\right) = 1 + \frac{q}{4}(q-5) > \frac{25}{24}q$$

for $q \geqslant 11$.

For $n = 6$ we have $m = 1$ or $m = 5$, hence

$$g_{2*}(m, n, q) \geqslant 1 + \frac{q^2}{2}(3q - 3 + 2q - 2 - 2q) = 1 + \frac{q^2}{2}(3q-5) > \frac{30}{24}q.$$

For $n \geqslant 7$ simpler

$$g_{2*}(m, n, q) \geqslant 1 + \frac{q^{n-4}}{2}\left(\frac{q-1}{2} \cdot 10 - 2q\right) = 1 + \frac{q^{n-4}}{2}(3q-5) > \frac{5qn}{24}.$$

The last two inequalities show that $g_{2*}(m, n, q) > 1$ for $n \geqslant 6$. □

Proof of Theorem 1. The case where $\deg F = 0$ or 1 has been considered in [7] or [8], respectively. Hence, let without loss of generality

$$F(x) = x^2 - Vx + W = (x - z_1)(x - z_2), \quad \text{where } V, W \in K(\boldsymbol{y}),\ z_1, z_2 \in \overline{K(\boldsymbol{y})},$$
$$Q(x; A, B) = \frac{x^{n_1} + Ax^{m_1} + B}{F(x)}.$$

Since $F(x) \mid x^{n_1} + Ax^{m_1} + B$ has a double factor, by Lemma 2

$$m_1^{m_1}(n_1 - m_1)^{n_1 - m_1}(-A)^{n_1} - n_1^{n_1} B^{n_1 - m_1} = 0$$

and $A^{-n_1} B^{n_1 - m_1} \in K$, contrary to $A^{-n} B^{n-m} \notin K$.

The equations $z_i^{n_1} + Az_i^{m_1} + B = 0$ $(i = 1, 2)$ give either $z_1^{m_1} - z_2^{m_1} = z_1^{n_1} - z_2^{n_1} = 0$, whence $z_1 = z_2$, or $z_1^{m_1} - z_2^{m_1} \neq 0$ and

$$A = -\frac{z_1^{n_1} - z_2^{n_1}}{z_1^{m_1} - z_2^{m_1}}, \quad B = (z_1 z_2)^{m_1} \frac{z_1^{n_1 - m_1} - z_2^{n_1 - m_1}}{z_1^{m_1} - z_2^{m_1}},$$

hence

$$
\begin{aligned}
A &= -V^{2\{(n_1-1)/2\}-2\{(m_1-1)/2\}}W^{[(n_1-1)/2]-[(m_1-1)/2]} \\
&\qquad \times f_{n_1}\Big(\frac{V^2}{W}\Big) f_{m_1}\Big(\frac{V^2}{W}\Big)^{-1} \\
&= -\Big(\frac{W}{V}\Big)^{n_1-m_1}\Big(\frac{V^2}{W}\Big)^{[n_1/2]-[m_1/2]} f_{n_1}\Big(\frac{V^2}{W}\Big) f_{m_1}\Big(\frac{V^2}{W}\Big)^{-1}, \\
B &= V^{2\{(n_1-m_1-1)/2\}-2\{(m_1-1)/2)\}}W^{m_1+[(n_1-m_1-1)/2]-[(m_1-1)/2]} \\
&\qquad \times f_{n_1-m_1}\Big(\frac{V^2}{W}\Big) f_{m_1}\Big(\frac{V^2}{W}\Big)^{-1} \\
&= \Big(\frac{W}{V}\Big)^{n_1}\Big(\frac{V^2}{W}\Big)^{[(n_1+m_1)/2]-[m_1/2]} f_{n_1-m_1}\Big(\frac{V^2}{W}\Big) f_{m_1}\Big(\frac{V^2}{W}\Big)^{-1}.
\end{aligned} \tag{20}
$$

It follows that

$$
\begin{aligned}
&A^{-n_1}B^{n_1-m_1} \\
&\qquad = (-1)^{n_1}\Big(\frac{V^2}{W}\Big)^{\rho} f_{n_1}\Big(\frac{V^2}{W}\Big)^{-n_1} f_{n_1-m_1}\Big(\frac{V^2}{W}\Big)^{n_1-m_1} f_{m_1}\Big(\frac{V^2}{W}\Big)^{m_1},
\end{aligned} \tag{21}
$$

where

$$
\rho = \begin{cases} (n_1-m_1)/2 & \text{if } n_1 \equiv m_1 \equiv 1 \bmod 2, \\ m_1/2 & \text{if } n_1 \equiv 1,\ m_1 \equiv 0 \bmod 2, \\ -n_1/2 & \text{if } n_1 \equiv 0,\ m_1 \equiv 1 \bmod 2, \end{cases}
$$

hence $A^{-n}B^{n-m} \notin K$, implies $V^2/W \notin K$. Moreover, by (20)

$$
f_m\left(\frac{V^2}{W}\right) Q(x; A, B) = \left(\frac{W}{V}\right)^{n_1-2} R_2^1\left(\frac{V}{W}\,x, \frac{V^2}{W}\right), \tag{22}
$$

where $R_2^1(x,t)$ is $R_2(x,t)$ with the parameters m, n replaced by m_1, n_1. The same formula is valid, by continuity or a similar argument, if $z_1 = z_2$.

If $T(x; A, B)F(x^{(m,n)})^{-1} = Q(x^{(m,n)}; A, B)$ is reducible over $K(\boldsymbol{y})$, then by Capelli's lemma (see [4], p. 662), either

$$
Q(x) := Q(x; A, B) \text{ is reducible over } K(\boldsymbol{y}), \tag{23}
$$

or

$$
x^{(m,n)} - \xi \text{ is reducible over } K(\boldsymbol{y}, \xi), \text{ where } Q(\xi; A, B) = 0. \tag{24}
$$

In the former case $Q(x)$ has in $K(\boldsymbol{y})[x]$ a factor $x^k + \sum_{i=1}^{k} a_i x^{k-i}$, where $1 \leqslant k \leqslant (n-2)/2$ and the field $L_2^*(k, m_1, n_1)$ is parametrized by rational functions as follows

$$
t = \frac{V^2}{W}, \quad \tau_i(x_1, \ldots, x_k) = (-1)^i a_i \Big(\frac{V}{W}\Big)^{-i} \quad (1 \leqslant i \leqslant k).
$$

By Lemma 2(b) of [7] $g_2^*(k, m_1, n_1) = 0$, contrary to Lemma 15. Assume now that we

have (24), but not (23). It follows by Capelli's theorem that either

$$\xi = \eta^p, \quad \text{where } p \text{ is a prime, } p \mid (m,n),\ \eta \in K(\boldsymbol{y}, \xi), \tag{25}$$

or

$$\xi = -4\eta^4, \quad \text{where } 4 \mid (m,n),\ \eta \in K(\boldsymbol{y}, \xi), \tag{26}$$

Let

$$R_2^1(x,t) = \prod_{j=1}^{n_1-2}(x - x_j), \quad y_{jq}^q = x_j.$$

It follows from (22) that if $t = V^2/W$ one can take

$$q = p,\ y_{jq} = \Big(\frac{V}{W}\Big)^{1/p}\eta_j, \quad \text{if (25) holds,}$$

$$q = 4,\ y_{jq} = \Big(\frac{V}{W}\Big)^{1/4}\eta_j, \quad \text{if (26) holds,}$$

where η_j are conjugates of η over $K(\boldsymbol{y})$. Hence the field

$$M_{2*}(m_1, n_1, q) = \overline{K}\big(t, (y_{1q} + \ldots + y_{n_1-2}, q)^q\big)$$

is parametrized by rational functions as follows:

$$t = V^2/W,\ \ (y_{1q} + \ldots + y_{n_1-2}, q)^q = \begin{cases} (V/W)(\eta_1 + \ldots + \eta_{n_1-2})^p & \text{if (25) holds,} \\ -4(V/W)(\eta_1 + \ldots + \eta_{n_1-2})^p & \text{if (26) holds} \end{cases}$$

and, by Lemma 2(b) of [7], $g_{2*}(m_1, n_1, q) = 0$, contrary to Lemma 23. □

Proof of Theorem 2. The case where $\deg F = 0$ or 1 has been considered in [7] and [8], respectively, hence let $F = x^2 - Vx + W$, where $V, W \in L$;

$$Q(x; A, B) = \frac{x^{n_1} + Ax^{m_1} + B}{F(x)}.$$

The sufficiency of the condition is obvious. The proof of the necessity is similar to the proof of Theorem 1.

Since $F(x) \mid x^{n_1} + Ax^{m_1} + B$ and $AB \neq 0$ we have $VW \neq 0$ and since $A^{-n}B^{n-m} \notin \overline{K}$ is follows from the identity (21) that $V^2/W \notin \overline{K}$.

If $T(x; A, B)F(x^{(m,n)})^{-1} = Q(x^{(m,n)}; A, B)$ is reducible over L, then by Capelli's lemma

$$Q(x) := Q(x; A, B) \text{ is reducible over } L, \tag{27}$$

or

$$x^{(m,n)} - \xi \text{ is reducible over } L(\xi), \quad \text{where } Q(\xi; A, B) = 0. \tag{28}$$

In the former case Q has in $L[x]$ a factor of degree k, where $1 \leqslant k \leqslant (n-2)/2$ and it follows from the identity (22) that the field $L_2^*(k, m_1, n_1)$ is isomorphic to a subfield of $\overline{K}L$. Hence, by Lemma 2(c) of [7], $g_2^*(k, m_1, n_1) \leqslant g$ and, by Lemma 15, either $n_1 < (24/5)g$, or $n \leqslant 6$. The condition given in the theorem holds with $l = (m,n)$, $\langle \nu, \mu \rangle = \langle n_1, m_1 \rangle$.

Moreover, again by Lemma 15, $g = 1$ implies $n_1 = 5$. Assume now that we have (28), but not (27). Then in the same way as in the proof of Theorem 1 we infer that for a certain $q \mid (m, n)$, $q = 4$ or a prime

$$x^q - \xi \text{ is reducible over } L(\xi), \tag{29}$$

and the field $M_{2*}(m_1, n_1, q)$ is isomorphic to a subfield of $\overline{K}L$. Hence, by Lemma 2(c) of [7] we have $g_{2*}(m_1, n_1, q) \leqslant g$, thus, by Lemma 23, we have either $n_1 q < (24/5)g$ or $n_1 q < 36$. On the other hand, by (29), $Q(x^q)$ is reducible over L. Hence the condition given in the theorem holds with $l = (n, m)/q$, $\langle v, \mu\rangle = \langle n_1 q, m_1 q\rangle$. Moreover, again by Lemma 23, $g = 1$ implies $n_1 = 5$. □

Proof of Theorem 3. The case where $\deg F = 0$ or 1 has been considered in [7] or [8], respectively. Therefore, let $\deg F = 2$. Replacing Lemmas 8 and 16 of [8] by Lemmas 15 and 23 above we can proceed as in the proof of Theorem 3 of [8]. We begin by defining the sets $F^2_{v,\mu}(K)$. This is done in three steps. First we put $q = (\mu, \nu)$, $\nu_1 = \nu/q$, $\mu_1 = \mu/q$ and introduce the field $L_2(k, \mu_1, \nu_1)$ and $M_2(\mu_1, \nu_1, q)$ as defined in Definitions 1, 2. Since K is infinite we have $L_2(k, \mu_1, \nu_1) = K(t, y(t))$, where $y(t)$ is defined up to a conjugacy over $K(t)$ as $\sum_{j=1}^{k} a^j \tau_j(x_1, \ldots, x_k)$, $x_1, \ldots, x_k$ being k distinct zeros of $R_2^*(x, t)$ and a being chosen so that $y(t)$ has $\binom{\nu-2}{k}$ distinct conjugates over $K(t)$. Here $R_2^*(x, t)$ is $R_2(x, t)$ with parameters m, n replaced by μ_1, ν_1. Let ϕ_k^2 be the minimal polynomial of $y(t)$ over $K[t]$ (it need not be monic). By Lemma 19 the function $\left(y_{1q} + \ldots + y_{\nu_1-2,q}\right)^q$ generating $M_2(\mu_1, \nu_1, q)$ over $K(t)$ is determined up to a conjugacy. Let ψ_q^2 be its minimal polynomial over $K[t]$.

If $\nu_1 > 6$, we put

$$S^2_{\nu,\mu}(K) = \begin{cases} \bigcup\limits_{0 \leqslant 2k \leqslant \nu_1 - 2} \{t_0 \in K : f_{\mu_1}(t_0) \neq 0,\ \phi_k^2(t_0, z) \text{ has a zero in } K\} & \text{if } q = 1, \\ \{t_0 \in K : f_{\mu_1}(t_0) \neq 0,\ \psi_k^2(t_0, z) \text{ has a zero in } K\} & \text{if } q > 1. \end{cases}$$

Since for $\nu_1 > 6$ and $k \geqslant 1$ or $q > 1$ we have, by Lemma 15, $g_2^*(k, \mu_1, \nu_1) > 1$, or, by Lemma 23, $g_{2*}(\mu_1, \nu_1, q) > 1$, it follows by the Faltings theorem (see [1]) that the sets $S^2_{\nu,\mu}(K)$ are finite. Now we put

$$T^2_{\nu,\mu}(K) = \begin{cases} \bigcup\limits_{t_0 \in S^2_{\nu,\mu}(K)} \Big\{\Big\langle -t_0^{[\nu_1/2]-[\mu_1/2]} f_{\nu_1}(t_0) f_{\mu_1}(t_0)^{-1}, \\ \qquad t_0^{[(\nu_1+\mu_1)/2]-[\mu_1/2]} f_{\nu_1-\mu_1}(t_0) f_{\mu_1}(t_0)^{-1}, -t_0, t_0\Big\rangle\Big\} & \text{if } q = 1, \\ \bigcup\limits_{t_0 \in S^2_{\nu,\mu}(K)} \Big\{\Big\langle -d^{\nu_1-\mu_1} t_0^{[\nu_1/2]-[\mu_1/2]} f_{\nu_1}(t_0) f_{\mu_1}(t_0)^{-1}, \\ \qquad d^{\nu_1} t_0^{[(\nu_1+\mu_1)/2]-[\mu_1/2]} f_{\nu_1-\mu_1}(t_0) f_{\mu_1}(t_0)^{-1}, -dt_0, d^2 t_0\Big\rangle : \\ \qquad \exists_{\xi_0}\, d \in S(q, K, \xi_0),\ R_2^*(\xi_0, t_0) = 0\Big\} & \text{if } q \text{ is a prime, or } q = 4, \\ \emptyset, \qquad \text{otherwise} \end{cases}$$

where $S(q, K, \xi_0)$ is defined in Lemma 18 of [8], not uniquely, as a finite subset of K with the property that if $c \in K^*$ and

$$c\xi_0 = \eta^q, \qquad \eta \in K(\xi_0)^* \quad \text{if } q \text{ is a prime},$$
$$c\xi_0 = -4\eta^4, \quad \eta \in K(\xi_0)^* \quad \text{if } q = 4,$$

then

$$c = de^q, \quad \text{where } d \in S(q, K, \xi_0),\ e \in K^*.$$

Finally we put

$$F^2_{\nu,\mu}(K) = \Big\{ \langle a, b, x^2 + fx + g\rangle : \langle a, b, f, g\rangle \in T^2_{\nu,\mu}(K), \\ \frac{x^\nu + ax^\mu + b}{x^{2q} + fx^q + g} \text{ is reducible over } K \Big\}.$$

Since the sets $S^2_{\nu,\mu}(K)$ and the sets $S(q, K, \xi_0)$ are finite, the latter by Lemma 18 of [8], so are the sets $F^2_{\nu,\mu}(K)$. We proceed to prove that they have all the other properties asserted in the theorem. By the assumption $n_1 > 6$ and $x^{n_1} + ax^{m_1} + b$ has in $K[x]$ a quadratic factor $F(x)$. Let

$$F(x) = x^2 - vx + w, \ Q(x; a, b) = \frac{x^{n_1} + ax^{m_1} + b}{F(x)}. \tag{30}$$

Since $b \neq 0$ we have $w \neq 0$. Putting $t_0 = v^2/w$ we have by the identity (22)

$$f_{m_1}(t_0) Q(x; a, b) = \Big(\frac{w}{v}\Big)^{n_1-2} R^1_2\Big(\frac{w}{v}\, x, t_0\Big), \tag{31}$$

thus $f_{m_1}(t_0) = 0$ would imply $t_0^{[(n_1+m_1)/2]-[m_1/2]-1} f_{n_1-m_1}(t_0) = R^1_2(0, t_0) = 0$, contrary to $\big(f_{m_1}(t), t f_{n_1-m_1}(t)\big) = 1$. Therefore, $f_{m_1}(t_0) \neq 0$. Assume now that

$$\frac{x^n + ax^m + b}{F\big(x^{(m,n)}\big)} = Q\big(x^{(m,n)}; a, b\big) \text{ is reducible over } K.$$

By Capelli's lemma either

$$Q(x; a, b) \text{ is reducible over } K, \tag{32}$$

or

$$x^{(m,n)} - \xi \text{ is reducible over } K, \quad \text{where } Q(\xi; a, b) = 0. \tag{33}$$

In the case (32) $Q(x; a, b)$ has a factor in $K[x]$ of degree $k \leqslant (n_1 - 2)/2$, say $\prod_{i=1}^{k} (x - \xi_i)$. It follows from the identity (31) that $R^1_2(x, t_0)$ has the factor

$$\prod_{i=1}^{k} \Big(x - \frac{v}{w}\, \xi_i\Big) \in K[x],$$

thus $\tau_i((v/w)\xi_1, \ldots, (v/w)\xi_k) \in K$ $(1 \leqslant i \leqslant k)$ and at least one value of the algebraic

function $y(t)$ at $t = t_0$ lies in K. Hence $t_0 \in S^2_{n_1,m_1}(K)$,

$$\langle -t_0^{[n_1/2]-[m_1/2]} f_{n_1}(t_0) f_{m_1}(t_0)^{-1}, \\ t_0^{[(n_1+m_1)/2]-[m_1/2]} f_{n_1-m_1}(t_0) f_{m_1}(t_0)^{-1}, -t_0, t_0 \rangle \in T^2_{n_1,m_1}(K),$$

and the condition given in the theorem holds with $l = (m, n)$, $\nu = n_1$, $\mu = m_1$, $F_0 = x^2 - t_0 x + t_0$, $u = w/v$.

In the case (33) note that $\xi \neq 0$, since $b \neq 0$. By Capelli's theorem, there exists a $q \mid (m, n)$ such that

(34) either q is a prime and $\xi = \eta^q,\ \eta \in K(\xi),$ or $q = 4$ and $\xi = -4\eta^4,\ \eta \in K(\xi)$.

If $\eta_1, \ldots, \eta_{n_1-2}$ are all the conjugates of η over K we have

$$Q(x; a, b) = \begin{cases} \prod_{i=1}^{n_1-2} (x - \eta_i^q) & \text{if } q \text{ is a prime,} \\ \prod_{i=1}^{n_1-2} (x + 4\eta_i^4) & \text{if } q = 4, \end{cases}$$

hence

$$Q(x^q; a, b) \text{ is reducible over } K. \tag{35}$$

By the identity (31) it follows that

$$R_2^1(x, t_0) = \begin{cases} \prod_{i=1}^{n_1-2} (x - (v/w)\eta_i^q) & \text{if } q \text{ is a prime,} \\ \prod_{i=1}^{n_1-2} (x + 4(v/w)\eta_i^4) & \text{if } q = 4. \end{cases}$$

Hence $\psi_q^2(t_0, u_0) = 0$, where

$$u_0 = \begin{cases} (v/w)(\eta_1 + \ldots + \eta_{n_1-2})^q & \text{if } q \text{ is a prime,} \\ -4(v/w)(\eta_1 + \ldots + \eta_{n_1-2})^4 & \text{if } q = 4 \end{cases}$$

and since $\eta_1 + \ldots + \eta_{n_1-2} \in K$ we have $u_0 \in K$, $t_0 \in S^2_{n_1,m_1}(K)$.

Further, it follows from (31) and (33) that $\xi_0 = (v/w)\xi$ is a zero of $R_2^1(x, t_0)$ and by (34)

$$\frac{w}{v}\,\xi_0 = \eta^q \text{ or } -4\eta^4, \quad \text{where } \eta \in K(\xi_0) \text{ and } q \text{ is a prime or } q = 4, \text{ respectively.}$$

By the definition of $S(q, K, \xi_0)$

$$\frac{w}{v} = de^q, \quad \text{where } d \in S(q, K, \xi_0),\ e \in K,$$

hence

$$\langle -d^{n_1-m_1}t_0^{[n_1/2]-[m_1/2]}f_{n_1}(t_0)f_{m_1}(t_0)^{-1},$$
$$d^{n_1}t_0^{[(n_1+m_1)/2]-[m_1/2]}f_{n_1-m_1}(t_0)f_{m_1}(t_0)^{-1}, -dt_0, d^2t_0\rangle \in T^2_{n_1q,m_1q}(K).$$

By the identity (31)

$$R_2^1\Big(\frac{x^q}{d}, t_0\Big) = \Big(\frac{v}{w}\Big)^{n_1-2} f_{m_1}(t_0)Q\big((ex)^q; a, b\big),$$

hence by (35) $R_2^1(x^q/d, t_0)$ is reducible over K and

$$\langle -d^{n_1-m_1}t_0^{[n_1/2]-[m_1/2]}f_{n_1}(t_0)f_{m_1}(t_0)^{-1},$$
$$d^{n_1}t_0^{[(n_1+m_1)/2]-[m_1/2]}f_{n_1-m_1}(t_0)f_{m_1}(t_0)^{-1}, x^2 - dt_0x + d^2t_0\rangle \in F_{n_1q,m_1q}(K).$$

Thus the condition given in the theorem holds with $l = (n, m)/q$, $\nu = n_1q$, $\mu = m_1q$,

$$a_0 = -d^{n_1-m_1}t_0^{[n_1/2]-[m_1/2]}f_{n_1}(t_0)f_{m_1}(t_0)^{-1},$$
$$b_0 = d^{n_1}t_0^{[(n_1+m_1)/2]-[m_1/2]}f_{n_1-m_1}(t_0)f_{m_1}(t_0)^{-1},$$
$$F_0 = x^2 - dt_0x + d^2t_0, \quad u = e.$$

Assume now that for an integer l, $\langle n/l, m/l\rangle =: \langle \nu, \mu\rangle \in \mathbb{N}^2$ and $a = u^{\nu-\mu}a_0$, $b = u^\nu b_0$, $F(x) = u^{2(\mu,\nu)}F_0\big(x/u^{(\mu,\nu)}\big)$, where $u \in K^*$, $\langle a_0, b_0, F_0\rangle \in F^2_{\nu,\mu}(K)$.

Then by the definition of $F^2_{\nu,\mu}(K)$

$$\frac{x^\nu + a_0x^\mu + b_0}{F_0\left(x^{(\mu,\nu)}\right)} \text{ is a polynomial reducible over } K$$

and by the substitution $x \mapsto x^l/u$ we obtain reducibility of $T(x; a, b)/F\big(x^{(m,n)}\big)$. □

References

[1] E. Bombieri, *The Mordell conjecture revisited*. Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) 17 (1990), 615–640.

[2] H. Hasse, *Number Theory*. Springer, Berlin 1980.

[3] P. Lefton, *On the Galois group of cubics and trinomials*. Acta Arith. 35 (1979), 239–246.

[4] L. Rédei, *Algebra* I. Akademische Verlagsgesellschaft, Geest & Portig, Leipzig 1959.

[5] T. J. Rivlin, *Chebyshev polynomials. From Approximation Theory to Algebra and Number Theory*. Second ed., Wiley, New York 1990.

[6] A. Schinzel, *On linear dependence of roots*. Acta Arith. 28 (1975), 161–175; this collection: C7, 238–252.

[7] —, *On reducible trinomials*. Dissert. Math. (Rozprawy Mat.) 329 (1993); *Errata*, Acta Arith. 73 (1995), 399–400; this collection: D10, 466–548.

[8] —, *On reducible trinomials* II. Publ. Math. Debrecen 56 (2000), 575–608; this collection: D13, 580–604.

[9] N. Tschebotaröw, *Grundzüge der Galoisschen Theorie*. Übersetzt und bearbeitet von H. Schwerdtfeger, Noordhoff, Groningen–Djakarta 1950.

Andrzej Schinzel
Selecta

Originally published in
A Panorama of Number Theory
or the View from Baker's Garden
Cambridge University Press, Cambridge 2002
Chapter 21, 337–352

On the greatest common divisor of two univariate polynomials I

P. Weinberger proposed at the West Coast Number Theory Meeting in 1976 the following problem. Does there exist a function $A(r, s)$ such that if polynomials f, g have exactly r and s non-zero coefficients, respectively, then the greatest common divisor (f, g) has at most $A(r, s)$ non-zero coefficients? We are going to study this problem in the case where $f, g \in K[x]$ and K is a field. Accordingly, we denote by $A(r, s, K)$ the supremum of the number of non-zero coefficients of (f, g), where f, g run over all univariate polynomials over K with r and s non-zero coefficients, respectively. Clearly, $A(r, s, K) = A(s, r, K)$, hence we may assume $r \leqslant s$ and trivially $A(1, s, K) = 1$. We shall denote by K_0 the prime field of K, by p its characteristic, by $\overline{K}$ its algebraic closure and by ${}^p\zeta_q$ a generator of the group of qth roots of unity in $\overline{K}$. We set $K^q = \{a^q : a \in K\}$. Moreover, for a Laurent polynomial F over K,

$$F(x_1, \dots, x_k) = F_0(x_1, \dots, x_k) \prod_{i=1}^{k} x_i^{\alpha_i},$$

where $F_0 \in K[x_1, \dots, x_k]$ is prime to $\prod_{i=1}^{k} x_i$, we set

$$JF = F_0.$$

We shall prove the following two theorems.

Theorem 1. *If m, n, q are positive integers with $(m, n, q) = 1$ and $a, b, c \in K^*$, then $(x^n + ax^m + b,\ x^q - c)$ is of degree at most 1, if $a^{-n/(m,n)} b^{(n-m)/(m,n)} \notin K_0\left({}^p\zeta_q\right)$, and of degree 0, if, additionally, $c \notin K^q$. Moreover, if $p = 0$ or $p > 6^{\varphi(q)}$, then $(x^n + ax^m + b,\ x^q - c)$ is of degree at most 2 and of degree 0, if, as well, $c^2 \notin K^q$.*

Theorem 2. *If $1 < r \leqslant s$ and $\langle r, s, p\rangle \neq \langle 3, 3, 0\rangle$ then*

$$A(r, s, K) = \begin{cases} 2, & \text{if } r = s = 2, \\ 3, & \text{if } r = 2,\ s = 3,\ p = 0, \\ \infty, & \text{otherwise.} \end{cases}$$

The case $\langle r, s, p\rangle = \langle 3, 3, 0\rangle$ has been studied in [9].

Lemma 1. *Let z_i $(1 \leqslant i \leqslant 4)$ be roots of unity in $\overline{K}$ such that $z_i^q = 1$, and*

$$\begin{vmatrix} 1 & 1 & 1 \\ z_1 & z_2 & 1 \\ z_3 & z_4 & 1 \end{vmatrix} = 0. \tag{1}$$

If either $p = 0$ or $p > 6^{\varphi(q)}$, then either two rows or two columns of the determinant are equal.

Proof. In the case $p = 0$ this is Lemma 9 of [3]. The proof outlined there was by a tedious consideration of cases. J. Browkin has supplied the following proof for $p = 0$ (it is enough to take $K = \mathbb{C}$), which is no longer tedious and works for arbitrary unimodular z_i (cf. [10], Corollary 3.3). The equation (1) gives

$$(z_1 - 1)(z_4 - 1) = (z_2 - 1)(z_3 - 1). \tag{2}$$

If $z_1 = 1$, then $z_2 = 1$ and the rows 1, 2 are equal, or $z_3 = 1$ and the columns 1, 3 are equal. Similarly, if $z_i = 1$ for $i \leqslant 4$. If $z_i \neq 1$ for all i we take the complex conjugates of both sides of (2) and obtain

$$z_1^{-1} z_4^{-1} (z_1 - 1)(z_4 - 1) = z_2^{-1} z_3^{-1} (z_2 - 1)(z_3 - 1), \tag{3}$$

hence, dividing side by side (2) and (3)

$$z_1 z_4 = z_2 z_3. \tag{4}$$

The formulae (2) and (4) give

$$z_1 + z_4 = z_2 + z_3, \tag{5}$$

while (4) and (5) give either $z_1 = z_3$, $z_2 = z_4$ (the rows 2 and 3 are equal), or $z_1 = z_2$, $z_3 = z_4$ (the columns 1 and 2 are equal).

The case $p > 6^{\varphi(q)}$ is reduced to the case $p = 0$ as follows. Let $\mathfrak{p}$ be a prime ideal factor of p in $\mathbb{Q}({}^0\zeta_q)$. The residues $\bmod \mathfrak{p}$ form a subfield of $\overline{K}$ containing q distinct zeros of $x^q - 1$, since $p \nmid q$, represented by residues of ${}^0\zeta_q^r$ $(0 \leqslant r < q)$. Hence

$$z_i \equiv {}^0\zeta_q^{r_i} \bmod \mathfrak{p} \quad (1 \leqslant i \leqslant 4) \tag{6}$$

and equation (1) gives

$$D := \begin{vmatrix} 1 & 1 & 1 \\ {}^0\zeta_q^{r_1} & {}^0\zeta_q^{r_2} & 1 \\ {}^0\zeta_q^{r_3} & {}^0\zeta_q^{r_4} & 1 \end{vmatrix} \equiv 0 \bmod \mathfrak{p}; \qquad N_{\mathbb{Q}({}^0\zeta_q)/\mathbb{Q}} D \equiv 0 \bmod \mathfrak{p}. \tag{7}$$

However D is the sum of six complex roots of unity. Hence each conjugate of D over $\mathbb{Q}$ does not exceed 6 in absolute value and

$$\left| N_{\mathbb{Q}({}^0\zeta_q)/\mathbb{Q}} D \right| \leqslant 6^{\varphi(q)} < p.$$

Since D is an algebraic integer, $N_{\mathbb{Q}({}^0\zeta_q)/\mathbb{Q}} D$ is an integer and the above inequality together with the second congruence of (7) gives

$$N_{\mathbb{Q}({}^0\zeta_q)/\mathbb{Q}} D = 0; \ D = 0.$$

By the already settled case $p = 0$ the determinant defining D has two rows or two columns equal and by (6) the same applies to the determinant

$$\begin{vmatrix} 1 & 1 & 1 \\ z_1 & z_2 & 1 \\ z_3 & z_4 & 1 \end{vmatrix}. \qquad \square$$

Proof of Theorem 1. Let $(n, m) = d$, $n = dn'$, $m = dm'$, $(x^n + ax^m + b,\ x^q - c)$ be of degree δ and assume first that

$$a^{-n'} b^{n'-m'} \notin K_0\left({}^p\zeta_q\right) \tag{8}$$

and

$$\delta \geqslant 2. \tag{9}$$

If $(x^n + ax^m + b,\ x^q - c)$ has a multiple zero in $\overline{K}$, then $p > 0$, $p \mid q$ and since $(n, m, q) = 1$, $p \nmid d$. Moreover,

$$\Delta := \operatorname{disc}\left(x^n + ax^m + b\right) = 0. \tag{10}$$

However (see [4])

$$\Delta = (-1)^{n(n-1)/2} b^{m-1} \left(n^{n'} b^{n'-m'} + (-1)^{n'-1} (n-m)^{n'-m'} m^{m'} a^{n'}\right)^d. \tag{11}$$

It follows from $p \nmid d$

$$a^{-n'} b^{n'-m'} = (-1)^{n'} (n-m)^{n'-m'} m^{m'} n^{-n'} \in K_0,$$

contrary to (8). Thus, by (9), $(x^n + ax^m + b,\ x^q - c)$ has two distinct zeros in $\overline{K}$. Denoting them by ξ_i $(i = 1, 2)$ we have for $i = 1, 2$, $\xi_i^q = c$ and

$$\xi_i^n + a\xi_i^m + b = 0. \tag{12}$$

If $\xi_1^m = \xi_2^m$, then also $\xi_1^n = \xi_2^n$, and since $\xi_1^q = \xi_2^q$, it follows from $(m, n, q) = 1$ that $\xi_1 = \xi_2$, a contradiction. Thus $\xi_1^m \neq \xi_2^m$ and solving the system (12) for a, b we find

$$a = \frac{\xi_2^n - \xi_1^n}{\xi_2^m - \xi_1^m}, \quad b = \frac{\xi_1^n \xi_2^m - \xi_1^m \xi_2^n}{\xi_2^m - \xi_1^m}.$$

Since $\xi_2 = {}^p\zeta_q^r \xi_1$ for a certain r, it follows that ${}^p\zeta_q^{rm} \neq 1$ and

$$a = \xi_1^{n-m} \frac{{}^p\zeta_q^{rn} - 1}{1 - {}^p\zeta_q^{rm}}, \quad b = \xi_1^n \frac{{}^p\zeta_q^{rm} - {}^p\zeta_q^{rn}}{1 - {}^p\zeta_q^{rm}}; \tag{13}$$

$$a^{-n'} b^{n'-m'} = \left(1 - {}^p\zeta_q^{rm}\right)^{m'} \left({}^p\zeta_q^{rm} - {}^p\zeta_q^{rn}\right)^{n'-m'} \left({}^p\zeta_q^{rn} - 1\right)^{-n'} \in K_0\left({}^p\zeta_q\right), \tag{14}$$

contrary to (8). Thus (8) implies that $\delta \leqslant 1$. If $\delta \neq 0$, then

$$\left(x^n + ax^m + b,\ x^q - c\right) = x - \xi, \quad \xi \in K,$$

hence $c = \xi^q \in K^q$.

It remains to consider the case where $p = 0$ or $p > 6^{\varphi(q)}$. Then $x^q - c$ has no multiple zeros and $\delta \geqslant 3$ implies the existence of three distinct zeros ξ_i of $x^q - c$ such that (12) holds

for $i = 1, 2, 3$. Putting $z_1 = (\xi_2/\xi_1)^n$, $z_2 = (\xi_2/\xi_1)^m$, $z_3 = (\xi_3/\xi_1)^n$, $z_4 = (\xi_3/\xi_1)^m$, we can rewrite the system (12) in the form

$$\begin{aligned} \xi_1^n + a\xi_1^m + b &= 0, \\ z_1\xi_1^n + z_2 a\xi_1^m + b &= 0, \\ z_3\xi_1^n + z_4 a\xi_1^m + b &= 0, \end{aligned} \tag{15}$$

hence

$$\begin{vmatrix} 1 & 1 & 1 \\ z_1 & z_2 & 1 \\ z_3 & z_4 & 1 \end{vmatrix} = 0$$

and by Lemma 1, either two rows or two columns of the determinant are equal. If two rows are equal we infer from $(m, n, q) = 1$ that $\xi_2 = \xi_1$, or $\xi_3 = \xi_1$, or $\xi_3 = \xi_2$, a contradiction. If two columns are equal, then equations (15) imply, since $ab \neq 0$ that $z_1 = z_2 = z_3 = z_4 = 1$, hence $\xi_3 = \xi_2 = \xi_1$, again a contradiction.

Hence $\delta \leqslant 2$. If $\delta = 1$, $(x^n + ax^m + b,\ x^q - c) = x - \xi$, where $\xi \in K$ and $c = \xi^q \in K^q$. If $\delta = 2$, $(x^n + ax^m + b,\ x^q - c) = (x - \xi_1)(x - \xi_2)$, hence $[K(\xi_1) : K] \leqslant 2$ and $\xi_1^q = c$ implies $\left(N_{K(\xi_1)/K}\xi_1\right)^q = N_{K(\xi_1)/K}c = c$ or c^2; $c^2 \in K^q$. □

Lemma 2. *Let* $0 = a_0 < a_1 < \ldots < a_r$ *and* $0 = b_0 < b_1 < \ldots < b_s$ *be integers and set*

$$R(t) = \sum_{t = a_i + b_j} 1.$$

If there exist at most two positive integers t *such that* $R(t) = 1$, *then there exist* $l \leqslant 2$ *integers* u_j $(1 \leqslant j \leqslant l)$ *such that*

$$a_i = \sum_{j=1}^{l} \alpha_{ij} u_j \ (0 \leqslant i \leqslant r), \quad b_i = \sum_{j=1}^{l} \beta_{ij} u_j \ (0 \leqslant i \leqslant s),$$

where α_{ij}, β_{ij} *are integers and*

$$\prod_{j=1}^{l} \max \left\{ \max_{0 \leqslant i \leqslant r} |\alpha_{ij}|,\ \max_{0 \leqslant i \leqslant s} |\beta_{ij}| \right\} \leqslant 2^{r+s-l}.$$

Proof. Clearly, we have

$$R(a_r + b_s) = 1,$$

thus, by the assumption, there exists at most one pair $\langle r_1, s_1 \rangle \neq \langle 0, 0 \rangle,\ \langle r, s \rangle$ such that

$$R\left(a_{r_1} + b_{s_1}\right) = 1.$$

If $0 \leqslant i \leqslant r$, $0 \leqslant j \leqslant s$ and $\langle i, j \rangle \neq \langle 0, 0 \rangle$, $\langle r, s \rangle$, $\langle r_1, s_1 \rangle$, there exists a pair $\langle g_{ij}, h_{ij} \rangle \neq \langle i, j \rangle$ such that

$$a_i + b_j = a_{g_{ij}} + b_{h_{ij}}. \tag{16}$$

Let us consider the system of equations for $r + s + 2$ unknowns x_i $(0 \leqslant i \leqslant r)$, y_j $(0 \leqslant j \leqslant s)$:

$$\begin{aligned} x_0 &= 0, \\ y_0 &= 0, \\ x_r + y_s &= 0, \\ x_{r_1} + y_{s_1} &= 0, \\ x_i + y_j - x_{g_{ij}} - y_{h_{ij}} &= 0 \quad \big(\langle i, j\rangle \neq \langle 0, 0\rangle,\ \langle r, s\rangle,\ \langle r_1, s_1\rangle\big). \end{aligned} \tag{17}$$

We assert that the system has only the zero solution. Indeed, suppose that $\langle c_0, \ldots, c_r, d_0, \ldots, d_s\rangle$ is a solution of this system and let

$$\begin{aligned} i_1 &\text{ be the least } i \text{ such that } c_i = \min c_k, \\ i_2 &\text{ be the least } i \text{ such that } c_i = \max c_k, \\ j_1 &\text{ be the least } j \text{ such that } d_j = \min d_k, \\ j_2 &\text{ be the least } j \text{ such that } d_j = \max d_k. \end{aligned}$$

If for $\nu = 1$ or 2 we have $\langle i_\nu, j_\nu\rangle \neq \langle 0, 0\rangle, \langle r, s\rangle, \langle r_1, s_1\rangle$, let

$$g_\nu = g_{i_\nu j_\nu}, \quad h_\nu = h_{i_\nu j_\nu}.$$

The equations (17) give

$$c_{i_\nu} + d_{j_\nu} = c_{g_\nu} + d_{h_\nu},$$

hence $c_{g_\nu} = c_{i_\nu}, d_{h_\nu} = d_{j_\nu}$; $g_\nu \geqslant i_\nu, h_\nu \geqslant j_\nu$ and since $\langle g_\nu, h_\nu\rangle \neq \langle i_\nu, j_\nu\rangle$ it follows that $a_{g_\nu} + b_{h_\nu} > a_{i_\nu} + b_{j_\nu}$, contrary to (16). Therefore, $\langle i_\nu, j_\nu\rangle \in \big\{\langle 0, 0\rangle,\ \langle r, s\rangle,\ \langle r_1, s_1\rangle\big\}$ for $\nu \leqslant 2$ and thus

$$c_{i_\nu} + d_{j_\nu} = 0 \quad (\nu = 1, 2).$$

However $c_{i_2} \geqslant c_{i_1}, d_{j_2} \geqslant d_{j_1}$, thus $c_{i_2} = c_{i_1}, d_{j_2} = d_{j_1}$ and by the definition of c_{i_ν} and d_{j_ν}, all c_i are equal $(0 \leqslant i \leqslant r)$ and all d_j are equal $(0 \leqslant j \leqslant s)$. Since $c_0 = d_0 = 0$ we infer that $c_i = 0$ $(0 \leqslant i \leqslant r)$ and $d_j = 0$ $(0 \leqslant j \leqslant s)$. It follows from the proved assertion that the rank of the matrix of the system (17) is $r + s + 2$ and thus the rank of the matrix of the reduced system

$$\begin{aligned} x_0 &= 0, \\ y_0 &= 0, \\ x_i + y_j - x_{g_{ij}} - y_{h_{ij}} &= 0 \quad \big(\langle i, j\rangle \neq \langle 0, 0\rangle,\ \langle r, s\rangle,\ \langle r_1, s_1\rangle\big) \end{aligned} \tag{18}$$

is $r + s + 2 - l$, where $l \leqslant 2$. By (16) we have $l > 0$.

Let Δ be a submatrix of the matrix of the system (18) consisting of $r+s+2-l$ linearly independent rows. By Steinitz's lemma we may assume that the submatrix contains the first two rows. By the Bombieri–Vaaler theorem ([1], Theorem 2) there exists a system of l linearly independent integer solutions $\boldsymbol{v}_j$ $(j \leqslant l)$ of the equation

$$\boldsymbol{x}\Delta = 0 \tag{19}$$

satisfying the inequality

$$\prod_{j=1}^{l} h(\boldsymbol{v}_j) \leqslant \sqrt{\det \Delta\Delta^T},$$

where $h(\boldsymbol{v}_j)$ is the maximum of the absolute values of the coordinates of $\boldsymbol{v}_j$. However, by an inequality of Fischer generalizing Hadamard's inequality (see [1], formula (2.6)) $\sqrt{\det \Delta\Delta^T}$ does not exceed the product of the Euclidean lengths of the rows of Δ, i.e. 2^{r+s-l}.

Now, from the system $\boldsymbol{v}_j$ $(j \leqslant l)$ of $l \leqslant 2$ linearly independent integer solutions of the equation (19) one can obtain a basis $\boldsymbol{w}_j$ $(j \leqslant l)$ of all integer solutions satisfying

$$h(\boldsymbol{w}_j) \leqslant h(\boldsymbol{v}_j) \quad (j \leqslant l)$$

(see [2], Chapter V, Lemma 8). It suffices now to take

$$\boldsymbol{w}_j = \left[\alpha_{0j}, \ldots, \alpha_{rj},\ \beta_{0j}, \ldots, \beta_{sj}\right] \quad (j \leqslant l). \qquad \square$$

Remark. In the same way one can prove the following generalization of Lemma 2. If, with the same notation, $R(t) = 1$ for at most k positive integers t, then there exist $l \leqslant k$ integers u_j $(1 \leqslant j \leqslant l)$ such that

$$a_i = \sum_{j=1}^{l} \alpha_{ij} u_j \ (0 \leqslant i \leqslant r), \quad b_i = \sum_{j=1}^{l} \beta_{ij} u_j \ (0 \leqslant i \leqslant s),$$

where α_{ij}, β_{ij} are integers and

$$\prod_{j=1}^{l} \max\left\{ \max_{0\leqslant i\leqslant r} |\alpha_{ij}|,\ \max_{0\leqslant i\leqslant s} |\beta_{ij}| \right\} \leqslant 2^{r+s-l}\, \frac{(l+m+1)!}{4^{l-m}(2m+1)!},$$

where $m = \left[(1+\sqrt{16l+7})/4\right]$.

Instead of a result quoted from [2] one has to use an argument from [7], pp. 701–702, due essentially to H. Weyl [11].

It is also possible to generalize Lemma 2 to the case of more than two increasing sequences of integers.

Lemma 3. *Let $a, b \in K^*$, $n > m > 0$. If $(n, m) \not\equiv 0 \bmod p$ and*

$$(*) \qquad x^n + ax^m + b = g(x)h(x),$$

where $g, h \in K[x] \setminus K$ and g, h have exactly $r+1$ and $s+1$ non-zero coefficients, respectively, then

$$2^{r+s+3} + 1 \geqslant \frac{n}{(n,m)}. \tag{20}$$

Proof. Let us put

$$g(x) = \sum_{i=0}^{r} g_i x^{a_i}, \quad h(x) = \sum_{j=0}^{s} h_j x^{b_j}, \tag{21}$$

where $0 < a_0 < a_1 < \ldots < a_r$, $0 < b_0 < b_1 < \ldots < b_s$ and $g_i \neq 0$ $(0 \leqslant i \leqslant r)$, $h_j \neq 0$ $(0 \leqslant j \leqslant s)$. In the notation of Lemma 2 for each positive integer $t \neq m, n$ we have $R(t) \neq 1$. Hence, by Lemma 2, there exist $l \leqslant 2$ integers u_j $(1 \leqslant j \leqslant l)$ such that

$$a_i = \sum_{j=1}^{l} \alpha_{ij} u_j \ (0 \leqslant i \leqslant r), \quad b_i = \sum_{j=1}^{l} \beta_{ij} u_j \ (0 \leqslant i \leqslant s),$$

where α_{ij}, β_{ij} are integers and

$$\prod_{j=1}^{l} \max \left\{ \max_{0 \leqslant i \leqslant r} |\alpha_{ij}|, \ \max_{0 \leqslant i \leqslant s} |\beta_{ij}| \right\} \leqslant 2^{r+s-l}. \tag{22}$$

Clearly,

$$\begin{aligned} n &= \sum_{j=1}^{l} u_j(\alpha_{rj} + \beta_{sj}), \\ m &= \sum_{j=1}^{l} u_j(\alpha_{r'j} + \beta_{s'j}), \end{aligned} \tag{23}$$

where $0 \leqslant r' \leqslant r$, $0 \leqslant s' \leqslant s$.

If $l = 1$, then $u_1 \mid (m, n)$ and by (22) and (23)

$$n \leqslant (n, m) 2^{r+s}$$

which is stronger than (20).

If $l = 2$, let us put for $j = 1, 2$

$$\begin{aligned} \nu_j &= \alpha_{rj} + \beta_{sj}, \\ \mu_j &= \alpha_{r'j} + \beta_{s'j}, \end{aligned} \tag{24}$$

$$\begin{aligned} F(x_1, x_2) &= J\left(x_1^{\nu_1} x_2^{\nu_2} + a x_1^{\mu_1} x_2^{\mu_2} + b\right), \\ G(x_1, x_2) &= J\left(\sum_{i=0}^{r} g_i x_1^{\alpha_{i1}} x_2^{\alpha_{i2}}\right), \\ H(x_1, x_2) &= J\left(\sum_{i=0}^{s} h_i x_1^{\beta_{i1}} x_2^{\beta_{i2}}\right), \end{aligned}$$

the notation being explained in the introduction.

By (21) and (23), (24)

$$x^n + a x^m + b = J F\left(x^{u_1}, x^{u_2}\right), \tag{25}$$

$$g(x) = J G\left(x^{u_1}, x^{u_2}\right), \quad h(x) = J H\left(x^{u_1}, x^{u_2}\right), \tag{26}$$

while, by (22)

$$\prod_{j=1}^{2} \max \left\{ \left|\mu_j\right|, \left|\nu_j\right| \right\} \leqslant 2^{r+s}. \tag{27}$$

It follows that

$$
\begin{aligned}
\deg_{x_j} F &\leqslant |\mu_j| + |\nu_j| \leqslant 2\max\left\{|\mu_j|, |\nu_j|\right\} \\
&\leqslant 4\max\left\{\max_i \left|\alpha_{ij}\right|, \max_i \left|\beta_{ij}\right|\right\}, \\
\deg_{x_j} G &= \max_i \alpha_{ij} - \min_i \alpha_{ij} \leqslant 2\max_i \left|\alpha_{ij}\right|, \\
\deg_{x_j} H &= \max_i \beta_{ij} - \min_i \beta_{ij} \leqslant 2\max_i \left|\beta_{ij}\right|.
\end{aligned} \tag{28}
$$

If $\nu_1\mu_2 - \nu_2\mu_1 = 0$, then by (23) and (24)

$$
\frac{u_1\nu_1 + u_2\nu_2}{(\nu_1, \nu_2)} \;\Big|\; (n, m),
$$

hence, by (27), $n \leqslant (n, m)(\nu_1, \nu_2) \leqslant (n, m)2^{(r+s)/2}$, which is stronger than (20).

If $\nu_1\mu_2 - \nu_2\mu_1 \neq 0$, $F(x_1, x_2)$ is irreducible over K, by Theorem 23 of [8]. Indeed, the only assumption of this theorem that needs to be verified is that $F(x_1, x_2)$ is not of the form cF_0^p, where $c \in K$, $F_0 \in K[x_1, x_2]$. If it were the case, we should have $\nu_j \equiv 0$, $\mu_j \equiv 0 \bmod p$ $(j = 1, 2)$, hence by (23) and (24) $(n, m) \equiv 0 \bmod p$, contrary to the assumption of the lemma.

If now $(F, G) \neq 1$, it follows by the irreducibility of F that $F \mid G$, hence, by (25) and (26), $x^n + ax^m + b \mid g(x)$ and, by (19), $h(x) \in K$, contrary to the assumption of the lemma. Therefore $(F, G) = 1$ and by Lemma 5 of [6] the number of solutions in $\overline{K}^2$ of the system of equations $F(x_1, x_2) = G(x_1, x_2) = 0$ does not exceed the degree of the resultant R of F and G with respect to x_1.

From the form of the resultant as the determinant of the Sylvester matrix we infer by (28) and (22)

$$
\begin{aligned}
\deg R &\leqslant \deg_{x_1} F \cdot \deg_{x_2} G + \deg_{x_2} F \cdot \deg_{x_1} G \\
&\leqslant 16 \prod_{j=1}^{2} \max\left\{\max_i \left|\alpha_{ij}\right|, \max_i \left|\beta_{ij}\right|\right\} \leqslant 2^{r+s+2}.
\end{aligned}
$$

Thus the number of solutions in $\overline{K}^2$ of the system of equations $F(x_1, x_2) = G(x_1, x_2) = 0$ does not exceed 2^{r+s+2} and the same applies to the system $F(x_1, x_2) = H(x_1, x_2) = 0$. Since ξ^{u_1}, ξ^{u_2} determine the value of $\xi^{(u_1,u_2)}$, they give (u_1, u_2) possibilities for ξ. Hence the systems of equations $F(\xi^{u_1}, \xi^{u_2}) = G(\xi^{u_1}, \xi^{u_2})$ and $F(\xi^{u_1}, \xi^{u_2}) = H(\xi^{u_1}, \xi^{u_2})$ have each at most $(u_1, u_2)2^{r+s+2}$ distinct solutions in $\overline{K}^2$. In view of $(*)$, (25) and (26) it follows that $x^n + ax^m + b$ has at most $2^{r+s+3}(n, m)$ distinct zeros in $\overline{K}$. Since each zero of $x^n + ax^m + b$ is at most double, and the number of double zeros is at most (m, n), we get

$$
n - (m, n) \leqslant 2^{r+s+3}(m, n),
$$

which gives the lemma. □

Lemma 4. *For every prime field $K_0 \neq \mathbb{F}_2$ and every integer $k > 1$ there exists a polynomial $f_k \in K_0[x]$ of degree at most k with exactly k non-zero coefficients, such that $f_k(0) = 1$, $f_k(1) = 0$ and $f_k'(1) \neq 0$. For $K_0 = \mathbb{F}_2$ such a polynomial exists, if k is even.*

Proof. We set

$$f_k(x) = \sum_{i=0}^{k-1}(-1)^i x^i \qquad \text{if } k \text{ is even, } k \not\equiv 0 \bmod 2p;$$

$$f_k(x) = \sum_{i=0}^{k-2}(-1)^i x^i - x^k \qquad \text{if } k \text{ is even, } k \equiv 0 \bmod 2p;$$

$$f_k(x) = \sum_{i=0}^{k-3}(-1)^i x^i - 2x^{k-2} + x^{k-1} \qquad \text{if } k \text{ is odd, } k \not\equiv 3 \bmod 2p;$$

$$f_k(x) = \sum_{i=0}^{k-3}(-1)^i x^i - 2x^{k-2} + x^k \qquad \text{if } k \text{ is odd, } k \equiv 3 \bmod 2p. \qquad \square$$

Definition. For convenience we set $f_1(x) = 0$.

Lemma 5. *For every $K \neq \mathbb{F}_2$, every $f \in K[x]$ and every positive integer k there exists a polynomial $h = h(x; k, f) \in K[x]$ with exactly k non-zero coefficients such that $(h(x^l), xf(x)) = 1$ for every positive integer l. For $K = \mathbb{F}_2$ such a polynomial exists if k is odd and, moreover, with the weaker property $(h(x), xf(x)) = 1$ also if $f(1) \neq 0$.*

Proof. If K contains $\mathbb{Q}$ or $\mathbb{F}_p(t)$ with t transcendental over $\mathbb{F}_p$, then the multiplicative group of K contains a free abelian group of infinite rank. Hence, denoting the zeros of f by $\xi_1, \ldots, \xi_n$ we can choose $a \in K^*$ such that for all $\nu \leqslant n$ and all l the element $a\xi_\nu^{-l}$ is not a root of unity, and then

$$h(x) = \frac{x^k - a^k}{x - a}$$

has the desired property.

If K contains neither $\mathbb{Q}$ nor $\mathbb{F}_p(t)$, then $K \subset \overline{\mathbb{F}}_p$, hence there exists an exponent $e > 0$ such that $\xi_\nu^e = 1$ for every $\xi_\nu \neq 0$ $(1 \leqslant \nu \leqslant n)$. Then we write $k = p^\kappa k_1$, where $(k_1, p) = 1$ and set

$$h(x) = \frac{x^{k_1 e} - 1}{x^e - 1}, \qquad \text{if } \kappa = 0, \tag{29}$$

$$h(x) = \left(\frac{x^{k_1 e} - 1}{x^e - 1}\right)^{p^\kappa} (x^e + a)^{p^\kappa - 1}, \quad \text{if } \kappa > 0,\ K \neq \mathbb{F}_2,\ a \in K \setminus \{0, -1\}, \tag{30}$$

$$h(x) = \left(\frac{x^{k_1 e} - 1}{x^e - 1}\right)^{2^\kappa} (x + 1)^{2^\kappa - 1}, \qquad \text{if } \kappa > 0,\ K = \mathbb{F}_2,\ f(1) \neq 0. \tag{31}$$

It is easy to see that $h(x)$ has exactly k non-zero coefficients and in cases (29), (30) $h(\xi_\nu^l) \neq 0$, in case (31) $h(\xi_\nu) \neq 0$ for all $\nu \leqslant n$. $\square$

Lemma 6. *If $n \equiv 1 \bmod 6$, over $\mathbb{F}_2$, then the trinomial*

$$T_n(x) = x^{2^{n+1}+1} + x^{2^n - 1} + 1$$

is the product of two non-constant factors, one of which divides $x^{2^{2n}-1}+1$ *and the other* $x^{2^{3n}-1}+1$; *both are prime to* $x^{2^n-1}+1$.

Proof. This is a special case of the result of Mills & Zierler [5], the case admitting a shorter proof. Let $r=2^n$. By the identity of Mills & Zierler

$$T_n(x^r)+x^{r^2-r}T_n(x)=\bigl(x^{r^2-1}+1\bigr)\bigl(x^{r^2+r+1}+1\bigr),$$

hence every irreducible factor of $T_n(x)$ divides one of the relevant binomials. Since $T_n(x)$ has no multiple zeros, $T_n(1)\neq 0$ and 1 is the only common zero of the two binomials, we have

$$T_n(x)=\bigl(T_n(x),\ x^{r^2-1}+1\bigr)\bigl(T_n(x),\ x^{r^2+r+1}+1\bigr).$$

In order to show that the factors are non-constant let us observe that for $n\equiv 1 \bmod 6$

$$2r+1\equiv 5 \bmod 21,\quad r-1\equiv 1 \bmod 21,$$
$$x^5+x+1=(x^2+x+1)(x^3+x^2+1)$$

and

$$x^2+x+1\,|\,x^3+1\,|\,x^{r^2-1}+1,$$
$$x^3+x^2+1\,|\,x^7+1\,|\,x^{r^2+r+1}+1\,|\,x^{r^3-1}+1,$$

hence

$$x^2+x+1\ \big|\ \bigl(T_n(x),\ x^{r^2-1}+1\bigr),$$
$$x^3+x^2+1\ \big|\ \bigl(T_n(x),\ x^{r^2+r+1}+1\bigr).$$

Finally,

$$\bigl(T_n(x),\ x^{r-1}+1\bigr)\ \big|\ T_n(x)+x^{r-1}+1=x^{2r+1},$$

hence

$$\bigl(T_n(x),\ x^{r-1}+1\bigr)=1$$

and we can also write

$$T_n(x)=\bigl(T_n(x),\ x^{r^2-1}+1\bigr)\bigl(T_n(x),\ x^{r^3-1}+1\bigr).$$ □

Lemma 7. *If* $n\equiv 1 \bmod 6$ *and* $T_n(x)=x^{2^{n+1}+1}+x^{2^n-1}+1\in\mathbb{F}_2[x]$, *then there exists* $c=c(n)\in\{2,3\}$ *such that* $\bigl(T_n(x),\ x^{2^{cn}-1}+1\bigr)$ *has at least* $n/2$ *non-zero coefficients.*

Remark. If 2 and 3 both have the required property, we put $c(n)=2$.

Proof. For $n\equiv 1 \bmod 6$ we have $(2^{n+1}+1,\,2^n-1)=1$. Hence, denoting by $r(i,n)$ $(i=2,3)$ the number of non-zero coefficients of $(T_n(x),\,x^{2^{in}-1}+1)$, we have by Lemmas 3 and 6

$$2^{r(2,n)+r(3,n)+1}+1\geqslant 2^{n+1}+1,$$

hence $\max\{r(2,n),r(3,n)\}\geqslant n/2$. □

Proof of Theorem 2. Consider first the case $r = s = 2$. It is nearly obvious that if $a_1, a_2 \in K^*$ and n_1, n_2 are positive integers, then

$$(x^{n_1} - a_1,\ x^{n_2} - a_2) = \begin{cases} 1, & \text{if } a_1^{n_2/(n_1,n_2)} \neq a_2^{n_1/(n_1,n_2)} \\ x^{(n_1,n_2)} - c & \text{if } a_1^{n_2/(n_1,n_2)} = a_2^{n_1/(n_1,n_2)} \text{ and } a_i = c^{n_i/(n_1,n_2)}. \end{cases}$$

This proves that $A(2, 2, K) = 2$.

Consider next the case $r = 2$, $s = 3$, $p = 0$. By Theorem 1 we have $A(2, 3, K) \leqslant 3$ and since $(x^3 - 1, x^2 + x + 1) = x^2 + x + 1$, $A(2, 3, K) = 3$. Therefore, we assume $\langle r, s\rangle \neq \langle 2, 2\rangle$, $\langle r, s, p\rangle \neq \langle 2, 3, 0\rangle$, $\langle 3, 3, 0\rangle$ and we have to prove $A(r, s, K) = \infty$.

Consider first the case $p \neq 2$.

If $r = 2$, $s = 3$, $p > 0$ we take $f(x) = x^{p^{(n-2)!}-1} - 1$, $g(x) = x^n - nx + n - 1$, where $n \not\equiv 0, 1 \bmod p$. The trinomial $g(x)$ has exactly one multiple zero in $\overline{K}$, namely $x = 1$, and this is a double zero. All other zeros are of degree at most $n - 2$, hence they are zeros of $f(x)$. Since 1 is not a multiple zero of this binomial, we obtain

$$(f, g) = \frac{x^n - nx + n - 1}{x - 1} = x^{n-1} + \ldots + 1 - n, \tag{32}$$

where on the right hand side we have n non-zero coefficients. Thus $A(2, 3, K) = \infty$.

If $r = 2$, $s \geqslant 4$, we take

$$f = x^{ab} - 1, \quad g = (x^a - 1)(x^b - 1) + f_{s-3}(x^{ab}),$$

where $1 < a < b$, $(a, b) = 1$, $ab \not\equiv 0 \bmod p$ and f_{s-3} has the meaning of Lemma 4. Since $f \mid f_{s-3}(x^{ab})$ we have $(f, g) = (f, (x^a - 1)(x^b - 1))$. However f has no multiple zeros and $(x^a - 1)(x^b - 1)$ has just one such zero, namely 1, which is a double zero. Hence

$$(f, g) = \frac{(x^a - 1)(x^b - 1)}{x - 1} = x^{b+a-1} + \ldots + x^b - x^{a-1} - \ldots - 1 \tag{33}$$

has $2a$ non-zero coefficients and we obtain $A(2, s, K) = \infty$.

If $r = 3$, $s \geqslant 3$, $p > 0$, we take

$$f = x^n - nx + n - 1, \quad g = f_s\left(x^{p^{(n-2)!}-1}\right).$$

Since $f \,\big|\, x^{p^{(n-2)!}-1} - 1 \,\big|\, f_s\left(x^{p^{(n-2)!}-1}\right)$ and $f_s'(1) \neq 0$ we have again (32), hence $A(3, s, K) = \infty$.

If $r = 3$, $s > 3$, $p = 0$, we take

$$f = x^{2ab} - 3x^{ab} + 2, \quad g(x) = (x^a - 1)(x^b - 1) + f_{s-3}(x^{ab}),$$

where again $1 < a < b$, $(a, b) = 1$. We have $f = (x^{ab} - 1)(x^{ab} - 2)$. It follows from the irreducibility of $x^{ab} - 2$ over $\mathbb{Q}$ that

$$\left(x^{ab} - 2,\ (x^a - 1)(x^b - 1) + f_{s-3}(2)\right) = 1,$$

hence

$$\left(x^{ab} - 2,\ (x^a - 1)(x^b - 1) + f_{s-3}(x^{ab})\right) = 1,$$

and we obtain again (33), thus $A(3, s, K) = \infty$.

If $r \geqslant 4$, $s \geqslant r$, we take

$$f = (x^a - 1)(x^b - 1) + f_{r-3}(x^{2ab}), \quad h = h\big(x; [(s-r)/2] + 1, f\big),$$

$$g = f(0)(x^{ab} - 1)h(x^{2rab}) + dh(0)f(x),$$

where

$$d = \begin{cases} 2 & \text{if } s \equiv r+1 \bmod 2, \\ 1 & \text{if } s \equiv r \bmod 2 \end{cases}$$

and obtain (33), hence $A(r, s, K) = \infty$.

Consider now $p = 2$.

If $r = 2$, $s \geqslant 3$, $s \equiv 0 \bmod 2$, we take

$$f = x^{ab} + 1, \quad g = (x^a + 1)(x^b + 1) + f_{s-2}(x^{ab}),$$

where $1 < a < b$, $(a, b) = 1$, $ab \not\equiv 0 \bmod 2$, and obtain (33), hence $A(2, 3, K) = \infty$.

If $r = 2$, $s \geqslant 3$, $s \equiv 1 \bmod 2$, we take

$$f = x^{2^{cn}-1} + 1, \quad g = T_n(x) + f_{s-1}\big(x^{2^{cn}-1}\big),$$

where $n \equiv 1 \bmod 6$ and $c = c(n)$ is the number defined in Lemma 7. By that lemma

$$(f, g) = \big(x^{2^{cn}-1} + 1,\ T_n(x)\big) \tag{34}$$

has at least $n/2$ non-zero coefficients, hence $A(2, s, K) = \infty$.

If $r = 3$, $s \geqslant 3$, $s \equiv 0 \bmod 2$, we write $s = 2^\sigma s_1$, s_1 odd, and take $n \equiv 1 \bmod 6$,

$$f = T_n(x), \quad g = g_s := \big(x^{2^{cn}-1} + 1\big)^{2^{sn}(2^\sigma - 1)} \frac{x^{(2^{(5-c)n}-1)s_1} + 1}{x^{2^{(5-c)n}-1} + 1}.$$

Since $x^{2^{cn}-1} + 1 \mid g_s$ we have

$$\big(f,\ x^{2^{cn}-1} + 1,\ g_s\big) = \big(f,\ x^{2^{cn}-1} + 1\big).$$

On the other hand, since s_1 is odd

$$\left(x^{2^{(5-c)n}-1} + 1,\ \frac{x^{(2^{(5-c)n}-1)s_1} + 1}{x^{2^{(5-c)n}-1} + 1}\right) = 1;$$

$$\big(x^{2^{(5-c)n}-1} + 1,\ g_s\big) = x^{2^n - 1} + 1$$

hence, by Lemma 6,

$$\big(f,\ x^{2^{(5-c)n}-1} + 1,\ g_s\big) = 1$$

and, again by Lemma 6,

$$\big(f,\ g_s\big) = \big(f,\ x^{2^{cn}-1} + 1\big).$$

Thus, by Lemma 7, (f, g_s) has at least $n/2$ non-zero coefficients and $A(3, s, K) = \infty$.

If $r = 3$, $s \geqslant 3$, $s \equiv 1 \bmod 2$ we take $n \equiv 1 \bmod 6$,

$$f = T_n(x), \quad g = f + g_{s-1}$$

and obtain that $(f, g) = (f, g_{s-1})$ has at least $n/2$ non-zero coefficients, hence $A(3, s, K) = \infty$.

If $r \geqslant 4$, $s \geqslant r$, $r \equiv 0 \bmod 2$, $s \equiv r \bmod 4$, we take $1 < a < b$, $(a, b) = 1$, $ab \equiv 1 \bmod 2$,

$$f = (x^a + 1)(x^b + 1) + f_{r-2}(x^{ab}), \quad h = h\big(x; (s-r)/2 + 1, f\big),$$
$$g = (x^{ab} + 1)h(x^{rab})x^a + h(0)f(x)$$

to obtain

$$(f, g) = \frac{(x^a + 1)(x^b + 1)x^a}{x + 1} = x^{b+2a-1} + \ldots + x^{b+a} + x^{2a-1} + \ldots + x^a,$$

hence $A(r, s, K) = \infty$.

If $r \geqslant 4$, $s \geqslant r$, $r \equiv 0 \bmod 2$, $s \equiv r + 2 \bmod 4$, we take $1 < a < b$, $(a, b) = 1$, $ab \equiv 1 \bmod 2$,

$$f = (x^a + 1)(x^b + 1) + f_{r-2}(x^{2ab}),$$
$$g = (x^{ab} + 1)h(x^{2rab}; (s-r)/2, f) + f$$

and obtain (33), hence $A(r, s, K) = \infty$.

If $r \geqslant 4$, $s \geqslant r$, $r \equiv 0 \bmod 2$, $s \equiv 1 \bmod 2$, we take $n \equiv 1 \bmod 6$,

$$g = T_n(x) + f_{s-1}\big(x^{2^{cn}-1}\big), \quad f = \big(x^{2^{cn}-1} + 1\big)h\big(x^{2^{cn}}; r/2, g\big)$$

and obtain (34).

If $r \geqslant 4$, $s \geqslant r$, $r \equiv 1 \bmod 2$, $s \equiv 0 \bmod 2$, we take $n \equiv 1 \bmod 6$,

$$f = T_n(x) + f_{r-1}\big(x^{2^{cn}-1}\big), \quad g = \big(x^{2^{cn}-1} + 1\big)h\big(x^{2^{cn}}; s/2, f\big)$$

and again obtain (34), hence $A(r, s, K) = \infty$.

Finally, if $r \geqslant 4$, $s \geqslant r$, $r \equiv s \equiv 1 \bmod 2$, we take $n \equiv 1 \bmod 6$,

$$f = T_n(x) + f_{r-1}\big(x^{2^{cn}-1}\big), \quad h = h\big(x; (s-r)/2 + 1, f\big),$$
$$g = \big(x^{2^{cn}-1} + 1\big)h\big(x^{2^{cn+r}}\big)x^{2^n-1} + h(0)f(x)$$

and infer that

$$(f, g) = x^{2^n-1}\big(x^{2^{cn}-1}, T_n(x)\big)$$

has at least $n/2$ non-zero coefficients, hence $A(r, s, K) = \infty$. □

References

[1] E. Bombieri, J. D. Vaaler, *On Siegel's Lemma*. Invent. Math. 73 (1983), 11–32; *Addendum*, ibid. 75 (1984), 377.

[2] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*. Springer, Berlin 1959.

[3] K. Győry, A. Schinzel, *On a conjecture of Posner and Rumsey*. J. Number Theory 47 (1994), 63–78; this collection: D11, 549–562.

[4] P. Lefton, *On the Galois group of cubics and trinomials*. Acta Arith. 35 (1979), 239–246.

[5] W. H. Mills, N. Zierler, *On a conjecture of Golomb*. Pacific J. Math. 28 (1969), 635–640.

[6] A. Schinzel, *Reducibility of lacunary polynomials* I. Acta Arith. 16 (1969), 123–159; *Corrigenda*: Acta Arith. 19 (1971), 201; ibid. 24 (1978), 265; this collection: D4, 344–380.

[7] —, *A decomposition of integer vectors* III. Bull. Polish Acad. Sci. Math. 35 (1987), 693–703.

[8] —, *Polynomials with Special Regard to Reducibility*. Encyclopaedia of Mathematics and its Applications 77, Cambridge Univ. Press, Cambridge 2000.

[9] —, *On the greatest common divisor of two univariate polynomials* II. Acta Arith. 98 (2001), 95–106; this collection: D16, 646–657.

[10] H. P. Schlickewei, E. Wirsing, *Lower bounds for the heights of solutions of linear equations*. Invent. Math. 129 (1997), 1–10.

[11] H. Weyl, *On geometry of numbers*. Proc. London Math. Soc. (2) 47 (1942), 268–289.

Andrzej Schinzel
Selecta

Originally published in
Acta Arithmetica XCVIII (2001), 95–106

On the greatest common divisor of two univariate polynomials II

To Andrzej Rotkiewicz on his 70th birthday

The first paper of this series [4] has concerned the supremum $A(r, s, K)$ of the number of non-zero coefficients of (f, g), where f, g run through all univariate polynomials over a field K with exactly r and s non-zero coefficients, respectively. The only case where $A(r, s, K)$ has remained to be evaluated is $r = s = 3$, $p = \operatorname{char} K = 0$. This case is studied in the present paper. Let us denote by ζ_q a primitive complex root of unity of order q, set

$$P_{n,m}(z) = \left(1 - z^m\right)^{m/(n,m)} \left(z^m - z^n\right)^{(n-m)/(n,m)} \left(z^n - 1\right)^{-n/(n,m)}$$

and for a trinomial

$$T(x) = x^n + ax^m + b \in \mathbb{C}[x], \quad \text{where} \quad n > m > 0,\ ab \neq 0,$$

put

$$\operatorname{inv} T = a^{-n/(n,m)} b^{(n-m)/(n,m)}.$$

We shall prove the following results:

Theorem 1. *Let $T_i = x^{n_i} + a_i x^{m_i} + b_i \in \mathbb{C}[x]$, $a_i b_i \neq 0$, $n_i > m_i > 0$ and $d_i = (n_i, m_i)$ $(i = 1, 2)$. If $(d_1, d_2) = 1$, then*

$$\deg(T_1, T_2) \leqslant \begin{cases} n_2/d_2 & \text{if } \operatorname{inv} T_1 \neq P_{n_1,m_1}(\zeta_{d_2}^r) \text{ for all } r, \\ n_2/d_2 + \min\{2, d_1\} & \text{if } n_1/d_1 \neq 4 \text{ or } d_2 \not\equiv 0 \bmod 10, \\ n_2/d_2 + \min\{3, n_2/d_2\} & \text{always.} \end{cases} \tag{1}$$

Theorem 2. *For every quadruple $\langle n_1, m_1, n_2, m_2\rangle \in \mathbb{N}^4$, where $n_1 > m_1$, $n_2 > m_2$, $\langle n_1, m_1\rangle \neq \langle n_2, m_2\rangle$ and $(n_1, m_1, n_2, m_2) = 1$ there exists an effectively computable finite subset S of $\overline{\mathbb{Q}}^4$ with the following property. If $T_i = x^{n_i} + a_i x^{m_i} + b_i \in \mathbb{C}[x]$, $a_i b_i \neq 0$ $(i = 1, 2)$, and $\deg(T_1, T_2) > 2$, then*

$$T_i = u^{n_i} T_i^*\left(\frac{x}{u}\right), \quad \text{where} \quad u \in \mathbb{C}^*,\ T_i^* = x^{n_i} + a_i^* x^{m_i} + b_i^* \tag{2}$$

and $\langle a_1^*, b_1^*, a_2^*, b_2^*\rangle \in S$.

Corollary 1. *If* $\operatorname{inv} T_i \notin \overline{\mathbb{Q}}$ *for at least one* $i \leqslant 2$, *or*

$$T_1(0)^{-\deg T_2} T_2(0)^{\deg T_1} \notin \overline{\mathbb{Q}}$$

then (T_1, T_2) *has at most three non-zero coefficients.*

Corollary 2. *We have*

$$\sup_{K \subset \mathbb{C}} A(3,3,K) = A(3,3,\overline{\mathbb{Q}}) = \sup_{[K:\mathbb{Q}]<\infty} A(3,3,K).$$

Theorem 3. *For every finite extension* K *of* $\mathbb{Q}$ *and every pair* $\langle n, m\rangle \in \mathbb{N}^2$, *where* $n > m$, *there exists a finite set* $E_{n,m}(K)$ *such that if* $T_i = x^{n_i} + a_i x^{m_i} + b_i \in K[x]$,

$$\operatorname{inv} T_i \notin E_{n_i,m_i}(K) \quad (i = 1, 2) \tag{3}$$

and $(n_1, m_1, n_2, m_2) = 1$ *then either* $T_1 = T_2$, *or* $\deg(T_1, T_2) \leqslant 9$.

Corollary 3. *If* (3) *holds, then* (T_1, T_2) *has at most* 10 *non-zero coefficients.*

At the end of the paper we give three examples of some interest.

R. Dvornicich has kindly looked through the paper and corrected several mistakes. The proofs of Theorems 1 and 3 use a recent result of his [2] on the so-called cyclotomic numbers, which we formulate below as

Lemma 1. *Let* z_1, z_2 *be two complex roots of unity and let* Q *be the least common multiple of their orders. If* m, n *are integers such that* $(m, n, Q) = 1$ *and*

$$\left|z_1^n - 1\right|^m \left|z_1^{n-m} - 1\right|^{n-m} \left|z_1^n - 1\right|^{-n} = \left|z_2^m - 1\right|^m \left|z_2^{n-m} - 1\right|^{n-m} \left|z_2^n - 1\right|^{-n}, \tag{4}$$

where none of the six absolute values is 0, *then either* $z_1 = z_2^{\pm 1}$, *or* $Q = 10$, $\{m, n-m, -n\} = \{x, 3x, -4x\}$ *with* $(x, 10) = 1$ *and* z_1, z_2 *are two primitive tenth roots of unity.*

Proof. See [2], Theorem 1. □

Remark. Lemma 1 can be extended to fields of arbitrary characteristic as follows. Let K be a field of characteristic p, $p = 0$ or a prime, let z_i $(i = 1, 2)$ be roots of unity in $\overline{K}$, $z_i^Q = 1$ and let m, n be positive integers such that $m < n$, $(m, n, Q) = 1$ and

$$1 \neq z_i^m \neq z_i^n \neq 1, \quad P_{n,m}(z_1) = P_{n,m}(z_2).$$

If either $p = 0$ or $p > 2^{(2n/(n,m)+1)\varphi(Q)}$, then either $z_2 = z_1 = z_1^{\pm 1}$, or $n/(n, m) = 4$ and z_1, z_2 are primitive tenth roots of unity.

Lemma 2. *If* $(n, m, q) = 1$ *and*

$$1 \neq \zeta_q^m \neq \zeta_q^n \neq 1, \ q \neq 10,$$

then $P_{n,m}(\zeta_q)$ *is an algebraic number of degree* $\frac{1}{2}\varphi(q)$.

Proof. We have $P_{n,m}(\zeta_q^{-1}) = P_{n,m}(\zeta_q)$. On the other hand, if $q > 2$, $0 < r < s < q/2$, $(r, s, q) = 1$ we have by Lemma 1,

$$\left|P_{n,m}\left(\zeta_q^r\right)\right| \neq \left|P_{n,m}\left(\zeta_q^s\right)\right|,$$

hence $P_{n,m}(\zeta_q)$ has $\frac{1}{2}\varphi(q)$ distinct conjugates. □

Lemma 3. *Let n, m, q be positive integers with $(n, m, q) = 1$, $n > m$ and $T = x^n + ax^m + b \in \mathbb{C}[x]$, $ab \neq 0$. Set*

$$C(T, q) = \left\{c^{(m,n)} : c \in \mathbb{C},\ \deg(T, x^q - c) \geqslant 2\right\}.$$

We have

$$\operatorname{card} C(T, q) \leqslant 1 \tag{5}$$

unless $n/(n, m) = 4$ and $q \equiv 0 \bmod 10$, in which case

$$\operatorname{card} C(T, q) \leqslant 2. \tag{6}$$

Moreover, if $C(T, q) \neq \emptyset$, then T is separable and

$$\operatorname{inv} T = P_{n,m}(\zeta_q^r) \quad \text{for an } r \text{ satisfying } 1 \neq \zeta_q^{rm} \neq \zeta_q^{rn} \neq 1. \tag{7}$$

Proof. By Theorem 1 of [4] we have $\deg(T, x^q - c) \leqslant 2$. Assume that $\deg(T, x^q - c) = 2$. Since the binomial $x^q - c$ is separable we have

$$(T, x^q - c) = (x - \xi_1)(x - \xi_2),$$

where $\xi_i^q = c$ $(i = 1, 2)$, $\xi_2 = \xi_1\zeta_q^r$, $\zeta_q^r \neq 1$.

By the formulae (13) and (14) of [4] we have

$$a^q = c^{n-m}\left(\frac{\zeta_q^{rn} - 1}{1 - \zeta_q^{rm}}\right)^q, \quad b^q = c^n\left(\frac{\zeta_q^{rm} - \zeta_q^{rn}}{1 - \zeta_q^{rm}}\right)^q, \tag{8}$$

where $1 \neq \zeta_q^{rm} \neq \zeta_q^{rn} \neq 1$ and

$$\operatorname{inv} T = P_{n,m}\left(\zeta_q^r\right),$$

which proves (7). Also, if for another value c' we have

$$(T, x^q - c') = (x - \xi_1')(x - \xi_2')$$

where $\xi_i'^q = c'$ $(i = 1, 2)$, $\xi_2' = \xi_1'\zeta_q^{r'}$, it follows that

$$\operatorname{inv} T = P_{n,m}\left(\zeta_q^{r'}\right), \quad \text{hence} \quad P_{n,m}(\zeta_q^r) = P_{n,m}\left(\zeta_q^{r'}\right).$$

Applying Lemma 1 with $z_1 = \zeta_q^r$, $z_2 = \zeta_q^{r'}$ we infer that either $r' = \pm r$ or $n_1/d_1 = 4$ and $q \equiv 0 \bmod 10$, $r' \equiv \pm 3r \bmod q$. In the former case, by (8),

$$c'^{n-m} = c^{n-m},\ c'^n = c^n,$$

hence $c'^{(n,m)} = c^{(n,m)}$, which proves (5). In the latter case for any value c'' with $\deg(T, x^q - c'') \geqslant 2$ we have $c''^{(n,m)} = c^{(n,m)}$ or $c'^{(n,m)}$, which proves (6).

It remains to prove that if $c(T, q) \neq \emptyset$, then T is separable. Now, by formula (11) of [4]

$$\operatorname{disc}_x T = (-1)^{n(n-1)/2} a^n b^{m-1} \big(n^{n'} \operatorname{inv} T + (-1)^{n'-1} (n-m)^{n'-m'} m^{m'}\big)^{(n,m)},$$

where $n' = n/(n, m)$, $m' = m/(n, m)$.

Thus, if T has double zeros we have

$$\operatorname{inv} T = (-1)^{n'} m'^{m'} (n' - m')^{n'-m'} n'^{-n'}.$$

Hence, by (7),

$$(-1)^{n'} m'^{m'} (n' - m')^{n'-m'} n'^{-n'} = \big(1 - \zeta_q^{rm}\big)^{m'} \big(\zeta_q^{rm} - \zeta_q^{rn}\big)^{n'-m'} \big(\zeta_q^{rn} - 1\big)^{-n'}. \tag{9}$$

Now, since $\big(n', m'(n' - m')\big) = 1$ it follows that in the ring of integers of $\mathbb{Q}(\zeta_q)$ we have

$$n'^{n'} \mid \big(\zeta_q^{rn} - 1\big)^{n'}, \quad n' \mid \zeta_q^{rn} - 1.$$

On taking norms from $\mathbb{Q}(\zeta_q^{rn})$ to $\mathbb{Q}$ we infer that $n' = 2$, $\zeta_q^{rn} = -1$, hence $m' = 1$, $\zeta_q^{rm} = \pm\zeta_4$ and (9) gives $1/4 = 1/2$. The contradiction obtained shows our contention. □

Proof of Theorem 1. Let

$$T_2\big(x^{1/d_2}\big) = \prod_{c \in \mathbb{C}} (x - c)^{e(c)}, \quad \sum_{c \in \mathbb{C}} e(c) = n_2/d_2.$$

We have

$$\deg(T_1, T_2) \leqslant \sum_{c \in \mathbb{C}} \deg\big(T_1, (x^{d_2} - c)^{e(c)}\big) \leqslant \sum_{c \in \mathbb{C}} e(c) \deg\big(T_1, x^{d_2} - c\big). \tag{10}$$

If $\deg\big(T_1, x^{d_2} - c\big) \leqslant 1$ for all $c \in \mathbb{C}$ with $e(c) \geqslant 1$ the inequalities (1) follow.

If for at least one c, say c_1, we have $e(c_1) \geqslant 1$ and $\deg\big(T_1, x^{d_2} - c_1\big) \geqslant 2$ then, by Lemma 3, T_1 is separable and $\operatorname{inv} T_1 = P_{n_1,m_1}(\zeta_{d_2}^r)$ for an r satisfying

$$1 \neq \zeta_{d_2}^{rm_1} \neq \zeta_{d_2}^{rn_1} \neq 1.$$

This shows the first inequality of (1). Moreover, by (10),

$$\begin{aligned} \deg(T_1, T_2) &\leqslant \sum_{c \in \mathbb{C}} \min\{e(c), 1\} \deg\big(T_1, x^{d_2} - c\big) \\ &\leqslant \sum_{c \in \mathbb{C}} e(c) + \sum_{e(c) \geqslant 1} \big(\deg\big(T_1, x^{d_2} - c\big) - 1\big) \\ &\leqslant \frac{n_2}{d_2} + \sum_{\substack{e(c) \geqslant 1 \\ \deg(T_1, x^{d_2} - c) = 2}} 1. \end{aligned} \tag{11}$$

If $n_1/d_1 \neq 4$ or $d_2 \not\equiv 0 \bmod 10$, then by Lemma 3, $\deg\big(T_1, x^{d_2} - c\big) = 2$ implies $c^{d_1} = c_1^{d_1}$,

hence by Theorem 1 of [4],

$$\sum_{\substack{e(c)\geqslant 1\\(T_1,x^{d_2}-c_1)=2}} 1 \leqslant \deg\bigl(T_2(x^{1/d_2}), x^{d_1}-c_1^{d_1}\bigr) \leqslant \min\{2, d_1\},$$

which together with (11) proves the second inequality of (1) and *a fortiori*, the third.

If $n_1/d_1 = 4$ and $d_2 \equiv 0 \bmod 10$, then by Lemma 3 there exists a c_2, possibly equal to c_1, such that $\deg\bigl(T_1, x^d - c\bigr) = 2$ implies $c^{d_1} = c_i^{d_i}$ for an $i \leqslant 2$. If $c_2^{d_1} = c_1^{d_1}$ we are in the previous case, otherwise

$$\sum_{\substack{e(c)\geqslant 1\\ \deg(T_1,x^{d_2}-c)=2}} 1 \leqslant \sum_{i=1}^{2} \deg\bigl(T_2(x^{1/d_2}), x^{d_1}-c_i^{d_1}\bigr). \tag{12}$$

However, since $d_2 \equiv 0 \bmod 10$ we have $d_1 \not\equiv 0 \bmod 10$, hence, by Lemma 3, $\operatorname{card} C(T_2(x^{1/d_2}), d_1) \leqslant 1$ and the right hand side of (12) does not exceed 3. Since it also does not exceed $\deg T_2\bigl(x^{1/d_2}\bigr) = n_2/d_2$ the third of the inequalities (1) follows. □

Lemma 4. *Let $n > m > 0$, $d = (n, m)$, $F = (1 - t^m)x^n + (t^n - 1)x^m + t^m - t^n$. All zeros of F in $\mathbb{C}((t))$ are given by the Puiseux expansions*

$$\zeta_d^{\delta},\ \zeta_d^{\delta} t: \quad 0 \leqslant \delta < d;$$

$$\zeta_m^{\mu} t + \frac{\zeta_m^{\mu n} - 1}{m}\,\zeta_m^{\mu} t^{n-m+1} + \ldots: \quad 0 \leqslant \mu < m,\ \mu \not\equiv 0 \bmod \frac{m}{d};$$

$$\zeta_{n-m}^{\nu} + \frac{\zeta_{n-m}^{\nu n} - 1}{n-m}\,\zeta_{n-m}^{\nu} t^{m} + \ldots: \quad 0 \leqslant \nu < n-m,\ \nu \not\equiv 0 \bmod \frac{n-m}{d}.$$

Proof. One applies the usual procedure (Newton polygons) for finding Puiseux expansions. □

Lemma 5. *Let $n_i > m_i > 0$, $d_i = (n_i, m_i)$, and $F_i = (1-t^{m_i})x^{n_i} + (t^{n_i} - 1)x^{m_i} + t^{m_i} - t^{n_i}$ $(i = 1, 2)$. If $(d_1, d_2) = 1$ then either $F_1 = F_2$, or*

$$(F_1, F_2) = (t-1)(x-1)(x-t).$$

Proof. The content $C(F_i)$ of F_i viewed as a polynomial in x is $t^{d_i} - 1$, hence $(C(F_1), C(F_2)) = t - 1$. On the other hand, by Lemma 4, F_1 and F_2 have two common zeros in $\mathbb{C}((t))$, namely 1 and t, each with multiplicity 1; if there are any other common zeros we have either

$$\zeta_{m_1}^{\mu_1} t + \frac{\zeta_{m_1}^{\mu_1 n_1} - 1}{m_1}\,\zeta_{m_1}^{\mu_1} t^{n_1-m_1+1} = \zeta_{m_2}^{\mu_2} t + \frac{\zeta_{m_2}^{\mu_2 n_2} - 1}{m_2}\,\zeta_{m_2}^{\mu_2} t^{n_2-m_2+1}, \tag{13}$$

where $\mu_i \not\equiv 0 \bmod \frac{m_i}{d_i}$ $(i = 1, 2)$, or

$$\zeta_{n_1-m_1}^{\nu_1} + \frac{\zeta_{n_1-m_1}^{\nu_1 n_1} - 1}{n_1 - m_1}\,\zeta_{n_1-m_1}^{\nu_1} t^{m_1} = \zeta_{n_2-m_2}^{\nu_2} + \frac{\zeta_{n_2-m_2}^{\nu_2 n_2} - 1}{n_2 - m_2}\,\zeta_{n_2-m_2}^{\nu_2} t^{m_2}, \tag{14}$$

where $\nu_i \not\equiv 0 \bmod \frac{n_i - m_i}{d_i}$ $(i = 1, 2)$.

If (13) holds, we have

$$\begin{aligned} &\zeta_{m_1}^{\mu_1} = \zeta_{m_2}^{\mu_2}, \quad n_1 - m_1 + 1 = n_2 - m_2 + 1, \\ &\frac{\zeta_{m_1}^{\mu_1 n_1} - 1}{m_1} = \frac{\zeta_{m_2}^{\mu_2 n_2} - 1}{m_2}. \end{aligned} \tag{15}$$

Dividing the last equality by its complex conjugate we obtain

$$-\zeta_{m_1}^{\mu_1 n_1} = -\zeta_{m_2}^{\mu_2 n_2} \neq -1,$$

hence $m_1 = m_2$, which together with (15) gives $F_1 = F_2$.

If (14) holds, we have

$$\begin{aligned} &\zeta_{n_1-m_1}^{\nu_1} = \zeta_{n_2-m_2}^{\nu_2}, \quad m_1 = m_2, \\ &\frac{\zeta_{n_1-m_1}^{\nu_1 n_1} - 1}{n_1 - m_1} = \frac{\zeta_{n_2-m_2}^{\nu_2 n_2} - 1}{n_2 - m_2}. \end{aligned} \tag{16}$$

Dividing the last equality by its complex conjugate we obtain

$$-\zeta_{n_1-m_1}^{\nu_1 n_1} = -\zeta_{n_2-m_2}^{\nu_2 n_2} \neq -1,$$

hence $n_1 - m_1 = n_2 - m_2$, which together with (16) gives $F_1 = F_2$. □

Proof of Theorem 2. Let $n_i > m_i > 0$, $(n_i, m_i) = d_i$ $(i = 1, 2)$, $(d_1, d_2) = 1$ and $\langle n_1, m_1\rangle \neq \langle n_2, m_2\rangle$. In the notation of Lemma 5 and by virtue of that lemma the polynomials $F_i/(t-1)(x-1)(x-t)$ $(i = 1, 2)$ are coprime, hence their resultant R with respect to x is non-zero. We set

$$\begin{aligned} S = &\left\{\left\langle \frac{-n_1}{m_1}, \frac{n_1 - m_1}{m_1}, \frac{-n_2}{m_2}, \frac{n_2 - m_2}{m_2}\right\rangle\right\} \\ &\cup \left\{\left\langle \frac{\zeta_{d_2}^{r_2 n_1} - 1}{1 - \zeta_{d_2}^{r_2 m_1}}, \frac{\zeta_{d_2}^{r_2 m_1} - \zeta_{d_2}^{r_2 n_1}}{1 - \zeta_{d_2}^{r_2 m_1}}, \frac{\zeta_{d_1}^{r_1 n_2} - 1}{1 - \zeta_{d_1}^{r_1 m_2}}, \frac{\zeta_{d_1}^{r_1 m_2} - \zeta_{d_1}^{r_1 n_2}}{1 - \zeta_{d_1}^{r_1 m_2}}\right\rangle : \right. \\ &\qquad\qquad \left. r_2 m_1 \not\equiv 0 \bmod d_2,\ r_1 m_2 \not\equiv 0 \bmod d_1\right\} \\ &\cup \left\{\left\langle \frac{t^{n_1} - 1}{1 - t^{m_1}}, \frac{t^{m_1} - t^{n_1}}{1 - t^{m_1}}, \frac{t^{n_2} - 1}{1 - t^{m_2}}, \frac{t^{m_2} - t^{n_2}}{1 - t^{m_2}}\right\rangle : R(t) = 0,\ t^{m_1} \neq 1 \neq t^{m_2}\right\}. \end{aligned}$$

We proceed to show that the set S has the property asserted in the theorem. Since $R \in \mathbb{Q}[t]$ we have $S \subset \overline{\mathbb{Q}}^4$. Assume that $\deg(T_1, T_2) \geqslant 3$. If (T_1, T_2) has a double zero ξ_0 we set

$$T_i^*(x) = \xi_0^{-n_i} T_i(\xi_0 x) \quad (i = 1, 2)$$

and from the equations $T_i^*(1) = 0 = \frac{dT_i^*}{dx}(1)$ $(i = 1, 2)$ we find that

$$a_i^* = -\frac{n_i}{m_i}, \quad b_i^* = \frac{n_i - m_i}{m_i} \quad (i = 1, 2),$$

hence $\langle a_1^*, b_1^*, a_2^*, b_2^*\rangle \in S$ and (2) holds with $u = \xi_0$.

If (T_1, T_2) has three distinct zeros ξ_0, ξ_1, ξ_2 we set

$$T_i^*(x) = \xi_0^{-n_i} T_i(\xi_0 x) \quad (i = 1, 2).$$

Changing, if necessary, the role of T_1 and T_2 we have one of the three cases:
(i) $(\xi_1/\xi_0)^{d_1} = 1$ and $(\xi_2/\xi_0)^{d_2} = 1$,
(ii) $(\xi_1/\xi_0)^{d_1} = 1$ and $(\xi_2/\xi_0)^{d_2} \neq 1$,
(iii) $(\xi_1/\xi_0)^{d_1} \neq 1$ and $(\xi_1/\xi_0)^{d_2} \neq 1$.

In case (i) we have $\xi_j/\xi_0 = \zeta_{d_j}^{r_j}$ $(j = 1, 2)$ and the equations $T_i^*(\xi_j/\xi_0) = 0$ $(i = 1, 2)$ give

$$a_i^* = \frac{\zeta_{d_{3-i}}^{r_{3-i}n_i} - 1}{1 - \zeta_{d_{3-i}}^{r_{3-i}m_i}}, \quad b_i^* = \frac{\zeta_{d_{3-i}}^{r_{3-i}m_i} - \zeta_{d_{3-i}}^{r_{3-i}n_i}}{1 - \zeta_{d_{3-i}}^{r_{3-i}m_i}}, \quad r_{3-i}m_i \not\equiv 0 \bmod d_{3-i} \quad (i = 1, 2).$$

Hence $\langle a_1^*, b_1^*, a_2^*, b_2^* \rangle \in S$ and (2) holds with $u = \xi_0$.

In case (ii) we have $(\xi_2/\xi_0)^{d_1} \neq 1$, since otherwise T_2 would have three common zeros with $x^{d_1} - \xi_0^{d_1}$, contrary to Theorem 1 of [4].

Hence $(\xi_2/\xi_0)^{d_i} \neq 1$ $(i = 1, 2)$ and the equations $T_i^*(\xi_2/\xi_0) = 0$ $(i = 1, 2)$ give

$$(\xi_2/\xi_0)^{m_1} \neq 1 \neq (\xi_2/\xi_0)^{m_2}$$

and

$$a_i^* = \frac{(\xi_2/\xi_0)^{n_i} - 1}{1 - (\xi_2/\xi_0)^{m_i}}, \quad b_i^* = \frac{(\xi_2/\xi_0)^{m_i} - (\xi_2/\xi_0)^{n_i}}{1 - (\xi_2/\xi_0)^{m_i}}.$$

The polynomials $T_i^*/(x - 1)(x - \xi_2/\xi_0)$ $(i = 1, 2)$ have a common zero ξ_1/ξ_0, hence $R(\xi_2/\xi_0) = 0$. It follows that $\langle a_1^*, b_1^*, a_2^*, b_2^* \rangle \in S$ and (2) holds with $u = \xi_0$.

In case (iii) we have $(\xi_1/\xi_0)^{d_i} \neq 1$ $(i = 1, 2)$ and we reach the desired conclusion replacing in the above argument ξ_2 by ξ_1. □

Proof of Corollary 1. Since f and $f(x^d)$ have for every $f \in \mathbb{C}[x]$ and every $d \in \mathbb{N}$ the same number of non-zero coefficients we may assume that $(n_1, m_1, n_2, m_2) = 1$. If $T_1 = T_2$ then $(T_1, T_2) = T_1$ has three non-zero coefficients. If $T_1 \neq T_2$, but $\langle n_1, m_1 \rangle = \langle n_2, m_2 \rangle$, then by Theorem 2 of [4]

$$(T_1, T_2) = \big((a_1 - a_2)x^{m_1} + b_1 - b_2, (a_1 - a_2)x^{n_1} + a_1 b_2 - a_2 b_1\big)$$

has at most two non-zero coefficients. If $\langle n_1, m_1 \rangle \neq \langle n_2, m_2 \rangle$ then by Theorem 2 either $\deg(T_1, T_2) \leqslant 2$, or (2) holds. However in the latter case

$$\operatorname{inv} T_i = \operatorname{inv} T_i^* \in \overline{\mathbb{Q}} \quad (i = 1, 2)$$

and

$$T_1(0)^{-\deg T_2} T_2(0)^{\deg T_1} = T_1^*(0)^{-\deg T_2} T_2^*(0)^{\deg T_1} \in \overline{\mathbb{Q}}.$$ □

Proof of Corollary 2. The second equality is clear. In order to prove the first, note that $A(3, 3, \overline{\mathbb{Q}}) \geqslant 3$. On the other hand, if (T_1, T_2) has more than three non-zero coefficients, then by Corollary 1,

$$\operatorname{inv} T_i \in \overline{\mathbb{Q}} \quad (i = 1, 2),$$

hence

$$T_i = u_i^{\deg T_i} T_i^{**}\Big(\frac{x}{u_i}\Big), \quad \text{where} \quad u_i \in \mathbb{C}^*,\ T_i^{**} \in \overline{\mathbb{Q}}[x].$$

Moreover, also by Corollary 1,

$$\Big(\frac{u_2}{u_1}\Big)^{\deg T_1 \deg T_2} T_1^{**}(0)^{-\deg T_2} T_2^{**}(0)^{\deg T_1} \in \overline{\mathbb{Q}},$$

hence $v = u_2/u_1 \in \overline{\mathbb{Q}}$ and (T_1, T_2) has the same number of non-zero coefficients as $(T_1^{**}, T_2^{**}(x/v))$, where both terms belong to $\overline{\mathbb{Q}}[x]$. □

Lemma 6. *Let n, m be positive integers, $n > m$ and $a, b \in K^*$, where K is a finite extension of $\mathbb{Q}$. If F is a monic factor of $x^{n/(n,m)} + ax^{m/(n,m)} + b$ in $K[x]$ of maximal possible degree $d \leqslant 2$ and $n/(n,m) > \max\{6, 9 - 3d\}$, then*

$$\frac{x^n + ax^m + b}{F(x^{(n,m)})}$$

is reducible over K if and only if there exists a positive integer $l \mid (n,m)$ such that

$$a = u^{(n-m)/l} a_0, \quad b = u^{n/l} b_0, \quad F = u^{d(n,m)/l} F_0\Big(\frac{x}{u^{(n,m)/l}}\Big),$$

where $u \in K^*$, $\langle a_0, b_0, F_0\rangle \in F^d_{n/l,m/l}(K)$ and $F^d_{n/l,m/l}(K)$ is a certain finite set, possibly empty.

Proof. See [3], Theorem 3. □

Lemma 7. *Let $a, b \in K^*$, $n > m > 0$, $d = (n,m)$. Let $f(x)$ be a factor of $x^{n/d} + ax^{m/d} + b$ of degree at most 2. If $n > 2d$, then (n,m) is the greatest common divisor of the exponents of powers of x occuring with non-zero coefficients in $(x^n + ax^m + b)/f(x^{(n,m)}) =: Q(x)$.*

Proof. We may assume that f is monic and $d = 1$. If $f(x) = 1$ the assertion is obvious. If $f(x) = x - c$, then $Q(x)$ contains terms x^{n-1} and cx^{n-2}, unless $m = n - 1$ and $a = -c$. But in the latter case $x - c \mid b$, which is impossible. If $f(x) = x^2 - px - q$, we first observe that $p \neq 0$. Otherwise, we should have $q^{n/2} + aq^{m/2} + b = 0$ and also $(-1)^n q^{n/2} + a(-1)^m q^{m/2} + b = 0$, which, since at least one of the numbers n, m is odd, gives $ab = 0$. Now $(x^n + ax^m + b)/(x^2 - px - q)$ contains the terms x^{n-2} and px^{n-3}, unless $m = n - 1$ and $a = -p$. It also contains the terms $-b/q$ and $(b/q^2)px$, unless $m = 1$, $a = (b/q)p$. However $m = n - 1$ and $m = 1$ give $n = 2$, contrary to the assumption. □

Lemma 8. *If $n > m > 0$, $n > 3$, $abc \neq 0$, then $(x^n + ax^m + b)(x - c)$ has six non-zero coefficients, unless either $m = n - 1$ or $m = 1$, when there are at least four non-zero coefficients. Only in the former case does x^{n-1} occur with a non-zero coefficient.*

Proof. We have

$$(x^n + ax^m + b)(x - c) = x^{n+1} - cx^n + ax^{m+1} - ax^m + bx - cb.$$

The cancellation can occur only between the second and the third term (if $m = n - 1$), or between the fourth and the fifth term (if $m = 1$). □

Lemma 9. *If $n > m > 0$, $n > 6$, $abpq \neq 0$, then $(x^n + ax^m + b)(x^2 - px + q)$ has nine non-zero coefficients, unless $m \geqslant n-2$ or $m \leqslant 2$, when there are at most eight. If $m = n-1$ there are at least five non-zero coefficients, including that of x^{n-1}; if $m = n - 2$ there are at least seven non-zero coefficients, including that of x^{n-2}. If $m \leqslant 2$ the coefficients of x^{n-1} and x^{n-2} are zero.*

Proof. We have

$$\begin{aligned}\big(x^n + ax^m + b\big)\big(x^2 - px + q\big)\\ = x^{n+2} - px^{n+1} + qx^n + ax^{m+2} - apx^{m+1} + aqx^m + bx^2 - bpx + bq.\end{aligned}$$

The cancellation can occur only if $m \geqslant n - 2$ or $m \leqslant 2$ and all the assertions are easily checked. □

Lemma 10. *Let $d_i = (n_i, m_i)$ $(i = 1, 2)$ and let $f_i(x)$ be a monic factor of degree $\leqslant 2$ of $x^{n_i/d_i} + a_i x^{m_i/d_i} + b_i$. If $n_i/d_i > 6$ and*

$$\frac{x^{n_1} + a_1 x^{m_1} + b_1}{f_1\big(x^{d_1}\big)} = \frac{x^{n_2} + a_2 x^{m_2} + b_2}{f_2\big(x^{d_2}\big)}, \tag{17}$$

then

$$x^{n_1} + a_1 x^{m_1} + b_1 = x^{n_2} + a_2 x^{m_2} + b_2. \tag{18}$$

Proof. By Lemma 7, $d_1 = d_2$, hence we may assume without loss of generality that $d_1 = d_2 = 1$. Then the equality (17) gives

$$\big(x^{n_1} + a_1 x^{m_1} + b_1\big) f_2(x) = \big(x^{n_2} + a_2 x^{m_2} + b_2\big) f_1(x) \tag{19}$$

and we may assume without loss of generality that $\deg f_1 \geqslant \deg f_2$. Moreover, since (19) is equivalent to

$$\begin{aligned}\big(x^{n_1} + a_1 b_1^{-1} x^{n_1 - m_1} + b_1^{-1}\big)\frac{x^{\deg f_2} f_2(x^{-1})}{f_2(0)}\\ = \big(x^{n_2} + a_2 b_2^{-1} x^{n_2 - m_2} + b_2^{-1}\big)\frac{x^{\deg f_1} f_1(x^{-1})}{f_1(0)},\end{aligned}$$

we may assume that

$$2m_2 \geqslant n_2. \tag{20}$$

If $\deg f_2 = 0$, then the left hand side of (19) has only three non-zero coefficients, thus by Lemmas 8 and 9 applied to the right hand side $\deg f_1 = 0$ and (18) follows.

If $\deg f_2 = 1 < 2 = \deg f_1$, then the left hand side of (19) has at most six non-zero coefficients, which by Lemma 9 and condition (20) gives $m_2 = n_2 - 1$. Since $n_i > 6$

taking the residues $\bmod x^4$ of both sides of (19) we obtain

$$(a_1x^{m_1}+b_1)f_2(x)\equiv b_2f_1(x)\bmod x^4, \tag{21}$$

hence $m_1=1$, (21) is an equality and subtracting it from (19) gives

$$x^{n_1}f_2(x)=\left(x^{n_2}+a_2x^{n_2-1}\right)f_1(x),$$

a contradiction $\bmod f_1$.

If $\deg f_2=1=\deg f_1$, then $n_1=n_2$. If $m_2\neq n_2-1$, then by Lemma 8 and (20) the right hand side of (19) has six non-zero coefficients, thus also on the left hand side no terms coalesce and we have $b_1f_2=b_2f_1$, hence $f_2=f_1$ and (18) follows. If $m_2=n_2-1$, then on the right hand side of (19) we have five or four non-zero coefficients, including that of x^{n_2-1}, hence by Lemma 8, $m_1=n_1-1$. Taking the residues of both sides of (19) $\bmod x^3$ we find $b_1f_2=b_2f_1$, hence $f_2=f_1$ and (18) follows. If $\deg f_1=\deg f_2=2$, then again $n_1=n_2$. If $m_2<n_2-2$, then on the right hand side of (19) we have nine non-zero coefficients, hence also on the left hand side no two terms coalesce and taking residues $\bmod x^3$ we obtain $b_1f_2=b_2f_1$, hence $f_2=f_1$ and (18) follows. If $m_2\geqslant n_2-2$, then by Lemma 9 the number of non-zero coefficients on the right hand side of (19) is at most eight and x^{m_2} occurs with a non-zero coefficient, hence also on the left hand side we have at most eight non-zero coefficients and either x^{n_1-1} or x^{n_1-2} occurs with a non-zero coefficient. Again by Lemma 9, $m_1\geqslant n_1-2$. Taking the residues of both sides of (19) $\bmod x^3$ we find $b_1f_2=b_2f_1$, hence $f_2=f_1$ and (18) follows. □

Proof of Theorem 3. Put

$$F_{n,m}(K)=K\cap\left\{P_{n,m}(\zeta_q^r):0\leqslant r<q,\ 1\neq\zeta_q^{rm}\neq\zeta_q^{rn}\neq 1\right\}.$$

The set $F_{n,m}(K)$ is finite since by Lemma 2 the condition $P_{n,m}(\zeta_q^r)\in K$ implies

$$\text{either } \frac{q}{(q,r)}=10 \quad\text{or}\quad \frac{1}{2}\varphi\left(\frac{q}{(q,r)}\right)\leqslant[K:\mathbb{Q}]$$

and this leaves only finitely many possibilities for ζ_q^r. We set

$$E_{n,m}(K)=F_{n,m}(K)\cup\bigcup_{d\leqslant 2}\bigcup_{l\mid(n,m)}\bigcup_{\langle a_0,b_0,F_0\rangle\in F^d_{n/l,m/l}(K)}\left\{a_0^{-n/(n,m)}b_0^{(n-m)/(n,m)}\right\},$$

where $F^d_{\nu,\mu}(K)$ are as in Lemma 6.

Now, let $d_i=(n_i,m_i)$ and let f_i be a monic polynomial over K of maximal possible degree $\delta_i\leqslant 2$ dividing $T_i\left(x^{1/d_i}\right)$ $(i=1,2)$. We may assume without loss of generality that $n_2/d_2\leqslant n_1/d_1$.

If $n_2/d_2\leqslant 9$, then, since $\operatorname{inv}T_2\notin F_{n_2,m_2}(K)$, by Theorem 1 we have

$$\deg(T_1,T_2)\leqslant n_2/d_2\leqslant 9. \tag{22}$$

If $n_2/d_2>9$, then by Lemma 6 either $T_i/f_i\left(x^{d_i}\right)$ is irreducible over K or there exist an integer $l\mid d_i$, an element u of K^* and $\langle a_0,b_0,F_0\rangle\in F^{\delta_i}_{n_i/l,m_i/l}(K)$ such that

$$T_i(x)=x^{n_i}+u^{(n_i-m_i)/l}a_0x^{m_i}+u^{n_i/l}b_0,\quad f_i=u^{\delta_id_i/l}F_0\left(\frac{x}{u^{d_i/l}}\right).$$

These conditions give

$$\operatorname{inv} T_i = a_0^{-n_i/d_i} b_0^{(n_i-m_i)/d_i} \in E_{n_i,m_i}(K),$$

contrary to the assumption. Therefore $T_i/f_i\left(x^{d_i}\right)$ is irreducible over K for $i = 1, 2$ and we have

$$\text{either } T_1/f_1(x^{d_1}) = T_2/f_2(x^{d_2}) \quad \text{or} \quad \left(T_1/f_1(x^{d_1}),\, T_2/f_2(x^{d_2})\right) = 1.$$

In the former case we have $T_1 = T_2$ by Lemma 10; in the latter case

$$(T_1, T_2) = \frac{\left(T_1,\, f_2(x^{d_2})\right)\left(T_2,\, f_1(x^{d_1})\right)}{\left(f_1(x^{d_1}),\, f_2(x^{d_2})\right)}. \tag{23}$$

However, by Lemma 3 if $\deg f_{3-i} = 1$, or if $\deg f_{3-i} = 2$ and $f'_{3-i}(0) = 0$ and by Theorem 1 otherwise, we have

$$\deg\left(T_i,\, f_{3-i}(x^{d_{3-i}})\right) \leqslant \deg f_{3-i} \leqslant 2,$$

which by (23) gives

$$\deg(T_1, T_2) \leqslant 2 + 2 = 4. \tag{24}$$

The alternative (22) or (24) gives the theorem. □

We shall now give the promised examples.

Example 1. Let $n_i > m_i > 0$, $d_i = (n_i, m_i)$, $0 \not\equiv m_i \not\equiv n_i \not\equiv 0 \bmod d_{3-i}$ for $i = 1, 2$, $(d_1, d_2) = 1$, and

$$T_i(x) = x^{n_i} + \frac{\zeta_{d_{3-i}}^{r_{3-i}n_i} - 1}{1 - \zeta_{d_{3-i}}^{r_{3-i}m_i}}\, x^{m_i} + \frac{\zeta_{d_{3-i}}^{r_{3-i}m_i} - \zeta_{d_{3-i}}^{r_{3-i}n_i}}{1 - \zeta_{d_{3-i}}^{r_{3-i}m_i}} \quad (i = 1, 2),$$

where r_{3-i} is chosen so that

$$1 \neq \zeta_{d_{3-i}}^{r_{3-i}m_i} \neq \zeta_{d_{3-i}}^{r_{3-i}n_i} \neq 1 \quad (i = 1, 2).$$

Here (T_1, T_2) has the following distinct zeros $1, \zeta_{d_1}^{r_1}, \zeta_{d_2}^{r_2}, \zeta_{d_1}^{r_1}\zeta_{d_2}^{r_2}$, hence

$$\deg(T_1, T_2) \geqslant 4.$$

If $n_2/d_2 = 2$ this shows that the second and the third inequality of (1) are exact in infinitely many essentially different cases and the condition for the first inequality is not superfluous.

Example 2. Let $T_1 = x^4 - 5x + 5$, $T_2 = x^{20} + 5^4x^{10} + 5^5$. Here $(T_1, T_2) = T_1$, hence

$$\deg(T_1, T_2) = 4 > n_2/d_2 + \min\{2, d_1\}.$$

This shows that the condition for the second inequality of (1) is not superfluous.

Example 3 (due to S. Chaładus [1]). Let

$$T_1 = x^7 + 9x^2 + 27 \quad \text{and} \quad T_2 = x^{15} - 27x^9 + 729.$$

Here

$$(T_1, T_2) = x^5 + 3x^4 + 6x^3 + 9x^2 + 9x + 9.$$

Since $\operatorname{inv} T_1 = 3$, $d_2 = 3$, and $P_{n_1,m_1}\left(\zeta_3^{\pm 1}\right) = 1$, in this case the first inequality of (1) is exact. Moreover (T_1, T_2) has six non-zero coefficients, which is the present record.

References

[1] S. Chaładus, Letter to the author of July 7, 1994.

[2] R. Dvornicich, *On an equation in cyclotomic numbers*. Acta Arith. 98 (2001), 71–94.

[3] A. Schinzel, *On reducible trinomials* III. Period. Math. Hungar. 43 (2001), 43–69; this collection: D14, 605–632.

[4] —, *On the greatest common divisor of two univariate polynomials* I. In: A Panorama of Number Theory or the View from Baker's Garden (ed. G. Wüstholz), Cambridge Univ. Press, Cambridge 2002, 337–352; this collection: D15, 632–645.

Andrzej Schinzel
Selecta

Originally published in
Functiones et Approximatio. Commentarii Mathematici
XXXV (2006), 271–306

On the reduced length of a polynomial with real coefficients

To Professor Eduard Wirsing
with best wishes for his 75th birthday

Abstract. The length $L(P)$ of a polynomial P is the sum of the absolute values of the coefficients. For $P \in \mathbb{R}[x]$ the properties of $l(P)$ are studied, where $l(P)$ is the infimum of $L(PG)$ for G running through monic polynomials over $\mathbb{R}$.

We shall consider only polynomials with real coefficients. For such a polynomial $P = \sum_{i=0}^{d} a_i x^{d-i}$ the length $L(P)$ is defined by the formula

$$L(P) = \sum_{i=0}^{d} |a_i|.$$

A. Dubickas [1] has introduced the reduced length by the formula

$$\widehat{l}(P) = \inf_{G \in \widehat{\Gamma}} L(PG),$$

where

$$\widehat{\Gamma} = \left\{ \sum_{i=0}^{n} b_i x^{n-i} \in \mathbb{R}[x], \text{ where } b_0 = 1 \text{ or } b_n = 1 \right\}.$$

It follows, see [1], p. 3, that

$$\widehat{l}(P) = \min\{l_0(P), l_0(P^*)\},$$

where

$$l_0(P) = \inf_{G \in \Gamma_0} L(PG), \quad \Gamma_0 = \left\{ \sum_{i=0}^{n} b_i x^{n-i} \in \mathbb{R}[x],\ b_n = 1 \right\}, \quad P^* = x^{\deg P} P(x^{-1}).$$

Since polynomials with the leading coefficient 1 have a name (monic) and polynomials with the constant term 1 have no name, I prefer to work with

$$l(P) = l_0(P^*) = \inf_{G \in \Gamma} L(PG), \quad \Gamma = \left\{ \sum_{i=0}^{n} b_i x^{n-i} \in \mathbb{R}[x],\ b_0 = 1 \right\}$$

Dubickas's results about l_0 translated in the language of l give the following

Proposition A. *Suppose that $\omega, \eta, \psi \in \mathbb{R}$, $\nu \in \mathbb{C}$, $\overline{\nu}$ is the complex conjugate to ν, $|\omega| \geqslant 1$, $|\eta| < 1$, $|\nu| < 1$, then for every $Q \in \mathbb{R}[x]$*

(i) $l(\psi Q) = |\psi| l(Q)$,
(ii) $l(x + \omega) = 1 + |\omega|$,
(iii) *if* $T(x) = Q(x)(x - \eta)$, *then* $l(T) = l(Q)$,
(iv) *if* $T(x) = Q(x)(x - \nu)(x - \overline{\nu})$, *then* $l(T) = l(Q)$.

We shall prove the following

Proposition. *For all monic polynomials P, Q in $\mathbb{R}[x]$ and all positive integers k*

(i) $\max\{l(P), l(Q)\} \leqslant l(PQ) \leqslant l(P)l(Q)$,
(ii) $M(P) \leqslant l(P)$, *where M is the Mahler measure,*
(iii) $l(P(-x)) = l(P(x))$,
(iv) $l(P(x^k)) = l(P(x))$.

Theorem 1. *If $P \in \mathbb{R}[x]$ is monic of degree d with $P(0) \neq 0$, then $l(P) = \inf_{Q \in S_d(P)} L(Q)$, where $S_d(P)$ is the set of all monic polynomials Q over $\mathbb{R}$ divisible by P with $Q(0) \neq 0$ and with at most $d + 1$ non-zero coefficients, all belonging to the field $K(P)$, generated by the coefficients of P.*

Theorem 2. *If $P \in \mathbb{R}[x]$ has all zeros outside the unit circle, then $l(P)$ is attained and effectively computable, moreover $l(P) \in K(P)$ ($l(P)$ is attained means that $l(P) = L(Q)$, where $Q/P \in \Gamma$).*

Corollary 1. *If $P \in \mathbb{R}[x]$ has no zeros on the unit circle, then $l(P)$ is effectively computable.*

Theorem 3. *Let $P, Q \in \mathbb{R}[x]$, Q be monic and have all zeros on the unit circle. Then for all $m \in \mathbb{N}$*

$$l(PQ^m) = l(PQ).$$

Theorem 4. *If $P \in \mathbb{R}[x]$ is monic and have all zeros on the unit circle, then $\widehat{l}(P) = l(P) = 2$, with $l(P)$ attained, if and only if all zeros are roots of unity and simple.*

Theorem 5. *Let $P(x) = P_0(x)(x - \varepsilon)^e$, where $P_0 \in \mathbb{R}[x]$, $\varepsilon = \pm 1$, $e \in \mathbb{N}$ and all zeros of P_0 are outside the unit circle. Assume that the set Z of zeros of P_0 has a subset Z_0, possibly empty, such that its elements are real of the same sign and the elements of $Z \setminus Z_0$ are algebraically independent over $\mathbb{Q}(Z_0)$. Then $l(P)$ can be effectively computed. Moreover, if* $\deg P_0 = d_0$, *then*

$$l(P) \leqslant \inf_{Q \in S_{d_0}(P_0)} \big\{ L(Q) + \big| Q(\varepsilon) \big| \big\}.$$

For quadratic polynomials P Theorems 2, 4 and 5 together with Proposition A(iii) and (iv) exhaust all possibilities, so that $l(P)$ can be effectively computed. A more precise information is given by the following

Theorem 6. *If $P(x) = (x-\alpha)(x-\beta)$, where $|\alpha| \geqslant |\beta| \geqslant 1$, then*

$$l(P) \geqslant 2|\alpha|$$

with the equality attained, if and only if $|\beta| = 1$.

Corollary 2. *If $P \in \mathbb{R}[x]$ is of degree at most two with no zeros inside the unit circle, then*

$$l(P) \in K(P).$$

Corollary 3. *If $P(x) = (x-\alpha)(x-\beta)$, where $|\alpha| \geqslant |\beta| \geqslant 0$, then*

$$\widehat{l}(P) = \begin{cases} |\alpha\beta| & \text{if } |\beta| > 1, \\ 2|\alpha| & \text{if } |\beta| = 1, \\ |\alpha| + \min\{1, |\alpha\beta|\} & \text{if } |\alpha| > 1 > |\beta|, \\ 2 & \text{if } |\alpha| = 1, \\ 1 & \text{if } |\alpha| < 1. \end{cases}$$

Corollary 4. *The function $\widehat{l}$ is not submultiplicative.*

The last corollary is of interest, because of Proposition, part (i).

The problem of computing $l(P)$ for cubic polynomials remains open already for $P = 2x^3 + 3x^2 + 4$. Another open question is whether $l(P) \in K(P)$ for all $P \in \mathbb{R}[x]$ with no zeros inside the unit circle.

We begin with

Proof of Proposition. We have by definition for all monic polynomials R, S in $\mathbb{R}[x]$

$$l(P) \leqslant L(PQR), \quad l(PQ) \leqslant L(PQRS) \leqslant L(PR)L(QS),$$

hence

$$l(P) \leqslant \inf_{R \in \Gamma} L(PQR) = l(PQ),$$

$$l(PQ) \leqslant \inf_{R \in \Gamma} L(PR) \inf_{S \in \Gamma} L(QS) = l(P)l(Q).$$

This proves (i). As to (ii) we have for every R in $\mathbb{R}[x]$

$$M(R) \leqslant L(R)$$

(see [4]), hence

$$M(P) \leqslant M(PQ) \leqslant L(PQ),$$

thus

$$M(P) \leqslant \inf_{Q \in \Gamma} L(PQ) = l(P)$$

and (ii) holds. The statement (iii) follows from

$$L\big(P(-x)\big) \leqslant L\big(P(-x)Q(-x)(-1)^{\deg Q}\big) = L(PQ),$$

whence

$$l\big(P(-x)\big) \leqslant \inf_{Q\in\Gamma} L(PQ) = l(P).$$

Similarly,

$$l\big(P(x^k)\big) \leqslant L\big(P(x^k)Q(x^k)\big) = L(PQ),$$

whence

$$l\big(P(x^k)\big) \leqslant \inf_{Q\in\Gamma} L(PQ) = l(P). \tag{1}$$

Finally, if

$$P(x^k)Q(x) = \sum_{i=0}^{k-1} x^i A_i(x^k), \quad \text{where} \quad A_i \in \mathbb{R}[x], \tag{2}$$

let $A_i = Q_i P + R_i$, where Q_i, $R_i \in \mathbb{R}[x]$ and $\deg R_i < \deg P$. It follows that

$$P(x^k) \;\Big|\; \sum_{i=0}^{k-1} x^i R_i(x^k)$$

and since the degree of the sum is less than that of $P(x^k)$, $R_i = 0$ $(0 \leqslant i < k)$. Let i be chosen so that $\deg x^i A_i(x^k)$ is the greatest. It follows from (2) that Q_i is monic. Hence, by (2)

$$L\big(P(x^k)Q(x)\big) \geqslant L(A_i) = L(PQ_i) \geqslant l(P),$$

thus $l(P(x^k)) \geqslant l(P)$, which together with (1) implies (iv). □

Remark. The above proof of (iv), simpler than author's original proof, has been kindly suggested by A. Dubickas.

For the proof of Theorem 2 we need two lemmas

Lemma 1. *Let $k \geqslant n$, $\boldsymbol{x} = (x_1, \ldots, x_n)$, $L_i(\boldsymbol{x})$ for $i \leqslant k$ be linear forms over $\mathbb{R}$; $L_1, \ldots, L_n$ linearly independent, $a_i \in \mathbb{R}$ $(1 \leqslant i \leqslant k)$. Then*

$$S(\boldsymbol{x}) = \sum_{i=1}^{k} |L_i(\boldsymbol{x}) + a_i|$$

attains its infimum.

Proof. Let $L_i(\boldsymbol{x}) = \sum_{j=1}^{n} a_{ij}x_j$ $(1 \leqslant i \leqslant k)$, $A = \max_{i,j\leqslant n} |a_{ij}|$,

$$D = \big|\det(a_{ij})_{i,j\leqslant n}\big|, \quad s = \sum_{i=1}^{k} |a_i|.$$

Let s_0 be the infimum of $S(\boldsymbol{x})$ in the hypercube (degenerated if $s = 0$)

$$H : \max_{1 \leqslant i \leqslant n} |x_i| \leqslant \frac{2n^{(n-1)/2} s A^{n-1}}{D}.$$

Since H is compact, there exists $\boldsymbol{x}_0 \in H$ such $S(\boldsymbol{x}_0) = s_0$. We shall show that $s_0 = \inf_{\boldsymbol{x} \in \mathbb{R}^n} S(\boldsymbol{x})$. Indeed, if for some $\boldsymbol{x}_1 \in \mathbb{R}^n$

$$S(\boldsymbol{x}_1) < s_0, \tag{3}$$

then

$$\sum_{i=1}^{n} |L_i(\boldsymbol{x}_1)| < s_0 + s \leqslant 2s.$$

Solving the system $L_i(\boldsymbol{x}) = L_i(\boldsymbol{x}_1)$ $(1 \leqslant i \leqslant n)$ by means of Cramer's formulae and using Hadamard's inequality to estimate the relevant determinants we obtain

$$\max_{1 \leqslant i \leqslant n} |x_{1i}| < \frac{2n^{(n-1)/2} s A^{n-1}}{D},$$

hence $\boldsymbol{x}_1 \in H$, a contradiction with (3) and the definition of s_0. □

Lemma 2. *Let $k \geqslant n$, $\boldsymbol{x} = (x_1, \ldots, x_n)$, K be a subfield of $\mathbb{R}$, $L_1(\boldsymbol{x}), \ldots, L_k(\boldsymbol{x})$ be linear forms over K, n of them linearly independent, $a_i \in K$. There exists a point $\boldsymbol{x}_0 \in K^n$ in which $S(\boldsymbol{x}) = \sum_{i=1}^{k} |L_i(\boldsymbol{x}) + a_i|$ attains its infimum over $\mathbb{R}^n$ and $L_i(\boldsymbol{x}_0) + a_i = 0$, for n indices $i = i_1, i_2, \ldots, i_n$ such that $L_{i_1}, L_{i_2}, \ldots, L_{i_n}$ are linearly independent.*

Proof by induction on k. If $k = 1$ we have $n = 1$ and the assertion is trivial. Assume it is true for $k - 1$ forms and consider the case of k forms, $k \geqslant 2$. If one of them, say L_k, is identically 0, then among $L_1, \ldots, L_{k-1}$ there are n linearly independent, hence $k - 1 \geqslant n$ and applying the inductive assumption to $L_1, \ldots, L_{k-1}$ we obtain the assertion. Therefore, we assume that all forms $L_1, \ldots, L_k$ are non-zero. Suppose that $\inf S(\boldsymbol{x}) = S(\boldsymbol{x}_1)$ and $L_i(\boldsymbol{x}_1) + a_i \neq 0$ for all $i \leqslant k$. Then there is an $\varepsilon > 0$ such that $|\boldsymbol{x} - \boldsymbol{x}_1| < \varepsilon$ implies $\operatorname{sgn}(L_i(\boldsymbol{x}) + a_i) =: \varepsilon_i$ for all $i \leqslant k$. We have

$$S(\boldsymbol{x}) = \sum_{i=1}^{k} \varepsilon_i (L_i(\boldsymbol{x}) + a_i) = M(\boldsymbol{x} - \boldsymbol{x}_1) + S(\boldsymbol{x}_1),$$

where

$$M(\boldsymbol{y}) = \sum_{i=1}^{k} \varepsilon_i L_i(\boldsymbol{y}).$$

If $M \neq 0$, then there exists a point $\boldsymbol{y}_0$ with $|\boldsymbol{y}_0| < \varepsilon$ and $M(\boldsymbol{y}) < 0$, hence taking $\boldsymbol{x}_2 = \boldsymbol{x}_1 + \boldsymbol{y}_0$ we obtain $S(\boldsymbol{x}_2) < S(\boldsymbol{x}_1)$, a contradiction. Thus either $L_{i_1}(\boldsymbol{x}_1) + a_{i_1} = 0$ for a certain i_1, or $M = 0$. In the latter case we take the point $\boldsymbol{x}_2$ nearest to $\boldsymbol{x}_1$ (or one of these) with $L_{i_2}(\boldsymbol{x}_2) + a_{i_2} = 0$ for a certain i_2. Since the hyperplanes $L_i(x) + a_i = 0$ either are disjoint with the ball $|\boldsymbol{x} - \boldsymbol{x}_1| \leqslant |\boldsymbol{x}_2 - \boldsymbol{x}_1|$, or are tangent to it, taking $\langle \boldsymbol{x}_3, i_3 \rangle$

equal either to $\langle \boldsymbol{x}_1, i_1\rangle$ or to $\langle \boldsymbol{x}_2, i_2\rangle$ we obtain $S(\boldsymbol{x}_3) = S(\boldsymbol{x}_1)$ and $L_{i_3}(\boldsymbol{x}_3) + a_{i_3} = 0$. Without loss of generality we may assume that $i_3 = k$ and L_k is of positive degree in x_n. The equation $L_k(\boldsymbol{x}) + a_k = 0$ is equivalent to $x_n = C(x_1, \ldots, x_{n-1}) + c$, where C is a linear form over K and $c \in K$. We now apply the inductive assumption to the forms $L'_i = L_i(x_1, \ldots, x_{n-1}, C(x_1, \ldots, x_{n-1}))$ and numbers $a'_i = a_i + L_i(0, \ldots, 0, c)$ $(1 \leqslant i \leqslant k-1)$. By virtue of the theorem about the rank of the product of matrices, the number of linearly independent among forms L'_i is $n-1$. By the inductive assumption there exists a point $\boldsymbol{x}'_0 \in K^{n-1}$ such that $\sum_{i=1}^{k-1} |L'_i(\boldsymbol{x}') + a'_i| = S'(\boldsymbol{x}')$ attains at $\boldsymbol{x}'_0$ its infimum over $\mathbb{R}^{n-1}$ and $L'_i(\boldsymbol{x}'_0) + a'_i = 0$ for $n-1$ indices $i = i'_1, \ldots, i'_{n-1}$ such that $L'_{i'_1}, \ldots, L'_{i'_{n-1}}$ are linearly independent. By the definition of L'_i and a'_i we have

$$S(\boldsymbol{x}_3) = S'(x_{3,1}, \ldots, x_{3,n-1}) \geqslant \inf_{\boldsymbol{x}' \in \mathbb{R}^{n-1}} S'(\boldsymbol{x}') \geqslant \inf_{\boldsymbol{x} \in \mathbb{R}^n} S(\boldsymbol{x}) = S(\boldsymbol{x}_3),$$

hence

$$S'(\boldsymbol{x}'_0) = \inf_{\boldsymbol{x}' \in \mathbb{R}^{n-1}} S'(\boldsymbol{x}') = \inf_{\boldsymbol{x} \in \mathbb{R}^n} S(\boldsymbol{x}).$$

Moreover, $L'_{i'_j}(\boldsymbol{x}'_0) + a'_{i'_j} = 0$ implies

$$L'_{i'_j}(x'_{0,1}, \ldots, x'_{0,n-1}, C(\boldsymbol{x}'_0)) + a_{ij} = 0$$

and the linear independence of $L'_{i'_1}, \ldots, L'_{i'_{n-1}}$ implies the linear independence of the forms $L_{i'_1}, \ldots, L_{i'_{n-1}}$. The latter forms are also linearly independent with L_k since the identity

$$L_1(x_1, \ldots, x_n) = \sum_{j=1}^{n-1} c_j L_{i'_j}(x_1, \ldots, x_n), \quad c_j \in \mathbb{R},$$

gives on substitution $x_n = C(x_1, \ldots, x_{n-1})$

$$0 = \sum_{j=1}^{n-1} c_j L'_{i_j}(x_1, \ldots, x_n), \quad \text{hence } c_j = 0 \ (1 \leqslant j < n).$$

Taking $\boldsymbol{x}_0 = (x'_{0,1}, \ldots, x'_{0,n-1}, C(x'_0))$, $i_j = i'_j$ $(1 \leqslant j < n)$, $i_n = k$ we obtain the inductive assertion. □

Proof of Theorem 1. We have by definition

$$l(P) = \inf L(PG),$$

where G runs through all monic polynomials. Let

$$P = x^d + \sum_{i=1}^{d} a_i x^{d-i}, \quad G = x^n + \sum_{i=1}^{n} x_i x^{n-i}.$$

We have

$$PG = x^{n+d} + \sum_{i=1}^{n+d} b_i x^{n+d-i},$$

where, with $a_0 = 1$, for $i \leqslant d$

$$b_i = a_i + \sum_{j=1}^{\min\{i,n\}} a_{i-j} x_j,$$

for $i > d$

$$b_i = \sum_{j=i-d}^{\min\{i,n\}} a_{i-j} x_j.$$

Therefore,

$$l(P) = 1 + \inf_{n,\boldsymbol{x}\in\mathbb{R}^n} \left\{ \sum_{i=1}^{d} |L_i(\boldsymbol{x}) + a_i| + \sum_{i=d+1}^{d+n} |L_i(\boldsymbol{x})| \right\},$$

where

$$L_i(\boldsymbol{x}) = \sum_{j=\max\{1,i-d\}}^{\min\{i,n\}} a_{i-j} x_j.$$

The forms L_i satisfy the assumptions of Lemma 2. Indeed, the n forms $L_{d+1}, \ldots, L_{d+n}$ are linearly independent, since $L_{d+1}(\boldsymbol{x}) = \ldots = L_{d+n}(\boldsymbol{x}) = 0$ gives $PG \equiv 0 \pmod{x^n}$, hence $G \equiv 0 \pmod{x^n}$, i.e. $x_1 = \ldots = x_n = 0$. Applying Lemma 2 and Proposition A(iii) with $\eta = 0$ we obtain that for a given n, PG with the minimal length occurs in $S_d(P)$. □

For the proof of Theorem 2 we need

Definition 1. Let $P = \prod_{s=1}^{r} (x - \alpha_s)^{m_s}$, where α_s are distinct and non-zero, $m_s \in \mathbb{N}$ $(1 \leqslant s \leqslant r)$, $m_1 + \ldots + m_r = d \geqslant \delta$, $n_0 > n_1 > \ldots > n_{\delta-1} > n_\delta \geqslant 0$ be integers. If $1 \leqslant i \leqslant d$, $0 \leqslant j \leqslant \delta$, then i can be written in the form $i = m_1 + \ldots + m_{s-1} + g$ for some $1 \leqslant s \leqslant r$ and $1 \leqslant g \leqslant m_s$. We put

$$c_{ij} = \alpha_s^{n_j} \prod_{f=0}^{g-2} (n_j - n_f), \text{ where the empty product is 1}$$

and for $\nu = 0, 1$

$$C(P; n_0, \ldots, n_\delta) = (c_{ij})_{\substack{1\leqslant i\leqslant d,\\ 0\leqslant j\leqslant\delta}}, \quad C_\nu(P; n_\nu, \ldots, n_{\delta-1+\nu}) = (c_{ij})_{\substack{1\leqslant i\leqslant d\\ \nu\leqslant j<\delta+\nu}}.$$

Definition 2. $T_d(P) = \{Q \in S_d(P) : Q = x^{n_0} + \sum_{j=1}^{\delta} b_j x^{n_j}$, where $n_0 > n_1 > \ldots > n_\delta = 0$, $\prod_{j=1}^{\delta} b_j \neq 0$, $\operatorname{rank} C_0(P; n_0, \ldots, n_{\delta-1}) = \delta = \operatorname{rank} C_1(P; n_1, \ldots, n_\delta)$, $L(Q) \leqslant L(P)\}$.

Lemma 3. *We have for* $x_j \in \mathbb{C}$

$$\sum_{j=0}^{d} x_j x^{n_j} \equiv 0 \pmod{P} \tag{4_1}$$

if and only if

$$\sum_{j=0}^{d} c_{ij} x_j = 0 \quad (1 \leqslant i \leqslant d). \tag{4_2}$$

Proof. Clearly the condition (4_1) is equivalent to

$$\sum_{j=0}^{d} x_j \binom{n_j}{g-1} \alpha_s^{n_j} = 0 \quad (1 \leqslant g \leqslant m_s,\ 1 \leqslant s \leqslant r),$$

that is to the vector equation

$$M\boldsymbol{x} = 0, \tag{5}$$

where $\boldsymbol{x} = (x_0, x_1, \ldots, x_d)^t$, $M = (m_{ij})_{\substack{1 \leqslant i \leqslant d \\ 0 \leqslant j \leqslant d}}$ and if $i = m_1 + \ldots + m_{s-1} + g$, $1 \leqslant g \leqslant m_s$, then

$$m_{ij} = \binom{n_j}{g-1} \alpha_s^{n_j}. \tag{6}$$

Now define the numbers b_{gh} by the equation

$$\prod_{f=0}^{g-2} (x - n_f) = \sum_{h=1}^{g} b_{gh} \binom{x}{h-1} \tag{7}$$

and put for $i = m_1 + \ldots + m_{s-1} + g$, $1 \leqslant g \leqslant m_s$, $1 \leqslant j \leqslant d$,

$$a_{ij} = \begin{cases} b_{gh} & \text{if } j = m_1 + \ldots + m_{s-1} + h,\ 1 \leqslant h \leqslant g, \\ 0 & \text{otherwise,} \end{cases} \tag{8}$$

$$A = (a_{ij})_{1 \leqslant i,j \leqslant d}. \tag{9}$$

The matrix A is lower triangular and non-singular, since $b_{gg} = (g-1)!$. Hence the equation (5) is equivalent to

$$AM\boldsymbol{x} = 0. \tag{10}$$

However, by (6)–(9) the element in i-th row ($1 \leqslant i \leqslant d$) and j-th column ($0 \leqslant j \leqslant d$) of AM for $i = m_1 + \ldots + m_{s-1} + g$, $1 \leqslant g \leqslant m_s$, is

$$\sum_{t=1}^{d} a_{it} m_{tj} = \sum_{h=1}^{g} b_{gh} \binom{n_j}{h-1} \alpha_s^{n_j} = \alpha_s^{n_j} \prod_{f=0}^{g-2} (n_j - n_f) = c_{ij},$$

hence (4_1) is equivalent to (4_2). □

Lemma 4. *We have* $\inf_{Q \in S_d(P)} L(Q) = \inf_{Q \in T_d(P)} L(Q)$.

Proof. Let P be as in Definition 1. We shall prove that for every $n \geqslant 0$

$$\inf_{\substack{Q \in S_d(P) \\ \deg Q = n+d}} L(Q) = \inf_{\substack{Q \in T_d(P) \\ \deg Q = n+d}} L(Q). \tag{11}$$

It follows from the proof of Theorem 1 that

$$\inf_{\substack{Q \in S_d(P) \\ \deg Q = n+d}} L(Q) = L(Q_0), \tag{12}$$

where

$$Q_0 = x^{n_0} + \sum_{j=1}^{\delta} b_j x^{n_j} \in K(P)[x], \quad \delta \leqslant d, \quad \prod_{j=1}^{\delta} b_j \neq 0, \tag{13}$$
$$n_0 > n_1 > \ldots > n_\delta = 0.$$

Let $L_i(\boldsymbol{x})$ be the linear forms defined in the proof of Theorem 1 and a_i have the meaning of that proof if $i \leqslant d$, $a_i = 0$ otherwise. We have

$$L(Q_0) = 1 + \inf_{\boldsymbol{x} \in \mathbb{R}^n} \sum_{i=1}^{n+d} |L_i(\boldsymbol{x}) + a_i|, \tag{14}$$

hence, by Lemma 2, the above infimum is attained at a point $\boldsymbol{x}_0$ such that for n indices $i_1, \ldots, i_n$ simultaneously $L_{i_j}(\boldsymbol{x}_0) + a_{i_j} = 0$ and $L_{i_1}, \ldots, L_{i_n}$ are linearly independent. Since the system of equations $L_{i_j}(\boldsymbol{x}_0) + a_{i_j} = 0$ $(1 \leqslant j \leqslant n)$ determines $\boldsymbol{x}_0$ uniquely, the coefficients of x^{n+d-i} in Q, where $i \neq i_1, i_2, \ldots, i_n$ (hence, in particular, $n + d - i = n_1, \ldots, n_\delta$) are uniquely determined by the condition $Q \equiv 0 \pmod P$, Q monic in $\mathbb{C}[x]$. On the other hand, if rank $C_0(P; n_0, \ldots, n_{\delta-1}) < \delta$, then there exists $[d_0, \ldots, d_{\delta-1}] \in \mathbb{C}^\delta \setminus \{\boldsymbol{0}\}$ such that

$$\sum_{j=0}^{\delta-1} c_{ij} d_j = 0 \quad (1 \leqslant i \leqslant d),$$

hence by Lemma 3

$$\sum_{j=0}^{\delta-1} d_j x^{n_j} \equiv 0 \pmod P. \tag{15}$$

If $d_0 = 0$, then

$$Q_1 := Q_0 + \sum_{j=1}^{\delta-1} d_j x^{n_j} \equiv 0 \pmod{P},$$

where the polynomial Q_1 is again monic, contrary to the uniqueness property. If $d_0 \neq 0$, then by the uniqueness property

$$Q_0 = d_0^{-1} \sum_{j=1}^{\delta-1} d_j x^{n_j},$$

hence $Q_0(0) = 0$, contrary to (13).

If rank $C_1(P; n_1, \ldots, n_\delta) < \delta$, then there exists $[e_1, \ldots, e_\delta] \in \mathbb{C}^\delta \setminus \{\mathbf{0}\}$ such that

$$\sum_{j=1}^{\delta} c_{ij} e_j = 0 \quad (1 \leqslant i \leqslant d),$$

hence by Lemma 3

$$\sum_{j=1}^{\delta} e_j x^{n_j} \equiv 0 \pmod{P}. \tag{16}$$

We have

$$Q_2 := Q_0 + \sum_{j=1}^{\delta} e_j x^{n_j} \equiv 0 \pmod{P}$$

and Q_2 is again monic, contrary to the uniqueness property.

In the remaining case

$$\operatorname{rank} C_0(P; n_0, \ldots, n_{\delta-1}) = \delta = \operatorname{rank} C_1(P; n_1, \ldots, n_\delta)$$

we have $Q_0 \in T_d(P)$, hence (11) holds. □

Lemma 5. *Let in the notation of Definition* 1, $i = m_1 + \ldots + m_{s(i)-1} + g(i)$, $1 \leqslant g(i) \leqslant m_{s(i)}$. *Then for every* $j \geqslant h \geqslant g(i) - 1$

$$|c_{ij}| \leqslant |c_{ih}| \max\left\{1, \frac{g(i)-1}{\log|\alpha_{s(i)}|}\right\}^{g(i)-1}. \tag{17}$$

Proof. For the sake of brevity, put $s(i) = s$, $g(i) = g$. For $g = 1$ we have $|c_{ij}| = |\alpha_s^{n_j}| \leqslant |\alpha_s^{n_h}| = |c_{ih}|$. Assume $g > 1$. For every $f \leqslant g - 2$ the function

$$\varphi(x) = \max\left\{1, \frac{g-1}{\log|\alpha_s|}\right\} |\alpha_s|^{(n_h - x)/(g-1)} - \frac{n_f - x}{n_f - n_h}$$

satisfies $\varphi(n_h) \geqslant 0$, $\varphi'(x) \leqslant 0$ for $x \leqslant n_h$. Hence $\varphi(n_j) \geqslant 0$,

$$\max\left\{1, \frac{g-1}{\log|\alpha_s|}\right\} |\alpha_s|^{n_h/(g-1)} (n_f - n_h) \geqslant |\alpha_s|^{n_j/(g-1)} (n_f - n_j)$$

and (17) follows on taking products over f from 0 to $g - 2$. □

Lemma 6. *Let $a, b, c, x \in \mathbb{R}$, $a > 1$, $b \geqslant 0$, $c > 0$, $x > 0$. If*

$$a^x/x^b \leqslant c, \tag{18}$$

then

$$x \leqslant \left(\frac{2b}{e \log a} + \sqrt{\frac{b^2}{e^2 (\log a)^2} + \frac{\log c}{\log a}} \right)^2 =: \psi(a, b, c). \tag{19}$$

The function ψ is decreasing in a, increasing in b and c.

Proof. Put $x = y^2$, $y > 0$. It follows from (18) that

$$y^2 \log a - 2b \log y \leqslant \log c$$

and, since $\log y \leqslant y/e$,

$$y^2 \log a - \frac{2b}{e} y \leqslant \log c.$$

Solving this inequality for y and squaring we obtain (19). □

Lemma 7. *For every subset I of $\{1, \dots, d\}$ of cardinality h we have*

$$\left| \det(c_{ij})_{\substack{i \in I \\ 1 \leqslant j \leqslant h}} \right| \leqslant h^{h/2} \prod_{i \in I} |\alpha_{s(i)}|^{n_{\max\{1, g(i)-1\}}} \prod_{f=0}^{g(i)-2} (n_f - n_h) \tag{20}$$

and

$$\left| \det(c_{ij})_{\substack{i \in I \\ 0 \leqslant j < h}} \right| \leqslant h^{h/2} \prod_{i \in I} |\alpha_{s(i)}|^{n_{g(i)-1}} \prod_{f=0}^{g(i)-2} (n_f - n_{h-1}). \tag{21}$$

Proof. For all $i \in I$ and $j \leqslant g(i) - 2$ we have $c_{ij} = 0$, while for $j > g(i) - 2$

$$|c_{ij}| = |\alpha_{s(i)}|^{n_j} \prod_{f=0}^{g(i)-2} (n_f - n_h) \leqslant \begin{cases} |\alpha_{s(i)}|^{n_{\max\{1, g(i)-1\}}} \prod_{f=0}^{g(i)-2} (n_f - n_h) & \text{if } 1 \leqslant j \leqslant h, \\ |\alpha_{s(i)}|^{n_{g(i)-1}} \prod_{f=0}^{g(i)-2} (n_f - n_{h-1}) & \text{if } 0 \leqslant j < h, \end{cases}$$

hence (20) and (21) follow by Hadamard's inequality. Note that if $g(i) > h+1$ or $g(i) > h$ for $i \in I$, then both sides of (20) or (21), respectively, are zero. □

Definition 3. In the notation of Definition 1 and of Lemma 5 put for a positive integer $h < d$, positive integers $e_1, \dots, e_h$ and a subset J of $\{1, \dots, d\}$ of cardinality $h + 1$ such

that $\max\limits_{i\in J} g(i) \leqslant h+1$

$$D(J; e_1, \dots, e_h) = \left|\det\left(\alpha_{s(i)}^{\sum_{\mu=j+1}^{h} e_\mu} \prod_{f=0}^{g(i)-2} \sum_{\nu=f+1}^{j} e_\nu\right)_{\substack{i\in J\\ 0\leqslant j\leqslant h}}\right| \times \prod_{i\in J} |\alpha_{s(i)}|^{-\sum_{\mu=\max\{2,g(i)\}}^{h} e_\mu} \prod_{i\in J}\prod_{f=0}^{g(i)-2}\Big(\sum_{\nu=f+1}^{h} e_\nu\Big)^{-1}.$$

Definition 4. $D(e_1, \dots, e_h) = \max D(J; e_1, \dots, e_h)$, where the maximum is taken over all subsets of $\{1, \dots, d\}$ of cardinality $h+1$ such that $\max\limits_{i\in J} g(i) \leqslant h+1$.

Remark. The definition is meaningful, since always there exists a subset J of $\{1, \dots, d\}$ with the required property. If for all $i \leqslant d$ we have $g(i) \leqslant h+1$ this is clear and if for some $i_0 : g(i_0) > h+1$ we take

$$J = \{i : m_1 + \dots + m_{s(i_0)-1} < i \leqslant m_1 + \dots + m_{s(i_0)-1} + h + 1\}.$$

Proof of Theorem 2. Using the notation of Definition 4 we define the sequence $d_1, \dots, d_d$ inductively as follows.

$$d_1 = \frac{\log\big(L(P)-1\big)}{\log|\alpha_1|} \tag{22}$$

and, if $d_1, \dots, d_h$ $(d > h \geqslant 1)$ are already defined, put

$$D_{h+1} = (h+1)^{-1} h^{h/2} \min\{D(e_1, \dots, e_h) : 1 \leqslant e_i \leqslant d_i,\ D(e_1, \dots, e_h) > 0\} \tag{23}$$

(the minimum over an empty set being ∞), $m = \max\limits_{1\leqslant s\leqslant r} m_s$,

$$d_{h+1} = \begin{cases} \max\Big\{d_1 + \dots + d_h, \\ \quad \psi\Big(|\alpha_r|, m-1, \Big(\max\Big\{2, \dfrac{2(m-1)}{\log|\alpha_r|}\Big\}\Big)^{m-1} D_{h+1}^{-1}\big(L(P)-1\big)\Big)\Big\} \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{if } D_{h+1} \neq \infty, \\ 0 \qquad\qquad\qquad\qquad\qquad\qquad \text{otherwise.} \end{cases} \tag{24}$$

We shall show that if $Q \in T_d(P)$, $Q = x^{n_0} + \sum\limits_{j=1}^{\delta} b_j x^{n_j}$, $\prod\limits_{j=1}^{\delta} b_j \neq 0$, then

$$n_{j-1} - n_j \leqslant d_j \quad (1 \leqslant j \leqslant \delta). \tag{25}$$

We proceed by induction on j. Since $Q \in T_d(P)$ the equation

$$\alpha_1^{n_0} + \sum_{j=1}^{\delta} b_j \alpha_1^{n_j} = 0$$

implies

$$|\alpha_1|^{n_0} \leqslant |\alpha_1|^{n_1} \sum_{j=1}^{\delta} |b_j| \leqslant |\alpha_1|^{n_1}\big(L(Q)-1\big) \leqslant |\alpha_1|^{n_1}\big(L(P)-1\big),$$

which, in view of (22), gives (25) for $j = 1$. Assume now that (25) holds for all $j \leqslant h$ ($h < \delta$) and consider the matrix $(c_{ij})_{\substack{1\leqslant i\leqslant d\\ 0\leqslant j\leqslant h}}$ for c_{ij} defined in Definition 1. Since $Q \in T_d(P)$ we have

$$\operatorname{rank}\big(c_{ij}\big)_{\substack{1\leqslant i\leqslant d\\ 0\leqslant j\leqslant h}} = h+1,$$

hence also

$$\operatorname{rank}\big(c_{ij}\alpha_{s(i)}^{-n_h}\big)_{\substack{1\leqslant i\leqslant d\\ 0\leqslant j\leqslant h}} = h+1.$$

Therefore, there exists a subset J of $\{1,\dots,d\}$ of cardinality $h+1$ such that

$$\Delta(J) = \det\big(c_{ij}\alpha_{s(i)}^{-n_h}\big)_{\substack{i\in J\\ 0\leqslant j\leqslant h}} \neq 0. \tag{26}$$

For every subset J with the above property consider

$$M(J) = \max_{i\in J}\left|\Big(c_{i0} + \sum_{j=1}^{h} c_{ij}b_j\Big)\alpha_{s(i)}^{-n_h}\right|.$$

Solving the system of equations

$$\Big(c_{i0}x_0 + \sum_{j=1}^{h} c_{ij}x_j\Big)\alpha_{s(i)}^{-n_h} = \Big(c_{i0} + \sum_{j=1}^{h} c_{ij}b_j\Big)\alpha_{s(i)}^{-n_h} \quad (i \in J)$$

by means of Cramer's formulae and developing the numerator according to the first column we obtain

$$1 \leqslant \frac{(h+1)M(J)\max\left|\det\big(c_{ij}\alpha_{s(i)}^{-n_h}\big)_{\substack{i\in I\\ 1\leqslant j\leqslant h}}\right|}{\big|\Delta(J)\big|},$$

where the maximum is taken over all subsets I of J of cardinality h. Now, by Lemma 7, since $|\alpha_{s(i)}| \geqslant 1$

$$\max\left|\det\big(c_{ij}\alpha_{s(i)}^{-n_h}\big)_{\substack{i\in I\\ 1\leqslant j\leqslant h}}\right| \geqslant h^{-h/2}\prod_{i\in J}\big|\alpha_{s(i)}\big|^{n_{\max\{1,g(i)-1\}}}\prod_{f=0}^{g(i)-2}(n_f - n_h).$$

This gives, by Definitions 3 and 4, for every J satisfying (26)

$$M(J) \geqslant (h+1)^{-1}h^{-h/2}D(J; n_0-n_1,\dots,n_{h-1}-n_h) > 0$$

and, since such J exist,

$$\max{}^{*}\, M(J) \geqslant (h+1)^{-1}h^{-h/2}D(J; n_0-n_1,\dots,n_{h-1}-n_h) < \infty,$$

where $\max^*$ is taken over all subsets J of $\{1,\dots,d\}$ such that $\operatorname{card} J = h+1$ and $\max\limits_{i\in J} g(i) \leqslant h+1$.

By the inductive assumption and (23)

$$\max{}^{*} M(J) \geqslant D_{h+1} > 0,$$

thus there exists a set $J_0 \subset \{1, \ldots, d\}$ such that card $J_0 = h+1$, $\max\limits_{i \in J_0} g(i) \leqslant h+1$ and

$$M(J_0) \geqslant D_{h+1}. \tag{27}$$

On the other hand, by Lemma 3

$$c_{i0} + \sum_{j=1}^{\delta} c_{ij} b_j = 0 \quad (i \in J_0),$$

hence

$$\left| \Big(c_{i0} + \sum_{j=1}^{h} c_{ij} b_j \Big) \alpha_{s(i)}^{-n_h} \right| \cdot \left| \alpha_{s(i)} \right|^{n_h} = \left| \sum_{j=h+1}^{\delta} c_{ij} b_j \right|. \tag{28}$$

By (27) for a certain $i_0 \in J_0$ the left hand side is at least $D_{h+1} \left| \alpha_{s(i)}^{n_h} \right|$. As to the right hand side, replacing in Lemma 5 h by $h+1$, we obtain

$$\begin{aligned} \left| \sum_{j=h+1}^{\delta} c_{i_0 j} b_j \right| &\leqslant |c_{i_0,h+1}| \left(\max\left\{ 1, \frac{g(i_0)-1}{\log \left| \alpha_{s(i_0)} \right|} \right\} \right)^{g(i_0)-1} \sum_{j=h+1}^{\delta} |b_j| \\ &\leqslant |c_{i_0,h+1}| \left(\max\left\{ 1, \frac{m_{s(i_0)}-1}{\log |\alpha_{s(i_0)}|} \right\} \right)^{m_{s(i_0)}-1} \big(L(P) - 1 \big). \end{aligned} \tag{29}$$

If $n_h - n_{h+1} \leqslant n_0 - n_h$, we obtain $n_h - n_{h+1} \leqslant d_1 + \ldots + d_h \leqslant d_{h+1}$, hence the inductive assertion holds. If $n_h - n_{h+1} > n_0 - n_h$, then

$$\begin{aligned} \left| c_{i_0,h+1} \right| &= \left| \alpha_{s(i_0)} \right|^{n_{h+1}} \prod_{f=0}^{g(i_0)-2} (n_f - n_{h+1}) \\ &\leqslant \left| \alpha_{s(i_0)} \right|^{n_{h+1}} \big(2(n_h - n_{h+1}) \big)^{g(i_0)-1} \\ &\leqslant \left| \alpha_{s(i_0)} \right|^{n_{h+1}} 2^{m_{s(i_0)}-1} (n_h - n_{h+1})^{m_{s(i_0)}-1}. \end{aligned} \tag{30}$$

Combining this inequality with (28) and (29) we obtain

$$\frac{D_{h+1} \left| \alpha_{s(i_0)} \right|^{n_h - n_{h+1}}}{(n_h - n_{h+1})^{m_{s(i_0)}-1}} \leqslant \left(\max\left\{ 2, \frac{2\big(m_{s(i_0)} - 1\big)}{\log \left| \alpha_{s(i_0)} \right|} \right\} \right)^{m_{s(i_0)}-1} \big(L(P) - 1 \big), \tag{31}$$

hence, by Lemma 6,

$$\begin{aligned} n_h - n_{h+1} &\leqslant \max_{1 \leqslant s \leqslant r} \psi \left(|\alpha_s|, m_s - 1, \left(\max\left\{ 2, \frac{2(m_s-1)}{\log |\alpha_s|} \right\} \right)^{m_s - 1} D_{h+1}^{-1} \big(L(P) - 1 \big) \right) \\ &\leqslant \psi \left(|\alpha_r|, m-1, \left(\max\left\{ 2, \frac{2(m-1)}{\log |\alpha_r|} \right\} \right)^{m-1} D_{h+1}^{-1} \big(L(P) - 1 \big) \right) \leqslant d_{h+1}. \end{aligned}$$

The inductive assertion being proved, it follows that

$$n_0 - n_\delta \leqslant \sum_{h=1}^{\delta} d_h.$$

However, $n_\delta = 0$, hence

$$l(P) = \inf_{Q \in U_d(P)} L(Q),$$

where $U_d(P) = \left\{ Q \in T_d(P) : \deg Q \leqslant \sum_{h=1}^{d} d_h \right\}$.

The set $U_d(P)$ is finite and effectively computable, since for

$$Q = x^{n_0} + \sum_{j=1}^{\delta} b_j x^{n_j} \in U_d(P), \quad \prod_{j=1}^{\delta} b_j \neq 0,$$

there are only finitely many choices for $\langle n_0, \dots, n_\delta \rangle$ and for each choice the coefficients b_j, if they exist, are determined uniquely and are effectively computable. Moreover, $Q \in T_d(P)$ implies $Q \in K(P)[x]$, hence $L(Q) \in K(P)$. The theorem follows. □

Proof of Corollary 1. If $P(x) = a_0 \prod_{i=1}^{c} (x - \alpha_i) \prod_{i=c+1}^{d} (x - \alpha_i)$, where $|\alpha_i| > 1$ for $i \leqslant c$, $|\alpha_i| < 1$ for $i > c$, then by Proposition A

$$l(P) = |a_0|\, l\left(\prod_{i=1}^{c} (x - \alpha_i) \right)$$

and the right hand side is effectively computable by Theorem 2. □

For the proof of Theorem 3 we need two lemmas.

Lemma 8. *If* $P_n \in \mathbb{R}[x]$, $p_n, q_n \in \mathbb{N}$ $(n = 0, 1, \dots)$ *and*

$$\liminf_{n \to \infty} L\left(P_n(x) - P_0(x^{p_n}) x^{q_n}\right) = 0, \tag{32}$$

then

$$\liminf_{n \to \infty} l(P_n) \leqslant l(P_0). \tag{33}$$

Proof. By definition of $l(P_0)$ for every n there exists G_n monic such that

$$L(P_0 G_n) \leqslant l(P_0) + \frac{1}{n}.$$

By (32) there exists $k_n \in \mathbb{N}$ such that $k_n > n$ and

$$L\left(P_{k_n}(x) - P_0(x^{p_{k_n}}) x^{q_{k_n}}\right) \leqslant \frac{1}{n L(G_n)}.$$

Hence

$$\begin{aligned} &L\big(P_{k_n}(x)G_n(x^{p_{k_n}})\big) \\ &\quad\leqslant L\big(P_0(x^{p_{k_n}})x^{q_{k_n}}G_n(x^{p_{k_n}})\big) + L\big((P_{k_n}(x) - P_0(x^{p_{k_n}})x^{q_{k_n}})G_n(x^{p_{k_n}})\big) \\ &\quad\leqslant L\big(P_0G_n\big) + L\big(P_{k_n}(x) - P_0(x^{p_{k_n}})x^{q_{k_n}}\big)L(G_n) \leqslant l(P_0) + \frac{2}{n}\,, \end{aligned}$$

thus

$$l(P_{k_n}) \leqslant l(P_0) + \frac{2}{n}\,.$$

This implies (33). □

Remark. The equality $\lim_{n\to\infty} L(P_n - P_0) = 0$ does not imply $\liminf_{n\to\infty} l(P_n) = l(P_0)$, as is shown by the example $P_n = x - \frac{n-1}{n}$, $P_0 = x - 1$, see Proposition A(ii) and (iii).

Lemma 9. *Let Q be a monic polynomial, irreducible over $\mathbb{R}$ of degree $d \leqslant 2$ with the zeros on the unit circle. There exists a sequence of monic polynomials R_n such that*

$$Q^2 \mid R_n \tag{34}$$

and

$$\lim_{n\to\infty} L(R_n - x^{dn}Q) = 0. \tag{35}$$

Proof. It suffices to take

$$R_n = x^{n+1} - \varepsilon\Big(1 + \frac{1}{n}\Big)x^n + \frac{\varepsilon^{n+1}}{n} \quad \text{if} \quad d = 1,\ Q = x - \varepsilon$$

and

$$R_n = \left(x^{n+1} - \zeta\Big(1 + \frac{1}{n}\Big)x^n + \frac{\zeta^{n+1}}{n}\right)\left(x^{n+1} - \overline{\zeta}\Big(1 + \frac{1}{n}\Big)x^n + \frac{\overline{\zeta}^{n+1}}{n}\right),$$

if $d = 2$, $Q = (x - \zeta)(x - \overline{\zeta})$.

Indeed, we have for every ε

$$(x - \varepsilon)^2 \mid x^{n+1} - \varepsilon\Big(1 + \frac{1}{n}\Big)x^n + \frac{\varepsilon^{n+1}}{n}\,,$$

which implies (34) and

$$L(R_n - x^{dn}Q) \leqslant \begin{cases} 2/n & \text{if } d = 1 \\ (8n+4)/n^2 & \text{if } d = 2, \end{cases}$$

which implies (35). □

Proof of Theorem 3. We proceed by induction with respect to the number N of irreducible factors of Q^{m-1} counted with multiplicities. If $N = 1$, then $m = 2$, Q is irreducible and by Lemma 9 we have

$$PQ^2 \mid PR_n \tag{36}$$

and

$$\lim_{n\to\infty} L(PR_n - x^{dn}PQ) = 0. \tag{37}$$

By (37) and Lemma 8 we have

$$\liminf_{n\to\infty} l(PR_n) \leqslant l(PQ).$$

However, by Proposition (i) and (36)

$$l(PQ) \leqslant l(PQ^2) \leqslant l(PR_n),$$

hence

$$l(PQ) \leqslant l(PQ^2) \leqslant l(PQ),$$

which gives the theorem for $N+1$.

Assume now that the number of irreducible factors of Q^{m-1} is $N > 1$ and the theorem is true for the number of irreducible factors less than N. If $m > 2$ then the number of irreducible factors of Q^{m-2} and of Q is less than N, hence applying the inductive assumption with P replaced first by PQ we obtain

$$l(PQ^m) = l(PQ^2) = l(PQ).$$

If $m = 2$ and the number of irreducible factors of Q^{m-1} is $N > 1$, then Q is reducible, $Q = Q_1Q_2$, where $\deg Q_i > 1$ $(i = 1, 2)$. The number of irreducible factors of Q_i is less than N, hence applying the inductive assumption with P replaced first by PQ_1^2 and then by PQ_2 we obtain

$$l(PQ^2) = l(PQ_1^2Q_2^2) = l(PQ_1^2Q_2) = l(PQ_1Q_2) = l(PQ).$$

The inductive proof is complete. □

Proof of Theorem 4. By Theorem 3 and Proposition A(ii) we have for $d \in \mathbb{N}$

$$l\big((x-1)^d\big) = l(x-1) = 2. \tag{38}$$

Now, let

$$P(x) = \prod_{j=1}^{d} \big(x - \exp 2\pi i r_j\big), \quad \text{where } r_j \in \mathbb{R}.$$

By Dirichlet's approximation theorem for every positive integer n there exists a positive integer p_n such that

$$\|p_n r_j\| \leqslant \frac{1}{2\pi n} \quad (1 \leqslant j \leqslant d),$$

hence

$$\big|\exp 2\pi i p_n r_j - 1\big| < \frac{1}{n}.$$

It follows that the polynomial

$$Q_n(x) = \prod_{j=1}^{d} \left(x^{p_n} - \exp 2\pi i p_n r_j\right)$$

satisfies

$$P \mid Q_n \tag{39}$$

and

$$L\left(Q_n - (x^{p_n} - 1)^d\right) \leqslant \left(2 + \frac{1}{n}\right)^d - 2^d. \tag{40}$$

Now, (39) implies by Proposition (i)

$$l(P) \leqslant \liminf_{n\to\infty} l(Q_n),$$

while (40), Lemma 8 and (38) imply

$$\liminf_{n\to\infty} l(Q_n) \leqslant l\left((x-1)^d\right) = 2.$$

Hence $l(P) \leqslant 2$. On the other hand, if $P \mid Q$, $Q = x^n + \sum_{j=1}^{n} b_j x^{n-j}$, then for a zero α of P we have

$$1 = |\alpha|^n = \left|\sum_{j=1}^{n} b_j x^{n-j}\right| \leqslant \sum_{j=1}^{n} |b_j| = L(Q) - 1,$$

hence $L(Q) \geqslant 2$; so

$$l(P) \geqslant 2,$$

which gives the first part of the theorem. In order to prove the second part assume that $P \mid Q$, Q monic and $L(Q) = 2$. Let

$$Q = x^n + \sum_{j=1}^{n} b_j x^{n-j}, \quad b_n \neq 0.$$

For every zero α of P we have

$$\alpha^n + \sum_{j=1}^{n} b_j \alpha^{n-j} = 0, \tag{41}$$

hence

$$\left|\sum_{i=1}^{n} b_i \alpha^{n-i}\right| = |\alpha^n| = 1 = \sum_{i=1}^{n} |b_i|.$$

It follows that for every j with $b_j \neq 0$

$$\arg b_j \alpha^{n-j} = \arg b_n.$$

Since $\arg b_i = 0$ or π, either α is a root of unity, or $b_j = 0$ for all $j < n$. However the latter case, by virtue of (41), leads to the former. Suppose now that α is a multiple zero

of P, hence also of Q. Then

$$n\alpha^{n-1} + \sum_{j=1}^{n-1} b_j(n-j)\alpha^{n-j-1} = 0,$$

hence

$$\left|\sum_{j=1}^{n-1} b_j(n-j)\alpha^{n-j-1}\right| = |n\alpha^n| = n > \sum_{j=1}^{n-1} |b_j|n,$$

which is impossible, since for each $j < n$, $\left|b_j(n-j)\alpha^{n-j-1}\right| \leqslant |b_j|n$. Thus all zeros of P are roots of unity and simple. If this condition is satisfied, then $P \mid x^m - 1$, where m is the least common multiple of orders of the roots of unity in question and

$$L(x^m - 1) = 2. \qquad \square$$

For the proof of Theorem 5 we need seven lemmas.

Lemma 10. *Let $d > 2$, I be a subset of $\{1, 2, \ldots, d-1\}$ and J a subset of $\{0, \ldots, d-2\}$, both of cardinality $d-2$. Then*

$$|\det(c_{ij})_{\substack{i\in I\\ j\in J}}| \leqslant (d-2)^{(d-2)/2} \prod_{i\in I} |\alpha_{s(i)}|^{n_{g(i)-1}} \prod_{f=0}^{g(i)-2} (n_f - n_{d-2}).$$

Proof is similar to the proof of Lemma 7. $\square$

Lemma 11. *Under the assumptions of Theorem* 5 *we have, in the notation of Definition* 1, *for every $h \leqslant d-e$ and $\nu = 0, 1$*

$$D_{h\nu} = \det(c_{ij})_{\substack{1\leqslant i\leqslant h\\ \nu\leqslant j<h+\nu}} \neq 0. \tag{42}$$

Proof. In the notation of Definition 1 we have $|\alpha_s| > 1$ for $s < r$, $\alpha_r = \varepsilon$, $m_r = e$. Assume that $\alpha_s \in Z_0$, if and only if $s \in S_0$. In the notation of Lemma 5

$$h = m_1 + \ldots + m_{s(h)-1} + g(h), \quad 1 \leqslant g(h) \leqslant m_{s(h)}.$$

If $\nu = 0$ or 1, $D_{h\nu} = 0$ and $\alpha_s \in Z_0$ for all $s \leqslant s(h)$, the system of equations

$$\sum_{j=\nu}^{h-1+\nu} c_{ij}x_j = 0 \quad (1 \leqslant i \leqslant h)$$

has a solution $\langle x_\nu, \ldots, x_{h-1+\nu}\rangle \in \mathbb{R}^h \setminus \{\mathbf{0}\}$. It follows by Lemma 3 that

$$\sum_{j=\nu}^{h-1+\nu} x_j x^{n_j} \equiv 0 \left(\mathrm{mod} \prod_{s=1}^{s(h)-1} (x-\alpha_s)^{m_s}(x-\alpha_{s(h)})^{g(h)}\right)$$

hence the polynomial $\sum_{j=\nu}^{h-1+\nu} x_j x^{n_j} \in \mathbb{R}[x]$ has h zeros of the same sign, counted with multiplicities. This, however, contradicts the Descartes rule of signs (see [3], Satz 12),

hence, if $\alpha_s \in Z_0$ $(s \leqslant s(h))$ (42) holds. It also shows that $D_{h\nu}$ as a polynomial in α_s $(s \notin S_0)$ is not identically zero for any fixed $\alpha_s \in Z_0$. Since the coefficients of the polynomial in question belong to $\mathbb{Q}(Z_0)$, the algebraic independence of α_s $(s \notin S_0)$ over $\mathbb{Q}(Z_0)$ implies $D_{h\nu} \neq 0$. □

Lemma 12. *Under the assumptions of Theorem* 5 *let* P_0 *be of degree* $d - e$. *For all positive integers* $e_1, \dots, e_{d-e}$ *there exists a unique polynomial* $Q = Q(P_0; e_1, \dots, e_{d-e})$ *such that*

$$Q = x^{\sum_{\mu=1}^{d-e} e_\mu} + \sum_{j=1}^{d-e} b_j x^{\sum_{\mu=j+1}^{d-e} e_\mu}$$

and

$$Q \equiv 0 \pmod{P_0}. \tag{43}$$

Moreover, $Q \in \mathbb{R}[x]$.

Proof. For $j = 0, \dots, d - e$ put $n_j = \sum_{\nu=j+1}^{d-e} e_\nu$ and for $i \leqslant d - e$, let c_{ij} be defined by Definition 1 with P replaced by P_0. By Lemma 3 the congruence (43) is equivalent to

$$\sum_{j=1}^{d-e} c_{ij} b_j = -c_{i0} \quad (1 \leqslant i \leqslant d - e).$$

By Lemma 11 with $h = d - e$ and $\nu = 1$ the determinant of this system is non-zero, hence b_j are uniquely determined. If we replace c_{ij} by $\overline{c}_{ij}$ we obtain the same system of equations, hence $b_j \in \mathbb{R}$. □

Lemma 13. *For every positive integer* $h < d - e$ *and all positive integers* $e_1, \dots, e_h$ *we have in the notation of Definition* 3

$$D\big(\{1, \dots, h+1\}, e_1, \dots, e_h\big) > 0.$$

Proof. We have

$$\max_{i \leqslant h+1} g(i) \leqslant \max_{i \leqslant h+1} i = h + 1,$$

hence $D(\{1, \dots, h+1\}, e_1, \dots, e_h)$ is defined. Its only factor, which could possibly vanish, is

$$\det\left(\alpha_{s(i)}^{\sum_{\mu=j+1}^{h} e_\mu} \prod_{f=0}^{g(i)-2} \sum_{\nu=f+1}^{j} e_\nu\right)_{\substack{1 \leqslant i \leqslant h+1 \\ 0 \leqslant j \leqslant h}} = \det\big(c_{ij} \alpha_{s(i)}^{-n_h}\big)_{\substack{1 \leqslant i \leqslant h+1 \\ 0 \leqslant j \leqslant h}},$$

where $n_j = \sum_{\mu=j+1}^{d} e_\mu$. By (42) with $\nu = 0$ the above determinant is non-zero. □

Definition 5. Let the sequence d_i $(1 \leqslant i \leqslant d-e)$ be defined inductively as follows.

$$d_1 = \frac{\log\bigl(L(P)-1\bigr)}{\log|\alpha_1|} \tag{44}$$

and if $d_1, \dots, d_h$ $(h < d-e)$ are already defined

$$D_{h+1} = (h+1)^{-1} h^{-h/2} \min\bigl\{D\bigl(\{1,\dots,h+1\}, e_1, \dots, e_h\bigr) : 1 \leqslant e_i \leqslant d_i\bigr\}, \tag{45}$$

$$\begin{aligned} d_{h+1} = \max\Biggl\{ & d_1, \dots, d_h, \\ & \psi\Biggl(|\alpha_{s(i)}|, m-1, \Biggl(\max\Biggl\{2, \frac{2(m-1)}{\log|\alpha_s(h+1)|}\Biggr\}\Biggr)^{m-1}\Biggr) D_{h+1}^{-1}\bigl(L(P)-1\bigr)\Biggr\}. \end{aligned} \tag{46}$$

Lemma 14. *For every* $Q \in T_d(P)$, $Q = x^{n_0} + \sum_{j=1}^{d} b_j x^{n_j}$ *we have*

$$n_{j-1} - n_j \leqslant d_j \quad (1 \leqslant j < d). \tag{47}$$

Proof is by induction on j. Since $Q \in T_d(P)$ the equation

$$\alpha_1^{n_0} + \sum_{j=1}^{d} b_j \alpha_1^{n_j} = 0$$

implies

$$|\alpha_1|^{n_0} \leqslant |\alpha_1|^{n_1} \sum_{j=1}^{d} |b_j| \leqslant |\alpha_1|^{n_1}\bigl(L(Q)-1\bigr) \leqslant |\alpha_1|^{n_1}\bigl(L(P)-1\bigr),$$

which, in view of (44), gives (47) for $j = 1$. Assume now that (47) holds for all $j \leqslant h$ $(h < d-1)$. By Lemma 11 we have

$$\Delta = \det\bigl(c_{ij}\alpha_{s(i)}^{-n_h}\bigr)_{\substack{1 \leqslant i \leqslant h+1 \\ 0 \leqslant j \leqslant h}} \neq 0.$$

Let

$$M = \max_{1 \leqslant i \leqslant h+1} \left| \left(c_{i0} + \sum_{j=1}^{h} c_{ij} b_j\right) \alpha_{s(i)}^{-n_h} \right|.$$

Solving the system of equations

$$\left(c_{i0}x_0 + \sum_{j=1}^{h} c_{ij}x_j\right)\alpha_{s(i)}^{-n_h} = \left(c_{i0} + \sum_{j=1}^{h} c_{ij}b_j\right)\alpha_{s(i)}^{-n_h} \quad (1 \leqslant i \leqslant h+1)$$

by means of Cramer's formulae and developing the numerator according to the first column we obtain

$$1 \leqslant \frac{(h+1)M \max\left|\det\bigl(c_{ij}\alpha_{s(i)}^{-n_h}\bigr)_{\substack{i \in I \\ 1 \leqslant j \leqslant h}}\right|}{|\Delta|},$$

where the maximum is taken over all subsets I of $\{1, \dots, h+1\}$ of cardinality h. Now, by Lemma 7, since $|\alpha_{s(i)}| > 1$, we have

$$\max\left|\det\left(c_{ij}\alpha_{s(i)}^{-n_h}\right)_{\substack{i\in I\\ 1\leqslant j\leqslant h}}\right| \leqslant h^{h/2}\prod_{i=1}^{h+1}\left|\alpha_{s(i)}\right|^{n_{\max\{1,g(i)-1\}}}\prod_{f=0}^{g(i)-2}(n_f - n_h).$$

This gives, by Definition 3,

$$m \geqslant (h+1)^{-1}h^{-1/2}D\left(\{1,\dots,h+1\}, n_0 - n_1, \dots, n_{h-1} - n_h\right)$$

and by the inductive assumption and (45)

$$M \geqslant D_{h+1}. \tag{48}$$

On the other hand, by Lemma 3

$$c_{i0} + \sum_{j=1}^{d} c_{ij}b_j = 0 \quad (1 \leqslant i \leqslant h+1),$$

hence

$$\left|\left(c_{i0} + \sum_{j=1}^{h} c_{ij}b_j\right)\alpha_{s(i)}^{-n_h}\right| \cdot \left|\alpha_{s(i)}\right|^{n_h} = \left|\sum_{j=1}^{h} c_{ij}b_j\right|. \tag{49}$$

By (48) for a certain $i_0 \leqslant h+1$ the left hand side is at least $D_{h+1}|\alpha_{s(i)}|^{n_h}$. As to the right hand side, by (29) we obtain

$$\left|\sum_{j=1}^{d} c_{i_0 j}b_j\right| \leqslant \left|c_{i_0,h+1}\right|\left(\max\left\{1, \frac{m_{s(i_0)-1}}{\log|\alpha_{s(i_0)}|}\right\}\right)^{m_{s(i_0)}-1}\left(L(P)-1\right). \tag{50}$$

If $n_h - n_{h+1} \leqslant n_0 - n_h$, we obtain $n_h - n_{h+1} \leqslant d_1 + \ldots + d_h \leqslant d_{h+1}$, hence the inductive assumption holds. If $n_h - n_{h+1} > n_0 - n_h$, then by (30)

$$\left|c_{i_0,h+1}\right| \leqslant \left|\alpha_{s(i_0)}\right|^{n_{h+1}} 2^{m_{s(i_0)}-1}(n_h - n_{h+1})^{m_{s(i_0)}-1}.$$

Combining the inequality with (49) and (50) we obtain (31), where, however, D_{h+1} has the new meaning given by (45).

It follows, by Lemma 6

$$\begin{aligned} n_h - n_{h+1} &\leqslant \max_{1\leqslant s\leqslant s(h+1)} \psi\left(|\alpha_s|, m_s - 1, \left(\max\left\{2, \frac{2(m_s-1)}{\log|\alpha_s|}\right\}\right)^{m_s-1} D_{h+1}^{-1}\left(L(P)-1\right)\right) \\ &\leqslant \psi\left(\alpha_{s(h+1)}, m-1, \left(\max\left\{2, \frac{2(m-1)}{\log|\alpha_{s(h+1)}|}\right\}\right)^{m-1} D_{h+1}^{-1}\left(L(P)-1\right)\right) \leqslant d_{h+1} \end{aligned}$$

and the inductive proof is complete. □

Definition 6. Assume that, under the assumptions of Theorem 5, $e = 1$. Put for positive

integers $n_1 > \ldots > n_{d-2} > n_{d-1}$

$$\left(c'_{ij}\right)_{\substack{1\leqslant i<d\\ 1\leqslant j\leqslant d}} = C(P_0; n_1, \ldots, n_{d-1}, 0), \quad c'_{dj} = 1 \quad (1 \leqslant j \leqslant d),$$

$$E(P_0; n_1 - n_{d-1}, \ldots, n_{d-2} - n_{d-1})$$

$$= \left|\det\left(c'_{ij}\alpha_{s(i)}^{-n_{d-1}}\right)_{1\leqslant i,j<d}\right|^{-1} \prod_{i=1}^{d-1} \left|\alpha_{s(i)}\right|^{n_{g(i)}-n_{d-1}} \prod_{f=1}^{g(i)-1} (n_f - n_{d-1}). \tag{51}$$

Remark. $E(P_0; n_1 - n_{d-1}, \ldots, n_{d-2} - n_{d-1})$ is well defined since $\det(c'_{ij}\alpha_{s(i)}^{-n_{d-1}})$ is non-zero by Lemma 11 with $h = d-1$, $v = 0$. Moreover the right hand side of (51) depends only on P_0 and the differences $n_j - n_{d-1}$ $(1 \leqslant j \leqslant d-2)$.

Lemma 15. *Assume that, under the assumptions of Theorem* 5 *and in the notation of Definition* 1, $e = 1$. *If for positive integers* $n_1 > \ldots > n_{d-1}$ *and for* $n > 1$, $a \in \mathbb{R}$,

$$n_{d-1} > \max\left\{n_1 - n_{d-1}, \psi\left(|\alpha_{r-1}|, m-1, d(d-1)^{(d+1)/2}2^{m-1}n \times E(P_0; n_1 - n_{d-1}, \ldots, n_{d-2} - n_{d-1}) \max\left\{1, \frac{nd|a|}{nd-1}\right\}\right)\right\}, \tag{52}$$

then there exists a polynomial $R \in \mathbb{R}[x]$, $R(x) = \sum_{j=1}^{d-1} r_j x^{n_j} + r_d$, *such that*

$$P_0 \mid R(x) - a, \tag{53}$$

$$x - 1 \mid R(x) \tag{54}$$

$$L(R) < \frac{1}{n}. \tag{55}$$

Proof. Put

$$R(x) = \sum_{j=1}^{d-1} r_j x^{n_j} + r_d, \quad r_j \in \mathbb{C}.$$

By Lemma 3 the conditions (53) and (54) are equivalent to the following system of linear equations for r_j

$$\begin{aligned} &\sum_{j=1}^{d} c'_{ij} r_j = c'_{id} a \quad (1 \leqslant i < d)\\ &\sum_{j=1}^{d} c'_{dj} r_j = 0. \end{aligned} \tag{56}$$

The determinant of this system equals

$$\Delta_0 = \prod_{i=1}^{d} \alpha_{s(i)}^{n_{d-1}} \det\left(c'_{ij}\alpha_{s(i)}^{-n_{d-1}}\right)_{1\leqslant i,j\leqslant d}.$$

Developing the last determinant according to the last column we obtain

$$\det\bigl(c'_{ij}\alpha_{s(i)}^{-n_{d-1}}\bigr)_{1\leqslant i,j\leqslant d} = \det\bigl(c'_{ij}\alpha_{s(i)}^{-n_{d-1}}\bigr)_{1\leqslant i,j<d} + \sum_{k=1}^{d-1}(-1)^{k+d}c'_{kd}\alpha_{s(k)}^{-n_{d-1}}\det\bigl(c'_{ij}\alpha_{s(i)}^{-n_{d-1}}\bigr)_{\substack{i\neq k\\ j<d}},$$

hence, by (21) with $h = d-1$, $I = \{1,\dots,d\}\setminus\{k\}$ and by the condition $\alpha_r = e = 1$

$$\left|\Delta_0\prod_{i=1}^{d}\alpha_{s(i)}^{-n_{d-1}} - \det\bigl(c'_{ij}\alpha_{s(i)}^{-n_{d-1}}\bigr)_{1\leqslant i,j<d}\right| < (d-1)^{(d+1)/2}\bigl|\alpha_{r-1}\bigr|^{-n_{d-1}}\left(\prod_{i=1}^{d-1}\bigl|\alpha_{s(i)}\bigr|^{n_{g(i)}-n_{d-1}}\prod_{f=1}^{g(i)-1}(n_f - n_{d-1})\right)\max_{1\leqslant k<d}|c'_{kd}|. \tag{57}$$

Since, by (52), $n_{d-1} > n_1 - n_{d-1}$, we have

$$\max_{1\leqslant k<d}|c'_{kd}| \leqslant \prod_{f=1}^{m-1}n_f \leqslant (2n_{d-1})^{m-1}. \tag{58}$$

In view of Definition 6 the right hand side of (57) does not exceed

$$(d-1)^{(d+1)/2}\bigl|\alpha_{r-1}\bigr|^{-n_{d-1}}\left|\det\bigl(c'_{ij}\alpha_{s(i)}^{-n_{d-1}}\bigr)_{1\leqslant i,j<d}\right| \times E(P_0; n_1 - n_{d-1},\dots,n_{d-2}-n_{d-1},0)2^{m-1}n_{d-1}^{m-1}.$$

Since, by (52),

$$n_{d-1} > \psi\bigl(|\alpha_{r-1}|, m-1, d(d-1)^{(d+1)/2}2^{m-1}nE(P_0; n_1 - n_{d-1},\dots,n_{d-2}-n_{d-1},0)\bigr)$$

we have by Lemma 6 and (57)

$$|\Delta_0| > \left(1 - \frac{1}{dn}\right)\left|\det\bigl(c'_{ij}\bigr)_{1\leqslant i,j<d}\right|, \tag{59}$$

hence by the Remark after Definition 6, $\Delta_0 \neq 0$. Thus the system (56) is uniquely solvable and since on replacing c'_{ij} by $\overline{c}'_{ij}$ we obtain the same system, r_j are real ($1 \leqslant j \leqslant d$).

The determinant Δ_k obtained by substituting in $(c'_{ij})_{1\leqslant i,j\leqslant d}$ for the k-th column the column

$$[c'_{1d},\dots,c'_{d-1\,d},0]^t a$$

satisfies for $k < d$

$$\Delta_k = \pm(\det c'_{ij})_{\substack{i<d\\ j\neq k}}a,$$

hence developing the last determinant according to the last column, using Lemma 10,

Definition 6 and (58) we obtain

$$|\Delta_k| \leqslant |a| \sum_{l=1}^{d-1} |c'_{ld}|(d-2)^{(d-2)/2} \prod_{\substack{i=1 \\ i\neq l}}^{d-1} \left|\alpha_{s(i)}\right|^{n_{g(i)}} \prod_{f=1}^{g(i)-1} (n_f - n_{d-1})$$

$$\leqslant |a|(d-1)(d-2)^{(d-2)/2}(2n_{d-1})^{m-1}\left|\alpha_{r-1}\right|^{-n_{d-1}} \left|\det\left(c'_{ij}\right)_{1\leqslant i,j<d}\right| \times E(P_0; n_1 - n_{d-1}, \ldots, n_{d-2} - n_{d-1}),$$

where $(d-2)^{(d-2)/2} = 1$ for $d = 2$.

Since $(d-1)(d-2)^{(d-2)/2} < (d-1)^{(d+1)/2}$ we obtain, by virtue of (52),

$$|\Delta_k| < \frac{dn-1}{d^2n^2}\left|\det\left(c'_{ij}\right)_{1\leqslant i,j<d}\right|$$

hence, by (59), $r_k = \Delta_k/\Delta_0$ satisfies

$$|r_k| < \frac{1}{dn} \quad (1 \leqslant k < d). \tag{60}$$

It remains to consider $k = d$. In this case developing Δ_d according to the last column we obtain

$$|\Delta_d| \leqslant |a| \sum_{l=1}^{d-1} |c'_{ld}| \left|\det\left(c'_{ij}\right)_{\substack{i\neq l \\ j<d}}\right|.$$

Using (21) with $h = d-1$, $I = \{1, \ldots, d\} \setminus \{l\}$, the condition $\alpha_r = e = 1$ and (58) we obtain

$$|\Delta_d| \leqslant |a|(d-1)^{(d+1)/2}(2n_{d-1})^{m-1}\left|\alpha_{r-1}\right|^{-n_{d-1}} \prod_{i=1}^{d-1} \left|\alpha_{s(i)}\right|^{n_{g(i)}} \prod_{f=1}^{g(i)-1} (n_f - n_{d-1})$$

$$\leqslant (d-1)^{(d+1)/2}2^{m-1}n_{d-1}^{m-1}\left|\alpha_{r-1}\right|^{-n_{d-1}} \left|\det(c'_{ij})_{1\leqslant i,j<d}\right| \times E(P_0; n_1 - n_{d-1}, \ldots, n_{d-2} - n_{d-1}).$$

Again, by virtue of (52) and of Lemma 6,

$$|\Delta_d| < \frac{dn-1}{d^2n^2}\left|\det\left(c'_{ij}\right)_{1\leqslant i,j<d}\right|,$$

hence $r_d = \Delta_d/\Delta_0$ satisfies

$$|r_d| < \frac{1}{dn}\,.$$

It follows now from (60) that

$$L(R) = \sum_{k=1}^{d} |r_k| < \frac{1}{n}\,,$$

which proves (55). □

Lemma 16. *Assume, under the assumptions of Theorem* 5, *that* $\varepsilon = e = 1$. *Then*

$$l(P) \leqslant \inf_{Q \in S_{d-1}(P_0)} \{L(Q) + |Q(1)|\}.$$

Proof. Let

$$Q = x^{q_0} + \sum_{j=1}^{d-1} b_j x^{q_j},$$

where $q_0 > q_1 > \ldots > q_{d-1} = 0$. By Lemma 15 with $a = Q(1)$, $n_j = n_{d-1} + q_j$ $(1 \leqslant j < d)$, if

$$n_{d-1} > \max\left\{q_1, \psi\left(\left|\alpha_{r-1}\right|, m-1, d(d-1)^{(d+1)/2} 2^{m-1} n \times E(P_0; q_1, \ldots, q_{d-2}) \max\left\{1, \frac{nd}{nd-1}\,|Q(1)|\right\}\right)\right\}$$

there exists a polynomial $R \in \mathbb{R}[x]$ of degree at most n_1 satisfying (53)–(55). We consider the polynomial

$$S(x) = Q(x) x^{n_{d-1}} + R(x) - Q(1).$$

It follows from (53)–(54) that

$$P_0 \mid S, \quad x - 1 \mid S, \quad \text{thus } P \mid S$$

and since S is monic

$$l(P) \leqslant L(S).$$

On the other hand, by (55),

$$L(S) \leqslant L(Q) + |Q(1)| + \frac{1}{n}.$$

Since n is arbitrary, the lemma follows. □

Proof of Theorem 5. Since, by Proposition (iii), $l(P(-x)) = l(P(x))$, we may assume that $\varepsilon = 1$ and, by virtue of Theorem 3, that $e = 1$. Thus Lemmas 15 and 16 are applicable. The second part of the theorem follows from Lemma 16. In order to prove the first part we shall show that for every $n > 1$

$$\begin{aligned} 0 \geqslant l(P) - \min\Big\{ & \min^{*} L\big(Q(P; n_0, \ldots, n_{d-2}, 0)\big), \\ & \min^{**} L\big(Q(P; n_0, \ldots, n_{d-1}, 0)\big), \\ & \min^{**}\Big(L\big(Q(P_0; n_0 - n_{d-1}, \ldots, n_{d-2} - n_{d-1}, 0)\big) \\ & \quad + \big|Q(P_0; n_0 - n_{d-1}, \ldots, n_{d-2} - n_{d-1}, 0)(1)\big|\Big)\Big\} > -\frac{1}{n}, \end{aligned} \tag{61}$$

where the min* is taken over all integers $n_0 > \ldots > n_{d-2} > n_{d-1} = 0$ such that $n_{j-1} - n_j \leqslant d_j$ $(1 \leqslant j < d)$ and the min** is taken over all integers $n_0 > \ldots > n_{d-1} > 0$

such that

$$n_{j-1} - n_j \leqslant d_j \quad (1 \leqslant j < d) \tag{62}$$

holds and

$$\begin{aligned} n_{d-1} \leqslant \max\Big\{ & n_1 - n_{d-1}, \psi\Big(|\alpha_{r-1}|, m-1, d(d-1)^{(d+1)/2} 2^{m-1} n \\ & \times E(P_0; n_1 - n_{d-1}, \dots, n_{d-2} - n_{d-1}) \\ & \times \max\Big\{1, \frac{nd}{nd-1} |Q(P_0; n_0 - n_{d-1}, \dots, n_{d-2} - n_{d-1}, 0)(1)|\Big\}\Big)\Big\} \end{aligned} \tag{63}$$

and, in the notation of Definition 1

$$|C_1(P; n_1, \dots, n_{d-1}, 0)| \neq 0. \tag{64}$$

By Lemma 12 for every sequence $n_0 > \dots > n_{d-1} = 0$ there is at most one polynomial $Q = x^{n_0} + \sum_{j=1}^{d-1} b_j x^{n_j}$ divisible by P; if the set of polynomials in question is empty we take $\min^* = \infty$.

The condition (64) implies that there is a unique polynomial

$$Q = x^{n_0} + \sum_{j=1}^{d-1} b_j x^{n_j} + b_d$$

divisible by P, denoted in (61) by $Q(P; n_0, \dots, n_{d-1}, 0)$. Analogously $Q(P_0; n_0 - n_{d-1}, \dots, n_{d-2} - n_{d-1}, 0)$ is the unique polynomial

$$Q = x^{n_0 - n_{d-1}} + \sum_{j=1}^{d-1} b_j x^{n_j - n_{d-1}}$$

divisible by P_0. The inequality

$$l(P) \leqslant \min\big\{\min^* L(Q(P; n_0, \dots, n_{d-2}, 0)), \min^{**} L(Q(P; n_0, \dots, n_{d-1}, 0))\big\}$$

is clear and the inequality

$$\begin{aligned} l(P) \leqslant \min{}^{**}\big(L\big(Q(P_0; n_0 - n_{d-1}, \dots, n_{d-2} - n_{d-1}, 0)\big) \\ + \big|Q(P_0; n_0 - n_{d-1}, \dots, n_{d-2} - n_{d-1}, 0)(1)\big|\big) \end{aligned}$$

follows from Lemma 16. This shows the first of inequalities (61). In order to prove the second one we notice that by Lemmas 4 and 14

$$l(P) = \min\big\{\min^* L(Q(P; n_0, \dots, n_{d-2}, 0)), \inf L(Q(P; n_0, \dots, n_{d-1}, 0))\big\}, \tag{65}$$

where the infimum is taken over all strictly decreasing sequences of d positive integers $\langle n_0, \dots, n_{d-1}\rangle$ satisfying (62) and (64). If (63) is satisfied then, clearly

$$L(Q(P; n_0, \dots, n_{d-1}, 0)) \geqslant \min^{**} L(Q(P; n_0, \dots, n_{d-1}, 0)) \tag{66}$$

and, if not, then by Lemma 15 there exists a polynomial $R \in \mathbb{R}[x]$, $R(x) = \sum_{j=1}^{d-1} r_j x^{n_j} + r_d$,

such that (53)–(55) hold with

$$a = Q(P_0; n_0 - n_{d-1}, \dots, n_{d-2} - n_{d-1}, 0)(1).$$

Then the polynomial

$$S(x) = Q(P_0; n_0 - n_{d-1}, \dots, n_{d-2} - n_{d-1}, 0)x^{n_{d-1}} + R(x) - Q(P_0; n_0 - n_{d-1}, \dots, n_{d-2} - n_{d-1}, 0)(1)$$

is monic, satisfies

$$P \mid S(x)$$

and, by (64),

$$S(x) = Q(P; n_0, \dots, n_{d-1}, 0). \tag{67}$$

By (55)

$$L(S) > L\big(Q(P_0; n_0 - n_{d-1}, \dots, n_{d-2} - n_{d-1}, 0)\big) + \big|Q(P_0; n_0 - n_{d-1}, \dots, n_{d-2} - n_{d-1}, 0)(1)\big| - \frac{1}{n}. \tag{68}$$

The formulae (66)–(68) imply

$$L\big(Q(P; n_0, \dots, n_{d-1}, 0)\big) \geqslant \min{}^{**} \min\Big\{L\big(Q(P; n_0, \dots, n_{d-1}, 0)\big), L\big(Q(P_0; n_0 - n_{d-1}, \dots, n_{d-2} - n_{d-1}, 0)\big) + \big|Q(P_0; n_0 - n_{d-1}, \dots, n_{d-2} - n_{d-1}, 0)(1)\big|\Big\} - \frac{1}{n}$$

for all sequences $\langle n_0, \dots, n_{d-1}\rangle$ satisfying (62) and (64), hence by (65) the second of the inequalities (61) follows. The conditions (62) and (63) are for a given n satisfied by only finitely many sequences $\langle n_0, \dots, n_{d-1}\rangle$, since

$$n_j - n_{d-1} \leqslant \sum_{\mu=j+1}^{d-1} d_\mu$$

and for all such sequences b_j can be effectively determined, hence $l(P)$ can be effectively computed. □

For the proof of Theorem 6 we need

Definition 7. For α, β in $\mathbb{C}$ and $n > m > 0$

$$Q_n(\alpha, \beta) = \begin{cases} \dfrac{\alpha^n - \beta^n}{\alpha - \beta} & \text{if } \alpha \neq \beta, \\ n\alpha^{n-1} & \text{if } \alpha = \beta, \end{cases}$$

$$E_{n,m}(\alpha, \beta) = \left|\frac{Q_n(\alpha, \beta)}{Q_m(\alpha, \beta)}\right| + |\alpha\beta|^m \left|\frac{Q_{n-m}(\alpha, \beta)}{Q_m(\alpha, \beta)}\right|,$$

$$F_{n,m}(x, \beta) = x_n - \beta^n + |\beta|^m x^m (x^{n-m} - \beta^{n-m}) - (2x - 1)(x^m - \beta^m).$$

Lemma 17. *In the notation of Definitions* 2 *and* 7, *if* $P(x) = (x-\alpha)(x-\beta)$, $\alpha\beta \neq 0$, *then all elements of* $T_2(P)$ *are of the form either* $x^n - \alpha^n$ *if* $Q_n(\alpha, \beta) = 0$, *or*

$$x^n - \frac{Q_n(\alpha,\beta)}{Q_m(\alpha,\beta)}x^m + (\alpha\beta)^m \frac{Q_{n-m}(\alpha,\beta)}{Q_m(\alpha,\beta)}, \quad \text{otherwise,} \tag{69}$$

where $n > m > 0$, $Q_m(\alpha,\beta)Q_{n-m}(\alpha,\beta) \neq 0$.

Proof. Let an element Q of $T_2(P)$ be $x^n + Ax^m + B$, where $n > m > 0$, $AB \neq 0$. By Lemma 3 the condition $Q \equiv 0 \pmod P$ is equivalent to

$$c_{i0} + c_{i1}A + c_{i2}B = 0 \quad (i = 1, 2), \tag{70}$$

where c_{ij} are given in Definition 1 for $\alpha_1 = \alpha$, $\alpha_2 = \beta$, hence

$$\begin{aligned} &c_{10} = \alpha^n, \ c_{11} = \alpha^m, && c_{12} = 1; \\ &c_{20} = \beta^n, \ c_{21} = \beta^m, && c_{22} = 1, \quad \text{if } \beta \neq \alpha; \\ &c_{20} = 0, \quad c_{21} = (m-n)\beta^m, && c_{22} = -n, \ \text{if } \beta = \alpha. \end{aligned}$$

Since $Q \in T_2(P)$ we have

$$|C_0(P; n, m)| \neq 0 \neq |C_1(P; n, m)|,$$

hence $Q_m(\alpha,\beta)Q_{n-m}(\alpha,\beta) \neq 0$. Solving the system (70) we obtain for Q the form (69).□

Lemma 18. *If* $\beta \in \mathbb{R}$, $|\beta| \geqslant 1$, *then for all positive integers* $n > m$ *and all integers* $k \geqslant 0$ *we have*

$$G_{n,m,k}(\beta) := \frac{1}{k!}\frac{d^k}{dx^k}F_{n,m}(x,\beta)|_{x=|\beta|} \geqslant 0$$

and if $|\beta| > 1$ *for* $k = 0$ *or* 1

$$\inf_{n>m} G_{n,m,k}(\beta) > 0.$$

Proof. Consider first the case $\beta > 0$. For $k = 0$ we have $G_{n,m,k}(\beta) = 0$. For $k \geqslant 1$ we have

$$\begin{aligned} G_{n,m,k}(\beta) &= \binom{n}{k}\beta^{n-k} + \binom{n}{k}\beta^{n+m-k} - \binom{m}{k}\beta^{n+m-k} \\ &\quad - 2\binom{m+1}{k}\beta^{m-k+1} + \binom{m}{k}\beta^{m-k} + 2\binom{1}{k}\beta^{m-k+1} \\ &= \beta^{m-k}\left(\binom{n}{k}\beta^{n-m} + \binom{n}{k}\beta^n - \binom{m}{k}\beta^n \right. \\ &\quad \left. - 2\binom{m+1}{k}\beta + \binom{m}{k} + 2\binom{1}{k}\beta\right). \end{aligned}$$

The expression in the parenthesis is non-negative, since for $\beta = 1$ it is equal to

$$2\binom{n}{k} - 2\binom{m+1}{k} + 2\binom{1}{k} \geqslant 0$$

and its derivative with respect to β is

$$\begin{aligned}\binom{n}{k}(n-m)\beta^{n-m-1} + \left(\binom{n}{k} - \binom{m}{k}\right)n\beta^{n-1} - 2\binom{m+1}{k} + \binom{1}{k}\\ \geqslant \binom{m+1}{k} + \left(\binom{m+1}{k} - \binom{m}{k}\right)(m+1) - 2\binom{m+1}{k} + 2\binom{1}{k}\\ = (k-1)\binom{m+1}{k} + 2\binom{1}{k} \geqslant 2\binom{1}{k}.\end{aligned}$$

It follows that

$$G_{n,m,k}(\beta) \geqslant 2(\beta - 1)$$

and the obtained lower bound, independent of n, m, is positive for $\beta > 1$. Consider now the case $\beta < 0$. We distinguish four cases according to the parity of n, m.

If $n \equiv m \equiv 0 \pmod 2$, then

$$G_{n,m,k}(\beta) = G_{n,m,k}\big(|\beta|\big)$$

and the case reduces to the former.

If $n \equiv 0, m \equiv 1 \pmod 2$, then

$$G_{n,m,0}(\beta) = 2\big(|\beta|\big)^m(|\beta|^n - 2|\beta| + 1) \geqslant 2\big(|\beta| - 1\big)^2$$

and the obtained lower bound, independent of n, m, is positive for $|\beta| > 1$. Further, for $k \geqslant 1$

$$\begin{aligned}G_{n,m,k}(\beta) &= \binom{n}{k}|\beta|^{n-k} + \binom{n}{k}|\beta|^{n+m-k} + \binom{m}{k}|\beta|^{n+m-k}\\ &\quad - 2\binom{m+1}{k}|\beta|^{m-k+1} + \binom{m}{k}|\beta|^{m-k} - 2\binom{1}{k}|\beta|^{m-k+1}\\ &= |\beta|^{m-k}\left(\binom{n}{k}|\beta|^{n-m} + \binom{n}{k}|\beta|^n + \binom{m}{k}|\beta|^n\right.\\ &\quad \left. - 2\binom{m+1}{k}|\beta| + \binom{m}{k} - 2\binom{1}{k}|\beta|\right).\end{aligned}$$

The expression in the parenthesis is non-negative, since

$$\binom{n}{k}|\beta|^{n-m} + \binom{n}{k}|\beta|^n \geqslant 2\binom{m+1}{k}|\beta|$$

and

$$\binom{m}{k}|\beta|^n + \binom{m}{k} \geqslant \binom{m}{k}(|\beta|^2 + 1) \geqslant 2\binom{1}{k}|\beta|.$$

If $n \equiv 1, m \equiv 0 \pmod 2$, then

$$G_{n,m,k}(\beta) \geqslant G_{n,m,k}\big(|\beta|\big)$$

and the case reduces to the already considered one.

Finally, if $n \equiv m \equiv 1 \pmod 2$, then

$$G_{n,m,0}(\beta) = 2|\beta|^m\big(|\beta|^{n-m} - 2|\beta| + 1\big) \geqslant 2\big(|\beta| - 1\big)^2$$

and the obtained lower bound, independent of n, m, is positive for $|\beta| > 1$.

Further, for $k \geqslant 1$

$$\begin{aligned} G_{n,m,k}(\beta) &= \binom{n}{k}|\beta|^{n-k} + \binom{n}{k}|\beta|^{n+m-k} - \binom{m}{k}|\beta|^{n+m-k} \\ &\quad - 2\binom{m+1}{k}|\beta|^{m-k+1} + \binom{m}{k}|\beta|^{m-k} - 2\binom{1}{k}|\beta|^{m-k+1} \\ &= |\beta|^{m-k}\bigg(\binom{n}{k}|\beta|^{n-m} + \binom{n}{k}|\beta|^n - \binom{m}{k}|\beta|^n - 2\binom{m+1}{k}|\beta| \\ &\quad + \binom{m}{k} - 2\binom{1}{k}|\beta|\bigg). \end{aligned}$$

The expression in the parenthesis is non-negative, since for $|\beta| = 1$ it is equal to

$$2\binom{n}{k} - 2\binom{m+1}{k} - 2\binom{1}{k} \geqslant 2\binom{m+2}{k} - 2\binom{m+1}{k} - 2\binom{1}{k} \geqslant 0$$

and its derivative with respect to $|\beta|$ is

$$\begin{aligned} &\binom{n}{k}(n-m)|\beta|^{n-m-1} + \binom{n}{k}n - |\beta|^{n-1} - \binom{m}{k}n|\beta|^{n-1} - 2\binom{m+1}{k} - 2\binom{1}{k} \\ &\geqslant \binom{n}{k}(n-m) + \binom{n}{k}n - \binom{m}{k}n - 2\binom{m+1}{k} - 2\binom{1}{k} \\ &\geqslant 2\binom{m+2}{k} + \bigg(\binom{m+2}{k} - \binom{m}{k}\bigg)(m+2) - 2\binom{m+1}{k} - 2\binom{1}{k} \geqslant 0. \end{aligned}$$

□

Proof of Theorem 6. For $n \geqslant 2$ we clearly have $1 + |\alpha|^n \geqslant 2|\alpha|$ with the equality attained if and only if $|\alpha| = 1$, hence we may restrict attention to $E_{n,m}(\alpha, \beta)$. Consider first the case of α, β real. Since, by Proposition (iii), $l(P(-x)) = l(P(x))$, we may assume that $\alpha > 0$, hence $\alpha \geqslant |\beta|$.

By the Taylor formula we have in the notation of Lemma 18

$$(\alpha^m - \beta^m)\big(E_{n,m}(\alpha, \beta) - 2\alpha + 1\big) = \sum_{k=0}^{n} G_{n,m,k}(\beta)\big(\alpha - |\beta|\big)^k,$$

hence, by the said lemma,

$$(\alpha^m - \beta^m)\big(E_{n,m}(\alpha, \beta) - 2\alpha + 1\big) \geqslant 0 \tag{71}$$

and, if $\alpha > |\beta| > 1$

$$\inf_{n>m} (\alpha^m - \beta^m)\big(E_{n,m}(\alpha, \beta) - 2\alpha + 1\big) > 0. \tag{72}$$

If $\alpha \neq \pm\beta$ then (71) gives

$$E_{n,m}(\alpha, \beta) \geqslant 2\alpha - 1,$$

hence by Lemma 17

$$\inf_{Q\in T_2(P)} L(Q) \geqslant 2\alpha$$

and by Lemma 4,

$$l(P) \geqslant 2\alpha. \tag{73}$$

Now, if $\beta = -1$, then $L(P) = 2\alpha$, hence $l(P) \leqslant 2\alpha$ and, by (73), $l(P) = 2\alpha$. If $\beta = 1$, then by Theorem 5 with $P_0 = x - \alpha$

$$l(P) \leqslant L(P_0) + |P_0(1)| = 1 + \alpha + \alpha - 1 = 2\alpha$$

and, by (73), $l(P) = 2\alpha$ again.

If $\alpha > |\beta| > 1$, then by (72)

$$\inf_{\substack{n>m\\ m<m_0}} E_{n,m}(\alpha, \beta) > 2\alpha - 1 \tag{74}$$

for every m_0. Choose now

$$m_0 = \frac{\log 4\alpha - \log\bigl(\alpha - |\beta|\bigr)}{\log|\beta|}.$$

Then for $m \geqslant m_0$: $E_{n,m}(\alpha, \beta) \geqslant |\alpha\beta|^m \frac{\alpha-|\beta|}{2\alpha^m} \geqslant 2\alpha$ and, by (74),

$$\inf_{n>m} E_{n,m}(\alpha, \beta) > 2\alpha - 1.$$

Using, as above, Lemmas 17 and 4 we obtain

$$l(P) > 2\alpha.$$

If $\alpha = -\beta$, then $P(x) = x^2 - \alpha^2$ and by Proposition (iv) and Proposition A(ii)

$$l(P) = l(x - \alpha^2) = 1 + \alpha^2 \begin{cases} = 2\alpha, & \text{if } \alpha = 1,\\ > 2\alpha, & \text{otherwise.}\end{cases}$$

If $\alpha = \beta$, then

$$E_{n,m}(\alpha, \beta) - 2\alpha + 1 = \frac{n\alpha^{n-m} + (n-m)\alpha^n}{m} - 2\alpha + 1.$$

The right hand side is equal to $2(n-m)/m > 0$ for $\alpha = 1$ and its derivative with respect to α is

$$\frac{n(n-m)}{m}(\alpha^{n-m-1} + \alpha^{n-m}) - 2 > \alpha - 1.$$

For $\alpha = \beta = 1$, $l(P) = 2 = 2\alpha$, by Theorem 4; otherwise

$$\inf_{n>m} E_{n,m}(\alpha, \alpha) > 2\alpha - 1$$

and, by Lemmas 17 and 4, $l(P) > 2\alpha$.

Consider now the case, where α, β are complex conjugate:

$$\alpha = |\alpha|e^{2i\varphi}, \quad \beta = |\alpha|e^{-2i\varphi}, \quad \varphi \in \bigl(0, \tfrac{\pi}{2}\bigr), \quad |\alpha| > 1$$

(the case $|\alpha| = 1$ is settled by Theorem 4). Then

$$E_{n,m}(\alpha, \beta) = |\alpha|^{n-m} \left| \frac{\sin n\varphi}{\sin m\varphi} \right| + |\alpha|^n \left| \frac{\sin(n-m)\varphi}{\sin m\varphi} \right|,$$

where, by virtue of the condition $Q_m(\alpha, \beta) \neq 0$, we have $\sin m\varphi \neq 0$. Since

$$|\sin m\varphi| \leqslant |\sin n\varphi| + |\sin(n-m)\varphi| \tag{75}$$

we have

$$E_{n,m}(\alpha, \beta) \geqslant |\alpha|^{n-m} \geqslant |\alpha|^2$$

unless $n - m = 1$. In this final case we have, by (75)

$$\left| \frac{\sin n\varphi}{\sin m\varphi} \right| \geqslant 1 - \left| \frac{\sin \varphi}{\sin m\varphi} \right|$$

and by the well known inequality

$$\left| \frac{\sin \varphi}{\sin m\varphi} \right| \geqslant \frac{1}{m}.$$

Hence

$$E_{n,m}(\alpha, \beta) \geqslant |\alpha| \left(1 - \left| \frac{\sin \varphi}{\sin m\varphi} \right| \right) + |\alpha|^{m+1} \left| \frac{\sin \varphi}{\sin m\varphi} \right|$$
$$\geqslant |\alpha| + \frac{|\alpha|^{m+1} - |\alpha|}{m} \geqslant |\alpha| + |\alpha|\big(|\alpha| - 1\big) = |\alpha|^2,$$

where in the middle we have used Bernoulli's inequality. It follows, by Lemma 17, that $L(Q) \geqslant 1 + |\alpha|^2$ for every $Q \in T_2(P)$, hence, by Lemma 4,

$$l(P) \geqslant 1 + |\alpha|^2 > 2|\alpha|. \qquad \square$$

Proof of Corollary 2. If $\deg P = 1$, then $l(P) \in K(P)$ follows from Proposition A. If $P = a(x - \alpha)(x - \beta)$, where $|\alpha| \geqslant |\beta| > 1$, then, by Theorem 2, $l(P)$ is attained and by Theorem 1, $l(P) \in K(P)$. If $P = a(x - \alpha)(x - \beta)$, where $|\beta| = 1$, then, by Theorem 6, $l(P) = 2|a\alpha|$. Since either $|\alpha| = 1$ or $\alpha \in \mathbb{R}$, $l(P) \in K(P)$ follows. $\square$

Proof of Corollary 3. If, in the notation of the Corollary, $|\beta| > 1$, then, by Proposition A, $l(P^*) = |\alpha\beta|$ and, by Proposition (ii) $l(P) \geqslant |\alpha\beta|$, thus $\widehat{l}(P) = |\alpha\beta|$. If $|\alpha| > 1 = |\beta|$, then, by Proposition (iii) and Theorem 6, $l(P^*) = 2|\alpha| = l(P)$, thus $\widehat{l}(P) = 2|\alpha|$. If $|\alpha| > 1 > |\beta|$, then, by Proposition A, $l(P^*) = 1 + |\alpha|$, $l(P) = |\alpha\beta|(1 + |\beta|^{-1})$, hence $\widehat{l}(P) = |\alpha| + \min\{1, |\alpha\beta|\}$. If $|\alpha| = 1 = |\beta|$, then by Theorem 6, $l(P) = l(P^*) = 2$. If $|\alpha| = 1 > |\beta|$, then, by Proposition A, $l(P) = 2$, by Theorem 6, $l(P^*) = |\alpha\beta|2|\beta|^{-1} = 2$, thus $\widehat{l}(P) = 2$. Finally, if $|\alpha| < 1$, then by Proposition A, $l(P) = 1$, by Proposition (ii) $l(P^*) \geqslant 1$, thus $\widehat{l}(P) = 1$. $\square$

Proof of Corollary 4. If $|\alpha| > 1 > |\beta| > 0$ we have $\widehat{l}(x - \alpha) = |\alpha|$, $\widehat{l}(x - \beta) = 1$,

$$\widehat{l}((x - \alpha)(x - \beta)) = |\alpha| + \min\{1, |\alpha\beta|\} > |\alpha|. \qquad \square$$

Note added in proof. An apparently similar problem has been considered in [2] and [3]. However, the restriction of G in the definition of $l(P)$ to polynomials with integer coefficients makes a great difference, shown by the fact, clear from Lemma 17 above, that no analogue of Lemma 2 of [2] or Lemma 3 of [3] holds in our case.

References

[1] A. Dubickas, *Arithmetical properties of powers of algebraic numbers*. Bull. London Math. Soc. 38 (2006), 70–80.

[2] M. Filaseta, M. L. Robinson, F. S. Wheeler, *The minimal Euclidean norm of an algebraic number is effectively computable*. J. Algorithms 16 (1994), 309–333.

[3] M. Filaseta, I. Solan, *Norms of factors of polynomials*. Acta Arith. 82 (1997), 243–255.

[4] K. Mahler, *On some inequalities for polynomials in several variables*. J. London Math. Soc. 37 (1962), 341–344.

[5] O. Perron, *Algebra*, Band II. Walter de Gruyter, 1927.

Part E

Polynomials in several variables

Commentary on E: Polynomials in several variables

by Umberto Zannier

Professor Schinzel's taste for polynomials is well known and the topic is quite central in the whole of his mathematical achievements. He has been interested in the algebraic, the arithmetical and the functional points of view. In this section I will describe in some detail nine of his contributions to the theory of polynomials in several variables.

E1. This paper raises nine interesting problems on polynomials, discussing their motivations and mutual relationships. Since that time, some of them have been solved, more or less completely, often with substantial contribution by Schinzel; in any case they have been rather influential.

Problems 1, 2, 3 enquire respectively *about the reducibility of* $f(X) - g(Y)$, $(f(X) - f(Y))/(X - Y)$ *and* $f(X) + g(Y, Z)$, *for polynomials* f, g *with complex coefficients*. Some families of examples of reducibility are given and it is asked whether they represent the most general possibility.

The problems proved to be substantial, involving several mathematical fields. In 1968 J. W. S. Cassels and M. Guy related the first problem to monodromy, combinatorial group theory and the classification of finite simple groups; soon new examples of reducibility were produced by B. Birch and subsequent work arose until recently in papers by Schinzel (see e.g. **E3**, **E7** below), M. Fried, W. Feit, P. Cassou-Nogues & J.-M. Couveignes and others. A complete classification of the reducible cases is now available when either f or g is indecomposable (i.e. not of the form $a \circ b$ non-trivially). In the most general form the problem still awaits a complete solution.

The second problem was solved in 1970 by Fried, who established at the same time a related conjecture of Schur on the "permutation polynomials modulo p". The methods were again linked with monodromy representations and group theory, opening a vast field of research, still alive.

As remarked in an "Added in proof", the third problem also was solved, by Schinzel himself jointly with H. Davenport, in a paper which answers the next Problem 4 as well. The solution shows that $f(X) + g(Y, Z)$ *is reducible if and only if* $g(Y, Z) = a(b(Y, Z))$, *where* $f(X) + a(T)$ *is reducible*; this also relates the question with Problem 1. (See **E2** below for an extension.)

The fourth problem reminds of Bertini (and Hilbert) Irreducibility Theorem: it asks for *complex irreducible polynomials* $f(X, Y, Z)$ *which become reducible for every special-*

ization of Z to a polynomial $Z(X, Y)$. Again, a family of examples is given and it is asked whether it represents all possible cases.

The relation of this problem with Hilbert's theorem is discussed, motivating the fifth and sixth problems; they are concerned with parametric Diophantine equations and ask resp. *whether a polynomial* $f \in \mathbb{Q}[X_1, \ldots, X_n, Y, Z]$ *exists such that the equation* $f(x_1, \ldots, x_n, Y, Z) = 0$ *is solvable in integers (resp. rational)* y, z, *for all* $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ *(resp.* $\in \mathbb{Q}^n$*) but the equation* $f(X_1, \ldots, X_n, \varphi, \psi) = 0$ *is not solvable identically in rational functions* $\varphi, \psi \in \mathbb{Q}(X_1, \ldots, X_n)$. The paper itself announces a (negative) solution of certain special cases in joint work by Schinzel with Davenport and D. J. Lewis. The general question may be seen as a kind of local–global principle for function fields and, as predicted by Schinzel, has proved to be very difficult. Further cases have been however solved (again in the negative) by Davenport, Lewis, Schinzel (they treated parametrized quadratic forms); for counterexamples based on Selmer's conjecture in the theory of elliptic curves see [9] and [3]. Some of such results have implications in the theory of the specializations of Brauer groups, developed by J-P. Serre and others.

Schinzel gives the striking example $f(X_1, Y, Z, T) = 28X_1^2 + 1 - Y^2 - Z^2 - T^2$ answering in the affirmative the analogue of Problem 5 for three free variables Y, Z, T and then states the seventh problem, in a related context; in practice it asks *to describe the irreducible polynomials* $f \in \mathbb{Q}(X, Y)$ *such that for an infinite set* $S = S_f \subset \mathbb{Q}$ *and for every* $x \in S$ *the equation* $f(x, Y) = 0$ *has a solution* $y \in S$. I do not know the actual state of knowledge for this problem. An example where f is neither linear in Y nor symmetric is $f(X, Y) = Y^2 - 2(X^2 + X)Y + (X^2 - X)^2$; then the set S of squares (in $\mathbb{Q}$ or even $\mathbb{Z}$) satisfies the condition.

The last two problems concern trinomials in one variable, and are motivated by certain classical results, like Capelli's theorem, known for binomials $X^n - a$. Problem 8 asks *whether there exists a number* K *such that any trinomial in* $\mathbb{Q}[X]$ *has an irreducible factor (over* $\mathbb{Q}$*) whose number of terms is* $\leqslant K$. Though much work on the irreducibility theory of lacunary polynomials has been done since then, mainly by Schinzel, this problem is to my knowledge still unsolved. However the results of Schinzel to be mentioned in connection with the next problem show that the answer is affirmative if we fix the coefficients of the trinomial and let the degrees of the terms vary. For partial results for k-nomials see [4] and for related results see [2]. The present record is $K \geqslant 9$ (see the paper [14], Table 5, entry 43b, p. 546).

Finally, here is the last, ninth, problem, solved by Schinzel himself. Let $f(X) = X^m + aX^n + b \in \mathbb{Z}[X]$ and let $\bar{f}(X)$ be the monic polynomial whose complex roots are precisely the roots of f which are not roots of unity. It may happen that even $\bar{f}$ is reducible over $\mathbb{Q}$; the problem asks *whether there exist* $a, b \neq 0$ *such that this phenomenon occurs correspondingly to infinitely many ratios* m/n. Schinzel's negative answer to this question was published in 1965 [10]. Since then, Schinzel has developed a much more general, difficult, theory, which appears for instance in his last book; so now the solution appears as merely a corollary of such research (see e.g. Thm. 76 of the book for trinomials with coefficients a, b in an arbitrary totally real field or a totally complex quadratic extension of such a field).

E2. This paper deals with a vast generalization of Problem 3 in **E1** above, namely with the question of the reducibility of $\Phi(F_1(\boldsymbol{X}_1), \ldots, F_n(\boldsymbol{X}_n))$ (over an arbitrary field K)

where $\boldsymbol{X}_i$ are non-empty disjoint sets of variables and Φ, F_i are polynomials over K such that Φ has positive degree in each variable and at least two of the F_i are non-constant. The main result reduces the problem to the case when each F_i depends on a single variable; in fact, it is proved that *$\Phi(F_1(\boldsymbol{X}_1), \dots, F_n(\boldsymbol{X}_n))$ is reducible over K if and only if $F_i(\boldsymbol{X}_i) = G_i(H_i(\boldsymbol{X}_i))$ where $G_i \in K[U]$, $H_i \in K[\boldsymbol{X}_i]$ and $\Phi(G_1(U_1), \dots, G_n(U_n))$ is reducible in K*.

To recover the solution of Problem 3 at **E1**, it suffices to take $\Phi(T_1, T_2) = T_1 + T_2$, $F_1(\boldsymbol{X}_1) = F(X)$, $F_2(\boldsymbol{X}_2) = G(Y, Z)$. This had already been obtained with Davenport, but the present result goes beyond that paper, also because it allows arbitrary characteristic.

The proof proceeds roughly as follows. A first step is by induction, to reduce to the case of a polynomial $\Psi(F(\boldsymbol{X}), Y)$ (i.e. to the case $n = 2$, $\boldsymbol{X}_1 = \boldsymbol{X}$, $\boldsymbol{X}_2 = Y$). Next, viewing a possible factor as a polynomial in Y, one observes that its roots are algebraic over $K(F(\boldsymbol{X}))$ and so the same is true of their symmetric functions $r_1(\boldsymbol{X}), \dots, r_s(\boldsymbol{X})$, say. Hence the field $K(F(\boldsymbol{X}), r_1(\boldsymbol{X}), \dots, r_s(\boldsymbol{X}))$ is the function field of a curve, parametrized by $\boldsymbol{X}$. Now a version of Lüroth Theorem implies that the parametrization for the curve may be suitably changed, so to depend on one variable $U = U(\boldsymbol{X})$ only, rather than the set of variables $\boldsymbol{X}$. Then, expressing $F(\boldsymbol{X})$ and the $r_i(\boldsymbol{X})$ as rational functions of U and reversing the arguments yields the sought result.

The results of this paper have been generalized by [12] and further by Geyer [8], with a different method.

E3. This paper deals with the reducibility of a polynomial of the shape $f(X) - g(Y)$, i.e. Problem 1 of **E1** above. Beyond the families of reducibility $a(b(X)) - a(c(Y))$ and $T_4(b(X)) + T_4(c(Y))$ ($T_4(z) = 8z^4 - 8z^2 + 1$) Birch, Cassels and Guy had found further examples (in degrees 7 and 11) involving however irrational coefficients. In this paper Schinzel shows that, although we seek reducibility over $\mathbb{C}$, rationality of the coefficients may be relevant! The main result in fact asserts that *if $f, g \in \mathbb{Q}[T]$ are non-constant and $\deg f = p$ is prime, then $f(X) - g(Y)$ is reducible over $\mathbb{C}$ if and only if $g(Y) = f(c(Y))$.* (Clearly now we fall into the first of the mentioned families.)

A further conclusion on the rationality of $c(T)$ is drawn (we omit this here) and also a Corollary stating that in the above assumptions reducibility over $\mathbb{C}$ and over $\mathbb{Q}$ are equivalent if one excludes the cases $f(X) - g(Y) = A(X + \alpha)^p - Bd(Y)^p$, $A, B, \alpha \in \mathbb{Q}$, $d \in \mathbb{Q}[X]$.

As to Schinzel's proof, first he uses a simple result of Ehrenfeucht to assume that p divides $\deg g = kp$. Now, a hypothetical factorization $f(X) - g(Y) = \prod_{i=1}^{r} h_i(X, Y)$ ($r > 1$) yields a factorization for the highest homogeneous parts (giving X the weight k): $X^p - aY^{kp} = \prod_{i=1}^{r} H_i(X, Y)$, say. Now the rationality enters into the picture, through comparison of the factorization over $\mathbb{Q}(\sqrt[p]{a})$ of the left side (Lemma 1 says there are just two factors of degrees 1, $p - 1$ in X) and of the right side. (Here $\sqrt[p]{a}$ is the rational root if a is a p-th power in $\mathbb{Q}$ and any root otherwise.) All the coefficients may be assumed to be algebraic so Galois action (over $\mathbb{Q}(\sqrt[p]{a})$) essentially permutes the factors h_i. Inspection of this action then shows that the H_i which is divisible by $X - \sqrt[p]{a}Y^k$, say H_1, must be linear in X, whence the same holds for h_1, yielding the sought conclusion.

Fried [6] has generalized the result to the case when $\deg f$ is an odd prime-power.

E4. It will be convenient to start by recalling a few points concerning the reducibility (over $\mathbb{Q}$) of lacunary polynomials, say of the form $f(X) = a_0 + a_1 X^{m_1} + \ldots + a_k X^{m_k}$. One of the main goals in Schinzel's theory is to establish reducibility criteria when the a_i are *given* rationals (or algebraic), and where the m_i are *variable* integers. Now, the possible *cyclotomic factors* occur periodically and are easy to detect. For these reasons it is sensible to look at the reducibility of "Kf", Schinzel's notation for f deprived of all its cyclotomic factors. Still other factors that play a special role are the *reciprocal* ones, i.e. those invariant by $f(X) \mapsto X^{\deg f} f(1/X)$; dividing out f by all the reciprocal irreducible factors leaves with "Lf", in Schinzel's notation.

Coming to the paper in question, the main theme is to understand the irreducibility of Kf and Lf when $f(X) = aX^m + bX^n + cX^p + d$ is a quadrinomial over $\mathbb{Q}$. The second question is given a solution which is in a way complete: for given integer coefficients a, b, c, d, Theorem 2 reduces the problem to test a certain explicit finite set of cases.

In particular it turns out that either f can be divided into two binomials with a common factor, or Lf can be reducible only if the mutual ratios $(m : n : p)$ belong to a certain finite set (depending only on the coefficients). This answers a (more difficult) analogue of Problem 9 in **E1**.

As to Kf, the authors have a Theorem 3, similar to Theorem 2 but for the cases $a = 1$, $b = \pm 1$, $c, d \in \mathbb{Z}$, $0 < |c| \leqslant |d|$, $m > n > p > 0$.

A fundamental tool in the rather intricate proofs is a 1969 result by Schinzel [11]; this is used to reduce to the case of two variables, which brings us to Theorem 1 of the present paper. This remarkable result gives a complete classification of the reducible quadrinomials in two variables, over any field of characteristic zero. It is found that a reducible quadrinomial in Y_1, Y_2 either is really a function of a single variable $Y_1^p Y_2^q$ or may be divided into two parts with a binomial common factor or is of one of certain three explicit types (that is, $c(U^3 + V^3 + W^3 - 3UVW)$, $c(U^2 - 4TUVW - T^2V^4 - 4T^2W^4)$ or $c(U^2 + 2UV + V^2 - W^2)$, for a constant c and monomials T, U, V, W in Y_1, Y_2).

The main points of the proof are as follows. First, via a suitable substitution $Y_i \mapsto X^{a_i} Y^{b_i}$, one writes the quadrinomial, up to a monomial factor, in the form $f(X) - g(Y)$ where f, g are binomials; so we essentially arrive at a special case of Problem 1 of **E1**. One views the curve $f(X) = g(Y)$ as the fibred product over the λ-sphere of the curves $f(X) = \lambda$, $g(Y) = \lambda$, so the splitting fields of these last equations over $K(\lambda)$ are relevant. One now uses a 1973 result by Fried [7] (i.e. [4] from **E4**, completely referred only in the Addendum([1])) to go to the case when such splitting fields are equal. The final point is a separate study of the permutation representations of the monodromy of both covers of the λ-sphere; this yields the Galois structure of the splitting fields and enables one to get informations from their equality; this comparison leads to the sought conclusion.

For the case of positive characteristic see Ch. II of Schinzel's second book [15]. For reducibility of Kf, f any non-reciprocal quadrinomial, see Schinzel [13]; the reducibility of reciprocal quadrinomials remains an open problem.

E5. This paper gives in the first place a sufficient irreducibility criterion depending only on the structure of the monomials which appear.

([1]) and in the present volume

Let $F(X_1, \dots, X_l) = \sum_{j=0}^{k} a_j \prod_{i=1}^{l} X_i^{\nu_{ij}}$ be a $(k+1)$-nomial over a field K, supposed not divisible by any variable X_i and such that $a_0 \cdots a_k \neq 0$. Theorem 1 of the paper asserts that *if the vectors* $\boldsymbol{v}_j := (\nu_{0j}, \dots, \nu_{lj})$ *are distinct and the rank of the matrix of the* $\boldsymbol{v}_j$ (*over the prime field*), *completed with* $(1, \dots, 1)$ *in the last column, is equal to its rank over* $\mathbb{Q}$ *and is* $> (k+3)/2$, *then* F *is irreducible over* K. (In Ch. II of Schinzel's second book it is shown that, with a genuine exception, it is sufficient to consider the rank over the rationals.) A Corollary also shows that if $K = \mathbb{C}$ and F contains a constant term it suffices that the rank of the $\boldsymbol{v}_j$ is $> (k+1)/2$. Note that the rank expresses how many of the monomials which appear are multiplicatively independent.

Finally, an application is given to Theorem 2 on the reducibility of $a_0 + \sum_{j=1}^{k} a_j X^{n_j}$ over $\mathbb{Q}$ ($a_i \in \mathbb{Z}$, n_j distinct positive integers). In practice it states that if there is more than one irreducible non-reciprocal factor (see **E4**) then the degrees n_j satisfy at least $[k/2]$ linearly independent linear equation $\sum \gamma_{ij} n_j = 0$ with integers γ_{ij} which are bounded by the k^2-th iterate exponential of $\sum a_j^2$.

It is also remarked that the results are in sense best possible, an example in this direction being $4 + 2\sum_{j=1}^{l} X_j + \sum_{j=l+1}^{2l-1} X_{j-l} X_l = (2 + X_l)(2 + \sum_{i=1}^{l-1} X_i)$.

The proof of Theorem 1 is by induction on l, carried out by means of combinatorial considerations and suitable "monomial" transformations, i.e. of the shape $X_i \mapsto \prod_{j=1}^{l} X_j^{a_{ij}}$.

As to Theorem 2, on the present assumptions a 1969 result by Schinzel (see also **E4**) implies that certain derived polynomials in several variables are reducible. Via Theorem 1 this yields an upper bound for the rank of the relevant matrices, leading to the sought linear relations.

E6. This paper concerns the behavior of polynomials in several variables under substitutions $(z_1, \dots, z_n) \mapsto (z^{r_1}, \dots, z^{r_n})$ for integers $r_i > 0$. A special role is played here by what the authors call *generalized cyclotomic polynomials* (=GCP below), i.e. those of the form $\pm\Phi_m(z_1^{r_1} \cdots z_n^{r_n})$, where Φ_m is the standard m-th cyclotomic polynomial.

Theorem 1 in the paper shows that: *If* $F \in \mathbb{Z}[z_1, \dots, z_n]$ *is irreducible and not GCP but* $F(z^{r_1}, \dots, z^{r_n})$ *is a product of cyclotomic polynomials, then* $(r_1, \dots, r_n)$ *lies in the union of a finite set of hyperplanes of* $\mathbb{Q}^n$ *depending* (*explicitly*) *only on* F.

Several consequences are drawn. A very interesting one is a generalization of a celebrated result by Kronecker, that an algebraic integer all of whose conjugates lie in the unit-disk must be a root of unity; in fact, Theorem 2 states that: *If* $F \in \mathbb{Z}[z_1, \dots, z_n]$ *has value* 1 *at the origin and has no zero in the poly-unit-disk then* F *is a product of GCP*.

The paper also offers further results, on the zeros of Dirichlet polynomials (which were a main motivation) and also on polynomials over the complex field; we do not pause on this here.

A main tool in the proof of Theorem 1 is played by a result of H. B. Mann on linear relations over $\mathbb{Z}$ among roots of unity; roughly speaking, it bounds the order of the involved roots in terms of the number of summands. Mann's conclusion is applied to the possible relations $F(\zeta^{r_1}, \dots, \zeta^{r_n}) = 0$ for ζ a root of unity.

The concept of GCP introduced in this paper has proved to be substantial and has later evolved into important investigations by Boyd, Lawton, Schinzel, Smith, Dobrowolski, Amoroso, David, Zhang, …. It has turned out that the GCP (where r_i are integers and the denominator is cancelled) and their products are just the polynomials of unit Mahler measure (see the second book by Schinzel for definitions) and essentially they correspond to *torsion subvarieties of* $\boldsymbol{G}_m^n$. In turn, this puts the topic in the general context of heights of algebraic subvarieties of group varieties, a subject which recently has been extremely lively and fruitful, leading to the proof of fundamental results in Diophantine Geometry (we do not attempt here to give more detail or pause on references).

E7. The present paper, though short, raises and solves several interesting questions. One motivation was an almost simultaneous paper [1] by S. Abhyankar and L. A. Rubel on the irreducibility of difference polynomials $p(X)-q(Y)$ (see also **E1**, **E3** above). Actually, in both papers *generalized difference polynomials* (g.d.p.) are considered; these are of the shape $P(X, Y) = AY^n + \sum_{i=1}^{n} P_i(X)Y^{n-i}$, for a constant $A \neq 0$, $n > 0$, $\deg P_n = m > 0$ and $\deg P_i < mi/n$ for $1 \leqslant i < n$. Beyond generalizing the "difference polynomials", the conditions for instance imply that all the Puiseux series in X for the equation $P(X, Y) = 0$ have order m/n at infinity.

In both papers it is proved (Thm. 1 here) that: *If P is a g.d.p. then any two non-constant factors Q, R of P have a common zero.*

This immediately yields some irreducibility criteria, as the Corollary, stating that *$p(X)-q(Y)$ may be reducible only if $p(\alpha) = q(\beta)$ for some α, β with $p'(\alpha) = q'(\beta) = 0$.* (This was however a rather special consequence of a previous 1961 result by Davenport, Lewis and Schinzel.)

Finally, the paper answers several problems raised in [1] about *hereditarily irreducible polynomials* (HIP) $P(x_1, \ldots, x_n)$, i.e. those such that $P(h_1(x_1), \ldots, h_n(x_n))$ is irreducible for all non-constant $h_1, \ldots, h_n$. For instance, the authors produce a HIP in two variables, namely $(x^2+1)y+1$. (Eisenstein criterion over $k[x]$ is used to show that $(a(x)^2+1)b(y)+1$ is anyway irreducible.)

E8. The paper considers representations of a given polynomial $F \in K[\boldsymbol{X}]$ as $\sum_{\mu=1}^{M} f_\mu(L_\mu(\boldsymbol{X}))$, where the L_μ are linear forms in $\boldsymbol{X} = (x_1, \ldots, x_n)$ and the f_μ depend on a single variable.

Generalizing previous results, several theorems are proved concerning (i) the smallest possible M (e.g. if $d := \deg F$ one may take $M \leqslant \binom{n+d-1}{n-1}$) and (ii) the possible choice of the forms L_μ in a given *finite* set. As corollaries, one improves results on the classical problem of the representation of a form of degree d as a linear combination of a bounded number of d-th powers of linear forms (*Waring's problem for forms*); for instance it is deduced from Thms. 1, 2 that $\binom{n+d-1}{n-1}$ (resp. d) summands suffice if $\operatorname{char} K = 0$ (resp. and if $n = 2$). (For the result concerning forms see [5].) Recently A. Białynicki-Birula and A. Schinzel replaced $\binom{n+d-1}{n-1}$ by $\binom{n+d-2}{n-1}$.

Some of the main arguments are *explicit*: to find the sought representations one equates coefficients of both sides, viewing the coefficients of the f_μ as unknowns (and letting the

L_μ vary in a "sufficiently large" finite set). This leads to (complicated) linear systems, which are shown to be non-singular (Lemma 2), yielding the required solutions.

Looking at a "generic" polynomial F the bounds sometimes may be lowered; in the case of binary forms, the best possible value is given in Thm. 6 (for algebraically closed K).

E9. This paper discusses the group of *automorphs* of a binary form $f(x, y) \in k[x, y]$ over a field k, i.e. the group $\mathrm{Aut}(f, k)$ of linear maps T, defined over k, such that $f(T(x, y)) = rf(x, y)$ for a constant $r = r_T$ (when $r = 1$ one speaks of *strict automorphs*).

This topic, plainly related to the well-known important theory of finite subgroups of PGL_2, has a very rich history dating back to long ago, and has been considered by mathematicians such as A. Clebsch, L. Dickson, P. Gordan, F. Klein, B. Segre, J-P. Serre and several others, until very recently.

When the ground field k is $\mathbb{C}$ all the possible finite subgroups of PGL_2 may actually appear as groups of automorphs, as was shown by Klein. The question becomes more delicate for general fields. The present paper discusses this in full generality (even in the case of fields of positive characteristic which are moreover non-perfect, which escaped from all previous investigations by Klein, Dickson, Segre). Section 2 determines all forms f with a given subgroup of $\mathrm{Aut}(f, k)$.

Section 3 bounds the order of $\mathrm{Aut}(f, k)$.

Another question, dealt with in Section 4, is to decide whether a given form has a nontrivial automorph defined over k; for $k = \mathbb{Q}$ this was considered by Segre, for quadratics and cubics; here an answer is given generally, in terms of the Galois group of $f(x, 1)$ over k.

The paper contains several other related results, stated in eight theorems and various corollaries and lemmas. There is also a preliminary Section 1, of considerable independent interest, on finite subgroups of $\mathrm{PGL}_2(k)$ for arbitrary fields k.

E10. Let K be a field and let $f \in K[x_1, \ldots, x_n]$ be a symmetric polynomial. Then f can be written as $f = F(\tau_1, \ldots, \tau_n)$, where F is also a polynomial over K and $\tau_1, \ldots, \tau_n$ are the elementary symmetric functions of $x_1, \ldots, x_n$.

In the present paper the reducibility (over K) of f is related to the reducibility of F. To my knowledge this question is new, despite its naturality.

Theorem 1 gives a remarkable very neat criterion, valid if the number of variables n is larger than $\max(4, \deg F + 1)$. Under this assumption it is proved that *f is reducible if and only if either F is reducible or F is of the shape*

$$c\,\mathrm{Norm}_K^{K(\alpha)}(\alpha^n + x_1\alpha^{n-1} + \ldots + x_n)$$

for $c \in K^*$ and α algebraic over K.

Observe that the stated shape produces in fact reducibility of f since

$$\alpha^n + \tau_1\alpha^{n-1} + \ldots + \tau_n = \prod_{i=1}^{n}(\alpha + x_i).$$

The proof of the necessity splits into two parts, according as one of the hypothetical irreducible factors of f depends on a single variable or not. In the first case one recovers the above stated norm-form shape. In the second case one acts on the factorization with

the symmetric group. If the factor is not symmetric one gets a contradictions through a lemma which considers degrees. If the factor is symmetric one recovers reducibility of F.

The paper also contains Theorem 2, working under the milder condition $n > \deg F + 1$ but assuming that f is isobaric with respect to the weight i for x_i.

This Theorem 2 implicitly also shows that the "$n > 4$" of Theorem 1 cannot be replaced by "$n > 3$". A counterexample occurs when $\mathrm{char}(K) \neq 3$, K contains a primitive cubic root of 1 and $F = a(x_2^2 - 3x_1x_3 + 12x_4)$ for $a \in K^*$.

References

[1] S. Abhyankar, L. A. Rubel, *Every difference polynomial has a connected zero-set*. J. Indian Math. Soc. (N.S.) 43 (1979), 69–78.

[2] A. Bremner, *On reducibility of trinomials*. Glasgow Math. J. 22 (1981), 155–156.

[3] J. W. S. Cassels, A. Schinzel, *Selmer's conjecture and families of elliptic curves*. Bull. London Math. Soc. 14 (1982), 345–348; this collection: A11, 62–66.

[4] A. Choudhry, A. Schinzel, *On the number of terms in the irreducible factors of a polynomial over* $\mathbb{Q}$. Glasgow Math. J. 34 (1992), 11–15.

[5] W. J. Ellison, *A 'Waring's problem' for homogeneous forms*. Proc. Cambridge Philos. Soc. 65 (1969), 663–672.

[6] M. Fried, *On the Diophantine equation* $f(y) - x = 0$. Acta Arith. 19 (1971), 79–87.

[7] —, *The field of definition of function fields and a problem in the reducibility of polynomials in two variables*. Illinois J. Math. 17 (1973), 128–146.

[8] W.-D. Geyer, *On the irreducibility of sums of rational functions with separated variables*. Israel J. Math. 85 (1994), 135–168.

[9] D. J. Lewis, A. Schinzel, *Quadratic Diophantine equations with parameters*. Acta Arith. 37 (1980), 133–141; this collection: A10, 54–61.

[10] A. Schinzel, *On the reducibility of polynomials and in particular of trinomials*. Acta Arith. 11 (1965), 1–34; *Errata*, ibid., 491; this collection: D2, 301–332.

[11] —, *Reducibility of lacunary polynomials* I. Acta Arith. 16 (1969), 123–159; *Corrigenda*: Acta Arith. 19 (1971), 201; ibid. 24 (1978), 265; this collection: D4, 344–380.

[12] —, *Reducibility of polynomials in several variables* II. Pacific J. Math. 118 (1985), 531–563.

[13] —, *Reducibility of lacunary polynomials* VI. Acta Arith. 47 (1986), 277–293.

[14] —, *On reducible trinomials*. Dissert. Math. (Rozprawy Mat.) 329 (1993); *Errata*, Acta Arith. 73 (1995), 399–400; this collection: D10, 466–548.

[15] —, *Polynomials with Special Regard to Reducibility*. Encyclopaedia of Mathematics and its Applications 77, Cambridge Univ. Press, Cambridge 2000.

Originally published in
Neki nerešeni problemi u matematici
Matematička Biblioteka 25, Beograd 1963, 63–70

Some unsolved problems on polynomials

The aim of this paper is to discuss 9 problems connected with the irreducibility of polynomials.

Let $k[x, y, \ldots]$ be the ring of polynomials over a field k, $k(x, y, \ldots)$ the corresponding field of rational functions. Further, let $\mathbb{Q}$ be the field of rationals, $\mathbb{C}$ the field of complex numbers, and let

$$T_n(x) = \frac{1}{2}\big(x + \sqrt{x^2-1}\big)^n + \frac{1}{2}\big(x - \sqrt{x^2-1}\big)^n$$

be the n-th Chebyshev polynomial.

We begin with problems concerning absolute irreducibility.

A polynomial

$$a\big(b(x)\big) - a\big(c(y)\big), \quad \text{where} \quad a, b, c \in \mathbb{C}[x], \ \text{degree}\, a > 1, \tag{1}$$

is of course reducible in $\mathbb{C}[x, y]$.

H. Davenport and D. J. Lewis found a polynomial of the form $f(x) - g(y)$ reducible in $\mathbb{C}[x, y]$ and not being of the form (1), namely $T_4(x) + T_4(y)$. Of course, polynomials

$$AT_4\big(b(x)\big) + AT_4\big(c(y)\big), \quad A\text{—constant}, \quad b, c \in \mathbb{C}[x], \tag{2}$$

are also reducible. A condition is given in [2] sufficient for the irreducibility of $f(x)-g(y)$ in $\mathbb{C}[x, y]$ but not necessary. This suggests

Problem 1. *Do there exist non-constant polynomials $f, g \in \mathbb{C}[x, y]$ such that $f(x)-g(y)$ is reducible in $\mathbb{C}[x, y]$ and is neither of the form* (1) *nor* (2)?

A similar question arises when instead of $f(x)-g(y)$, we consider $\dfrac{f(x) - f(y)}{x - y}$. This polynomial is clearly reducible if

$$f(x) = a\big(b(x)\big), \quad \text{degree}\, a > 1, \quad \text{degree}\, b > 1. \tag{3}$$

There exist, however, other cases of reducibility, e.g.

$$f(x) = A(Bx + C)^p + D \quad \text{or} \quad f(x) = AT_p(Bx + C) + D, \tag{4}$$
$$(A, B, C, D\text{—constants}).$$

This suggests

Problem 2. *Does there exist a polynomial* $f \in \mathbb{C}[x]$ *such that* $\dfrac{f(x)-f(y)}{x-y}$ *is reducible in* $\mathbb{C}[x, y]$ *and is neither of the form* (3) *nor* (4)?

A negative answer to this question would furnish a complete solution of the so-called Dickson–Schur problem. The problem consists on determining all polynomials $f \in \mathbb{Q}[x]$ such that for infinitely many primes p, the numbers $f(0)$, $f(1)$, ..., $f(p-1)$ are all different mod p. If the answer to Problem 2 is negative then every such polynomial is obtainable by repeated superposition of a linear function, x^m and $T_n(x)$.

Passing to polynomials in 3 variables we note first the following theorem.

For arbitrary non-constant polynomials $f, g, h \in \mathbb{C}[x]$

$$f(x)+g(y)+h(z) \quad \textit{is irreducible in } \mathbb{C}[x, y, z].$$

This result was proved some years ago by A. Ehrenfeucht and A. Pełczyński, but their proof has not been published: it is short enough to be outlined here.

It is known (cf. [4]) that a polynomial $f(x)+k(t)$ is irreducible in $\mathbb{C}[x,t]$ if (degree f, degree k) $= 1$. Let

$$f(x)=a_\mu x^\mu+\ldots+a_0, \quad g(y)=b_\nu y^\nu+\ldots+b_0,$$
$$h(z)=c_\varrho z^\varrho+\ldots+c_0$$

and suppose that

$$f(x)+g(y)+h(z)=p(x, y, z)q(x, y, z),$$

where neither of the polynomials p, q is constant.

It is possible to find complex numbers A, B, C, D such that

$$\begin{aligned} b_\nu A^\nu + c_\varrho C^\varrho &= 0, \\ \nu b_\nu A^{\nu-1}B + \varrho c_\varrho C^{\varrho-1}D &\neq 0, \end{aligned} \tag{5}$$

$$\begin{aligned} p(x,t) &= p\big(x, t^{2\mu\varrho-1}(At+B), t^{2\mu\nu-1}(Ct+D)\big) \not\equiv \text{const}, \\ q(x,t) &= q\big(x, t^{2\mu\varrho-1}(At+B), t^{2\mu\nu-1}(Ct+D)\big) \not\equiv \text{const}. \end{aligned} \tag{6}$$

Assuming that A, B, C, D satisfy the above conditions and putting

$$k(t)=g\big(t^{2\mu\varrho-1}(At+B)\big)+h\big(t^{2\mu\nu-1}(Ct+D)\big)$$

we find easily from (5) that degree $k = 2\mu\nu\varrho-1$, hence (degree f, degree k) $= 1$.

The polynomial $f(x)+k(t)$ is, therefore, irreducible in $\mathbb{C}[x,t]$ and on the other hand

$$f(x)+k(t)=p(x,t)q(x,t),$$

which contradicts formulae (6).

The theorem is thus proved. It suggests

Problem 3. *Do there exist non-constant polynomials* $f \in \mathbb{C}[x]$, $g \in \mathbb{C}[y,z]$ *such that* $f(x)+g(y,z)$ *is reducible in* $\mathbb{C}[x, y]$ *and* g *is not of the form* $a(b(y,z))$, *where* $a \in \mathbb{C}[t]$, $b \in \mathbb{C}[y,z]$ *and* $f(x)+a(t)$ *is reducible in* $\mathbb{C}[x,t]$?

Let us consider now a general polynomial in three variables $f(x, y, z)$ irreducible in $\mathbb{C}[x, y, z]$. It can happen that for every value of z, f becomes reducible in $\mathbb{C}[x, y]$, e.g. if $f(x, y, z) = (xy)^2 - z$. There is the same situation, if

$$f(x, y, z) = q(x, y, z)^n h\left(\frac{p(x, y, z)}{q(x, y, z)}, z\right), \tag{7}$$

where $p, q \in \mathbb{C}[x, y, z]$ and $h(t, z)$ is of degree $n > 1$ in t.

This suggests the next problem.

Problem 4. *Does there exist a polynomial $f(x, y, z)$ irreducible in $\mathbb{C}[x, y, z]$, reducible for every $z \in \mathbb{C}[x, y]$ and not of the form* (7)?

It follows from a certain theorem of E. Noether [7] that a polynomial $f(x, y, z)$ is reducible in $\mathbb{C}[x, y]$ either only for finitely many z or for all but finitely many z.

Problem 4 has brought us near the circle of ideas connected with Hilbert's Irreducibility Theorem. It is a particular case of this theorem that if

$$f(x_1, x_2, \ldots, x_n, y) = \prod_{j=1}^{k} f_j(x_1, x_2, \ldots, x_n, y)$$

is the factorization of a polynomial $f \in \mathbb{Q}[x_1, x_2, \ldots, x_n, y]$ into polynomials irreducible in $\mathbb{Q}[x_1, x_2, \ldots, x_n, y]$, then for infinitely many integer systems $(x_1, x_2, \ldots, x_n)$ the polynomials f_j are irreducible in $\mathbb{Q}[y]$. It follows hence that if an equation

$$f(x_1, x_2, \ldots, x_n, y) = 0 \tag{8}$$

is soluble in an integer y for all integer systems $(x_1, x_2, \ldots, x_n)$, then there exists a polynomial $\varphi \in \mathbb{Q}[x_1, x_2, \ldots, x_n]$ such that

$$f(x_1, x_2, \ldots, x_n, \varphi) \equiv 0 \tag{9}$$

identically.

Similarly, if the equation (8) is for all rational systems $(x_1, x_2, \ldots, x_n)$ soluble in rational y, then there exists a rational function

$$\varphi \in \mathbb{Q}(x_1, x_2, \ldots, x_n)$$

such that (9) holds identically.

This suggests

Problem 5. *Does there exist a polynomial*

$$f \in \mathbb{Q}[x_1, x_2, \ldots, x_n, y, z]$$

such that for all integer systems $(x_1, x_2, \ldots, x_n)$ the equation

$$f(x_1, x_2, \ldots, x_n, y, z) = 0 \tag{10}$$

is soluble in integers y, z and for no rational functions

$$\varphi, \psi \in \mathbb{Q}(x_1, x_2, \ldots, x_n),$$

the identity

$$f(x_1, x_2, \ldots, x_n, \varphi, \psi) \equiv 0 \tag{11}$$

holds?

Problem 6. *Does there exist a polynomial*

$$f \in \mathbb{Q}[x_1, x_2, \ldots, x_n, y, z]$$

such that for all rational systems $(x_1, x_2, \ldots, x_n)$ *the equation* (10) *is soluble in rational* y, z *and for no rational functions*

$$\varphi, \psi \in \mathbb{Q}(x_1, x_2, \ldots, x_n),$$

the identity (11) *holds*?

To answer these problems seems to me very difficult even for $n = 1$. A negative answer to Problem 5 in some interesting particular cases can be deduced from a certain theorem of Bauer (cf. [3]).

It is noteworthy that an equation $f(x, y, z, t) = 0$ can be soluble in integers y, z, t for all integer values of x, in spite of the fact that for no rational functions $\varphi, \psi, \chi \in \mathbb{Q}(x)$, the identity $f(x, \varphi, \psi, \chi) \equiv 0$ holds. As an example we can take

$$f(x, y, z, t) = 28x^2 + 1 - y^2 - z^2 - t^2.$$

It follows from the theorem of Gauss on sums of three squares that for every integer x, there are integers y, z, t such that $y^2 + z^2 + t^2 = 28x^2 + 1$. Suppose that rational functions $\varphi, \psi, \chi \in \mathbb{Q}(x)$ satisfy the identity

$$\varphi^2(x) + \psi^2(x) + \chi^2(x) = 28x^2 + 1.$$

Clearly

$$\varphi(x) = \frac{ax + O(1)}{m}, \quad \psi(x) = \frac{cx + O(1)}{m}, \quad \chi(x) = \frac{ex + O(1)}{m},$$

where a, c, e, m are integers, and we get

$$a^2 + c^2 + e^2 = 28m^2 = 4^h(8k + 7).$$

This is however impossible by Gauss's theorem.

As a last question connected with Hilbert's theorem we shall formulate

Problem 7. *Does there exist an infinite set* $S \subset \mathbb{Q}$ *and a polynomial* f *irreducible in* $\mathbb{Q}[x, y]$ *satisfying the following conditions*:
(i) *for every* $x \in S$ *there exists a* $y \in S$ *such that* $f(x, y) = 0$,
(ii) $f(x, y)$ *is neither linear in* y *nor symmetric in* x *and* y?

In order to see that (i) can hold if $f(x, y)$ is symmetric in x and y, it suffices to define S as the set of all rational x for which $f(x, y)$ is soluble in rational y (this set clearly can be infinite).

It follows from Hilbert's theorem that the answer to Problem 7 is negative if $S = \mathbb{Q}$; W. Narkiewicz [6] has shown that the answer is negative if f is linear in x.

Now we pass to problems concerning the irreducibility of trinomials in $\mathbb{Q}[x]$.

K. Th. Vahlen [11] and A. Capelli [1] gave a simple criterion for the reducibility of a binomial in $\mathbb{Q}[x]$: $x^n - a$, where a is an integer, is reducible in $\mathbb{Q}[x]$ if and only if, for some $p > 1$, $p \mid n$ and $a = b^p$ or $4 \mid n$ and $a = -4b^4$, b an integer.

It follows from this criterion that *every binomial* $\in \mathbb{Q}[x]$ *has an irreducible factor, which is either binomial or trinomial.*

We shall prove it for $x^m - a$, a integer, by induction with respect to m. For $m = 1$, the theorem is trivially true. Suppose that it is true for all $m < n$ and all integers $a \neq 0$. Now, if $x^n - a$ is irreducible, it is itself its required factor. If $p > 1$, $p \mid n$, $n = pk$ and $a = b^p$ then $x^k - b \mid x^n - a$, and the inductive assumption applies to $x^k - b$. By the theorem of Vahlen–Capelli it remains to consider the case $4 \mid n$; $n = 4k$, $a = -4b^4$. We have then

$$x^n - a = (x^{2k} - 2bx^k + 2b^2)(x^{2k} + 2bx^k + 2b^2).$$

If $x^{2k} - 2bx^k + 2b^2$ is irreducible, it is the required factor of $x^n - a$. If it is reducible, $g(x) \mid x^{2k} - 2bx^k + 2b^2$, $g(x) \in \mathbb{Q}[x]$ monic, degree $g < 2k$, we have

$$g(x) = (x - \lambda_1)(x - \lambda_2) \cdots (x - \lambda_j), \quad \text{where } j < 2k$$

and

$$\lambda_i^{4k} = -4b^4 \quad (i = 1, 2, \ldots, j). \tag{12}$$

It follows from (12) that $|\lambda_i|^{2k} = 2b^2$, thus

$$|\lambda_1 \lambda_2 \cdots \lambda_j|^{2k} = (2b^2)^j.$$

Since $g \in \mathbb{Q}[x]$, $|\lambda_1 \lambda_2 \cdots \lambda_j|$ is an integer, thus putting $2k/(j, 2k) = l$ we must have $2b^2 = c^l$, c integer. l is clearly odd, thus

$$x^{n/l} + c^2 \mid x^n + c^{2l} = x^n - a$$

and since $j < 2k$, l is > 1 and the inductive assumption applies to $x^{n/l} + c^2$. The theorem is thus proved. It suggests

Problem 8. *Does there exist an absolute constant K such that every trinomial $\in \mathbb{Q}[x]$ has a factor irreducible in $\mathbb{Q}[x]$ which has at most K terms*?

The identity found by Mrs. H. Smyczek:

$$x^{10} - 12x^2 - 196 = (x^5 + 2x^4 + 2x^3 - 4x^2 - 10x - 14) \times (x^5 - 2x^4 + 2x^3 + 4x^2 - 10x + 14)$$

where both factors are irreducible by Eisenstein's criterion, shows that, if it exists, $K > 6$.

A summary of the few known results concerning the reducibility of trinomials was given by E. S. Selmer [9]. Since the publication of that paper, new results have been obtained by W. Ljunggren [5] and H. Tverberg [10].

For a given $f \in \mathbb{Q}[x]$, let $\overline{f}(x) = \prod(x - \lambda)$, where λ runs through all those roots of f which are not roots of unity. Then the theorem of Ljunggren and Tverberg can be stated as follows:

If $m > n > 1$, $f(x) = x^m \pm x^n \pm 1$, *then* $\overline{f}(x)$ *is irreducible in* $\mathbb{Q}[x]$.

Using Ljunggren's method I proved [8]:

If $m > n > 1$, $\dfrac{n}{m} \neq \dfrac{2}{7}, \dfrac{5}{7}$, $f(x) = x^m - 2x^n + 1$, *then* $\overline{f}(x)$ *is irreducible in* $\mathbb{Q}[x]$.

This suggests the following

Problem 9. *Do there exist integers* $a, b \neq 0$ *such that for infinitely many rational* r, *integers* m, n *can be found satisfying*

(i) $n/m = r$,

(ii) *if* $f(x) = x^m + ax^n + b$, *then* $\overline{f}(x)$ *is reducible in* $\mathbb{Q}[x]$?

Note added in proof. Problems 3 and 4 have been solved by H. Davenport and the writer in [3a].

References

[1] A. Capelli, *Sulla riduttibilità della funzione* $x^n - A$ *in campo qualunque di razionalità*. Math. Ann. 54 (1901), 602–603.

[2] H. Davenport, D. J. Lewis, A. Schinzel, *Equations of the form* $f(x) = g(y)$. Quart. J. Math. Oxford Ser. (2) 12 (1961), 304–312.

[3] —, —, —, *Polynomials of certain special types*. Acta Arith. 9 (1964), 107–116; this collection: A6, 27–35.

[3a] H. Davenport, A. Schinzel, *Two problems concerning polynomials*. J. Reine Angew. Math. 214/215 (1964), 386–391; *Corrigendum* 218 (1965), 220.

[4] A. Ehrenfeucht, *Kryterium absolutnej nierozkładalności wielomianów* (*A criterion of absolute irreducibility of polynomials*). Prace Mat. 2 (1958), 167–169 (Polish).

[5] W. Ljunggren, *On the irreducibility of certain trinomials and quadrinomials*. Math. Scand. 8 (1960), 65–70.

[6] W. Narkiewicz, *Remark on polynomial transformations*. Colloq. Math. 10 (1963), 139–142.

[7] E. Noether, *Ein algebraisches Kriterium für absolute Irreduzibilität*. Math. Ann. 85 (1922), 26–33.

[8] A. Schinzel, *Solution d'un problème de K. Zarankiewicz sur les suites de puissances consécutives de nombres irrationnels*. Colloq. Math. 9 (1962), 291–296; *Correction*, ibid. 12 (1964), 289; this collection: D1, 295–300.

[9] E. S. Selmer, *On the irreducibility of certain trinomials*. Math. Scand. 4 (1956), 287–302.

[10] H. Tverberg, *On the irreducibility of the trinomials* $x^n \pm x^m \pm 1$. Math. Scand. 8 (1960), 121–126.

[11] K. Th. Vahlen, *Über reductible Binome*. Acta Math. 19 (1895), 195–198.

Originally published in
Bulletin de l'Academie Polonaise des Sciences
Série des sciences math., astr. et phys.
XI (1963), 633–638

Reducibility of polynomials in several variables

H. Davenport and the writer proved recently [1] the following theorem: the polynomial $f(x_1, \dots, x_r) + g(y_1, \dots, y_s)$ over any field K of characteristic 0, is reducible if and only if

$$f(x_1, \dots, x_r) = F\big(R(x_1, \dots, x_r)\big),$$
$$g(y_1, \dots, y_s) = G\big(S(y_1, \dots, y_s)\big),$$

where F, G, R, S are polynomials over K and $F(u) + G(v)$ is reducible in K.

The aim of this paper is to prove the following more general

Theorem. *Let $X_1, X_2, \dots, X_n$ be non-empty finite disjoint sets of variables and let $\Phi(v_1, v_2, \dots, v_n)$ and $F_1(X_1), F_2(X_2), \dots, F_n(X_n)$ be polynomials over an arbitrary field K. Suppose that Φ is of positive degree in each v_i $(1 \leqslant i \leqslant n)$ and at least two polynomials among F_i $(1 \leqslant i \leqslant n)$ are non-constant. The polynomial*

$$\Phi\big(F_1(X_1), \dots, F_n(X_n)\big)$$

is reducible in K if and only if

$$F_i(X_i) = G_i\big(H_i(X_i)\big) \quad (1 \leqslant i \leqslant n),$$

where G_i, H_i are polynomials over K and

$$\Phi\big(G_1(u_1), \dots, G_n(u_n)\big)$$

is reducible in K.

Lemma 1. *For every pair of positive integers i and j, where $i \leqslant j$, there exists a polynomial $\Omega_{i,j}(t; v_1, \dots, v_j)$ with integral coefficients and the coefficient at the highest power of t equal to 1 and with the following property. If L is an arbitrary field,*

$$A(y) = \sum_{\nu=0}^{j} a_\nu y^{j-\nu}, \quad B(y) = \sum_{\nu=0}^{h} b_\nu y^{h-\nu} \quad (a_0 b_0 \neq 0)$$

are polynomials over L and $B(y)$ divides $A(y)$, then

$$\Omega_{i,j}\left(\frac{b_i}{b_0}; \frac{a_1}{a_0} \dots, \frac{a_j}{a_0}\right) = 0. \tag{1}$$

Presented by W. Sierpiński on July 23, 1963.

Proof. Denote for a given finite set S of indeterminates by $\tau_\nu(S)$ the ν-th fundamental symmetric function of these indeterminates. Let $U_1, U_2, \dots, U_l$ $(l = 2^j - 1)$ be all the non-empty subsets of the set $U = \{u_1, \dots, u_j\}$.

Put

$$T_{i,k}(u_1, \dots, u_j) = \tau_k\big(\tau_i(U_1), \dots, \tau_i(U_l)\big) \quad (0 \leqslant k \leqslant l). \tag{2}$$

$T_{i,k}(u_1, \dots, u_j)$ is a symmetric polynomial with integral coefficients, thus there exists a polynomial $V_{i,k}(v_1, \dots, v_j)$ with integral coefficients such that

$$T_{i,k}(u_1, \dots, u_j) = V_{i,k}\big(\tau_1(U), \dots, \tau_j(U)\big). \tag{3}$$

Put

$$\Omega_{i,j}(t; v_1, \dots, v_j) = t^l + \sum_{k=1}^{l} (-1)^k V_{i,k}(v_1, \dots, v_j) t^{l-k}. \tag{4}$$

The polynomial $\Omega_{i,j}$ has integral coefficients and the coefficient at the highest power of t equals 1. Suppose now that polynomials $A(y)$, $B(y)$ over a field L satisfy the conditions of the lemma, and let

$$A(y) = a_0(y + \eta_1)(y + \eta_2) \cdots (y + \eta_j)$$

be the factorization of $A(y)$ in a suitable extension of L.

Since $B(y)$ divides $A(y)$, there exists a set $\{\nu_1, \dots, \nu_h\}$ of positive integers $\leqslant j$ such that

$$B(y) = b_0(y + \eta_{\nu_1}) \cdots (y + \eta_{\nu_h}).$$

Hence $b_i/b_0 = \tau_i(\eta_{\nu_1}, \dots, \eta_{\nu_h})$ and

$$\Pi = \prod \left(\frac{b_i}{b_0} - \tau_i(\eta_{\nu_1}, \dots, \eta_{\nu_g}) \right) = 0, \tag{5}$$

where the product is taken over all non-empty sets $\{\nu_1, \dots, \nu_g\}$ of positive integers $\leqslant j$. Now by (2), (3) and (4)

$$\Pi = \Omega_{i,j}\left(\frac{b_i}{b_0}; \tau_1(\eta_1, \dots, \eta_j), \dots, \tau_j(\eta_1, \dots, \eta_j) \right) \tag{6}$$

and since

$$\tau_i(\eta_1, \dots, \eta_j) = \frac{a_i}{a_0} \quad (i \leqslant j),$$

the equality (1) follows from (5) and (6). □

Lemma 2. *Let $F(x_1, \dots, x_k)$ and $\chi_i(t, v)$ be polynomials, $r_i(x_1, \dots, x_k)$ be rational functions over a field K $(1 \leqslant i \leqslant j)$.*

If F is not constant and

$$\begin{matrix} \chi_i(t, v) \neq 0 \\ \chi_i(r_i, F) = 0 \end{matrix} \quad (1 \leqslant i \leqslant j) \tag{7}$$

identically, then there exist polynomials $G(u)$ and $H(x_1, \dots, x_k)$ and rational functions $p_i(u)$ over K such that

$$F(x_1, \dots, x_k) = G\big(H(x_1, \dots, x_k)\big)$$
$$r_i(x_1, \dots, x_k) = p_i\big(H(x_1, \dots, x_k)\big) \quad (1 \leqslant i \leqslant j)$$

identically.

Proof. In the course of the proof, we shall denote by capital letters polynomials over K.

It follows from (7) that the functions F and r_i $(1 \leqslant i \leqslant j)$ generate a subextension of $K(x_1, \dots, x_k)$ of degree of transcendence over K equal to 1. According to a theorem of J. Igusa [2] (cf. Samuel [3]) this is a simple extension of K. Therefore, there exists a rational function $l(x_1, \dots, x_k)$ such that F and r_i $(1 \leqslant i \leqslant j)$ are expressible rationally in terms of l. (For fields K of characteristic 0 this was proved much earlier by P. Gordan and E. Noether, cf. [1].) Let

$$l(x_1, \dots, x_k) = \frac{P(x_1, \dots, x_k)}{Q(x_1, \dots, x_k)}, \quad F = \frac{R(l)}{S(l)}, \quad \text{where} \quad (P, Q) = (R, S) = 1.$$

Denote by r and s the degrees of R and S, respectively. Q, $Q^r R(P/Q)$ and $Q^s S(P/Q)$ are polynomials, relatively prime in pairs, since $(P, Q) = (R, S) = 1$. Now, it follows from the identity

$$F = \frac{Q^r R(P/Q)}{Q^s S(P/Q)} \cdot Q^{s-r} \tag{8}$$

that $Q^s S(P/Q)$ is a constant, say β.

Let $S(x) = \alpha(x - \xi_1) \cdots (x - \xi_s)$ be the factorization of $S(x)$ in a suitable extension K' of K. We have

$$\alpha(P - \xi_1 Q) \cdots (P - \xi_s Q) = Q^s S(P/Q) = \beta,$$

whence $P - \xi_i Q = \gamma_i$ and $\gamma_i \in K'$ $(1 \leqslant i \leqslant s)$. If any two ξ's were distinct, e.g. $\xi_1 \neq \xi_2$, we would get $(\xi_2 - \xi_1)Q = \gamma_1 - \gamma_2$, whence Q and P would be constants which is impossible. Thus $S(x) = \alpha(x - \xi)^s$ and either $s = 0$ or $P - \xi Q = \gamma$, where $\xi, \gamma \in K'$.

If $s = 0$, it follows from (8) that Q is a constant, say $\delta \in K$, and the lemma is satisfied with $H = l = P/\delta$, $G = R/a$.

If $P - \xi Q = \gamma$, Q cannot be a constant; thus $\xi, \gamma \in K$. On the other hand, it follows from (8) that

$$s \geqslant r. \tag{9}$$

Since $l = P/Q = \xi + \gamma/Q$, every function expressible rationally in terms of l can be expressed rationally in terms of Q/γ. Putting $H = Q/\gamma$, we find $F = G(H)$, where

$$G(u) = u^s R\Big(\xi + \frac{1}{u}\Big)/\alpha$$

is a polynomial in view of (9). This completes the proof. □

Lemma 3. *Let $F(x_1, \ldots, x_k)$ and $\Psi(t; y_1, \ldots, y_l)$ be polynomials over K, the former non-constant, the latter of positive degree in each variable. The polynomial*

$$\Psi\big(F(x_1, \ldots, x_k); y_1, \ldots, y_l\big)$$

is reducible in K only if

$$F(x_1, \ldots, x_k) = G\big(H(x_1, \ldots, x_k)\big)$$

where G, H are polynomials over K and

$$\Psi\big(G(u); y_1, \ldots, y_l\big)$$

is reducible in K.

Proof. For the sake of brevity put $(x_1, \ldots, x_k) = X$, $(y_1, \ldots, y_l) = Y$ and let

$$\Psi\big(F(X), Y\big) = P(X, Y)Q(X, Y) \tag{10}$$

be the factorization of $\Psi\big(F(X), Y\big)$. Let

$$\begin{aligned} \Psi\big(F(X), Y\big) &= \sum_{i=0}^{m} A_i\big(F(X)\big)M_i(Y), \quad A_0\big(F(X)\big) \neq 0, \\ P(X, Y) &= \sum_{i=0}^{p} B_i(X)P_i(Y), \quad B_0(X) \neq 0, \end{aligned} \tag{11}$$

$$Q(X, Y) = \sum_{i=0}^{q} C_i(X)Q_i(Y), \quad C_0(X) \neq 0, \tag{12}$$

where M_i, P_i, Q_i are distinct products of powers of $y_1, \ldots, y_l$ ordered so that M_0, P_0, Q_0 are first in inverse lexicographic order.

Consider the greatest common factor $d(u)$ of the polynomials $A_i(u)$ $(0 \leqslant i \leqslant m)$. If $d(u)$ is not constant,

$$\Psi(u, Y) = d(u) \sum_{i=0}^{m} \frac{A_i(u)}{d(u)} M_i(Y)$$

is a factorization of $\Psi(u, Y)$, and the lemma holds with $G(u) = u$, $H = F$.

If $d(u) = 1$, there exist polynomials $D_i(u)$ over K such that

$$\sum_{i=0}^{m} A_i(u)D_i(u) = 1.$$

Hence,

$$\sum_{i=0}^{m} A_i\big(F(X)\big)D_i\big(F(X)\big) = 1$$

and the polynomials $A_i\big(F(X)\big)$ $(0 \leqslant i \leqslant m)$ are relatively prime. In this case P and Q must be of positive degree with respect to Y. Choose an integer d so large that Ψ, P and Q

have degree $< d$ in each of the variable $y_1, \dots, y_l$. Make Kronecker's substitution

$$S_d N(y_1, \dots, y_l) = N(y, y^d, \dots, y^{d^{l-1}})$$

(N arbitrary polynomial).

Clearly, $S_d M_i$ $(0 \leqslant i \leqslant m)$ are distinct and the same is true for $S_d P_i$ $(0 \leqslant i \leqslant p)$ and $S_d Q_i$ $(0 \leqslant i \leqslant q)$.

We get

$$S_d \Psi = \sum_{\nu=0}^{\mu} a_\nu y^{\mu-\nu}, \quad S_d P = \sum_{\nu=0}^{\pi} b_\nu y^{\pi-\nu},$$

where $y^\mu = S_d M_0$, $y^\pi = S_d P_0$,

$$a_\nu = \begin{cases} A_i\big(F(X)\big), & \text{if there is an } i \leqslant m \text{ such that } S_d M_i = y^{\mu-\nu} \\ 0 & \text{otherwise,} \end{cases} \tag{13}$$

$$b_\nu = \begin{cases} B_i(X), & \text{if there is an } i \leqslant p \text{ such that } S_d P_i = y^{\pi-\nu} \\ 0 & \text{otherwise.} \end{cases}$$

It follows that $B_0 = b_0$, $B_i = b_{\nu(i)}$ where $S_d P_i = y^{\mu-\nu(i)}$. Since $S_d P$ divides $S_d \Psi$, we have by Lemma 1 with $L = K(X)$,

$$\Omega_{\nu(i),\mu}\left(\frac{B_i}{B_0}; \frac{a_1}{a_0}, \dots, \frac{a_\mu}{a_0}\right) = 0 \quad (1 \leqslant i \leqslant p). \tag{14}$$

Since by (13), a_ν $(0 \leqslant \nu \leqslant \mu)$ are expressible integrally in terms of $F(X)$ with coefficients from K, equation (14) takes the form

$$\chi_i\left(\frac{B_i(X)}{B_0(X)}, F(X)\right) = 0 \quad (1 \leqslant i \leqslant p),$$

where $\chi_i(t, v)$ is a polynomial over K with the coefficient at the highest power of t equal to a power of $A_0(v)$, whence

$$\chi_i(t, v) \neq 0.$$

Similarly we get

$$\chi_{p+i}\left(\frac{C_i(X)}{C_0(X)}, F(X)\right) = 0 \quad (1 \leqslant i \leqslant q),$$

where again $\chi_{p+i}(t, v) \neq 0$.

It follows now from Lemma 2 that there exist polynomials $G(u)$ and $H(X)$ and rational functions $p_i(u)$ $(1 \leqslant i \leqslant p)$ and $q_i(u)$ $(1 \leqslant i \leqslant q)$ over K such that

$$F(X) = G\big(H(X)\big),$$

$$\frac{B_i(X)}{B_0(X)} = p_i\big(H(X)\big) \quad (1 \leqslant i \leqslant p),$$

and

$$\frac{C_i(X)}{C_0(X)} = q_i\big(H(X)\big) \quad (1 \leqslant i \leqslant q)$$

identically. Since $B_0(X)C_0(X) = A_0\big(F(X)\big) = A_0\big(G\big(H(X)\big)\big)$, we get from (10)–(12)

$$\Psi\big(G(u), Y\big) = A_0\big(G(u)\big)\Big(\sum_{i=0}^{p} p_i(u)P_i(Y)\Big)\Big(\sum_{i=0}^{q} q_i(u)Q_i(Y)\Big)$$

and since both factors in brackets are of positive degree with respect to Y, the polynomial $\Psi\big(G(u), Y\big)$ treated as polynomial in Y is reducible in the field $K(u)$. By Gauss's lemma this implies that $\Psi\big(G(u), Y\big)$ is reducible in the ring $K[u]$, i.e. it is simply reducible and the proof is complete. □

Proof of the Theorem. The condition for reducibility given in the theorem is clearly sufficient. To prove that it is necessary we proceed by induction with respect to the total number of variables $N = \overline{\overline{X}}_1 + \ldots + \overline{\overline{X}}_n$. If $N = n$ so that $\overline{\overline{X}}_i = 1$ $(1 \leqslant i \leqslant n)$, the result is trivially true.

We suppose the result holds if $N < N_0$, where $N_0 > n$, and have to establish its truth when $N = N_0$. We can suppose without loss of generality that $\overline{\overline{X}}_1 = k > 1$ and $F_1(X_1)$ is not constant. Arrange all the variables belonging to $X_2 + \ldots + X_n$ on which $\Phi\big(F_1(X_1), \ldots, F_n(X_n)\big)$ really depends in a sequence $y_1, \ldots, y_l$. Put

$$\Psi(t; y_1, \ldots, y_l) = \Phi\big(t, F_2(X_2), \ldots, F_n(X_n)\big).$$

If $\Phi\big(F_1(X_1), \ldots, F_n(X_n)\big)$ is reducible, we apply Lemma 3 to $\Psi\big(F_1(X_1); y_1, \ldots, y_l\big)$ and conclude that

$$F_1(X_1) = G\big(H(X_1)\big),$$

where G, H are polynomials over K and

$$\Psi\big(G(u); y_1, \ldots, y_l\big) = \Phi\big(G(u), F_2(X_2), \ldots, F_n(X_n)\big)$$

is reducible. Now the total number of variables is $N_0 - k + 1$ and an application of the inductive hypothesis leads to the desired conclusion. □

Note added in proof. Dr. A. Białynicki-Birula has remarked that the polynomials G_i occurring in the Theorem depend only upon F_i and not upon Φ.

References

[1] H. Davenport, A. Schinzel, *Two problems concerning polynomials*. J. Reine Angew. Math. 214/215 (1964), 386–391; *Corrigendum* 218 (1965), 220.

[2] J. Igusa, *On a theorem of Lueroth*. Mem. Coll. Sci. Univ. Kyoto. Ser. A. Math. 26 (1951), 251–253.

[3] P. Samuel, *Some remarks on Lüroth's Theorem*. Mem. Coll. Sci. Univ. Kyoto. Ser. A. Math. 27 (1953), 223–224.

Originally published in
Colloquium Mathematicum XVIII (1967), 213–218

Reducibility of polynomials of the form $f(x) - g(y)$

I have proposed in [3] the following problem: do there exist non-constant polynomials $f(x)$ and $g(y)$ such that $f(x) - g(y)$ is reducible over the complex field and is neither of the form

$$a\big(b(x)\big) - a\big(c(y)\big), \tag{1}$$

nor of the form

$$AT_4\big(b(x)\big) + AT_4\big(c(y)\big),$$

where a, b, c are polynomials, the degree of a is greater than 1, A is a constant and

$$T_4(z) = \cos(4 \arccos z) = 8z^4 - 8z^2 + 1$$

(for earlier results on this topic see [1])?

Recently B. J. Birch, J. W. S. Cassels and M. Guy have solved this problem in the affirmative by finding the following example:

$$\begin{aligned} f(x) - g(y) &= x^7 - 7\lambda t x^5 + (4-\lambda)t x^4 + (14\lambda - 35)t^2 x^3 \\ &\quad - (8\lambda + 10)t^2 x^2 + \big((3-\lambda)t^2 + 7(3\lambda + 2)t^3\big)x \\ &\quad - y^7 + 7\mu t y^5 + (4-\mu)t y^4 - (14\mu - 35)t^2 y^3 \\ &\quad - (8\mu + 10)t^2 y^2 - \big((3-\mu)t^2 + 7(3\mu + 2)t^3\big)y - 7t^3 \\ &= \big[x^3 + \lambda x^3 y - \mu x y^2 - y^3 - (3\lambda + 2)tx + (3\mu + 2)ty + t\big] \\ &\quad \times \big[x^4 - \lambda x^3 y - x^2 y^2 - \mu x y^3 + y^4 + 2(\mu - \lambda)t x^2 - 7txy \\ &\quad + 2(\lambda - \mu)t y^2 + (3-\lambda)tx - (3-\mu)ty - 7t^2\big]. \end{aligned}$$

In this example, t is a parameter, $\lambda = (1 + \sqrt{-7})/2$, $\mu = (1 - \sqrt{-7})/2$. Since λ/μ is irrational, the coefficients of f and g are not all rational except for $t = 0$, when $f(x) - g(y) = x^7 - y^7$ is of the form (1). The aim of the present note is to show that this is necessarily the case if at least one of the degrees of f and g is a prime. More exactly, we prove the

Theorem. *Let f and g be non-constant polynomials with rational coefficients and let the degree of f be a prime, say p. Then $f(x) - g(y)$ is reducible over the complex field if and only if $g(y) = f\big(c(y)\big)$ and either c has rational coefficients or*

$$f(x) - g(y) = A(x + \alpha)^p - Bd(y)^p, \tag{2}$$

where d has rational coefficients and A, B and α are rationals.

Corollary. *Under the assumptions of the theorem, the case* (2) *being excepted,* $f(x)-g(y)$ *is reducible over the complex field only if it is reducible over the rational field.*

In the sequel, we shall denote by $\mathbb{C}$ the complex field, by $\mathbb{Q}$ the rational field, and, for any given field K, by $|K|$ its degree and by $K[x]$ the ring of polynomials in x over K. By ζ_p is meant the primitive p-th root of unity. We have

Lemma 1. *Let* $a \in \mathbb{Q}$, $a \neq 0$ *and* $\sqrt[p]{a}$ *be a rational root of the equation* $x^p - a = 0$ *if there are such roots or any root otherwise. Then* $(x^p - a)/(x - \sqrt[p]{a})$ *is irreducible over* $\mathbb{Q}(\sqrt[p]{a})$.

Proof. Setting $K = \mathbb{Q}(\sqrt[p]{a})$ we have

$$\big(|K|, |\mathbb{Q}(\zeta_p)|\big) = \begin{cases} (1,\, p-1) & \text{if } \sqrt[p]{a} \text{ is rational,} \\ (p,\, p-1) & \text{if } \sqrt[p]{a} \text{ is irrational.} \end{cases}$$

Thus in any case $\big(|K|, |\mathbb{Q}(\zeta_p)|\big) = 1$. Hence

$$\big|K\mathbb{Q}(\zeta_p)\big| = |K|\,|\mathbb{Q}(\zeta_p)| = (p-1)|K|$$

and

$$\big|K(\zeta_p \sqrt[p]{a})\big| = |K(\zeta_p)| = |K\mathbb{Q}(\zeta_p)| = (p-1)|K|.$$

Since $\zeta_p \sqrt[p]{a}$ is a zero of the polynomial $(x^p - a)/(x - \sqrt[p]{a})$ and $(p-1)$ is its degree over K, the polynomial is irreducible over K. □

Lemma 2. *If polynomials* f *and* g *satisfy the conditions of the Theorem and* $g(y) = f\big(c(y)\big)$, *where* $c(y) \in \mathbb{C}[y]$, *then either* $c(y) \in \mathbb{Q}[y]$ *or* (2) *holds.*

Proof. Let

$$f(x) = \sum_{i=0}^{p} a_i x^{p-i}, \quad g(x) = \sum_{i=0}^{q} b_i x^{q-i}, \quad c(x) = \sum_{j=0}^{r} c_j x^{r-j}.$$

It follows from the identity

$$g(x) = \sum_{i=0}^{q} b_i x^{q-i} = \sum_{i=0}^{p} a_i \Big(\sum_{j=0}^{r} c_j x^{r-j}\Big)^{p-i} \tag{3}$$

that

$$b_0 = a_0 c_0^p \tag{4}$$

and that for each positive $j < r$ the polynomial

$$D_j(x) = \frac{g(x)}{pb_0} - \frac{1}{p}\Big(\sum_{i=0}^{j-1} \frac{c_i}{c_0}\, x^{r-i}\Big)^p$$

has the leading coefficient c_j/c_0. The induction with respect to j shows that

$$\frac{c_j}{c_0} \in \mathbb{Q} \quad (0 \leqslant j < r). \tag{5}$$

Thus the leading coefficient of the polynomial $D_r(x)$ equal to ϱ, say, is rational. On the other hand, it follows from (3) that

$$\varrho = \frac{c_r}{c_0} + \frac{a_1}{pa_0c_0}, \quad c_r = \varrho c_0 - \frac{a_1}{pa_0}. \tag{6}$$

Suppose now that (2) does not hold; thus the polynomial

$$f\Big(x - \frac{a_1}{a_0 p}\Big) - a_0 x^p$$

is non-constant. Let d_0x^s be its leading term ($0 < s < p$, d_0 rational). The polynomial

$$f\big(c(x)\big) - a_0\Big(c(x) + \frac{a_1}{a_0 p}\Big)^p = g(x) - b_0\Big(\sum_{j=0}^{r-1} \frac{c_j}{c_0}\, x^{r-j} + \varrho\Big)^p$$

has rational coefficients and the leading coefficient $d_0c_0^s$. Thus $c_0^s \in \mathbb{Q}$ and since, by (4), $c_0^p \in \mathbb{Q}$, we get $c_0^{(s,p)} = c_0 \in \mathbb{Q}$. It follows by (5) and (6) that $c(x) \in \mathbb{Q}[x]$. The proof is complete. □

Remark. The method used in the above proof gives the following more general statement.

Let K be a field of characteristic χ and L an arbitrary extension of K. If $f(x), g(x) \in K[x]$, $c(x) \in L[x]$, $g(x) = f\big(c(x)\big)$ and χ does not divide the degree of f, then there exist a positive integer q and $\kappa, \lambda \in L$, $d(x), h(x) \in K[x]$ such that

$$\lambda^q \in K, \quad c(x) = \lambda d(x) - \kappa, \quad f(x) = h\big((x + \kappa)^q\big).$$

The condition

$$\text{degree of } f \not\equiv 0 \pmod{\chi}$$

is necessary as is shown by the example:

$$\chi = 2, \quad K = GF[2], \quad L = GF[4] = K(\omega),$$
$$f(x) = x^2 + x, \quad g(x) = x^2 + 1, \quad c(x) = x + \omega.$$

Proof of the theorem. The sufficiency of the conditions given in the theorem follows immediately from the factorization

$$f(x) - f\big(c(y)\big) = \big(x - c(y)\big) \sum_{n=1}^{p} \frac{f^{(n)}(x)}{n!} \big(c(y) - x\big)^{n-1}.$$

In order to prove the necessity of the conditions we assume without loss of generality that the leading coefficient of f is 1 and that of g is, say, a. Let

$$f(x) - g(y) = h_1(x, y)h_2(x, y) \cdots h_r(x, y) \quad (r > 1) \tag{7}$$

be the decomposition of $f(x) - g(y)$ into factors irreducible over $\mathbb{C}$ with the coefficient of the highest power of x in each $h_i(x, y)$ equal to 1. Since $f(x) - g(y)$ is reducible, it follows from a theorem of Ehrenfeucht [2] that the degree of g is divisible by p and equals, say, kp, where k is an integer. Give x the weight k and y the weight 1 and denote the highest isobaric part of $h_i(x, y)$ by $H_i(x, y)$ $(1 \leqslant i \leqslant r)$. It follows from (7) that

$$x^p - ay^{kp} = H_1(x, y)H_2(x, y) \cdots H_r(x, y). \tag{8}$$

Let $\sqrt[p]{a}$ be defined as in Lemma 1. Since $x - \sqrt[p]{a}\, y^k \mid x^p - ay^{kp}$ and $x - \sqrt[p]{a}\, y^k$ is irreducible over $\mathbb{C}$ we may assume without loss of generality that

$$x - \sqrt[p]{a}\, y^k \mid H_1(x, y). \tag{9}$$

Suppose that $H_1(x, y) \neq x - \sqrt[p]{a}\, y^k$. In view of the normalization of $h_i(x, y)$, $H_1(x, 1)/(x - \sqrt[p]{a})$ is not a constant. On the other hand, by (8) we get

$$\frac{x^p - a}{x - \sqrt[p]{a}} = \frac{H_1(x, 1)}{x - \sqrt[p]{a}}\, H_2(x, 1) \cdots H_r(x, 1). \tag{10}$$

It follows from Lemma 1 that $H_1(x, 1) \notin K[x]$, where $K = \mathbb{Q}(\sqrt[p]{a})$, and, a fortiori, $h_1(x, y) \notin K[x, y]$. The field of coefficients of h_1 is algebraic over K, thus there is a polynomial $h_1'(x, y)$ with coefficients algebraically conjugate over K to those of h_1 such that

$$h_1'(x, y) \neq h_1(x, y).$$

In view of the normalization of h_1, the coefficient of the highest power of x in $h_1'(x, y)$ equals 1, and since $h_1'(x, y)$ is irreducible over $\mathbb{C}$ it must occur in the factorization (7) as, say, h_2. We get

$$H_1'(x, y) = H_2(x, y),$$

where the coefficients of $H_1'(x, y)$ are algebraically conjugate over K to those of $H_1(x, y)$. By (9) we have

$$x - \sqrt[p]{a}\, y^k \mid H_2(x, y),$$

and by (10)

$$x - \sqrt[p]{a} \;\Big|\; \frac{x^p - a}{x - \sqrt[p]{a}},$$

which is impossible, since $x^p - a$ has no multiple zeros. Therefore

$$H_1(x, y) = x - \sqrt[p]{a}\, y^k,$$

and, by the definition of H_1,

$$h_1(x, y) = x - c(y).$$

We obtain now from (7) that $g(y) = f\big(c(y)\big)$ and the theorem follows from Lemma 2.□

Note added in proof. The following new non-trivial example of reducibility of $f(x)-g(y)$ has been found by Birch, Cassels and Guy:

$$\begin{aligned}
&x^{11} + 11\big(\lambda, -2, -3\mu\tau, -16\lambda, 3\mu^2(\lambda-4), 30\mu\tau, -63\mu, -20\mu^4, 3\mu^4\tau^2, -9\theta\big)(x,1)^9\\
&- y^{11} - 11\big(\mu, -2, -3\lambda\sigma, -16\mu, 3\lambda^2(\mu-4), 30\lambda\sigma, -63\lambda, -20\lambda^4, 3\lambda^4\sigma^2, 9\theta\big)(y,1)^9\\
&\quad = \big[\big(1, -\lambda, -1, 1, \mu, -1\big)(x,y)^5 + \theta\big(2, -\lambda, -\mu, 2\big)(x,y)^3\\
&\qquad\qquad - 2\theta\big(\mu, -3, \lambda\big)(x,y)^2 + \theta\big(\mu^3, \lambda^3\big)(x,y) - 6\theta\big]\\
&\qquad \times \big[\big(1, \lambda, \sigma, 2, \tau, \mu, 1\big)(x,y)^6 + \theta\big(\mu\tau, -\lambda^3, -2\theta, \mu^3, -\lambda\sigma\big)(x,y)^4\\
&\qquad + 2\theta\big(\lambda, \lambda^2, -\mu^2, -\mu\big)(x,y)^3 - \theta\big(\mu(2\theta+3), 3\theta, \lambda(2\theta-3)\big)(x,y)^2\\
&\qquad\qquad + 4\theta\big(-\mu^3, \lambda^3\big)(x,y) + 33\big],
\end{aligned}$$

where

$$\theta^2 = -11, \quad \lambda = \frac{-1+\theta}{2}, \quad \mu = \frac{-1-\theta}{2},$$
$$\sigma = \mu - 1, \quad \tau = \lambda - 1.$$

References

[1] H. Davenport, D. J. Lewis, A. Schinzel, *Equations of the form* $f(x) = g(y)$. Quart. J. Math. Oxford Ser. (2) 12 (1961), 304–312.

[2] A. Ehrenfeucht, *Kryterium absolutnej nierozkładalności wielomianów* (*A criterion of absolute irreducibility of polynomials*). Prace Mat. 2 (1958), 167–169 (Polish).

[3] A. Schinzel, *Some unsolved problems on polynomials*. In: Neki nerešeni problemi u matematici, Matematička Biblioteka 25, Beograd 1963, 63–70; this collection: E1, 703–708.

Originally published in
Acta Arithmetica XXI (1972), 153–171

Reducibility of quadrinomials

with M. Fried (*Stony Brook*)

In memory of Professor Wacław Sierpiński

This paper is based on [8] and the notation of that paper is retained. In particular if

$$\Phi(y_1, \dots, y_k) = y_1^{\alpha_1} \cdots y_k^{\alpha_k} f(y_1, \dots, y_k),$$

where α_i are integers and f is a polynomial not divisible by y_i $(1 \leqslant i \leqslant k)$ then

$$J\Phi(y_1, \dots, y_k) = f(y_1, \dots, y_k).$$

A polynomial $g(y_1, \dots, y_k)$ is called *reciprocal* if

$$Jg(y_1^{-1}, \dots, y_k^{-1}) = \pm g(y_1, \dots, y_k).$$

Reducibility means reducibility over the rational field $\mathbb{Q}$ unless stated to the contrary.

$L\Phi(y_1, \dots, y_k)$ is $J\Phi(y_1, \dots, y_k)$ deprived of all its irreducible reciprocal factors and $K\Phi(x)$ is $J\Phi(x)$ deprived of all its cyclotomic factors.

Ljunggren [5] has proved the irreducibility of $K(x^m + \varepsilon_1 x^n + \varepsilon_2 x^p + \varepsilon_3)$ where $m > n > p$, $\varepsilon_1, \varepsilon_2, \varepsilon_3$ are ± 1 and the case $m = n + p$, $\varepsilon_3 = \varepsilon_1\varepsilon_2$ is excluded. He has also proved [6] the irreducibility ([1]) of $K(x^m + \varepsilon_1 x^n + \varepsilon_2 x^p + \varepsilon_3 r)$, where r is a prime. The aim of this paper is to treat a general quadrinomial $q(x) = ax^m + bx^n + cx^p + d$ by means of Theorem 2 of [8]. In order to apply this theorem it is necessary to investigate first the reducibility of a quadrinomial in two variables. The result of the investigation is given below as Theorem 1. Combining this theorem with Theorem 2 of [8] we obtain a necessary and sufficient condition for the reducibility of $Lq(x)$ (Theorem 2). In general we have no such condition for the reducibility of $Kq(x)$ but in the case $a = 1$, $b = \varepsilon_1$, $0 < |c| \leqslant |d|$ (c, d integers) $Kq(x) = Lq(x)$ which leads to a generalization of the results of Ljunggren (Theorem 3). We prove

Theorem 1. *A quadrinomial* $Q(y_1, y_2) = J\left(a_0 + \sum_{i=1}^{3} a_i y_1^{v_{1i}} y_2^{v_{2i}}\right)$, *where* $a_i \neq 0$ $(0 \leqslant i \leqslant 3)$, $[v_{1i}, v_{2i}]$ *distinct and different from* $[0, 0]$, $[v_{ij}]$ *of rank* 2, *is reducible over a field* $\boldsymbol{K}$ *of*

Corrigendum and addendum, Acta Arith. 99 (2001), 409–410.

([1]) Ljunggren's theorem has been corrected by W. H. Mills [7a].

characteristic zero if and only if either it can be divided into two parts with the highest common factor $D(y_1, y_2)$ being a binomial or it can be represented in one of the forms

$$
\begin{aligned}
&k(U^3+V^3+W^3-3UVW)\\
&\qquad = k(U+V+W)(U^2+V^2+W^2-UV-UW-VW),\\
&k(U^2-4TUVW-T^2V^4-4T^2W^4)\\
&\qquad = k(U-TV^2-2TVW-2TW^2)(U+TV^2-2TVW+2TW^2),\\
&k(U^2+2UV+V^2-W^2) = k(U+V+W)(U+V-W),
\end{aligned}
\tag{1}
$$

where $k \in \boldsymbol{K}$ and T, U, V, W are monomials in $\boldsymbol{K}[y_1, y_2]$. In the former case QD^{-1} is
c *either irreducible over $\boldsymbol{K}$ and non-reciprocal or binomial. In the latter case the factors on*
c *the right hand side of* (1) *are irreducible over $\boldsymbol{K}$ and non-reciprocal unless $\zeta_3 \in \boldsymbol{K}$ when*

$$U^2+V^2+W^2-UV-UW-VW = (U+\zeta_3 V+\zeta_3^2 W)(U+\zeta_3^2 V+\zeta_3 W).$$

Theorem 2. *Let a, b, c, d be any non-zero integers, $m > n > p$ any positive integers and assume that $q(x) = ax^m + bx^n + cx^p + d$ is not a product of two binomials. $Lq(x)$ is reducible if and only if either $q(x)$ can be divided into two parts which have a non-reciprocal common factor or it can be represented in one of the forms* (1) *where $k \in \mathbb{Q}$; T, U, V, W are monomials in $\mathbb{Q}[x]$ and the factors on the right hand side of* (1) *are not reciprocal or finally $m = vm_1$, $n = vn_1$, $p = vp_1$,*

$$m_1 < C(a,b,c,d) = \exp_2\bigl(3\cdot 2^{a^2+b^2+c^2+d^2+2}\log(a^2+b^2+c^2+d^2)\bigr)$$

and $L(ax^{m_1} + bx^{n_1} + cx^{p_1} + d)$ is reducible.

Theorem 3. *Let $\varepsilon = \pm 1$, c, d be integers, $0 < |c| \leqslant |d|$, $m > n > p$ be positive integers and assume that $q(x) = x^m + \varepsilon x^n + cx^p + d$ is not a product of two binomials. $Kq(x)$ is reducible if and only if either there occurs one of the cases*

$$
\begin{aligned}
&(-\varepsilon d)^{(m-p)/\delta_1} = (-c)^{n/\delta_1} \neq \pm 1, \quad \delta_1 = (m-p, n);\\
&(-\varepsilon c)^{m/\delta_2} = (-d)^{(n-p)/\delta_2} \neq \pm 1, \quad \delta_2 = (m, n-p);\\
&m = 2m_1,\ n = 2p,\ \varepsilon = -1,\ c^2 = -4d,\\
&m = 2p,\ n = 2n_1,\ \varepsilon = -1,\ c^2 = 4d,\\
&m = 3m_1,\ n = 3n_1,\ p = m_1 + n_1,\ c^3 = -27\varepsilon d,\\
&m = 2m_1,\ n = 4n_1,\ p = m_1 + n_1,\ \varepsilon = -1,\ c^4 = -64d,\\
&m = 4m_1,\ n = 2n_1,\ p = m_1 + n_1,\ \varepsilon = -1,\ c^4 = 64d
\end{aligned}
\tag{2}
$$

or $m = vm_1$, $n = vn_1$, $p = vp_1$,

$$m_1 < C(1, \varepsilon, c, d)$$

and $K(x^{m_1} + \varepsilon x^{n_1} + cx^{p_1} + d)$ is reducible.

Corollary. *Under the assumptions of Theorem* 3 *the quadrinomial $x^m + \varepsilon x^n + cx^p + d$ is reducible if and only if either there occurs one of the cases* (2) *or we have one of the*

equalities

$$(-\varepsilon d)^{(m-p)/\delta_1} = (-c)^{n/\delta_1} = \pm 1, \quad \delta_1 = (m-p, n);$$
$$(-\varepsilon c)^{m/\delta_2} = (-d)^{(n-p)/\delta_2} = \pm 1, \quad \delta_2 = (m, n-p);$$
$$(-\varepsilon)^{p/\delta_3} = (-d/c)^{(m-n)/\delta_3}, \quad \delta_3 = (m-n, p);$$
$$\zeta^{m/\delta} + \varepsilon\zeta^{n/\delta} + c\zeta^{p/\delta} + d = 0, \quad \zeta^6 = 1, \quad \delta = (m, n, p)$$

or $m = vm_1$, $n = vn_1$, $p = vp_1$,

$$m_1 < C(1, \varepsilon, c, d),$$

and $x^{m_1} + \varepsilon x^{n_1} + cx^{p_1} + d$ *is reducible.*

Lemma 1. *If* $m > n$ *non-zero integers,* $ab \neq 0$ *and*

$$ax^m + bx^n = f_1\big(f_2(x)\big),$$

where f_1, f_2 *rational functions, then for a suitable homography* h *we have either*

$$f_1 h(x) = ax, \quad h^{-1} f_2(x) = x^m + \frac{b}{a} x^n$$

or

$$f_1 h(x) = ax^{m/\delta} + bx^{n/\delta}, \quad h^{-1} f_2(x) = x^\delta$$

or

$$m = -n, \quad f_1 h(x) = 2ac^{m/\delta} T_{m/\delta}\big(\tfrac{1}{2}c^{-1}x\big), \quad h^{-1} f_2(x) = x^\delta + c^2 x^{-\delta},$$

where $c^{2m/\delta} = b/a$ *and* T_m *is the* m*-th Chebyshev polynomial.*

Proof. Assume first that $n > 0$. Then by a known lemma (see [2]) for suitable homography h, $f_1 h$ and $h^{-1} f_2$ are polynomials. We may assume the same about f_1, f_2 and suppose moreover that f_2 is monic with $f_2(0) = 0$. Let

$$f_1(x) = a \prod_{i=1}^{k} (x - x_i)^{\alpha_i}, \quad x_i \text{ distinct}, \quad \alpha_1 + \ldots + \alpha_k = \alpha.$$

Since $f_2(x) - x_i$ are relatively prime in pairs exactly one factor, say $f_2(x) - x_1$, is divisible by x and we have $f_2(x) - x_1 = x^l g(x)$, where $l\alpha_1 = n$. However, $g(x)^{\alpha_1} \mid ax^{m-n} + b$, hence either $g(x) = 1$ or $\alpha_1 = 1$.

In the first case the lemma follows, one obtains also $x_1 = 0$. In the second case $l = n$; if now $g(x) = x^\gamma + a_1 x^{\gamma_1} + \ldots$, where $\gamma > \gamma_1 > \ldots$ and $a_1 \neq 0$, then $f_1\big(f_2(x)\big)$ begins with two non-zero terms

$$ax^{(\gamma+n)\alpha} + \alpha a a_1 x^{\alpha(\gamma+n)+\gamma_1-\gamma}.$$

It follows that $\alpha(\gamma + n) + \gamma_1 - \gamma = n$; $\alpha = 1$, $\gamma = m - n$, $\gamma_1 = 0$, $f_1(x) = ax$, $f_2(x) = x^m + \dfrac{b}{a} x^n$.

The case $n < 0$, $m < 0$ can be reduced to the former by substitution $x \to 1/x$.

Assume now that $m > 0, n < 0$. Set

$$f_1(x) = \frac{R(x)}{S(x)}, \quad f_2(x) = \frac{P(x)}{Q(x)},$$

where P, Q, R, S are polynomials of degrees p, q, r, s respectively and $(P, Q) = (R, S) = 1$. Applying to P/Q a suitable homography we can achieve that $p > q, r > s$ and that P, Q are monic. Consider the identity

$$\frac{ax^{m-n} + b}{x^{-n}} = \frac{R(P, Q)}{S(P, Q)Q^{r-s}},$$

where $R(P, Q) = Q^r R(P/Q)$, etc. Since $R(P, Q)$, $S(P, Q)$, Q are relatively prime in pairs we have either

$$S(P, Q) = cx^{-n}, \quad Q^{r-s} = 1 \quad \text{or} \quad S(P, Q) = c, \quad Q^{r-s} = x^{-n}.$$

In the first case $Q = 1$, by a suitable linear transformation we can achieve $P(0) = 0$ and thus $P(x) = x^\delta$, $S(x) = cx^{-n/\delta}$,

$$f_1(x) = ax^{m/\delta} + bx^{n/\delta}, \quad f_2(x) = x^\delta.$$

In the second case it follows in view of $p > q$ that $Q = x^{-n/r}$, $s = 0$, f_1 is a polynomial and we have $p = \dfrac{m-n}{r}$,

$$f_1(x^{n/r} P) = ax^m + bx^n.$$

If P contains terms $c_1 x^{p_1}$ with $c_1 \neq 0$, $p > p_1 > -n/r$ then taking the largest possible p_1 we get on the left hand side a term $arc_1 x^{m+p_1-p}$ lacking on the right hand side. Similarly we get a contradiction if P contains a term $c_2 x^{p_2}$ with $-n/r > p_2 > 0$. Therefore, $P = x^{(m-n)/r} + c_3 x^{-n/r} + c_4$ and applying to f_2 a suitable linear transformation we obtain $P = x^{(m-n)/r} + c_4$.

Let β be any $(m-n)$th root of $-b/a$. Then $c_4 = \beta^{(m-n)r} \zeta_{2r}^{2h+1}$ for suitable h. Moreover

$$f_1\big(\beta^{(m-n)/r}(\zeta_{m-n}^{im/r} + \zeta_{2r}^{2h+1}\zeta_{m-n}^{in/r})\big) = 0$$

for all $i = 1, 2, \ldots, m-n$.

Suppose that for two values of i we get the same zero of f_1, i.e.

$$\zeta_{m-n}^{im/r} + \zeta_{2r}^{2h+1}\zeta_{m-n}^{in/r} = \zeta_{m-n}^{jm/r} + \zeta_{2r}^{2h+1}\zeta_{m-n}^{jn/r}.$$

It follows hence (see [7]) that either both sums are zero, or the terms are equal in pairs, i.e. either

$$\zeta_{m-n}^{i(m-n)/r} = \zeta_{m-n}^{j(m-n)/r} = \zeta_{2r}^{2h+r+1}$$

or

$$\zeta_{m-n}^{(i-j)m/r} = \zeta_{m-n}^{(i-j)n/r} = 1$$

or

$$\zeta_{m-n}^{(im-jn)/r} = \zeta_{m-n}^{(jm-in)/r} = \zeta_{2r}^{2h+1}.$$

The first equality implies $2i \equiv 2j \equiv 2h' + r + 1 \bmod 2r$ (h' fixed, determined by h and the choice of ζ_{m-n}, ζ_{2r}), the second $i \equiv j \bmod r(m-n)/(m,n)$, the third $i \equiv j \bmod r(m-n)/(m-n, m+n)$. Thus all but at most $\dfrac{m-n}{(m-n, m+n)} - 1$ zeros of f_1 obtained for $i \leqslant r\,\dfrac{m-n}{(m-n, m+n)}$ are distinct. Hence

$$r\,\frac{m-n}{(m-n, m+n)} \leqslant r + \frac{m-n}{(m-n, m+n)} - 1$$

and either $r = 1$ or $m - n \mid m + n$ thus $m + n = 0$. In the former case we get $f_1(x) = ax$, $f_2(x) = x^m + (b/a)x^n$, in the latter case

$$f_1(x) = 2a\big(\sqrt{c_4}\big)^r T_r\left(\frac{x}{2\sqrt{c_4}}\right), \qquad f_2(x) = x^{m/r} + c_4 x^{-m/r}. \qquad \square$$

Lemma 2. *Let m_i be integers different from zero, $m_0 \neq m_1$, $m_0 + m_1 \geqslant 0$; $m_2 \neq m_3$, $m_2 + m_3 \geqslant 0$, a_i ($i = 0, 1, 2, 3$) complex numbers different from zero and the case $m_0 + m_1 = m_2 + m_3 = 0$, $a_0 a_1 = a_2 a_3$ be excluded. If the quadrinomial*

$$q(x, y) = J(a_0 x^{m_0} + a_1 x^{m_1} + a_2 y^{m_2} + a_3 y^{m_3})$$

is reducible over the complex field $\mathbb{C}$ then either it can be divided into two parts with the highest common factor $d(x, y)$ being a binomial or it can be represented in one of the forms

$$\begin{aligned} &u^3 + v^3 + w^3 - 3uvw = (u + v + w)(u + \zeta_3 v + \zeta_3^2 w)(u + \zeta_3^2 v + \zeta_3 w), \\ &u^2 - 4tuvw - t^2 v^4 - 4t^2 w^4 \\ &\qquad = (u - tv^2 - 2tvw - 2tw^2)(u + tv^2 - 2tvw + 2tw^2), \end{aligned} \tag{3}$$

where t, u, v, w are monomials in $\mathbb{C}[x, y]$.

In the former case qd^{-1} is irreducible over $\mathbb{C}$ and non-reciprocal, in the latter case the factors on the right hand side of (3) *are irreducible over $\mathbb{C}$ and non-reciprocal. Moreover, if the first equality of* (3) *holds, $u^2 + v^2 + w^2 - uv - uw - vw$ is also not reciprocal.*

Proof. In view of symmetry we may assume that $m_0 \geqslant |m_1|$, $m_2 \geqslant |m_3|$. Set $f(x) = a_0 x^{m_0} + a_1 x^{m_1}$, $g(y) = -a_2 y^{m_2} - a_3 y^{m_3}$ and denote by $\boldsymbol{\Omega}_{f-z}$ the splitting field of $f(x) - z$ over $\mathbb{C}(z)$. By Proposition 2 of [4] there exist rational functions f_1, f_2, g_1, g_2 such that $f = f_1(f_2)$, $g = g_1(g_2)$, $\boldsymbol{\Omega}_{f_1 - z} = \boldsymbol{\Omega}_{g_1 - z}$ and $f - g$, $f_1 - g_1$ have the same number of irreducible factors over $\mathbb{C}$. (The number of irreducible factors of $F_1/F_2 - G_1/G_2$, where $F_i \in \mathbb{C}[x]$, $G_i \in \mathbb{C}[y]$, $(F_1, F_2) = 1 = (G_1, G_2)$, is defined as the number of irreducible factors of $F_1 G_2 - F_2 G_1$.) Since both conditions are invariant with respect to transformations $f_1 \to f_1 h$, $g_1 \to g_1 j$ where h, j are homographies we can apply Lemma 1 and

infer that there occurs one of the cases

$$\begin{aligned}
&1.\ f_1 = a_0x^{n_0} + a_1x^{n_1}, \quad -g_1 = a_2y^{n_2} + a_3y^{n_3},\\
&2.\ f_1 = a_0x^{n_0} + a_1x^{n_1}, \quad -g_1 = 2\sqrt{a_2a_3}\,T_{n_2}(y),\ n_3 = -n_2,\\
&3.\ f_1 = 2\sqrt{a_0a_1}\,T_{n_0}(x), \quad -g_1 = a_2y^{n_2} + a_3y^{n_3},\ n_1 = -n_0,\\
&4.\ f_1 = 2\sqrt{a_0a_1}\,T_{n_0}(x), \quad -g_1 = 2\sqrt{a_2a_3}\,T_{n_2}(y),\ n_1 = n_0,\ n_3 = -n_2,
\end{aligned}$$

where $n_i = m_i/\delta$ $(i = 0, 1)$, $n_i = m_i/\varepsilon$ $(i = 2, 3)$. Set

c $$n_i' = n_i/(n_0, n_1)\ (i = 0, 1); \quad n_i' = n_i/(n_2, n_3)\ (i = 2, 3).$$

Let $\sigma_\alpha(f_1)$ be the branch permutation for the Riemann surface for $f_1(x) - z$ over the place $z = \alpha$ on the z sphere and let ω be a generator of the extension $\boldsymbol{\Omega}_{f_1-z}/\mathbb{C}(z)$. ω is expressible rationally in terms of z and of $x^{(i)}(z)$'s $(i = 1, \dots, k)$, where

$$f_1(x) - z = F(x)^{-1}\prod_{i=1}^{k}\bigl(x - x^{(i)}(z)\bigr), \quad F(x) \in \mathbb{C}[x].$$

$|\sigma_\alpha(f_1)|$, the order of $\sigma_\alpha(f_1)$, is the least positive integer M such that each $x^{(i)}(z)$ is expressible as Laurent series in $(z-\alpha)^{1/M}$ in the neighbourhood of $z = \alpha$. It follows that ω is expressible as such series in $(z-\alpha)^{1/|\sigma_\alpha(f_1)|}$. On the other hand, if ω is expressible as a Laurent series in $(z-\alpha)^{1/N}$ then all $x^{(i)}(z)$ are so expressible and hence $|\sigma_\alpha(f_1)| \leqslant N$. Thus $|\sigma_\alpha(f_1)|$ is the least integer N such that ω is expressible as a Laurent series in $(z-\alpha)^{1/N}$ and therefore it is determined by $\boldsymbol{\Omega}_{f_1-z}$. From $\boldsymbol{\Omega}_{f_1-z} = \boldsymbol{\Omega}_{g_1-z}$ we have

$$|\sigma_\alpha(f_1)| = |\sigma_\alpha(g_1)|.$$

We use this observation separately in each of the cases 1–4.

1. If $n_1 > 0$ a simple computation shows that the branch permutations for $\boldsymbol{\Omega}_{f_1-z}$ are
c σ_0 (an n_1 cycle), σ_∞ (an n_0 cycle), and $(n_0 - n_1)/(n_0, n_1)$ other finite branch permutations (of order 2 and type $\sigma = \underbrace{(2)(2)\dots(2)}_{(n_0,n_1)\text{ times}}$ corresponding to the branch points

$$z_i = \zeta_{n_0-n_1}^{in_1}\left(\frac{a_1(n_0-n_1)}{n_0}\right)\left(-\frac{a_1n_1}{a_0n_0}\right)^{n_1/(n_0-n_1)}, \quad i = 0, 1, \dots, \frac{n_0-n_1}{(n_0,n_1)} - 1.$$

If $n_1 < 0$, $\sigma_\infty(f_1)$ is a product $\gamma_1\gamma_2$, where γ_1, γ_2 are disjoint cycles of length n_0 and $|n_1|$ respectively. The finite branch points are again z_i and the corresponding permutations are of type $\sigma = \underbrace{(2)(2)\dots(2)}_{(n_0,n_1)\text{ times}}$. We have to consider several cases.

A. $n_1 > 0$, $n_3 > 0$. From $|\sigma_0(f_1)| = |\sigma_0(g_1)|$ we get $n_1 = n_3$, from $|\sigma_\infty(f_1)| = |\sigma_\infty(g_1)|$ we get $n_0 = n_2$. Also the branch points must be the same, which implies

$$\left(\frac{-a_0}{a_2}\right)^{n_1'} = \left(\frac{-a_1}{a_3}\right)^{n_0'}.$$

Since $(n_0', n_1') = 1$ there exists a unique number r such that

$$r^{n_0'} = -a_2/a_0, \quad r^{n_1'} = -a_3/a_1.$$

On substitution $x = zy$ the quadrinomial $f_1(x) - g_1(y)$ takes the form

$$f_1(x) - g_1(y) = a_0 y^{n_0}\left(z^{n_0} - r^{n_0'}\right) + a_1 y^{n_1}\left(z^{n_1} - r^{n_1'}\right).$$

Since $\dfrac{z^{n_0} - r^{n_0'}}{z^{n_1} - r^{n_1'}}$ is not a power in $\mathbb{C}(z)$ and

$$\left(z^{n_0} - r^{n_0'}, z^{n_1} - r^{n_1'}\right) = z^{(n_0,n_1)} - r$$

we infer in virtue of Capelli's theorem that

$$f_1(x) - g_1(y) = y^{n_1}\left(z^{(n_0,n_1)} - r\right)F(z, y)$$

where F is irreducible over $\mathbb{C}$. It follows that

$$f_1(x) - g_1(y) = \left(x^{(n_0,n_1)} - r y^{(n_0,n_1)}\right)G(x, y)$$

where G is irreducible over $\mathbb{C}$. Thus the number of irreducible factors of $f_1 - g_1$ is $(n_0, n_1) + 1$. On the other hand

$$d(x, y) = \left(a_0 x^{m_0} + a_2 y^{m_2}, a_1 x^{m_1} + a_3 y^{m_3}\right) = x^{(n_0,n_1)\delta} - r y^{(n_0,n_1)\varepsilon},$$

thus the number of irreducible factors of $f(x) - g(y)$ is at least $(n_0, n_1)(\delta, \varepsilon) + \nu$, where ν is the number of irreducible factors of qd^{-1} (q has no multiple factors). It follows that

$$(n_0, n_1)(\delta, \varepsilon) + \nu \leqslant (n_0, n_1) + 1, \quad \nu = 1,$$

hence qd^{-1} is irreducible over $\mathbb{C}$. Moreover it is not reciprocal since the degree of $Jq(x^{-1}, y^{-1})$ is greater than the degree of q and the degrees of $Jd(x^{-1}, y^{-1})$ and of d are equal.

B. $n_1 n_3 < 0$. In view of symmetry we may assume $n_1 > 0$. From $|\sigma_0(f_1)| = |\sigma_0(g_1)|$ we get $n_1 = 1$, from $|\sigma_\infty(f_1)| = |\sigma_\infty(g_1)|$, $n_0 = [n_2, n_3]$.

Counting the number of remaining finite branch points we get

$$n_0 - 1 = \frac{n_2 + |n_3|}{(n_2, n_3)} \quad \text{or} \quad [n_2, n_3] - 1 = \frac{n_2 + |n_3|}{(n_2, n_3)}$$

or

$$n_2|n_3| - n_2 - |n_3| - (n_2, n_3) = 0; \quad (n_2 - 1)(|n_3| - 1) = (n_2, n_3) + 1.$$

This equation has three solutions with $n_2 \geqslant -n_3 > 0$:

$$\langle n_2, n_3\rangle = \langle 3, -2\rangle,\ \langle 3, -3\rangle,\ \langle 4, -2\rangle.$$

The first solution gives $n_0 = 6$,

$$f_1(x) - g_1(y) = a_0 x^6 + a_1 x + a_2 y^3 + a_3 y^{-2} = \left(a_2 y^5 + (a_0 x^6 + a_1 x)y^2 + a_3\right)y^{-2}$$

and the numerator of the fraction obtained is irreducible over $\mathbb{C}$. Indeed, it clearly has no factor linear in y, thus a possible factorization would have the form

$$a_2 y^5 + (a_0 x^6 + a_1 x)y^2 + a_3 = a_2\left(y^2 + f_1(x)y + c_1\right)(y^3 + f_2(x)y^2 + f_3(x)y + c_2).$$

It follows hence

$$f_2(x) + f_1(x) = 0,$$
$$f_3(x) + f_1(x) f_2(x) + c_1 = 0,$$
$$c_2 f_1(x) + c_1 f_3(x) = 0,$$
$$-c_1 f_1^2(x) - c_2 f_1(x) + c_1^2 = 0;$$

$f_1(x) = -f_2(x) = \text{const}$, $f_3(x) = \text{const}$, which is impossible.

The second solution $\langle n_2, n_3\rangle = \langle 3, -3\rangle$ gives $n_0 = 3$. Since the branch points must be the same

$$\pm\frac{2}{3}\, a_1\sqrt{\frac{-a_1}{3a_0}} = \mp 2a_3\sqrt{\frac{a_2}{a_3}}; \quad a_1^3 = -27a_0a_2a_3.$$

It follows that

$$q(x, y) = J\big(f(x) - g(y)\big) = (a_0x^{3\delta} + a_1x^{\delta})y^{3\varepsilon} + a_2y^{6\varepsilon} + a_3$$
$$= u^3 + v^3 + w^3 - 3uvw = (u + v + w)(u + \zeta_3 v + \zeta_3^{-1} w)(u + \zeta_3^{-1} v + \zeta_3 w),$$

where

$$u = a_0^{1/3}x^{\delta}y^{\varepsilon}, \quad v = a_2^{1/3}y^{2\varepsilon}, \quad w = a_3^{1/3}$$

and suitable values of the cubic roots are taken. The trinomials $u + \zeta_3^i v + \zeta_3^{-i} w$ are irreducible over $\mathbb{C}$ in virtue of Capelli's theorem since $\zeta_3^i a_2^{1/3}y^{\varepsilon} + \zeta_3^{-i} a_3^{1/3}y^{-\varepsilon}$ is not power in $\mathbb{C}(y)$. Moreover one verifies directly that $u + \zeta_3^i v + \zeta_3^{-i} w$ $(i = 0, \pm 1)$ and $u^2 + v^2 + w^2 - uv - uw - vw$ are not reciprocal.

The third solution $\langle n_2, n_3\rangle = \langle 4, -2\rangle$ gives $n_0 = 4$. Since the branch points must be the same we have for suitable values of the cubic roots

$$\frac{3}{4}\, a_1\left(\frac{-a_1}{4a_0}\right)^{1/3} = -\frac{6}{4}\, a_3\left(\frac{2a_3}{4a_2}\right)^{-1/3}; \quad a_1^4 = 64a_0a_2a_3^2.$$

It follows that

$$q(x, y) = J\big(f(x) - g(y)\big) = (a_0x^{4\delta} + a_1x^{\delta})y^{2\varepsilon} + a_2y^{6\varepsilon} + a_3$$
$$= u^2 - 4tuvw - t^2v^4 - 4t^2w^4$$
$$= (u - tv^2 - 2tvw - 2tw^2)(u + tv^2 - 2tvw + 2tw^2),$$

where

$$t = y^{\varepsilon}, \quad u = a_3^{1/2}, \quad v = (-a_2)^{1/4}y^{\varepsilon}, \quad w = (-a_0/4)^{1/4}x^{\delta}$$

and suitable values of the quadratic and the quartic roots are taken. The quadrinomials $u \pm tv^2 - 2tvw \pm 2tw^2$ are irreducible over $\mathbb{C}$ since after the substitution

$$x = x_1y_1^{\varepsilon}, \quad y = y_1^{\delta}$$

we obtain

$$u \pm tv^2 - 2tvw \pm 2tw^2$$
$$= a_3^{1/2} + y_1^{3\delta\varepsilon}\left[\pm(-a_2)^{1/2} - 2(a_0a_2/4)^{1/4}x_1^{-\delta} \pm 2(-a_0/4)^{1/2}x_1^{2\delta}\right]$$

and the expression in the brackets is not a power in $\mathbb{C}[x_1]$. Moreover, one verifies directly that the quadrinomials $u \pm tv^2 - 2tvw \pm 2tw^2$ are not reciprocal.

C. $n_1 < 0, n_3 < 0$. From $|\sigma_\infty(f_1)| = |\sigma_\infty(g_1)|$ we get

$$[n_0, n_1] = [n_2, n_3]. \tag{4}$$

Counting the number of finite branch points we get

$$\frac{n_0 + |n_1|}{(n_0, n_1)} = \frac{n_2 + |n_3|}{(n_2, n_3)}\,. \tag{5}$$

If $(n_0, n_1) = (n_2, n_3) = 1$ we infer from (4), (5) and the inequalities $n_0 \geqslant -n_1 > 0$, $n_2 \geqslant -n_3 > 0$ that $n_0 = n_2, n_1 = n_3$. The same conclusion holds if

$$\frac{n_0 + |n_1|}{(n_0, n_1)} = \frac{n_2 + |n_3|}{(n_2, n_3)} = 2,\ 3 \text{ or } 4$$

since 2, 3 and 4 have only one partition into sum of two coprime positive integers. Since the branch points must be the same we get

$$\left(\frac{-a_2}{a_0}\right)^{n_1'} = \left(\frac{-a_3}{a_1}\right)^{n_0'}$$

and there exists a unique r such that

$$r^{n_0'} = -a_2/a_0, \quad r^{n_1'} = -a_3/a_1.$$

On substitution $x = zy$ the quadrinomial $J\big(f_1(x) - g_1(y)\big)$ takes the form

$$J\big(f_1(x) - g_1(y)\big) = a_0 y^{n_0+2|n_1|} z^{|n_1|}(z^{n_0} - r^{n_0'}) + a_1 y^{|n_1|}(1 - r^{n_1'} z^{|n_1|}).$$

Since the case $m_0 + m_1 = m_2 + m_3 = 0, a_0a_1 = a_2a_3$ has been excluded

$$\frac{1 - r^{n_1'} z^{|n_1|}}{z^{n_0} - r^{n_0'}}$$

is not a power in $\mathbb{C}(z)$. Also

$$\big(z^{n_0} - r^{n_0'}, 1 - r^{n_1} z^{|n_1|}\big) = z^{(n_0,n_1)} - r.$$

Thus in virtue of Capelli's theorem

$$J\big(f_1(x) - g_1(y)\big) = y^{|n_1|}\big(z^{(n_0,n_1)} - r\big)F(z, y)$$

where F is irreducible over $\mathbb{C}$.

It follows hence like in the case A that

$$d(x, y) = \big(a_0x^{m_0} + a_2y^{m_2}, a_1x^{m_1} + a_3y^{m_3}\big) = x^{(n_0,n_1)\delta} - ry^{(n_0,n_1)\varepsilon}$$

and qd^{-1} is irreducible over $\mathbb{C}$.

Since the case $m_0+m_1=m_2+m_3=0, a_0a_1=a_2a_3$ has been excluded the degree of $Jq(x^{-1}, y^{-1})$ is greater than that of q. The degrees of $Jd(x^{-1}, y^{-1})$ and of d are equal, thus qd^{-1} is not reciprocal.

Assume therefore that

$$\frac{n_0+|n_1|}{(n_0, n_1)}=n_0'+n_1'>4 \tag{6}$$

and set

$$f_3(x)=a_0x^{n_0'}+a_1x^{n_1'}, \quad g_3(y)=-a_2y^{n_2'}-a_3y^{n_3'}.$$

If $\boldsymbol{\Omega}_{f_3-z}=\boldsymbol{\Omega}_{g_3-z}$ we get the assertion of the lemma by the previous argument. Without loss of generality we may assume that

$$\boldsymbol{\Omega}_{f_3-z}\neq\boldsymbol{\Omega}_{f_3-z}\boldsymbol{\Omega}_{g_3-z}.$$

By Lemma 1, f_3 is indecomposable. It follows by Lüroth theorem that there is no field between $\mathbb{C}(z)$ and $\mathbb{C}(x_1)$, where $f_3(x_1)=z$, thus the monodromy group $G\big(\boldsymbol{\Omega}_{f_3-z}/\mathbb{C}(z)\big)$ is primitive (cf. [3], Lemma 2).

On the other hand, this group contains a 2-cycle, thus it must be the symmetric group $\mathfrak{S}_{n_0'+n_1'}$ (see [9], p. 35). $\boldsymbol{\Omega}_{f_3-z}\cap\boldsymbol{\Omega}_{g_3-z}$ is a normal proper subfield of $\boldsymbol{\Omega}_{f_3-z}$ which corresponds to a normal subgroup of $G\big(\boldsymbol{\Omega}_{f_3-z}/\mathbb{C}(z)\big)$. It follows from the well known property of symmetric groups that this subgroup is $\mathfrak{S}_{n_0'+|n_1'|}$ or $\mathfrak{A}_{n_0'+|n_1'|}$ (see [9], p. 67). By the theorem of natural irrationalities

$$G\big(\boldsymbol{\Omega}_{f_3-z}/(\boldsymbol{\Omega}_{f_3-z}\cap\boldsymbol{\Omega}_{g_3-z})\big)\cong G\big(\boldsymbol{\Omega}_{f_3-z}\boldsymbol{\Omega}_{g_3-z}/\boldsymbol{\Omega}_{g_3-z}\big).$$

However, $G\big(\boldsymbol{\Omega}_{f_3-z}\boldsymbol{\Omega}_{g_3-z}/\boldsymbol{\Omega}_{g_3-z}\big)$ is a quotient group of $G(\boldsymbol{\Omega}_{g-z}/\boldsymbol{\Omega}_{g_3-z})$.

Since $g=g_3(x^{\varepsilon(n_2,n_3)})$ we easily see that $G(\boldsymbol{\Omega}_{g-z}/\boldsymbol{\Omega}_{g_3-z})$ is a cyclic group and since by (6) none of the groups $\mathfrak{S}_{n_0'+|n_1'|}, \mathfrak{A}_{n_0'+|n_1'|}$ is cyclic we get a contradiction.

2. Riemann surface $2\sqrt{a_2a_3}\,T_{n_2}(x)=z$ has an n_2-cycle at ∞ and for $n_2>2$ two branch points $2\eta\sqrt{a_2a_3}$ with the permutations of type $\underbrace{(2)(2)\dots(2)}_{(n_2-1)/2 \text{ times}}$ if n_2 is odd and $\underbrace{(2)(2)\dots(2)}_{(n_2-1-\varepsilon)/2 \text{ times}}$ if n_2 is even ($\eta=\pm1$); for $n_2=2$ there is only one branch point ($\eta=-1$).

A. $n_0>n_1>0$. Then

$$n_0=n_2, \quad n_1=1,$$

and either

$$n_0-1=2; \quad \pm\frac{2}{3}a_1\sqrt{\frac{-a_1}{3a_0}}=\pm2\sqrt{a_2a_3}, \quad a_1^3=-27a_0a_2a_3,$$

the case considered under 1B, or

$$n_0-1=1; \quad -\frac{a_1^2}{4a_0}=-2\sqrt{a_2a_3}; \quad a_1^4=64a_0^2a_2a_3$$

and

$$q(x, y)=a_0x^{2\delta}y^{2\varepsilon}+a_1x^{\delta}y^{2\varepsilon}+a_2y^{4\varepsilon}+a_3=u^2-4tuvw-t^2v^4-4t^2w^4,$$

where $t = 1$, $u = a_0^{1/2}x^\delta y^\varepsilon$, $v = (-a_2)^{1/4}y^\varepsilon$, $w = (-a_3/4)^{1/4}$ and suitable values of the quadratic roots and quartic roots are taken. In the latter case the factors $u \pm tv^2 - 2tvw \pm 2tw^2$ are irreducible over $\mathbb{C}$, since they equal

$$a_0^{1/2}x^\delta y^\varepsilon \pm \left[(-a_2)^{1/2}y^{2\varepsilon} - 2(-a_2)^{1/4}(-a_3/4)^{1/4}y^\varepsilon + 2(-a_3/4)^{1/4}\right]$$

and the expression in brackets is not a power in $\mathbb{C}[y_1]$. Moreover, one verifies directly that the factors are non-reciprocal.

B. $n_0 > 0 > n_1$. Then

$$[n_0, n_1] = n_2, \quad \frac{n_0 + |n_1|}{(n_0, n_1)} = 2, \quad n_0 = -n_1 = n_2 = -n_3;$$

$$\pm 2a_1\sqrt{\frac{a_0}{a_1}} = \pm 2\sqrt{a_2a_3}, \quad a_0a_1 = a_2a_3,$$

$m_0 + m_1 = m_2 + m_3 = 0$, the case excluded.

3. The case is symmetric to the former.

4. Then $n_0 = -n_1 = n_2 = -n_3$, $\pm 2\sqrt{a_0a_1} = \pm 2\sqrt{a_2a_3}$, $a_0a_1 = a_2a_3$, $m_0 + m_1 = m_2 + m_3 = 0$, the case excluded. □

Lemma 3. *Let* $\boldsymbol{K}$ *be any field of characteristic* 0, $a_i \in \boldsymbol{K}$, $a_i \neq 0$ $(i = 0, 1, 2, 3)$, m_i *integers,* $m_0 + m_1 \geqslant 0$, $m_0 \neq m_1$, $m_2 + m_3 \geqslant 0$, $m_2 \neq m_3$ *and exactly one among* m_i *be zero. If* $q(x, y) = J\left(a_0x^{m_0} + a_1x^{m_1} + a_2y^{m_2} + a_3y^{m_3}\right)$ *is reducible over* $\boldsymbol{K}$ *then it can be represented in the form*

$$t(u^2 + 2uv + v^2 - w^2) = t(u + v + w)(u + v - w) \tag{7}$$

where $t \in \boldsymbol{K}$ *and* u, v, w *are monomials in* $\boldsymbol{K}[x, y]$. *The factors on the right hand side of* (7) *are irreducible over* $\boldsymbol{K}$ *and non-reciprocal.*

Proof. We may assume without loss of generality that $m_3 = 0$. Then $q(x, y)$ is a binomial over $\boldsymbol{K}(x)$. By Capelli's theorem, it is reducible only if either for some prime $l \mid m_2$, $a_2^{-1}(a_0x^{m_0} + a_1x^{m_1} + a_3) = -g(x)^l$ or $4 \mid m_2$ and $a_2^{-1}(a_0x^{m_0} + a_1x^{m_1} + a_3) = 4g(x)^4$, $g(x) \in \boldsymbol{K}(x)$. However $a_0x^{m_0} + a_1x^{m_1} + a_3$ may have at most double zero, therefore $l = 2$, $a_0x^{m_0} + a_1x^{m_1} + a_3 = -a_2g(x)^2$ and $g(x)$ has only simple zeros. Moreover, $g(x)$ must have only two terms and taking

$$k = -a_2, \quad u + v = Jg(x), \quad w = \frac{Jg(x)}{g(x)}\,y^{m_2/2}$$

we get the representation of $q(x, y)$ in the form (7). Again by Capelli's theorem the trinomials

$$u + v \pm w = J\left(g(x) \pm y^{m_2/2}\right)$$

are irreducible over $\boldsymbol{K}$. One verifies directly that they are not reciprocal. □

Lemma 4. *If any of the equations*

$$Q(y_1, y_2) = Z_0(U_0^2 + 2U_0V_0 + V_0^2 - 1), \tag{8}$$

$$Q(y_1, y_2) = Z_0(U_0^3 + V_0^3 + 1 - 3U_0V_0), \tag{9}$$

$$Q(y_1, y_2) = Z_0(U_0^2 - 4U_0V_0 - V_0^4 - 4) \tag{10}$$

is satisfied by rational functions U_0, V_0, Z_0 of the type $cy_1^{\alpha_1}y_2^{\alpha_2}$, $c \in \boldsymbol{K}$, then $Q(y_1, y_2)$ is representable in the corresponding form (1)*, where $k \in \boldsymbol{K}$, T, U, V, W are monomials over $\boldsymbol{K}$ and moreover*

$$UU_0^{-1} = VV_0^{-1} = W \quad \textit{if} \quad (8) \textit{ or } (9),$$
$$UU_0^{-1} = W^2T, \quad VV_0^{-1} = W \quad \textit{if} \quad (10).$$

Proof. Let y_i divide U_0, V_0, Z_0 with the exponent u_i, v_i, z_i. Since $\big(Q(y_1, y_2), y_1y_2\big) = 1$ we have

$$z_i = \begin{cases} -\min(2u_i, u_i + v_i, 2v_i, 0) & \text{if (8)}, \\ -\min(3u_i, 3v_i, u_i + v_i, 0) & \text{if (9)}, \\ -\min(2u_i, u_i + v_i, 4v_i, 0) & \text{if (10)}. \end{cases}$$

Since

$$u_i + v_i \geqslant \min(2u_i, 2v_i),$$
$$u_i + v_i \geqslant \min(3u_i, 3v_i, 0),$$
$$u_i + v_i \geqslant \min(2u_i, 4v_i, 0),$$

it follows that

$$z_i = \begin{cases} -\min(2u_i, 2v_i) = 2z_i' & \text{if (8)}, \\ -\min(3u_i, 3v_i, 0) = 3z_i' & \text{if (9)}, \\ -\min(2u_i, 4v_i, 0) = 2z_i' & \text{if (10)}, \end{cases}$$

where $z_i' \geqslant 0$ is an integer. We set in case (8) and (9)

$$k = Z_0y_1^{-z_1}y_2^{-z_2}, \quad W = y_1^{z_1'}y_2^{z_2'}, \quad U = U_0W, \quad V = V_0W;$$

in case (10)

$$k = Z_0y_1^{-z_1}y_2^{-z_2}, \ W = y_1^{[z_1'/2]}y_2^{[z_2'/2]}, \ T = y_1^{z_1'}y_2^{z_2'}W^{-2}, \ U = U_0W^2T, \ V = V_0W$$

and the conditions of the lemma are satisfied. □

Proof of Theorem 1. The sufficiency of the condition is obvious. In order to prove the necessity and the other assertions of the theorem set

$$\Delta_1 = \begin{vmatrix} \nu_{11} & \nu_{12} \\ \nu_{21} & \nu_{22} \end{vmatrix}, \quad \Delta_2 = \begin{vmatrix} \nu_{12} & \nu_{13} \\ \nu_{22} & \nu_{23} \end{vmatrix}, \quad \Delta_3 = \begin{vmatrix} \nu_{13} & \nu_{11} \\ \nu_{23} & \nu_{21} \end{vmatrix};$$

$$\delta = \begin{cases} 1 & \text{if } \Delta_1 + 2\Delta_2 + \Delta_3 \geqslant 0, \\ -1 & \text{if } \Delta_1 + 2\Delta_2 + \Delta_3 < 0; \end{cases} \qquad \varepsilon = \begin{cases} 1 & \text{if } \Delta_1 - \Delta_3 \geqslant 0, \\ -1 & \text{if } \Delta_1 - \Delta_3 < 0. \end{cases}$$

Since the matrix $[\nu_{ij}]$ is of rank 2 we may assume without loss of generality that $\Delta_1 + \Delta_3 \neq 0$. On substitution

$$y_1 = x^{\delta(\nu_{22}-\nu_{23})} y^{-\varepsilon\nu_{21}}, \quad y_2 = x^{\delta(\nu_{13}-\nu_{12})} y^{\varepsilon\nu_{11}}$$

we get

$$\begin{aligned}\Phi(y_1, y_2) &:= a_0 + \sum_{i=1}^{3} a_i y_1^{\nu_{1i}} y_2^{\nu_{2i}} \\ &= x^{-\delta\Delta_2}(a_0 x^{m_0} + a_1 x^{m_1} + a_2 y^{m_2} + a_3 y^{m_3}) =: x^{-\delta\Delta_2}\varphi(x, y),\end{aligned}$$

where

$$m_0 = \delta\Delta_2, \quad m_1 = \delta(\Delta_1 + \Delta_2 + \Delta_3), \quad m_2 = \varepsilon\Delta_1, \quad m_3 = -\varepsilon\Delta_3.$$

We have $m_0 \neq m_1$, $m_2 \neq m_3$ and by the choice of δ and ε, $m_0 + m_1 \geqslant 0$, $m_2 + m_3 \geqslant 0$.

Moreover setting $q(x, y) = J\varphi(x, y)$ we get

$$Q(y_1, y_2) = x^A y^B q(x, y). \tag{11}$$

Assume that

$$Q(y_1, y_2) = F_1(y_1, y_2) F_2(y_1, y_2),$$

where F_1, F_2 are non-constant polynomials over $\boldsymbol{K}$. It follows that

$$\begin{aligned}q(x, y) = J F_1\big(x^{\delta(\nu_{22}-\nu_{23})} y^{-\varepsilon\nu_{21}}, x^{\delta(\nu_{13}-\nu_{12})} y^{\varepsilon\nu_{11}}\big) \\ \times J F_2\big(x^{\delta(\nu_{22}-\nu_{23})} y^{-\varepsilon\nu_{12}}, x^{\delta(\nu_{13}-\nu_{12})} y^{\varepsilon\nu_{11}}\big),\end{aligned} \tag{12}$$

where the factors on the right hand side are non-constant. We distinguish three cases

(i) $m_0 = -m_1$, $m_2 = -m_3$, $a_0 a_1 = a_2 a_3$;

(ii) $m_0 m_1 m_2 m_3 \neq 0$ and (i) does not hold;

(iii) $m_0 m_1 m_2 m_3 = 0$.

(i) We have here $\Delta_1 = -\Delta_2 = \Delta_3$. Hence

$$\nu_{i1} = \nu_{i2} + \nu_{i3} \quad (i = 1, 2)$$

and

$$\Phi(y_1, y_2) = (a_0 + a_2 y_1^{\nu_{12}} y_2^{\nu_{22}})\Big(1 + \frac{a_3}{a_0} y_1^{\nu_{13}} y_2^{\nu_{23}}\Big),$$

thus $Q(y_1, y_2)$ can be divided into two parts with the highest common factor

$$D = J(a_0 + a_2 y_1^{\nu_{12}} y_2^{\nu_{22}})$$

being a binomial. The complementary factor

$$QD^{-1} = J\Big(1 + \frac{a_3}{a_0} y_1^{\nu_{13}} y_2^{\nu_{23}}\Big)$$

is also a binomial.

(ii) Assuming, as we may, that $\boldsymbol{K} \subset \mathbb{C}$, we can apply Lemma 2 and we infer that either $q(x, y)$ can be divided into two parts with the highest common factor $d(x, y)$ being a binomial or $q(x, y)$ can be represented in one of the forms (2), where t, u, v, w are monomials in $\mathbb{C}[x, y]$. In the former case qd^{-1} is irreducible over $\mathbb{C}$ and non-reciprocal, in the latter case the factors on the right hand side of (2) are irreducible over $\mathbb{C}$ and non-reciprocal. Now, if

$$d_i(x, y) = \big(J(a_0 x^{m_0} + a_i y^{m_i}),\, J(a_1 x^{m_1} + a_{5-i} y^{m_{5-i}})\big) \quad (i = 2 \text{ or } 3),$$
$$D_i(x, y) = \big(J(a_0 + a_i y_1^{\nu_{1i}} y_2^{\nu_{2i}}),\, J(a_1 y_1^{\nu_{11}} y_2^{\nu_{21}} + a_{5-i} y_1^{\nu_{1,5-i}} y_2^{\nu_{2,5-i}})\big)$$

then

$$d_i(y_1, y_2) = J D_i\big(x^{\delta(\nu_{22}-\nu_{23})} y^{-\varepsilon\nu_{21}},\, x^{\delta(\nu_{13}-\nu_{12})} y^{\varepsilon\nu_{11}}\big),$$

thus the properties of d_i imply the corresponding properties of D_i.

If

$$q(x, y) = u^3 + v^3 + w^3 - 3uvw = (u + v + w)(u + \zeta_3 v + \zeta_3^{-1} w)(u + \zeta_3^{-1} v + \zeta_3 w) \tag{13}$$

then by the absolute irreducibility of the factors on the right hand side and by (12) we have for suitable $i = 1$ or 2, suitable $j = 0$ or ± 1 and suitable α, β, γ

$$F_i(y_1, y_2) = \gamma x^\alpha y^\beta (u + \zeta_3^j v + \zeta_3^{-j} w).$$

We may assume without loss of generality that $j = 0$. It follows that

$$U_0 = u w^{-1} \in \boldsymbol{K}(y_1, y_2), \quad V_0 = v w^{-1} \in \boldsymbol{K}(y_1, y_2) \tag{14}$$

and by (11) and (13)

$$Q(y_1, y_2) = x^A y^B w^3 (U_0^3 + V_0^3 + 1 - 3U_0 V_0).$$

Since u, v, w are monomials in $\mathbb{C}[x, y]$, U_0, V_0 and $Z = x^A y^B w^3$ are of the form $c y_1^{\alpha_1} y_2^{\alpha_2}$, $c \in \boldsymbol{K}$. By Lemma 4 there exist monomials U, V, W in $\boldsymbol{K}[y_1, y_2]$ and $k \in \boldsymbol{K}$ such that

$$Q(y_1, y_2) = k(U^3 + V^3 + W^3 - 3UVW), \quad U U_0^{-1} = V V_0^{-1} = W.$$

It follows by (14) that

$$U u^{-1} = V v^{-1} = W w^{-1},$$
$$J(U + \zeta_3^j V + \zeta_3^{-j} W)\big(x^{\delta(\nu_{22}-\nu_{23})} y^{-\varepsilon\nu_{21}},\, x^{\delta(\nu_{13}-\nu_{12})} y^{\varepsilon\nu_{11}}\big) = \eta(u + \zeta_3^j v + \zeta_3^{-j} w) \quad (\eta \in \mathbb{C},\ j = 0,\ \pm 1)$$

and since $u + \zeta_3^j v + \zeta_3^{-j} w$ is irreducible over $\mathbb{C}$ and non-reciprocal, $U + \zeta_3^j V + \zeta_3^{-j} W$ has the same property. If $\zeta_3 \notin \boldsymbol{K}$

$$U^2 + V^2 + W^2 - UV - UW - VW = (U + \zeta_3 V + \zeta_3^{-1} W)(U + \zeta_3^{-1} V + \zeta_3 W)$$

is irreducible over $\boldsymbol{K}$. It is also non-reciprocal by the corresponding property of $u^2 + v^2 + w^2 - uv - uw - vw$.

Assume now that

$$q(x, y) = u^2 - 4tuvw - t^2v^4 - 4t^2w^4 \\ = (u - tv^2 - 2tvw - 2tw^2)(u + tv^2 - 2tvw + 2tw^2).$$

Then by the absolute irreducibility of the factors on the right hand side and by (12) we have for a suitable sign and suitable α, β, γ

$$F_1(y_1, y_2) = \gamma x^\alpha y^\beta (u \pm tv^2 - 2tvw \pm 2tw^2).$$

It follows that

$$U_0 = ut^{-1}w^{-2} \in \boldsymbol{K}(y_1, y_2), \quad V_0 = vw^{-1} \in \boldsymbol{K}(y_1, y_2) \tag{15}$$

and by (11)

$$Q(y_1, y_2) = x^A y^B t^2 w^4 (U_0^2 - 4U_0V_0 - V_0^4 - 4).$$

By Lemma 4 there exist monomials T, U, V, W in $\boldsymbol{K}[x, y]$ and $k \in \boldsymbol{K}$ such that

$$Q(y_1, y_2) = k(U^2 - 4TUVW - V^4 - 4T^2W^4), \quad UU_0^{-1} = TW^2, \quad VV_0^{-1} = W.$$

It follows by (15) that

$$Uu^{-1} = TV^2t^{-1}v^{-2} = TVWt^{-1}v^{-1}w^{-1} = TW^2t^{-1}w^{-2},$$

$$J\left(U \pm TV^2 - 2TVW \pm 2TW^2\right)\left(x^{\delta(\nu_{22}-\nu_{23})}y^{-\varepsilon\nu_{21}}, x^{\delta(\nu_{13}-\nu_{12})}y^{\varepsilon\nu_{11}}\right) \\ = \eta(u \pm tv^2 - 2tvw \pm 2tw^2) \quad (\eta \in \mathbb{C})$$

and since $u \pm tv^2 - 2tvw \pm 2tw^2$ is irreducible over $\mathbb{C}$ and non-reciprocal, $U \pm TV^2 - 2TVW \pm 2TW^2$ has the same property.

(iii) If two of the numbers m_0, m_1, m_2, m_3 were equal to zero, two of the vectors $[0, 0]$, $[\nu_{1i}, \nu_{2i}]$ $(i \leqslant 3)$ would be equal. Thus exactly one m_i is zero, we can apply Lemma 3 and infer that $q(x, y)$ is representable in the form (7), where $k \in \boldsymbol{K}$, u, v, w are monomials in $\boldsymbol{K}[x, y]$, the trinomials $u + v \pm w$ are irreducible over $\boldsymbol{K}$ and non-reciprocal.

It follows from (12) that for a suitable sign and suitable α, β, γ

$$F_1(y_1, y_2) = \gamma x^\alpha y^\beta (u + v \pm w).$$

Thus

$$U_0 = uw^{-1} \in \boldsymbol{K}(y_1, y_2), \quad V_0 = vw^{-1} \in \boldsymbol{K}(y_1, y_2) \tag{16}$$

and by (11)

$$Q(y_1, y_2) = x^A y^B w^2 (U_0^2 + 2U_0V_0 + V_0^2 - 1).$$

By Lemma 4 there exist monomials U, V, W in $\boldsymbol{K}[x, y]$ and $k \in \boldsymbol{K}$ such that

$$Q(y_1, y_2) = k(U^2 + 2UV + V^2 - W^2), \quad UU_0^{-1} = VV_0^{-1} = W.$$

It follows by (16) that

$$Uu^{-1} = Vv^{-1} = Ww^{-1},$$

$$J(U+V\pm W)(x^{\delta(\nu_{22}-\nu_{23})}y^{-\varepsilon\nu_{21}}, x^{\delta(\nu_{13}-\nu_{12})}y^{\varepsilon\nu_{11}}) = \eta(u+v\pm w) \quad (\eta\in \boldsymbol{K})$$

and since $u+v\pm w$ is irreducible over $\boldsymbol{K}$ and non-reciprocal, $U+V\pm W$ has the same property. The proof of Theorem 1 is complete. □

Proof of Theorem 2. In order to prove the necessity of the condition we apply Theorem 2 of [8] setting there

$$F(x_1, x_2, x_3) = ax_1 + bx_2 + cx_3 + d$$

so that

$$g(x) = F(x^m, x^n, x^p).$$

By the said theorem there exists a matrix $\boldsymbol{N} = [\nu_{ij}]_{\substack{i\leqslant r\\ j\leqslant 3}}$ of rank $r \leqslant 3$ such that

$$0 < \max|\nu_{ij}| < c_r(F), \tag{17}$$

$$[m, n, p] = [v_1, \ldots, v_r]\boldsymbol{N}, \tag{18}$$

$$L\Big(a\prod_{i=1}^{r} y_i^{\nu_{i1}} + b\prod_{i=1}^{r} y_i^{\nu_{i2}} + c\prod_{i=1}^{r} y_i^{\nu_{i3}} + d\Big) \overset{\text{can}}{=} \text{const}\prod_{\sigma=1}^{s} F_\sigma(y_1, \ldots, y_r)^{e_\sigma} \tag{19}$$

implies

$$Lq(x) \overset{\text{can}}{=} \text{const}\prod_{\sigma=1}^{s} LF_\sigma(x^{v_1}, \ldots, x^{v_r})^{e_\sigma}. \tag{20}$$

Therefore, if $Lq(x)$ is reducible then the left hand side of (19) is reducible. It follows by Lemma 14 of [8] that $r < 3$.

If $r = 2$, set in Theorem 1: $a_0 = d$, $a_1 = a$, $a_2 = b$, $a_3 = c$ so that the left hand side of (19) becomes $LQ(y_1, y_2)$ in the notation of that theorem. The vectors $[0, 0]$, $[\nu_{1i}, \nu_{2i}]$ $(i \leqslant 3)$ are all different in view of (18) and of the assumption $m > n > p > 0$. If $Q(y_1, y_2)$ is a product of two binomials, $q(x) = JQ(x^{v_1}, x^{v_2})$ is also such a product. This case has been excluded, but the condition is satisfied also here, since one of the binomials must be non-reciprocal and it is the desired non-reciprocal common factor of two parts of $q(x)$. Apart from this case, in virtue of Theorem 1, $LQ(y_1, y_2)$ is reducible if and only if either Q can be divided into two parts which have a non-reciprocal common factor or it can be represented in one of the forms (1), where $k \in \mathbb{Q}$ and T, U, V, W are monomials in $\mathbb{Q}[y_1, y_2]$. If $F_\sigma(y_1, y_2)$ is an irreducible non-reciprocal factor of $\mathbb{Q}(y_1, y_2)$, $LF_\sigma(x^{v_1}, x^{v_2})$ is by (20) an irreducible non-reciprocal factor of $q(x)$. Therefore, we get either a partition of $q(x)$ into two parts which have a common non-reciprocal factor or a representation of $q(x)$ in one of the forms (1), where T, U, V, W are monomials in $\mathbb{Q}[x]$ and the factors on the right hand side are non-reciprocal.

Finally, if $r = 1$ then $m = vm_1$, $n = vn_1$, $p = vp_1$,

$$m_1 < c_1(F) = \exp_2\big(24\cdot 2^{a^2+b^2+c^2+d^2-1}\log(a^2+b^2+c^2+d^2)\big) = C(a, b, c, d)$$

by (17), (18) and the formula for $c_1(F)$ given in [8](2). Moreover

$$L(ax^{m_1} + bx^{n_1} + cx^{p_1} + d) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(x)^{e_\sigma}$$

implies

$$L(ax^m + bx^n + cx^p + d) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} LF_\sigma(x^v)^{e_\sigma}.$$

Thus the necessity of the condition is proved. In order to prove the sufficiency it is enough to consider the case where $q(x)$ can be divided into two parts which have a common non-reciprocal factor $\delta(x)$. Since the highest common factor of two binomials is either 1 or a binomial and since binomial with a non-reciprocal factor is itself non-reciprocal we may assume that $\delta(x)$ is the highest common factor of two parts of $q(x)$ and hence a binomial. We prove that $q\delta^{-1}$ is non-reciprocal. Indeed, otherwise, we should have

$$\delta(x) = x^r + e, \quad e \neq \pm 1, \tag{21}$$

$$\pm(ax^m + bx^n + cx^p + d)(ex^r + 1) = (dx^m + cx^{m-p} + bx^{m-n} + a)(x^r + e) \tag{22}$$

and either

$$\delta(x) = (ax^m + bx^n, cx^p + d) \tag{23}$$

or

$$\delta(x) = (ax^m + cx^p, bx^n + d) \tag{24}$$

or

$$\delta(x) = (ax^m + d, bx^n + cx^p). \tag{25}$$

It follows from (22) that

$$\pm ae = d \tag{26}$$

thus by (21) $\delta(x)$ cannot divide $ax^m + d$ and (25) is excluded. If (23) or (24) holds we have $m \neq n + p$, since otherwise

$$\delta(x) = x^{m-n} + \frac{b}{a} = x^p + \frac{d}{c} \quad \text{or} \quad \delta(x) = x^{m-p} + \frac{c}{a} = x^n + \frac{d}{b}$$

and $q(x)$ is a product of two binomials. We may assume without loss of generality that $m > n + p$. If $r < p$ then comparing the coefficients of x^m on both sides of (22) we get $\pm a = ed$, which together with (26) gives $e = \pm 1$, contrary to (21). If $r > p$ the on the right hand side of (22) occurs the term cx^{m-p+r} lacking on the left hand side. If $r = p$ then comparing the coefficients of x^m on both sides of (22) we get

$$\pm a = de + c. \tag{27}$$

(2) Page 346 in this volume.

If (23) holds then $e = d/c$ and since $\pm ae = d$ we get $\pm a = c$, $de = 0$, a contradiction. If (24) holds, then $\delta(x) \mid ax^m + cx^p$ gives

$$p \mid m, \quad c/a = -(-e)^{m/p-1}$$

and by (26) and (27) $e^2 \mp (-e)^{m/p-1} = 1$, which has no rational solution. □

Proof of Theorem 3. In virtue of Theorem 2 $L(x^m + \varepsilon x^n + cx^p + d)$ is reducible if and only if at least one of the conditions specified in the assertion is satisfied.

Suppose that $\dfrac{x^m + \varepsilon x^n + cx^p + d}{L(x^m + \varepsilon x^n + cx^p + d)}$ is non-constant and let

$$\lambda^m + \varepsilon\lambda^n + c\lambda^p + d = 0 = \lambda^{-m} + \varepsilon\lambda^{-n} + c\lambda^{-p} + d.$$

Thus $d\lambda^{n+m} + c\lambda^{n+m-p} + \varepsilon\lambda^m + \lambda^n = 0$, $\varepsilon\lambda^m + \lambda^n + c\varepsilon\lambda^p + d = 0$, hence

$$F(\lambda) = d\lambda^{n+m} + c\lambda^{n+m-p} - c\varepsilon\lambda^p - d\varepsilon = 0.$$

By a theorem of A. Cohn ([1], p. 113), the equations $F(x) = 0$ and $x^{m+n-1}F'(x^{-1}) = 0$ have the same number of zeros inside the unit circle. We have

$$\lambda^{m+n-1}F'(\lambda^{-1}) = \lambda^{m+n-1}\big(d(m+n)\lambda^{1-m-n} + c(m+n-p)\lambda^{1+p-m-n} - c\varepsilon p\lambda^{1-p}\big)$$

$$= d(m+n) + c(m+n-p)\lambda^p - c\varepsilon p\lambda^{n+m-p}.$$

Assuming $|\lambda| < 1$ we obtain

$$|d(m+n)| < |c|(n+m-p) + |c|p = |c|(m+n),$$

which is impossible.

Consequently F has no zero inside the unit circle and since F is reciprocal all zeros are on the boundary of the unit circle. It follows that the same is true for $\dfrac{x^m + \varepsilon x^n + cx^p + d}{L(x^m + \varepsilon x^n + cx^p + d)}$. However the last polynomial is monic with integer coefficients, thus by Kronecker's theorem all its zeros are roots of unity.

Therefore $K(x^m + \varepsilon x^n + cx^p + d) = L(x^m + \varepsilon x^n + cx^p + d)$ and the proof of the theorem is complete. □

Proof of Corollary. In virtue of Theorem 3, $x^m + \varepsilon x^n + cx^p + d$ is reducible if and only if either one of the conditions specified in the theorem is satisfied or $x^m + \varepsilon x^n + cx^p + d$ has a proper cyclotomic factor. Now, by a theorem of Mann [7] if a root of unity λ satisfies

$$\lambda^m + \varepsilon\lambda^n + c\lambda^p + d = 0$$

then either the left hand side can be divided into two vanishing summands or $\lambda^{6(m,n,p)} = 1$. The first possibility corresponds to the first three equalities specified in the corollary, the second gives

$$\zeta^{m/\delta} + \varepsilon\zeta^{n/\delta} + c\zeta^{p/\delta} + d = 0,$$

where $\zeta^6 = 1$, $\delta = (m, n, p)$. □

Addendum. The proof of Theorem 1 amounts to investigating factors of rational functions of the form $f(x) - g(y)$ (variables separated). When both f and g are polynomials the investigation is easier and [4] has far-reaching results. We know of little work beyond the quadrinomial case of this paper on the investigation of factors of rational functions with variables separated.

References

[1] A. Cohn, *Über die Anzahl der Wurzeln einer algebraischer Gleichung in einem Kreise*. Math. Z. 14 (1922), 110–148.

[2] H. T. Engstrom, *Polynomial substitutions*. Amer. J. Math. 63 (1941), 249–255.

[3] M. Fried, *On a conjecture of Schur*. Michigan Math. J. 17 (1970), 41–55.

[4] —, *The field of definition of function fields and a problem in the reducibility of polynomials in two variables*. Illinois J. Math. 17 (1973), 128–146.

[5] W. Ljunggren, *On the irreducibility of certain trinomials and quadrinomials*. Math. Scand. 8 (1960), 65–70.

[6] —, *On the irreducibility of certain lacunary polynomials*. Norske Vid. Selsk. Forh. (Trondheim) 36 (1963), 159–164.

[7] H. B. Mann, *On linear relations between roots of unity*. Mathematika 12 (1965), 107–117.

[7a] W. H. Mills, *The factorization of certain quadrinomials*. Math. Scand. 57 (1985), 44–50.

[8] A. Schinzel, *Reducibility of lacunary polynomials* I. Acta Arith. 16 (1969), 123–159; *Corrigenda*: Acta Arith. 19 (1971), 201; ibid. 24 (1978), 265; this collection: D4, 344–380.

[9] N. Tschebotaröw, *Grundzüge der Galoisschen Theorie*. Übersetzt und bearbeitet von H. Schwerdtfeger, Noordhoff, Groningen–Djakarta 1950.

Andrzej Schinzel
Selecta

Originally published in
Journal of the Indian Mathematical Society
37 (1973), 1–8

A general irreducibility criterion

In memory of Wilhelm Ljunggren

The aim of this paper is to prove the following theorem, which in a slightly different form (see Corollary) was conjectured in [1].

Theorem 1. *Let K be any field over a prime field Π and let $a_j \neq 0$ $(0 \leqslant j \leqslant k)$ be elements of K. If the rank of an integral matrix*

$$M = \begin{pmatrix} 1 & \dots & 1 \\ \nu_{10} & \dots & \nu_{1k} \\ \dots & \dots & \dots \\ \nu_{l0} & \dots & \nu_{lk} \end{pmatrix}$$

over Π is equal to its rank over $\mathbb{Q}$ and is greater than $(k+3)/2$ and vectors $[\nu_{1j}, \dots, \nu_{lj}]$ are all different $(0 \leqslant j \leqslant k)$, then

$$F(x_1, \dots, x_l) = \Big(\sum_{j=0}^{k} a_j \prod_{i=1}^{l} x_i^{\nu_{ij}}\Big) \prod_{i=1}^{l} x_i^{-\min_j \nu_{ij}} \tag{1}$$

is irreducible over K.

For a given rational function ϕ of the form $\sum_{j=0}^{k} a_j \prod_{i=1}^{l} x_i^{\nu_{ij}}$ where $a_j \neq 0$ and the vectors $[\nu_{1j}, \dots, \nu_{lj}]$ are all different (such a representation is unique) $\phi \prod_{i=1}^{l} x_i^{-\min_j \nu_{ij}}$ was denoted in [1] by $J\phi$. Theorem 1 implies

Corollary. *If $a_j \neq 0$ $(0 \leqslant j \leqslant k)$ are complex numbers and the rank of an integral matrix $[\nu_{ij}]$ is greater than $(k+1)/2$ then*

$$J\Big(a_0 + \sum_{j=1}^{k} a_j \prod_{i=1}^{l} x_i^{\nu_{ij}}\Big)$$

is absolutely irreducible.

In virtue of the results of [1] Corollary implies easily:

Theorem 2. *If* $a_j \neq 0\ (0 \leqslant j \leqslant k)$ *are integers,* n_j *are positive integers and* $a_0 + \sum_{j=1}^{k} a_j x^{n_j}$ *has more than one or multiple, irreducible over* $\mathbb{Q}$*, non-reciprocal factor, then there exist* $[k/2]$ *linearly independent integral vectors* $[\gamma_{i1}, \ldots, \gamma_{ik}]$ *such that*

$$\sum_{j=1}^{k} n_i \gamma_{ij} = 0 \quad (1 \leqslant i \leqslant [k/2]),$$

$$\max_{i,j} |\gamma_{ij}| \leqslant \exp_{k^2}\Big(\sum_{j=0}^{k} a_j^2\Big). \tag{2}$$

Theorems 1 and 2 are best possible in the following sense: they cease to be true if the number $(k+3)/2$ in Theorem 1 is diminished or the number $[k/2]$ in Theorem 2 is increased, no matter by what function of a_j's one replaces the right hand side of (2). We prove it at the end of the paper.

Proof of Theorem 1. We proceed by induction with respect to l. If $l = 1$ the theorem holds since its assumption is never satisfied. Assume therefore that the theorem holds for all polynomials in $l-1$ variables ($l \geqslant 2$) over any field and suppose that the polynomial (1) is reducible over K:

$$F(x_1, \ldots, x_l) = F_1(x_1, \ldots, x_l) F_2(x_1, \ldots, x_l), \quad F_n \neq \text{const.} \quad (n = 1, 2). \tag{3}$$

Let the matrix M be of rank $r+1$. We can assume, without loss of generality, that

$$D = \det[v_{ij} - v_{i0}]_{1 \leqslant i,j \leqslant r} \neq 0 \text{ in } \Pi, \quad D > 0.$$

Let

$$[\alpha_{ij}] = [v_{ij} - v_{i0}]^{-1}_{1 \leqslant i,j \leqslant r}$$

$$x_i = \begin{cases} \prod_{s=1}^{r} \Big(y_s \prod_{t=r+1}^{l} y_t^{-v_{ts}+v_{t0}} \Big)^{D\alpha_{si}} & \text{if } i \leqslant r, \\ y_i^D & \text{if } i > r. \end{cases} \tag{4}$$

We get $\prod_{i=1}^{l} x_i^{v_{ij}-v_{i0}} = \prod_{i=1}^{l} y_i^{\lambda_{ij}}$, where for $j \leqslant r$,

$$\lambda_{ij} = \begin{cases} D \sum_{q=1}^{r} \alpha_{iq}(v_{qj} - v_{q0}) = D & \text{if } i = j, \\ D \sum_{q=1}^{r} \alpha_{iq}(v_{qj} - v_{q0}) = 0 & \text{if } i \neq j,\ i \leqslant r, \\ D \sum_{q,s=1}^{r} \alpha_{sq}(v_{qj} - v_{q0})(-v_{is} + v_{i0}) + D(v_{ij} - v_{i0}) & \text{if } i > r. \end{cases} \tag{5}$$

It follows from (3) that $G(y_1, \dots, y_l) = G_1(y_1, \dots, y_l)G_2(y_1, \dots, y_l)$, where

$$G(y_1, \dots, y_l) = JF\big(P_1, \dots, P_r, y_{r+1}^D, \dots, y_l^D\big),$$
$$G_n(y_1, \dots, y_l) = JF_n\big(P_1, \dots, P_r, y_{r+1}^D, \dots, y_l^D\big) \quad (n = 1, 2),$$
$$P_i = \prod_{s=1}^{r}\Big(y_s \prod_{t=1}^{l} y_t^{-\nu_{ts}+\nu_{t0}}\Big)^{D\alpha_{si}} \quad (i = 1, \dots, r).$$

Since on setting

$$y_j = \prod_{i=1}^{l} z_i^{\nu_{ij}-\nu_{i0}} \ (j \leqslant r), \quad y_j = z_j \ (j > r),$$

we get $x_i = z_i^D$ $(1 \leqslant i \leqslant l)$ the transformation (4) transforms distinct monic monomials in x_i's into distinct monic monomials in y_i's. It follows that the vectors $[\lambda_{1j}, \dots, \lambda_{lj}]$ are all different and setting

$$\lambda_i = \min_{0 \leqslant j \leqslant k} \lambda_{ij} \quad (1 \leqslant i \leqslant l)$$

we have

$$G(y_1, \dots, y_l) = \Big(\sum_{j=0}^{k} a_j \prod_{i=1}^{l} y_i^{\lambda_{ij}}\Big) \prod_{i=1}^{l} y_i^{-\lambda_i},$$

$$G_n(y_1, \dots, y_l) \neq \text{const.} \quad (n = 1, 2). \tag{6}$$

$G(y_1, \dots, y_l)$ contains the terms $a_j y_j^D \prod_{i=1}^{l} y_i^{-\lambda_i}$ $(1 \leqslant j \leqslant r)$; therefore treated as a polynomial in $y_2, \dots, y_l$, it has at least r terms. If it had a non-constant factor depending only on y_1 then treated as a polynomial in $y_1, \dots, y_l$ it would have at least $2r$ terms. This contradicts the assumption $r+1 > (k+3)/2$, thus G has no non-constant factor depending only on y_1 and in particular neither G_n depends only on y_1. It follows that for at least one $j > 1$ we have $\sum_{i=2}^{l} \lambda_{ij} \neq D$. Otherwise by the substitution $y_j = y_2 z_j$ $(j > 2)$ we would get

$$\begin{aligned} &JG(y_1, y_2, y_2z_3, \dots, y_2z_l) \\ &= \Big((a_0 + a_1 y_1^D) + y_2^D \sum_{j=2}^{k} a_j y_1^{\lambda_{1j}} \prod_{i=3}^{l} z_i^{\lambda_{ij}}\Big) \cdot y_1^{-\lambda_1} \prod_{i=3}^{l} z_i^{-\lambda_i} \\ &= JG_1(y_1, y_2, y_2z_3, \dots, y_2z_l) \cdot JG_2(y_1, y_2, y_2z_3, \dots, y_2z_l). \end{aligned}$$

$JG(y_1, y_2, y_2z_3, \dots, y_2z_l)$ again has no factor depending only on y_1, hence the polynomials

$$(a_0 + a_1 y_1^D) y_1^{-\lambda_1} \prod_{i=3}^{l} z_i^{-\lambda_i}$$

and

$$\Big(\sum_{j=2}^{k} a_j y_1^{\lambda_{1j}} \prod_{i=3}^{l} z_i^{\lambda_{ij}}\Big) y_1^{-\lambda_1} \prod_{i=3}^{l} z_i^{-\lambda_i}$$

are relatively prime.

Since $a_0 + a_1 y_1^D$ is not a constant multiple of a power, by Capelli's theorem $JG(y_1, y_2, y_2 z_3, \ldots, y_2 z_l)$ is irreducible and, for some n, $JG_n(y_1, y_2, y_2 z_3, \ldots, y_2 z_l)$ is constant, contrary to (6).

Thus for some $\sigma > 1$

$$\sum_{i=2}^{l} \lambda_{i\sigma} \neq D \tag{7}$$

and by (5) it follows $k \geqslant \sigma > r$.

Since $r + 1 > (k+3)/2$ we get $r \geqslant 3$.

We consider two cases:

(i) there exist distinct indices $p > 0$ and $q > 0$ such that

$$\lambda_{ip} = \lambda_{iq} \quad \text{for all} \quad i > 1,$$

(ii) for any two distinct indices $p > 0$ and $q > 0$ and a suitable $i > 1$,

$$\lambda_{ip} \neq \lambda_{iq}.$$

Case (i). Divide the indices $j \leqslant k$ into classes assigning two indices j_1, j_2 to the same class C_s if $\lambda_{ij_1} = \lambda_{ij_2} = \mu_{is}$ for all $i > 1$. Let C_0 be the class characterized by $\mu_{i0} = 0$ for all $i > 1$, C_s $(1 \leqslant s < r)$ be the class characterized by $\mu_{is} = D$ for $i = s+1$, $\mu_{is} = 0$ for all $i > 1$, $i \neq s+1$, $C_r, \ldots, C_t$ be all the other classes and let

$$A_s(y_1) = \sum_{j \in C_s} a_j y_1^{\lambda_{1j}} \quad (0 \leqslant s \leqslant t).$$

By the assumption (i) we have either $|C_0| \geqslant 3$ or $|C_s| \geqslant 2$ for some $s > 0$, thus $t + 2 \leqslant k$, $t + 3 \leqslant k + 1 < 2r$. The vectors $[1, \mu_{2s}, \ldots, \mu_{ls}]$ $(0 \leqslant s < r)$ are linearly independent, thus the rank of the matrix

$$\begin{pmatrix} 1 & \ldots & 1 \\ \mu_{20} & \ldots & \mu_{2t} \\ \ldots & \ldots & \ldots \\ \mu_{l0} & \ldots & \mu_{lt} \end{pmatrix}$$

is at least r. Since the vectors $[\lambda_{1j}, \ldots, \lambda_{lj}]$ $(0 \leqslant j \leqslant k)$ are all different, $A_s(y_1)$ are all non-zero. We now apply the inductive assumption to the polynomial

$$\Big(\sum_{s=0}^{t} A_s(y_1) \prod_{i=2}^{l} y_i^{\mu_{is}}\Big) \prod_{i=2}^{l} y_i^{-\min_s \mu_{is}} = G(y_1, \ldots, y_l) y_1^{\lambda_1}$$

in $l-1$ variables over the field $K(y_1)$. It follows that in any factorization of $G(y_1, \ldots, y_l)$ one of the factors depends only on y_1 which contradicts (6).

Case (ii). Make the substitution

$$y_1 = \left(\frac{-a_0}{a_1}\right)^{1/D} = \eta.$$

Then

$$(8)\quad G(\eta, y_2, \dots, y_l) = \left(\sum_{j=2}^{k} a_j \eta^{\lambda_{1j}} \prod_{i=2}^{l} y_1^{\lambda_{1j}}\right)\eta^{-\lambda_1} \prod_{i=2}^{l} y_i^{-\lambda_i} = G_1(\eta, y_2, \dots, y_l)G_2(\eta, y_2, \dots, y_l).$$

Since $r \geqslant 3$ and for $i > 1$

$$\lambda_{i0} = \lambda_{i1} = 0 = \begin{cases} \lambda_{ir} & \text{if } i \neq r, \\ \lambda_{i,r-1} & \text{if } i = r \end{cases}$$

we have

$$\lambda_i = \min_{2 \leqslant j \leqslant k} \lambda_{ij} \quad (i > 1).$$

On the other hand, for σ satisfying (7) the vectors $[1, \lambda_{2j}, \dots, \lambda_{lj}]$ $(2 \leqslant j \leqslant r)$ and $[1, \lambda_{2\sigma}, \dots, \lambda_{l\sigma}]$ are linearly independent; thus the rank of the matrix

$$\begin{pmatrix} 1 & \dots & 1 \\ \lambda_{22} & \dots & \lambda_{2k} \\ \dots & \dots & \dots \\ \lambda_{l2} & \dots & \lambda_{lk} \end{pmatrix}$$

is at least r. Moreover by (ii) the vectors $[\lambda_{2j}, \dots, \lambda_{lj}]$ $(2 \leqslant j \leqslant k)$ are all distinct, hence there is no cancellation on the right hand side of (8) and the degree of $G(\eta, y_2, \dots, y_l)$ is equal to that of $G(y_1, \dots, y_l)$.

It follows that the degree of $G_n(\eta, y_2, \dots, y_l)$ in $y_2, \dots, y_l$ is equal to that of $G_n(y_1, \dots, y_l)$ and therefore is positive. On the other hand, it follows by the inductive assumption applied to $G(\eta, y_2, \dots, y_l)$ over the field $K(\eta)$ that $G(\eta, y_2, \dots, y_l)$ is irreducible. The obtained contradiction completes the proof. □

Proof of the Corollary. Divide all the nonnegative indices $j \leqslant k$ into classes assigning
c two indices j_1, j_2 to the same class C_s if $\nu_{ij_1} = \nu_{ij_2} = \mu_{is}$ for all $i \leqslant l$ (we set $\mu_{i0} = 0$). Let $n + 1$ be the number of classes and let us put

$$b_s = \sum_{j \in C_s} a_j \quad (0 \leqslant s \leqslant n).$$

We can number the classes in such a way that $b_s \neq 0$ for all $s \leqslant m$, $b_s = 0$ for all $s > m$. For all $s > m$ we have then $|C_s| \geqslant 2$, thus $k \geqslant m + 2(n - m)$. Now

$$J\left(a_0 + \sum_{j=1}^{k} a_j \prod_{i=1}^{l} x_i^{\nu_{ij}}\right) = \left(\sum_{s=0}^{m} b_s \prod_{i=1}^{l} x_i^{\mu_{is}}\right) \prod_{i=1}^{l} x_i^{-\min_s \mu_{is}}.$$

The corollary follows from Theorem 1 in virtue of the inequality

$$\operatorname{rank}\begin{pmatrix} 1 & \dots & 1 \\ \mu_{10} & \dots & \mu_{1m} \\ \dots & \dots & \dots \\ \mu_{l0} & \dots & \mu_{lm} \end{pmatrix} \geqslant \operatorname{rank}\big[v_{ij}\big] + 1 - (n-m) \geqslant \frac{k+3}{2} - (n-m) \geqslant \frac{m+3}{2}. \quad \square$$

Proof of Theorem 2. Set in Theorem 2 of [1] $F(x_1, \dots, x_k) = a_0 + \sum_{j=1}^{k} a_j x_j$. If $a_0 + \sum_{j=1}^{k} a_j x^{n_j}$ has more than one or multiple irreducible (over $\mathbb{Q}$) non-reciprocal factor then we infer from the said theorem the existence of an integral matrix $(v_{ij})_{i \leqslant r,\, j \leqslant k} = N$ of rank r and of an integral vector $\boldsymbol{v}$ such that $\max_{i,j} |v_{ij}| \leqslant c_r$,

$$[n_1, \dots, n_k] = \boldsymbol{v} N, \tag{9}$$

$$J\Big(a_0 + \sum_{j=1}^{k} a_j \prod_{i=1}^{r} x_i^{v_{ij}}\Big) \text{ is reducible.} \tag{10}$$

Moreover

$$c_r = \begin{cases} \exp 9k2^{A-5} & \text{if } r = k, \\ \exp(5 \cdot 2^{A^2-4} + 2A \log 2) & \text{if } r + k = 3, \\ \exp_{(k-r)(k+r-3)}(8k2^{A-1} \log A) & \text{otherwise,} \end{cases}$$

where $A = \sum_{j=0}^{k} a_j^2$.

By Corollary to Theorem 1 it follows from (10) that $r \leqslant (k+1)/2$. Using Cramer's formulae and Hadamard's inequality we can find linearly independent integral vectors $\overline{\boldsymbol{\gamma}}_i = [\gamma_{i1}, \dots, \gamma_{ik}]$ $(1 \leqslant i \leqslant k-r)$ such that $\max_{i,j} |\gamma_{ij}| \leqslant r^{r/2} c_r^r$ and

$$\overline{\boldsymbol{\gamma}}_i N = 0 \quad (1 \leqslant i \leqslant k-r). \tag{11}$$

If $k + r = 3$, we have $k = 2$, $r = 1$;

$$\max_{i,j} |\gamma_{ij}| \leqslant c_1 \leqslant \exp_2 A^2 < \exp_4 A.$$

If $k + r > 3$ we use the inequalities valid for $x \geqslant 4$

$$r^{r/2} x^r \leqslant 2(x/2)^{2^r} < \exp_r x, \quad kx \leqslant 2(x/2)^{2^{k-1}} < \exp_{k-1} x$$

and obtain

$$\begin{aligned} \max_{i,j} |\gamma_{ij}| &\leqslant \exp_r c_r = \exp_{(k-r)(k+r-3)+r}(8k2^{A-1} \log A) \\ &\leqslant \exp_{k^2-3k+4}(k \cdot 2^{A+2} \log A) \leqslant \exp_{k^2-2k+3}(2^{A+2} \log A) < \exp_{k^2} A. \end{aligned}$$

By (9) and (11) we have

$$\sum_{j=1}^{k} n_j \gamma_{ij} = 0 \quad (1 \leqslant i \leqslant k-r)$$

and since $k - r \geqslant [k/2]$ the proof is complete. □

In order to show that Theorems 1 and 2 are best possible in the sense made precise in the introduction, consider the polynomial

$$F_0(x_1, \ldots, x_l) = 4 + 2\sum_{j=1}^{l} x_j + \sum_{j=l+1}^{2l-1} x_{j-l}x_l = (2 + x_l)\Big(2 + \sum_{i=1}^{l-1} x_i\Big).$$

It has $k + 1 = 2l$ terms, the rank of the relevant matrix

$$\begin{pmatrix} 1 & 1 \ldots 1 & 1 \ldots 1 \\ 0 & \boxed{I_l} & \boxed{I_{l-1}} \\ 0 & & 1 \ldots 1 \end{pmatrix} \qquad (I_j \text{ the identity matrix of order } j)$$

is $l + 1 = (k + 3)/2$ and $F_0(x_1, \ldots, x_l)$ is reducible. Moreover $F_0(x, x^{2h+1}, \ldots, \ldots, x^{(2h+1)^{l-1}})$ has at least two (counting the multiplicity) irreducible non-reciprocal factors. If

$$\sum_{j=1}^{l} (2h+1)^{j-1}\gamma_j + \sum_{j=l+1}^{2l-1} \{(2h+1)^{j-l-1} + (2h+1)^{l-1}\}\gamma_j = 0, \tag{12}$$

$$\max_{1 \leqslant j \leqslant 2l-1} |\gamma_j| \leqslant h \tag{13}$$

then

$$\sum_{j=1}^{l-1} (2h+1)^{j-1}(\gamma_j + \gamma_{l+j}) + (2h+1)^{l-1}\sum_{j=l}^{2l-1} \gamma_j = 0.$$

Let $(2h+1)^{m-1}$ be the highest power of $2h+1$ occurring in the above equation with the non-vanishing coefficient. We get

$$(2h+1)^{m-1} \leqslant \sum_{j=1}^{m-1} (2h+1)^{j-1}|\gamma_j + \gamma_{l+j}| \leqslant \sum_{j=1}^{m-1} (2h+1)^{j-1} \cdot 2h = (2h+1)^{m-1} - 1$$

which is impossible. Thus all the coefficients of $(2h+1)^{j-1}$ $(1 \leqslant j \leqslant l)$ vanish and

$$\gamma_{l+j} = -\gamma_j \quad (1 \leqslant j < l), \qquad \sum_{j=1}^{l} \gamma_j = \gamma_l,$$

$$[\gamma_1, \ldots, \gamma_{2l-1}] = \sum_{j=1}^{l-1} \gamma_j \big[\underbrace{0, \ldots, 0, 1}_{j}, \overbrace{\underbrace{0, \ldots, 0, 1}_{l}}^{l-j}, 0, \ldots, 0, -1, 0, \ldots, 0\big]$$

which shows that there are at most $l - 1$ linearly independent vectors $[\gamma_1, \ldots, \gamma_{2l-1}]$ satisfying (12) and (13).

Reference

[1] A. Schinzel, *Reducibility of lacunary polynomials* I. Acta Arith. 16 (1969), 123–159; *Corrigenda*: Acta Arith. 19 (1971), 201; ibid. 24 (1978), 265; this collection: D4, 344–380.

Originally published in
Transcendence Theory: Advances and Applications
Academic Press, London 1977
Chapter XIII, 195–203

Some arithmetic properties of polynomials in several variables

with H. L. Montgomery (Ann Arbor)*

1. Statement of results

In this paper we formulate certain properties of a polynomial $F(\boldsymbol{z}) \in \mathbb{Z}[z_1, \dots, z_N]$ in terms of similar properties of the polynomials

$$P_{\boldsymbol{r}}(z) = F(z^{r_1}, \dots, z^{r_N}), \tag{1}$$

$P_{\boldsymbol{r}} \in \mathbb{Z}[z]$, $\boldsymbol{r} > \boldsymbol{0}$. (We say $\boldsymbol{v} > \boldsymbol{0}$ if all coordinates of the vector $\boldsymbol{v}$ are positive.) In this manner we obtain information concerning the zero set of F, and also concerning zeros of certain generalized Dirichlet polynomials. In particular we generalize to N variables the following classical theorem of Kronecker [4]:

Theorem A. *Let $P(z)$ be a monic irreducible polynomial with integral coefficients. If all zeros of P lie in the disc $|z| \leqslant 1$, then P is a cyclotomic polynomial, or $P(z) \equiv z$.*

We write

$$F(\boldsymbol{z}) = F(z_1, \dots, z_N) = \sum_{\boldsymbol{j} \in \mathscr{J}} a(\boldsymbol{j}) z_1^{j_1} \cdots z_N^{j_N},$$

where $\boldsymbol{j} = (j_1, \dots, j_N)$, the j_n are non-negative integers, and $\mathscr{J}$ is a finite set such that $a(\boldsymbol{j}) \neq 0$ for $\boldsymbol{j} \in \mathscr{J}$. We let $\mathscr{J} - \mathscr{J} = \{\boldsymbol{j}_1 - \boldsymbol{j}_2 : \boldsymbol{j}_i \in \mathscr{J}\}$, $J = |\mathscr{J}|$, $D = \max\limits_{\boldsymbol{j} \in \mathscr{J}} \max\limits_{1 \leqslant n \leqslant N} j_n$. We let Φ_m denote the cyclotomic polynomial of degree $\phi(m)$ whose roots are the primitive mth roots of unity, and we say that F is a generalized cyclotomic polynomial if $F(\boldsymbol{z}) = \pm \Phi_m(z_1^{v_1} \cdots z_N^{v_N})$ for some set of non-negative integers v_n, not all zero.

As a special case of a conjecture of Schinzel [6], we have

* Work supported in part by the Alfred P. Sloan Foundation, and by National Science Foundation Grant MPS 7507948.

Theorem 1. *Let $F(\boldsymbol{z}) \in \mathbb{Z}[z_1, \ldots, z_N]$ be irreducible and not generalized cyclotomic. If the polynomial $P_{\boldsymbol{r}}$ given by* (1) *with $\boldsymbol{r} > \boldsymbol{0}$ is a product of cyclotomic polynomials then $\boldsymbol{v} \cdot \boldsymbol{r} = 0$ for some vector $\boldsymbol{v} \in \mathbb{Z}^N$, $\boldsymbol{v} \neq \boldsymbol{0}$, such that $|v_n| \leqslant C_0(F) \leqslant e^{3J} D$ for $1 \leqslant n \leqslant N$.*

For large J we find that $C_0(F) \leqslant e^{J+o(J)} D$.

Corollary 1. *Let F be as in Theorem* 1*, and suppose that $F(\boldsymbol{0}) = 1$. Then F has a zero $\boldsymbol{z}$ for which*

$$|z_n| \leqslant 1 - 1/C_1(N, J, D).$$

It would be interesting to know whether one can replace C_1 above by a constant depending only on the total degree of F.

Corollary 2. *Let $F(\boldsymbol{z}) \in \mathbb{Z}[z_1, \ldots, z_N]$. Then F is a product of generalized cyclotomic polynomials if and only if $\pm P_{\boldsymbol{r}}$ is a product of cyclotomic polynomials for all $\boldsymbol{r} > \boldsymbol{0}$.*

Let $\mathbb{U}^N = \{\boldsymbol{z} \in \mathbb{C}^N : |z_n| < 1\}$. Concerning zeros in the polydisc $\mathbb{U}^N$ we prove

Theorem 2. *Let $F(\boldsymbol{z}) \in \mathbb{Z}[z_1, \ldots, z_N]$, $F(\boldsymbol{0}) = 1$, and suppose that $F(\boldsymbol{z}) \neq 0$ for $\boldsymbol{z} \in \mathbb{U}^N$. Then F is a product of generalized cyclotomic polynomials.*

Of course the converse of the above is trivial: A generalized cyclotomic polynomial is non-vanishing in $\mathbb{U}^N$. Theorem A is the case $N = 1$ of the above, with $F(z_1)$ replaced by $z_1^D F(1/z_1)$. We derive Theorem 2 easily from Corollary 2 and Theorem A. However, by using the following theorem, which pertains to the more general $F \in \mathbb{C}[z_1, \ldots, z_N]$, we find that Corollary 2 can be derived from Theorem 2.

Theorem 3. *If $F \in \mathbb{C}[z_1, \ldots, z_N]$, and F has a zero in $\mathbb{U}^N$, then there are positive integers $r_1, \ldots, r_N$ such that $P_{\boldsymbol{r}}(z) = F(z^{r_1}, \ldots, z^{r_N})$ has a zero in $\mathbb{U}$.*

It is not possible to strengthen the above in the same way that Theorem 1 strengthens Corollary 2, as we see from the example $F(\boldsymbol{z}) = z_1 - 2z_2$.

We apply Theorem 2 to a question of Deutsch [3] concerning generalized Dirichlet polynomials. In this connection we require some new information concerning zeros of a generalized Dirichlet polynomial $D(s)$. Following Bohr [2] we may write a generalized Dirichlet polynomial $D(s)$ in the form

$$D(s) = F(e^{-\mu_1 s}, \ldots, e^{-\mu_N s}),$$

where $F \in \mathbb{C}[z_1, \ldots, z_N]$, and the μ_n are positive real numbers which are linearly independent over $\mathbb{Q}$. We define the sets

$$\begin{aligned} U &= \{D(it) : t \in \mathbb{R}\}, \\ V &= \{F(\boldsymbol{z}) : |z_n| = 1\}, \\ W &= \bigcap_{\delta > 0} \{D(s) : |\operatorname{Re} s| < \delta\}, \\ X &= \{D(s) : 0 < \operatorname{Re} s \leqslant \infty\}, \\ Y &= \{F(\boldsymbol{z}) : \boldsymbol{z} \in \mathbb{U}^N\}. \end{aligned}$$

Bohr demonstrated that U is dense in W, and that

$$U \subset W = V. \tag{2}$$

To this we add

Theorem 4. *In the above notation, $X = Y$.*

From Theorem 2 and Theorem 4 we obtain an answer to the question which stimulated this work, namely

Theorem 5. *Let*

$$D(s) = 1 + \sum_{j=1}^{J} a_j e^{-\lambda_j s}, \tag{3}$$

where $a_j \in \mathbb{Z}$, $a_J \neq 0$, and $\lambda_j > 0$. Then $D(s)$ has zeros in the half-plane $\operatorname{Re} s \geqslant 0$. If $D(s) \neq 0$ for $\operatorname{Re} s > 0$ then

$$D(s) = \pm \prod_{k=1}^{K} \Phi_{m_k}(e^{-\nu_k s}) \tag{4}$$

for suitable positive $m_k \in \mathbb{Z}$, and positive $\nu_k \in \mathbb{R}$.

We note that conversely if $D(s)$ is of the form (4), then $D(s) \neq 0$ for $\operatorname{Re} s > 0$. We obtain Theorem A again by taking $\lambda_j = j$, $1 \leqslant j \leqslant J$. From the hypotheses of Theorem 5, Deutsch [3] deduced the weaker result that $D(s)$ must vanish in the half-plane $\operatorname{Re} s > -\varepsilon$, for any $\varepsilon > 0$.

The authors express their appreciation to Professors B. J. Birch, A. Selberg, B. A. Taylor, and H. Tornehave, whose comments and suggestions contributed to the form and content of this paper.

2. Proof of Theorem 1

We shall require:

Lemma 1. *Let $F(z) = \sum_{j \in \mathscr{J}} a_j z^j \in \mathbb{C}[z]$, and suppose that F has a zero $c \neq 0$ of multiplicity $\geqslant J = |\mathscr{J}|$. Then $F \equiv 0$.*

Proof. Let $c \neq 0$, and suppose that $F^{(i)}(c) = 0, 0 \leqslant i \leqslant J-1$. The a_j thus satisfy J linear equations with coefficient matrix $C = \left(\binom{j}{i} i! c^{j-i}\right)$, $0 \leqslant i \leqslant J-1$, $j \in \mathscr{J}$. After factoring out powers of c we have a matrix which is row equivalent to (j^i); thus C is non-singular and hence the a_j vanish. □

We quote from Mann [5, Theorem 1] the following

Lemma 2. *Let $a_1, \dots, a_R$ be distinct non-zero integers, let q be an integer, and suppose that $(a_1, \dots, a_R, q) = 1$. Put $a_0 = 0$. Let b_r, $0 \leqslant r \leqslant R$, be non-zero integers. Suppose that*

$$\sum_{r=0}^{R} b_r e(a_r/q) = 0,$$

and that no sub-sum of this sum vanishes. Then q is square-free, and is composed entirely of primes $p \leqslant R + 1$.

Here $e(\theta) = e^{2\pi i\theta}$. We now come to the main step in the proof of Theorem 1.

Lemma 3. *Suppose $\Phi_m(z) \mid P_{\boldsymbol{r}}(z)$, where $P_{\boldsymbol{r}}(z)$ is given by* (1) *with F belonging to $\mathbb{Z}[z_1, \dots, z_N]$, $F(\mathbf{0}) \neq 0$, F is irreducible and not a constant multiple of a generalized cyclotomic polynomial. Then there are linearly independent vectors $\boldsymbol{v}^{(i)} \in \mathscr{J} - \mathscr{J}$, $i = 1, 2$, for which $m \mid \big(\boldsymbol{v}^{(1)} \cdot \boldsymbol{r}, \boldsymbol{v}^{(2)} \cdot \boldsymbol{r}\big)P$, where $P = \prod_{p \leqslant J} p$.*

If $N = 1$ then the conclusion above is clearly impossible; the lemma remains valid by virtue of the fact that in this case the hypotheses are never fulfilled. To see this, note that if F is irreducible and F is not of the form $c\Phi_k(z^v)$ then none of the roots of F are roots of unity. Hence none of the roots of $P_r(z) = F(z^r)$ are roots of unity, and so $\Phi_m(z) \nmid P_r(z)$. In the proof below, we may assume that $N > 1$, although strictly speaking the proof is vacuously correct when $N = 1$.

Proof. By hypothesis $e(1/m)$ is the root of $P_{\boldsymbol{r}}$; that is,

$$\sum_{\boldsymbol{j} \in \mathscr{J}} a(\boldsymbol{j}) e(\boldsymbol{j} \cdot \boldsymbol{r}/m) = 0.$$

We may partition $\mathscr{J}$ into subsets $\mathscr{J}_i$, $1 \leqslant i \leqslant I$, such that

$$\sum_{\boldsymbol{j} \in \mathscr{J}_i} a(\boldsymbol{j}) e(\boldsymbol{j} \cdot \boldsymbol{r}/m) = 0, \tag{5}$$

and so that no sub-sum of these vanish. Let $\boldsymbol{h}^{(i)} \in \mathscr{J}_i$ be chosen so that $\sum_{n=1}^{N} h_n^{(i)}$ is minimal. From (5) we have

$$\sum_{\boldsymbol{j} \in \mathscr{J}_i} a(\boldsymbol{j}) e\big((\boldsymbol{j} - \boldsymbol{h}^{(i)}) \cdot \boldsymbol{r}/m\big) = 0. \tag{6}$$

Let g_i be the greatest common divisor of the numbers $(\boldsymbol{j} - \boldsymbol{h}^{(i)}) \cdot \boldsymbol{r}$ for $\boldsymbol{j} \in \mathscr{J}_i$. Then by Lemma 2 with $q = m/(g_i, m)$, $R < J$, we find that $m \mid (g_i, m)P$. As this is true for all i, we deduce that

$$m \mid gP, \tag{7}$$

where $g = (g_1, \dots, g_I)$, $P = \prod_{p \leqslant J} p$.

We show that the set $\mathscr{W} = \bigcup_{i=1}^{I} \{\boldsymbol{v} = \boldsymbol{j} - \boldsymbol{h}^{(i)} : \boldsymbol{j} \in \mathscr{J}_i\}$ contains a pair of linearly independent vectors. This suffices, for if $\boldsymbol{v}^{(1)}$, $\boldsymbol{v}^{(2)}$ are linearly independent members of $\mathscr{W} = \mathscr{J} - \mathscr{J}$ then $g \mid \big(\boldsymbol{v}^{(1)} \cdot \boldsymbol{r}, \boldsymbol{v}^{(2)} \cdot \boldsymbol{r}\big)$, and we obtain the desired result from (7). Suppose, to the contrary, that all members of $\mathscr{W}$ lie on a line through the origin. Then there is a $\boldsymbol{v} \in \mathbb{Z}^N$ and integers $b(\boldsymbol{j})$ such that $\boldsymbol{j} - \boldsymbol{h}^{(i)} = b(\boldsymbol{j})\boldsymbol{v}$ for all $\boldsymbol{j} \in \mathscr{J}$. Then

$$F(\boldsymbol{z}) = \sum_{i=1}^{I} z_1^{h_1^{(i)}} \cdots z_N^{h_N^{(i)}} \sum_{\boldsymbol{j} \in \mathscr{J}_i} a(\boldsymbol{j}) \big(z_1^{v_1} \cdots z_N^{v_N}\big)^{b(\boldsymbol{j})}. \tag{8}$$

But from (6) we see that

$$\sum_{\boldsymbol{j} \in \mathscr{J}_i} a(\boldsymbol{j}) e\big(b(\boldsymbol{j})\boldsymbol{v} \cdot \boldsymbol{r}/m\big) = 0,$$

so that if $l = m/(m, \boldsymbol{r} \cdot \boldsymbol{v})$ then

$$\Phi_l(z) \Big| \sum_{\boldsymbol{j} \in \mathscr{J}_i} a(\boldsymbol{j}) z^{b(\boldsymbol{j})}. \tag{9}$$

From (8) we thus find that $F(\boldsymbol{z}) = 0$ if $z_1^{v_1} \cdots z_N^{v_N} = e(1/l)$. If the v_n take on both signs then there are $\boldsymbol{z}$ with the above property for which $|z_n| < \varepsilon$, $1 \leqslant n \leqslant N$. Then by continuity $F(\boldsymbol{0}) = 0$, contrary to the hypothesis. Hence the non-zero v_n all have the same sign; by multiplying $\boldsymbol{v}$ and all the $b(\boldsymbol{j})$ by -1 if necessary we may suppose that the v_n are non-negative. From the way that $\boldsymbol{h}^{(i)}$ was chosen we see that $\boldsymbol{j} - \boldsymbol{h}^{(i)}$ has at least one positive coordinate. Hence $b(\boldsymbol{j}) \geqslant 0$ for all $\boldsymbol{j} \in \mathscr{J}$. From (8) and (9) we see that $\Phi_l(z_1^{v_1} \cdots z_N^{v_N}) \mid F(\boldsymbol{z})$. This contradicts the hypothesis that F is irreducible and not a constant multiple of a generalized cyclotomic polynomial; hence $\mathscr{W}$ contains a pair of linearly independent vectors. □

We now prove Theorem 1. When $F(\boldsymbol{0}) \neq \pm 1$ we have nothing to prove, for then $P_{\boldsymbol{r}}(0) \neq \pm 1$ and hence $P_{\boldsymbol{r}}$ is never a product of cyclotomic polynomials. Thus we assume that $F(\boldsymbol{0}) = \pm 1$. Suppose that

$$P_{\boldsymbol{r}}(z) = \prod_{m \in \mathscr{M}} \Phi_m(z)^{\gamma(m)}, \tag{10}$$

where the $\gamma(m)$ are positive integers. If $P_{\boldsymbol{r}}$ has fewer than J terms then $\boldsymbol{j}^{(1)} \cdot \boldsymbol{r} = \boldsymbol{j}^{(2)} \cdot \boldsymbol{r}$ for some $\boldsymbol{j}^{(i)} \in \mathscr{J}$, and it suffices to take $\boldsymbol{v} = \boldsymbol{j}^{(1)} - \boldsymbol{j}^{(2)}$. If $P_{\boldsymbol{r}}$ has J distinct terms then the degree of $P_{\boldsymbol{r}}$ is given by $\Delta = \max_{\boldsymbol{j} \in \mathscr{J}} \boldsymbol{j} \cdot \boldsymbol{r}$. On the other hand, from (10) and Lemma 1 we see that

$$\Delta = \sum_{m \in \mathscr{M}} \gamma(m)\phi(m) < J \sum_{m \in \mathscr{M}} \phi(m).$$

Let $\mathscr{V} = \big\{(\boldsymbol{u}, \boldsymbol{w}) : \boldsymbol{u}, \boldsymbol{w} \in \mathscr{J} - \mathscr{J},\ \operatorname{rank}(\boldsymbol{u}, \boldsymbol{w}) = 2\big\}$. Then by Lemma 3,

$$\Delta < J \sum_{(\boldsymbol{u}, \boldsymbol{w}) \in \mathscr{V}} \sum_{m \mid (\boldsymbol{u} \cdot \boldsymbol{r}, \boldsymbol{w} \cdot \boldsymbol{r}) P} \phi(m) = PJ \sum_{(\boldsymbol{u}, \boldsymbol{w}) \in \mathscr{V}} (\boldsymbol{u} \cdot \boldsymbol{r}, \boldsymbol{w} \cdot \boldsymbol{r}).$$

But $\mathscr{V}$ contains less than J^2 elements, so there is a pair $(\boldsymbol{u}, \boldsymbol{w}) \in \mathscr{V}$ for which $d = (\boldsymbol{u}\cdot\boldsymbol{r}, \boldsymbol{w}\cdot\boldsymbol{r}) > \Delta P^{-1}J^{-3}$. Put $u = \boldsymbol{u}\cdot\boldsymbol{r}/d$, $w = \boldsymbol{w}\cdot\boldsymbol{r}/d$. Then

$$|u| \leqslant PJ^3|\boldsymbol{u}\cdot\boldsymbol{r}|/\Delta \leqslant PJ^3,$$

and similarly $|w| \leqslant PJ^3$. Put $\boldsymbol{v} = w\boldsymbol{u} - u\boldsymbol{w}$. Then $\boldsymbol{v}\cdot\boldsymbol{r} = 0$, $\boldsymbol{v} \neq \boldsymbol{0}$, and $|v_n| \leqslant 2PJ^3D < e^{3J}D$. □

Proof of Corollary 1. Take $r_n = \big(C_0(F)+1\big)^{n-1}$, so that by Theorem 1, $P_{\boldsymbol{r}}$ is not the product of cyclotomic polynomials. Then by Theorem 1 of Blanksby–Montgomery [1], $P_{\boldsymbol{r}}$ has a zero z for which $|z| < 1 - 1/C(\deg P_{\boldsymbol{r}})$. Then $|z_n| = |z^{r_n}| \leqslant 1 - 1/C(N, J, D)$.□

3. Proof of Theorem 2

From the hypotheses of Theorem 2 we see that $P_{\boldsymbol{r}}(z) \in \mathbb{Z}[z]$, and $P_{\boldsymbol{r}}(z) \neq 0$ for $z \in \mathbb{U}$. Then by Theorem A applied to $P(z) = z^d P_{\boldsymbol{r}}(1/z)$ we find that P, and hence also $\pm P_{\boldsymbol{r}}$, is a product of cyclotomic polynomials. Thus, by Corollary 2, F is a product of generalized cyclotomic polynomials. □

4. Proof of Theorem 3

We shall require:

Lemma 4. *Let $F \in \mathbb{C}[z_1, \ldots, z_N]$, and let μ_n, $1 \leqslant n \leqslant N$, be positive real numbers. Then*

$$\big\{F(\boldsymbol{z}) : \boldsymbol{z} \in \mathbb{U}^N\big\} = \bigcup_{0<a\leqslant\infty} \big\{F(\boldsymbol{z}) : \forall n\ |z_n| = e^{-\mu_n a}\big\}.$$

Proof. The set on the right is clearly contained in the one on the left, so we establish the reverse inclusion. Since the constant term of F is arbitrary, it suffices to consider zeros of F. Suppose F has a zero in $\mathbb{U}^N$. For $a > 0$ let $m(a) = \min|F(\boldsymbol{z})|$ over $\boldsymbol{z}$ satisfying $|z_n| \leqslant e^{-\mu_n a}$ for $1 \leqslant n \leqslant N$. Put $a_0 = \inf_{m(a)>0} a$. Then $0 < a_0 \leqslant \infty$. If $a_0 = \infty$ then $F(\boldsymbol{0}) = 0$, and we are done. Suppose that $0 < a_0 < \infty$. For $a_0 < a < \infty$ let $\boldsymbol{z}(a)$ be chosen so that $\big|F\big(\boldsymbol{z}(a)\big)\big| = m(a)$, $|z_n(a)| \leqslant e^{-\mu_n a}$. By the minimum modulus theorem, $|z_n(a)| = e^{-\mu_n a}$. Let $\boldsymbol{c}$ be a limit point of the sequence $\boldsymbol{z}(a_0 + 1/k)$. Then $|c_n| = e^{-\mu_n a_0}$, and $|F(\boldsymbol{c})| = \lim_k m(a_0 + 1/k) = 0$. Hence $F(\boldsymbol{c}) = 0$, and the proof is complete. □

We now prove Theorem 3. By Lemma 4 with $\mu_1 = \ldots = \mu_N = 1$, we see that $F(\boldsymbol{z})$ has a zero $\boldsymbol{c}$ with $|c_1| = \ldots = |c_N| < 1$. Thus for suitable unimodular $\gamma_n = e(\theta_n)$ the function $G(z) = F(\gamma_1 z, \ldots, \gamma_N z)$ has a zero c, $0 \leqslant c < 1$. Choose ϕ, ρ, $\rho < 1$, and
c $m > 0$ so that the semidisc $\mathscr{S} = \{z : \operatorname{Re} ze(\frac{1}{4} - \phi) \geqslant 0,\ |z| \leqslant \rho\}$ contains c, and so that $|G(z)| \geqslant m$ for z on the boundary of $\mathscr{S}$. This may be done, unless $G(0) = 0$, in which case there is nothing to do (since then $P_{\boldsymbol{r}}(0) = 0$ for any $\boldsymbol{r}$). Let $\delta > 0$ be so small that if
c $z \in \mathscr{S}$, $|z_n - \gamma_n z| < \delta$, $1 \leqslant n \leqslant N$, then $|F(\boldsymbol{z}) - G(z)| \leqslant m/2$.

Since $\sqrt{2}$ is irrational, we may determine a positive integer b_n such that $\|b_n\sqrt{2} - \theta_n\| < \delta/20$. We now put $r_n = q + b_n$, and show that for all large q the polynomial $P_{\boldsymbol{r}}$ has a zero in $\mathbb{U}$. Let $\varepsilon = (1/q)\{\phi - q\sqrt{2}\}$, and consider the sector $\Sigma_q = \{z = re(\theta) : |\theta - \sqrt{2} - \varepsilon| < 1/(4q),\ 0 \leqslant r \leqslant \rho^{1/q}\}$. If q is large and $z \in \Sigma_q$, then $|z^{r_n} - \gamma_n z^q| < \delta$, and $z^q \in \mathscr{S}$. Thus $|P_{\boldsymbol{r}}(z) - G(z^q)| \leqslant m/2$ for $z \in \Sigma_q$. But $G(z^q)$ has a zero in Σ_q, and $|G(z^q)| \geqslant m$ for z on the boundary of Σ_q, since z^q is then on the boundary of $\mathscr{S}$. Hence by Rouché's theorem $P_{\boldsymbol{r}}(z)$ has a zero in $\Sigma_q \subset \mathbb{U}$. □

5. Proof of Theorem 4

From (2) we see that for each $a > 0$,

$$\big\{F(\boldsymbol{z}) : |z_n| = e^{-\mu_n a}\big\} = \bigcap_{\delta>0}\big\{D(s) : |a - \operatorname{Re} s| < \delta\big\}.$$

Taking the union of this over $a > 0$, we find that

$$Y' =: \bigcup_{0<a\leqslant\infty} \big\{F(\boldsymbol{z}) : |z_n| = e^{-\mu_n a}\big\} = X.$$

But by Lemma 4, $Y = Y'$, so we are done. □

6. Proof of Theorem 5

It suffices to prove the last assertion of Theorem 5. For $D(s)$ determined by (3), we may find positive μ_n, linearly independent over $\mathbb{Q}$, and a polynomial $F(\boldsymbol{z}) \in \mathbb{Z}[z_1, \ldots, z_N]$ such that

$$D(s) = F\big(e^{-\mu_1 s}, \ldots, e^{-\mu_N s}\big),$$

$F(\boldsymbol{0}) = 1$. If $D(s) \neq 0$ for $\operatorname{Re} s > 0$ then by Theorem 4, $F(\boldsymbol{z}) \neq 0$ for $\boldsymbol{z} \in \mathbb{U}^N$. Then by Theorem 2,

$$F(\boldsymbol{z}) = \prod_{k=1}^{K} \Phi_{m_k}\big(z_1^{r_{1k}} \cdots z_N^{r_{Nk}}\big).$$

This gives (4), with $\nu_k = \sum_{n=1}^{N} r_{nk}\mu_n$. □

References

[1] P. E. Blanksby, H. L. Montgomery, *Algebraic integers near the unit circle*. Acta Arith. 18 (1971), 355–369.

[2] H. Bohr, *Zur Theorie der allgeimenen Dirichletschen Reihen*. Math. Ann. 79 (1918), 136–156.

[3] C. Deutsch, *Deux remarques sur les séries et les polynômes de Dirichlet*. Ann. Inst. Fourier (Grenoble) 24 (1974), 165–169.

[4] L. Kronecker, *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten*. J. Reine Angew. Math. 53 (1857), 173–175.

[5] H. B. Mann, *On linear relations between roots of unity*. Mathematika 12 (1965), 107–117.

[6] A. Schinzel, *On the reducibility of polynomials and in particular of trinomials*. Acta Arith. 11 (1965), 1–34; *Errata*, ibid., 491; this collection: D2, 301–332.

Originally published in
Journal of Number Theory 12 (1980), 230–235

On difference polynomials and hereditarily irreducible polynomials

with L. A. Rubel (Urbana) and H. Tverberg (Bergen)*

Abstract. A difference polynomial is one of the form $P(x, y) = p(x) - q(y)$. Another proof is given of the fact that every difference polynomial has a connected zero set, and this theorem is applied to give an irreducibility criterion for difference polynomials. Some earlier problems about hereditarily irreducible polynomials (HIPs) are solved. For example, $P(x, y)$ is called a HIP (two-variable case) if $P\big(a(x), b(y)\big)$ is always irreducible, and it is shown that such two-variable HIPs actually exist.

Let k be a field. A difference polynomial over k is a polynomial P in two variables x, y, of the form

$$P(x, y) = p(x) - q(y),$$

where $p(x)$ and $q(y)$ are nonconstant polynomials in one variable. In what follows, $k = \mathbb{C}$, the complex field. In this note, we revisit the paper [1]—we give a different proof of the main theorem, use the theorem to prove an irreducibility criterion, and answer some of the problems raised at the end about hereditarily irreducible polynomials.

Theorem (1). *If $P(x, y)$ is a generalized difference polynomial and if $Q(x, y)$ and $R(x, y)$ are two nonconstant factors of $P(x, y)$, then Q and R have a common zero.*

Note. By "generalized difference polynomial" (g.d.p.), we mean a polynomial of the form

$$P(x, y) = Ay^n + \sum_{i=1}^{n} P_i(x) y^{n-i},$$

where A is a non-zero constant, $n > 0$, and polynomials $P_i(x)$ satisfy

$$\deg P_n(x) = m > 0 \quad \text{and} \quad \deg P_i(x) < mi/n \quad \text{for} \quad 1 \leqslant i < n.$$

Communicated by H. L. Montgomery

* The research of this author was partially supported by a grant from the National Science Foundation.

Note. It was pointed out in [1] that if $P(x, y)$ is a g.d.p., then $P(y, x)$ is a g.d.p. and so is $P\big(a(x), b(y)\big)$ if $a(x)$ and $b(y)$ are nonconstant polynomials in one variable. It is clear that any difference polynomial is a g.d.p.

Corollary (Irreducibility criterion for difference polynomials). *Let $P(x, y) = p(x) - q(y)$ be a difference polynomial and let $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$ be the zeros of the derivatives $p'(x)$ and $q'(y)$, respectively. Consider the $m \times n$ points (α_i, β_j). If for every i, j we have $p(\alpha_i) \neq q(\beta_j)$, then $P(x, y)$ must be irreducible.*

Remark. A much stronger result is given as Theorem 1 of [2], p. 306.

Proof of the corollary. Suppose, to the contrary, that $P(x, y) = Q(x, y)R(x, y)$ were a nontrivial factorization. On taking derivatives, we would have

$$p'(x) = Q_x R + Q R_x; \quad -q'(y) = Q_y R + Q R_y,$$

and if we take $(x, y) = (x_0, y_0)$ as a common zero of Q and R (whose existence is guaranteed by the theorem above), then

$$p'(x_0) = 0 \quad \text{and} \quad q'(y_0) = 0,$$

so that $x_0 = \alpha_i$, $y_0 = \beta_j$ for some i and j, and then $P(x_0, y_0) = P(\alpha_i, \beta_j) = 0$, which contradicts $p(\alpha_i) \neq q(\beta_j)$. □

We turn now to the new proof of the theorem, which uses the (weak) Hilbert Nullstellensatz [4] instead of relying directly on resultants. (There is, of course, a close connection between resultants and the Nullstellensatz as shown, for instance, by the proof of the latter given in [4].)

Proof of the theorem. We want to show that the two factors Q and R have a common zero, so let us proceed by contradiction and suppose that they do not. Writing $P = QRS$ we get

$$P(x^n, y^m) = Q(x^n, y^m)R(x^n, y^m)S(x^n, y^m).$$

By our remark after the definition of g.d.p., we see that $P(x^n, y^m)$ is also a g.d.p. Furthermore $Q(x^n, y^m)$ and $R(x^n, y^m)$ have no common zero. The gist of this is that we may as well assume that $m = n$, i.e., that

$$P(x, y) = Ay^n + Bx^n + L(x, y),$$

where the degree of L is less than n and A and B are both non-zero constants.

Since Q and R have no common zero, we may, by the Nullstellensatz write

$$1 = GQ + HR \quad \text{with} \quad G, H \in \mathbb{C}[x, y].$$

Now consider G and R as polynomials in x alone, with coefficients in $\mathbb{C}(y)$ (rational functions) and put $G = MR + N$ with $\deg_x N < \deg_x R$. The leading coefficient of R is in $\mathbb{C}$, as R divides $Bx^n + \ldots$. The division algorithm then shows that M and N are in $\mathbb{C}[y][x]$ and not merely in $\mathbb{C}(y)[x]$. We now have

$$(MR + N)Q + HR = NQ + (H + MQ)R = 1.$$

In other words, changing notation,

$$GQ + HR = 1 \quad \text{with} \quad \deg_x G < \deg_x R.$$

Now let G^* be the part of G of maximal degree, with similar notation for the other polynomials. We get

$$G^*Q^* + H^*R^* = 0.$$

Now R^* and Q^* have no common factor, as $Ay^n + Bx^n$ has no multiple factor. Thus $R^* \mid G^*$. We now have

$$\deg_x R^* \leqslant \deg_x R \leqslant \deg R = \deg R^* = \deg_x R^*$$

(as R^* divides $Ay^n + Bx^n$, so that R^* is a product of linear homogeneous factors). Hence

$$\deg_x R^* = \deg_x R.$$

Furthermore,

$$\deg_x R = \deg_x R^* \leqslant \deg_x G^* \leqslant \deg_x G < \deg_x R.$$

The first inequality is because $R^* \mid G^*$ and the last inequality is by construction. The resulting inequality $\deg_x R < \deg_x R$ is the contradiction that proves the theorem. □

We now give solutions to Problems 1(a), 5(a), 6(a), 7(n), 10(n), and 15(a) of [1]. (The designation (a) signifies an *affirmative* answer, while (n) signifies a *negative* one.) Some of the solutions now seem embarrassingly simple, but this is hindsight. We recall the next pertinent definition from [1].

Definition. The polynomial $P(x_1, \ldots, x_n)$ is a *hereditarily irreducible polynomial* (HIP) if $P\big(h_1(x_1), \ldots, h_n(x_n)\big)$ is irreducible for every n-tuple $h_1(x_1), \ldots, h_n(x_n)$ of nonconstant one-variable polynomials. Moreover, P is a *basic HIP* if whenever $P(x_1, \ldots, x_n) = Q\big(h_1(x_1), \ldots, h_n(x_n)\big)$ where Q is a HIP, we must have all the h_i affine (i.e., $h_i(x) = \alpha_i x + \beta_i$).

Answer to Problem 1. *We claim that* $(x^2 + 1)y + 1$ *is a HIP that involves only two variables.*

Proof. We suppose that

$$\big(a(x)^2 + 1\big)b(y) + 1$$

is reducible, and reach a contradiction. First, we claim that $h(x) = a(x)^2 + 1$ has at least one simple zero ξ. For if ξ_i is a zero of $h(x)$, of multiplicity n_i, then it is a zero of $h'(x) = 2a(x)a'(x)$ of multiplicity $n_i - 1$, hence of $a'(x)$, as $0 = a(\xi_i)^2 + 1$. Thus if every $n_i \geqslant 2$, we get $\deg h(x) - 2 = 2 \deg a'(x) \geqslant 2 \sum (n_i - 1) \geqslant 2 \sum n_i/2 = \deg h(x)$, which is a contradiction.

So we may choose ξ as a simple root of $h(x)$. We let $p(x) = x - \xi$, and we regard $Q(x, y) = \big(a(x)^2 + 1\big)b(y) + 1$ as a polynomial $A(y)$ in y whose coefficients are polynomials in x, say, $A(y) = a_n y^n + \ldots + a_0$, and we can apply the (reverse) Eisenstein

criterion since $a_0 \not\equiv 0 \bmod p$, $a_i \equiv 0 \bmod p$ for $i = 1, \ldots, n$, and $a_n \not\equiv 0 \bmod p^2$, to conclude that Q is irreducible.

Remark. The same proof shows that if $f(x)$ is any square-free polynomial of degree exceeding 1, then $f(x)y + 1$ is a HIP.

Remark. The question (Problem 2) whether a difference polynomial can be a HIP remains open, and seems hard. Michael Fried has reduced this problem to a question, although a complicated one, in combinatorial group theory.

Answer to Problem 10. *From the penultimate remark,* $k(x, y) = (1 - x^2)y - 1$ *is a HIP, but if we make the substitutions of* $\sin x$ *for* x *and* y^2 *for* y*, we get*

$$k(\sin x, y^2) = (1 - \sin^2 x)y^2 - 1 = y^2 \cos^2 x - 1 = (y \cos x + 1)(y \cos x - 1),$$

so that even though $k(x, y)$ *is a HIP,* $k(\sin x, y^2)$ *is not an irreducible entire function.*

Remark. It would be interesting to find all HIPs $P(x_1, \ldots, x_n)$ so that $P\big(h_1(x_1), \ldots, \ldots, h_n(x_n)\big)$ is always an irreducible entire function whenever the one-variable functions $h_i(x)$ are entire and nonconstant. It is shown in [3] that $x + y + z$ and $xy + xz + yz$ do have this property.

Answer to Problem 5. *If* P *is a HIP, then there does exist a basic HIP* Q *so that*

$$(\gamma) \qquad P(x_1, \ldots, x_n) = Q\big(h_1(x_1), \ldots, h_n(x_n)\big).$$

Proof. Among all systems $(Q; h_1, \ldots, h_n)$ that satisfy (γ) with Q a HIP (and they surely exist since P is itself a HIP), choose one for which the sum $\deg h_1 + \ldots + \deg h_n$ is the greatest. The relevant Q must be a basic HIP. □

Answer to Problem 6. *There can be two really different basis HIPs* Q *that give rise* (*as in* (γ) *above*) *to the same HIP* P.

Example 1. $P = T_6(x)y + 1$, $Q_1 = T_2(x)y + 1$, $Q_2 = T_3(x)y + 1$, where $T_n(x) = \cos(n \arccos x)$. By the remark after the answer to Problem 1, P, Q_1, and Q_2 are all HIPs. Since $T_6(x) = T_3(T_2(x)) = T_2(T_3(x))$ we see that both Q_1 and Q_2 give rise to P.

Example 2. $P = (x^2 + 1)(y^2 + 1) + 1$, $Q_1 = (x^2 + 1)y + 1$, and $Q_2 = x(y^2 + 1) + 1$.

Answer to Problem 7. $P\big(h_1(x_1), \ldots, h_n(x_n)\big)$ *can be a HIP even though* $P(x_1, \ldots, x_n)$ *is not a HIP. For consider* $P = xy + 1$, $h_1(x) = x^2 + 1$ *and* $h_2(y) = y$*, and use the answer to Problem* 1.

Answer to Problem 15. *Yes,* $x^3 + xy + y^3$ *is indeed the sum of three squares of polynomials that vanish at* $(0, 0)$*:*

$$x^3 + xy + y^3 = \left(\frac{x^2 + y^2}{2} + \frac{x + y}{2}\right)^2 - \left(\frac{x^2 - y^2}{2} - \frac{x - y}{2}\right)^2 - (xy)^2.$$

Finally, we remark that in view of the answers to Problems 5, 6, 7, the hopes seem dim for a reasonable classification of HIPs asked for in Problem 9.

References

[1] S. Abhyankar, L. A. Rubel, *Every difference polynomial has a connected zero-set*. J. Indian Math. Soc. (N.S.) 43 (1979), 69–78.

[2] H. Davenport, D. J. Lewis, A. Schinzel, *Equations of the form* $f(x) = g(y)$. Quart. J. Math. Oxford Ser. (2) 12 (1961), 304–312.

[3] L. A. Rubel, W. A. Squires, B. A. Taylor, *Irreducibility of certain entire functions, with applications to harmonic analysis*. Ann. of Math. (2) 108 (1978), 553–567.

[4] B. L. van der Waerden, *Modern Algebra*. Ungar, New York 1949/1950.

Andrzej Schinzel
Selecta

Originally published in
Journal de Théorie des Nombres de Bordeaux
14 (2002), 647–666

On a decomposition of polynomials in several variables

Dedicated to Michel Mendès France

Résumé. On considère la représentation d'un polynôme à plusieurs variables comme une somme de polynômes à une variable en combinaisons linéaires des variables.

Abstract. One considers representation of a polynomial in several variables as the sum of values of univariate polynomials taken at linear combinations of the variables.

K. Oskolkov has called my attention to the following theorem used in the theory of polynomial approximation (see [6], Lemma 1 and below, Lemma 4): for every sequence of $d+1$ pairwise linearly independent vectors $[\alpha_{\mu 1}, \alpha_{\mu 2}] \in \mathbb{R}^2$ $(1 \leqslant \mu \leqslant d+1)$ and every polynomial $F \in \mathbb{C}[x_1, x_2]$ of degree d there exist polynomials $f_\mu \in \mathbb{C}[z]$ $(1 \leqslant \mu \leqslant d+1)$ such that

$$F = \sum_{\mu=1}^{d+1} f_\mu\big(\alpha_{\mu 1} x_1 + \alpha_{\mu 2} x_2\big).$$

He has asked for a generalization and a refinement of this result. The following theorem is a step in this direction.

Theorem 1. *Let n, d be positive integers and K a field with* $\operatorname{char} K = 0$ *or* $\operatorname{char} K > d$. *For every sequence S_ν $(2 \leqslant \nu \leqslant n)$ of subsets of K each of cardinality at least $d+1$ there exist $M = \binom{n+d-1}{n-1}$ vectors $[\alpha_{\mu 1}, \alpha_{\mu 2}, \ldots, \alpha_{\mu n}] \in \{1\} \times S_2 \times \ldots \times S_n$ with the following property. For every polynomial $F \in K[x_1, \ldots, x_n]$ of degree at most d there exist polynomials $f_\mu \in K[z]$ $(1 \leqslant \mu \leqslant M)$ such that*

$$F = \sum_{\mu=1}^{M} f_\mu\left(\sum_{\nu=1}^{n} \alpha_{\mu\nu} x_\nu\right). \tag{1}$$

It is not true that polynomials f_μ satisfying (1) exist for every sequence of vectors $[\alpha_{\mu 1}, \ldots, \alpha_{\mu n}]$ $(1 \leqslant \mu \leqslant M)$ such that each n of them are linearly independent. See the example at the end of the paper.

Let $P(n, d, K)$ be the set of all polynomials $F \in K[x_1, \ldots, x_n]$ of degree d. Let $M(n, d, K)$ be the least number M such that for every $F \in P(n, d, K)$ (1) holds for some

sequence of vectors $[\alpha_{\mu 1}, \ldots, \alpha_{\mu n}] \in K^n$ and some sequence of polynomials $f_\mu \in K[z]$ $(1 \leqslant \mu \leqslant M)$ if such sequences exist and ∞ otherwise. For an infinite field K, let $m(n, d, K)$ be the least number M such that for a Zariski open subset S of $P(n, d, K)$ and for every $F \in S$, (1) holds for some sequences of vectors and polynomials as before, if such sequences exist and ∞, otherwise. Theorem 1 implies

Corollary. *$M(n, d, K) < \infty$ if and only if either $n = 1$ or* char $K = 0$ *or* char $K > d$. *If K is infinite the same equivalence holds for $m(n, d, K)$.*

The problem of determination of $m(n, d, K)$ is related to the problem, much studied in the XIX-th century (see [5], for a modern account), of representation of a general n-ary form of degree d as the sum of powers of linear forms. The two problems are not equivalent even for K algebraically closed, since in our case neither F nor f_μ are supposed homogeneous.

Theorem 2. *For every infinite field K such that* char $K = 0$ *or* char $K > d$ *we have*

$$\binom{n+d-1}{n-1} \geqslant M(n, d, K) \geqslant m(n, d, K) \geqslant \max_{0 \leqslant e < d} \frac{1}{n+d-1-e} \left[\binom{n+d}{n} - \binom{n+e}{n} \right].$$

For $K = \mathbb{F}_q$, char $K > d$, *we have*

$$\binom{n+d-1}{n-1} \geqslant M(n, d, K) \geqslant \max_{0 \leqslant e < d} \frac{\left[\binom{n+d}{n} - \binom{n+e}{n}\right] \log q}{\log\left[(q^{d-e} - 1)\frac{q^n - 1}{q-1} + 1\right]}.$$

In particular, every n-ary form of degree d over a field K of characteristic 0 is representable as a linear combination of $\binom{n+d-1}{n-1}$ d-th powers of linear forms over K. This has been first proved, but not explicitly stated by Ellison [3].

Clearly $M(1, d, K) = M(n, 1, K) = 1$ and one easily proves

Theorem 3. *If* char $K \neq 2$, *then $M(n, 2, K) = n$ and if, in addition, K is infinite, then $m(n, 2, K) = n$.*

Diaconis and Shahshahani asserted without a formal proof that $M(2, d, \mathbb{R}) = d$ ([2], Application 2).

We shall show

Theorem 4. *For every field K such that either* char $K = 0$, *or* char $K > d$ *and* card $K \geqslant 2d - 2$ *we have*

$$M(2, d, K) = d.$$

In particular, every binary form F of degree d over a field K of characteristic 0 is representable as a linear combination of d d-th powers of linear forms over K, which slightly improves Theorem A of [4]. For $K = \mathbb{C}$ this was proved by Reznick [8].

The following theorem shows that the condition card $K \geqslant 2d-2$ in Theorem 4 may be superfluous.

Theorem 5. *For every field K such that*

$$\text{char } K > d \text{ and } \text{card } K \leqslant d+2$$

we have

$$M(2, d, K) = d.$$

Theorem 6. *For every algebraically closed field K, if* $\text{char } K = 0$ *or* $\text{char } K > d$, *then*

$$m(2, d, K) = \left\lceil \frac{2d+5-\sqrt{8d+17}}{2} \right\rceil.$$

The proof of Theorem 1 is based on two lemmas.

Lemma 1. *Let $n \geqslant 2$, T_i $(1 \leqslant i \leqslant n-1)$ be a subset of K of cardinality $d+1$. Then $F = 0$ is the only polynomial in $K[x_1, \ldots, x_{n-1}]$ of degree at most d in each variable such that $F(a_1, a_2, \ldots, a_{n-1}) = 0$ for all $[a_1, a_2, \ldots, a_{n-1}] \in T_1 \times \ldots \times T_{n-1}$.*

Proof. See [1], Lemma 2.2. □

Lemma 2. *Let for each $k = 0, 1, \ldots, n-2$ elements $\beta_{k,l}$ of K $(0 \leqslant l \leqslant d)$ be distinct and let for a positive integer $q \leqslant (d+1)^{n-1}$*

$$q-1 = \sum_{k=0}^{n-2} c_k(q)(d+1)^k, \text{ where } c_k(q) \in \mathbb{Z},\ 0 \leqslant c_k(q) \leqslant d$$

be the expansion of $q-1$ in base $d+1$.

Define $A\big((\beta_{kl})\big)$ as the matrix (a_{rs}), where

$$a_{rs} = \prod_{k=0}^{n-2} \beta_{k,c_k(r)}^{c_k(s)} \quad (1 \leqslant r, s \leqslant (d+1)^{n-1}). \tag{2}$$

Then $\det A\big((\beta_{kl})\big) \neq 0$.

Proof. Let us put in Lemma 1: $T_i = \{\beta_{i-1,l} : 0 \leqslant l \leqslant d\}$ $(1 \leqslant i \leqslant n-1)$. By the lemma the only polynomial $F \in K[x_1, \ldots, x_{n-1}]$ of degree at most d in each variable such that

$$F\big(\beta_{0,l_0}, \ldots, \beta_{n-2,l_{n-2}}\big) = 0 \text{ for all } [l_0, \ldots, l_{n-2}] \in \{0, 1, \ldots, d\}^{n-1} \tag{3}$$

is $F = 0$.

Now, all the vectors $[l_0, \ldots, l_{n-2}] \in \{0, 1, \ldots, d\}^{n-1}$ can be ordered lexicographically, so that the vector $[l_0, \ldots, l_{n-2}]$ occupies the position $1 + \sum_{i=0}^{n-2} l_i (d+1)^i$ and then the system

of equations (3) reads

$$F\big(\beta_{0,c_0(r)}, \beta_{1,c_1(r)}, \ldots, \beta_{n-2,c_{n-2}(r)}\big) = 0 \quad (1 \leqslant r \leqslant (d+1)^{n-1}).$$

Also the polynomial F can be written as

$$\sum_{s=1}^{(d+1)^{n-1}} A_s \prod_{j=1}^{n-1} x_j^{c_{j-1}(s)}, \quad \text{where } A_s \in K,$$

and (3) can be rewritten as

$$\sum_{s=1}^{(d+1)^{n-1}} A_s \prod_{j=0}^{n-2} \beta_{j,c_j(r)}^{c_j(s)} = 0 \quad (1 \leqslant r \leqslant (d+1)^{n-1}).$$

The fact that the only solution of this system is

$$A_s = 0 \quad (1 \leqslant r \leqslant (d+1)^{n-1}),$$

corresponding to $F = 0$, implies in view of (2) that

$$\det\big(a_{sr}\big) \neq 0.$$

But then also $\det A\big((\beta_{kl})\big) = \det(a_{rs}) \neq 0$. □

Proof of Theorem 1. Let us choose in S_ν distinct integers $\beta_{\nu-2,0}, \ldots, \beta_{\nu-2,d}$ $(2 \leqslant \nu \leqslant n)$. By Lemma 2

$$\det A\big((\beta_{kl})\big) \neq 0, \tag{4}$$

hence the matrix B consisting of the rows r of $A\big((\beta_{kl})\big)$ for which $\sum_{k=0}^{n-2} c_k(r) \leqslant d$ is of rank equal to the number of such rows $M = \binom{n+d-1}{n-1}$. Therefore B has M linearly independent columns $s_1, s_2, \ldots, s_M$. We put

$$\alpha_{\mu 1} = 1, \ \alpha_{\mu\nu} = \beta_{\nu-2,c_{\nu-2}(s_\mu)} \quad (1 \leqslant \mu \leqslant M, \ 2 \leqslant \nu \leqslant n). \tag{5}$$

Let

$$F(x_1, \ldots, x_n) = \sum_{i_1+i_2+\ldots+i_n \leqslant d} \binom{i_1 + \ldots + i_n}{i_1, \ldots, i_n} a_{i_1 \ldots i_n} \prod_{j=1}^{n} x_j^{i_j} \tag{6}$$

(note that the multinomial coefficient is non-zero).

For each $l \leqslant d$ we determine $b_{\mu l}$ $(1 \leqslant \mu \leqslant M)$ from the system of equations

$$\sum_{\mu=1}^{M} b_{\mu l} \prod_{\nu=2}^{n} \alpha_{\mu\nu}^{i_\nu} = a_{i_1 \ldots i_n} \quad (i_1 + \ldots + i_n = l), \tag{7}$$

which can be rewritten as

$$\sum_{\mu=1}^{M} b_{\mu l} \prod_{\nu=0}^{n-2} \beta_{\nu, c_\nu(s_\mu)}^{c_\nu(r)} = a_{l-\sum_{\nu=0}^{n-2} c_\nu(r), c_0(r), \ldots, c_{n-2}(r)}$$

$$\left(1 \leqslant r \leqslant (d+1)^{n-1},\ \sum_{\nu=0}^{n-2} c_\nu(r) \leqslant l\right).$$

By the choice of $s_1, \ldots, s_M$ the matrix of this system has rank equal to the number of equations, hence the system is solvable for $b_{\mu l} \in K$. We set

$$f_\mu = \sum_{l=0}^{d} b_{\mu l} z^l$$

and (1) follows from (6) and (7). □

Proof of Corollary. In view of Theorem 1 it suffices to show that $M(n, d, K) = \infty$ if $n > 1$ and

$$0 < p = \operatorname{char} K \leqslant d.$$

Let us consider an arbitrary polynomial F of the form (6) in which $a_{d,0,\ldots,0} \neq 0$ and $a_{p-1,1,0,\ldots,0} \neq 0$. If K is infinite such polynomials exist in every open subset of $P(n, d, K)$. If (1) holds, then the part F_{d-p} of degree p of F satisfies

$$F_{d-p} = \sum_{\mu=1}^{M} b_\mu \left(\sum_{\nu=1}^{n} \alpha_{\mu\nu} x_\nu\right)^p, \quad b_\mu \in K,$$

which is impossible, since $x_1^{p-1} x_2$ occurs with a non-zero coefficient on the left hand side, but not on the right. □

Proof of Theorem 2. The dimension of the set of all n-ary polynomials of degree not exceeding d and greater than e is $\binom{n+d}{d} - \binom{n+e}{e}$. On the other hand, the dimension of the set of all polynomials of the form $f(\boldsymbol{\alpha x})$, where $f = \sum_{l=e+1}^{d} b_l z^l$ is at most $d-e+n-1$ since the vectors $\boldsymbol{\alpha}$ can be normalized by taking the first non-vanishing coordinate equal to 1. This gives the upper bound $m(n + d - 1 - e)$ for the dimension of the set of all polynomials of the form $\sum_{\mu=1}^{m} f_\mu(\boldsymbol{\alpha}_\mu \boldsymbol{x})$ and, by the definition of $m(n, d, K)$,

$$m(n, d, K)(n + d - 1 - e) \geqslant \binom{n+d}{d} - \binom{n+e}{e},$$

which implies the first part of the theorem.

In order to prove the second part let us observe that the number of normalized vectors $\boldsymbol{\alpha} \in \mathbb{F}_q^n$ is $\dfrac{q^n-1}{q-1}$, while the number of non-zero polynomials $\sum_{l=e+1}^{d} b_l z^l \in \mathbb{F}_q[z]$ is $q^{d-e}-1$. Hence we obtain at most $(q^{d-e}-1)\dfrac{q^n-1}{q-1}+1$ polynomials of the form $f(\boldsymbol{\alpha}\boldsymbol{x})$ and at most $\left((q^{d-e}-1)\dfrac{q^n-1}{q-1}+1\right)^m$ polynomials of the form $\sum_{\mu=1}^{m} f_\mu(\boldsymbol{\alpha}_\mu \boldsymbol{x})$. On the other hand, the number of n-ary polynomials over $\mathbb{F}_q$ of degree not exceeding d and greater than e is

$$q^{\binom{n+d}{d}-\binom{n+e}{e}}.$$

By the definition of $M(n,d,\mathbb{F}_q)$ this gives

$$M(n,d,\mathbb{F}_q)\log\left((q^{d-e}-1)\frac{q^n-1}{q-1}+1\right) \geqslant \left(\binom{n+d}{d}-\binom{n+e}{e}\right)\log q,$$

which implies the second part of the theorem. □

Proof of Theorem 3. Let F_0, the leading quadratic form of F, be of rank r. By Lagrange's theorem there exist linearly independent vectors $[\alpha_{\mu 1},\dots,\alpha_{\mu n}]$ in K^n $(1 \leqslant \mu \leqslant r)$ such that

$$F_0 = \sum_{\mu=1}^{r} a_\mu \left(\sum_{\nu=1}^{n} \alpha_{\mu\nu} x_\nu\right)^2, \quad a_\mu \in K.$$

We set $a_\mu = 0$ for $r < \mu \leqslant n$ and choose $n-r$ vectors $[\alpha_{\mu 1},\dots,\alpha_{\mu n}]$ in K^n $(r+1 \leqslant \mu \leqslant n)$ such that $\det(\alpha_{\mu\nu})_{\mu,\nu\leqslant n} \neq 0$. Then there exist $b_\mu \in K$ $(1 \leqslant \mu \leqslant n)$ such that

$$F - F_0 - F(0,\dots,0) = \sum_{\mu=1}^{n} b_\mu \sum_{\nu=1}^{n} \alpha_{\mu\nu} x_\nu$$

and (1) follows with $M = n$

$$f_1(z) = a_1 z^2 + b_1 z + F(0,\dots,0),$$
$$f_\mu(z) = a_\mu z^2 + b_\mu z \quad (1 < \mu \leqslant n).$$

On the other hand, the polynomial $F = \sum_{\nu=1}^{n} c_\nu x_\nu^2$ where $c_\nu \neq 0$ is clearly not representable in the form (1) with $M < n$.

For the proof of Theorem 4 we need

Lemma 3. *We have the identity*

$$\begin{vmatrix} 1 & \dots & 1 & A_0 \\ x_1 & \dots & x_d & A_1 \\ \vdots & \ddots & \vdots & \vdots \\ x_1^d & \dots & x_d^d & A_d \end{vmatrix} = \prod_{1\leqslant i<j\leqslant d} (x_j - x_i) \sum_{i=0}^{d} (-1)^i A_{d-i}\,\tau_i(x_1,\dots,x_d),$$

where τ_i is the i-th fundamental symmetric function of $x_1,\dots,x_d$, $\tau_0 = 1$.

Proof. See [7], p. 333. □

Lemma 4. *Let* $\boldsymbol{\alpha}_\mu$ $(1 \leqslant \mu \leqslant d)$ *be arbitrary pairwise linearly independent vectors in* K^2. *If* $\operatorname{char} K = 0$ *or* $\operatorname{char} K \geqslant d$, *for every polynomial* $F \in K[x_1, x_2]$ *of degree at most* $d-1$ *there exist polynomials* $f_\mu \in K[z]$ *such that*

$$F = \sum_{\mu=1}^{d} f_\mu\big(\alpha_{\mu 1}x_1 + \alpha_{\mu 2}x_2\big).$$

Proof. Since $\boldsymbol{\alpha}_\mu$ are pairwise linearly independent we may assume that either

(i) $\alpha_{\mu 1} = 1$, $\alpha_{\mu 2}$ are all distinct $(1 \leqslant \mu \leqslant d)$, or
(ii) $\alpha_{\mu 1} = 1$, $\alpha_{\mu 2}$ are all distinct $(1 \leqslant \mu < d)$, $\alpha_{d1} = 0$, $\alpha_{d2} = 1$.

Let now

$$F = \sum_{i_1+i_2<d} \binom{i_1+i_2}{i_1} a_{i_1 i_2} x_1^{i_1} x_2^{i_2}$$

(note that the binomial coefficient is non-zero). In the case (i) for each $l < d$ we can solve for $b_{\mu l}$ in K the system of equations

$$a_{l-i,i} = \sum_{\mu=1}^{d} b_{\mu l}\alpha_{\mu 2}^{i} \quad (0 \leqslant i \leqslant l),$$

since the rank of the matrix of the coefficients equals the number of equations. Then we set

$$f_\mu(z) = \sum_{l=0}^{d-1} b_{\mu l} z^l.$$

In the case (ii) for each $l < d$ we can solve for $b_{\mu l}$ in K the system of equations

$$a_{l-i,i} = \sum_{\mu=1}^{d-1} b_{\mu l}\alpha_{\mu 2}^{i} \quad (0 \leqslant i < l),$$

and then we set

$$f_\mu(z) = \sum_{l=0}^{d-1} b_{\mu l} z^l \quad (\mu < d), \qquad f_d(z) = \sum_{l=0}^{d-1}\Big(a_{0l} - \sum_{\mu=1}^{d-1} b_{\mu l}\alpha_{\mu 2}^{l}\Big) z^l. \qquad \square$$

Proof of Theorem 4. In view of Theorem 3 we may assume $d \geqslant 3$. We shall prove first that $M(2, d, K) \leqslant d$.

Let $F \in P(2, d, K)$ and let F_0 be the highest homogeneous part of F. Supposing that we have represented F_0 in the form (1) with $M = d$ we may assume that $\boldsymbol{\alpha}_\mu$ $(1 \leqslant \mu \leqslant d)$ are pairwise linearly independent and then apply Lemma 4 to represent $F - F_0$ in the form (1) with the same $\boldsymbol{\alpha}_\mu$. Therefore, it is enough to find a representation (1) for F homogeneous of degree d. By Lemma 1 there exist c_{11}, c_{21} in K such that $F(c_{11}, c_{21}) \neq 0$.

Replacing F by $F(c_{11}x_1 + c_{12}x_2, c_{21}x_1 + c_{22}x_2)$, where c_{12}, c_{22} are chosen in K so that $c_{11}c_{22} - c_{12}c_{21} \neq 0$ we may assume that the coefficient of x_1^d in $F(x_1, x_2)$ is non-zero. Let then

$$F(x_1, x_2) = \sum_{i=0}^{d} \binom{d}{i} a_i x_1^{d-i} x_2^i, \quad a_0 \neq 0 \tag{8}$$

and let us consider the polynomial

$$\begin{aligned} G(y_1, \ldots, y_{d-2}) = {} & \prod_{1 \leqslant i < j \leqslant d-2} (y_j - y_i) \cdot \sum_{i=2}^{d} (-1)^{i-1} a_{d-i} \tau_{i-2}(y_1, \ldots, y_{d-2}) \\ & \times \prod_{j=1}^{d-2} \Bigg(a_{d-1} + \sum_{i=2}^{d-1} (-1)^{i-1} a_{d-i} \big(\tau_{i-1}(y_1, \ldots, y_{d-2}) + y_j \tau_{i-2}(y_1, \ldots, y_{d-2}) \big) \\ & \qquad + (-1)^{d-1} a_0 y_j \tau_{d-2}(y_1, \ldots, y_{d-2}) \Bigg). \end{aligned}$$

Since $a_0 \neq 0$ the polynomial G is not identically 0 and we have for each $i \leqslant d-2$

$$\deg_{y_i} G = 2d - 3.$$

Since card $K \geqslant 2d - 2$, by Lemma 1 there exist elements $\beta_1, \ldots, \beta_{d-2}$ of K such that

$$G(\beta_1, \ldots, \beta_{d-2}) \neq 0. \tag{9}$$

We now put

$$\beta_{d-1} = -\frac{\sum_{i=1}^{d-1} (-1)^{i-1} a_{d-i} \tau_{i-1}(\beta_1, \ldots, \beta_{d-2})}{\sum_{i=2}^{d} (-1)^{i-1} a_{d-i} \tau_{i-2}(\beta_1, \ldots, \beta_{d-2})}, \tag{10}$$

which makes sense, since by (9) the denominator is non-zero. Again by (9) we have $\beta_i \neq \beta_j$ for $1 \leqslant i < j < d$. Hence

$$D_0 = \begin{vmatrix} 1 & \ldots & 1 & 1 \\ \beta_1 & \ldots & \beta_{d-2} & \beta_{d-1} \\ \vdots & \ddots & \vdots & \vdots \\ \beta_1^{d-2} & \ldots & \beta_{d-2}^{d-2} & \beta_{d-1}^{d-2} \end{vmatrix} = \prod_{1 \leqslant i < j < d} (\beta_j - \beta_i) \neq 0.$$

However, by (10) and Lemma 3,

$$
\begin{aligned}
D &= \begin{vmatrix} 1 & \dots & 1 & a_0 \\ \beta_1 & \dots & \beta_{d-1} & a_1 \\ \vdots & \ddots & \vdots & \vdots \\ \beta_1^{d-1} & \dots & \beta_{d-1}^{d-1} & a_{d-1} \end{vmatrix} \\
&= \prod_{1 \leqslant i < j < d} (\beta_j - \beta_i) \cdot \sum_{i=1}^{d} (-1)^{i-1} a_{d-i} \tau_{i-1}(\beta_1, \dots, \beta_{d-1}) \\
&= D_0 \Bigg(a_{d-1} + \sum_{i=2}^{d-1} (-1)^{i-1} a_{d-i} \big(\beta_{d-1} \tau_{i-2}(\beta_1, \dots, \beta_{d-2}) \\
&\qquad + \tau_{i-1}(\beta_1, \dots, \beta_{d-2}) \big) + (-1)^{d-1} a_0 \beta_{d-1} \tau_{d-2}(\beta_1, \dots, \beta_{d-2}) \Bigg) = 0.
\end{aligned}
$$

Hence the system of equations

$$
\sum_{\mu=1}^{d-1} b_\mu \beta_\mu^j = a_j \quad (0 \leqslant j < d) \tag{11}
$$

is solvable for elements b_μ of K.

We set

$$
\begin{aligned}
&\alpha_{\mu 1} = 1, \quad \alpha_{\mu 2} = \beta_\mu, \quad f_\mu(z) = b_\mu z^d \quad (1 \leqslant \mu < d); \\
&\alpha_{d1} = 0, \quad \alpha_{d2} = 1, \qquad f_d(z) = \Bigg(a_d - \sum_{\mu=1}^{d-1} b_\mu \beta_\mu^d \Bigg) z^d
\end{aligned}
$$

and obtain (1) from (8) and (11).

It remains to show that $M(2, d, K) \geqslant d$. Let us consider the equation

$$
x_1 x_2^{d-1} + a x_2^d = \sum_{\mu=1}^{d-1} f_\mu\big(\alpha_{\mu 1} x_1 + \alpha_{\mu 2} x_2\big). \tag{12}
$$

In order to prove that it is impossible for every $a \in K$ it is clearly sufficient to consider $f_\mu = b_\mu z^d$, $\alpha_{\mu 1} = 1$, $\alpha_{\mu 2}$ distinct. Comparing the coefficients of $x_1^{d-j} x_2^j$ on both sides of (12) we obtain

$$
0 = \sum_{\mu=1}^{d-1} b_\mu \alpha_{\mu 2}^j \quad (0 \leqslant j < d-1).
$$

The determinant of this system is $\prod_{1 \leqslant \mu < \nu < d} (\alpha_{\nu 2} - \alpha_{\mu 2}) \neq 0$, hence $b_\mu = 0$ for $1 \leqslant \mu < d$ and by (12)

$$
x_1 x_2^{d-1} + a x_2^d = 0,
$$

a contradiction. This argument is valid without the assumption on card K. □

For the proof of Theorem 5 we need

Lemma 5. *Let $a_1, \dots, a_k$ be distinct elements of $\mathbb{F}_p^*$, $k \geqslant p-3$. Then*

$$\tau_j(a_1, \dots, a_k) = \begin{cases} 0 & \text{if } k = p-1,\ 0 < j < k \\ (-r)^j & \text{if } 0 \leqslant j \leqslant k = p-2, \\ & \quad \text{and } \{r\} = \mathbb{F}_p^* \setminus \{a_1, \dots, a_k\} \\ (-1)^j \dfrac{r^{j+1} - s^{j+1}}{r-s} & \text{if } 0 \leqslant j \leqslant k = p-3, \\ & \quad \text{and } \{r, s\} = \mathbb{F}_p^* \setminus \{a_1, \dots, a_k\} \end{cases}$$

Proof. If $k = p-1$ we use the identity

$$x^{p-1} - 1 = \prod_{a \in \mathbb{F}_p^*} (x - a).$$

If $k = p-2$ we argue by induction. For $j = 0$ the statement is true, for $k \geqslant j \geqslant 1$ we have the identity

$$0 = \tau_j(a_1, \dots, a_k, r) = \tau_j(a_1, \dots, a_k) + r\tau_{j-1}(a_1, \dots, a_k),$$

hence, by induction

$$\tau_j(a_1, \dots, a_k) = -r\tau_{j-1}(a_1, \dots, a_k) = -r(-r)^{j-1} = (-r)^j.$$

If $k = p-3$ we argue again by induction. If $j = 0$ the statement is true. If $k \geqslant j \geqslant 1$ we have the identity

$$(-r)^j = \tau_j(a_1, \dots, a_k, s) = \tau_j(a_1, \dots, a_k) + s\tau_{j-1}(a_1, \dots, a_k),$$

hence, by induction

$$\tau_j(a_1, \dots, a_k) = (-r)^j - s\tau_{j-1}(a_1, \dots, a_k) = (-1)^j r^j + (-1)^j s \frac{r^j - s^j}{r-s}$$
$$= (-1)^j \frac{r^{j+1} - s^{j+1}}{r-s}. \qquad \square$$

Proof of Theorem 5. By the last statement in the proof of Theorem 4 we have $M(2, d, K) \geqslant d$, thus it remains to prove the reverse inequality. Let $F \in P(2, d, K)$. By Lemma 4 we may assume that F is homogeneous. Let

$$F(x_1, x_2) = \sum_{i=0}^{d} \binom{d}{i} a_i x_1^{d-i} x_2^i \tag{13}$$

and consider first card $K = p = d+1$.

Let us assume first that the mapping $\mathbb{F}_p^* \to \mathbb{F}_p$ given by $t \mapsto f(t) = \sum_{i=0}^{p-1} a_{p-1-i} t^i$ is

not injective. Then there exist $r, s \in \mathbb{F}_p^*$ such that $r \neq s$ and $f(r) = f(s)$, hence

$$\sum_{i=1}^{p-2} a_{p-1-i} \frac{r^i - s^i}{r - s} = 0. \tag{14}$$

Setting $\alpha_{12} = 0$, $\{\alpha_{22}, \ldots, \alpha_{p-2,2}\} = \mathbb{F}_p^* \setminus \{r, s\}$ we have by Lemma 5

$$\tau_i(\alpha_{12}, \ldots, \alpha_{p-2,2}) = \tau_i(\alpha_{22}, \ldots, \alpha_{p-2,2}) = (-1)^i \frac{r^{i+1} - s^{i+1}}{r - s} \quad (i \leqslant p-3),$$
$$\tau_{p-2}(\alpha_{12}, \ldots, \alpha_{p-2,2}) = 0,$$

hence, by (14),

$$\sum_{i=1}^{p-1} (-1)^{i-1} a_{p-1-i} \tau_{i-1}(\alpha_{12}, \ldots, \alpha_{p-2,2}) = 0$$

and, by Lemma 3,

$$\begin{vmatrix} 1 & \ldots & 1 & a_0 \\ \alpha_{12} & \ldots & \alpha_{p-2,2} & a_1 \\ \vdots & \ddots & \vdots & \vdots \\ \alpha_{12}^{p-2} & \ldots & \alpha_{p-2,2}^{p-2} & a_{p-2} \end{vmatrix} = 0.$$

Since $\det(\alpha_{\mu 2}^j)_{\substack{0 \leqslant j < p-2 \\ 1 \leqslant \mu \leqslant p-2}} \neq 0$, this suffices for solvability over $\mathbb{F}_p$ of the system of equations

$$\sum_{\mu=1}^{p-2} b_\mu \alpha_{\mu 2}^j = a_j \quad (0 \leqslant j < p-1). \tag{15}$$

Then we obtain from (13)–(15) that

$$F(x_1, x_2) = \sum_{\mu=1}^{p-2} b_\mu (x_1 + \alpha_{\mu 2} x_2)^{p-1} + \left(a_{p-1} - \sum_{\mu=1}^{p-2} b_\mu \alpha_{\mu 2}^{p-1} \right) x_2^{p-1}.$$

Assume now that the mapping $\mathbb{F}_p^* \to \mathbb{F}_p$ given by $t \mapsto f(t)$ is injective. We shall consider three cases

(i) $a_0 \in f(\mathbb{F}_p^*)$,

(ii) $a_{p-1} \in f(\mathbb{F}_p^*)$,

(iii) $a_{p-1} \notin f(\mathbb{F}_p^*)$, $a_0 \notin f(\mathbb{F}_p^*)$.

In the case (i), let $a_0 = f(r)$, $r \in \mathbb{F}_p^*$, so that

$$\sum_{i=0}^{p-2} a_{p-1-i} r^i = 0. \tag{16}$$

Setting $\alpha_{12} = 0$, $\{\alpha_{22}, \dots, \alpha_{p-1,2}\} = \mathbb{F}_p^* \setminus \{r\}$ we have by Lemma 5

$$\tau_i(\alpha_{12}, \dots, \alpha_{p-1,2}) = \tau_i(\alpha_{22}, \dots, \alpha_{p-1,2}) = (-r)^i \quad (i \leqslant p-2),$$
$$\tau_{p-1}(\alpha_{12}, \dots, \alpha_{p-1,2}) = 0,$$

hence, by (16),

$$\sum_{i=0}^{p-1} (-1)^i a_{p-1-i} \tau_i(\alpha_{12}, \dots, \alpha_{p-1,2}) = 0$$

and, by Lemma 3,

$$\begin{vmatrix} 1 & \dots & 1 & a_0 \\ \alpha_{12} & \dots & \alpha_{p-1,2} & a_1 \\ \vdots & \ddots & \vdots & \vdots \\ \alpha_{12}^{p-1} & \dots & \alpha_{p-1,2}^{p-1} & a_{p-1} \end{vmatrix} = 0.$$

Since $\det(\alpha_{\mu 2}^j)_{\substack{0 \leqslant j < p-1 \\ 1 \leqslant \mu \leqslant p-1}} \neq 0$, this suffices for solvability over $\mathbb{F}_p$ of the system of equations

$$\sum_{\mu=1}^{p-1} b_\mu \alpha_{\mu 2}^j = a_j \quad (0 \leqslant j \leqslant p-1). \tag{17}$$

Then we obtain from (13) and (17) that

$$F(x_1, x_2) = \sum_{\mu=1}^{p-1} b_\mu (x_1 + \alpha_{\mu 2} x_2)^{p-1}.$$

In the case (ii), let $a_{p-1} = f(r^{-1})$, $r \in \mathbb{F}_p^*$, so that

$$\sum_{i=0}^{p-2} a_i r^i = \sum_{i=1}^{p-1} a_{p-1-i} r^{p-1-i} = 0. \tag{18}$$

Setting $\alpha_{11} = 0$, $\{\alpha_{21}, \dots, \alpha_{p-1,1}\} = \mathbb{F}_p^* \setminus \{r\}$ we have by Lemma 5

$$\tau_i(\alpha_{11}, \dots, \alpha_{p-1,1}) = \tau_i(\alpha_{21}, \dots, \alpha_{p-1,1}) = (-r)^i \quad (i \leqslant p-2),$$
$$\tau_{p-1}(\alpha_{11}, \dots, \alpha_{p-1,1}) = 0,$$

hence, by (18),

$$\sum_{i=0}^{p-1} (-1)^i a_i \tau_i(\alpha_{11}, \dots, \alpha_{p-1,1}) = 0$$

and, by Lemma 3,

$$\begin{vmatrix} 1 & \dots & 1 & a_{p-1} \\ \alpha_{11} & \dots & \alpha_{p-1,1} & a_{p-2} \\ \vdots & \ddots & \vdots & \vdots \\ \alpha_{11}^{p-1} & \dots & \alpha_{p-1,1}^{p-1} & a_0 \end{vmatrix} = 0.$$

Since $\det(\alpha_{\mu 1}^{j})_{\substack{0\leqslant j<p-1 \\ 1\leqslant\mu\leqslant p-1}} \neq 0$, this suffices for solvability over $\mathbb{F}_p$ of the system of equations

$$\sum_{\mu=1}^{p-1} b_\mu \alpha_{\mu 1}^{j} = a_{p-1-j} \quad (0 \leqslant j \leqslant p-1). \tag{19}$$

Then we obtain from (13) and (19)

$$F(x_1, x_2) = \sum_{l=0}^{p-1} b_\mu \big(\alpha_{\mu 1} x_1 + x_2\big)^{p-1}.$$

In the case (iii), since

$$\operatorname{card} f(\mathbb{F}_p^*) = \operatorname{card} \mathbb{F}_p^* = p-1,$$

we have $a_0 = a_{p-1}$. Hence the first and the last row of the determinant

$$\begin{vmatrix} 1 & \dots & 1 & a_0 \\ 1 & \dots & p-1 & a_1 \\ \vdots & \ddots & \vdots & \vdots \\ 1^{p-1} & \dots & (p-1)^{p-1} & a_{p-1} \end{vmatrix}.$$

are equal and the determinant vanishes.

Since $\det(\mu^j)_{\substack{0\leqslant j<p-1 \\ 1\leqslant\mu\leqslant p-1}} \neq 0$, this suffices for solvability over $\mathbb{F}_p$ of the system of equations

$$\sum_{\mu=1}^{p-1} b_\mu \mu^j = a_j \ (0 \leqslant j \leqslant p-1). \tag{20}$$

Then we obtain from (13) and (20)

$$F(x_1, x_2) = \sum_{\mu=1}^{p-1} b_\mu (x_1 + \mu x_2)^{p-1}.$$

Consider now the case where $\operatorname{card} K = p = d+2$. Again, let us assume first that the mapping $\mathbb{F}_p^* \to \mathbb{F}_p$ given by $t \mapsto f(t) = \sum_{i=0}^{p-2} a_{p-2-i} t^i$ is not injective. Then there exist

$r, s \in \mathbb{F}_p^*$ such that $r \neq s$ and $f(r) = f(s)$, hence

$$\sum_{i=1}^{p-2} a_{p-2-i} \frac{r^i - s^i}{r - s} = 0. \tag{21}$$

Setting $\{\alpha_{12}, \ldots, \alpha_{p-3,2}\} = \mathbb{F}_p^* \setminus \{r, s\}$ we have by Lemma 5

$$\tau_i\big(\alpha_{12}, \ldots, \alpha_{p-3,2}\big) = (-1)^i \frac{r^{i+1} - s^{i+1}}{r - s} \quad (i \leqslant p-3)$$

hence, by (21),

$$\sum_{i=1}^{p-2} (-1)^{i-1} a_{p-2-i} \tau_{i-1}\big(\alpha_{12}, \ldots, \alpha_{p-3,2}\big) = 0$$

and, by Lemma 3,

$$\begin{vmatrix} 1 & \ldots & 1 & a_0 \\ \alpha_{12} & \ldots & \alpha_{p-3,2} & a_1 \\ \vdots & \ddots & \vdots & \vdots \\ \alpha_{12}^{p-3} & \ldots & \alpha_{p-3,2}^{p-3} & a_{p-3} \end{vmatrix} = 0.$$

Since $\det(\alpha_{\mu 2}^j)_{\substack{0 \leqslant j < p-3 \\ 1 \leqslant \mu \leqslant p-3}} \neq 0$, this suffices for solvability over $\mathbb{F}_p$ of the system of equations

$$\sum_{\mu=1}^{p-3} b_\mu \alpha_{\mu 2}^j = a_j \quad (0 \leqslant j < p-2). \tag{22}$$

Then we obtain from (13) and (22) that

$$F(x_1, x_2) = \sum_{\mu=1}^{p-3} b_\mu \big(x_1 + \alpha_{\mu 2} x_2\big)^{p-2} + \left(a_{p-2} - \sum_{\mu=1}^{p-3} b_\mu \alpha_{\mu 2}^{p-2}\right) x_2^{p-2}.$$

Assume now that the mapping $\mathbb{F}_p^* \to \mathbb{F}_p$ given by $t \mapsto f(t)$ is injective. We shall consider two cases

(iv) $0 \in f(\mathbb{F}_p^*)$,

(v) $0 \notin f(\mathbb{F}_p^*)$.

In the case (iv) let $0 = f(r)$, $r \in \mathbb{F}_p^*$, so that

$$\sum_{i=0}^{p-2} a_{p-2-i} r^i = 0. \tag{23}$$

Setting $\{\alpha_{12}, \ldots, \alpha_{p-2,2}\} = \mathbb{F}_p^* \setminus \{r\}$ we have by Lemma 5

$$\tau_i\big(\alpha_{12}, \ldots, \alpha_{p-2,2}\big) = (-r)^i \quad (1 \leqslant i \leqslant p-2),$$

hence, by (23),

$$\sum_{i=0}^{p-2}(-1)^i a_{p-2-i}\,\tau_i\big(\alpha_{12},\dots,\alpha_{p-2,2}\big)=0 \tag{24}$$

and, by Lemma 3,

$$\begin{vmatrix} 1 & \dots & 1 & a_0 \\ \alpha_{12} & \dots & \alpha_{p-2,2} & a_1 \\ \vdots & \ddots & \vdots & \vdots \\ \alpha_{12}^{p-2} & \dots & \alpha_{p-2,2}^{p-2} & a_{p-2} \end{vmatrix} = 0.$$

Since $\det(\alpha_{\mu 2}^{j})_{\substack{0\leqslant j<p-2\\ 1\leqslant\mu\leqslant p-2}} \neq 0$, this suffices for solvability over $\mathbb{F}_p$ of the system of equations

$$\sum_{\mu=1}^{p-2} b_\mu \alpha_{\mu 2}^{j} = a_j \quad (0\leqslant j\leqslant p-2). \tag{25}$$

Then we obtain from (13) and (25) that

$$F(x_1,x_2)=\sum_{\mu=1}^{p-2} b_\mu\big(x_1+\alpha_{\mu 2}x_2\big)^{p-2}.$$

In the case (v) $t\mapsto f(t)$ is a bijective mapping of $\mathbb{F}_p^*$ onto $\mathbb{F}_p^*$. If the mapping $t\mapsto tf(t)$ had the same property we should obtain

$$-1=\prod_{t\in\mathbb{F}_p^*} tf(t)=\prod_{t\in\mathbb{F}_p^*} t\cdot\prod_{t\in\mathbb{F}_p^*} f(t)=(-1)^2=1,$$

which is impossible. Hence there exist $r,s\in\mathbb{F}_p^*$ such that $r\neq s$ and $rf(r)=sf(s)$:

$$\sum_{i=0}^{p-2} a_{p-2-i}\,\frac{r^{i+1}-s^{i+1}}{r-s}=0. \tag{26}$$

Setting $\alpha_{12}=0$, $\{\alpha_{22},\dots,\alpha_{p-2,2}\}=\mathbb{F}_p^*\setminus\{r,s\}$ we have by Lemma 5

$$\tau_i\big(\alpha_{12},\dots,\alpha_{p-2,2}\big)=\tau_i\big(\alpha_{22},\dots,\alpha_{p-2,2}\big)=(-1)^i\,\frac{r^{i+1}-s^{i+1}}{r-s}\quad(i\leqslant p-3),$$

$$\tau_{p-2}\big(\alpha_{12},\dots,\alpha_{p-2,2}\big)=0,$$

hence, by (26), (24) holds and we conclude the argument as in the case (iv). The proof of Theorem 5 is complete. □

Proof of Theorem 6. We shall prove first that

$$m(2,d,K)\geqslant\left\lceil\frac{2d+5-\sqrt{8d+17}}{2}\right\rceil=:m. \tag{27}$$

Let $2d+4 = u^2 + v$, where u, v are integers, $|v| \leqslant u$. We have

$$\left(u + \frac{2d+4}{u}\right)^2 = \left(2u + \frac{v}{u}\right)^2 \leqslant 4u^2 + 4v + 1 = 8d + 17,$$

hence on taking $e = d + 1 - u$ we obtain from Theorem 2

$$m(2, d, K) \geqslant \frac{1}{d+1-e}\left[\binom{d+2}{2} - \binom{e+2}{2}\right]$$
$$= \frac{(u-1)(2d+5-u)}{2u} \geqslant \frac{2d+5-\sqrt{8d+17}}{2},$$

which gives (27).

In order to show that

$$m(2, d, K) \leqslant m$$

we notice that

$$\rho := m - \binom{d-m+2}{2} \geqslant 0.$$

Let us consider independent variables $a_{i,j}$, where $i, j \geqslant 0$, $m \leqslant i + j \leqslant d$ and the matrix $B = (b_{\mu\nu})_{\substack{1 \leqslant \mu \leqslant m-\rho \\ 0 \leqslant \nu \leqslant m-\rho}}$, where

$$b_{\mu 0} = a_{\binom{k_\mu+1}{2}-\mu, m-\binom{k_\mu}{2}-1+\mu}$$
$$b_{\mu\nu} = a_{\rho+\binom{k_\mu+1}{2}+\nu-\mu, m-\rho-\binom{k_\mu}{2}-1+\mu-\nu} \quad (1 \leqslant \nu \leqslant m-\rho),$$

k_μ being determined by the inequality

$$\binom{k_\mu}{2} < \mu \leqslant \binom{k_\mu+1}{2}.$$

Let B_ν be the minor of the matrix B obtained by omitting the ν-th column and D be the discriminant of the polynomial

$$B_0 x^m + \sum_{\nu=1}^{m-\rho} (-1)^\nu B_\nu x^{m-\rho-\nu}.$$

Polynomials B_0 and D in the variables a_{ij} are not identically zero.

In order to see that $B_0 \neq 0$ let us order all variables a_{ij} linearly assuming $a_{ij} \prec a_{kl}$ if either $i + j < k + l$ or $i + j = k + l$ and $j < l$. Then all products of a_{ij} are ordered lexicographically. The product

$$\pm \prod_{\mu+\nu=m-\rho+1} b_{\mu\nu} = \pm \prod_{\mu=1}^{m-\rho} a_{m+\binom{k_\mu+1}{2}+1-2\mu, 2\mu-\binom{k_\mu}{2}-2}$$

occurring in the expansion of B_0 precedes in the lexicographic order any other term in this expansion, hence it does not cancel and $B_0 \neq 0$. On the other hand

$$D = B_0^{2m-2} D_0,$$

where D_0 is the discriminant of the polynomial

$$x^m + \sum_{\nu=1}^{m-\rho} (-1)^\nu \frac{B_\nu}{B_0} x^{m-\rho-\nu}.$$

Now, the discriminant of the polynomial

$$x^m - \sum_{\nu=1}^{m-\rho} t_\nu x^{m-\rho-\nu}$$

is not identically 0 as a function of t_ν (it is different from 0 for $t_\nu = 0$ for $\nu < m-\rho$, $t_{m-\rho} = 1$), hence $D_0 = 0$ implies an algebraic dependence over the prime field Π of K between $(-1)^{\nu-1} B_\nu / B_0$ $(1 \leqslant \nu \leqslant m-\rho)$. Let

$$\Omega = \Pi\big(a_{m+k-1-i,i} : \ 1 \leqslant k \leqslant d-m+1, \ 0 \leqslant i \leqslant m+k-1\big).$$

We assert that for $1 \leqslant k \leqslant d-m+1$, $0 \leqslant i \leqslant m+k-1$

$$a_{m+k-1-i,i} \in \Omega\Big(\frac{B_1}{B_0}, \ldots, \frac{B_{m-\rho}}{B_0}\Big). \tag{28}$$

This is obviously true for $i \leqslant m-1$. Assume that it is true for all $i < j$, where $m \leqslant j \leqslant m+k-1$. Since, by the Cramer formulae, for $\mu = \binom{k}{2} + j - m + 1 \leqslant \binom{k+1}{2}$

$$\sum_{\nu=1}^{m-\rho} (-1)^{\nu-1} \frac{B_\nu}{B_0} a_{\rho+\binom{k+1}{2}+\nu-\mu, m-\rho-\binom{k}{2}-1+\mu-\nu} = a_{\binom{k+1}{2}-\mu, m-\binom{k}{2}-1+\mu} = a_{k-j+m-1,j} \tag{29}$$

and all a's occurring on the left hand side have the second index at most

$$m - \rho - \binom{k}{2} - 1 + \binom{k}{2} + j - m + 1 - 1 = j - \rho - 1 < j,$$

it follows that $a_{m+k-1-j,j} \in \Omega\Big(\frac{B_1}{B_0}, \ldots, \frac{B_{m-\rho}}{B_0}\Big)$ and the inductive proof of (28) is complete. But then

$$\mathrm{tr.deg.}\, \Omega\Big(\frac{B_1}{B_0}, \ldots, \frac{B_{m-\rho}}{B_0}\Big) \Big/ \Omega < m-\rho$$

implies

$$\mathrm{tr.deg.}\, \Omega\big(a_{m+k-1-j,j} : \ 1 \leqslant k \leqslant d-m+1, \ m \leqslant j \leqslant m+k-1\big)/\Omega < m-\rho,$$

while the number of independent variables $a_{m+k-1-j,j}$ $(1 \leqslant k \leqslant d-m+1, m \leqslant j \leqslant m+k-1)$ equals

$$\sum_{k=1}^{d-m+1} k = \binom{d-m+2}{2} = m-\rho.$$

The obtained contradiction shows that $D_0 \neq 0$, and hence $D \neq 0$.

We now assert that if for a polynomial

$$F = \sum_{i_1+i_2 \leqslant d} \binom{i_1+i_2}{i_1} a_{i_1 i_2} x_1^{i_1} x_2^{i_2} \tag{30}$$

we have $B_0 D \neq 0$, then there exist $f_\mu \in K[z]$ and $\alpha_\mu \in K$ $(1 \leqslant \mu \leqslant m)$ such that

$$F(x_1, x_2) = \sum_{\mu=1}^{m} f_\mu\big(x_1 + \alpha_\mu x_2\big). \tag{31}$$

Indeed, using the notation introduced earlier we take for α_μ $(1 \leqslant \mu \leqslant m)$ the m distinct zeros of the polynomial

$$B_0 x^m + \sum_{\nu=1}^{m-\rho} (-1)^\nu B_\nu x^{m-\rho-\nu}.$$

Now for each $l \leqslant d$ we solve the system of equations

$$\sum_{\mu=1}^{m} b_{\mu l} \alpha_\mu^i = a_{l-i,i} \quad (0 \leqslant i \leqslant \min(l, m-1))$$

for $b_{\mu l}$ in K and assert that the solution satisfies the larger system

$$\sum_{\mu=1}^{m} b_{\mu l} \alpha_\mu^j = a_{l-j,j} \quad (0 \leqslant j \leqslant l). \tag{32}$$

The proof is by induction on j. We assume that (32) is true for all $j < i$, where $l \geqslant i \geqslant m$ and obtain

$$\begin{aligned} \sum_{\mu=1}^{m} b_{\mu l} \alpha_\mu^i &= \sum_{\mu=1}^{m} b_{\mu l} \alpha_\mu^{i-m} \sum_{\nu=1}^{m-\rho} (-1)^{\nu-1} \frac{B_\nu}{B_0} \alpha_\mu^{m-\rho-\nu} \\ &= \sum_{\nu=1}^{m-\rho} (-1)^{\nu-1} \frac{B_\nu}{B_0} \sum_{\mu=1}^{m} b_{\mu l} \alpha_\mu^{i-\rho-\nu} = \sum_{\nu=1}^{m-\rho} (-1)^{\nu-1} \frac{B_\nu}{B_0} a_{l-i+\rho+\nu,\, i-\rho-\nu}. \end{aligned} \tag{33}$$

However the sum on the right hand side of (33) coincides with the sum on the left hand side of (29) on putting there $k = l - m + 1$, $\mu = i - m + \binom{k}{2} + 1 \leqslant \binom{k+1}{2}$. Hence by (29)

$$\sum_{\mu=1}^{m} b_{\mu l} \alpha_\mu^i = a_{\binom{k+1}{2}-\mu,\, m-\binom{k}{2}-1+\mu} = a_{l-i,i}$$

which proves (32).

Now, on taking

$$f_\mu(z) = \sum_{l=0}^{d} b_{\mu l} z^l,$$

we obtain (31) from (30) and (32). □

Example. Each three of the vectors [1, 0, 0], [0, 1, 0], [0, 0, 1], [3, 1, 1], [1, 3, 1], [3, 3, 2] are linearly independent over $\mathbb{Q}$, nevertheless for all polynomials $f_i \in \mathbb{Q}[z]$ $(1 \leqslant i \leqslant 6)$ we have

$$3x_1x_2 + 2x_1x_3 \neq \sum_{i=1}^{3} f_i(x_i) + f_4(3x_1 + x_2 + x_3) + f_5(x_1 + 3x_2 + x_3) + f_6(3x_1 + 3x_2 + 2x_3).$$

Indeed, it is enough to consider the case $f_i = b_i z^2$ $(1 \leqslant i \leqslant 6)$. Assuming the equality in (33) we obtain comparing the coefficients of x_1x_2, x_1x_3 and x_2x_3

$$\begin{aligned} 6b_4 + 6b_5 + 18b_6 &= 3, \\ 6b_4 + 2b_5 + 12b_6 &= 2, \\ 2b_4 + 6b_5 + 12b_6 &= 0, \end{aligned}$$

which is impossible, since

$$\begin{vmatrix} 6 & 6 & 18 \\ 6 & 2 & 12 \\ 2 & 6 & 12 \end{vmatrix} = 0, \qquad \begin{vmatrix} 6 & 6 & 3 \\ 6 & 2 & 2 \\ 2 & 6 & 0 \end{vmatrix} \neq 0.$$

I conclude by expressing my thanks to U. Zannier for a remark helpful in the proof of Theorem 5.

Note added in proof. M. Kula has checked that $M(2, d, K) = d$ in the simplest cases not covered by Theorems 4 and 5: $d = 7$ or 8, $K = \mathbb{F}_{11}$.

References

[1] N. Alon, M. B. Nathanson, I. Ruzsa, *The polynomial method and restricted sums of congruence classes*. J. Number Theory 56 (1996), 404–417.

[2] P. Diaconis, M. Shahshahani, *On nonlinear functions of linear combinations*. SIAM J. Sci. Statist. Comput. 5 (1984), 175–191.

[3] W. J. Ellison, *A 'Waring's problem' for homogeneous forms*. Proc. Cambridge Philos. Soc. 65 (1969), 663–672.

[4] U. Helmke, *Waring's problem for binary forms*. J. Pure Appl. Algebra 80 (1992), 29–45.

[5] A. Iarrobino, *Inverse system of a symbolic power II. The Waring problem for forms*. J. Algebra 174 (1995), 1091–1110.

[6] B. F. Logan, L. A. Shepp, *Optimal reconstruction of a function from its projections*. Duke Math. J. 42 (1975), 645–659.

[7] T. Muir, *A Treatise on the Theory of Determinants*. Dover, New York 1960.

[8] B. Reznick, *Sums of powers of complex linear forms*. Unpublished manuscript of 1992.

Originally published in
Dissertationes Mathematicae 434 (2005)

On weak automorphs of binary forms over an arbitrary field

To Jerzy Browkin on his 70th birthday

Contents

Introduction

The present paper deals with the circle of problems considered by several mathematicians, beginning with F. Klein in 1876 and ending with L. Summerer in 2004. Even before Klein's fundamental paper [15], A. Clebsch and P. Gordan [6] in 1867 and A. Clebsch [5] in 1872 made important contributions to one of the problems in question without formulating it explicitly.

Let K be a field of characteristic $\pi \geqslant 0$, $T \in \mathrm{GL}_2(K)$ and $f \in K[x, y]$ be a form such that

$$f(T(x, y)) = rf(x, y), \qquad \text{where } r \in K^*.$$

Segre [22] calls T a *weak automorph* of f ("automorfismo in senso lato"), as opposed to a *strict automorph* ("automorfismo in senso stritto"), for which $r = 1$, and considers for $K = \mathbb{Q}$ the quotient group $\mathrm{Aut}(f, K)$ (notation mine, some authors denote similarly the group of strict automorphs) of the group of all weak automorphs of f defined over K divided by the group of trivial weak automorphs, given by $T(x, y) = (\varrho x, \varrho y)$ for $\varrho \in K^*$ (this definition extends immediately to forms defined over any field L containing K; then $r \in L^*$).

Segre determines the forms $f \in \mathbb{Q}[x, y]$ such that $\mathrm{Aut}(f, \mathbb{Q})$ contains a given non-trivial group $\mathcal{G}$ of one of the possible eight types: cyclic of order 2, 3, 4, 6 and dihedral of order 4, 6, 8, 12. For every group $\mathcal{G}$ Segre takes a convenient conjugate in the group $\mathrm{PGL}_2(\mathbb{Q})$, which simplifies calculation. Earlier for $\mathbb{C}$ instead of $\mathbb{Q}$ a similar result was obtained by Klein [16, Chapter 2]: here all cyclic and dihedral groups are possible and,

in addition, three polyhedral groups. Dickson [9], [10] obtained analogous results for K being a finite field. For a modern treatment of the case $K = \mathbb{C}$, see Huffman [14].

The characterization of forms in question given by Klein and Segre is the following ($K = \mathbb{C}$ or $\mathbb{Q}$, $\overline{K}$ is an algebraic closure of K).

For a given finite subgroup $\mathcal{G}$ of $\mathrm{PGL}_2(K)$ of order $|\mathcal{G}| = \nu$ all forms $f \in K[x, y]$ for which $\mathcal{G} \subset \mathrm{Aut}(f, K)$ and only those are expressible as

$$f(x, y) = \prod_{i=1}^{h} \chi_i(x, y)^{c_i} \psi(p(x, y), q(x, y)),$$

where $p, q \in K[x, y]$, $\chi_i \in \overline{K}[x, y]$ are forms determined by $\mathcal{G}$; p, q are of degree ν, χ_i are of degree ν/m_i, c_i are integers satisfying $0 \leqslant c_i < m_i$ and if χ_i, χ_j are conjugate over K, then $c_i = c_j$; ψ is a binary form over K. Klein's proof is not rigorous and in Segre's proof given in Subsection 19 of [22] several details are missing. In particular, no connection is indicated between p, q and χ_i. On the other hand, in Subsections 20 and 24, 29 of [22] Segre explicitly determines p, q and χ_i for every $\mathcal{G}$ up to conjugation.

Having proved in §1 of the present paper several lemmas about $\mathrm{PGL}_2(K)$ we determine in §2 the forms p, q and χ_i for every cyclic subgroup of $\mathrm{PGL}_2(K)$ with a given generator (Theorem 1). Then we prove an analogue of the above result of Klein, Dickson and Segre for an arbitrary field K (Theorems 2 and 3). Consideration of fields K that are not perfect is the only novel feature of this proof. As an application we prove in §3 an upper bound for the order of $\mathrm{Aut}(f, K)$ (Theorems 4 and 5). The bound is sharp for every π and for $\pi = 0$ it is better for $\deg f > 12$ than Olver's bound [19], [1].

In Subsections 22–23 of [22] Segre gives a method to decide whether a given cubic or quadratic binary form f over $\mathbb{Q}$ has a strict non-trivial automorph defined over $\mathbb{Q}$, the only trivial automorph being here the identity. The method involves invariants and covariants of f. In §4 we consider an analogous question for weak automorphs defined over K and give an answer in terms of the Galois group $\mathrm{Gal}(f, K)$ of the polynomial $f(x, 1)$ over K (Theorem 6). For cubic forms and $K = \mathbb{Q}$ a necessary and sufficient condition (if f is irreducible, the discriminant of f has to be a square in $\mathbb{Q}$) has been given in a recent unpublished manuscript of A. Choudhry [4]. For forms of odd degree with non-zero discriminant (in what follows called *non-singular*), existence of a weak non-trivial automorph is equivalent to existence of a strict non-trivial automorph (see [22, p. 40] and [20, Theorem 3.5]), but it is not obvious that Choudhry's condition and Segre's condition ([22, p. 48]) are equivalent. For non-singular cubic forms with $f(1, 0) \neq 0$ the structure of $\mathrm{Gal}(f, K)$ determines the isomorphism class of $\mathrm{Aut}(f, K)$, for quartic forms it does not in general. On the other hand, for K algebraically closed and f a non-singular quartic, the isomorphism class of $\mathrm{Aut}(f, K)$ is determined by invariants of f (§5, Theorem 7). For $K = \mathbb{C}$ this is well known ([1, Example 3.6], cf. also [24, Proposition 3.2]), but at least for char $K = 2, 3$ it seems new.

For forms f of degree 5 a characterization of the isomorphism class of $\mathrm{Aut}(f, \mathbb{C})$ by invariants and covariants of f can be deduced from the work of Clebsch and Gordan [6] and of Clebsch [5] on the so called typical representations of binary forms. For f non-singular of degree 6 a characterization of the isomorphism class of $\mathrm{Aut}(f, \mathbb{C})$ by covariants

of f was obtained by Maiasano [17] and one by invariants of f by Bolza [2]. Recently a practical way of finding $\mathrm{Aut}(f, \mathbb{C})$ by means of covariants of f has been proposed by Berchenko and Olver [1]. However, it is not clear from it whether for non-singular forms f of degree greater than 6 the condition $|\mathrm{Aut}(f, K)| > 1$ can be characterized by invariants of f. We shall show (Theorem 8) that the set of forms $f \in \mathbb{C}[x, y]$ with $|\mathrm{Aut}(f, \mathbb{C})| > 1$ is Zariski closed only for $n \leqslant 5$.

I conclude this introduction by expressing my thanks to A. Choudhry for sending me his unpublished manuscript [4] as well as a copy of [2], to A. Pokrzywa for factoring several multivariate polynomials that appeared in an earlier version of the paper and to A. Sładek who suggested many corrections and a simplification.

1. Lemmas on $\mathrm{PGL}_2(K)$

Definition 1. Let K be a field of characteristic π. If

$$T_0(x, y) = (\alpha x + \beta y,\ \gamma x + \delta y) \in \mathrm{GL}_2(K),$$

the image of T_0 in $\mathrm{PGL}_2(K)$ will be denoted by $T = \left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)K^*$, or if $\mathrm{PGL}_2(K)$ is represented as the group of fractional linear transformations, by T^*. The order of T in $\mathrm{PGL}_2(K)$ will be denoted by $o(T)$, the unit element by E. Moreover, ζ_ν is a primitive root of unity of order ν in $\overline{K}$, if it exists.

Lemma 1. $\mathrm{PGL}_2(K)$ *contains an element of order* $\nu > 1$ *if and only if either* $\nu = \pi$, *or* $\nu \not\equiv 0 \bmod \pi$ *and* $\zeta_\nu + \zeta_\nu^{-1} \in K$. *If this condition is satisfied, then* $\mathrm{PGL}_2(K)$ *contains a dihedral group of order* 2ν *except for* $K = \mathbb{F}_2$, $\nu = 2$.

Proof. Let $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)K^*$ be an element of order $\nu > 1$ in $\mathrm{PGL}_2(K)$. By the Jordan normal form theorem (see [26, §88]) there exist a, b, c, d in $\overline{K}$ such that $ad - bc \neq 0$ and

$$\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} = \begin{pmatrix}a & b\\ c & d\end{pmatrix}^{-1}\begin{pmatrix}\lambda_1 & \mu\\ 0 & \lambda_2\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix},$$

where $\lambda_1\lambda_2 \neq 0$ and either $\mu = 0$, or $\lambda_1 = \lambda_2 = \lambda$ and $\mu = 1$. In the former case λ_1/λ_2 is a primitive root of unity ζ of order ν, hence $\nu \not\equiv 0 \bmod \pi$ and

$$\lambda_2(1 + \zeta) = \lambda_1 + \lambda_2 = \mathrm{Tr}\begin{pmatrix}\lambda_1 & \mu\\ 0 & \lambda_2\end{pmatrix} = \mathrm{Tr}\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} = \alpha + \delta \in K,$$

$$\lambda_2^2\zeta = \lambda_1\lambda_2 = \begin{vmatrix}\lambda_1 & \mu\\ 0 & \lambda_2\end{vmatrix} = \begin{vmatrix}\alpha & \beta\\ \gamma & \delta\end{vmatrix} = \alpha\delta - \beta\gamma \in K.$$

Hence $\zeta + \zeta^{-1} = (\lambda_2(1 + \zeta))^2/\lambda_2^2\zeta - 2 \in K$. In the latter case

$$\begin{pmatrix}\lambda_1 & \mu\\ 0 & \lambda_2\end{pmatrix}^\nu = \begin{pmatrix}\lambda^\nu & \nu\lambda^{\nu-1}\\ 0 & \lambda^\nu\end{pmatrix},$$

hence $\nu = \pi$.

If the asserted condition is satisfied, then $\mathrm{PGL}_2(K)$ contains a dihedral group of order 2ν generated by

$$\begin{pmatrix} 1+\zeta+\zeta^{-1} & -1 \\ 1 & 1 \end{pmatrix} K^* \text{ and } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} K^* \quad \text{if } \nu \not\equiv 0 \bmod \pi,$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} K^* \text{ and } \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} K^* \quad \text{if } \nu = \pi \neq 2,$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} K^* \text{ and } \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} K^* \quad \text{if } \nu = \pi = 2,\ a \in K \setminus \mathbb{F}_2. \qquad \square$$

Remark 1. For $K = \mathbb{Q}$ Lemma 1 has been proved by Segre in Subsection 9 of [22].

Lemma 2. $\mathrm{PGL}_2(K)$ *contains a subgroup isomorphic to* $\mathfrak{A}_4$ *if and only if either* $\pi \neq 2$ *and* level $K \leqslant 2$, *or* $\pi = 2$ *and* $\mathbb{F}_4 \subset K$. *If and only if the former condition is satisfied,* $\mathrm{PGL}_2(K)$ *contains a subgroup isomorphic to* $\mathfrak{S}_4$.

$\mathrm{PGL}_2(K)$ *contains a subgroup isomorphic to* $\mathfrak{A}_5$ *if and only if either* $\pi \neq 2$, level $K \leqslant 2$ *and* $\sqrt{5} \in K$, *or* $\pi = 2$ *and* $\mathbb{F}_4 \subset K$.

Remark 2. The *level* of a field K is the minimal number k such that for some $x_i \in K$ we have $x_1^2 + \ldots + x_k^2 = -1$.

Proof. If $\pi = 3$ the condition on the level is trivially satisfied, so assume $\pi \neq 3$ and let M be a matrix over K such that MK^* is of order 3 in $\mathrm{PGL}_2(K)$. Then M is equivalent over $\overline{K}$ to a matrix $\left(\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right)$, where λ_1/λ_2 is a primitive root of unity ζ of order 3 and $M(1+\zeta^{-1})/\lambda_2$ is equivalent over $\overline{K}$ to

$$\begin{pmatrix} 1+\zeta & 0 \\ 0 & 1+\zeta^{-1} \end{pmatrix} = \begin{pmatrix} 1 & -\zeta^2 \\ 1 & -\zeta \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -\zeta^2 \\ 1 & -\zeta \end{pmatrix}^{-1}.$$

But (see the proof of Lemma 1) $\lambda_2(1+\zeta) \in K$ and $(1+\zeta^2)/\zeta \in K$, hence, on division, $\lambda_2/(1+\zeta^{-1}) \in K$ and $M(1+\zeta^{-1})/\lambda_2$ is defined over K. It follows that

$$M\,\frac{1+\zeta^{-1}}{\lambda_2} \text{ is equivalent to } \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \text{ over } K.$$

Hence a subgroup of $\mathrm{PGL}_2(K)$ isomorphic to $\mathfrak{A}_4$ is conjugate to a subgroup $\mathcal{G}$ containing $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)K^* = T$. Thus there exists $S \in \mathcal{G}$ such that

$$S^2 = E \quad \text{and} \quad TST = ST^{-1}S.$$

Taking $S = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)K^*$ we obtain by calculation $\delta = -\alpha$, $(2\alpha+\gamma-\beta)^2 + \beta^2 + \gamma^2 = 0$ and if $\pi = 2$, then $\beta^2 - \beta\gamma + \gamma^2 = 0$. Thus level $K \leqslant 2$ and if $\pi = 2$, then β/γ is a primitive root of unity of order 3, hence $\mathbb{F}_4 \subset K$.

In the opposite direction, if $\pi = 2$ and ζ is a primitive root of unity of order 3, then the group

$$\left\langle \begin{pmatrix} 0 & \zeta \\ 1 & 0 \end{pmatrix} K^*, \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} K^* \right\rangle$$

is isomorphic to $\mathfrak{A}_4$. If $\pi \neq 2$, then the assumption that level $K \leqslant 2$ implies existence of x_1, x_2 in K such that $x_1^2 + x_2^2 + 1 = 0$. Then the group generated by

$$S = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} K^*, \quad T = \begin{pmatrix} x_1 & x_2 + 1 \\ x_2 - 1 & -x_1 \end{pmatrix} K^*$$

is isomorphic to $\mathfrak{S}_4$. Indeed, $S^4 = E$, $T^2 = E$ and $(ST)^3 = E$, which gives the required property (see [7, Table 1]). If $\pi = 2$, then $\mathrm{PGL}_2(K)$ does not contain a subgroup isomorphic to $\mathfrak{S}_4$ since, by Lemma 1, it contains no element of order 4.

Assume now that $\mathrm{PGL}_2(K)$ contains a subgroup isomorphic to $\mathfrak{A}_5$. Since $\mathfrak{A}_5$ contains $\mathfrak{A}_4$ and $\mathfrak{C}_5$, it follows from the already proved part of the lemma and from Lemma 1 that either $\pi \neq 2$ and level $K \leqslant 2$, or $\pi = 2$ and $\mathbb{F}_4 \subset K$; moreover, either $\zeta + \zeta^{-1} \in K$, where ζ is a primitive root of unity of order 5, or $\pi = 5$. If $\pi = 2$ and $\mathbb{F}_4 \subset K$, then $\mathrm{PGL}_2(K)$ contains an isomorphic image of $\mathrm{PGL}_2(\mathbb{F}_4) \cong \mathfrak{A}_5$; if $\pi \neq 2$, then the condition $\zeta + \zeta^{-1} \in K$ implies $\varrho = (\sqrt{5} - 1)/2 \in K$, which also holds for $\pi = 5$. Conversely, if $\sqrt{5} \in K$ and level $K \leqslant 2$, we have $x_1^2 + x_2^2 + 1 = 0$ for some x_1, x_2 in K, hence the group $\langle R, S \rangle$, where

$$R = \begin{pmatrix} -1 + x_2\varrho & x_1 + x_2\varrho - \varrho - 1 \\ 2 & 1 - x_2\varrho \end{pmatrix} K^*, \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} K^*,$$

is isomorphic to $\mathfrak{A}_5$, provided

$$\begin{vmatrix} -1 + x_2\varrho & x_1 + x_2\varrho - \varrho - 1 \\ 2 & 1 - x_2\varrho \end{vmatrix} = -x_2^2\varrho^2 - 2x_1 + 2\varrho + 2 \neq 0,$$

and this follows from $\pi \neq 2$ if $x_1 = 0$, while it can be achieved by changing the sign of x_1 if $x_1 \neq 0$. Indeed, we have $R^2 = E$, $S^3 = E$ and $(RS)^5 = E$, which implies $\langle R, S \rangle \cong \mathfrak{A}_5$ (see [7, Table 5]). □

Remark 3. Lemma 2 in an equivalent formulation is given without proof by Serre [23]. Segre only proves ([22, Subsection 12]) that if K is real, then $\mathrm{PGL}_2(K)$ does not contain a copy of $\mathfrak{A}_4$.

Lemma 3. *Let $\mathcal{G}$ be a non-trivial subgroup of* $\mathrm{PGL}_2(K)$. *If for all elements S of $\mathcal{G} \setminus \{E\}$ the equation $S^*\xi = \xi$ has exactly one solution in $\overline{K} \cup \{\infty\}$, then $\pi > 0$ and $\mathcal{G}$ is a π-group. Every such finite group is generated by elements*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} \lambda_i & 1 \\ 0 & \lambda_i \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} K^* \quad (1 \leqslant i \leqslant g)$$

where $ad - bc \neq 0$, the λ_i^{-1} are linearly independent over $\mathbb{F}_\pi$ and either a, b, c, d, λ_i belong to K, or $\pi = 2$, $a = 0$, $b = 1$, $c \in K$, $K(d)$ is a quadratic inseparable extension of K and $\lambda_i + d \in K$. Every infinite π-group contained in $\mathrm{PGL}_2(K)$ *contains the above finite groups for all g.*

Proof. Let $S_1 = \left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)K^* \in \mathcal{G} \setminus \{E\}$, hence $\alpha\delta - \beta\gamma \neq 0$. By the Jordan normal form theorem there exists a non-singular matrix $\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$ over $\overline{K}$ such that

$$\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} = \begin{pmatrix}a & b\\ c & d\end{pmatrix}^{-1}\begin{pmatrix}\lambda & \mu\\ 0 & \nu\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix},$$

where $\lambda\nu \neq 0$ and either $\mu = 0$, or $\lambda = \nu$ and $\mu = 1$. In the former case the equation $S_1^*\xi = \xi$ has two solutions in $\overline{K} \cup \{\infty\}$, namely $-b/a$ and $-d/c$. Since the case $\lambda = \nu$, $\mu = 0$ is excluded by the assumption $S_1 \neq E$, we obtain $\mu = 1$ and

$$4\lambda^2 = (\alpha + \delta)^2 = 4(\alpha\delta - \beta\gamma). \tag{1}$$

The second equality of (1) holds for all elements S of $\mathcal{G}$. Let

$$S = \begin{pmatrix}a & b\\ c & d\end{pmatrix}^{-1}\begin{pmatrix}\varepsilon & \zeta\\ \eta & \vartheta\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}K^* \in \mathcal{G} \setminus \{E\}.$$

Since $S_1^i S \in \mathcal{G}$ and

$$\begin{pmatrix}\lambda & i\\ 0 & \lambda\end{pmatrix}\begin{pmatrix}\varepsilon & \zeta\\ \eta & \vartheta\end{pmatrix} = \begin{pmatrix}\lambda\varepsilon + i\eta & \lambda\zeta + i\vartheta\\ \lambda\eta & \lambda\vartheta\end{pmatrix}$$

we obtain from (1)

$$(\lambda\varepsilon + \lambda\vartheta + i\eta)^2 = 4\lambda^2(\varepsilon\vartheta - \eta\zeta) \quad (i = 0, 1, 2),$$

hence

$$\eta = 0, \quad \varepsilon = \vartheta, \quad \zeta \neq 0,$$

hence S is of infinite order in $\mathrm{PGL}_2(K)$ unless $\pi > 0$, in which case $S^\pi = E$ and $\mathcal{G}$ is a π-group. This proves the first part of the lemma.

In order to prove the second part let us again consider S_1. The condition $S_1^\pi = E \neq S_1$ implies in the above notation

$$\lambda^\pi = \nu^\pi, \quad \mu \neq 0,$$

hence $\lambda = \nu =: \lambda_1$ and $\mu = 1$. It follows that we have again equation (1) and for every S in $\mathcal{G}$,

$$S = \begin{pmatrix}a & b\\ c & d\end{pmatrix}^{-1}\begin{pmatrix}\varepsilon & \zeta\\ 0 & \varepsilon\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}K^*.$$

If $\lambda_1 \in K$, then a, b, c, d can be chosen in K and hence $\varepsilon, \zeta \in K$ and

$$S = \begin{pmatrix}a & b\\ c & d\end{pmatrix}^{-1}\begin{pmatrix}1 & \zeta/\varepsilon\\ 0 & 1\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}K^*.$$

For S running through $\mathcal{G}$, ζ/ε runs through a linear space L over $\mathbb{F}_\pi$ and letting $\lambda_1^{-1}, \ldots, \lambda_g^{-1}$ be a basis of this space we obtain the assertion of the lemma.

If $\lambda_1 \notin K$, then the polynomial $z^2 - (\alpha + \delta)z + (\alpha\delta - \beta\gamma)$ is irreducible inseparable over K, hence $\pi = 2$, $\gamma \neq 0$ and we can choose $a = 0$, $b = 1$, $c = \gamma$, $d = \lambda_1 - \alpha$. Then

the condition $S \in \mathrm{PGL}_2(K)$ gives $\varepsilon + d\zeta \in K$, $d^2\zeta \in K$, hence $\zeta \in K$ and

$$S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} \varepsilon/\zeta & 1 \\ 0 & \varepsilon/\zeta \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} K^*.$$

Taking again a basis $\lambda_1^{-1}, \ldots, \lambda_g^{-1}$ of L we obtain $\lambda_i + d \in K$, which completes the proof for finite groups $\mathcal{G}$. If $\mathcal{G}$ is infinite, so is L and for every g it contains $\lambda_1^{-1}, \ldots, \lambda_g^{-1}$ linearly independent. □

Lemma 4. *Let $\mathcal{G}$ be a non-trivial finite subgroup of* $\mathrm{PGL}_2(K)$ *and let*

$$O(\mathcal{G}) = \bigcup_{S \in \mathcal{G} \setminus \{E\}} \left\{ \xi \in \overline{K} \cup \{\infty\} : S^*\xi = \xi \right\}.$$

If $\mathcal{G}$ is not a π-group, then the number h of orbits of $O(\mathcal{G})$ under the action of $\mathcal{G}$ is either two or three.

Proof. Let the orbits in question be $O_1, \ldots, O_h$. For each $\xi \in O_i$ the number $|\{S \in \mathcal{G} : S^*\xi = \xi\}|$ is the same, say ν_i. Clearly $|\mathcal{G}| = \nu_i \mu_i$, where $\mu_i = |O_i|$ and

$$\sum_{i=1}^{h} (\nu_i - 1)\mu_i = \sum_{\xi \in \overline{K} \cup \{\infty\}} \sum_{\substack{S \in \mathcal{G} \setminus \{E\} \\ S^*\xi = \xi}} 1 = \sum_{S \in \mathcal{G} \setminus \{E\}} \sum_{\substack{\xi \in \overline{K} \cup \{\infty\} \\ S^*\xi = \xi}} 1.$$

But for each $S \in \mathcal{G} \setminus \{E\}$ the equation $S^*\xi = \xi$ has in $\overline{K} \cup \{\infty\}$ either one or two solutions and, by Lemma 3, the latter possibility occurs at least once. It follows that

$$2|\mathcal{G}| - 2 \geqslant \sum_{i=1}^{h} (\nu_i - 1)\, \mu_i > |\mathcal{G}| - 1.$$

Since

$$\sum_{i=1}^{h} (\nu_i - 1)\mu_i = h|\mathcal{G}| - \sum_{i=1}^{h} \mu_i \in \left[\frac{h}{2} |\mathcal{G}|,\ h|\mathcal{G}| - h \right],$$

we obtain $2 \leqslant h \leqslant 3$. □

Remark 4. For $K = \mathbb{C}$ and $K = \mathbb{F}_\pi$, $|\mathcal{G}| \not\equiv 0 \bmod \pi$, Lemma 4 and the above proof are well known (see [27, Vol. II, §68 and §87].

Lemma 5. *In the notation of the proof of Lemma* 4, *if $T \in \mathcal{G}$, $\xi \in O_j$ and $T^*\xi = \xi$, then $o(T) \mid |\mathcal{G}|/|O_j|$.*

Proof. The group $\langle T \rangle$ of order $o(T)$ is a subgroup of the stabilizer of ξ in $\mathcal{G}$ of order $|\mathcal{G}|/|O_j|$. □

Lemma 6. *Under the assumptions of Lemma* 4, *let* $K_j = K(O_j \setminus \{\infty\})$. *Then* $[K_j : K] \leqslant 2$ *for all* $j \leqslant h$. *We have the following possibilities*:

(2) *for all* $j \leqslant h$ *either* $[K_j : K]_s = 1$ *or* $[K_j : K]_s = 2$, $\infty \notin O_j$, $\mathrm{Gal}(K_j/K) = \langle \sigma_j \rangle$, *and* $\sigma_j(O_j) = O_j$;

(3) *for a suitable numbering of* O_j, $[K_1 : K]_s = 2, \mathrm{Gal}(K_1/K) = \langle \sigma_1 \rangle$, $\infty \notin O_1$, $\sigma_1(O_1) = O_2$ *and either* $h = 2$, *or* $h = 3, [K_3 : K]_s = 1$, *or* $h = 3, [K_3 : K]_s = 2$, $\mathrm{Gal}(K_3/K) = \langle \sigma_3 \rangle, \infty \notin O_3, \sigma_3(O_3) = O_3$.

Proof. If $\xi \in O(\mathcal{G}) \setminus \{\infty\}$, then $S^*\xi = \xi$ for an $S \in \mathcal{G}$, hence $[K(\xi) : K] \leqslant 2$ and if $\xi \in O_j$, then $[K_j : K] \leqslant 2$. If $[K_j : K] = 2$, then $\infty \notin O_j$ since $S^*(\infty) \in K \cup \{\infty\}$ for all $S \in \mathcal{G}$. If (2) does not hold, then for some j we have $[K_j : K]_s = 2, \mathrm{Gal}(K_j/K) = \langle \sigma_j \rangle$ and $\sigma_j(O_j) \neq O_j$. Therefore, there exists $\xi_0 \in O_j$ such that $\sigma_j(\xi_0) \notin O_j$. But $S_0^*\xi_0 = \xi_0$ for some $S_0 \in \mathcal{G} \setminus \{E\}$; then also $S_0^*\sigma_j(\xi_0) = \sigma_j(\xi_0)$, hence $\sigma_j(\xi_0) \in O_k$ for some $k \neq j$ and renumbering the O_i we may assume that $j = 1$, $k = 2$, $\sigma_1(O_1) = O_2$. If $h = 3$ the situation cannot repeat itself with $j = 3$ since there exists no suitable k, thus either $[K_3 : K]_s = 1$, or $[K_3 : K]_s = 2$, $\mathrm{Gal}(K_3/K) = \langle \sigma_3 \rangle$ and $\sigma_3(O_3) = O_3$. This gives (3). □

Lemma 7. *For every finite subgroup* $\mathcal{G}$ *of* $\mathrm{PGL}_2(K)$ *of order not divisible by* π *the sequence* $\langle |O_1|, \ldots, |O_h| \rangle$ *in the notation of the proof of Lemma* 4 *is a permutation of one of the sequences*: $\langle 1, 1 \rangle$ ($\mathcal{G} \cong \mathfrak{C}_\nu$), $\langle |\mathcal{G}|/2, |\mathcal{G}|/2, 2 \rangle$ ($\mathcal{G} \cong \mathfrak{D}_\nu$), $\langle 4, 4, 6 \rangle$ ($\mathcal{G} \cong \mathfrak{A}_4$), $\langle 6, 8, 12 \rangle$ ($\mathcal{G} \cong \mathfrak{S}_4$), $\langle 12, 20, 30 \rangle$ ($\mathcal{G} \simeq \mathfrak{A}_5$).

Proof. If $|\mathcal{G}| \not\equiv 0 \bmod \pi$, then by Lemma 3 for every $S \in \mathcal{G} \setminus \{E\}$ the number of solutions of $S^*\xi = \xi$ is 2, hence following the proof of Lemma 4 we obtain

$$2|\mathcal{G}| - 2 = \sum_{i=1}^{h} (\nu_i - 1)\mu_i = h|\mathcal{G}| - \sum_{i=1}^{h} |\mathcal{G}|/\nu_i$$

for $h = 2$ or 3. This equation is well known (see [27, Vol. II, §68]) and gives for decreasing ν_i either $h = 2$, $\nu_1 = \nu_2 = |\mathcal{G}|$, or $h = 3$, $\langle \nu_1, \nu_2, \nu_3 \rangle = \langle |\mathcal{G}|/2, 2, 2 \rangle$, or $h = 3$, $\langle |\mathcal{G}|; \nu_1, \nu_2, \nu_3 \rangle = \langle 12; 3, 3, 2 \rangle$, $\langle 24; 4, 3, 2 \rangle$, $\langle 60; 5, 3, 2 \rangle$. Since $\mu_i = |\mathcal{G}|/\nu_i$ we obtain the lemma. □

Lemma 8. *Let* $\mathcal{G} = \mathrm{PSL}_2(\mathbb{F}_q)$. *In the notation of Lemma* 4 *we have*

$$O(\mathcal{G}) = \mathbb{F}_{q^2} \cup \{\infty\} \tag{4}$$

and, up to a permutation, $O_1 = \mathbb{F}_q \cup \{\infty\}$, $O_2 = \mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

Proof. The formulae

$$S \in \mathcal{G} \setminus \{E\}, \quad \xi \in \overline{\mathbb{F}}_q \cup \{\infty\}, \quad S^*\xi = \xi \tag{5}$$

imply $\xi \in \mathbb{F}_{q^2} \cup \{\infty\}$. On the other hand, if $\xi \in \mathbb{F}_q$ or $\xi \in \mathbb{F}_{q^2}, \xi^2 + a\xi + b = 0, a, b \in \mathbb{F}_q$,

or $\xi = \{\infty\}$, then (5) holds for

$$S = \begin{pmatrix} 1+\xi & -\xi^2 \\ 1 & 1-\xi \end{pmatrix}\mathbb{F}_q^* \quad \text{or} \quad \begin{pmatrix} \alpha\varepsilon^{-1} & -b\varepsilon^{-1} \\ \varepsilon^{-1} & \alpha\varepsilon^{-1}+a\varepsilon^{-1} \end{pmatrix}\mathbb{F}_q^* \quad \text{or} \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\mathbb{F}_q^*,$$

respectively, where α and ε are chosen in $\mathbb{F}_q$ so that $\alpha^2 + a\alpha + b = \varepsilon^2$; $\varepsilon \neq 0$ since $x^2 + ax + b$ is irreducible over $\mathbb{F}_q$. This proves (4).

Moreover, if $\xi = 0$, $S = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)\mathbb{F}_q^*$ or $\xi \in \mathbb{F}_q^*$, $S = \left(\begin{smallmatrix} \xi & 0 \\ 1 & \xi^{-1} \end{smallmatrix}\right)\mathbb{F}_q^*$, we have

$$S \in \mathcal{G}, \quad S^*\infty = \xi.$$

Finally, if $\xi, \eta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and ξ', η' are conjugates of ξ, η with respect to $\mathbb{F}_q$ we have $(\eta - \eta')/(\xi - \xi') \in \mathbb{F}_q$. There exist δ, ε in $\mathbb{F}_q$ such that

$$\frac{\eta - \eta'}{\xi - \xi'}(\delta + \xi)(\delta + \xi') = \varepsilon^2 \neq 0.$$

Then taking

$$S = \begin{pmatrix} \dfrac{\delta(\eta - \eta') + (\eta\xi - \eta'\xi')}{\varepsilon(\xi - \xi')} & \dfrac{\delta(\eta'\xi - \eta\xi') + \xi\xi'(\eta' - \eta)}{\varepsilon(\xi - \xi')} \\ \varepsilon^{-1} & \delta\varepsilon^{-1} \end{pmatrix}\mathbb{F}_q^*$$

we find $S \in \mathcal{G}$ such that $S^*\xi = \eta$, which completes the proof. □

Lemma 9. *The statement of Lemma* 8 *is also true for* $\mathcal{G} = \mathrm{PGL}_2(\mathbb{F}_q)$.

Proof. If $\mathcal{H}_1 = \mathrm{PGL}_2(\mathbb{F}_q)$, $\mathcal{H}_2 = \mathrm{PSL}_2(\mathbb{F}_q)$ we have, in the notation of Lemma 4,

$$O(\mathcal{H}_2) \subset O(\mathcal{H}_1);$$

but, clearly, $O(\mathcal{H}_1) \subset \mathbb{F}_{q^2} \cup \{\infty\}$, hence by Lemma 8,

$$O(\mathcal{H}_1) = \mathbb{F}_{q^2} \cup \{\infty\}.$$

Since $\mathcal{H}_2 \subset \mathcal{H}_1$ the orbits of $\mathbb{F}_{q^2} \cup \{\infty\}$ under the action of $\mathcal{H}_1$ are unions of orbits under the action of $\mathcal{H}_2$; Lemma 8 shows that they are either $\mathbb{F}_q \cup \{\infty\}$ and $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$, or $\mathbb{F}_{q^2} \cup \{\infty\}$. As the image of $\mathbb{F}_q \cup \{\infty\}$ under the action of $\mathcal{H}_1$ is again $\mathbb{F}_q \cup \{\infty\}$, the former case holds. □

Definition 2. If K, L are fields, $K \subset L$ and $\mathcal{G}$ is a subgroup of $\mathrm{PGL}_2(K)$, then $\mathcal{G}L^*/L^*$ is the subgroup of $\mathrm{PGL}_2(L)$ defined as

$$\{ML^* : M \in \mathrm{GL}_2(K),\ MK^* \in \mathcal{G}\}.$$

Lemma 10. *For* $\pi > 0$ *every finite subgroup of* $\mathrm{PGL}_2(K)$ *is isomorphic to a subgroup of* $\mathrm{PSL}_2(\mathbb{F}_s)$*, where* s *is a power of* π.

Proof. Let $\mathcal{G} = \left\{\left(\begin{smallmatrix} \alpha_i & \beta_i \\ \gamma_i & \delta_i \end{smallmatrix}\right)K^* : 1 \leqslant i \leqslant k\right\}$. The isomorphism class of $\mathcal{G}$ is determined by finitely many equalities $F_i(\alpha_1, \ldots, \delta_k) = 0$ and inequalities $G_j(\alpha_1, \ldots, \delta_k) \neq 0$, where F_i and G_j are polynomials over $\mathbb{F}_\pi$. By the theorem on elimination of existential

quantifiers in algebraically closed fields, if this system of equalities and inequalities is solvable in K, it is also solvable in the algebraic closure of $\mathbb{F}_\pi$, hence also in a field $\mathbb{F}_q$, where q is a power of π. Thus $\mathcal{G}$ is isomorphic to a subgroup of $\mathrm{PGL}_2(\mathbb{F}_q)$. Since for $s = q^2$, $\mathrm{PGL}_2(\mathbb{F}_q)\mathbb{F}_s^*/\mathbb{F}_s^*$ is contained in $\mathrm{PSL}_2(\mathbb{F}_s)$, it follows that s satisfies the assertion of the lemma. □

Lemma 11. *For $\pi > 0$ and a finite subgroup $\mathcal{G}$ of $\mathrm{PGL}_2(K)$ of order divisible exactly by π^g $(g > 0)$ let σ be the number of π-Sylow subgroups in $\mathcal{G}$. We have the following possibilities*:

$$\begin{aligned}
&\sigma = 1;\\
&\sigma = \pi^g + 1, \quad \mathcal{G} \cong \mathrm{PGL}_2(\mathbb{F}_{\pi^g}) \text{ or } \mathrm{PSL}_2(\mathbb{F}_{\pi^g});\\
&\pi^g = 2, \quad \sigma = 2\varrho + 1\ (\varrho \geqslant 1), \quad \mathcal{G} \cong \mathfrak{D}_{2\varrho+1};\\
&\pi^g = 3, \quad \sigma = 10, \quad \mathcal{G} \cong \mathfrak{A}_5.
\end{aligned}$$

Proof. In view of Lemma 10 this follows from an analogous property of subgroups of $\mathrm{PSL}_2(\mathbb{F}_s)$ (see [12, Chapter XII, Sections 249–253], with m replaced by g and f by ϱ). □

Lemma 12. *Let $\mathcal{H}_1 = \mathrm{PGL}_2(\mathbb{F}_q)$ and $\mathcal{H}_2 = \mathrm{PSL}_2(\mathbb{F}_q)$, where $q = \pi^g$. Every subgroup of $\mathrm{PGL}_2(\overline{K})$ isomorphic to $\mathcal{H}_i$ is conjugate to $\mathcal{H}_i\overline{K}^*/\overline{K}^*$.*

Proof. The existence of a subgroup of $\mathrm{PGL}_2(\overline{K})$ isomorphic to $\mathcal{H}_i$, but not conjugate to $\mathcal{H}_i\overline{K}^*/\overline{K}^*$, is a statement involving finitely many existential and universal quantifiers and equalities and inequalities concerning polynomials with coefficients in $\mathbb{F}_q$. By the theorem on elimination of existential quantifiers in algebraically closed fields, if this statement is true, it is also true in $\overline{\mathbb{F}}_q$. Therefore, there exists a subgroup $\mathcal{G}$ of $\mathrm{PGL}_2(\overline{\mathbb{F}}_q)$ isomorphic to $\mathcal{H}_i$, but not conjugate to $\mathcal{H}_i\overline{\mathbb{F}}_q^*/\overline{\mathbb{F}}_q^*$. For A running through $\mathrm{GL}_2(\overline{\mathbb{F}}_q)$ such that $A\overline{\mathbb{F}}_q^* \in \mathcal{G}$, $A/\sqrt{\det A}$ runs through finitely many matrices, which all lie in $\mathrm{SL}_2(\mathbb{F}_s)$ for some s which is a power of q. If

$$\mathcal{G}_0 = \left\{ \frac{M}{\sqrt{\det M}}\,\mathbb{F}_s^* : M\mathbb{F}_q^* \in \mathcal{G} \right\}, \tag{6}$$

then $\mathcal{G}_0$ is isomorphic to $\mathcal{G}$, hence to $\mathcal{H}_i$. By the known property of $\mathrm{PSL}_2(\mathbb{F}_s)$ (see [12, Chapter XII, italicized statements on pp. 274 and 278 and the normalization of G_Ω on p. 273]), $\mathcal{G}_0$ is conjugate in $\mathrm{PGL}_2(\mathbb{F}_s)$ to $\mathcal{H}_i\mathbb{F}_s^*/\mathbb{F}_s^*$. Hence there exists $A_0 \in \mathrm{GL}_2(\mathbb{F}_s)$ such that

$$\mathcal{G}_0 = A_0\mathcal{H}_iA_0^{-1}.$$

By (6) this gives

$$\mathcal{G}_0 = A_0\mathcal{H}_iA_0^{-1}\overline{\mathbb{F}}_q^*/\overline{\mathbb{F}}_q^*,$$

thus $\mathcal{G}$ is conjugate in $\mathrm{PGL}_2(\overline{\mathbb{F}}_q)$ to $\mathcal{H}_i\overline{\mathbb{F}}_q^*/\overline{\mathbb{F}}_q^*$, a contradiction. □

Lemma 13. *If $\mathbb{F}_q \subset K$, then every subgroup $\mathcal{G}$ of $\mathrm{PGL}_2(K)$ isomorphic to $\mathcal{H}_i$ (notation of Lemma* 12*) is conjugate to $\mathcal{H}_iK^*/K^*$.*

Proof. By Lemma 12 there exists $A \in \mathrm{GL}_2(\overline{K})$ such that for $i = 1$ or 2,

$$\mathcal{G}\overline{K}^*/\overline{K}^* = A\mathcal{H}_i A^{-1}\overline{K}^*/\overline{K}^*. \tag{7}$$

It follows that for all $M \in \mathrm{SL}_2(\mathbb{F}_q)\mathbb{F}_q^{*2}$ there exists $t \in \overline{K}^*$ such that

$$tAMA^{-1} \in \mathrm{GL}_2(K). \tag{8}$$

Now, if

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad M = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

then

$$AMA^{-1} = \frac{1}{ad-bc}\begin{pmatrix} ad\alpha - ac\beta + bd\gamma - bc\delta & -ab\alpha + a^2\beta - b^2\gamma + ab\delta \\ cd\alpha - c^2\beta + d^2\gamma - cd\delta & -bc\alpha + ac\beta - bd\gamma + ad\delta \end{pmatrix}.$$

Applying (8) with

$$M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix},$$

we obtain

$$(9_1) \quad t\frac{ad}{ad-bc} \in K, \qquad (9_2) \quad t\frac{ac}{ad-bc} \in K, \qquad (9_3) \quad t\frac{bc}{ad-bc} \in K;$$

$$(10_1) \quad t\frac{ab}{ad-bc} \in K, \qquad (10_2) \quad t\frac{a^2}{ad-bc} \in K;$$

$$(11_1) \quad t\frac{c^2}{ad-bc} \in K, \qquad (11_2) \quad t\frac{cd}{ad-bc} \in K.$$

Since $ad - bc \neq 0$ we have $a \neq 0$ or $c \neq 0$. If $a \neq 0$, then (9_1) and (10_2) imply $d/a \in K$, (9_2) and (10_2) imply $c/a \in K$, and (10_1) and (10_2) imply $b/a \in K$, hence $a^{-1}A \in \mathrm{GL}_2(K)$. If $c \neq 0$ the same conclusion follows from (9_2), (9_3), (11_2) and (11_1). By (7),

$$\mathcal{G}\overline{K}^*/\overline{K}^* = a^{-1}A\mathcal{H}_i A^{-1}a\overline{K}^*/\overline{K}^*,$$

hence $\mathcal{G} = a^{-1}A\mathcal{H}_i A^{-1}a\overline{K}^*/\overline{K}^*$, which gives the assertion. □

2. Determination of all binary forms with a given group of weak automorphs

Definition 3. If

$$\langle \alpha, \beta, \gamma, \delta \rangle \in K^4, \quad \alpha\delta - \beta\gamma \neq 0, \quad \langle \alpha, \beta, \gamma, \delta \rangle \neq \langle \alpha, 0, 0, \alpha \rangle \tag{12}$$

and

$$z^2 - (\alpha + \delta)z + (\alpha\delta - \beta\gamma) = (z - \lambda_1)(z - \lambda_2), \quad \lambda_1, \lambda_2 \in \overline{K},\ \lambda_1 \neq \lambda_2, \tag{13}$$

we put

$$\begin{aligned} &\chi_i = \gamma x + (\lambda_i - \alpha)y \quad (i = 1, 2) \quad &&\text{if } \gamma \neq 0, \\ &\chi_1 = (\alpha - \delta)x + \beta y, \quad \chi_2 = y &&\text{otherwise.} \end{aligned}$$

Definition 4. If (12) holds and

$$z^2 - (\alpha + \delta)z + (\alpha\delta - \beta\gamma) = (z - \lambda)^2, \qquad \lambda \in \overline{K}, \tag{14}$$

we put

$$\chi_1 = \gamma x + (\lambda - \alpha)y, \quad \chi_2 = y \quad \text{if } \gamma \neq 0,$$
$$\chi_1 = \beta y, \quad \chi_2 = x \quad \text{otherwise.}$$

Theorem 1. *Let* $\langle \alpha, \beta, \gamma, \delta \rangle$ *satisfy* (12) *and* $T = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) K^*$ *be of order* ν *in* $\mathrm{PGL}_2(K)$. *A form* $f \in \overline{K}[x, y] \setminus \{0\}$ *satisfies the conditions*

$$f \in K[x, y] \tag{15}$$

and

$$T \in \mathrm{Aut}(f, K) \tag{16}$$

if and only if either (13) *holds and*

$$f = \chi_1^{c_1} \chi_2^{c_2} \psi(\chi_1^{\nu} + \chi_2^{\nu}, \lambda_1 \chi_1^{\nu} + \lambda_2 \chi_2^{\nu}), \tag{17}$$

where χ_1, χ_2 *are given in Definition* 3, ψ *is a binary form over* K, *while* c_i *are integers satisfying* $0 \leqslant c_i < \nu$ *and* $c_1 = c_2$ *if* χ_1, χ_2 *are conjugate over* K, *or* (14) *holds and*

$$f = \chi_1^{c_1} \psi(\chi_1^{\pi}, \lambda^{\pi-1}\chi_2^{\pi} - \chi_2\chi_1^{\pi-1}), \tag{18}$$

where χ_1, χ_2 *are given in Definition* 4, ψ *is a binary form over* K, *while* c_1 *is a non-negative integer satisfying* $c_1 < \pi = \nu$ *unless either* $\pi = 0$, *in which case* $\psi \in K^*$, c_1 *arbitrary, or* $\pi = 2 = \nu$, $\lambda \notin K$, *in which case* $c_1 = 0$.

Corollary 1. *If a form* $f \in K[x, y]$ *of degree* $n \not\equiv 0 \bmod \pi$ *has a weak automorph of order* ν *in* $\mathrm{PGL}_2(K)$, *then either* $\nu \mid n$ *and* $\zeta_\nu + \zeta_\nu^{-1} \in K$, *or* f *is the product of two forms with such automorphs, one of which, say* g, *is linear or quadratic.*

Corollary 2. *If a form* $f \in K[x, y]$ *of degree* $n \not\equiv 1 \bmod \pi$, $n > 2$, *has a weak automorph of order* ν *in* $\mathrm{PGL}_2(K)$ *and* f *is the product of a linear factor and another factor defined and irreducible over* K, *then* $\nu \mid n - 1$ *and* $\zeta_\nu \in K$.

Corollary 3. *If a quartic form* $f \in K[x, y]$ *has in* $\mathrm{PGL}_2(K)$ *a weak automorph of order* 3, *then either* $\sqrt{-3} \in K$ *or* f *is a square in* $\overline{K}[x, y]$.

Corollary 4. *If* $T_0 \in \mathrm{GL}_2(K)$ *and* $T = T_0 K^*$ *is of finite order in* $\mathrm{PGL}_2(K)$, *then there exists* $c(T_0) \in K$ *such that if* $T \in \mathrm{Aut}(f, K)$, *then*

$$f(T_0)^{o(T)} = c(T_0)^{\deg f} f$$

and if, moreover, $f(\xi, 1) = 0$ *implies* $T^*\xi \neq \xi$, *then* $o(T) \mid \deg f$ *and*

$$f(T_0) = c(T_0)^{\deg f / o(T)} f.$$

Here $f(\infty, 1) = 0$ *means* $f(1, 0) = 0$.

Corollary 5. *Under the assumption of Theorem* 1 *about* T, *a form* $f \in \overline{K}[x, y] \setminus \{0\}$ *satisfies* (16) *if and only if either* (13) *and* (17) *hold, where* χ_1, χ_2 *are given in Definition* 3, ψ *is a binary form over* $\overline{K}$, *while* c_i *are integers satisfying* $0 \leqslant c_i < \nu$, *or* (14) *and* (18) *hold, where* χ_1, χ_2 *are given in Definition* 4, *while* c_1 *is a non-negative integer satisfying* $c_1 < \pi = \nu$ *unless* $\pi = 0$, *in which case* $\psi \in K^*$, c_1 *arbitrary.*

The proof of Theorem 1 is based on three lemmas.

Lemma 14. *The linear forms* χ_1, χ_2 *given in Definition* 3 *are linearly independent and satisfy* $\chi_i(\alpha x + \beta y, \gamma x + \delta y) = \lambda_i \chi_i$ $(i = 1, 2)$, *provided for* $\gamma = 0$ *we have* $\lambda_1 = \alpha$, $\lambda_2 = \delta$. *Moreover, either* $\chi_i \in K[x, y]$ $(i = 1, 2)$, *or* χ_1, χ_2 *are conjugate over* K.

If $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) K^*$ *is of order* $\nu > 2$ *in* $\mathrm{PGL}_2(K)$, *then* $\chi_i \in K[x, y]$ *if and only if* K *contains a primitive root of unity of order* ν.

Proof. The first two assertions are proved by calculation and inspection. To prove the third assertion notice that $\chi_i \in K[x, y]$ if and only if $\lambda_i \in K$. If $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) K^*$ is of order $\nu > 2$ in $\mathrm{PGL}_2(K)$ we know from the proof of Lemma 1 that λ_1/λ_2 is a primitive root of unity of order ν and that

$$\lambda_2(1 + \lambda_1/\lambda_2) = \alpha + \delta \in K,$$

hence $\lambda_i \in K$ $(i = 1, 2)$ is equivalent to existence in K of a primitive root of unity of order ν. □

Lemma 15. *The linear forms* χ_1, χ_2 *given in Definition* 4 *are linearly independent and satisfy*

$$\chi_1(\alpha x + \beta y, \gamma x + \delta y) = \lambda \chi_1, \qquad \chi_2(\alpha x + \beta y, \gamma x + \delta y) = \lambda \chi_2 + \chi_1.$$

Moreover $\chi_1 \in K[x, y]$ *unless* $\pi = 2$ *and* $\lambda \notin K$.

Proof. By calculation and inspection. □

Lemma 16. *If* $G \in K[x] \setminus K$, $\lambda \in \overline{K}^*$ *and*

$$G(x + \lambda^{-1}) = rG(x), \qquad r \in K(\lambda)^*, \tag{19}$$

then $\pi \neq 0$ *and*

$$G(x) = H(\lambda^{\pi-1} x^\pi - x), \qquad \text{where } H \in K(\lambda)[x]. \tag{20}$$

Remark 5. For K being a finite field and $\lambda \in K$ the lemma is due to Dickson.

Proof. By comparing the leading coefficients on both sides of (19) we obtain $r = 1$. Now (19) implies that

$$G\left(l\lambda^{-1}\right) = G(0) \qquad \text{for all } l \in \mathbb{Z},$$

hence $\pi \neq 0$. We shall prove (20) by induction on the degree of G, say n. If $n = 0$, then (20) holds with $H = G$. Assume that (20) is true for all G satisfying (19) of degree less than n and that $\deg G = n$. From (19) we obtain

$$\prod_{l=0}^{\pi-1}(x - l\lambda^{-1}) \Big| G(x) - G(0).$$

But

$$\prod_{l=0}^{\pi-1}(x - l\lambda^{-1}) = \lambda^{1-\pi}(\lambda^{\pi-1}x^{\pi} - x)$$

and

$$\lambda^{\pi-1}(x + \lambda^{-1})^{\pi} - (x + \lambda^{-1}) = \lambda^{\pi-1}x^{\pi} - x.$$

Taking

$$G_1(x) = \frac{G(x) - G(0)}{\lambda^{\pi-1}x^{\pi} - x}$$

we deduce from (19) that $G_1(x + \lambda^{-1}) = G_1(x)$, hence by the inductive assumption

$$G_1(x) = H_1(\lambda^{\pi-1}x^{\pi} - x), \qquad H_1 \in K(\lambda)[x],$$

and (20) holds with $H = xH_1(x) + G(0)$. □

Proof of Theorem 1. *Necessity.* First assume (13). Since by Lemma 14, χ_1, χ_2 are linearly independent over $\overline{K}$ we can write

$$f(x, y) = \sum_{i=0}^{n} a_i \chi_1^{n-i}\chi_2^{i}, \qquad \text{where } a_i \in K(\lambda_1, \lambda_2), \tag{21}$$

and we set

$$I = \{i : a_i \neq 0\}.$$

It follows from (16) and Lemma 14 that

$$\begin{aligned} r\sum_{i\in I} a_i \chi_1^{n-i}\chi_2^{i} = f(\alpha x + \beta y, \gamma x + \delta y) &= \sum_{i\in I} a_i \lambda_1^{n-i}\lambda_2^{i}\chi_1^{n-i}\chi_2^{i} \\ &= \lambda_1^{n}\sum_{i\in I} a_i(\lambda_2/\lambda_1)^{i}\chi_1^{n-i}\chi_2^{i}. \end{aligned} \tag{22}$$

Since T is in $\mathrm{PGL}_2(K)$ of order ν, λ_2/λ_1 is a primitive root of unity of order ν in $\overline{K}$.

If $I = \{j\}$, then we have (17) with $\psi = a_j$. If $|I| > 1$, then the condition (22) implies that there exist integers c_1, c_2 such that $0 \leqslant c_j < \nu$ and $i \equiv c_2, n - i \equiv c_1 \bmod \nu$ for all

$i \in I$. Since

$$p = \chi_1^{\nu} + \chi_2^{\nu},\ q = \lambda_1\chi_1^{\nu} + \lambda_2\chi_2^{\nu} \tag{23}$$

$$\text{is equivalent to} \quad \chi_1^{\nu} = \frac{q - \lambda_2 p}{\lambda_1 - \lambda_2},\ \chi_2^{\nu} = \frac{\lambda_1 p - q}{\lambda_1 - \lambda_2},$$

if λ_1, λ_2 are in K we obtain (17) with

$$\psi(p, q) = \sum_{i\in I} a_i(\lambda_1 - \lambda_2)^{(c_1+c_2-n)/\nu}(q - \lambda_2 p)^{(n-i-c_1)/\nu}(\lambda_1 p - q)^{(i-c_2)/\nu}. \tag{24}$$

If $\lambda_1 \notin K$, then χ_1, χ_2 are conjugate over K by Lemma 14, and denoting conjugation by prime, from (14) and (21) we obtain

$$0 = f'(x, y) - f(x, y) = \sum_{i=0}^{n} a_i'\chi_2^{n-i}\chi_1^i - \sum_{i=0}^{n} a_i\chi_1^{n-i}\chi_2^i = \sum_{i=0}^{n}(a_i' - a_{n-i})\chi_2^{n-i}\chi_1^i,$$

hence $a_i' = a_{n-i}$ for all $i \leqslant n$. It follows that i and $n - i$ belong simultaneously to I, thus $c_1 = c_2$. Now, the form $\psi(p, q)$ given by (24) satisfies

$$\begin{aligned}\psi'(p, q) - \psi(p, q) &= \sum_{i\in I} a_i'(\lambda_2 - \lambda_1)^{(2c_1-n)/\nu}(q - \lambda_1 p)^{(n-i-c_1)/\nu}(\lambda_2 p - q)^{(i-c_1)/\nu} \\ &\quad - \sum_{i\in I} a_i(\lambda_1 - \lambda_2)^{(2c_1-n)/\nu}(q - \lambda_2 p)^{(n-i-c_1)/\nu}(\lambda_1 p - q)^{(i-c_1)/\nu} \\ &= \sum_{i\in I} a_{n-i}(\lambda_2 - \lambda_1)^{(2c_1-n)/\nu}(q - \lambda_1 p)^{(n-i-c_1)/\nu}(\lambda_2 p - q)^{(i-c_1)/\nu} \\ &\quad - \sum_{i\in I} a_{n-i}(\lambda_1 - \lambda_2)^{(2c_1-n)/\nu}(q - \lambda_2 p)^{(i-c_1)/\nu}(\lambda_1 p - q)^{(n-i-c_1)/\nu} = 0\end{aligned}$$

and since the extension $K(\lambda_1, \lambda_2)/K$ is separable, we get $\psi \in K[x, y]$ and from (21) and (23) we again obtain (17).

Assume now that (14) holds. Since, by Lemma 15, χ_1, χ_2 are linearly independent over $\overline{K}$, we have

$$f(x, y) = g(\chi_1, \chi_2), \qquad g \in K(\lambda)[x, y].$$

By (16) and Lemma 15,

$$\begin{aligned}g(\lambda\chi_1, \lambda\chi_2 + \chi_1) &= g\big(\chi_1(\alpha x + \beta y, \gamma x + \delta y), \chi_2(\alpha x + \beta y, \gamma x + \delta y)\big) \\ &= f(\alpha x + \beta y, \gamma x + \delta y) = rf(x, y) = rg(\chi_1, \chi_2),\end{aligned}$$

hence $G(x) = g(1, x)$ satisfies

$$G(x + \lambda^{-1}) = rG(x)$$

and, by Lemma 16, we have either $G \in K$, or $\pi \neq 0$ and

$$G(x) = H(\lambda^{\pi-1}x^{\pi} - x), \qquad H \in K(\lambda)[x].$$

In the former case we have (18) with

$$\psi(p,q)=1, \qquad c_1=n \qquad \text{if } \pi=0,$$
$$\psi(p,q)=p^{\lfloor n/\pi\rfloor}, \qquad c_1=n-\pi\left\lfloor\frac{n}{\pi}\right\rfloor \qquad \text{if } \pi>0,\ \lambda\in K,$$
$$\psi(p,q)=p^{n/2}, \qquad c_1=0 \qquad \text{if } \pi=2,\ \lambda\notin K.$$

In the latter case we have for $n\equiv c_1 \bmod \pi$, $0\leqslant c_1<\pi$,

$$g(\chi_1,\chi_2)=\chi_1^n G\left(\frac{\chi_2}{\chi_1}\right)=\chi_1^n H\left(\lambda^{\pi-1}\left(\frac{\chi_2}{\chi_1}\right)^{\pi}-\frac{\chi_2}{\chi_1}\right),$$

thus (18) holds with

$$\psi(p,q)=p^{(n-c_1)/\pi}H(q/p).$$

If $\lambda\in K$, then clearly $\psi\in K[p,q]$.

It remains to consider the case $\pi=2$, $\lambda\notin K$. Let

$$\psi(p,q)=p^m\psi_1(p,q), \qquad \text{where } \psi_1(0,1)\neq 0 \tag{25}$$

($m=(n-c_1-\deg g)/2$), so that

$$(\psi_1(\chi_1^2,\lambda\chi_2^2-\chi_2\chi_1),\chi_1)=1. \tag{26}$$

By (18) we have $\chi_1^{2m+c_1}\mid f$, $(\chi_1^2)^{2m+c_1}\mid f^2$, and since χ_1^2 is irreducible over K, also $(\chi_1^2)^{m+\lceil c_1/2\rceil}\mid f$. By (18), (25) and (26) this gives

$$2m+2\lceil c_1/2\rceil=2m+c_1,$$

hence $c_1=0$, $\psi(\chi_1^2,\lambda\chi_2^2-\chi_2\chi_1)=f\in K[x,y]$ and since

$$\chi_1^2=\gamma^2x^2+\beta\gamma y^2\in K[x,y], \quad \lambda\chi_2^2-\chi_1\chi_2=\gamma xy+\alpha y^2\in K[x,y] \tag{27}$$

and χ_1^2, $\lambda\chi_2^2-\chi_1\chi_2$ are algebraically independent over K, it follows that $\psi\in K[p,q]$.

Sufficiency. If (13) holds and T is of order ν in $\mathrm{PGL}_2(K)$, then we have $\lambda_1^\nu=\lambda_2^\nu$, hence $\chi_i(\alpha x+\beta y,\gamma x+\delta y)^\nu=\lambda_1^\nu\chi_i^\nu$ and, by (17),

$$f(\alpha x+\beta y,\gamma x+\delta y)=\lambda_1^{c_1}\lambda_2^{c_2}\lambda_1^{\nu\deg\psi}f,$$

thus (16) holds. Also, if $\lambda_1,\lambda_2\in K$, then (15) holds. If λ_1,λ_2 are conjugate over K, then (15) holds again by the condition $c_1=c_2$, since $\chi_1\chi_2$, $\chi_1^\nu+\chi_2^\nu$ and $\lambda_1\chi_1^\nu+\lambda_2\chi_2^\nu$ are invariant under conjugation.

If (14) holds and $\pi=0$, then, by (18), $f(\alpha x+\beta y,\gamma x+\delta y)=\lambda^{c_1}f$, thus (16) holds. Also (15) holds, since in this case $\lambda\in K$. If $\pi>0$, then by (18) and Lemma 15,

$$f(\alpha x+\beta y,\gamma x+\delta y)$$
$$=\lambda^{c_1}\chi_1^{c_1}\psi\big(\lambda^\pi\chi_1^\pi,\lambda^{\pi-1}(\lambda^\pi\chi_2^\pi+\chi_1^\pi)-(\lambda\chi_2+\chi_1)\lambda^{\pi-1}\chi_1^{\pi-1}\big)=\lambda^{c_1+\deg\psi}f,$$

thus (16) holds. Also if $\lambda\in K$, then (15) holds. If $\lambda\notin K$, then $\pi=2$, $c_1=0$ and (15) follows from (27). □

Proof of Corollary 1. If $T = \left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)K^* \in \mathrm{Aut}(f, K)$ of order $\nu > 1$ in $\mathrm{PGL}_2(K)$ satisfies (13), then, by Lemma 1, $\zeta + \zeta^{-1} \in K$, where $\zeta = \lambda_2/\lambda_1$ is a primitive root of unity of order ν in $\overline{K}$. If $n \equiv 0 \bmod \nu$ the first term of the alternative holds. By Theorem 1 we have $n \equiv c_1 + c_2 \bmod \nu$, thus $n \not\equiv 0 \bmod \nu$ implies $c_i := \max\{c_1, c_2\} > 0$. If $\chi_i \in K[x, y]$ we take $g = \chi_i$, and if χ_1, χ_2 are conjugate over K, we take $g = \chi_1\chi_2$.

If T satisfies (14), then either $\pi = 0$ and $f = \chi_1^{c_1}$, in which case we take $g = \chi_1$, or $\pi > 0$, in which case we have $n \equiv c_1 \bmod \pi$. By assumption, $n \not\equiv 0 \bmod \pi$, thus $c_1 > 0$, $\pi \neq 2$ and we take $g = \chi_1$. □

Proof of Corollary 2. Let $T_0(x, y) = (\alpha x + \beta y, \gamma x + \delta y)$, $T = \left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)K^* \in \mathrm{Aut}(f, K)$ be of order $\nu > 1$ in $\mathrm{PGL}_2(K)$, and L be a linear factor of f in $K[x]$ such that f/L is irreducible over K. Since $L(T_0) \mid f(T_0) \mid f$ and f/L is of degree $n - 1 > 1$ we have $L(T_0)/L \in K^*$, hence (cf. Lemmas 14 and 15)

$$L = a\chi_i, \quad a \in K^*, \quad \text{where } i = 1 \text{ or } 2 \text{ in case (13)}, \ i = 1 \text{ in case (14)}. \tag{28}$$

In case (13) it follows that $\lambda_1, \lambda_2 \in K$, thus a primitive root of unity $\zeta_\nu = \lambda_2/\lambda_1$ is in K. Now (17) implies that either $c_i = 1$ and $c_{3-i} = 0$, in which case $\nu \mid n - 1$, or $c_i = c_{3-i} = 0$ and

$$\chi_i \mid \psi(\chi_1^\nu + \chi_2^\nu, \lambda_1\chi_1^\nu + \lambda_2\chi_2^\nu).$$

This gives

$$\chi_i \mid \psi(\chi_{3-i}^\nu, \lambda_{3-i}\chi_{3-i}^\nu) = \chi_{3-i}^{\nu \deg \psi}\psi(1, \lambda_{3-i}),$$

hence $\psi(1, \lambda_{3-i}) = 0$,

$$\psi = (\lambda_{3-i}p - q)\psi_1, \quad \psi_1 \in K[p, q],$$

and

$$f/\chi_i = (\lambda_{3-i} - \lambda_i)\chi_i^{\nu-1}\psi_1(\chi_1^\nu + \chi_2^\nu, \lambda_1\chi_1^\nu + \lambda_2\chi_2^\nu)$$

is reducible for $n > 2$, contrary to assumption.

In case (14) it follows from (28) that $\lambda \in K$ and, by (18), we have $\pi > 0$. If $c_1 = 1$ we have $n \equiv 1 \bmod \pi$, contrary to assumption, while if $c_1 = 0$,

$$\chi_1 \mid \psi(\chi_1^\pi, \lambda^{\pi-1}\chi_2^\pi - \chi_2\chi_1^{\pi-1}).$$

This gives

$$\chi_1 \mid \psi(0, \lambda^{\pi-1}\chi_2^\pi) = (\lambda^{\pi-1}\chi_2^\pi)^{\deg\psi}\psi(0, 1),$$

hence $\psi(0, 1) = 0$, $\psi = p\psi_1$, $\psi_1 \in K[p, q]$ and

$$f/\chi_1 = \chi_1^{\pi-1}\psi_1(\chi_1^\pi, \lambda^{\pi-1}\chi_2^\pi - \chi_2\chi_1^{\pi-1})$$

is reducible for $n > 2$, contrary to assumption. □

Proof of Corollary 3. If $\pi = 3$ the conclusion holds trivially. If $\pi \neq 3$ then by Theorem 1,

$$f = \chi_1^{c_1}\chi_2^{c_2}\psi(\chi_1^3 + \chi_2^3, \lambda_1\chi_1^3 + \lambda_2\chi_2^3),$$

where χ_1, χ_2 are given in Definition 3, c_1, c_2 are non-negative integers and ψ is a binary form over K. If $\sqrt{-3} \notin K$, then $\chi_i \notin K[x, y]$, by Lemma 14; hence, by Theorem 1, $c_1 = c_2$ and the above equation for f gives $4 \equiv 2c_1 \bmod 3$. It follows that $c_1 = c_2 = 2$, $\psi \in K^*$ and f is a square in $\overline{K}[x, y]$. □

Proof of Corollary 4. For $T_0 = (\alpha x + \beta y, \gamma x + \delta y)$ we take

$$c(T_0) = \begin{cases} \lambda_1^{o(T)} = \lambda_2^{o(T)} & \text{if (13) holds,} \\ \lambda^{o(T)} & \text{if (14) holds.} \end{cases}$$

If $T_0K^* \in \mathrm{Aut}(f, K)$ we have, by Theorem 1, for the case (13),

$$f(T_0)^{o(T)} = \lambda_1^{c_1 o(T)}\lambda_2^{c_2 o(T)}c(T_0)^{\deg\psi\cdot o(T)}f = c(T_0)^{c_1+c_2+\deg\psi\cdot o(T)}f = c(T_0)^{\deg f}f;$$

and for the case (14),

$$f(T_0)^{o(T)} = \lambda^{c_1 o(T)}c(T_0)^{\deg\psi\cdot o(T)}f = c(T_0)^{c_1+\deg\psi\cdot o(T)}f = c(T_0)^{\deg f}f.$$

If, moreover, $f(\xi, 1) = 0$ implies $T^*\xi \neq \xi$, then $c_1 = c_2 = 0$ if (13) holds, and $c_1 = 0$ if (14) holds, hence

$$\deg f = \deg\psi \cdot o(T) \quad \text{and} \quad f(T_0) = c(T_0)^{\deg\psi}f = c(T_0)^{\deg f/o(T)}f. \qquad \square$$

Proof of Corollary 5. It suffices to apply Theorem 1 with K replaced by $\overline{K}$ and T replaced by $\left(\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix}\right)\overline{K}^*$. □

Definition 5. Let $\mathcal{G}$ be a finite subgroup of $\mathrm{PGL}_2(K)$ which is not a π-group, and let, in the notation of Lemma 6,

$$\chi_{j0} = \prod_{\eta\in O_j\setminus\{\infty\}}(x - \eta y)\prod_{\eta\in O_j\cap\{\infty\}} y, \qquad \chi_j = \chi_{j0}^{[K_j:K]_i} \quad (1 \leqslant j \leqslant h).$$

Further, if (2) holds, set

$$p = \chi_1^{|\mathcal{G}|/\deg\chi_1}, \quad q = \chi_2^{|\mathcal{G}|/\deg\chi_2};$$

and if (3) holds and $K_1 = K(\vartheta)$, set

$$p = \chi_1^{|\mathcal{G}|/\deg\chi_1} + \chi_2^{|\mathcal{G}|/\deg\chi_2}, \quad q = \vartheta\chi_1^{|\mathcal{G}|/\deg\chi_1} + \sigma_1(\vartheta)\chi_2^{|\mathcal{G}|/\deg\chi_2}.$$

Corollary 6. *Either $\chi_j \in K[x, y]$ for all $j \leqslant h$, or χ_1, χ_2 are conjugate over K and for $h = 3$, $\chi_3 \in K[x, y]$. Moreover $\mathcal{G} \subset \mathrm{Aut}(\chi_j, K)$ for all $j \leqslant h$.*

Proof. This is an immediate consequence of Lemma 6. □

Corollary 7. *We have $p, q \in K[x, y]$ and $(p, q) = 1$.*

Proof. First, p and q are forms over $\overline{K}$. If (3) holds, or (2) holds and $[K_1 : K]_i = [K_2 : K]_i = 1$, this is clear, since $\deg \chi_j = |O_j|$ divides $|\mathcal{G}|$ for all $j \leqslant h$. If (2) holds and $[K_j : K]_i = 2$, then for each $S \in \mathcal{G} \setminus \{E\}$ and $\xi \in O_j$ with $S^*\xi = \xi$ we have $o(S) \equiv 0 \bmod 2$, hence $2|O_j|\,||\mathcal{G}|$ by Lemma 5.

Now, if (2) holds we have $\chi_j \in K[x, y]$ $(1 \leqslant j \leqslant h)$, hence $p, q \in K[x, y]$. If (3) holds, then $\chi_2 = \sigma_1(\chi_1)$, hence $\sigma_1(p) = p$, $\sigma_1(q) = q$, thus $p, q \in K[x, y]$. Since $(\chi_1, \chi_2) = 1$ we have $(p, q) = 1$. □

Theorem 2. *Let $\mathcal{G}$ be a finite subgroup of $\mathrm{PGL}_2(K)$ which is not a π-group. A form $f \in \overline{K}[x, y] \setminus \{0\}$ satisfies*

$$f \in K[x, y] \tag{29}$$

and

$$\mathcal{G} \subset \mathrm{Aut}(f, K) \tag{30}$$

if and only if

$$f = \prod_{j=1}^{h} \chi_j^{c_j} \psi(p, q), \tag{31}$$

where χ_j and p, q are given in Definition 5, ψ is a binary form over K and c_j are integers satisfying $0 \leqslant c_j < |\mathcal{G}|/\deg \chi_j$ and $c_1 = c_2$ if χ_1, χ_2 are conjugate over K.

Corollary 8. *Under the assumption of Theorem 2 about $\mathcal{G}$, a form $f \in \overline{K}[x, y]$ satisfies* (30) *if and only if* (31) *holds, where χ_j are given in Definition 5,*

$$p = \chi_1^{|\mathcal{G}|/\deg \chi_1}, \quad q = \chi_2^{|\mathcal{G}|/\deg \chi_2},$$

ψ is a binary form over $\overline{K}$ and c_j are integers satisfying $0 \leqslant c_j < |\mathcal{G}|/\deg \chi_j$.

The proof of Theorem 2 is based on five lemmas.

Lemma 17. *Let $f \in \overline{K}[x, y] \setminus \{0\}$ be a form and, for $\xi \in \overline{K}$, $e_f(\xi)$ be the multiplicity of ξ as a zero of $f(x, 1)$, and $e_f(\infty)$ be the multiplicity of 0 as a zero of $f(1, y)$. We have*

$$S \in \mathrm{Aut}(f, K) \tag{32}$$

if and only if for all $\xi \in \overline{K} \cup \{\infty\}$,

$$e_f(S^*\xi) = e_f(\xi). \tag{33}$$

Proof. By making a preliminary linear transformation we may assume that

$$f = \prod_{i=1}^{n} (x - \xi_i y) \quad \text{and} \quad S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} K^*,$$

where

$$\alpha\delta - \beta\gamma \neq 0. \tag{34}$$

Necessity. If (32) holds and for some ξ_i we have $\gamma\xi_i + \delta = 0$, then with an $r \in K^*$,

$$(\alpha\xi_i + \beta)^n = f(\alpha\xi_i + \beta, \gamma\xi_i + \delta) = rf(\xi_i, 1) = 0,$$

hence $\alpha\xi_i + \beta = 0$ and $\alpha\delta - \beta\gamma = 0$, contrary to (34). Thus $\gamma\xi_i + \delta \neq 0$ $(i = 1, \dots, n)$ and

$$\begin{aligned}\prod_{i=1}^{n}\left(\alpha x + \beta y - \frac{\alpha\xi_i + \beta}{\gamma\xi_i + \delta}(\gamma x + \delta y)\right) &= \frac{(\alpha\delta - \beta\gamma)^n}{(-1)^n f(-\delta, \gamma)} \prod_{i=1}^{n}(x - \xi_i y)\\ &= \frac{(\beta\gamma - \alpha\delta)^n}{f(-\delta, \gamma)} f(x, y) = \frac{(\beta\gamma - \alpha\delta)^n}{rf(-\delta, \gamma)} f(\alpha x + \beta y, \gamma x + \delta y)\\ &= \frac{(\beta\gamma - \alpha\delta)^n}{rf(-\delta, \gamma)} \prod_{i=1}^{n}(\alpha x + \beta y - \xi_i(\gamma x + \delta y)),\end{aligned}$$

hence (33) holds.

Sufficiency. If (33) holds, there is a permutation σ of $\{1, \dots, n\}$ such that

$$\frac{\alpha\xi_i + \beta}{\gamma\xi_i + \delta} = \xi_{\sigma(i)}.$$

Then by (34) we have $\gamma\xi_i + \delta \neq 0$ for all $i \leqslant n$ and it follows that

$$\begin{aligned}f(\alpha x + \beta y, \gamma x + \delta y) &= \prod_{i=1}^{n}(\alpha x + \beta y - \xi_{\sigma(i)}(\gamma x + \delta y))\\ &= \prod_{i=1}^{n}\left(\alpha x + \beta y - \frac{\alpha\xi_i + \beta}{\gamma\xi_i - \delta}(\gamma x + \delta y)\right)\\ &= \frac{(\alpha\delta - \beta\gamma)^n}{(-1)^n f(-\delta, \gamma)} \prod_{i=1}^{n}(x - \xi_i y) = \frac{(\beta\gamma - \alpha\delta)^n}{f(-\delta, \gamma)} f(x, y),\end{aligned}$$

hence (32) holds. □

Lemma 18. *If $e_f(\eta) = 0$ for all $\eta \in O(\mathcal{G})$ and $\mathcal{G} \subset \mathrm{Aut}(f, K)$, then*

$$\deg f \equiv 0 \bmod |\mathcal{G}|.$$

Proof. Let us divide all $\xi \in \overline{K} \cup \{\infty\}$ with $e_f(\xi) > 0$ into classes by assigning ξ_1 and ξ_2 to the same class C if $\xi_1 = S^*\xi_2$ for some $S \in \mathcal{G}$. Since $e_f(\eta) = 0$ for all $\eta \in O(\mathcal{G})$, we have $\xi \neq S^*\xi$ for all ξ with $e_f(\xi) > 0$, hence by Lemma 17, the number of elements in each class is $|\mathcal{G}|$. On the other hand, by Lemma 17, for each C in the set Γ of all classes, there is $e(C) \in \mathbb{N}$ such that $e_f(\xi) = e(C)$ for all $\xi \in C$. We obtain

$$\deg f = \sum_{\xi \in \overline{K} \cup \{\infty\}} e_f(\xi) = \sum_{C \in \Gamma} e(C)|\mathcal{G}| \equiv 0 \bmod |\mathcal{G}|.$$ □

Lemma 19. *If $f \in K[x, y] \setminus \{0\}$, $\mathcal{G} \subset \mathrm{Aut}(f, K)$ and $(\chi_j, f) \neq 1$ then $\chi_j \mid f$.*

Proof. Assume that $e_f(\eta) > 0$ for some $\eta \in O_j$. By Lemma 17 we have $e_f(S^*\eta) > 0$ for all $S \in \mathcal{G}$, hence $\chi_{j0} \mid f$. Therefore,

$$\chi_j \mid f^{[K_j:K]_i}. \tag{35}$$

If $[K_j : K]_i = 1$ the assertion is proved. If $[K_j : K]_i = 2$, then $O_j \subset K_j \setminus K$. Therefore, for all $\eta \in O_j$, $(x - \eta y)^2$ is irreducible over K and (35) implies

$$(x - \eta y)^2 \mid f,$$

which gives $\chi_j \mid f$, as asserted. □

Remark 6. For $K = \mathbb{C}$ the lemma is well known (see [27, Vol. II, §70]) and for $\pi \neq 2$ the proof given there needs no modification.

Lemma 20. *The field* $L = \{\varphi \in K(t) : \varphi(S^*) = \varphi \text{ for all } S \in \mathcal{G}\}$ *is generated by* $p(t, 1)/q(t, 1)$, *where* p, q *are given in Definition* 5.

Proof. By Definition 5, $\mathcal{G} \subset \mathrm{Aut}(\chi_{j0}, K)$, hence, by Corollary 3, for every S_0 in $\mathrm{GL}_2(K)$ with $S = S_0K^* \in \mathcal{G}$ we have

$$\chi_{j0}(S_0)^{o(S)} = c(S_0)^{\deg \chi_{j0}} \chi_{j0}.$$

If $S^*\xi = \xi$ for some $\xi \in O_j$, we have, by Lemma 5,

$$o(S) \mid |\mathcal{G}|/|O_j| = |\mathcal{G}|/\deg \chi_{j0},$$

and so

$$\chi_j(S_0)^{|\mathcal{G}|/\deg \chi_j} = \chi_{j0}(S_0)^{|\mathcal{G}|/\deg \chi_{j0}} = c(S_0)^{|\mathcal{G}|/o(S)} \chi_j^{|\mathcal{G}|/\deg \chi_j}. \tag{36}$$

If $S_0^*\xi \neq \xi$ for all $\xi = O_j$ the same conclusion holds by the second part of Corollary 4. Therefore,

$$p(S_0) = c(S_0)^{|\mathcal{G}|/o(S)} p, \quad q(S_0) = c(S_0)^{|\mathcal{G}|/o(S)} q \tag{37}$$

and

$$\frac{p(S_0^*t, 1)}{q(S_0^*t, 1)} = \frac{p(t, 1)}{q(t, 1)}, \quad \text{thus} \quad \frac{p(t, 1)}{q(t, 1)} \in L.$$

Since $(\chi_1, \chi_2) = 1$ we have $p(t, 1)/q(t, 1) \notin K$ and, by Lüroth's theorem, $L = K(r)$, where $r \in K(t) \setminus K$. Without loss of generality we may assume that $r = p_1/q_1$, where p_1 and q_1 are coprime polynomials of the same degree d. Let

$$p_2 = p_1(x/y)y^d, \quad q_2 = q_1(x/y)y^d.$$

Since $r(S^*t) = r(t)$ for all $S \in \mathcal{G}$ we have, for all $S_0 \in \mathrm{GL}_2(K)$ with $S_0K^* \in \mathcal{G}$,

$$p_2(S_0) = c_1(S_0)p_2, \quad q_2(S_0) = c_1(S_0)q_2,$$

where $c_1(S_0) \in K^*$. It follows that

$$\lambda p_2(S_0) + \mu q_2(S_0) = c_1(S_0)(\lambda p_2 + \mu q_2) \tag{38}$$

for all λ, μ in $\overline{K}$. Now, choose λ_0 and μ_0 in $\overline{K}$ such that

$$\begin{aligned} &\lambda_0 p_2(\eta, 1) + \mu_0 q_2(\eta, 1) \neq 0 \qquad \text{for all } \eta \in O(\mathcal{G}) \setminus \{\infty\}, \\ &\lambda_0 p_2(1, 0) + \mu_0 q_2(1, 0) \neq 0 \qquad \text{if } \infty \in O(\mathcal{G}). \end{aligned} \tag{39}$$

This is possible, since $\langle p_2(\eta, 1), q_2(\eta, 1)\rangle \neq \langle 0, 0\rangle$ and $p(1, 0) \neq 0$. By Lemma 18 we have

$$d \equiv 0 \bmod |\mathcal{G}|.$$

On the other hand, since $p(t, 1)/q(t, 1) \in K(r)$ we have

$$|\mathcal{G}| = \deg p(t, 1)/q(t, 1) \equiv 0 \bmod d.$$

It follows that $d = \deg p(t, 1)/q(t, 1)$ and $K(p(t, 1)/q(t, 1)) = K(r) = L$. □

Lemma 21. *If f_1 is a binary form over K of degree divisible by $|\mathcal{G}|$ and for every $S_0 \in \mathrm{GL}_2(K)$ with $S = S_0 K^* \in \mathcal{G}$ we have*

$$f_1(S_0) = c(S_0)^{\deg f_1/o(S)} f_1,$$

then $f_1 = \psi_1(p, q)$, where p, q are given in Definition 5 and ψ_1 is a binary form over K.

Proof. By (37) for every S_0 in question

$$q(S_0)^{\deg f_1/|\mathcal{G}|} = c(S_0)^{\deg f_1/|\mathcal{G}|} q^{\deg f_1/|\mathcal{G}|},$$

hence

$$\frac{f_1(S^*t, 1)}{q(S^*t, 1)^{\deg f_1/|\mathcal{G}|}} = \frac{f_1(t, 1)}{q(t, 1)^{\deg f_1/|\mathcal{G}|}},$$

and since this holds for every $S \in \mathcal{G}$,

$$\frac{f_1(t, 1)}{q(t, 1)^{\deg f_1/|\mathcal{G}|}} \in L.$$

By Lemma 20 we have

$$\frac{f_1(t, 1)}{q(t, 1)^{\deg f_1/|\mathcal{G}|}} = u\left(\frac{p(t, 1)}{q(t, 1)}\right).$$

Let $u = v/w$, where v, w are coprime polynomials over K. Putting $v(x, y) = v(x/y)y^{\deg v}$ and $w(x, y) = w(x/y)y^{\deg w}$, we obtain

$$\frac{f_1(t, 1)}{q(t, 1)^{\deg f_1/|\mathcal{G}|}} = \frac{v(p(t, 1),\ q(t, 1))q(t, 1)^{\deg w}}{w(p(t, 1),\ q(t, 1))q(t, 1)^{\deg v}}.$$

Since $(p(t, 1),\ q(t, 1)) = 1$ by Corollary 7, we have

$$(w(p(t, 1), q(t, 1)),\ v(p(t, 1), q(t, 1))) = 1$$

and

$$(v(p(t, 1), q(t, 1))w(p(t, 1), q(t, 1)), q(t, 1)) = 1,$$

hence $w \in K^*$ and $\deg f_1/|\mathcal{G}| \geqslant \deg v$, and

$$f_1(t,1) = w^{-1} v(p(t,1),\ q(t,1)) q^{\deg f_1/|\mathcal{G}| - \deg v}.$$

Substituting $t = x/y$ and cancelling the denominators we obtain

$$f_1 = w^{-1} v(p,q) q^{\deg f_1/|\mathcal{G}| - \deg v}. \qquad \square$$

Proof of Theorem 2. *Necessity.* By Lemma 19 we may write

$$f = \prod_{j=1}^{h} \chi_j^{c_j} f_0, \quad \text{where} \quad f_0 \in \overline{K}[x,y],\ \Big(f_0, \prod_{j=1}^{h} \chi_j\Big) = 1. \tag{40}$$

If $\chi_1 \notin K[x,y]$, then by Corollary 6, χ_1, χ_2 are conjugate and $\chi_1^{c_1} \mid f$ implies $\chi_2^{c_1} \mid f$, hence $c_1 \leqslant c_2$. Similarly $c_2 \leqslant c_1$, hence $c_1 = c_2$ as asserted and $f_0 \in K[x,y]$. Now,

$$e_{f_0}(\eta) = 0 \quad \text{for all } \eta \in O(\mathcal{G})$$

and by Lemma 18,

$$\deg f_0 \equiv 0 \bmod |\mathcal{G}|.$$

Moreover, by Corollary 4, for every $S_0 \in \mathrm{GL}_2(K)$ with $S = S_0 K^* \in \mathcal{G}$ we have

$$f_0(S_0) = c(S_0)^{\deg f_0/o(S)} f_0.$$

By Lemma 21 with $f_1 = f_0$,

$$f_0 = \psi(p,q),$$

where ψ is a binary form over K, thus (31) follows from (40).

Now, by (34) for each $j \leqslant k$ and every $S_0 \in \mathrm{GL}_2(K)$ with $S_0 K^* \in \mathcal{G}$,

$$\chi_j^{|\mathcal{G}|/\deg \chi_j}(S_0) = c(S_0)^{|\mathcal{G}|/o(S)} \chi_j^{|\mathcal{G}|/\deg \chi_j},$$

hence, applying Lemma 21 with $f_1 = \chi_j^{|\mathcal{G}|/\deg \chi_j}$ if $\chi_j \in K[x,y]$, or with $f_1 = (\chi_1\chi_2)^{n|\mathcal{G}|/\deg \chi_j}$ if χ_1, χ_2 are conjugate, we obtain

$$\chi_j^{|\mathcal{G}|/\deg \chi_j} = \psi_j(p,q) \quad \text{or} \quad (\chi_1\chi_2)^{|\mathcal{G}|/\deg \chi_j} = \psi_1(p,q),$$

respectively, where ψ_j are binary forms over K. This gives the required upper bound for c_j.

Sufficiency. Assuming (31) we obtain (29) by Corollary 6 and the condition $c_1 = c_2$ if χ_1, χ_2 are conjugate over K. On the other hand, for every $S_0 \in \mathrm{GL}_2(K)$ such that $S = S_0 K^* \in \mathcal{G}$ we have, by (31),

$$\psi(p(S_0),\ q(S_0)) = c(S_0)^{|\mathcal{G}|/o(S)} \psi(p,q),$$

thus $\mathcal{G} \subset \mathrm{Aut}(\psi(p,q), K)$ and (30) follows from (31) by Corollary 6. $\square$

Proof of Corollary 8. It suffices to apply Theorem 2 with K replaced by $\overline{K}$ and $\mathcal{G}$ replaced by $\mathcal{G}\overline{K}^*/\overline{K}^*$. $\square$

Example. We give without proof formulae for χ_1, χ_2, χ_3 for dihedral subgroups of $\mathrm{PGL}_2(K)$. For the dihedral subgroup of order 4 generated by

$$\begin{pmatrix} a & b \\ c & -a \end{pmatrix} K^*, \begin{pmatrix} d & e \\ f & -d \end{pmatrix} K^*, \quad \text{where} \quad a, \ldots, f \in K,\ (a^2+bc)(d^2+ef) \neq 0,\ 2ad+bf+ce=0$$

(the last condition ensures commutativity) we have

$$\chi_1 = cx^2 - 2axy - by^2, \quad \chi_2 = fx^2 - 2dxy - ey^2,$$

$$\chi_3 = (cd-af)x^2 - 2(ad+bf)xy - (bd-ae)y^2.$$

For the dihedral group of order $2\nu > 4$ generated by

$$\begin{pmatrix} a & b \\ a(\zeta+\zeta^{-1})+b & -a \end{pmatrix} K^* \quad \text{and} \quad \begin{pmatrix} 1+\zeta+\zeta^{-1} & -1 \\ 1 & 1 \end{pmatrix} K^*,$$

where $a, b \in K$, $(a\zeta+b)(a\zeta^{-1}+b) \neq 0$, ζ is a primitive root of unity of order $\nu \not\equiv 0 \bmod \pi$, the polynomials χ_i $(1 \leqslant i \leqslant 3)$ are given by the formulae

$$\begin{aligned} \chi_3 &= x^2 - (\zeta+\zeta^{-1})xy + y^2, \\ \chi_{(3-\varepsilon)/2} &= \frac{B-A}{\zeta^{-1}-\zeta}\left(\zeta^{-1}(x-\zeta y)^\nu + \zeta(x-\zeta^{-1}y)^\nu\right) \\ &\quad + \left(\varepsilon\sqrt{AB} - \frac{\zeta B - \zeta^{-1}A}{\zeta^{-1}-\zeta}\right)\left((x-\zeta y)^\nu + (x-\zeta^{-1})^\nu\right) \quad (\varepsilon = \pm 1) \end{aligned}$$

if

$$A = (-a\zeta^2 - b\zeta)^\nu \neq B = (-a\zeta^{-2} - b\zeta^{-1})^\nu,$$

and

$$\begin{aligned} \chi_1 &= (\zeta-\zeta^{-1})(x-\zeta y)^\nu + (\zeta^{-1}-\zeta)(x-\zeta^{-1}y)^\nu, \\ \chi_2 &= (x-\zeta y)^\nu + (x-\zeta^{-1}y)^\nu, \end{aligned}$$

otherwise. We shall use the fact, easy to check directly, that for $a = 1$, $b = 0$ the two generators of the group are weak automorphs of χ_i, hence $\mathrm{Aut}(\chi_i, K)$ contains the group for $i = 2$ or 3.

For the dihedral group generated by

$$\begin{pmatrix} -1 & b \\ 0 & 1 \end{pmatrix} K^* \quad \text{and} \quad \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} K^*,$$

where $\pi > 0$, $\lambda \in K^*$, $b \in K$, the polynomials χ_i $(1 \leqslant i \leqslant 2)$ are given by the formulae

$$\chi_1 = y, \quad \chi_2 = -2\lambda^{\pi-1}x^\pi + 2xy^{\pi-1} + (\lambda^{\pi-1}b^\pi - b)y^\pi.$$

Definition 6. Let $\mathcal{G}$ be a π-subgroup of $\mathrm{PGL}_2(K)$ generated by elements $S_i K^*$, where

$$S_i = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} \lambda_i & 1 \\ 0 & \lambda_i \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad (1 \leqslant i \leqslant g), \tag{41}$$

$ad - bc \neq 0$, $\lambda_1^{-1}, \dots, \lambda_g^{-1}$ are linearly independent over $\mathbb{F}_\pi$ and either a, b, c, d, λ_j are in K, or $a = 0$, $b = 1$, $c \in K$, $K(d)$ is a quadratic inseparable extension of K and $d + \lambda_j \in K$. Then we put

$$\chi_1 = cx + dy, \qquad \chi_2 = ax + by,$$
$$p = \chi_1^{\pi^g}, \qquad q = \chi_2 \prod_{\langle a_1,\dots,a_g\rangle \in \mathbb{F}_\pi^g \setminus \{\mathbf{0}\}} \Big(\chi_1 + \chi_2\Big(\sum_{j=1}^{g} a_j \lambda_j^{-1}\Big)^{-1}\Big).$$

Corollary 9. *We have $p \in K[x, y]$, $q \in K[x, y]$, $(p, q) = 1$ and p, q are algebraically independent.*

Proof. The assertion is clear unless $\pi = 2, \lambda_1 \notin K$. In the exceptional case $c \in K, \lambda_1^2 \in K$, hence $p \in K[x, y]$. Also for each $j \leqslant g$,

$$d\lambda_j^{-2} + \lambda_j^{-1} \in K,$$

hence for all $\langle a_1, \dots, a_g\rangle \in \mathbb{F}_2^g \setminus \{\mathbf{0}\}$,

$$d\Big(\sum_{j=1}^{g} a_j \lambda_j^{-1}\Big)^2 + \sum_{j=1}^{g} a_j \lambda_j^{-1} \in K,$$

which gives $\chi_1 + \chi_2\big(\sum_{j=1}^{g} a_j \lambda_j^{-1}\big)^{-1} \in K[x, y]$ and $q \in K[x, y]$. Moreover, $(p, q) = 1$, since $(\chi_1, \chi_2) = 1$, and since p, q are forms, it follows that they are algebraically independent. □

Theorem 3. *Let $\mathcal{G}$, χ_1, p, q be as in Definition 6. A form $f \in \overline{K}[x, y] \setminus \{0\}$ satisfies* (29) *and* (30) *if and only if*

$$f = \chi_1^{c_1} \psi(p, q), \tag{42}$$

where ψ is a binary form over K, c_1 is an integer, $0 \leqslant c_1 < |\mathcal{G}|$ and if $\chi_1 \notin K[x, y]$ then c_1 is even.

Corollary 10. *Under the assumption of Theorem 3 about $\mathcal{G}$, χ_1, p, q a form $f \in \overline{K}[x, y]$ satisfies* (30) *if and only if* (42) *holds, where ψ is a binary form over $\overline{K}$ and c_1, c_2 are integers with $0 \leqslant c_1 < |\mathcal{G}|$.*

Corollary 11. *If a binary form f has at least two coprime linear factors over K and $\mathcal{G}$ is a π-group contained in* $\mathrm{Aut}(f, K)$, *then $|\mathcal{G}| \leqslant \deg f$.*

The proof of Theorem 3 is based on the following lemma.

Lemma 22. *If $\pi > 0$, $G \in K[x]$, $\lambda_i \in K(\lambda_1)^*$ $(1 \leqslant i \leqslant g)$, $\lambda_1^{-1}, \dots, \lambda_g^{-1}$ are linearly independent over $\mathbb{F}_\pi$ and*

$$G(x + \lambda_i^{-1}) = r_i G(x), \qquad r_i \in K^* \quad (1 \leqslant i \leqslant g), \tag{43}$$

then

$$G(x) = H(P(x)), \quad H \in K(\lambda_1)[x], \tag{44}$$

where

$$P(x) = \prod_{\langle a_1,\dots,a_g\rangle \in \mathbb{F}_\pi^g} \Big(x + \sum_{j=1}^{g} a_j \lambda_j^{-1}\Big).$$

Remark 7. For K being a finite field of characteristic π and $\lambda_i \in K$ the lemma is due to Dickson.

Proof. On comparing the leading coefficients on both sides of (43) we obtain $r_i = 1$ $(1 \leqslant i \leqslant g)$. We shall prove (44) by induction on the degree of G, say n. If $n = 0$ then (44) holds with $H = G$. Assume that (44) is true for all G satisfying (43) of degree less than n, and that $\deg G = n$. From (43) we obtain, for all $\langle a_1, \dots, a_g\rangle \in \mathbb{F}_\pi^g$,

$$G\Big(-\sum_{j=1}^{g} a_j \lambda_j^{-1}\Big) = G(0),$$

hence by the linear independence of $\lambda_1^{-1}, \dots, \lambda_g^{-1}$ over $\mathbb{F}_\pi$,

$$P(x) \mid G(x) - G(0).$$

Taking

$$G_1(x) = \frac{G(x) - G(0)}{P(x)}$$

we deduce from (43) that $G_1(x + \lambda_i^{-1}) = G_1(x)$ $(1 \leqslant i \leqslant g)$, hence by the inductive assumption

$$G_1(x) = H_1\big(P(x)\big), \quad H_1 \in K(\lambda_1)[x],$$

and (44) holds with $H(x) = xH_1(x) + G(0)$. □

Proof of Theorem 3. *Necessity.* Since $ad - bc \neq 0$ and χ_1, χ_2 are linearly independent over K, we have

$$f(x, y) = g(\chi_1, \chi_2), \quad g \in K(\lambda_1)[x, y].$$

By (41),

$$\chi_1(S_i) = \lambda_i \chi_1, \quad \chi_2(S_i) = \lambda_i \chi_2 + \chi_1, \tag{45}$$

hence, by (30), for some $r_i \in K$,

$$g(\lambda_i \chi_1, \lambda_i \chi_2 + \chi_1) = g\big(\chi_1(S_i), \chi_2(S_i)\big) = f(S_i) = r_i f = r_i g(\chi_1, \chi_2),$$

thus $G(x) = g(1, x)$ satisfies

$$G(x + \lambda_i^{-1}) = r_i G(x).$$

By Lemma 22 we have

$$G(x) = H\big(P(x)\big), \quad H \in K(\lambda_1)[x].$$

Hence

$$g(\chi_1, \chi_2) = \chi_1^n G\left(\frac{\chi_2}{\chi_1}\right) = \chi_1^n H\left(P\left(\frac{\chi_2}{\chi_1}\right)\right)$$

and for $n \equiv c_1 \bmod \pi^g$ with $0 \leqslant c_1 < \pi^g$, (42) holds with

$$\psi(p, q) = p^{(n-c_1)/\pi^g} H\left(\frac{q}{p} \prod_{\langle a_1,\dots,a_g\rangle \in \mathbb{F}_\pi^g \setminus \{\mathbf{0}\}} \sum_{j=1}^{g} a_j \lambda_j^{-1}\right).$$

If $\lambda_1 \in K$ we have $\psi \in K[p, q]$.

It remains to consider the case $\pi = 2$, $K(\lambda_1)$ a quadratic inseparable extension of K. In this case $\chi_1 \notin K[x, y]$ and χ_1^2 is irreducible over K. Let $\psi(p, q) = p^m \psi_1$, where $\psi_1 \in K[p, q]$ and $\psi_1(0, 1) \neq 0$. Since, by Corollary 9, $(p, q) = 1$ we have $(\psi_1(p, q), \chi_1) = 1$ and it follows from (42) that

$$\chi_1^{2^g m + c_1} \mid f, \quad \chi_1^{2^g m + c_1 + 1} \nmid f.$$

Further

$$\chi_1^{2^{g+1} m + 2c_1} \mid f^2$$

and since χ_1^2 is irreducible,

$$\chi_1^{2^g m + 2\lceil c_1/2 \rceil} \mid f, \quad 2^g m + 2\lceil c_1/2 \rceil = 2^g m + c_1,$$

$c_1 \equiv 0 \bmod 2$, and $\chi_1^{c_1} \in K[x, y]$. It now follows from (42) that

$$\psi(p, q) \in K[x, y].$$

By Corollary 9, $p, q \in K[x, y]$ and p, q are algebraically independent. Hence $\psi \in K[p, q]$.

Sufficiency. Since χ_1 or χ_1^2 in the exceptional case and p, q are defined over K, (29) is clear. On the other hand, by (45),

$$p(S_i) = \lambda_i^{\pi^g} p,$$

$$q(S_i) = (\lambda_i \chi_2 + \chi_1) \prod_{\langle a_1,\dots,a_g\rangle \in \mathbb{F}_\pi^g \setminus \{\mathbf{0}\}} \Big(\lambda_i \chi_1 + (\lambda_i \chi_2 + \chi_1)\Big(\sum_{j=1}^{g} a_j \lambda_j^{-1}\Big)^{-1}\Big)$$

$$= (\lambda_i \chi_2 + \chi_1)\lambda_i^{\pi^g - 1} \prod_{\langle a_1,\dots,a_g\rangle \in \mathbb{F}_\pi^g \setminus \{\mathbf{0}\}} \Big(\sum_{j=1}^{g} a_j \lambda_j^{-1}\Big)^{-1}$$

$$\times \prod_{\langle a_1,\dots,a_g\rangle \in \mathbb{F}_\pi^g \setminus \{\mathbf{0}\}} \Big(\chi_1 \sum_{j=1}^{g} a_j \lambda_j^{-1} + \chi_2 + \chi_1 \lambda_i^{-1}\Big) =$$

$$= \lambda_i^{\pi^g} \prod_{\langle a_1,\dots,a_g\rangle \in \mathbb{F}_\pi^g \setminus \{\mathbf{0}\}} \Big(\sum_{j=1}^{g} a_j \lambda_j^{-1}\Big)^{-1} \prod_{\langle a_1,\dots,a_g\rangle \in \mathbb{F}_\pi^g} \Big(\chi_1 \sum_{j=1}^{g} a_j \lambda_j^{-1} + \chi_2\Big)$$

$$= \lambda_i^{\pi^g} q,$$

hence

$$f(S_i) = \chi_1(S_i)^{c_1} \psi(p(S_i),\, q(S_i)) = \lambda_i^{c_1+\pi^g \deg \psi} \chi_1^{c_1} \psi(p, q) = \lambda_i^{c_1+\pi^g \deg \psi} f$$

and (30) holds. □

Proof of Corollary 10. It suffices to apply Theorem 3 with K replaced by $\overline{K}$ and $\mathcal{G}$ replaced by $\mathcal{G}\overline{K}^*/\overline{K}^*$. □

Proof of Corollary 11. Since $\mathrm{Aut}(f, K) \subset \mathrm{Aut}(f, \overline{K})$ we may assume that $K = \overline{K}$. By Lemma 3 every π-group contained in $\mathrm{PGL}_2(K)$ must contain a π-group considered in Theorem 3. Since f has at least two coprime linear factors, the case $\psi \in K$ in (42) is excluded. Hence

$$|\mathcal{G}| \leqslant \deg \psi(p, q) \leqslant n.$$ □

3. Upper bounds for $|\mathrm{Aut}(f, K)|$

We shall prove

Theorem 4. *If a form $f \in \overline{K}[x, y] \setminus \{0\}$ of degree n has at least three coprime linear factors over $\overline{K}$, then $\mathrm{Aut}(f, K)$ is finite. Moreover, if*

(46) $\quad f = cf_0(\alpha x + \beta y, \gamma x + \delta y)^k, \quad$ *where* $c \in \overline{K}^*,\ \alpha, \beta, \gamma, \delta \in K,\ \alpha\delta - \beta\gamma \neq 0,$

$f_0 = x^q y - x y^q$, $\mathbb{F}_q \subset K$, $k \in \mathbb{N}$, *then* $\mathrm{Aut}(f, K) \cong \mathrm{PGL}_2(\mathbb{F}_q)$; *otherwise either*

(47) $$\pi = 2, \quad n = 2\varrho + 1, \quad \mathrm{Aut}(f, K) \cong \mathfrak{D}_{2\varrho+1},$$

or

(48) $$\pi = 3, \quad n = 10, \quad \mathrm{Aut}(f, K) \cong \mathfrak{A}_5,$$

or

(49) $$|\mathrm{Aut}(f, K)| = lm,$$

where $l \not\equiv 0 \bmod \pi$, $\zeta_l + \zeta_l^{-1} \in K$, $l < n$, $m \leqslant n$.

Remark 8. It is not clear whether there exist f and K satisfying (48).

Corollary 12. *Assume that $f \in K[x, y]$ and all factors of $f(x, 1)$ irreducible over K are separable. Then $\mathrm{Aut}(f, K)$ is finite if and only if either K is finite, or f has at least three coprime linear factors over $\overline{K}$.*

Definition 7. For $\pi = 0$ or $\pi > n$ we put

$$U_n(K) = \left\{\nu \in \mathbb{N} : \nu \leqslant n \text{ and } \zeta_\nu + \zeta_\nu^{-1} \in K\right\},$$
$$V_n(K) = \{\nu \in \mathbb{N} : \nu \leqslant n \text{ and } \zeta_\nu \in K\},$$
$$a_1(n, K) = \sup U_n(K), \quad a_2(n, K) = \sup\{\nu \in U_n(K) : \nu \equiv n \bmod 2\},$$
$$b(n, K) = \sup V_n(K),$$
$$\mathcal{M} = \{6, 10, 15, 21, 22\} \cup \{25, \ldots\} \setminus \{29, 32, 44\},$$

where the dots represent consecutive integers greater than 25.

Corollary 13. *We have* $a_2(n, K) \leqslant a_1(n, K) \leqslant n$ *for every* n *and* $a_2(n, K) = a_1(n, K) = n$ *for* $n \leqslant 4$, $a_1(n, K) \geqslant 6$ *for* $n \geqslant 6$, $a_2(n, K) \geqslant 6$ *for even* $n \geqslant 6$, $2 \leqslant b(n, K) \leqslant a_1(n, K)$ *for* $n \geqslant 2$.

Definition 8. Let $A(n, K)$ and $B(n, K)$ for $n \geqslant 3$ be the maximum of $|\mathrm{Aut}(f, K)|$ over all forms f of degree n in $\overline{K}[x, y]$ or $K[x, y]$ respectively with at least three coprime linear factors over $\overline{K}$ and which are not perfect powers in $\overline{K}[x, y]$.

Theorem 5. *We have*

$$A(n, K) = B(n, K) = \pi^{3g} - \pi^g \quad \text{if } n = \pi^g + 1,\ \mathbb{F}_{\pi^g} \subset K,$$

and

$$A(n, K) \leqslant n(n-1) \quad \text{otherwise.}$$

Moreover, if $\pi = 0$ *or* $\pi > n$ *then*

$$A(n, K) = \begin{cases} 12 \quad \text{if level } K \leqslant 2,\ n = 4, \\ \max\{a_1(n, K), 2a_2(n, K), 24\} \text{ if level } K \leqslant 2 \text{ and either} \\ \qquad n = 6, 8, 14 \text{ or } n = 12,\ \sqrt{5} \notin K \text{ or} \\ \qquad n = 2m,\ m \geqslant 9 \text{ and } \sqrt{5} \notin K \text{ if } m \in \mathcal{M}, \\ \max\{a_1(n, K), 2a_2(n, K), 60\} \text{ if level } K \leqslant 2, \sqrt{5} \in K \\ \qquad \text{and } n/2 \in \mathcal{M}, \\ \max\{a_1(n, K), 2a_2(n, K)\} \text{ otherwise}; \end{cases}$$

$$B(n, K) = \begin{cases} 12 \quad \text{if } n = 4,\ \sqrt{-3} \in K, \\ \max\{b(n-1, K), 2a_2(n, K), 24\} \text{ if level } K \leqslant 2 \text{ and either} \\ \qquad n = 6, 8, 14 \text{ or } n = 12,\ \sqrt{5} \notin K \text{ or} \\ \qquad n = 2m,\ m \geqslant 9 \text{ and } \sqrt{5} \notin K \text{ if } m \in \mathcal{M}, \\ \max\{b(n-1, K), 2a_2(n, K), 60\} \text{ if level } K \leqslant 2, \sqrt{5} \in K \\ \qquad \text{and } n/2 \in \mathcal{M}, \\ \max\{b(n-1, K), 2a_2(n, K)\} \text{ otherwise.} \end{cases}$$

Corollary 14. *We have* $A(n, \mathbb{C}) = 2n$ *unless* $n = 4, 6, 8, 12, 20$, *when* $A(n, \mathbb{C}) = 12, 24, 24, 60, 60$, *respectively.*

Remark 9. P. Olver [19] and then I. Berchenko and P. Olver [1] gave a bound for $|\mathrm{Aut}(f, \mathbb{C})|$ assumed finite, which asserts that

$$A(n, \mathbb{C}) \leqslant 6n - 12$$

and apart from an exceptional case

$$A(n, \mathbb{C}) \leqslant 4n - 8.$$

The bound given in Corollary 14 is better for all $n > 4$, $n \neq 6, 8, 12$. This bound for $n > 30$ has been anticipated by Summerer in an unpublished paper [25], dealing only with non-singular forms.

Remark 10. Let $A_0(n, \pi) = \max A(n, K)$, where K runs through all fields of characteristic π. By an analysis of subgroups of $\mathrm{PSL}_2(\mathbb{F}_q)$ listed in [12, Chapter 12] one can guess explicit values for $A_0(n, \pi)$ also for $0 < \pi \leqslant n$. Namely, if $n > 20$ and $\pi^g \leqslant n < \pi^{g+1}$, then conjecturally $A_0(\pi^g + 1, \pi) = \pi^{3g} - \pi^g$, otherwise $A_0(n, \pi) = \pi^{2g} - \pi^g$ unless $g = 1$, $(\pi^2 - \pi)/2 < n$, $n \not\equiv \bmod \pi$ or $n = \pi^2 - \pi$ or $g = 3$, $n = \pi^4 - \pi^2$, when $A_0(n, \pi) = 2n$ or $\pi^3 - \pi$ or $\pi^6 - \pi^2$, respectively. For $n \leqslant 20$ there are apparently three exceptions to this rule: $A_0(8, 5) = 24$, $A_0(12, 7) = A_0(20, 7) = 60$.

For the proof of Theorem 4 we need the following

Definition 9. For $\xi \in \overline{K} \cup \{\infty\}$, we set

$$\mathrm{Aut}(f, K, \xi) = \{S \in \mathrm{Aut}(f, K) : S^*\xi = \xi\},$$

$$\mathrm{Aut}_\pi(f, K, \xi) = \begin{cases} \{S \in \mathrm{Aut}(f, K, \xi) : S^{*\pi} = E\} & \text{if } \pi > 0, \\ \{E\} & \text{otherwise.} \end{cases}$$

Lemma 23. *Let $f \in \overline{K}[x, y] \setminus \{0\}$ be a form of degree n, let $Z = \{\xi \in \overline{K} \cup \{\infty\} : e_f(\xi) > 0\}$ and suppose $|Z| \geqslant 3$. For every $\xi \in Z$ the set $\mathrm{Aut}_\pi(f, K, \xi)$ is a finite normal subgroup of $\mathrm{Aut}(f, K, \xi)$ and the quotient group is cyclic of order $l < n$ with $l \not\equiv 0 \bmod \pi$ such that $\zeta_l \in K(\xi)$, where $K(\infty) = K$.*

Proof. Assume first $\xi = \infty$. Then $S^*\xi = \xi$ is equivalent to $S = \left(\begin{smallmatrix} \alpha & \beta \\ 0 & 1 \end{smallmatrix}\right) K^*$, where $\alpha \in K^*$, $\beta \in K$. Let

$$\mathcal{H} = \left\{\alpha \in K^* : \text{there exists } \beta \in K \text{ such that } \begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} K^* \in \mathrm{Aut}(f, K)\right\}.$$

Then $\mathcal{H}$ is a subgroup of the multiplicative group K^* and if $\alpha \in \mathcal{H}$ and $S = \left(\begin{smallmatrix} \alpha & \beta \\ 0 & 1 \end{smallmatrix}\right) K^* \in \mathrm{Aut}(f, K)$, then the order of α in K^* is finite. Indeed, otherwise, taking ξ_1, ξ_2 in $Z \setminus \{\infty\}$, $\xi_1 \neq \xi_2$, we should obtain, by Lemma 17,

$$S^{*i}\xi_j \in Z \quad \text{for all } i \in \mathbb{N} \text{ and } j = 1, 2,$$

hence for some $i'_j < i''_j = i'_j + i_j$,

$$S^{*i'_j}\xi_j = S^{*i''_j}\xi_j \quad (j = 1, 2);$$

$$\alpha^{i_j}\xi_j + \beta(\alpha^{i_j} - 1)/(\alpha - 1) = S^{*i_j}\xi_j = \xi_j;$$

$$(\alpha - 1)\xi_j + \beta = 0 \quad (j = 1, 2), \quad \xi_1 = \xi_2, \quad \text{a contradiction.}$$

The above calculation also shows that if $\alpha \in \mathcal{H} \setminus \{1\}$ and $S = \left(\begin{smallmatrix} \alpha & \beta \\ 0 & 1 \end{smallmatrix}\right) K^* \in \mathrm{Aut}(f, K)$, then the order of α in K^* is equal to the order ν of S in $\mathrm{PGL}_2(K)$ and is not divisible by π. Since $|Z| \geqslant 3$, in Theorem 1 applied to f, $\overline{K}$ and S the case $\psi \in \overline{K}$ is excluded and we have $\nu \leqslant n$ with equality possible only if

$$f = a\big((\alpha - 1)x + \beta y\big)^n + by^n, \quad a, b \text{ in } \overline{K}.$$

It now follows from $e_f(\infty) > 0$ that $f(1, 0) = 0$, hence $a = 0$, $f = by^n$, $|Z| = 1$, a contradiction. Hence $\nu < n$. Since there are only finitely many $\alpha \in K^*$ with $\alpha^\nu = 1$ for some $\nu < n$, $\mathcal{H}$ is finite and cyclic by the well known lemma (see [3, Algebraic Supplement, §3]). Its order l equal to the order of a generator satisfies

$$|\mathcal{H}| = l < n, \quad l \not\equiv 0 \bmod \pi, \quad \zeta_l \in K. \tag{50}$$

Let

$$\mathcal{G} = \left\{ \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} K^* \in \mathrm{Aut}(f, K) \right\}.$$

Then $\mathcal{G}$ is a normal subgroup of $\mathrm{Aut}(f, K, \infty)$, which in turn is a subgroup of $\mathrm{Aut}(f, K)$. If $\pi = 0$, then $\mathcal{G} = \{E\}$, for otherwise taking $\xi_1 \in Z \setminus \{\infty\}$ and $\beta \in K^*$ such that $S = \left(\begin{smallmatrix} 1 & \beta \\ 0 & 1 \end{smallmatrix}\right) K^* \in \mathcal{G}$ we should obtain, by Lemma 17, $\xi_1 + i\beta = S^{*i}\xi_1 \in Z$, a contradiction, since $\xi_1 + i\beta$ $(i = 0, \ldots, n)$ are distinct. If $\pi > 0$ then

$$\mathcal{G} = \mathrm{Aut}_\pi(f, K, \infty)$$

is a π-group and, by Corollary 11,

$$|\mathcal{G}| = \pi^g \leqslant n.$$

The quotient group $\mathrm{Aut}(f, K, \infty)/\mathcal{G}$ is isomorphic to $\mathcal{H}$, hence the assertion follows from (50).

Assume now $\xi \neq \infty$ and put $f_1 = f(\xi x + y, x)$. We have $f_1(1, 0) = f(\xi, 1) = 0$, hence $e_{f_1}(\infty) > 0$ and, by the already proved case of the lemma, $\mathrm{Aut}_\pi(f_1, K(\xi), \infty)$ is a finite normal subgroup of $\mathrm{Aut}(f_1, K(\xi), \infty)$ and the quotient group is cyclic of order $l < n$ with $l \not\equiv 0 \bmod \pi$ such that $\zeta_l \in K(\xi)$.

Now

$$\mathrm{Aut}(f, K, \xi) \subset \begin{pmatrix} \xi & 1 \\ 1 & 0 \end{pmatrix} \mathrm{Aut}(f_1, K(\xi), \infty) \begin{pmatrix} \xi & 1 \\ 1 & 0 \end{pmatrix}^{-1},$$

$$\mathrm{Aut}_\pi(f, K, \xi) \subset \begin{pmatrix} \xi & 1 \\ 1 & 0 \end{pmatrix} \mathrm{Aut}_\pi(f_1, K(\xi), \infty) \begin{pmatrix} \xi & 1 \\ 1 & 0 \end{pmatrix}^{-1},$$

and the assertion of the lemma follows from simple facts from group theory. □

Lemma 24. *For $\xi \in Z$ (notation of Lemma 23), let m be the length of the orbit of ξ under the action of $\mathrm{Aut}(f, K)$. If $|\mathrm{Aut}(f, K, \xi)| \equiv 0 \bmod \pi$, then $m \equiv 1 \bmod \pi$, also either $\xi \in K$ or*

$$\pi = 2, \quad \mathrm{Aut}(f, K, \xi) = \mathrm{Aut}_\pi(f, K, \xi). \tag{51}$$

Proof. By Lemma 17, $\mathrm{Aut}(f, K)$, hence also $\mathrm{Aut}_\pi(f, K, \xi)$, acts on Z. Let $O(\xi)$ be the orbit of ξ under the action of $\mathrm{Aut}(f, K)$. Since for $\eta \in Z$ and $S \in \mathrm{Aut}_\pi(f, K, \xi) \setminus \{E\}$, $S^*\eta = \eta$ implies $\eta = \xi$, $\mathrm{Aut}_\pi(f, K, \xi)$ acts on $O(\xi) \setminus \{\xi\}$ and all orbits are of length $|\mathrm{Aut}_\pi(f, K, \xi)|$. Hence $m = |O(\xi)| \equiv 1 \bmod \pi$. By Lemma 3, $\mathrm{Aut}_\pi(f, K, \xi)$ has an element

$$S_0 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} K^*,$$

where $ad - bc \neq 0$, $\lambda \neq 0$ and either $a, b, c, d, \lambda \in K$, or $\pi = 2$, $c \in K^*$, and $K(d)$ is a quadratic inseparable extension of K. The condition $S_0^*\xi = \xi$ gives $\xi = -d/c$. In the former case it follows that $\xi \in K$, in the latter case $K(\xi)$ is a quadratic inseparable extension of K and for $S = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) K^* \in \mathrm{Aut}(f, K, \xi)$ the equation $S^*\xi = \xi$ gives $\alpha = \delta$, $S^\pi = e$, hence (51) holds. □

Proof of Theorem 4. Suppose $|\mathrm{Aut}(f, K)|$ is divisible exactly by $\pi^g = q$, and for $\xi \in Z$, let $m(\xi)$ be the length of the orbit of ξ under the action of $\mathrm{Aut}(f, K)$. For all $\xi \in Z$ we have

$$|\mathrm{Aut}(f, K)| = |\mathrm{Aut}(f, K, \xi)| m(\xi) \tag{52}$$

and, by Lemma 17,

$$m(\xi) \leqslant |Z| \leqslant n. \tag{53}$$

If $|\mathrm{Aut}(f, K, \xi)| \not\equiv 0 \bmod \pi$ for at least one $\xi \in Z$ then, by Lemma 23, $\mathrm{Aut}(f, K, \xi)$ is cyclic of order $l < n$ with $l \not\equiv 0 \bmod \pi$. By Lemma 1 we have $\zeta_l + \zeta_l^{-1} \in K$. Moreover, by (52),

$$|\mathrm{Aut}(f, K)| = lm(\xi),$$

which together with (53) gives (49).

If $|\mathrm{Aut}(f, K, \xi)| \equiv 0 \bmod \pi$ for all $\xi \in Z$, then, by Lemma 24, $m(\xi) \not\equiv 0 \bmod \pi$, hence by (52),

$$|\mathrm{Aut}(f, K, \xi)| \equiv 0 \bmod q$$

and $\mathrm{Aut}_\pi(f, K, \xi)$ is a π-Sylow subgroup of $\mathrm{Aut}(f, K)$. Since all π-Sylow subgroups are conjugate and the only conjugates of $\mathrm{Aut}_\pi(f, K, \xi)$ in $\mathrm{Aut}(f, K)$ are, by Lemma 17, the groups $\mathrm{Aut}_\pi(f, K, \eta)$, where $e_f(\eta) = e_f(\xi)$, it follows that for all $\xi \in Z$, $m(\xi) = |Z|$, $e_f(\xi)$ has the same value, say k, and the number σ of π-Sylow subgroups is $|Z| \geqslant 3$. It follows, by Lemma 11, that either

$$\pi = 2, \quad |Z| = 2\varrho + 1, \quad \mathrm{Aut}(f, K) \cong \mathfrak{D}_{2\varrho+1}, \tag{54}$$

or

$$\pi = 3, \quad |Z| = 10, \quad \mathrm{Aut}(f, K) \cong \mathfrak{A}_5, \tag{55}$$

or

$$|Z| = q + 1, \quad \mathrm{Aut}(f, K) \cong \mathcal{H}_i, \tag{56}$$

where $\mathcal{H}_1 = \mathrm{PGL}_2(\mathbb{F}_q)$ and $\mathcal{H}_2 = \mathrm{PSL}_2(\mathbb{F}_q)$.

For $k = 1$ the case (54) gives (47), while (55) gives (48). For $k > 1$, (54) and (55) give (49) with $l = 2\varrho + 1, m = 2$ or $l = 10, m = 6$, respectively. The case (56) for $q = 2$ gives (47) with $\varrho = 1$. For $q > 2$, (56) gives

$$|\operatorname{Aut}(f, K, \xi)| = q^2 - q \quad \text{or} \quad (q^2 - q)/(\pi + 1, 2).$$

In the notation of Lemma 23, $l = q - 1$ or $(q - 1)/(\pi + 1, 2)$, hence $q > 1$ and, by Lemma 24, $\xi \in K$. The condition $\zeta_l \in K(\xi)$ of Lemma 23 now gives $\mathbb{F}_q \subset K$.

By Lemma 13, $\operatorname{Aut}(f, K)$ is conjugate in $\mathrm{PGL}_2(K)$ to $\mathcal{H}_i K^*/K^*$, hence there exist $\alpha, \beta, \gamma, \delta$ in K such that $\alpha\delta - \beta\gamma \neq 0$ and

$$\operatorname{Aut}(f, K) = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^{-1} \mathcal{H}_i \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} K^*/K^*. \tag{57}$$

Since $e_f(\xi) = k$ for all $\xi \in Z$, we have

$$f = f_1^k, \quad \text{where} \quad f_1 \in \overline{K}[x, y], \ \deg f_1 = |Z|. \tag{58}$$

Put

$$f_2 = f_1(\delta x - \beta y, -\gamma x + \alpha y), \quad a_0 = (\alpha\delta - \beta\gamma)^{-n}.$$

It follows from (58) that

$$f = a_0 f_2(\alpha x + \beta y, \gamma x + \delta y)^k, \quad \deg f_2 = q + 1, \tag{59}$$

and

$$\operatorname{Aut}(f, K) = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^{-1} \operatorname{Aut}(f_2, K) \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}. \tag{60}$$

Hence, by (57),

$$\operatorname{Aut}(f_2, K) = \mathcal{H}_i K^*/K^*. \tag{61}$$

By Corollary 8, applied with $\mathcal{G} = \operatorname{Aut}(f_2, K)\overline{K}^*/\overline{K}^*$, by Definition 5 and Lemmas 8 and 9 we obtain

$$f_2 = \chi_1^{c_1} \chi_2^{c_2} \psi(p, q),$$

where

$$\chi_1 = y \prod_{\xi \in \mathbb{F}_q} (x - \xi y), \quad \chi_2 = \prod_{\xi \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q} (x - \xi y), \quad p = \chi_1^{|\mathcal{H}_i|/(q+1)}, \quad q = \chi_2^{|\mathcal{H}_i|/(q^2-q)}$$

and ψ is a form over $\overline{K}$. The condition $\deg f_2 = q + 1$ implies $c_1 = 1, c_2 = 0, \psi \in \overline{K}$, $f_2 = (x^q y - x y^q)\psi$, hence (46) follows from (59). Since $\operatorname{Aut}(x^q y - x y^q, K) \supset \mathrm{PGL}_2(\mathbb{F}_q)K^*/K^*$ we have $i = 1$ in (61) and $\operatorname{Aut}(f, K) \cong \mathrm{PGL}_2(\mathbb{F}_q)$ by (60). This has been deduced from the assumption that $|\operatorname{Aut}(f, K, \xi)| \equiv 0 \bmod \pi$ for all ξ, while in the opposite case one of the formulae (47)–(49) holds. Since f_2 does not satisfy (47)–(49), we have, indeed, $\operatorname{Aut}(f, K) \cong \operatorname{Aut}(f_2, K) \cong \mathrm{PGL}_2(\mathbb{F}_q)$. □

Proof of Corollary 12. By Theorem 4 the condition given in the corollary is sufficient. In order to prove that it is necessary assume that K is infinite and f has at most two coprime

linear factors over $\overline{K}$. We distinguish three cases: the zeros of $f(x, 1)$ are in K; the zeros of $f(x, 1)$ are conjugate quadratic irrationalities over K and $\pi \neq 2$; and the zeros of $f(x, 1)$ are conjugate quadratic irrationalities over K and $\pi = 2$.

In the first case f is equivalent over K to a form $f_1 = ax^m y^n$, where $a \in K$, m, n are non-negative integers and f has infinitely many pairwise inequivalent weak automorphs $\left(\begin{smallmatrix}\alpha & 0\\ 0 & 1\end{smallmatrix}\right)K^*$, $\alpha \in K^*$.

In the second case f is equivalent over K to a form $f_2 = a(x^2 - cy^2)^m$, where $a, c \in K^*$, $m \in \mathbb{N}$ and f_1 has infinitely many pairwise inequivalent weak automorphs $\left(\begin{smallmatrix}\alpha & c\gamma\\ \gamma & \alpha\end{smallmatrix}\right)K^*$, where $\langle \alpha, \gamma \rangle$ runs through infinitely many solutions in K of the equation $\alpha^2 - c\gamma^2 = 1$, and from each pair $\langle \alpha, \gamma \rangle$, $\langle -\alpha, -\gamma \rangle$ we use only one solution.

In the third case f is equivalent over K to a form $f_3 = a(x^2 + bxy + cy^2)^m$, where $a, b, c \in K^*$ and $m \in \mathbb{N}$. Now we distinguish two subcases.

If c/b^2 is algebraic over $\mathbb{F}_2$ then $(c/b^2)^{2k-1} = 1$ for a certain $k \in \mathbb{N}$, hence $c = d^2$, where $d = b(c/b^2)^k \in K^*$. It follows that f_3 has infinitely many pairwise inequivalent weak automorphs $\left(\begin{smallmatrix}d\alpha & bd\alpha + d^2\\ 1 & d\alpha\end{smallmatrix}\right)K^*$, where α runs over K^*. On the other hand, f_3 has a weak automorph $\left(\begin{smallmatrix}c & bc\\ b & b^2 + c\end{smallmatrix}\right)K^*$.

If c/b^2 is transcendental over $\mathbb{F}_2$, then this automorph is of infinite order in $\mathrm{PGL}_2(K)$. Indeed, otherwise we should have (see proof of Lemma 1) for a certain $\lambda \in \overline{K}$ and a root of unity ζ, $\lambda(1 + \zeta) = b^2$, $\lambda^2\zeta = c^2$, hence $\zeta + \zeta^{-1} = b^4/c^2$, a contradiction. □

Proof of Corollary 13. We have $\zeta_\nu \in K$ for $\nu \leqslant 2$, and $\zeta_\nu + \zeta_\nu^{-1} \in K$ for $\nu \leqslant 4$ or $\nu = 6$.□

For the proof of Theorem 5 we need six lemmas.

Lemma 25. *Assume $n \geqslant 3$ and either $\pi = 0$ or $\pi > n$. If f of degree n has at least three coprime linear factors over $\overline{K}$ and* $\mathrm{Aut}(f, K)$ *is cyclic, then*

$$|\mathrm{Aut}(f, K)| \leqslant \begin{cases} a_1(n, K) & \text{if } f \in \overline{K}[x, y], \\ \max\{a_2(n, K), b(n-1, K)\} & \text{if } f \in K[x, y]. \end{cases}$$

There exist forms $f_1 \in \overline{K}[x, y]$, $f_2, f_3 \in K[x, y]$ of degree n, each with at least three coprime linear factors over $\overline{K}$ and not a perfect power in $\overline{K}[x, y]$, such that

$$\begin{aligned} \big|\mathrm{Aut}(f_1, K)\big| &\geqslant a_1(n, K), \\ \big|\mathrm{Aut}(f_2, K)\big| &\geqslant a_2(n, K), \\ \big|\mathrm{Aut}(f_3, K)\big| &\geqslant b(n-1, K). \end{aligned}$$

Proof. If $\mathcal{G} = \mathrm{Aut}(f, K)$ is cyclic, then by Theorem 1 and Corollary 5,

$$f = \chi_1^{c_1}\chi_2^{c_2}\psi(p, q), \tag{62}$$

where

$$\deg \chi_i = 1, \quad \deg p = \deg q = |\mathcal{G}|,$$

and ψ is a form over $\overline{K}$ or over K if $f \in \overline{K}[x, y]$ or $f \in K[x, y]$, respectively. By the assumption on linear factors of f, we have $\deg \psi \geqslant 1$, hence

$$n = \deg f = c_1 + c_2 + |\mathcal{G}| \deg \psi \geqslant |\mathcal{G}|. \tag{63}$$

On the other hand, by Lemma 1,

$$\eta_{|\mathcal{G}|} := \zeta_{|\mathcal{G}|} + \zeta_{|\mathcal{G}|}^{-1} \in K, \tag{64}$$

hence by Definition 7,

$$|\mathcal{G}| \leqslant a_1(n, K). \tag{65}$$

To estimate $|\mathcal{G}|$ for $f \in K[x, y]$ a division into cases is necessary.

If $c_1 + c_2 \equiv 0 \bmod 2$, then

$$n \equiv |\mathcal{G}| \deg \psi \bmod 2.$$

For n odd this implies $n \equiv |\mathcal{G}| \bmod 2$, hence

$$|\mathcal{G}| \leqslant a_2(n, K). \tag{66}$$

For n even either $\deg \psi \equiv 1 \bmod 2$, and then again (66) holds, or $\deg \psi \equiv 0 \bmod 2$, in which case by (63) and (64),

$$|\mathcal{G}| \leqslant a_1(n/2, K).$$

But

$$n \equiv 0 \bmod 2 \quad \text{implies} \quad a_1(n/2, K) \leqslant a_2(n, K), \tag{67}$$

since if $a_1(n/2, K) \equiv 1 \bmod 2$, we have

$$2a_1(n/2, K) \leqslant n \quad \text{and} \quad \eta_{2a_1(n/2,K)} \in K.$$

If $c_1 + c_2 \equiv 1 \bmod 2$, then $c_1 \neq c_2$, hence $\chi_1 \in K[x, y]$ by Theorem 1, and $\zeta_{|\mathcal{G}|} \in K$ by Lemma 14. Now (63) implies $|\mathcal{G}| \leqslant n - 1$, hence by Definition 7,

$$|\mathcal{G}| \leqslant b(n - 1, K),$$

which together with (65) and (66) proves the first part of the lemma.

To prove the second part we put

$$f_1 = \chi_1^{n-a_1(n,K)}(p + q), \ f_2 = (\chi_1\chi_2)^{(n-a_2(n,K))/2}(p + q), \ f_3 = \chi_1^{n-b(n-1,K)}(p + q),$$

where χ_1, χ_2 and p, q are given in Definition 5 for $\mathcal{G}$ cyclic of order $a_1(n, K)$, $a_2(n, K)$, $b(n - 1, K)$, respectively. Now $p + q$ is prime to $\chi_1\chi_2$, is not a perfect power in $\overline{K}[x, y]$ and has $|\mathcal{G}|$ coprime linear factors over $\overline{K}$. Hence the f_i are not perfect powers and since for $n \geqslant 3$, by Corollary 13, $a_1(n, K) \geqslant 3$, $a_2(n, K) \geqslant 3$, $b(n - 1, K) \geqslant 2$, each f_i has at least three coprime linear factors over $\overline{K}$. □

Lemma 26. *Assume $n \geqslant 3$ and either $\pi = 0$ or $\pi > n$. If f of degree n has at least three coprime linear factors over $\overline{K}$ and* $\mathrm{Aut}(f, K)$ *is dihedral, then*

$$|\mathrm{Aut}(f, K)| \leqslant 2a_2(n, K).$$

There exists a form $f_0 \in K[x, y]$ *of degree n, with at least three coprime linear factors over* $\overline{K}$ *and not a perfect power in* $\overline{K}[x, y]$*, such that*

$$|\mathrm{Aut}(f_0, K)| \geqslant 2a_2(n, K).$$

Proof. If $\mathcal{G} = \mathrm{Aut}(f, K)$ is dihedral, then by Lemma 7, Theorem 2 and Corollary 8,

$$f = \chi_1^{c_1}\chi_2^{c_2}\chi_3^{c_3}\psi(p, q), \tag{68}$$

where

$$\deg \chi_1 = \deg \chi_2 = |\mathcal{G}|/2, \quad \deg p = \deg q = |\mathcal{G}|$$

and ψ is a binary form over $\overline{K}$ or K if $f \in \overline{K}[x, y]$ or $f \in K[x, y]$, respectively. On the other hand, by Lemma 1,

$$\eta_{|\mathcal{G}|/2} \in K. \tag{69}$$

It follows from (68) that

$$n = c_1|\mathcal{G}|/2 + c_2|\mathcal{G}|/2 + 2c_3 + |\mathcal{G}| \deg \psi. \tag{70}$$

For n odd it follows that $|\mathcal{G}|/2 \equiv 1 \bmod 2$ and $c_1 + c_2 \equiv 1 \bmod 2$, hence

$$|\mathcal{G}|/2 \leqslant n, \quad |\mathcal{G}|/2 \equiv n \bmod 2,$$

thus by Definition 7 and (69),

$$|\mathcal{G}| \leqslant 2a_2(n, K). \tag{71}$$

For n even, if $c_1 + c_2 \equiv 1 \bmod 2$, the same inequality holds; if $c_1 + c_2 \equiv 0 \bmod 2$, then, by (70) and the assumption on linear factors of f, either $c_1 + c_2 \geqslant 2$ or $\psi \notin K$, hence

$$|\mathcal{G}|/2 \leqslant n/2, \quad |\mathcal{G}|/2 \leqslant 2a_1(n/2, K),$$

and by (67) we again obtain (71).

In order to prove the second part of the lemma we put

$$f_0 = \chi_2\chi_3^{(n-a_2(n,K))/2},$$

where χ_2, χ_3 are given in the Example (p. 802) for $\mathcal{G}$ dihedral of order $2a_2(n, K)$ with $a = 1, b = 0$. Since $\deg \chi_2 = a_2(n, K)$ and $\deg \chi_3 = 2$ we have $\deg f_0 = n$, and since $\chi_2, \chi_3 \in K[x, y]$ we have $f_0 \in K[x, y]$.

Now, χ_2 is prime to χ_3, is not a perfect power in $\overline{K}[x, y]$ and has $a_2(n, K) \geqslant 3$ coprime linear factors over $\overline{K}$. Hence f_0 is not a perfect power in $\overline{K}[x, y]$ and has at least three coprime linear factors over $\overline{K}$. □

Lemma 27. *Let* $n \geqslant 3$ *and either* $\pi = 0$ *or* $\pi > n$ *and let* $f \in \overline{K}[x, y]$ *be a form of degree n and not a perfect power. If* $\mathrm{Aut}(f, K)$ *contains a subgroup isomorphic to* $\mathcal{G}_i$*, where* $\mathcal{G}_1 = \mathfrak{A}_4$, $\mathcal{G}_2 = \mathfrak{S}_4$, $\mathcal{G}_3 = \mathfrak{A}_5$, *then*

$$n = c_1\frac{|\mathcal{G}_i|}{i+2} + c_2\frac{|\mathcal{G}_i|}{3} + c_3\frac{|\mathcal{G}_i|}{2} + c_4|\mathcal{G}_i|, \tag{72}$$

where c_i are non-negative integers and

$$\text{either } (c_1, c_2, c_3) = 1 \text{ or } c_4 \neq 0. \tag{73}$$

Moreover,

$$\text{level } K \leqslant 2 \quad \text{and} \quad \text{if} \quad i = 3, \text{ then } \sqrt{5} \in K. \tag{74}$$

If (72)–(74) *are satisfied with $c_4 = 0$, then there exists a form $f \in \overline{K}[x, y]$ of degree n, with at least three coprime linear factors over $\overline{K}$ and not a perfect power in $\overline{K}[x, y]$, such that* $\mathrm{Aut}(f, K)$ *contains $\mathcal{G}_i$. Moreover, for $i > 1$ such a form f exists in $K[x, y]$.*

Proof. If $\mathrm{Aut}(f, K)$ contains a subgroup isomorphic to $\mathcal{G}_i$, then $\mathrm{PGL}_2(K)$ contains such a subgroup, hence (74) holds by Lemma 2. Further, by Corollary 8, we have

$$f = \prod_{i=1}^{k} \chi_i^{c_i} \psi(p, q), \tag{75}$$

where χ_i and p, q are given in Definition 5 and ψ is a binary form over $\overline{K}$. By Lemma 7 we have $h = 3$,

$$\deg \chi_1 = \frac{|\mathcal{G}_i|}{i+2}, \quad \deg \chi_2 = \frac{|\mathcal{G}_i|}{3}, \quad \deg \chi_3 = \frac{|\mathcal{G}_i|}{2}, \tag{76}$$

while, by Definition 5,

$$\deg p = \deg q = |\mathcal{G}_i|.$$

Now (72) follows from (75) with $c_4 = \deg \psi$, and (73) follows from (75) and the condition that f is not a perfect power in $\overline{K}[x, y]$.

In the opposite direction, if (72)–(74) hold with $c_4 = 0$, we take

$$f = \prod_{i=1}^{3} \chi_i^{c_i}.$$

By Definition 5, χ_i are coprime and separable, hence the number of coprime linear factors of f over $\overline{K}$ is at least

$$|\mathcal{G}_i| \left(\frac{\operatorname{sgn} c_1}{i+2} + \frac{\operatorname{sgn} c_2}{3} + \frac{\operatorname{sgn} c_3}{2} \right) \geqslant \frac{|\mathcal{G}_i|}{i+2} \geqslant 4.$$

Also f is not a perfect power in $\overline{K}[x, y]$, since $(c_1, c_2, c_3) = 1$ by (73). For $i > 1$, χ_i are of distinct degrees, hence no two of them are conjugate over K and, by Corollary 6, they are in $K[x, y]$. Thus $f \in K[x, y]$. □

Lemma 28. *Assume $\pi = 0$ or $\pi > 3$. A quartic form $f \in K[x, y]$ with at least three coprime linear factors over $\overline{K}$, which is not a perfect power in $\overline{K}[x, y]$ and for which* $\mathrm{Aut}(f, K)$ *contains a subgroup isomorphic to $\mathfrak{A}_4$, exists if and only if $\sqrt{-3} \in K$.*

Proof. If $\mathrm{Aut}(f, K)$ contains a subgroup isomorphic to $\mathfrak{A}_4$, then it has an element of order 3. By Corollary 3 it follows that either $\sqrt{-3} \in K$, or f is square in $K[x, y]$, the possibility excluded by the condition on f.

For the opposite direction, we take $f = x^4 - xy^3$. This form has two non-trivial weak automorphs defined over K,

$$S = \begin{pmatrix} -1 & 1 \\ 2 & 1 \end{pmatrix} K^*, \quad T = \begin{pmatrix} \zeta_3 & 0 \\ 0 & 1 \end{pmatrix} K^*.$$

They satisfy the equations $S^2 = E$, $T^3 = E$, $TST = ST^{-1}S$, hence $\langle S, T\rangle \cong \mathfrak{A}_4$. □

Lemma 29. *If* level $K \leqslant 2$, $\sqrt{5} \in K$ *and either* $\pi = 0$ *or* $\pi > 5$, *then there exists a form* $f \in K[x, y]$ *of degree* 60, *with at least three coprime linear factors over* $\overline{K}$ *and not a perfect power in* $\overline{K}[x, y]$, *such that* $\mathrm{Aut}(f, K)$ *contains a subgroup isomorphic to* $\mathfrak{A}_5$.

Proof. By Lemma 2, $\mathrm{PGL}_2(K)$ contains a subgroup isomorphic to $\mathfrak{A}_5$. Let χ_1, χ_2, χ_3 be the polynomials defined in Definition 5 for this group $\mathcal{G}$, such that $\chi_i \in K[x, y]$ and

$$\deg \chi_1 = 12, \quad \deg \chi_2 = 20, \quad \deg \chi_3 = 30$$

(see the proof of Lemma 27). We assert that for a certain $\varepsilon = \pm 1$,

$$f_\varepsilon = \chi_1^5 + \varepsilon \chi_2^\varepsilon$$

has the required properties.

If r_ε is the number of distinct zeros of $f_\varepsilon(x, 1)$, then by the *abc*-theorem for polynomials (see [18])

$$r_\varepsilon > 60 - \deg \chi_1(x, 1) - \deg \chi_2(x, 1) \geqslant 28,$$

thus f_ε has at least 29 coprime linear factors over $\overline{K}$. If f_ε is a perfect power in $\overline{K}[x, y]$, then

$$f_\varepsilon = g_\varepsilon^2, \quad g_\varepsilon \in \overline{K}[x, y].$$

Moreover, $\mathrm{Aut}(g_\varepsilon, K) = \mathrm{Aut}(f_\varepsilon, K)$, hence $\mathrm{Aut}(g_\varepsilon, K)$ contains $\mathcal{G}$ and, by Corollary 8,

$$g_\varepsilon = \prod_{i=1}^{3} \chi_i^{d_{\varepsilon i}} \psi_\varepsilon, \quad \psi_\varepsilon \in \overline{K}.$$

Since $(f_\varepsilon, \chi_1\chi_2) = 1$ and $\deg f_\varepsilon = 2 \deg \chi_3$ we conclude that

$$d_{\varepsilon 1} = d_{\varepsilon 2} = 0, \quad d_{\varepsilon 3} = 1$$

and

$$f_\varepsilon = \psi_\varepsilon^2 \chi_3^2.$$

If this holds for $\varepsilon = 1$ and $\varepsilon = -1$, then

$$2\chi_1^5 = f_1 + f_{-1} = (\psi_1^2 + \psi_{-1}^2)\chi_3^2,$$

which contradicts $(\chi_1, \chi_3) = 1$. □

Lemma 30. *The equation*

$$m = 3c_1 + 4c_2 + 6c_3 \tag{77}$$

is solvable in relatively prime non-negative integers for every $m \geqslant 9$, and the equation

$$m = 6c_1 + 10c_2 + 15c_3 \tag{78}$$

is solvable in such integers if and only if $m \in \mathcal{M} \setminus \{30\}$.

Proof. Solvability of (77) for $m < 12$ can be checked case by case. By a classical theorem due to Curran Sharp [8] every integer greater than $ab - a - b$ is a linear combination of a, b with non-negative coefficients. For $m \geqslant 12$ we have $m - 6 \geqslant 6$ and hence $m - 6 = 3c_1 + 4c_2$, where c_1, c_2 are non-negative integers. It suffices to take $c_3 = 1$.

Solvability of (78) for odd $m < 31$ and for even $m < 76$ can be checked case by case. For odd $m \geqslant 31$, $(m - 15)/2 \geqslant 8$ is an integer and, by Curran Sharp's theorem, $(m - 15)/2 = 3c_1 + 5c_2$, where c_1, c_2 are non-negative integers. It suffices to take $c_3 = 1$. For even $m \geqslant 76$, $(m - 30)/2 \geqslant 23$ is an integer, hence by Curran Sharp's theorem $(m - 30)/2 = 3d_1 + 5d_2$, where d_1, d_2 are non-negative integers. Moreover, since $23 > 3 \cdot 4 + 5 \cdot 2$, we have either $d_1 \geqslant 5$ or $d_2 \geqslant 3$. If at least one d_i is odd we take $c_1 = d_1, c_2 = d_2, c_3 = 2$, otherwise we take $c_3 = 2$ and either $c_1 = d_1 - 5, c_2 = d_2 + 3$ or $c_1 = d_1 + 5, c_2 = d_2 - 3$. □

Proof of Theorem 5. The assumption that f is not a perfect power in $\overline{K}[x, y]$ implies in the case (46) that $k = 1, n = q + 1$. This gives $A(\pi^g + 1, K) = B(\pi^g + 1, K) = \pi^{3g} - \pi^g$ if $\mathbb{F}_{\pi^g} \subset K$. On the other hand, (47)–(49) imply

$$|\mathrm{Aut}(f, K)| \leqslant n(n-1),$$

hence $A(n, K) \leqslant n(n-1)$ if either $n \neq \pi^g + 1$ or $\mathbb{F}_{\pi^g} \not\subset K$. This bound is attained for every $\pi > 0$ and $n = \pi^g$. Indeed, for $q = \pi^g$,

$$\mathrm{Aut}(x^q - xy^{q-1}, \mathbb{F}_q) \supset \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} K^* : \alpha \in \mathbb{F}_q^*,\ \beta \in \mathbb{F}_q \right\}.$$

Assume now that $\pi = 0$ or $\pi > n$. By Theorem 4,

$$|\mathrm{Aut}(f, K)| \not\equiv 0 \bmod \pi$$

and, by Lemma 7, $\mathcal{G} = \mathrm{Aut}(f, K)$ is either cyclic, dihedral or polyhedral. The first two cases are considered in Lemmas 25 and 26. If $\mathcal{G}$ is a polyhedral group, then (72) holds by Lemma 27, and since all terms on the right hand side are even, n is even.

For n odd it follows that $\mathrm{Aut}(f, K)$ is either cyclic or dihedral, and by Lemmas 25, 26,

$$A(n, K) \leqslant \max\{a_1(n, K), 2a_2(n, K)\},$$
$$B(n, K) \leqslant \max\{b(n-1, K), 2a_2(n, K)\}.$$

The inequalities in the opposite direction follow from the second part of Lemmas 25 and 26. This gives the theorem for n odd.

For n even a further study of polyhedral groups is necessary. For $n = 4$ equation (72) gives $i = 1$, $|\mathcal{G}_i| = 12$, $c_3 = c_4 = 0$. Since $12 > 8 = \max\{a_1(4, K), 2a_2(4, K)\}$ we obtain from Lemmas 25–27,

$$A(4, K) = \begin{cases} 12 & \text{if level } K \leqslant 2, \\ \max\{a_1(4, K), 2a_2(4, K)\} & \text{otherwise,} \end{cases}$$

and from Lemmas 25, 26 and 28,

$$B(4, K) = \begin{cases} 12 & \text{if } \sqrt{-3} \in K, \\ \max\{b(3, K), 2a_2(4, K)\} & \text{otherwise.} \end{cases}$$

For even $n > 4$ we have $2a_2(n, K) \geqslant 12$, hence the equation (72) is of interest only for $i > 1$, and if $n < |\mathcal{G}|$, then $(c_1, c_2, c_3) = 1$ by (72), (73).

For $n = 6, 8, 14$ and $i > 1$, (72) gives $i = 2$ and $\langle c_1, c_2, c_3\rangle = \langle 1, 0, 0\rangle$ or $\langle 0, 1, 0\rangle$ or $\langle 1, 1, 0\rangle$, respectively. It follows by Lemmas 25–27 that for $n = 6, 8, 14$,

$$A(n, K) = \begin{cases} \max\{a_1(n, K), 2a_2(n, K), 24\} & \text{if level } K \leqslant 2, \\ \max\{a_1(n, K), 2a_2(n, K)\} & \text{otherwise;} \end{cases}$$

$$B(n, K) = \begin{cases} \max\{b(n-1, K), 2a_2(n, K), 24\} & \text{if level } K \leqslant 2, \\ \max\{b(n-1, K), 2a_2(n, K)\} & \text{otherwise.} \end{cases}$$

For $n = 10, 16$ the equation (72) has no solution with $i > 1$ and $(c_1, c_2, c_3) = 1$, hence, by Lemmas 25–27,

$$A(n, K) = \max\{a_1(n, K), 2a_2(n, K)\},$$
$$B(n, K) = \max\{b(n-1, K), 2a_2(n, K)\}.$$

For $n = 12$, $i > 1$ and $(c_1, c_2, c_3) = 1$, (72) gives $i = 2$, $\langle c_1, c_2, c_3\rangle = \langle 0, 0, 1\rangle$ or $i = 3$, $\langle c_1, c_2, c_3\rangle = \langle 1, 0, 0\rangle$. Hence, by Lemmas 25–27,

$$A(12, K) = \begin{cases} \max\{a_1(n, K), 2a_2(n, K), 24\} & \text{if level } K \leqslant 2,\ \sqrt{5} \notin K, \\ 60 & \text{if level } K \leqslant 2,\ \sqrt{5} \in K, \\ \max\{a_1(n, K), 2a_2(n, K)\} & \text{otherwise;} \end{cases}$$

$$B(12, K) = \begin{cases} \max\{b(n-1, K), 2a_2(n, K), 24\} & \text{if level } K \leqslant 2,\ \sqrt{5} \notin K, \\ 60 & \text{if level } K \leqslant 2,\ \sqrt{5} \in K, \\ \max\{b(n-1, K), 2a_2(n, K)\} & \text{otherwise.} \end{cases}$$

By Lemma 30 for $n = 2m$, $m \geqslant 9$, (72) always has a solution with $i = 2$, $c_4 = 0$, $(c_1, c_2, c_3) = 1$, and has a solution with $i = 3$, $c_4 = 0$, $(c_1, c_2, c_3) = 1$ if and only if $m \in \mathcal{M} \setminus \{30\}$. Since $\mathcal{M}$ contains all integers greater than 29 except 32 and 44, by Lemmas 25–27, the formulae for $A(n, K)$ and $B(n, K)$ hold for all even n, except possibly for $n = 2m, m = 30, 32, 44$. For $m = 30$ the formulae follow from Lemmas 25, 26 and 29, for $m = 32$ or 44 the only solution of (72) does not satisfy (73), hence the formulae follow from Lemmas 25–27. □

Proof of Corollary 14. For $K = \mathbb{C}$ we have $a_1(n, K) = n = a_2(n, K)$. □

4. Criteria for a form to have a non-trivial automorph over a given arbitrary field

Theorem 6. *Let $f \in K[x, y]$ be a form of degree $n > 2$ without multiple factors over $\overline{K}$. If* $\mathrm{Aut}(f, K)$ *is non-trivial and $f(x, 1)$ of degree m is irreducible over K, then the Galois*

group of $f(x,1)$ over K is either imprimitive or cyclic of prime order m. For $n \leqslant 4$ the converse holds unless $n = 4$ and $m = 3$.

Corollary 15. *Assume that K contains no primitive cubic root of unity and $f \in K[x,y]$ is a form of degree $2, 3$ or 4 without multiple factors over $\overline{K}$. The group $\mathrm{Aut}(f,K)$ is non-trivial if and only if the Galois group of $f(x,1)$ over K is either transitive imprimitive or abelian with the lengths of orbits not $\langle 3,1\rangle$.*

Corollary 16. *Let $f \in K[x,y]$ be a cubic form with $f(1,0) \neq 0$ and without multiple factors over $\overline{K}$ and $\mathfrak{G}$ be the Galois group of $f(x,1)$ over K. Then $\mathrm{Aut}(f,K) \cong \mathfrak{D}_3$ if $\mathfrak{G} \cong \mathfrak{C}_1$, $\mathrm{Aut}(f,K) \cong \mathfrak{C}_2$ if $\mathfrak{G} \cong \mathfrak{C}_2$, $\mathrm{Aut}(f,K) \cong \mathfrak{C}_3$ if $\mathfrak{G} \cong \mathfrak{C}_3$, and $\mathrm{Aut}(f,K) \cong \mathfrak{C}_1$ if $\mathfrak{G} \cong \mathfrak{D}_3$.*

Remark 11. For quartic forms f the structure of the Galois group $\mathfrak{G}(f)$ of $f(x,1)$ over $\mathbb{Q}$ does not determine in general the structure of $\mathrm{Aut}(f,\mathbb{Q})$, for instance for $f_1 = x^4+x^3y+x^2y^2+xy^3+y^4$, $f_2 = x^4+4x^3y-6x^2y^2-4xy^3+y^4$, $\mathfrak{G}(f_i) \cong \mathfrak{C}_4$, while $\mathrm{Aut}(f_1,\mathbb{Q}) \cong \mathfrak{C}_2$ (proof by means of Lemma 17), and $\mathrm{Aut}(f_2,\mathbb{Q})$ contains $\mathfrak{C}_4$ generated by $\left(\begin{smallmatrix} 1 & 1 \\ -1 & 1 \end{smallmatrix}\right)\mathbb{Q}^*$.

The proof of Theorem 6 is based on the following

Lemma 31. *Given a pair $\langle g,h\rangle$ of coprime binary forms over K each of degree at most 2 and not both in $K[x^\pi, y^\pi]$, there exists a non-trivial common weak automorph T of g and h. Moreover, if*

$$g = \sum_{i=0}^{2} a_i x^{2-i} y^i, \quad h = \sum_{i=0}^{2} b_i x^{2-i} y^i$$

we can take

$$T = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} K^*, \quad \textit{where} \quad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} -a_0b_2 + a_2b_0 & -a_1b_2 + a_2b_1 \\ a_0b_1 - a_1b_0 & a_0b_2 - a_2b_0 \end{pmatrix}.$$

Proof. If g, h are both of degree 2 and T is as above we have

$$\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = -R(g,h) \neq 0,$$

where $R(g,h)$ is the resultant of g and h (see [21, p. 219]). Also $\langle \alpha,\beta,\gamma,\delta\rangle = \langle \alpha,0,0,\alpha\rangle$ implies $\pi = 2$, $a_i = b_i = 0$, $g \in K[x^\pi, y^\pi]$, $h \in K[x^\pi, y^\pi]$, contrary to assumption. Moreover

$$g(\alpha x + \beta y,\ \gamma x + \delta y) = R(g,h)g(x,y),$$
$$h(\alpha x + \beta y,\ \gamma x + \delta y) = R(g,h)h(x,y),$$

thus T is a common weak automorph of g and h. The case where one of the forms g, h is linear is reduced to the former by replacing this form by its square. □

Proof of Theorem 6. *Necessity.* By the assumption f is not divisible by y^2, hence $f(x,1)$ is of degree $m \geqslant n-1 \geqslant 2$. If $m = 2$ the assertion is trivial, thus assume $m \geqslant 3$. Let

$Z = \{\xi \in \overline{K} \cup \{\infty\} : e_f(\xi) > 0\}$. By Lemma 17, if $T \in \mathrm{Aut}(f, K)$, we have $T^*(Z) = Z$ and since $T^*\infty \in K \cup \{\infty\}$, f has no zeros in K and $T^*(Z \setminus \{\infty\}) = Z \setminus \{\infty\}$. If T is non-trivial, the orbits of $Z \setminus \{\infty\}$ under the action of T^*, say $O_1, \ldots, O_l$, are of lengths greater than 1, since the equation $T^*\xi = \xi$ gives $[K(\xi) : K] \leqslant 2 < m$. They are blocks of imprimitivity of the Galois group $\mathcal{G}$ in question, provided $l > 1$. Indeed, if $\tau \in \mathcal{G}$ and $\xi \in O_i$, $\tau(\xi) \in O_j$, then $\tau(T^*\xi) = T^*\tau(\xi) \in O_j$. If $l = 1$, but m is composite, $m = m_1 m_2$, $m_i > 1$, we replace T by T^{m_1} and l by m_1. It remains to consider the case $l = 1$, m a prime. Then $T^* \in \mathcal{G}$. Indeed, since $f(x, 1)$ is irreducible, $\mathcal{G}$ is transitive, thus if $f(\xi, 1) = 0$ there exists $\tau_0 \in \mathcal{G}$ such that $\tau_0(\xi) = T^*\xi$. It follows that $\tau_0(T^{*i}\xi) = T^{*i}\tau_0(\xi) = T^{*i+1}(\xi)$, hence $\tau_0 = T^*$. Also for every $\tau \in \mathcal{G}$ we have $\tau(\xi) = T^{*j}\xi$ for some j, thus $\tau(T^{*i}\xi) = T^{*i}\tau(\xi) = T^{*i+j}\xi = T^{*j}(T^{*i}\xi)$ for each i, so $\tau = T^{*j}$, hence $\mathcal{G}$ is cyclic, generated by T^*.

Sufficiency for $n \leqslant 4$. In view of Lemma 31 and the condition $\langle n, m\rangle \neq \langle 4, 3\rangle$ it suffices to consider $f(x, 1)$ of degree n and monic. Let $n = 3$ and $f(x, 1) = x^3 + ax^2 + bx + c$. Since $\mathcal{G}$ is cyclic there exist d, e, g in K such that $f(\xi, 1) = 0$ implies $f(d\xi^2 + e\xi + g, 1) = 0$ where $\langle d, e, g\rangle \neq \langle 0, 0, g\rangle, \langle 0, 1, 0\rangle$. The system of three linear equations for $\alpha, \beta, \gamma, \delta$,

$$\begin{aligned} (e - ad)\gamma + d\delta &= 0,\\ -\alpha + (g - bd)\gamma + e\delta &= 0,\\ -\beta - cd\gamma + g\delta &= 0, \end{aligned}$$

has a non-zero solution $\langle \alpha, \beta, \gamma, \delta\rangle \in K^4$. This solution satisfies for all zeros ξ of $f(x, 1)$ the equation

$$(d\xi^2 + e\xi + g)(\gamma\xi + \delta) = \alpha\xi + \beta.$$

Note that $\gamma\xi + \delta = 0$ would give $\alpha = \beta = \gamma = \delta = 0$ since $\xi \notin K$, a contradiction. Hence $\gamma\xi + \delta \neq 0$ and

$$d\xi^2 + e\xi + g = \frac{\alpha\xi + \beta}{\gamma\xi + \delta}\,.$$

It follows that for some $r \in K$,

$$f\left(\frac{\alpha x + \beta}{\gamma x + \delta}\,, 1\right)(\gamma x + \delta)^3 = rf(x, 1)$$

and

$$f(\alpha x + \beta y,\ \gamma x + \delta y) = rf(x, y).$$

Observe that $\alpha\delta - \beta\gamma = 0$ or $\langle \alpha, \beta, \gamma, \delta\rangle = \langle \alpha, 0, 0, \alpha\rangle$ would give $d\xi^2 + e\xi + g \in K$ or $d\xi^2 + e\xi + g = \xi$, contrary to $[K(\xi) : K] = 3$.

Now, let $n = 4$. Since $m = 4$, $\mathcal{G}$ is imprimitive. It follows that f is reducible over a separable quadratic extension of K, say $K(\eta)$. Thus we have

$$f = b\Big(\sum_{i=0}^{2} a_i x^{2-i} y^i\Big)\Big(\sum_{i=0}^{2} a_i' x^{2-i} y^i\Big),$$

where $a_i, a_i' \in K(\eta)$ and a_i, a_i' are conjugate over K, while $b \in K$. Applying Lemma 31

with $b_i = a_i'$ we find that the factors of f have a common non-trivial automorph with the matrix

$$M = \begin{pmatrix} -a_0a_2' + a_2a_0' & -a_1a_2' + a_2a_1 \\ a_0a_1' - a_1a_0' & a_0a_2' - a_2a_0' \end{pmatrix},$$

hence also with the matrix $M/(\eta - \eta')$. However, the last matrix is invariant with respect to conjugation, so its elements are in K. □

Proof of Corollary 15. This follows at once from Theorem 6 and Corollary 2. □

Remark 12. The assumption $\zeta \notin K$, where ζ is a primitive cubic root of unity, cannot be omitted in Corollary 15, as the following example shows: $K = \mathbb{Q}(\zeta)$, $T = \left(\begin{smallmatrix} \zeta & 0 \\ 0 & 1 \end{smallmatrix}\right) K^*$, $f = x(x^3 + 2y^3)$.

Proof of Corollary 16. By Corollary 1, $\mathrm{Aut}(f, K)$ can contain a cyclic group $\mathfrak{C}_\nu$ for $\nu = 2$ or 3 only. The lengths of the orbits of an arbitrary set under the action of $\mathfrak{D}_2$ are even, hence, by Lemma 17, $\mathrm{Aut}(f, K)$ cannot contain a copy of $\mathfrak{D}_2$. On the other hand, $|\mathrm{Aut}(f, K)| \leqslant 6$ by Theorem 5. This limits the possible types of $\mathrm{Aut}(f, K)$ to $\mathfrak{D}_3$, $\mathfrak{C}_3$, $\mathfrak{C}_2$ and $\mathfrak{C}_1$. If $\mathcal{G} \cong \mathfrak{C}_1$, then f is equivalent over K to $axy(x+y)$ and $\mathrm{Aut}(f, K)$ contains the automorphs $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) K^*$ and $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right) K^*$ of orders 2 and 3, respectively, thus $\mathrm{Aut}(f, K) \cong \mathfrak{D}_3$. If $\mathcal{G} \cong \mathfrak{C}_2$, then, by Corollary 2, $\mathrm{Aut}(f, K)$ does not contain $\mathfrak{C}_3$ and, by Lemma 31, $\mathrm{Aut}(f, K)$ contains a $\mathfrak{C}_2$, thus $\mathrm{Aut}(f, K) \cong \mathfrak{C}_2$. If $\mathcal{G} \cong \mathfrak{C}_3$, then, by Theorem 6, $\mathrm{Aut}(f, K)$ is non-trivial, while, by Corollary 1, it does not contain $\mathfrak{C}_2$, hence $\mathrm{Aut}(f, K) \cong \mathfrak{C}_3$. Finally, if $\mathcal{G} \cong \mathfrak{D}_3$, then $\mathrm{Aut}(f, K) \cong \mathfrak{C}_1$ by Theorem 6. □

5. The case of an algebraically closed field

In this section K is an algebraically closed field of characteristic π, and f is a non-singular binary form over K of degree n.

If $n = 3$, then $\mathrm{Aut}(f, K) \cong \mathfrak{D}_3$ by Corollary 16. We shall now consider $n = 4$.

Definition 10. For a form $f(x, y) = \sum_{i=0}^{4} a_i x^{4-i} y^i$ put

$$A(f) = a_2^2 - 3a_1a_3 + 12a_0a_4,$$
$$B(f) = 27a_1^2a_4 + 27a_0a_3^2 + 2a_2^3 - 72a_0a_2a_4 - 9a_1a_2a_3.$$

Remark 13. $A(f)$, $B(f)$ are invariants of f and satisfy

$$27D(f) = 4A(f)^3 - B(f)^2,$$

where $D(f)$ is the discriminant of f (see [27, Bd I, §70]).

Theorem 7. *For a non-singular quartic binary form f over K we have*

$$\mathrm{Aut}(f, K) \cong \begin{cases} \mathfrak{S}_4 & \text{if } A(f) = B(f) = 0, \\ \mathfrak{A}_4 & \text{if } A(f) = 0,\ B(f) \neq 0, \\ \mathfrak{D}_4 & \text{if } A(f) \neq 0,\ B(f) = 0, \\ \mathfrak{D}_2 & \text{if } A(f)B(f) \neq 0. \end{cases}$$

The proof is based on three lemmas.

Lemma 32. *For a non-singular quartic binary form f over K, $\mathrm{Aut}(f, K)$ contains $\mathfrak{C}_3$ if and only if $A(f) = 0$.*

Proof. Necessity. If $\pi \neq 3$ and the cyclic group in question is generated by $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) K^*$ we have, by Theorem 1,

$$f = \chi_i(a\chi_i^3 + b\chi_{3-i}^3) = a\chi_i^4 + b\chi_i\chi_{3-i}^3,$$

where $i \in \{1, 2\}$, χ_1, χ_2 are given in Definition 3 and a, b are in K. Denoting by R_1 the resultant of χ_1, χ_2 and by f_1 the form $ax^4 + bxy^3$ we obtain, by the above Remark,

$$A(f) = R_1^2 A(f_1) = 0.$$

If $\pi = 3$ we have, again by Theorem 1,

$$f = \chi_1(a\chi_1^3 + b(\lambda^2\chi_2^3 - \chi_2\chi_1^2)) = a\chi_1^4 - b\chi_1^3\chi_2 + b\lambda^2\chi_1\chi_2^3,$$

where λ, χ_1, χ_2 are as in Definition 4 and a, b are in K. Denoting by R_2 the resultant of χ_1, χ_2 and by f_2 the form $ax^4 - bx^3y + b\lambda^2xy^3$ we obtain, by the Remark,

$$A(f) = R_2^2 A(f_2) = 0.$$

Sufficiency. The form f is clearly equivalent, by a linear transformation over K, to a form

$$f_3 = xy(x^2 + axy - y^2).$$

The condition $A(f) = 0$ gives $a^2 + 3 = A(f_3) = 0$. If $\pi \neq 3$ we choose a primitive cubic root of unity ϱ and conclude that $a = \pm(\varrho^2 - \varrho)$. Then the transformation $T_2(x, y) = (\varrho^2 x \pm \varrho y, y)$ of order 3 in $\mathrm{PGL}_2(K)$ satisfies $f_3(T_2) = f_3$, hence $\mathrm{Aut}(f, K)$ conjugate to $\mathrm{Aut}(f_3, K)$ contains $\mathfrak{C}_3$.

If $\pi = 3$ the condition $A(f_3) = 0$ gives $a = 0$. Then the transformation $T_2(x, y) = (x+y, y)$ of order 3 in $\mathrm{PGL}_2(K)$ satisfies $f_3(T_2) = f_3$, hence again $\mathrm{Aut}(f, K)$ contains $\mathfrak{C}_3$. □

Lemma 33. *For a non-singular quartic binary form f over K, $\mathrm{Aut}(f, K)$ contains $\mathfrak{C}_4$ if and only if $B(f) = 0$.*

Proof. Necessity. If $\pi = 2$, then by Lemma 1 no element of $\mathrm{PGL}_2(K)$ is of order 4, hence the assumption implies $\pi \neq 2$. If $\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) K^*$ is an element of order 4 in $\mathrm{Aut}(f, K)$, then by Theorem 1,

$$f = a\chi_1^4 + b\chi_2^4,$$

where χ_1, χ_2 are given in Definition 3. Denoting by R_3 the resultant of χ_1, χ_2 and by f_4 the form $ax^4 + by^4$ we have, by the Remark,

$$B(f) = R_3^3 B(f_4) = 0.$$

Sufficiency. Since $D(f) \neq 0$ the assumption $B(f) = 0$ implies $\pi \neq 2$ by the Remark. Then (see [11, §13]) f is equivalent, by a linear transformation over K, to a form

$$f_5 = x^4 + mx^2y^2 + y^4, \qquad m \in K.$$

The condition $B(f) = 0$ gives

$$2m^3 - 72m = B(f_5) = 0,$$

hence $m = 0, \pm 6$. But the forms $x^4 \pm 6x^2y^2 + y^4$ are equivalent to $f_6 = x^4 + y^4$, since

$$x^4 + 6x^2y^2 + y^4 = \tfrac{1}{2}(x + y)^4 + \tfrac{1}{2}(x - y)^4,$$
$$x^4 - 6x^2y^2 + y^4 = \tfrac{1}{2}(x + \zeta y)^4 + \tfrac{1}{2}(x - \zeta y)^4,$$

where ζ is a primitive quartic root of unity. On the other hand, the transformation $T_3 = (\zeta x, y)$ of order 4 in $\mathrm{PGL}_2(K)$ satisfies $f_6(T_3) = T_3$, hence $\mathrm{Aut}(f, K)$ conjugate to $\mathrm{Aut}(f_6, K)$ contains $\mathfrak{C}_4$. □

Lemma 34. *For a non-singular quartic binary form f over K, $\mathrm{Aut}(f, K)$ contains $\mathfrak{D}_2$, but no $\mathfrak{D}_2 \times \mathfrak{C}_2$.*

Proof. If $\pi \neq 2$ then by the already quoted result f is equivalent by a linear transformation over K to a form

$$f_5 = x^4 + mx^2y^2 + y^4, \qquad m \in K.$$

The transformations $T_4(x, y) = (y, x)$ and $T_5(x, y) = (-x, y)$ satisfy $T_4^2 = E = T_5^2$, $T_4T_5 = T_5T_4$, $f_5(T_4) = f_5 = f_5(T_5)$, hence $\mathrm{Aut}(f, K)$ conjugate to $\mathrm{Aut}(f_5, K)$ contains $\mathfrak{D}_2$. On the other hand, it contains no $\mathfrak{D}_2 \times \mathfrak{C}_2$, since this group is not on the list given in the proof of Lemma 7.

If $\pi = 2$ then f is equivalent, by a linear transformation over K, to a form

$$f_7 = xy(x + \xi y)(x + \xi^{-1}y), \quad \xi \in K \setminus \{0, 1\}.$$

The transformations $T_6(x, y) = (x + \xi y, \xi x + y)$, $T_7(x, y) = (\xi x + y, x + \xi y)$ satisfy $T_6^2 = e = T_7^2$, $T_6T_7 = T_7T_6$, $f_7(T_6) = (\xi + 1)^4 f_7 = f_7(T_7)$, hence $\mathrm{Aut}(f, K)$ conjugate to $\mathrm{Aut}(f_7, K)$ contains $\mathfrak{D}_2$. On the other hand, it contains no $\mathfrak{D}_2 \times \mathfrak{C}_2$ by Corollary 11. □

Proof of Theorem 7. If $A(f) = B(f) = 0$, then since $D(f) \neq 0$ we have $\pi = 3$ by the Remark. The form f is equivalent, by a linear transformation over K, to a form

$$f_3 = xy(x^2 + axy - y^2)$$

and the condition $A(f) = 0$ implies $a = 0$. Hence $\mathrm{Aut}(f, K) \cong \mathrm{Aut}(f_3, K) \cong \mathrm{PGL}_2(\mathbb{F}_3) \cong \mathfrak{S}_4$ by Theorem 4.

If $A(f)$, $B(f)$ are not both 0, then (46) is not satisfied, hence by Theorem 4 and Lemma 34,

(79) $\qquad |\mathrm{Aut}(f, K)| \text{ divides 8 or 12.}$

If $A(f) = 0$ and $B(f) \neq 0$, then by Lemmas 32–34, $\mathrm{Aut}(f, K)$ contains $\mathfrak{C}_3$ and $\mathfrak{D}_2$, but no $\mathfrak{C}_4$ and no $\mathfrak{D}_2 \times \mathfrak{C}_2$. Hence its 2-Sylow subgroup is $\mathfrak{D}_2$. On the other hand, $\mathrm{Aut}(f, K)$ contains no $\mathfrak{C}_6$ by Theorem 1. Hence, $\mathrm{Aut}(f, K) \cong \mathfrak{A}_4$ by (79).

If $A(f) \neq 0$ and $B(f) = 0$, then by Lemmas 32–34, $\mathrm{Aut}(f, K)$ contains $\mathfrak{C}_4$ and $\mathfrak{D}_2$, but no $\mathfrak{C}_3$ and no $\mathfrak{D}_2 \times \mathfrak{C}_2$. Therefore, by (79), $|\mathrm{Aut}(f, K)| = 8$ and $\mathrm{Aut}(f, K) \cong \mathfrak{D}_4$.

If $A(f)B(f) \neq 0$, then by Lemmas 32–34, $\mathrm{Aut}(f, K)$ contains $\mathfrak{D}_2$, but no $\mathfrak{C}_3$, no $\mathfrak{C}_4$ and no $\mathfrak{D}_2 \times \mathfrak{C}_2$. Therefore, by (79), $|\mathrm{Aut}(f, K)| = 4$ and $\mathrm{Aut}(f, K) \cong \mathfrak{D}_2$. □

Now, we proceed to the case $n \geqslant 5$.

Definition 11. $\mathfrak{F}_n(K)$ is the set of all binary forms f of degree n defined over K such that $\mathrm{Aut}(f, K)$ is non-trivial.

Theorem 8. $\mathfrak{F}_n(\mathbb{C})$ *is Zariski closed for* $n \leqslant 5$ *only.*

Lemma 35. $\mathfrak{F}_5(\mathbb{C})$ *is Zariski closed.*

Proof. $f \in \mathfrak{F}_5(\mathbb{C})$ if and only if $R = 0$, where R is the Hermite invariant of f of degree 18. Indeed, if $f \in \mathfrak{F}_5(\mathbb{C})$, then, by Theorem 1, f is equivalent over $\mathbb{C}$ to one of the forms

$$x^{5-i}y^i \ (0 \leqslant i \leqslant 2), \qquad xy(x^3 + y^3), \qquad x^5 + y^5, \tag{80}$$

or

$$x(Ax^4 + Bx^2y^2 + Cy^4). \tag{81}$$

In each case we check in the tables of Faà di Bruno [13, Anhang, Tabelle III, Die irreduciebeln Invarianten IV5] that $R = 0$. To prove the converse, let α be the covariant of f of degree 1 and order 5. If $\alpha = 0$, then according to Clebsch [5, §93], f is either equivalent over $\mathbb{C}$ to one of the forms (80), or has a factor of multiplicity at least three, in which case it has a non-trivial automorph by Lemma 31. If $\alpha \neq 0$, but $R = 0$, then again according to Clebsch [5, §94], f is equivalent over $\mathbb{C}$ to a form (81). It now suffices to apply Theorem 1 in the opposite direction. □

Lemma 36. *For* $k \geqslant 2$ *and* $n \geqslant k + 3$ *we have*

$$f_0(x, y) = x^k \prod_{i=1}^{n-k} (x - iy) \notin \mathfrak{F}_n(\mathbb{C}).$$

Proof. Assuming $f_0(\alpha x + \beta y, \gamma x + \delta y) = f_0(x, y)$ we obtain

$$(\alpha x + \beta y)^k \mid f_0(x, y),$$

hence $k \geqslant 2$ implies $\beta = 0$ and we have

$$\alpha^k \prod_{i=1}^{n-k} \big((\alpha - i\gamma)x - i\delta y\big) = \prod_{i=1}^{n-k} (x - iy),$$

thus the sequence $\langle(\alpha - i\gamma)/i\delta\rangle_{1\leqslant i\leqslant n-k}$ is a permutation of $\langle 1/i\rangle_{1\leqslant i\leqslant n-k}$. Clearly, $\alpha/\delta, \gamma/\delta \in \mathbb{Q}$ and comparing the maxima and minima in both sequences we obtain

$$\text{for } \alpha/\delta > 0, \quad \frac{\alpha}{\delta} - \frac{\gamma}{\delta} = 1, \quad \frac{\alpha}{\delta(n-k)} - \frac{\gamma}{\delta} = \frac{1}{n-k},$$
$$\text{for } \alpha/\delta < 0, \quad \frac{\alpha}{\delta} - \frac{\gamma}{\delta} = \frac{1}{n-k}, \quad \frac{\alpha}{\delta(n-k)} - \frac{\gamma}{\delta} = 1.$$

In the former case it follows that $\alpha/\delta = 1$, $\gamma/\delta = 0$, thus the automorph is trivial; in the latter case

$$\frac{\alpha}{\delta} = -1, \quad \frac{\gamma}{\delta} = -1 - \frac{1}{n-k},$$

thus comparing the second greatest terms in both sequences we get

$$-\frac{1}{n-k-1} + 1 + \frac{1}{n-k} = \frac{1}{2},$$

which gives $n - k = 2$, contrary to assumption. □

Lemma 37. *For an integer $n \geqslant 5$ and a real number $t \in (0, 1)$ we have $f_t(x, y) \in \mathfrak{F}_n(\mathbb{C})$, where*

$$f_t(x,y) = \begin{cases} \displaystyle\prod_{i=1}^{n/2} (x - iy)\left(x - \frac{2(i-1)t}{i + it - 2t}\, y\right) & \text{if } n \equiv 0 \bmod 2, \\ \displaystyle\prod_{i=1}^{(n-1)/2} (x - iy)\left(x - \frac{it}{i + it - t}\, y\right) & \text{if } n \equiv 1 \bmod 2. \end{cases}$$

Proof. For $t \in (0, 1)$ let

$$g(x,y) = \prod_{i=1}^{\lfloor n/2\rfloor} (x - iy),$$

$$h_t(x,y) = \begin{cases} \displaystyle\prod_{i=1}^{n/2}\left(x - \frac{2(i-1)t}{i + it - 2t}\, y\right) & \text{if } n \equiv 0 \bmod 2, \\ \displaystyle x \prod_{i=1}^{(n-1)/2}\left(x - \frac{it}{i + it - t}\, y\right) & \text{if } n \equiv 1 \bmod 2, \end{cases}$$

$$T(x,y) = \begin{cases} (2tx - 2ty,\ (t+1)x - 2ty) & \text{if } n \equiv 0 \bmod 2, \\ (tx,\ (t+1)x - ty) & \text{if } n \equiv 1 \bmod 2. \end{cases}$$

For $n \equiv 0 \bmod 2$ we have

$$g(T(x,y)) = g(2t, t+1)h_t(x,y), \quad h_t(T(x,y)) = h_t(2t, t+1)g(x,y),$$

hence

$$f_t(T(x,y)) = f_t(2t, t+1)\, f_t(x,y)$$

and T is a non-trivial weak automorph of f_t.

Similarly, for $n \equiv 1 \bmod 2$,

$$g(T(x, y)) = g(t, t+1)h_t(x, y), \qquad h_t(T(x, y)) = h_t(t, t+1)g(x, y),$$

hence

$$f_t(T(x, y)) = f_t(t, t+1)\, f_t(x, y)$$

and T is again a non-trivial weak automorph of f_t. □

Proof of Theorem 8. For $n \leqslant 4$, $\mathfrak{F}_n(\mathbb{C})$ consists of all binary forms over $\mathbb{C}$ by Lemma 31; the case $n = 5$ is covered by Lemma 35. Suppose that, for $n \geqslant 6$, $\mathfrak{F}_n(\mathbb{C})$ is given by the alternative of systems of equations $F_{ij}(a_0, \ldots, a_n) = 0$ $(j \in J_i)$. Using Lemma 37 and denoting the coefficients of $f_t(x, y)$ by $a_0(t), \ldots, a_n(t)$ we obtain for at least one i_0 and t arbitrarily close to 0,

$$F_{i_0 j}(a_0(t), \ldots, a_n(t)) = 0 \quad (j \in J_{i_0}).$$

Taking the limit as t tends to 0 we obtain

$$F_{i_0 j}(a_0, \ldots, a_n) = 0 \quad (j \in J_{i_0}),$$

where $\sum_{i=0}^{n} a_i x^{n-i} y^i = f_0(x, y)$. Thus by our assumption $f_0 \in \mathfrak{F}_n(\mathbb{C})$, contrary to Lemma 36.

□

References

[1] I. Berchenko, P. J. Olver, *Symmetries of polynomials*. J. Symbolic Comput. 29 (2000), 485–514.

[2] O. Bolza, *On binary sextics with linear transformations into themselves*. Amer. J. Math. 10 (1887), 47–70.

[3] Z. I. Borevich, I. R. Shafarevich, *Number Theory*. Academic Press, New York 1966.

[4] A. Choudhry, *A study of certain properties of forms with applications to Diophantine equations*. Unpublished manuscript, 2003.

[5] A. Clebsch, *Theorie der binären algebraischen Formen*. Leipzig 1872.

[6] A. Clebsch, P. Gordan, *Sulla reppresentazione tipica delle forme binarie*. Ann. Mat. Pura Appl. (2) 1 (1867), 23–79.

[7] H. S. M. Coxeter, W. O. J. Moser, *Generators and Relations for Discrete Groups*, 3nd ed. Springer, New York 1972.

[8] W. J. Curran Sharp, *Solution to Problem 7382 (Mathematics)*. Educational Times 41 (1884).

[9] L. E. Dickson, *An invariantive investigation of irreducible binary modular forms*. Trans. Amer. Math. Soc. 12 (1911), 1–18.

[10] —, *Binary modular groups and their invariants*. Amer. J. Math. 33 (1911), 175–192; The Collected Papers, Vol. I, Chelsea, New York 1975, 289–395.

[11] —, *Modern Algebraic Theories*. B. H. Sanborn, 1926.

[12] —, *Linear Groups with an Exposition of the Galois Field Theory*. Reprint, Dover, New York 1958.

[13] F. Faà di Bruno, *Einleitung in die Theorie der binären Formen*. Leipzig 1891.

[14] W. C. Huffman, *Polynomial invariants of finite linear groups of degree two*. Canad. J. Math. 32 (1980), 317–330.

[15] F. Klein, *Ueber binäre Formen mit linearen Transformationen in sich selbst*. Math. Ann. 9 (1875–1876), 183–208; Gesammelte Mathematische Abhandlungen, Bd. II, Springer, 1922, 275–301.

[16] —, *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen von fünften Grade*. Leipzig 1894.

[17] G. Maiasano, *La sestica binaria*. Atti R. Accad. Lincei Mem. (3) 19 (1884), 9–60.

[18] R. C. Mason, *Equations over function fields*. In: Number Theory (Noordwijkerhout, 1983), Lecture Notes in Math. 1068, Springer, Berlin 1984, 149–157.

[19] P. J. Olver, *Classical Invariant Theory*. Cambridge Univ. Press, Cambridge 1999.

[20] M. O'Ryan, *On the similarity group of forms of higher degree*. J. Algebra 168 (1994), 968–980.

[21] O. Perron, *Algebra*, Band I. Walter de Gruyter, 1927.

[22] B. Segre, *Equivalenza ed automorfismi delle forme binarie in un dato anello o campo numerico*. Univ. Nac. Tucumán. Revista A. 5 (1946), 7–68.

[23] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math. 15 (1972), 259–331; Oeuvres (Collected Papers), Vol. 3, Springer, Berlin 1986, 1–73.

[24] L. Summerer, *Decomposable forms and automorphisms*. J. Number Theory 99 (2003), 232–254.

[25] —, *Automorphisms of binary forms*. Preprint, 2004.

[26] B. L. van der Waerden, *Algebra* II Teil, 5th ed. Springer, Berlin 1967.

[27] H. Weber, *Lehrbuch der Algebra*. Reprint, Chelsea, New York 1961.

Andrzej Schinzel
Selecta

Originally published in
Bulletin of the Polish Academy of Sciences. Mathematics
53 (2005), 251–258

Reducibility of symmetric polynomials

To Donald J. Lewis on his 80th birthday

Abstract. A necessary and sufficient condition is given for reducibility of a symmetric polynomial whose number of variables is large in comparison to degree.

Let K be a field and $\tau_i(x_1, \dots, x_m)$ the i-th elementary symmetric polynomial of the variables $x_1, \dots, x_m$. We shall show

Theorem 1. *Let $F \in K[y_1, \dots, y_n] \setminus K$, $n > \max\{4, \deg F + 1\}$, $\tau_i = \tau_i(x_1, \dots, x_n)$. Then $F(\tau_1, \dots, \tau_n)$ is reducible in $K[x_1, \dots, x_n]$ if and only if either F is reducible over K, or*

$$F = cN_{K(\alpha)/K}\Big(\alpha^n + \sum_{j=1}^{n} \alpha^{n-j} y_j\Big), \quad c \in K^*, \ \alpha \text{ algebraic over } K.$$

Theorem 2. *Let $F \in K[y_1, \dots, y_n] \setminus K$ be isobaric with respect to weights $1, \dots, n$ (y_i of weight i) and $n > \deg F + 1$. Then $F(\tau_1, \dots, \tau_n)$ is reducible over K if and only if either F is reducible over K, or $F = cy_n$, $c \in K^*$, or $n = 4$, $\operatorname{char} K \neq 3$, K contains a primitive cubic root of 1 and*

$$F = a(y_2^2 - 3y_1y_3 + 12y_4), \quad a \in K^*.$$

The last part of Theorem 2 shows that the 4 in the formulation of Theorem 1 cannot be replaced by 3. The example given at the end of the paper shows that $\deg F + 1$ cannot be replaced by $\deg F$.

For a polynomial $f \in K[x_1, \dots, x_n]$ and a permutation $\sigma \in \mathfrak{S}_n$ we set

$$f^\sigma = f(x_{\sigma(1)}, \dots, x_{\sigma(n)}).$$

The proof of Theorem 1 is based on three lemmas.

Lemma 1. *For $n \geqslant 5$ the alternating group $\mathfrak{A}_n$ is generated by products $(ab)(cd)$ of two transpositions with a, b, c, d distinct.*

Proof. See [1], p. 342. □

Lemma 2. *Assume that $C \in K[x_1, \dots, x_n]$ is invariant with respect to $\mathfrak{A}_n$, but not symmetric. Then for $n \geqslant 3$,*

$$\deg_{x_n} C \geqslant n - 1.$$

Proof. By the theorem of P. Samuel (see [2], p. 13)

$$C = A + BD_n$$

where $A, B \in K[x_1, \ldots, x_n]$ are symmetric, $B \neq 0$ and

$$D_n = \frac{1}{2}\Big(\prod_{i<j}(x_i - x_j) + \prod_{i<j}(x_i + x_j)\Big).$$

For $n \geqslant 3$ we have $\deg_{x_n} D_n \geqslant n-1$, hence $\deg_{x_n} C \geqslant n-1$, except possibly when $\deg_{x_n} A = \deg_{x_n} BD_n$. In that case, let $\alpha = \deg_{x_n} A$, $\beta = \deg_{x_n} B$, and let a, b be the leading coefficients of A and B with respect to x_n. The coefficient of $x_n^{\beta+n-1}$ in C equals

$$c = a + bD_{n-1}$$

and since D_{n-1} is not symmetric, $c \neq 0$, thus again

$$\deg_{x_n} C \geqslant n-1. \qquad \square$$

Lemma 3. *If* $f \in K[x_1, \ldots, x_n] \setminus \bigcup_{i=1}^{n} K[x_i]$ *is irreducible over* K *and not symmetric, then for* $n \geqslant 5$

$$\deg_{x_n} \operatorname*{l.c.m.}_{\sigma \in \mathfrak{S}_n} f^\sigma \geqslant n-1. \tag{1}$$

Proof. Let f depend on exactly r variables, where $1 \leqslant r < n$. The case $r = 1$ is excluded by the conditions that f irreducible and $f \neq cx_i$. For every subset R of $\{1, \ldots, n\}$ of cardinality r and containing n there exists $\sigma \in \mathfrak{S}_n$ such that f^σ depends on the variables x_i $(i \in R)$ exclusively. For different sets R the forms f^σ are projectively different and hence coprime. For $1 < r < n$ the number of sets R in question is $\binom{n-1}{r-1} \geqslant n-1$, thus (1) holds.

Consider now the case $r = n$ and let

$$\mathcal{G} = \{\sigma \in \mathfrak{S}_n : f^\sigma / f \in K\}, \qquad \mathcal{H} = \{\sigma \in \mathfrak{S}_n : f^\sigma = f\}.$$

By Bertrand's theorem (see [1], pp. 348–352) we have either $\mathcal{G} = \mathfrak{S}_n$ or $\mathcal{G} = \mathfrak{A}_n$ or $[\mathfrak{S}_n : \mathcal{G}] \geqslant n$. In the first case, if $f^\tau = f$ for each transposition τ, then $f^\sigma = f$ for all $\sigma \in \mathfrak{S}_n$, since $\mathfrak{S}_n$ is generated by transpositions, thus f is symmetric, contrary to assumption. Therefore, there exists a transposition $\tau = (ij)$, $i \neq j$, such that

$$f^\tau = cf, \qquad c \neq 1.$$

Since $\tau^2 = \mathrm{id}$, we have $c^2 = 1$, thus $\operatorname{char} K \neq 2$, $c = -1$, and $x_i = x_j$ implies $f = 0$. Since f is irreducible,

$$f = a(x_i - x_j), \qquad a \in K,$$

and it is easy to see that

$$\deg_{x_n} \operatorname*{l.c.m.}_{\sigma \in \mathfrak{S}_n} f^\sigma \geqslant n-1.$$

Consider now the case $\mathcal{G} = \mathfrak{A}_n$. By Lemma 1, $\mathfrak{A}_n$ is generated by the products $\pi = (ab)(cd)$, where a, b, c, d are distinct. Since $\pi^2 = \mathrm{id}$, we have $f^\pi = cf$, where

$c^2 = 1$. It follows that $(f^2)^\sigma = f^2$ for all $\sigma \in \mathfrak{A}_n$. On the other hand, $\mathcal{H} < \mathcal{G}$ gives either $\mathcal{H} = \mathfrak{A}_n$ or $[\mathfrak{S}_n : \mathcal{H}] \geqslant n$.

If $\mathcal{H} = \mathfrak{A}_n$, then by Lemma 2, $\deg_{x_n} f \geqslant n-1$, hence (1) holds. If $[\mathfrak{S}_n : \mathcal{H}] \geqslant n$, then f^2 cannot be symmetric, hence by Lemma 2, $\deg_{x_n} f^2 \geqslant n-1$, thus

$$\deg_{x_n} f \geqslant \left\lceil \frac{n-1}{2} \right\rceil.$$

Now, by the definition of $\mathcal{G}$ it follows that for $\tau = (12)$ we have $f^\tau/f \notin K$, hence $(f^\tau, f) = 1$, thus

$$\deg_{x_n}[f, f^\tau] \geqslant 2\left\lceil \frac{n-1}{2} \right\rceil \geqslant n-1,$$

and (1) holds.

It remains to consider the case $[\mathfrak{S}_n : \mathcal{G}] \geqslant n$. Then among the polynomials f^σ there are at least n projectively distinct, hence coprime. Since each of them is of degree at least 1 in x_n, (1) follows. □

Proof of Theorem 1. *Necessity.* If $F(\tau_1, \ldots, \tau_n)$ is reducible over K, then

$$F(\tau_1, \ldots, \tau_n) = f_1 f_2, \tag{2}$$

where $f_\nu \in K[x_1, \ldots, x_n] \setminus K$ $(\nu = 1, 2)$ and f_1 is irreducible over K.

Clearly

$$\deg_{x_n} \operatorname*{l.c.m.}_{\sigma \in \mathfrak{S}_n} f_1^\sigma \leqslant \deg F < n-1.$$

If f_1 is not symmetric and $f_1 \notin K[x_i]$ $(1 \leqslant i \leqslant n)$, this contradicts Lemma 3, thus either

$$f_1 \text{ is symmetric} \tag{3}$$

or

$$f_1 \in K[x_i] \quad \text{for some } i. \tag{4}$$

In the case (3), $f_\nu = F_\nu(\tau_1, \ldots, \tau_n)$, $\nu = 1, 2$, where $F_\nu \in K[y_1, \ldots, y_n] \setminus K$, and it follows from (2) that

$$F(\tau_1, \ldots, \tau_n) = \prod_{\nu=1}^{2} F_\nu(\tau_1, \ldots, \tau_n).$$

By the algebraic independence of $\tau_1, \ldots, \tau_n$ over K,

$$F = F_1 F_2,$$

thus F is reducible over K.

In the case (4), since f_1 is irreducible over K, we have

$$f_1 = c_1 N_{L/K}(\alpha + x_i), \qquad \text{where } L = K(\alpha),\ \alpha \text{ algebraic over } K,\ c_1 \in K.$$

Since $F(\tau_1, \ldots, \tau_n)$ is symmetric, we have

$$f_1(x_j) \mid F(\tau_1, \ldots, \tau_n) \quad (1 \leqslant j \leqslant n),$$

thus

$$\prod_{j=1}^{n} f_1(x_j) \;\Big|\; F(\tau_1, \ldots, \tau_n).$$

However,

$$\prod_{j=1}^{n} f_1(x_j) = c_1^n \prod_{j=1}^{n} N_{L/K}(\alpha + x_j) = c_1^n N_{L/K}\Big(\alpha^n + \sum_{j=1}^{n} \alpha^{n-j}\tau_j\Big),$$

hence

$$N_{L/K}\Big(\alpha^n + \sum_{j=1}^{n} \alpha^{n-j}\tau_j\Big) \;\Big|\; F(\tau_1, \ldots, \tau_n)$$

and by the algebraic independence of $\tau_1, \ldots, \tau_n$,

$$N_{L/K}\Big(\alpha^n + \sum_{j=1}^{n} \alpha^{n-j} y_j\Big) \;\Big|\; F.$$

Therefore, either F is reducible over K or

$$F = cN_{L/K}\Big(\alpha^n + \sum_{j=1}^{n} \alpha^{n-j} y_j\Big), \qquad c \in K^*.$$

Sufficiency. If $F = F_1 F_2$, where $F_i \in K[y_1, \ldots, y_n] \setminus K$, then

$$F(\tau_1, \ldots, \tau_n) = \prod_{\nu=1}^{2} F_\nu(\tau_1, \ldots, \tau_n),$$

and since $\tau_1, \ldots, \tau_n$ are algebraically independent,

$$F_\nu(\tau_1, \ldots, \tau_n) \notin K,$$

thus $F(\tau_1, \ldots, \tau_n)$ is reducible over K.

If $F = cN_{K(\alpha)/K}(\alpha^n + \sum_{j=1}^{n} \alpha^{n-j} y_j)$, then

$$F(\tau_1, \ldots, \tau_n) = cN_{K(\alpha)/K}\Big(\prod_{i=1}^{n}(\alpha + x_i)\Big) = c\prod_{i=1}^{n} N_{K(\alpha)/K}(\alpha + x_i),$$

and since $n > 1$, $F(\tau_1, \ldots, \tau_n)$ is reducible over K. □

The proof of Theorem 2 is based on two lemmas.

Lemma 4. *For $n = 3$, $\tau_1^2 + a\tau_2$ is reducible over K only if either $a = 0$, or $a = -3$,* char $K \neq 3$ *and K contains a primitive cubic root ϱ of* 1. *In the latter case*

$$\tau_1^2 + a\tau_2 = (x_1 + \varrho x_2 + \varrho^2 x_3)(x_1 + \varrho^2 x_2 + \varrho x_3). \tag{5}$$

Proof. Assuming reducibility we have

$$\tau_1^2 + a\tau_2 = (x_1 + \alpha x_2 + \beta x_3)(x_1 + \beta x_2 + \alpha x_3), \qquad \alpha, \beta \in K,$$

which gives

$$\alpha\beta = 1, \qquad \alpha + \beta = a + 2, \qquad \alpha^2 + \beta^2 = a + 2.$$

Hence

$$a + 2 = \alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta = (a + 2)^2 - 2 = a^2 + 4a + 2,$$

so that $a(a + 3) = 0$, thus either $a = 0$, or $a = -3$ and $\operatorname{char} K \neq 3$. In the latter case $(x - \alpha)(x - \beta) = x^2 + x + 1$, hence α and β are two primitive cubic roots of 1. The identity (5) is easily verified. □

Lemma 5. *For $n = 3$, $\tau_2^2 + a\tau_1\tau_3$ is reducible over K if and only if either $a = 0$, or $a = -3$, $\operatorname{char} K \neq 3$ and K contains a primitive cubic root ϱ of 1. In the latter case*

$$\tau_2^2 + a\tau_1\tau_3 = (x_2x_3 + \varrho x_1x_3 + \varrho^2 x_1x_2)(x_2x_3 + \varrho^2 x_1x_3 + \varrho x_1x_2). \tag{6}$$

Proof. We have

$$\tau_1^2 + a\tau_2 = \tau_3^2\big(\tau_2(x_1^{-1}, x_2^{-1}, x_3^{-1})^2 + a\tau_1(x_1^{-1}, x_2^{-1}, x_3^{-1})\tau_3(x_1^{-1}, x_2^{-1}, x_3^{-1})\big).$$

Therefore, if

$$\tau_2^2 + a\tau_1\tau_3 = f_1 f_2, \qquad f_\nu \in K[x_1, x_2, x_3] \setminus K \qquad (\nu = 1, 2),$$

we obtain

$$\tau_1^2 + a\tau_2 = \tau_3 f_1(x_1^{-1}, x_2^{-1}, x_3^{-1})\tau_3 f_2(x_1^{-1}, x_2^{-1}, x_3^{-1}),$$

where $\tau_3 f_\nu(x_1^{-1}, x_2^{-1}, x_3^{-1}) \in K[x_1, x_2, x_3] \setminus K$, hence by Lemma 4 either $a = 0$, or $a = -3$, $\operatorname{char} K \neq 3$ and K contains a primitive cubic root ϱ of 1. The identity (6) is easily verified. □

Proof of Theorem 2. *Necessity.* If $\deg F = 1$, then since F is isobaric, $F = cy_i$, $c \in K^*$, $i \leqslant n$. If $c\tau_i$ is reducible in $K[x_1, \ldots, x_n]$, then $i = n$. If $n \geqslant 5$, then Theorem 1 applies and either F is reducible or

$$F = cN_{K(\alpha)/K}\Big(\alpha^n + \sum_{j=1}^{n} \alpha^{n-j} y_j\Big), \qquad c \in K^*. \tag{7}$$

Since F is isobaric, we have $\alpha = 0$ and $F = cy_n$.

It remains to consider the case $2 \leqslant \deg F < n - 1 \leqslant 3$, hence $n = 4$ and $\deg F = 2$. We distinguish the following subcases:

$$\begin{aligned}
&F = y_1^2 + ay_2 =: F_1, && a \neq 0,\\
&F = y_1y_2 + ay_3 =: F_2, && a \neq 0,\\
&F = ay_2^2 + by_1y_3 + cy_4 =: F_3, && ab \neq 0, \text{ or } ac \neq 0, \text{ or } bc \neq 0,\\
&F = y_2y_3 + ay_1y_4 =: F_4, && a \neq 0,\\
&F = y_3^2 + ay_2y_4 =: F_5, && a \neq 0.
\end{aligned}$$

We have $F_1(\tau_1, \tau_2) = x_4^2 + (a+2)\tau_1' + (\tau_1'^2 + a\tau_2')$, where $\tau_i' = \tau_i(x_1, x_2, x_3)$. If $F_1(\tau_1, \tau_2) = (x_4 + g)(x_4 + h)$, where g, h are linear forms over K in x_1, x_2, x_3, then $gh = \tau_1'^2 + a\tau_2'$, hence by Lemma 4, $a = -3$, char $K \neq 3$ and without loss of generality

$$g = b(x_1 + \varrho x_2 + \varrho^2 x_3), \quad h = b^{-1}(x_1 + \varrho^2 x_2 + \varrho x_3), \quad b \in K^*.$$

Therefore,

$$b + b^{-1} = -1, \quad b\varrho + b^{-1}\varrho^2 = -1, \quad b\varrho^2 + b^{-1}\varrho = -1.$$

The first equation gives $b = \varrho$ or $b = \varrho^2$, thus either $b\varrho^2 + b^{-1}\varrho \neq -1$ or $b\varrho + b^{-1}\varrho^2 \neq -1$, a contradiction. Therefore $F_1(\tau_1, \tau_2)$ is irreducible over K. Since

$$F_1(\tau_1, \tau_2) = \tau_4^2 F_5\big(\tau_2(x_1^{-1}, \ldots, x_4^{-1}),\ \tau_3(x_1^{-1}, \ldots, x_4^{-1}),\ \tau_4(x_1^{-1}, \ldots, x_4^{-1})\big),$$

the same applies to $F_5(\tau_2, \tau_3, \tau_4)$ (cf. proof of Lemma 5).

We have further

$$F_2(\tau_1, \tau_2, \tau_3) = \tau_1' x_4^2 + (\tau_1'^2 + (a+1)\tau_2')x_4 + (\tau_1'\tau_2' + a\tau_3'),$$

hence, if $F_2(\tau_1, \tau_2, \tau_3)$ is reducible over K then

$$F_2(\tau_1, \tau_2, \tau_3) = (\tau_1' x_4 + b\tau_1'^2 + c\tau_2')(x_4 + d\tau_1'), \quad b, c, d \in K,$$

and

$$\tau_1'\tau_2' + a\tau_3' = bd\tau_1'^3 + cd\tau_1'\tau_2'.$$

Since $\tau_1', \tau_2', \tau_3'$ are algebraically independent, it follows that $a = 0$, a contradiction. Therefore $F_2(\tau_1, \tau_2, \tau_3)$ is irreducible over K. Since

$$F_2(\tau_1, \tau_2, \tau_3) = \tau_4^2 F_4\big(\tau_1(x_1^{-1}, \ldots, x_4^{-1}), \ldots, \tau_4(x_1^{-1}, \ldots, x_4^{-1})\big)$$

the same applies to $F_4(\tau_1, \ldots, \tau_4)$ (cf. proof of Lemma 5).

It remains to consider F_3. We have

$$\begin{aligned} F_3(\tau_1, \ldots, \tau_4) &= a(\tau_1' x_4 + \tau_2')^2 + b(x_4 + \tau_1')(\tau_2' x_4 + \tau_3') + c\tau_3' x_4 \\ &= (a\tau_1'^2 + b\tau_2')x_4^2 + \big((2a+b)\tau_1'\tau_2' + (b+c)\tau_3'\big)x_4 + (a\tau_2'^2 + b\tau_1'\tau_3'). \end{aligned}$$

If $a\tau_1'^2 + b\tau_2'$ were the leading coefficient with respect to x_4 of a proper factor over K of $F_3(\tau_1, \ldots, \tau_4)$, then since it does not divide $a\tau_2'^2 + b\tau_1'\tau_3'$, the complementary factor of $F_3(\tau_1, \ldots, \tau_4)$ would be $x_4 + d\tau_1'$, $d \in K^*$, which implies $a = 0$, $b\tau_1'\tau_2' + (b+c)\tau_3' = bd\tau_1'\tau_2' + (b/d)\tau_3'$, $d = 1$, $c = 0$, a contradiction.

If $a\tau_1'^2 + b\tau_2'$ is not the leading coefficient of any proper factor of $F_3(\tau_1, \ldots, \tau_4)$ and the latter polynomial is reducible over K, then $a\tau_1'^2 + b\tau_2'$ is reducible over K, hence, by Lemma 4, either $b = 0$, or $b = -3a$, char $K \neq 3$ and K contains a primitive cubic root ϱ of 1. In the former case

$$\begin{aligned} &F_3(\tau_1, \ldots, \tau_4) = a(\tau_1' x_4 + d_1\tau_1'^2 + e_1\tau_2')(\tau_1' x_4 + d_2\tau_1'^2 + e_2\tau_2'); \\ &a(d_1\tau_1'^2 + e_1\tau_2')(d_2\tau_1'^2 + e_2\tau_2') = a\tau_2'^2; \quad d_1 = d_2 = 0, \\ &(ae_1 + ae_2)\tau_1'\tau_2' = 2a\tau_1'\tau_2' + c\tau_3', \quad c = 0, \quad \text{a contradiction.} \end{aligned}$$

In the latter case, by Lemmas 4 and 5, either

$$F_3(\tau_1,\dots,\tau_4) = a\big((x_1+\varrho x_2+\varrho^2 x_3)x_4 + d(x_2x_3+\varrho x_1x_3+\varrho^2 x_1x_2)\big) \times \big((x_1+\varrho^2 x_2+\varrho x_3)x_4 + d^{-1}(x_2x_3+\varrho^2 x_1x_3+\varrho x_1x_2)\big)$$

or

$$F_3(\tau_1,\dots,\tau_4) = a\big((x_1+\varrho x_2+\varrho^2 x_3)x_4 + d(x_2x_3+\varrho^2 x_1x_3+\varrho x_1x_2)\big) \times \big((x_1+\varrho^2 x_2+\varrho x_3)x_4 + d^{-1}(x_2x_3+\varrho x_1x_3+\varrho^2 x_1x_2)\big).$$

In the first subcase

$$d\big(x_2x_3+\varrho x_1x_3+\varrho^2 x_1x_2\big)\big(x_1+\varrho^2 x_2+\varrho x_3\big) + d^{-1}\big(x_2x_3+\varrho^2 x_1x_3+\varrho x_1x_2\big)\big(x_1+\varrho x_2+\varrho^2 x_3\big) = -\tau_1'\tau_2' + (c/a-3)\tau_3',$$

in the second subcase

$$d\big(x_2x_3+\varrho^2 x_1x_3+\varrho x_1x_2\big)\big(x_1+\varrho^2 x_2+\varrho x_3\big) + d^{-1}\big(x_2x_3+\varrho x_1x_3+\varrho^2 x_1x_2\big)\big(x_1+\varrho x_2+\varrho^2 x_3\big) = -\tau_1'\tau_2' + (c/a-3)\tau_3'.$$

In both subcases, the right hand side is invariant with respect to the conjugation $\varrho \mapsto \varrho^2$ and to any permutation $\sigma \in \mathfrak{S}_3$. The first condition implies $d = \pm 1, \pm\varrho, \pm\varrho^2$, the second condition eliminates the second subcase and in the first subcase restricts d to ± 1. Thus we obtain

$$d(6x_1x_2x_3 - x_1^2x_2 - x_2^2x_3 - x_3^2x_1 - x_1x_2^2 - x_2x_3^2 - x_3x_1^2) = -\tau_1'\tau_2' + (c/a-3)\tau_3',$$
$$d(9\tau_3' - \tau_1'\tau_2') = -\tau_1'\tau_2' + (c/a-3)\tau_3', \quad d = 1, \quad c = 12a.$$

Sufficiency. In view of Theorem 1 it suffices to consider $n = 4$ and $F = y_2^2 - 3y_1y_3 + 12y_4$. Then

$$F(\tau_1,\dots,\tau_4) = \big(x_1x_4 + x_2x_3 + \varrho(x_2x_4+x_1x_3) + \varrho^2(x_3x_4+x_1x_2)\big) \times \big(x_1x_4 + x_2x_3 + \varrho^2(x_2x_4+x_1x_3) + \varrho(x_3x_4+x_1x_2)\big). \ \square$$

Example. Take $F = \sum_{i=2}^{n} (-1)^i\, y_1^{n-i} y_i$. We have $\deg F = n-1$ and

$$F(\tau_1,\dots,\tau_n) = \prod_{i=1}^{n} (\tau_1 - x_i).$$

This example also shows that the estimate in Lemma 3 cannot be improved.

References

[1] R. Fricke, *Lehrbuch der Algebra*. Vieweg, Braunschweig 1924.

[2] L. Smith, *Polynomial Invariants of Finite Groups*. A K Peters, Wellesley 1995.

Part F

Hilbert's Irreducibility Theorem

Commentary on F: Hilbert's Irreducibility Theorem

by Umberto Zannier

The theorem in question (HIT in the sequel) in a basic form asserts that *for irreducible polynomials* $f_1, \dots, f_n \in \mathbb{Q}[t_1, \dots, t_r, x_1, \dots, x_s]$*, the set of rational points* $(t_1^*, \dots, t_r^*) \in \mathbb{Q}^r$ *such that* $f_i(t_1^*, \dots, t_r^*, x_1, \dots, x_s)$*,* $i = 1, \dots, n$*, are irreducible in* $\mathbb{Q}[x_1, \dots, x_s]$ *is Zariski-dense in* $\mathbb{Q}^n$ (namely, there is no nontrivial equation $g(t_1, \dots, t_r) = 0$ valid for all such points and in particular the set of such points is infinite).

I will be concerned with three papers by Schinzel on this topic.

F1. In this paper a substantial strengthening of the above formulation of Hilbert's theorem is proved. Namely, Theorem 1 states that: *For irreducible* $f_1, \dots, f_n \in \mathbb{Q}[t_1, \dots, t_r, x_1, \dots, x_s]$*, the set of points* $(t_1^*, \dots, t_r^*) \in \mathbb{Z}^r$ *such that*

$$f_i(t_1^*, \dots, t_r^*, x_1, \dots, x_s), \quad i = 1, \dots, n,$$

are irreducible in $\mathbb{Q}[x_1, \dots, x_s]$ *contains a product* $P_1 \times \dots \times P_r$ *of arithmetical progressions.*

Through a usual reduction step in the theory of HIT, the proof relies on a fundamental Lemma 1, which deals with equations $F(t_1, \dots, t_r, u) = 0$ in u; the lemma compares the identical solvability with $u \in \mathbb{Q}(t_1, \dots, t_r)$ and the solvability with $u \in \mathbb{Q}$, after specializations $t_i \mapsto t_i^* \in \mathbb{Q}$. The proof of the lemma follows a principle already exploited in a previous paper by Davenport, Lewis, Schinzel [1]; it uses theorems of Chebotarev type to relate equations $F(t_1^*, \dots, t_r^*, u) = 0$ with congruences $F(t_1^*, \dots, t_r^*, u) \equiv 0 \pmod{p}$, for suitable primes p and integers t_i^* (the relevant arithmetical progressions arise from such congruences).

Schinzel's sharpening of Hilbert's theorem, which motivated further research by authors like S. D. Cohen, M. Fried and others, points out a very elegant and important one among the striking properties of the "good" specialization sets in HIT; each of these properties may be crucial in the many applications of Hilbert's theorem.

F2. The present paper falls into the general theme of *value sets* $f(\mathbb{Z})$ *of polynomials* $f(x) \in \mathbb{Z}[x]$ *on* $\mathbb{Z}$. Let $\varphi \in \mathbb{Z}[x]$ be a fixed polynomial and suppose that, for another polynomial $f \in \mathbb{Z}[x]$, each value $f(a)$ of f on $a \in \mathbb{Z}$ is taken on $\mathbb{Z}$ also by φ, namely $f(\mathbb{Z}) \subset \varphi(\mathbb{Z})$. This will certainly happen if there exists a polynomial $h \in \mathbb{Z}[x]$ with

$f(x) = \varphi(h(x))$. If conversely, for all polynomials f, this is the only possibility for $f(\mathbb{Z})$ being a subset of $\varphi(\mathbb{Z})$ then $\varphi(x)$ is said to be "good".

This concept, which appears natural, was introduced by I. Korec in connection with palindromic squares (see the paper for references).

The object of the paper is to give a simple characterization of good polynomials. In a Theorem it is proved that *φ is good if and only if no polynomial $\varphi(x/m)$, for integer $m > 1$, has integer coefficients*.

The proof of the necessity of the condition exploits the polynomial $f(x) := \varphi((m-1)!\binom{x}{m})$; plainly $f(\mathbb{Z}) \subset \varphi(\mathbb{Z})$, leading easily to the sought conclusion that if φ is good then $\varphi(x/m) \notin \mathbb{Z}[x]$.

The proof of the sufficiency is more involved and uses Hilbert's Irreducibility Theorem (which for instance readily yields that if $f(\mathbb{Z}) \subset \varphi(\mathbb{Z})$ then $f(x) = \varphi(h(x))$ for some $h \in \mathbb{Q}[x]$).

F3. This paper offers quantitative versions of HIT, in the case of polynomials $f_1, \ldots, f_h \in \mathbb{Z}[t, x]$ in two variables. Assuming the f_i to be irreducible, one seeks a "small" integer specialization $t \mapsto t^* \in \mathbb{Z}$ such that all the $f_i(t^*, x)$ remain irreducible as polynomials in x.

Let $m = \max \deg_t f_i$, $n = \max \deg_x f_i$ and let $H \geqslant 20$ be an upper bound for the "height", i.e. here the maximum absolute value of the involved coefficients. In a Theorem it is proved that $|t^*|$ may be taken $\leqslant \max\{\exp(2(6m)^5), \exp(36^6), h^9 \exp(450(\log H)^{5/6} + 11250m^5 + 45(m+1)^2 n + 45n(\log H)^{2/5})\}$.

This improved on a previous estimate by Dèbes, where the exponent of $\log H$ was 2.

The Theorem is deduced from another quantitative form of HIT, i.e. Lemma 2, which bounds by $c(H, m, n)T^{8/9}$ the number of integers $t^* \in [0, T]$ such that $F(t^*, x)$ is reducible, where $f \in \mathbb{Z}[t, x]$ is irreducible, of height $\leqslant H$; here $c(m, n, H)$ is a certain explicit function of the arguments.

The proofs use a rather sharp and uniform estimate on the distribution of integer points on algebraic curves, due to E. Bombieri and J. Pila. Actually, it is necessary here to go into the Bombieri–Pila's proof and adapt it for the present purposes; this is done in Lemma 1.

More recently, a p-adic version of the Bombieri–Pila's approach has been developed by D. R. Heath-Brown (who treats varieties of any dimension). The p-adic context is sometimes advantageous, in particular in the present application. This use of Heath-Brown's estimates in place of the Bombieri–Pila's has been recently carried out by Y. Walkowiak in his Ph.D. thesis, see [2].

References

[1] H. Davenport, D. J. Lewis, A. Schinzel, *Polynomials of certain special types*. Acta Arith. 9 (1964), 107–116; this collection: A6, 27–35.

[2] Y. Walkowiak, *Théorème d'irréductibilité de Hilbert effectif*. Acta Arith. 116 (2005), 343–362.

Andrzej Schinzel
Selecta

Originally published in
Annales Polonici Mathematici XVI (1965), 333–340

On Hilbert's Irreducibility Theorem

In this paper irreducibility means irreducibility over the rational field and all polynomials and rational functions considered are supposed to have rational coefficients. Hilbert's Irreducibility Theorem asserts that if polynomials $f_m(t_1, \dots, t_r, x_1, \dots, x_s)$ $(m = 1, 2, \dots, n)$ are irreducible as polynomials in $r + s$ variables and a polynomial $z(t_1, t_2, \dots, t_r)$ is not identically 0, then there exist infinitely many integer systems $(t_1', t_2', \dots, t_r')$ such that all the polynomials $f_m(t_1', t_2', \dots, t_r', x_1, \dots, x_s)$ are irreducible as polynomials in $x_1, \dots, x_s$ and $z(t_1', t_2', \dots, t_r') \neq 0$ (cf. [3], Chapter VIII, §2). The main aim of this paper is to prove the following refinement of this theorem.

Theorem 1. *Let $f_m(t_1, \dots, t_r, x_1, \dots, x_s)$ $(1 \leqslant m \leqslant n)$ be irreducible polynomials in $r + s$ variables and let $z(t_1, \dots, t_r)$ be any polynomial $\neq 0$. There exist r arithmetical progressions $P_1, \dots, P_r$ such that if $t_l' \in P_l$ $(1 \leqslant l \leqslant r)$, then all the polynomials $f_m(t_1', \dots, t_r', x_1, \dots, x_s)$ are irreducible as polynomials in $x_1, \dots, x_s$ and $z(t_1', \dots, t_r') \neq 0$.*

The theorem applies also to fractional values of t_l if we adopt the following definition.

Definition. An *arithmetical progression* consists of all rational numbers $\equiv b \pmod a$, where a, b are fixed integers, $a \neq 0$ and the congruence for rationals is understood in the ordinary sense.

The proof of the fundamental lemma follows closely the proof of Theorem 1 in [1].

Lemma 1. *Let $F(t_1, \dots, t_r, u)$ be a polynomial such that for no rational function $\varphi(t_1, \dots, t_r)$, $F\big(t_1, \dots, t_r, \varphi(t_1, \dots, t_r)\big) = 0$ identically. There exist r arithmetical progressions $P_1, \dots, P_r$ such that if $t_l \in P_l$ $(1 \leqslant l \leqslant r)$, then $F(t_1, \dots, t_r, u) \neq 0$ for all rational u.*

Proof. We may assume without loss of generality that F has integer coefficients. Using Gauss's Lemma we factorize F into a product of polynomials with integer coefficients:

$$F(t_1, \dots, t_r, u) = F_0(t_1, \dots, t_r) F_1(t_1, \dots, t_r, u) \cdots F_k(t_1, \dots, t_r, u), \tag{1}$$

where $k \geqslant 0$ and each F_j $(1 \leqslant j \leqslant k)$ is irreducible, of positive degree d_j in u. Let $a_j(t_1, \dots, t_r)$ be the coefficient at u^{d_j} in F_j $(1 \leqslant j \leqslant k)$.

It follows from the assumption that $d_j > 1$ $(1 \leqslant j \leqslant k)$. It follows from Hilbert's theorem that there exist integers $t_1', t_2', \ldots, t_r'$ such that all the polynomials $F_j(t_1', \ldots, t_r', u)$ are irreducible and

$$F_0(t_1', \ldots, t_r') \prod_{j=1}^{k} a_j(t_1', \ldots, t_r') \neq 0.$$

Since each $F_j(t_1', \ldots, t_r', u)$ is irreducible of degree > 1, there exist for each $j \leqslant k$ infinitely many primes q such that the congruence

$$F_j(t_1', \ldots, t_r', u) \equiv 0 \pmod{q}$$

is insoluble ([2], cf. also proof of Theorem 1 in [1]), and in particular there is a prime q_j with the above property, such that

$$F_0(t_1', \ldots, t_r') a_j(t_1', \ldots, t_r') \not\equiv 0 \pmod{q_j} \quad (1 \leqslant j \leqslant k). \tag{2}$$

Now, let P_l be the progression $q_1 q_2 \cdots q_k v + t_l'$ and assume that $t_l \in P_l$ $(1 \leqslant l \leqslant r)$, i.e.

$$t_l \equiv t_l' \pmod{q_1 \cdots q_k} \quad (1 \leqslant l \leqslant r). \tag{3}$$

It follows that

$$F_0(t_1, \ldots, t_r) a_j(t_1, \ldots, t_r) \equiv F_0(t_1', \ldots, t_r') a_j(t_1', \ldots, t_r') \pmod{q_1 q_2 \cdots q_k}$$

and by (2)

$$F_0(t_1, \ldots, t_r) \neq 0, \tag{4}$$

$$a_j(t_1, \ldots, t_r) \not\equiv 0 \pmod{q_j} \quad (1 \leqslant j \leqslant k). \tag{5}$$

Suppose now that for some rational u_0, $F(t_1, \ldots, t_r, u_0) = 0$. It follows from (1) and (4) that $k > 0$ and for some $j_0 \leqslant k$

$$F_{j_0}(t_1, \ldots, t_r, u_0) = 0. \tag{6}$$

By (3) the denominators of $t_1, \ldots, t_r$ are not divisible by q_{j_0}. In view of (5) the same is true for the denominator of u_0 and (3) and (6) imply

$$F_{j_0}(t_1', \ldots, t_r', u_0) \equiv 0 \pmod{q_{j_0}},$$

which is impossible by the choice of q_{j_0}.

This contradiction completes the proof. □

Proof of Theorem 1. It follows from Kronecker's criterion for the reducibility of polynomials in several variables (cf. [3], Chapter VIII, §3) that for every irreducible polynomial $f(t_1, \ldots, t_r, x_1, \ldots, x_s)$ there exist a finite number of irreducible polynominals $g_j(t_1, \ldots, t_r, y)$ and a polynomial $\Phi(t_1, \ldots, t_r) \neq 0$ such that if for some $t_1', \ldots, t_r'$ all the polynomials $g_j(t_1', \ldots, t_r', y)$ are irreducible and $\Phi(t_1', \ldots, t_r') \neq 0$, then $f(t_1', \ldots, t_r', x_1, \ldots, x_s)$ is irreducible. In view of this fact it is sufficient to prove our Theorem for $s = 1$. We shall do that by induction with respect to n.

For $n = 1$ let

$$f_1(t_1, \ldots, t_r, x) = f = \sum_{\nu=0}^{j} \alpha_\nu(t_1, \ldots, t_r) x^{j-\nu}.$$

By Lemma 1 of [5], for each positive integer $i \leqslant j$ there exists a polynomial $\Omega_{i,j}(u; v_1, \ldots, v_j)$ with integer coefficients (the coefficient at the highest power of u being equal to 1) having the following property.

If $A(x)$, $B(x)$ are arbitrary polynomials,

$$A(x) = \sum_{\nu=0}^{j} a_\nu x^{j-\nu}, \quad B(x) = \sum_{\nu=0}^{h} b_\nu x^{h-\nu}, \quad a_0 b_0 \neq 0, \quad h \geqslant i$$

and $B(x)$ divides $A(x)$, then

$$\Omega_{i,j}\Big(\frac{b_i}{b_0}; \frac{a_1}{a_0}, \ldots, \frac{a_j}{a_0}\Big) = 0. \tag{7}$$

For $i \leqslant j$ let

$$\begin{aligned} \Omega_{i,j}\big(u; \alpha_1(t_1, \ldots, t_r), \alpha_0(t_1, \ldots, t_r)\alpha_2(t_1, \ldots, t_r), \ldots, \\ \ldots, \alpha_0(t_1, \ldots, t_r)^{j-1}\alpha_j(t_1, \ldots, t_r)\big) = F_i(t_1, \ldots, t_r, u) \prod_{\mu=1}^{m_i} \big(u - \psi_{i,\mu}(t_1, \ldots, t_r)\big), \end{aligned} \tag{8}$$

where $m_i \geqslant 0$, F_i and $\psi_{i,\mu}$ $(1 \leqslant \mu \leqslant m_i)$ are polynomials and for no polynomial $\psi(t_1, \ldots, t_r)$

$$F_i\big(t_1, \ldots, t_r, \psi(t_1, \ldots, t_r)\big) = 0 \text{ identically.}$$

Since $F_i(t_1, \ldots, t_r, u)$ has the coefficient at the highest power of u equal to 1, it follows that for no rational function $\varphi(t_1, \ldots, t_r)$, $F_i\big(t_1, \ldots, t_r, \varphi(t_1, \ldots, t_r)\big) = 0$ identically, and thus for no rational function $\varphi(t_1, \ldots, t_r)$,

$$\prod_{i=1}^{j} F_i\big(t_1, \ldots, t_r, \varphi(t_1, \ldots, t_r)\big) = 0 \text{ identically.} \tag{9}$$

Now, let i_0 be the least value of $i \leqslant j$ such that $m_i = 0$, if such values exist; otherwise let $i_0 = j$. For each positive integer $h < i_0$ and each system $\mu_1, \ldots, \mu_h$, where $1 < \mu_i \leqslant m_i$ $(1 \leqslant i \leqslant h)$, put

$$\begin{aligned} g_{\mu_1,\ldots,\mu_h}(t_1, \ldots, t_r, x) \\ = \big(a_0(t_1, \ldots, t_r)x\big)^h + \sum_{i=1}^{h} \psi_{i,\mu_i}(t_1, \ldots, t_r)\big(a_0(t_1, \ldots, t_r)x\big)^{h-i}. \end{aligned} \tag{10}$$

Since f is irreducible and $h < j$, the polynomials f and $g_{\mu_1,\ldots,\mu_h}$ are relatively prime; thus there exist polynomials $Q_{\mu_1,\ldots,\mu_h}(t_1, \ldots, t_r, x)$, $S_{\mu_1,\ldots,\mu_h}(t_1, \ldots, t_r, x)$ and $R_{\mu_1,\ldots,\mu_h}(t_1, \ldots, t_r)$ such that

$$Q_{\mu_1,\ldots,\mu_h} f + S_{\mu_1,\ldots,\mu_h} g_{\mu_1,\ldots,\mu_h} = R_{\mu_1,\ldots,\mu_h} \neq 0. \tag{11}$$

Now by Lemma 1 and (9) there exist r progressions $P_1, \dots, P_r$ such that if $t_l \in P_l$ $(1 \leqslant l \leqslant r)$, then

$$a_0(t_1, \dots, t_r) z(t_1, \dots, t_r) \prod_{\substack{\mu_1, \dots, \mu_h \\ h < i_0}} R_{\mu_1, \dots, \mu_h}(t_1, \dots, t_r) \prod_{i=1}^{j} F_i(t_1, \dots, t_r, u) \neq 0 \tag{12}$$

for all rational u.

We are going to prove that these progressions $P_1, \dots, P_r$ have the properties required in the theorem. Suppose, therefore, that for some $t_1', \dots, t_r'$ where $t_l' \in P_l$ $(1 \leqslant l \leqslant r)$, $f(t_1', \dots, t_r', x)$ is reducible and divisible by a monic polynomial

$$g(x) = x^h + \sum_{\nu=1}^{h} \beta_\nu x^{h-\nu}, \quad \text{where} \quad 1 \leqslant h < j. \tag{13}$$

By (12), $\alpha_0(t_1', \dots, t_r') \neq 0$. Put $\alpha_\nu = \alpha_\nu(t_1', \dots, t_r')$ $(0 \leqslant \nu \leqslant j)$,

$$A(x) = \alpha_0^{j-1} f\Big(t_1', \dots, t_r', \frac{x}{\alpha_0}\Big) = x^j + \sum_{\nu=1}^{j} \alpha_0^{\nu-1} \alpha_\nu x^{j-\nu},$$

$$B(x) = \alpha_0^h g\Big(\frac{x}{\alpha_0}\Big) = x^h + \sum_{\nu=1}^{h} \alpha_0^\nu \beta_\nu x^{h-\nu}.$$

Clearly $B(x)$ divides $A(x)$, and by (7) for each $i \leqslant h$

$$\Omega_{i,j}\big(\alpha_0^i \beta_i; \alpha_1, \alpha_0 \alpha_2, \dots, \alpha_0^{j-1} \alpha_j\big) = 0.$$

By (8) and (12) it follows that $i_0 > 1$, $h < i_0$ and that for some system $\mu_1', \dots, \mu_h'$

$$\alpha_0^i \beta_i = \psi_{i,\mu_1'}(t_1', \dots, t_r') \quad (1 \leqslant i \leqslant h,\ 1 \leqslant \mu_i' \leqslant m_i).$$

This gives by (13) and (10)

$$\alpha_0^h g(x) = (\alpha_0 x)^h + \sum_{i=1}^{h} \psi_{i,\mu_i'}(t_1', \dots, t_r')(\alpha_0 x)^{h-i} = g_{\mu_1', \dots, \mu_h'}(t_1', \dots, t_r', x). \tag{14}$$

Since $h < j$, we have by (11) and (12)

$$Q_{\mu_1', \dots, \mu_h'}(t_1', \dots, t_r', x) f(t_1', \dots, t_r', x) + S_{\mu_1', \dots, \mu_h'}(t_1', \dots, t_r', x) g_{\mu_1', \dots, \mu_h'}(t_1', \dots, t_r', x) = R_{\mu_1', \dots, \mu_h'}(t_1', \dots, t_r') \neq 0.$$

It follows hence by (14) that $g(x)$ divides

$$R_{\mu_1', \dots, \mu_h'}(t_1', \dots, t_r') \neq 0,$$

which is impossible.

The contradiction obtained completes the proof for $n = 1$. Assume now that the theorem holds for $n - 1$ polynomials $(n > 1)$ and that we are given n irreducible polynomials $f_m(t_1, \dots, t_r, x)$ $(1 \leqslant m \leqslant n)$ and a polynomial $z(t_1, \dots, t_r)$ not identically 0. By the inductive assumption there exist r progressions, say $a_l u + b_l$ $(1 \leqslant l \leqslant r)$, such that

if $t'_l \equiv b_l \pmod{a_l}$ $(1 \leqslant l \leqslant r)$ then $f_m(t'_1, \ldots, t'_r, x)$ for $m < n$ are irreducible and $z(t'_1, \ldots, t'_r) \neq 0$.

Now, $f_n(a_1u_1 + b_1, \ldots, a_ru_r + b_r, x)$ is an irreducible polynomial in $u_1, \ldots, u_r, x$ and therefore by the already proved case of our theorem there exist r progressions, say $c_lv + d_l$ $(1 \leqslant l \leqslant r)$, such that if $u'_l \equiv d_l \pmod{c_l}$ then $f_n(a_1u'_1 + b_1, \ldots, \ldots, a_ru'_r + b_r, x)$ is irreducible. Denote by P_l the progression $a_lc_lv + (a_ld_l + b_l)$ $(1 \leqslant l \leqslant r)$. If $t'_l \in P_l$, then the polynomials $f_m(t'_1, \ldots, t'_r, x)$ $(1 \leqslant m \leqslant n)$ are irreducible and $z(t'_1, \ldots, t'_r) \neq 0$, which completes the inductive proof. □

Since rational numbers belonging to a progression according to our definition form a dense set, we get

Corollary. *Let $f_m(t_1, \ldots, t_r, x_1, \ldots, x_s)$ $(1 \leqslant m \leqslant n)$ be irreducible polynomials in $r + s$ variables. The set of all rational points $(t'_1, \ldots, t'_r)$ for which the polynomials $f_m(t'_1, \ldots, t'_r, x_1, \ldots, x_s)$ $(1 \leqslant m \leqslant n)$ are irreducible contains a Cartesian product of r dense linear sets.*

As the second application of Lemma 1 we prove the following generalization of Theorem 1 in [1].

Theorem 2. *Let $F(t_1, \ldots, t_r, u)$ be a polynomial such that for no polynomial $\psi(t_1, \ldots, t_r)$,*

$$F\big(t_1, \ldots, t_r, \psi(t_1, \ldots, t_r)\big) = 0$$

identically. There exist r arithmetical progressions $P_1, \ldots, P_r$ such that if $t_l \in P_l$ $(1 \leqslant l \leqslant r)$, then

$$F(t_1, \ldots, t_r, u) \neq 0 \quad \textit{for all integers } u.$$

Lemma 2. *Let $\varphi_m(t_1, \ldots, t_r)$ $(1 \leqslant m \leqslant n)$ be rational but not integer functions. There exist r arithmetical progressions $P_1, \ldots, P_r$ such that if $t_l \in P_l$, then neither of the numbers $\varphi_m(t_1, \ldots, t_r)$ is an integer.*

Proof by induction with respect to n. For $n = 1$, let

$$\varphi_1(t_1, \ldots, t_r) = \frac{g(t_1, \ldots, t_r)}{h(t_1, \ldots, t_r)},$$

where g, h are coprime polynomials with integer coefficients and h is not a constant. Without loss of generality we may assume that h is of positive degree in t_1. Denote by $a_0(t_2, \ldots, t_r)$ the coefficient at the highest power of t_1 in h.

Since $(g, h) = 1$, there exist polynomials $Q(t_1, \ldots, t_r)$, $S(t_1, \ldots, t_r)$ and $R(t_2, \ldots, t_r)$ such that

$$Qg + Sh = R \neq 0. \tag{15}$$

Choose integers $t'_2, \ldots, t'_r$ so that $a_0(t'_2, \ldots, t'_r)R(t'_2, \ldots, t'_r) \neq 0$. Since $h(t_1, t'_2, \ldots, t'_r)$ depends upon t_1, there exists an integer t'_1 such that

$$c = |h(t'_1, \ldots, t'_r)| > |R(t'_2, \ldots, t'_r)|.$$

Denote by P_l the progression $cv + t_l'$ $(1 \leqslant l \leqslant r)$. If $t_l \in P_l$ $(1 \leqslant l \leqslant r)$, we have

$$h(t_1, \ldots, t_r) \equiv h(t_1', \ldots, t_r') \equiv 0 \pmod{c},$$
$$R(t_2, \ldots, t_r) \equiv R(t_2', \ldots, t_r') \not\equiv 0 \pmod{c}$$

and in view of (15)

$$g(t_1, \ldots, t_r) \not\equiv 0 \pmod{c},$$

which proves that $g(t_1, \ldots, t_r)/h(t_1, \ldots, t_r)$ is not an integer.

Assume now that the lemma is true for $n-1$ rational functions and that we are given n rational but not integer functions $\varphi_m(t_1, \ldots, t_r)$ $(1 \leqslant m \leqslant n)$. By the inductive assumption there exist r progressions, say $a_l u + b_l$ $(1 \leqslant l \leqslant r)$, such that if $t_l \equiv b_l \pmod{a_l}$, then none of the numbers $\varphi_m(t_1, \ldots, t_r)$ $(1 \leqslant m \leqslant n-1)$ is an integer. Now $\varphi_n(a_1u_1+b_1, \ldots, \ldots, a_ru_r+b_r)$ is a rational but not an integer function of $u_1, \ldots, u_r$, and therefore, by the already proved case of our lemma, there exist r progressions, say $c_l v+d_l$ $(1 \leqslant l \leqslant r)$, such that if $u_l \equiv d_l \pmod{c_l}$ then the number $\varphi_n(a_1u_1 + b_1, \ldots, a_ru_r + b_r)$ is not an integer. Denote by P_l the progression $a_lc_lv + (a_ld_l + b_l)$ $(1 \leqslant l \leqslant r)$. If $t_l \in P_l$ $(1 \leqslant l \leqslant r)$, then none of the numbers $\varphi_m(t_1, \ldots, t_r)$ $(1 \leqslant m \leqslant n)$ is an integer, which completes the inductive proof. □

Proof of Theorem 2. By the assumption, polynomial F can be written in the form

$$F(t_1, \ldots, t_r, u) = F_0(t_1, \ldots, t_r, u) \prod_{m=1}^{n} \big(u - \varphi_m(t_1, \ldots, t_r)\big),$$

where F_0 is a polynomial such that for no rational function φ, $F_0\big(t_1, \ldots, t_r, \varphi(t_1, \ldots, t_r)\big) = 0$ identically, $n \geqslant 0$ and φ_m $(1 \leqslant m \leqslant n)$ are rational but not integer functions.

By Lemma 1 there exist r progressions, say $a_l u + b_l$ $(1 \leqslant l \leqslant r)$, such that if $t_l \equiv b_l \pmod{a_l}$, then

$$F_0(t_1, \ldots, t_r, u) \neq 0 \quad \text{for all rational } u.$$

By Lemma 2 there exist r progressions, say $c_l v + d_l$ $(1 \leqslant l \leqslant r)$, such that if $u_l \equiv d_l \pmod{c_l}$, then none of the numbers $\varphi_m(a_1u_1 + b_1, \ldots, a_ru_r + b_r)$ $(1 \leqslant m \leqslant n)$ is an integer. It follows that the progressions $a_lc_lv + (a_ld_l + b_l)$ have the properties required in the theorem. □

The following modifications of Lemma 1 and Theorem 2 could seem plausible (cf. [6]).

M1. *Let $F(t_1, \ldots, t_r, u, v)$ be a polynomial such that for no pair of rational functions $\varphi(t_1, \ldots, t_r)$, $\psi(t_1, \ldots, t_r)$*

$$F\big(t_1, \ldots, t_r, \varphi(t_1, \ldots, t_r), \psi(t_1, \ldots, t_r)\big) = 0 \quad \textit{identically.} \tag{16}$$

There exist r arithmetical progressions $P_1, \ldots, P_r$ (respectively an infinite set S of integer points) such that if $t_l \in P_l$ $(1 \leqslant l \leqslant r)$ (respectively $(t_1, \ldots, t_r) \in S$), then

$$F(t_1, \ldots, t_r, u, v) \neq 0 \quad \textit{for all rational } u, v.$$

M2. *Let* $F(t_1, \dots, t_r, u, v)$ *be a polynomial such that for no pair of rational functions* $\varphi(t_1, \dots, t_r)$, $\psi(t_1, \dots, t_r)$, (16) *holds. There exist* r *arithmetical progressions* $P_1, \dots, P_r$ (*respectively an infinite set* S *of integer points*) *such that if* $t_l \in P_l$ $(1 \leqslant l \leqslant r)$ (*respectively* $(t_1, \dots, t_r) \in S$), *then*

$$F(t_1, \dots, t_r, u, v) \neq 0 \quad \textit{for all integers } u, v.$$

Now, the strong form of M1 and both forms of M2 are false, as shown by the examples

$$F_1(t, u, v) = t + u^2 + v^3 \quad \text{and} \quad F_2(t, u, v) = (2t - 1)u - (v^2 + 1)(v^2 + 2)(v^2 - 2),$$

respectively. Indeed, as to the former, it is known that the equation $3s^6 + u^2 + v^3 = 0$ is insoluble in rational u, v for every rational $s \neq 0$, which would not be possible if for some rational functions $\varphi(t)$, $\psi(t)$ we had an identity $F_1\big(t, \varphi(t), \psi(t)\big) = 0$.

On the other hand, if $av + b$ is an arbitrary progression P, then according to a well-known theorem (cf. [4]) there exist integers u_0, v_0 such that $-u_0^2 - v_0^3 \in P$ and thus for $t_0 = -u_0^2 - v_0^3$, $t_0 \in P$ and $F_1(t_0, u_0, v_0) = 0$.

As to the second counterexample, if for some polynomials $\varphi(t)$, $\psi(t)$ we had an identity $F_2\big(t, \varphi(t), \psi(t)\big) = 0$, then

$$\big(\psi(\tfrac{1}{2})^2 + 1\big)\big(\psi(\tfrac{1}{2})^2 + 2\big)\big(\psi(\tfrac{1}{2})^2 - 2\big) = 0,$$

which is impossible. On the other hand, if t is any integer, we easily see by factorizing $2t - 1$ into prime factors that the congruence

$$(v^2 + 1)(v^2 + 2)(v^2 - 2) \equiv 0 \pmod{2t - 1}$$

is soluble and so is the equation $F_2(t, u, v) = 0$.

As to the weak form of M1, I am unable to disprove it and to prove it seems to me very difficult even for $r = 1$.

References

[1] H. Davenport, D. J. Lewis, A. Schinzel, *Polynomials of certain special types*. Acta Arith. 9 (1964), 107–116; this collection: A6, 27–35.

[2] H. Hasse, *Zwei Bemerkungen zu der Arbeit „Zur Arithmetik der Polynome" von U. Wegner in den Math. Ann. 105, S. 628–631*. Math. Ann. 106 (1932), 455–456.

[3] S. Lang, *Diophantine Geometry*. Interscience, New York and London 1962.

[4] L. J. Mordell, *Note on cubic equations in three variables with an infinity of integer solutions*. Ann. Mat. Pura Appl. (4) 29 (1949), 301–305.

[5] A. Schinzel, *Reducibility of polynomials in several variables*. Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys. 11 (1963), 633–638; this collection: E2, 709–714.

[6] —, *Some unsolved problems on polynomials*. In: Neki nerešeni problemi u matematici, Matematička Biblioteka 25, Beograd 1963, 63–70; this collection: E1, 703–708.

Andrzej Schinzel
Selecta

Originally published in
Mathematica Slovaca 41 (1991), 295–298

A class of polynomials

Abstract. We characterize the polynomials $\varphi(x) \in \mathbb{Z}[x]$ such that for any $f(x) \in \mathbb{Z}[x]$ from inclusion $\{f(a) : a = k, k+1, \dots\} \subset \{\varphi(b) : b = 0, \pm 1, \pm 2, \dots\}$ follows $f(x) = \varphi(h(x))$ for some $h(x) \in \mathbb{Z}[x]$.

Call a polynomial $\varphi(x)$ *good* if it has the following property:

For every polynomial $f(x) \in \mathbb{Z}[x]$ such that for every sufficiently large integer $a \in \mathbb{Z}$ there is $b \in \mathbb{Z}$ such that $f(a) = \varphi(b)$ there is a polynomial $h(x) \in \mathbb{Z}[x]$ such that $f(x) = \varphi(h(x))$.

I. Korec suggested to study good polynomials in connection with his results concerning palindromic squares in [1].

In this note we prove the following criterion:

Theorem. *A polynomial $\varphi \in \mathbb{Z}[x]$ is good if and only if $\varphi(x/m) \notin \mathbb{Z}[x]$ for all $m > 1$.*

To prove this result we need the

Lemma. *Let for a polynomial F with algebraic coefficients $C(F)$ denote the content of F, i.e. the ideal generated by the coefficients of F. If $p \in \mathbb{Z}[x]$, $q \in \mathbb{Q}[x]$ and $p(0) = 0$, then*

$$C\big(q(p)\big) \mid C(q)C(p)^{\deg q}.$$

Proof. We have

$$q(x) = q_0 \prod_{i=1}^{\deg q} (x - \varrho_i),$$

and by the generalized Gauss lemma

$$C(q) = (q_0) \prod_{i=1}^{\deg q} C(x - \varrho_i) = (q_0) \prod_{i=1}^{\deg q} (1, \varrho_i).$$

Similarly

$$C\big(q(p)\big) = (q_0) \prod_{i=1}^{\deg q} C(p(x) - \varrho_i) = (q_0) \prod_{i=1}^{\deg q} (C(p), \varrho_i),$$

and since $C(p)$ is integral, the lemma follows. □

Proof of the Theorem. We shall prove first that the condition is necessary. If for an $m > 1$ $\varphi(x/m) \in \mathbb{Z}[x]$, we have

$$f(x) = \varphi\left((m-1)!\binom{x}{m}\right) \in \mathbb{Z}[x].$$

Also for every $x^* \in \mathbb{Z}$ there exists a $y^* \in \mathbb{Z}$ such that

$$f(x^*) = \varphi(y^*).$$

If, however, we had $f(x) = \varphi(g(x))$, $g \in \mathbb{Z}[x]$, it would follow that

$$\varphi\left((m-1)!\binom{x}{m}\right) = \varphi(g(x)),$$

which gives a contradiction, since the leading coefficient of the left hand side is smaller than the leading coefficient of the right hand side.

In order to prove that the condition is sufficient, let a be the leading coefficient of φ
c and assume that for an $f \in \mathbb{Z}[x]$ we have $f(x^*) = \varphi(y^*)$ for every $x^* \in \mathbb{Z}$, $x^* \geqslant K$ and a suitable $y^* \in \mathbb{Z}$. Let

$$\varphi(y) - f(x) = \prod_{i=1}^{n} F_i(x, y), \tag{1}$$

where the polynomials $F_i \in \mathbb{Z}[x, y]$ are irreducible and F_i viewed as a polynomial in y has the leading coefficient $a_i(x)$. Clearly

$$a = \prod_{i=1}^{n} a_i(x),$$

hence $a_i(x) \in \mathbb{Z}$ for all $i \leqslant n$. Without loss of generality we may assume that

$$F_i(y) = a_i y - h_i(x) \quad \text{for} \quad i \leqslant m,$$
$$\deg_y F_i > 1 \quad \text{for} \quad i > m.$$

By Hilbert's Irreducibility Theorem there exists an integer t^* such that $at^* \geqslant K$, $F_i(at^*, y)$ is irreducible for all $i > m$ and hence

$$F_i(at^*, y) = 0$$

has no rational root. Since by the assumption

$$\varphi(y^*) - f(at^*) = 0 \quad \text{for a } y^* \in \mathbb{Z},$$

by (1) there is a $j \leqslant m$ such that

$$F_j(at^*, y^*) = 0,$$

which gives

$$a_j y^* - h_j(at^*) = 0,$$

and since $a_j \mid a$

$$h_j(0) \equiv h_j(at^*) \equiv 0 \pmod{a_j}. \tag{2}$$

Let

$$C\big(h_j(x) - h_j(0)\big) = (c),$$

and take in the lemma

$$p(x) = \frac{h_j(x) - h_j(0)}{(c, a_j)}, \quad q(x) = \varphi\left(\frac{x}{a_j/(c, a_j)} + \frac{h_j(0)}{a_j}\right).$$

We obtain

$$C\big(q(p)\big) \mid C(q)C(p)^{\deg q} = C(q) \cdot \left(\frac{c}{(c, a_j)}\right)^{\deg q},$$

and since by (1) $q(p) = f \in \mathbb{Z}[x]$

$$C(q) \cdot \left(\frac{c}{(c, a_j)}\right)^{\deg q} \subset \mathbb{Z}.$$

However by (2)

$$C(q) \cdot \left(\frac{a_j}{(c, a_j)}\right)^{\deg q} \subset \mathbb{Z},$$

and since

$$\left(\frac{c}{(c, a_j)}, \frac{a_j}{(c, a_j)}\right) = 1$$

the two inclusions give

$$C(q) \subset \mathbb{Z};$$

$$q \in \mathbb{Z}[x], \quad \varphi\left(\frac{x}{a_j/(c, a_j)}\right) = q\left(x - \frac{h_j(0)}{(c, a_j)}\right) \in \mathbb{Z}[x].$$

c

By the condition on φ:

$$|a_j|/(c, a_j) = 1,$$

hence $a_j \mid c$ and by (2)

$$\frac{h_j(x)}{a_j} = \frac{h_j(x) - h_j(0)}{a_j} + \frac{h_j(0)}{a_j} \in \mathbb{Z}[x].$$

Since by (1)

$$f(x) = \varphi\left(\frac{h_j(x)}{a_j}\right),$$

the proof is complete. □

Reference

[1] I. Korec, *Palindromic squares for various number system bases*. Math. Slovaca 41 (1991), 261–276.

Originally published in
Acta Arithmetica 69 (1995), 293–302

The least admissible value of the parameter in Hilbert's Irreducibility Theorem

with Umberto Zannier (*Venezia*)

Dedicated to Professor Wolfgang M. Schmidt on the occasion of his 60th birthday

The simplest case of Hilbert's Irreducibility Theorem asserts that if $F(t,x)$ is irreducible over $\mathbb{Q}$, then there exists $t^* \in \mathbb{Q}$ such that $F(t^*,x)$ is irreducible over $\mathbb{Q}$. Many different proofs have been given for this theorem, namely Hilbert's (1892) [10], Mertens's (1911) [13], Skolem's (1921) [17], Dörge's (1927) [5], Siegel's (1929) [16], Eichler's (1939) [6], Inaba's (1943) [11], Fried's (1974) [8], Roquette's (1975) [14], Cohen's (1981) [2], Sprindzhuk's (1981) [18], Dèbes's (1986) [3], (1993) [4].

Only the last of the quoted papers explicitly mentions the problem of estimating the size of a t^* with the above property in terms of the degree and height of F. By the *height* of F, to be abbreviated $H(F)$, we mean the maximum absolute value of the coefficients of a constant multiple of F that has coprime integer coefficients. Dèbes gives actually an estimate value for several polynomials F_i. His result reads (see Cor. 3.7 of [4]):

Let $F_1, \dots, F_h$ be irreducible polynomials in $\mathbb{Q}[t,x]$ such that $\deg F_i \leqslant D$ *and* $H(F_i) \leqslant H$ ([1]). *Then there exists a rational number $t^* = u/v$ such that each $F_i(t^*,x)$ is irreducible over $\mathbb{Q}$ and*

$$\max(|u|,|v|) \leqslant \exp\bigl(10^{10} D^{100hD^2 \log D} (\log^2 H + 1)\bigr). \tag{1}$$

Dèbes also gives a corresponding result for algebraic number fields. We observe that Cohen's result, formulated for algebraic number fields, is partially explicit and gives, in the case of the rational field, the following bound:

Under the same assumptions as before, for $H \geqslant e^e$ one may find a $t^* \in \mathbb{Z}$ with the above property such that

$$|t^*| \leqslant h^2 \log(eh) H^c, \tag{2}$$

where c depends only on D.

([1]) Dèbes in fact formulates his result in terms of the logarithmic height.

Actually, assuming the Riemann Hypothesis for zeta functions of number fields, Cohen obtained an estimate implying the sharp bound

$$|t^*| \leqslant \max\{ch^2 \log(eh), \log^4 H\}.$$

This includes a result by Fogels [7] concerning the special case $h = 1$, $F(t, x) = f_1(x) + tf_2(x)$. Yasumoto [19] asked whether for $h = 1$ there exists a bound for $|t^*|$ independent of H.

The aim of the present paper is to prove the following theorem, which improves on both (1) and (2), as far as the dependence on D and H is concerned.

Theorem. *Let $F_1, \ldots, F_h \in \mathbb{Z}[t, x]$ be irreducible over $\mathbb{Q}$. There exists a positive integer t^* such that $F_i(t^*, x)$ are irreducible for all $i \leqslant h$ and*

$$|t^*| \leqslant \max\{\exp(2(6m)^5), \exp(36^6), h^9 \exp\big(450(\log H)^{5/6} + 11250m^5 + 45(m+1)^2 n + 45n(\log H)^{2/5}\big)\},$$

where $m = \max\{\deg_t F_i\}$, $n = \max\{\deg_x F_i\}$, $H = \max\{20, H(F_i)\}$.

Auxiliary lemmas

Our proof will make use of a sharp estimate by Bombieri and Pila [1] of the number of integral points on algebraic plane curves. A direct application of their Theorem 5 would lead, however, to a bound weaker than the stated above. Nevertheless it is possible to modify their proof to produce a result which is more suitable for our purposes. This will be done in the course of the proof of our first lemma.

Lemma 1. *Let $\Phi \in \mathbb{Q}[t, y]$ be a polynomial irreducible over $\mathbb{Q}$, of total degree D. Then, for every positive integer $\delta < D$ and for every $N \geqslant 1$, the number of integer points (t^*, y^*) such that $\Phi(t^*, y^*) = 0$ and $\max\{|t^*|, |y^*|\} \leqslant N$ is bounded by*

$$(3D\Delta)^{\Delta+4} N^{8/(3(\delta+3))},$$

where $\Delta = (\delta + 1)(\delta + 2)/2$.

Proof. Consider first the case when Φ is reducible over $\mathbb{C}$. Then $\Phi(t^*, y^*) = 0$ implies that $\Psi(t^*, y^*) = 0$ for some factor Ψ of Φ, irreducible over $\mathbb{C}$ and with the coefficient of the leading term (in the inverse lexicographic order) equal to 1, hence also $\Psi'(t^*, y^*) = 0$, where Ψ' is conjugate to Ψ over $\mathbb{Q}$, and so is another factor of Φ. Since $\mathrm{Res}_y(\Psi, \Psi')^2 \mid \mathrm{disc}_y \Phi$, it follows that the number of integers t^* such that for some integer y^*, $\Psi(t^*, y^*) = \Psi'(t^*, y^*) = 0$, does not exceed $\frac{1}{2}\deg(\mathrm{disc}_y \Phi) \leqslant D(D-1)$. Since the same estimate applies to integers y^*, the total number of integer points is $\leqslant D^2(D-1)^2 < (3D\Delta)^{\Delta+4}$.

Assume therefore that Φ is absolutely irreducible. Let $G(N) = G(D, N)$ be the maximum number of integer points on the graph of a C^∞ function $g(t)$, on an interval $\mathcal{I}$ of length at most N, with $|g'(t)| \leqslant 1$ and g satisfying some algebraic relation $\Gamma(t, g) = 0$, with Γ absolutely irreducible of degree D. Clearly we may assume $\mathcal{I} \subset [0, N]$.

Now fix some positive integer $\delta < D$ and let $g(t)$ be such a C^∞ function. Given $A \geqslant 1$, by appealing to Lemma 6 of [1], we can divide the domain $\mathcal{I}$ of g into at most $2D^2(\Delta-1)^2 \leqslant 2D^2\Delta^2$ subintervals $\mathcal{I}_\nu$ such that, for each $\mathcal{I}_\nu$ and each $l = 1, \ldots, \Delta-1$, either (i) or (ii) holds:

(i) $|g^{(l)}(t)| \leqslant l!\, A^{l/(\Delta-1)} N^{1-l}$ for all $t \in \mathcal{I}_\nu$;
(ii) $|g^{(l)}(t)| > l!\, A^{l/(\Delta-1)} N^{1-l}$ for all $t \in \mathcal{I}_\nu$.

After translating the graph of $g(t)$ on each $\mathcal{I}_\nu$ by an integer, we can assume, since $|g'(t)| \leqslant 1$, that $|g(t)| \leqslant N$ for all $t \in \mathcal{I}_\nu$. Now, for each $\mathcal{I}_\nu$, either (i) or (ii) holds:

(i) $|g^{(l)}(t)| \leqslant l!\, A^{l/(\Delta-1)} N^{1-l}$ for all $t \in \mathcal{I}_\nu$ and all $l = 0, \ldots, \Delta-1$;
(ii) $|g^{(l)}(t)| \leqslant l!\, A^{l/(\Delta-1)} N^{1-l}$ for all $t \in \mathcal{I}_\nu$ and all $l < k$, and
$|g^{(k)}(t)| \geqslant k!\, A^{k/(\Delta-1)} N^{1-k}$ for all $t \in \mathcal{I}_\nu$.

In the case (i) we have

$$\|g\|_{\Delta-1} := \max_{0 \leqslant k \leqslant \Delta-1} \max_{t \in \mathcal{I}_\nu} \frac{|g^{(k)}(t)|}{k!}\, N^{1-k} \leqslant A.$$

In the case (ii) the hypotheses of Lemma 7 of [1] hold with $A^{k/(\Delta-1)}$ in place of A, and hence

$$|\mathcal{I}_\nu| \leqslant 2A^{-1/(\Delta-1)} N.$$

For the $\mathcal{I}_\nu$ of the first type we apply the Main Lemma of [1], with d replaced by δ, D replaced by Δ, f replaced by g. We infer that integral points on $y = g(t)$, $t \in \mathcal{I}_\nu$, lie on the union of at most $4(A^{1/2}N)^{8/(3(\delta+3))}$ real algebraic curves of degree $\leqslant d$. Since $\delta < D$ these curves cannot contain the appropriate translation of $\Gamma(t, y) = 0$, thus we infer from Bézout's theorem that each of them intersects the translation in question in at most δD points. We thus obtain the following recurrence relation for $G(N)$:

$$G(N) \leqslant K_1 N^\alpha + K_2 G(\lambda N),$$

where

$$K_1 = 8D^3\delta\Delta^2 A^{4/(3(\delta+3))}, \quad K_2 = 2D^2\Delta^2, \quad \alpha = \frac{8}{3(\delta+3)}, \quad \lambda = 2A^{-1/(\Delta-1)}.$$

Continuing, we find that, provided $\lambda^{\nu-1} N \geqslant 1$,

$$G(N) \leqslant K_1 N^\alpha \left(1 + K_2\lambda^\alpha + \ldots + (K_2\lambda^\alpha)^{\nu-1}\right) + K_2^\nu G(\lambda^\nu N).$$

We now choose λ so that $K_2\lambda^\alpha = 1/2$, that is, we set

$$\lambda = \left(\frac{1}{2K_2}\right)^{1/\alpha} = (4D^2\Delta^2)^{-3(\delta+3)/8} < 1$$

and thus

$$A = \left(\frac{2}{\lambda}\right)^{\Delta-1} > 1.$$

Finally, we choose ν so that $\lambda/N \leqslant \lambda^\nu < 1/N$. Then $G(\lambda^\nu N) \leqslant 1$ and

$$G(N) \leqslant 2K_1 N^\alpha + 2^{-\nu}\lambda^{-\alpha} N^\alpha \leqslant 2(K_1 + K_2) N^\alpha.$$

Now,

$$\begin{aligned} K_1 + K_2 &= 8D^3\delta\Delta^2 A^{4/(3(\delta+3))} + 2D^2\Delta^2 \\ &= 8D^3\delta\Delta^2 2^{4(\Delta-1)/(3(\delta+3))}(4D^2\Delta^2)^{(\Delta-1)/2} + 2D^2\Delta^2 \\ &< 10D^3\delta\Delta^2(8D^2\Delta^2)^{(\Delta-1)/2}, \end{aligned}$$

which gives

$$G(N) < 20D^3\delta\Delta^2(8D^2\Delta^2)^{(\Delta-1)/2}N^\alpha.$$

Our original curve $\mathcal{C} : \Phi(t, y) = 0$ has at most $\frac{1}{2}D(D-1)$ singular points, and at most $2D(D-1)$ points of slope ± 1. Hence $\mathcal{C} \cap [0, N]^2$ is made up of at most $3D^2$ graphs of C^∞ functions with slope bounded by 1 with respect to one of the axes. The number of integral points is therefore at most

$$3D^2G(N) < 60D^5\delta\Delta^2(8D^2\Delta^2)^{(\Delta-1)/2}N^\alpha < \tfrac{1}{2}(3D\Delta)^{\Delta+4}N^\alpha.$$

Replacing N with $2N$ we obtain the lemma. □

Let $F(t, x) \in \mathbb{Z}[t, x]$, write $F(t, x) = a_0(t)\prod_{i=1}^{n}(x - x_i)$, where x_i are elements of $\overline{\mathbb{Q}(t)}$, and let $D(t)$ be the discriminant of F with respect to x. For a nonempty subset ω of $\{1, \ldots, n\}$ and for every positive integer $j \leqslant \#\omega$, let $P_{\omega,j}(t, y)$ be the minimal polynomial of $a_0(t)\tau_j(x_i : i \in \omega)$ over $\mathbb{Q}(t)$, where τ_j is the jth fundamental symmetric function. We remark that, in virtue of an old theorem of Kronecker (see [15], Theorem 10, p. 48), $a_0(t)\tau_j(x_i : i \in \omega)$ is in any case integral over $\mathbb{Z}[t]$, whence $P_{\omega,j}$ is a polynomial in $\mathbb{Z}[t, y]$, monic in y.

Lemma 2. *For all $t^* \in \mathbb{Z}$, if $a_0(t^*)D(t^*) \neq 0$ and $F(t^*, x)$ is reducible over $\mathbb{Q}$, then for some $\omega \subset \{1, \ldots, n\}$ of cardinality $k \leqslant n/2$ all the polynomials $P_{\omega,j}(t^*, y)$, $j \leqslant k$, have a zero $y_j \in \mathbb{Z}$.*

Proof. Let K be the splitting field of $F(t, x)$ over $\mathbb{Q}(t)$, and let Δ be the discriminant of K (over $\mathbb{Q}[t]$). If $D(t^*) \neq 0$, then $t - t^*$ is not ramified in K, hence $\Delta(t^*) \neq 0$. By a well known result (see [9], p. 464) there exists a generator θ of K integral over $\mathbb{Q}[t]$ and such that $\operatorname{disc}_x T(t^*) \neq 0$, where $T(t, x)$ is the minimal polynomial of θ over $\mathbb{Q}(t)$. We have accordingly

$$x_i = \frac{L_i(t, \theta)}{M(t)} \quad (1 \leqslant i \leqslant n),$$

where $M \in \mathbb{Q}[t]$, $L_i \in \mathbb{Q}[t, u]$ and $M(t^*) \neq 0$ provided $a_0(t^*) \neq 0$. It follows that in the ring $\mathbb{Q}[t, u, x]$ we have the congruences

$$a_0(t)M(t)^n F(t, x) \equiv a_0(t)\prod_{i=1}^{n}(M(t)x - L_i(t, u)) \pmod{T(t, u)} \tag{3}$$

and

$$M(t)^{j \deg P} P_{\omega,j}\big(t, a_0(t)\tau_j(L_i/M : i \in \omega)\big) \equiv 0 \pmod{T(t, u)} \tag{4}$$

for every nonempty $\omega \subset \{1, \dots, n\}$ and every $j \leqslant \#\omega$.

Assume now that $a_0(t^*)D(t^*) \neq 0$ and $F(t^*, x)$ is reducible over $\mathbb{Q}$. Without loss of generality we may suppose that

$$F(t^*, x) = a_0(t^*) \prod_{i=1}^{n} (x - x_i^*)$$

and that

$$a_0(t^*) \prod_{i=1}^{k} (x - x_i^*) \in \mathbb{Z}[x] \tag{5}$$

where $1 \leqslant k \leqslant n/2$.

Choose $u^* \in \mathbb{C}$ such that $T(t^*, u^*) = 0$. By (3),

$$a_0(t^*) \prod_{i=1}^{n} (x - x_i^*) = a_0(t^*) \prod_{i=1}^{n} \left(x - \frac{L_i(t^*, u^*)}{M(t^*)} \right);$$

hence there exists a subset ω of $\{1, \dots, n\}$ of cardinality k such that

$$\{x_1^*, \dots, x_k^*\} = \left\{ \frac{L_i(t^*, u^*)}{M(t^*)} : i \in \omega \right\}.$$

By (4), for every $j \leqslant k$,

$$P_{\omega, j}\big(t^*, a_0(t^*)\tau_j(x_1^*, \dots, x_k^*)\big) = 0$$

and since $y_j := a_0(t^*)\tau_j(x_1^*, \dots, x_k^*) \in \mathbb{Z}$ by (5), the assertion follows. □

Let F have degree m in t and n in x. We have

Lemma 3. *The polynomials $P_{\omega, j}(t, y)$ defined before the statement of Lemma 2 have, for $k \leqslant n/2$, the property that, if $|t^*| \geqslant 1$, $a_0(t^*)D(t^*) \neq 0$ and $P_{\omega, j}(t^*, y^*) = 0$, then*

$$|y^*| \leqslant 2^k \sqrt{n+1}(m+1)H|t^*|^m, \tag{6}$$

where H is the height of F. Moreover, $\deg(P_{\omega, j}) \leqslant m \deg_y(P_{\omega, j}) \leqslant m\binom{n}{k}$.

Proof. We retain the notation of the proof of Lemma 2. First observe that the polynomial

$$\prod_{\#\omega = k} \big(y - a_0(t)\tau_j(x_i : i \in \omega)\big),$$

the product being extended over all subsets ω of $\{1, \dots, n\}$ having cardinality k, lies clearly in $\mathbb{Q}[t, y]$, and has degree $\binom{n}{k}$ in y. Hence, since $P_{\omega, j}$ divides this polynomial, we have $\deg_y P_{\omega, j} \leqslant \binom{n}{k}$.

For the same reason we may write

$$P_{\omega, j}(t, y) = \prod_{I \in \Omega} \left(y - a_0(t)\tau_j\Big(\frac{L_i(t, \theta)}{M(t)} : i \in I \Big) \right),$$

the product being extended over a certain family Ω of subsets I of $\{1, \dots, n\}$ with $\#I = k$. Let

$$Q_{\omega,j}(t, u, y) = \prod_{I \in \Omega} \Big(y - a_0(t) \tau_j \Big(\frac{L_i(t, u)}{M(t)} : i \in I \Big) \Big).$$

Then, as in the proof of Lemma 2, we have the congruence

$$M(t)^{j \deg P} \big(Q_{\omega,j}(t, u, y) - P_{\omega,j}(t, y) \big) \equiv 0 \pmod{T(t, u)}$$

whence, setting $t = t^*$, $u = u^*$, where $T(t^*, u^*) = 0$, we get

$$P_{\omega,j}(t^*, y) = Q_{\omega,j}(t^*, u^*, y).$$

Hence all the zeros of $P_{\omega,j}(t^*, y)$ are of the form

$$a_0(t^*) \tau_j \Big(\frac{L_i(t^*, u^*)}{M(t^*)} : i \in I \Big),$$

namely of the form $a_0(t^*)\tau_j^*$, where τ_j^* is the jth symmetric function of a certain subset of cardinality k of the set $\{x_1^*, \dots, x_n^*\}$ of all zeros of $F(t^*, x)$.

By a classical theorem of Landau [12], for each $t^* \in \mathbb{C}$,

$$M := |a_0(t^*)| \prod_{i=1}^{n} \max\{1, |x_i^*|\} \leqslant \sqrt{\sum_{i=0}^{n} |a_i(t^*)|^2},$$

where $a_i(t)$ are the coefficients of $F(t, x)$ viewed as polynomial in x.

For $|t^*| \geqslant 1$ we have

$$|a_i(t^*)| \leqslant (m + 1) H |t^*|^m,$$

hence, by the above observations,

$$|y^*| \leqslant \binom{k}{j} \sqrt{n + 1} (m + 1) H |t^*|^m \leqslant 2^k \sqrt{n + 1} (m + 1) H t^{*m}$$

and the first part of the lemma follows

In order to prove the second part, write

$$P_{\omega,j}(t, y) = y^p + \sum_{i=1}^{p} P_i(t) y^{p-i}.$$

For every fixed $t^* \in \mathbb{C}$, $P_i(t^*)$ is, up to a sign, the ith fundamental symmetric function in the zeros of $P_{\omega,j}(t^*, y)$. Hence, if $|t^*| \geqslant 1$, by (6) we have

$$|P_i(t^*)| \leqslant \binom{p}{i} 2^{ki}(n+1)^{i/2}(m+1)^i H^i |t^*|^{mi} = O(|t^*|^{mi}),$$

which implies that $\deg(P_i) \leqslant mi$, so

$$\deg(P_{\omega,j}) = \max_{0 \leqslant i \leqslant p} \{p - i + \deg(P_i)\} \leqslant mp.$$

This completes the proof. □

Lemma 4. *Let $F(t, x) \in \mathbb{Z}[t, x]$ be a polynomial irreducible over $\mathbb{Q}$, of degree m in t and $n \geqslant 2$ in x, and let $H \geqslant \max\{20, H(F)\}$. If*

$$T \geqslant \max\{\exp(2(6m)^5), \exp(36^6)\},$$

then the number of positive integers $t^* \leqslant T$ such that $F(t^*, x)$ is reducible over $\mathbb{Q}$ does not exceed

$$T^{8/9} \exp\big(50(\log H)^{5/6} + 1250m^4 \log(m+1) + 5(m+1)^2 n + 5n(\log H)^{2/5}\big).$$

Proof. Retaining the notation used in Lemma 2, we let $S(T)$ be the number of positive integers $t^* \leqslant T$ such that $a_0(t^*)D(t^*) \neq 0$ and $F(t^*, x)$ is reducible over $\mathbb{Q}$.

Let ω be a nonempty subset of $\{1, \ldots, n\}$, of cardinality $k \leqslant n/2$. We contend that at least one of the polynomials $P_{\omega,j}(t, y)$, $j \leqslant k$, has degree $\geqslant 2$ in y. If not then, by definition of the $P_{\omega,j}$'s, all the symmetric functions $\tau_j(x_i : i \in \omega)$ would lie in $\mathbb{Q}(t)$, whence $F(t, x)$ would have a factor in $\mathbb{Q}(t)[x]$ of positive degree $k < n$, contrary to the assumptions. Pick for each ω one such polynomial and denote it by $P_\omega(t, y)$. Then P_ω is a polynomial with rational integral coefficients, irreducible over $\mathbb{Q}$, monic and of degree $\geqslant 2$ in y. Moreover, if t^* is such that $a_0(t^*)D(t^*) \neq 0$ and $F(t^*, x)$ is reducible over $\mathbb{Q}$, then, by Lemma 2, some polynomial $P_\omega(t^*, y)$ has an integral zero. So

$$S(T) \leqslant \sum_{\#\omega \leqslant n/2} S_\omega(T), \tag{7}$$

where $S_\omega(T)$ is the number of positive integers $t^* \leqslant T$ such that $P_\omega(t^*, y)$ has an integral zero and $a_0(t^*)D(t^*) \neq 0$.

Letting $d_\omega = \deg_y P_\omega$, $D_\omega = \deg P_\omega$, we have, by Lemma 3,

$$2 \leqslant d_\omega \leqslant \binom{n}{k}, \quad D_\omega \leqslant m d_\omega. \tag{8}$$

To estimate $S_\omega(T)$ we shall use Lemma 1 and distinguish three cases, putting, for simplicity of notation, $L_1 = \log H$, $L_2 = \log\log H$.

Case 1. $d_\omega \geqslant 3$ and $D_\omega \geqslant \big[\max\{3m, (L_1/L_2)^{1/5}\}\big] + 1$. In this case, if $P_\omega(t^*, y^*) = 0$, where $|t^*| \leqslant T$, then, by (6),

$$\max\{|t^*|, |y^*|\} \leqslant 2^{n/2}\sqrt{n+1}(m+1)HT^m \leqslant 2^n(m+1)HT^m,$$

so we may apply Lemma 1 with

$$N = 2^n(m+1)HT^m, \quad \delta = \big[\max\{3m, (L_1/L_2)^{1/5}\}\big]$$

and obtain

$$\begin{aligned} S_\omega(T) &< \big(2^n(m+1)T^m\big)^{8/(3(3m+3))} H^{(8/3)(L_2/L_1)^{1/5}} (3D_\omega\Delta)^{\Delta+4} \\ &\leqslant T^{8/9} \exp\bigg(\frac{8}{3}(L_1)^{4/5}(L_2)^{1/5} + \frac{8n\log 2}{3(3m+3)} \\ &\qquad + \frac{8\log(m+1)}{9(m+1)} + (\Delta+4)\log(3D_\omega\Delta)\bigg). \end{aligned}$$

To estimate the expression

$$\mathcal{E} = \frac{8\log(m+1)}{9(m+1)} + (\Delta+4)\log(3\Delta_\omega\Delta) \leqslant \frac{8}{9e} + (\Delta+4)\log(3\Delta_\omega\Delta)$$

we distinguish two cases, according as $3m \geqslant (L_1/L_2)^{1/5}$ or not. In the first case a calculation shows that $\mathcal{E} \leqslant 26(m+1)^2\log(m+1) + 4(m+1)^2 n$. In the other case we use the crude bound $\Delta + 5 \leqslant 2(L_1/L_2)^{2/5}$ and obtain

$$\mathcal{E} \leqslant L_1^{2/5} L_2^{3/5} + 4n(L_1/L_2)^{2/5}.$$

Adding the bounds obtained we finally have

$$\begin{aligned} S_\omega(T) &< T^{8/9} \exp\big(4L_1^{4/5}L_2^{1/5} + 5n(L_1/L_2)^{2/5}\big) \\ &\qquad \times \exp\big(26(m+1)^2\log(m+1) + 4(m+1)^2 n\big). \end{aligned}$$

Case 2. $3 \leqslant d_\omega \leqslant D_\omega < \big[\max\{3m, (L_1/L_2)^{1/5}\}\big] + 1$. In this case we take

$$E = \big[\max\{3m, (L_1/L_2)^{1/5}\}\big] + 2$$

and apply Lemma 1 to the polynomial $P_\omega(t, t^E + y)$. Now, for every zero (t^*, y^*) with $|t^*| \leqslant T$ we have, again by (6), $|y^*| \leqslant T^E + 2^n(m+1)HT^m < (m+1)2^n HT^E$, so we may take $N = (m+1)2^n HT^E$ and $\delta = d_\omega E - 1$ (note that the polynomial $P_\omega(t, t^E + y)$ is of exact degree $d_\omega E$).

We readily see that $\Delta + 4 \leqslant E^4/2$. Distinguishing again whether $3m > (L_1/L_2)^{1/5}$ or not, and adding the bounds obtained for $\log((3D_\omega\Delta)^{\Delta+4})$ in these cases, we obtain

$$S_\omega(T) < T^{8/9} \exp\bigg(25(L_1)^{4/5}(L_2)^{1/5} + 1250m^4\log(m+1) + \frac{8n\log 2}{9(m+1)}\bigg).$$

Case 3. $d_\omega = 2$. In this case, by Lemma 3, $D_\omega \leqslant 2m$. We take

$$E = \big[\max\big\{3m, \tfrac{1}{2}L_1^{1/6}\big\}\big]$$

and apply Theorem 5 of [1] to the polynomial $P_\omega(t, t^E + y)$, assumed irreducible over $\mathbb{C}$ (if it is reducible over $\mathbb{C}$ the opening argument in the proof of Lemma 1 applies). As in Case 2 we may take $N = (m+1)2^n HT^E > T^E + (m+1)2^n HT^m$ (note that the degree of $P_\omega(t, t^E + y)$ is $2E$).

Observe that the condition $N > \exp(2^6 E^6)$ (an assumption of the theorem in question) is equivalent to

$$(m+1)2^n H T^E > \exp\bigl(\max\{(6m)^6, \log H\}\bigr)$$

and is satisfied provided $T \geqslant \exp(2(6m)^5)$, as we are assuming.

The mentioned theorem gives

$$S_\omega(T) < N^{1/(2E)} \exp\bigl(12\sqrt{2E \log N \log\log N}\bigr).$$

Now $2E \leqslant (\log N)^{1/6}$, and $\log\log N \leqslant (\log N)^{1/6}$, since $\log N \geqslant \log T \geqslant 36^6$ by assumption. Hence

$$\begin{aligned} S_\omega(T) &< \exp\left(\frac{\log N}{2E}\left(1 + 12(2E)^{3/2}\sqrt{\frac{\log\log N}{\log N}}\right)\right) \\ &\leqslant \exp\left(\frac{\log N}{2E}\left(1 + 12\Bigl(\frac{1}{\log N}\Bigr)^{1/6}\right)\right) \\ &\leqslant \exp\left(\frac{2\log N}{3E}\right) \leqslant T^{2/3} \exp\left(2L_1^{5/6} + \frac{2n\log 2}{9m}\right). \end{aligned}$$

Observe now that since $H > 20$ we have

$$L_1^{4/5} L_2^{1/5} < 2L_1^{5/6}.$$

Using this inequality in the first two cases, comparing the three estimates and summing over ω, an operation which at most multiplies the bound by 2^n, we obtain

$$S(T) \leqslant T^{8/9} \exp\bigl(50L_1^{5/6} + 250m^4 \log(m+1) + 4(m+1)^2 n + 5nL_1^{2/5}\bigr).$$

We have still to take into account the solutions of $a_0(t^*)D(t^*) = 0$, but these are at most $2m(n+1) < \exp((m+1)^2 n)$ in number. This concludes the proof. □

Proof of Theorem. Let m, n, H be as in the statement of the Theorem, and let T satisfy the lower bound in the statement of Lemma 4. Then the total number $\mathcal{R}$ of positive integers $t^* \leqslant T$ such that at least one of the polynomials $F_i(t^*, x)$ is reducible over $\mathbb{Q}$ satisfies

$$\mathcal{R} \leqslant hT^{8/9} \exp\bigl(50(\log H)^{5/6} + 250m^4 \log(m+1) + 5(m+1)^2 n + 5n(\log H)^{2/5}\bigr).$$

To find a suitable value of $t^* \leqslant T$ it thus suffices that this quantity is less than T, which holds if

$$T > h^9 \exp\bigl(450(\log H)^{5/6} + 2250m^5 + 45(m+1)^2 n + 45n(\log H)^{2/5}\bigr).$$

Combining this with the lower bound necessary for an application of Lemma 4, we obtain the Theorem. □

Remark. It is obviously possible by changing the splitting into cases to obtain a corresponding theorem, with different numerical values for the coefficients appearing in the final estimate.

References

[1] E. Bombieri, J. Pila, *The number of integral points on arcs and ovals*. Duke Math. J. 59 (1989), 337–357.

[2] S. D. Cohen, *The distribution of Galois groups and Hilbert's irreducibility theorem*. Proc. London Math. Soc. (3) 43 (1981), 227–250.

[3] P. Dèbes, *Parties hilbertiennes et progressions géométriques*. C. R. Acad. Sci. Paris Sér. I Math. 302 (1986), 87–90.

[4] —, *Hilbert subsets and S-integral points*. Manuscripta Math. 89 (1996), 107–137.

[5] K. Dörge, *Einfacher Beweis des Hilbertschen Irreduzibilitätssatzes*. Math. Ann. 96 (1927), 176–182.

[6] M. Eichler, *Zum Hilbertschen Irreduzibilitätssatz*. Math. Ann. 116 (1939), 742–748.

[7] E. Fogels, *On the abstract theory of primes* III. Acta Arith. 11 (1966), 293–331.

[8] M. Fried, *On Hilbert's irreducibility theorem*. J. Number Theory 6 (1974), 211–231.

[9] H. Hasse, *Number Theory*. Springer, Berlin 1980.

[10] D. Hilbert, *Über die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten*. J. Reine Angew. Math. 110 (1892), 104–129; Ges. Abhandlungen II, Springer, Berlin 1970, 264–286.

[11] E. Inaba, *Über den Hilbertschen Irreduzibilitätssatz*. Jap. J. Math. 19 (1944), 1–25.

[12] E. Landau, *Sur quelques théorèmes de M. Petrovitch relatifs aux zéros des fonctions analytiques*. Bull. Soc. Math. France 33 (1905), 1–11.

[13] F. Mertens, *Über die Zerfällung einer ganzen Funktion einer Veränderlichen in zwei Faktoren*. Sitzungsber. K. Akad. Wiss. Wien 120 (1911), Math. Naturwiss. Cl., 1485–1502.

[14] P. Roquette, *Nonstandard aspects of Hilbert's Irreducibility Theorem*. In: Model Theory and Algebra (A memorial tribute to Abraham Robinson), Lecture Notes in Math. 498, Springer, Berlin 1975, 231–275.

[15] A. Schinzel, *Selected Topics on Polynomials*. University of Michigan Press, Ann Arbor 1982.

[16] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*. Abh. Preuss. Akad. Wiss. Phys.-Math. Kl. Nr. 1 (1929); Ges. Abhandlungen I, Springer, Berlin 1966, 209–266.

[17] Th. Skolem, *Untersuchungen über die möglichen Verteilungen ganzzahliger Lösungen gewisser Gleichungen*. Kristiania Vid. Selskab. Skrifter I (1921), No. 17.

[18] V. G. Sprindzhuk, *Diophantine equations with prime unknowns*. Trudy Mat. Inst. Steklov. 158 (1981), 180–196 (Russian).

[19] M. Yasumoto, *Algebraic extensions of nonstandard models and Hilbert's irreducibility theorem*. J. Symbolic Logic 53 (1988), 470–480.

Heritage of European Mathematics

Andrzej Schinzel in 2007

Andrzej Schinzel

Selecta

Volume II

Elementary, Analytic and Geometric Number Theory

Edited by
Henryk Iwaniec
Władysław Narkiewicz
Jerzy Urbanowicz

European Mathematical Society

Author:

Andrzej Schinzel
Institute of Mathematics
Polish Academy of Sciences
ul. Śniadeckich 8, skr. poczt. 21
00-956 Warszawa 10
Poland

Editors:

Henryk Iwaniec
Department of Mathematics
Rutgers University
New Brunswick, NJ 08903
U.S.A.
iwaniec@math.rutgers.edu

Władysław Narkiewicz
Institute of Mathematics
University of Wrocław
pl. Grunwaldzki 2/4
50-384 Wrocław
Poland
narkiew@math.uni.wroc.pl

Jerzy Urbanowicz
Institute of Mathematics
Polish Academy of Sciences
ul. Śniadeckich 8, skr. poczt. 21
00-956 Warszawa 10
Poland
urbanowi@impan.gov.pl

2000 Mathematics Subject Classification: 11, 12

ISBN 978-3-03719-038-8 (Set Vol I & Vol II)

The Swiss National Library lists this publication in The Swiss Book, the Swiss national bibliography, and the detailed bibliographic data are available on the Internet at http://www.helveticat.ch.

Contact address:

European Mathematical Society Publishing House
Seminar for Applied Mathematics
ETH-Zentrum FLI C4
CH-8092 Zürich
Switzerland

Phone: +41 (0)44 632 34 36
Email: info@ems-ph.org
Homepage: www.ems-ph.org

Printed in Germany

9 8 7 6 5 4 3 2 1

Contents

Volume 2

Volume 1

Part G

Arithmetic functions

Commentary on G: Arithmetic functions

by Kevin Ford

Schinzel spent much of the early years of his career studying Euler's totient function $\varphi(n)$ and the sum of divisors function $\sigma(n)$. His teacher Wacław Sierpiński and Pál Erdős corresponded about numerous problems concerning φ and σ, and Sierpiński encouraged Schinzel to work on some of these. Papers **G1–G6** showcase Schinzel's considerable skill with elementary methods.

G1, **G4**. **Arithmetic functions at consecutive integers**

Somayajulu [27] proved in 1950 that the ratio $\varphi(n+1)/\varphi(n)$ takes arbitrarily large and arbitrarily small values. In a series of four papers ([20], [21], [23], **G1**), Schinzel improved and generalized this result, finally proving in **G1** for any positive integer h that the vectors $(g(n+1)/g(n), \dots, g(n+h)/g(n+h-1))$ are dense in $[0,\infty)^h$, where $g=\varphi$ or $g=\sigma$.

A few years later, he teamed with Erdős in **G4** to study analogous problems for a wide class of multiplicative functions. For a positive multiplicative function $g(n)$, $f(n)=\log g(n)$ is additive, and the authors chose to state their results in terms of additive functions. To obtain results about φ and σ, one applies these theorems with $f(n)=\log(n/\varphi(n))$ and with $f(n)=\log(\sigma(n)/n)$. There is a vast literature on the distribution of additive functions, and paper **G4** is a major contribution to the topic. Erdős and Schinzel give necessary and sufficient conditions on f so that for any $h\geqslant 1$, there is a c_h so that for any $a_1,\dots,a_h\geqslant c_h$ and $\varepsilon>0$, there are $\gg x$ integers $n\leqslant x$ satisfying $|f(n+i)-a_i|<\varepsilon$ $(1\leqslant i\leqslant h)$ (Theorem 2 and discussion at the end of §1). They also give sufficient (and conjecturally necessary) conditions on f in order to conclude that for any real $a_1,\dots,a_h$ and $\varepsilon>0$, there are $\gg x$ integers $n\leqslant x$ with $|f(n+i)-f(n+i-1)-a_i|<\varepsilon$ $(1\leqslant i\leqslant h)$ (Theorem 1 and discussion at the end of §1). Finally, they give very general conditions under which $(f(n+1),\dots,f(n+h))$ and $(f(n+1)-f(n),\dots,f(n+h)-f(n+h-1))$ have continuous distribution functions (Theorems 3 and 4). There is no claim that these conditions are necessary, but likely they cannot be relaxed too much. Condition 1 of Theorem 1 is closely related to the classical Kolmogorov three series theorem of probability theory ([1]).

([1]) The editors thank Kevin Ford for correcting a serious mistake in the proof of Lemma and an inaccuracy in the proof of Theorem 1 in **G4**. The corrections have been incorporated in the text.

Although the results of **G4** are "best possible" (or nearly so), the theorems in **G1** may be extended in other directions. For example, Erdős in [8] determined the maximum rate of growth of $h(n)$ in order to have

$$\liminf_{n\to\infty} \max_{1\leqslant i\leqslant h(n)} \varphi(n+i)/\min_{1\leqslant i\leqslant h(n)} \varphi(n+i) = 1.$$

The answer (Theorems 1, 2 of [8]) involves the 6th iterate of the logarithm! In another direction, Alkan, Ford and Zaharescu [2] have proven, for a wide class of multiplicative functions g including φ and σ, that for every $h \geqslant 1$ there is a $C_h > 0$ so that for any positive $a_1, \ldots, a_h$ there are infinitely many n so that

$$|g(n+i)/g(n+i-1) - a_i| < n^{-C_h} \qquad (1 \leqslant i \leqslant h).$$

G2, **G3**, parts of **J1**, **J2**. **Multiplicity problems**

Let $A(m)$ be the number of solutions x of $\varphi(x) = m$, and let $B(m)$ be the number of solutions of $\sigma(x) = m$. The famous Carmichael Conjecture ([4], [5]) states that $A(m) \neq 1$ for all m. Around 1955, Sierpiński made related conjectures that for all $k \geqslant 0$, there are infinitely many m with $B(m) = k$ and for all $k \geqslant 0$, $k \neq 1$, $A(m) = k$ for infinitely many m. Sierpiński in 1956 gave an infinite sequence of numbers m with $A(m) = 2$ and in **G2**, Schinzel gives explicit infinite sequences of numbers m with $A(m) = 3$. Schinzel also provides explicit infinite sequences of m for which (i) $A(m) = 0$ (in **G2**) and (ii) $A(m)$ is unbounded (in **G3**). In fact, in **G2** Schinzel gives a construction, for any positive integer n, of an infinite sequence of integers k with (iii) $A(kn) = 0$. The existence of sequences satisfying (i), (ii) or (iii) (without giving them explicitly) had earlier been proved by Pillai [18] in 1929, as a corollary of his bound $V(x) \ll x/(\log x)^{(\log 2)/e}$, where $V(x)$ is the number of $m \leqslant x$ with $A(m) > 0$. A couple of years later, Erdős [8] showed with sieve methods that if there is one integer m with $A(m) = k$, then there are infinitely many such integers (the same method works also for $B(m)$). Later, in **J2**, Schinzel deduced both conjectures of Sierpiński (labelled C_{14} and C_{15} in **J2**) from his Hypothesis H, using a clever construction requiring the values of certain polynomials to be simultaneously prime for some argument n.

There has been much activity on these problems since Schinzel's papers. The Sierpiński conjectures for $A(m)$ and $B(m)$ have now been proved (in [12] and [14], respectively). Carmichael's conjecture remains open, but any counterexample m must exceed $10^{10^{10}}$ and a single counterexample implies that a positive proportion of all m with $A(m) > 0$ are counterexamples [11]. Estimates for $V(x)$ have been progressively refined by Erdős [6], Erdős and Hall, Pomerance, Maier and Pomerance, and Ford [11] (see [11] for more on the history of the problem and further references). Combining the results of [11], [12] and [14], it is now known that for any $k \geqslant 2$, a positive proportion of numbers with $A(m) > 0$ have $A(m) = k$ and for every $k \geqslant 1$, a positive proportion of numbers with $B(m) > 0$ have $B(m) = k$. Erdős in [6] showed that for some $c > 0$ there are infinitely many m with $A(m) > m^c$. This was proved for any $c < 3 - 2\sqrt{2}$ by Wooldridge in 1979, and larger c values were obtained successively by Pomerance, Balog, Fouvry and Grupp, and Friedlander. The current record is $c = 0.7039$, due to Baker and Harman [3]. The best value of c is closely tied to the problem of finding primes p for which $p - 1$ is composed only of small prime factors (see [3] and the references therein). Trivial modifications of

the analysis yield infinitely many m with $B(m) > m^c$ with the same value of c. Erdős' conjecture that one may take any $c < 1$ remains open.

G5. Compositions of φ and σ

Mąkowski and Schinzel examined in **G5** the lim sup and lim inf of the functions $\varphi(\varphi(n))/n$, $\varphi(\sigma(n))/n$, $\sigma(\varphi(n))/n$ and $\sigma(\sigma(n))/n$. Alaoglu and Erdős [1] had earlier shown that $\liminf \varphi(\sigma(n))/n = 0$ and that $\limsup \sigma(\varphi(n)) = \infty$. Five of the six remaining cases are resolved in **G5**. The proofs use a combination of elementary methods and a result of Rényi that implies that for some $c > 0$ and infinitely many primes p, $p - 1$ has no prime factor $> p^c$. They could not determine $\liminf \sigma(\varphi(n))/n$, but showed that

$$\liminf \sigma(\varphi(n))/n \leqslant \frac{1}{2} + \frac{1}{2^{34} - 4}$$

and conjectured, but could not prove, that the left side is > 0. This last assertion was proved by Pomerance [19] in 1989 using sieve methods. The authors in **G5** also pose a problem **P486**: *Is the inequality*

$$\sigma(\varphi(n))/n \geqslant \frac{1}{2} \tag{1}$$

true for all n ? This remains open, the best result to date being $\sigma(\varphi(n))/n \geqslant \frac{1}{39.4}$ and due to Ford [13]. Inequality (1) has been verified for integers of certain types, and Luca and Pomerance [17] showed that (1) holds for a set of integers of asymptotic density 1.

G6. Integers of the form $n - \varphi(n)$

Sierpiński conjectured [26] that there are infinitely many integers which are not of the form $n - \varphi(n)$. Erdős in [9] settled the analogous conjecture for numbers of the form $\sigma(n) - n$, but it was not until 1995 that Sierpiński's conjecture was proved by Browkin and Schinzel in **G6**. The proof uses the fact that there are integers n such that $n2^k - 1$ is composite for all natural numbers k. This fact is proved using covering congruences, a method introduced by Erdős [7]. The smallest known value of n is 509203 and was discovered by H. Riesel in 1956. This may be the smallest n with this property, but a few smaller candidates have not been eliminated yet. In **G6**, Browkin and Schinzel show that none of the numbers $509203 \cdot 2^k$ are of the form $n - \varphi(n)$. Computer calculations are needed for the case $k = 1$, and then the proof proceeds by induction on k. Building upon these ideas, Flammenkamp and Luca [10] have discovered similar families of numbers not of the form $n - \varphi(n)$. Based on computations performed by D. H. Lehmer and A. Odlyzko, Browkin and Schinzel conjecture that a positive proportion of numbers are not of the form $n - \varphi(n)$, and this remains an open problem.

Other problems

For every $k \geqslant 1$, it is unknown if the equation

$$\varphi(n) = \varphi(n + k) \tag{2}$$

has infinitely many solutions n. Sierpiński [25] showed that for each k there is at least one solution of (2), and by the work of Schinzel [22] and Schinzel and Wakulicz [24], we know that there are at least two solutions for each $k \leqslant 2 \cdot 10^{58}$. When k is even, Schinzel and

Sierpiński deduced from Hypothesis H (**J1**, Conjecture $C_{2,1,2}$) that (2) has infinitely many solutions. For discussions about the distribution of solutions of (2), see the paper of Graham, Holt and Pomerance [15] and the references therein. In particular, it is conjectured that most solutions of (2) when $2 \mid k$ are generated by certain pairs of generalized twin primes ([15], Theorems 1 and 2). Solutions when $k \equiv 3 \pmod 6$ are particularly rare.

The infinitude of solutions of the equation $\sigma(m) = \varphi(n)$ is also unknown, although it follows easily if there are infinitely many twin primes or infinitely many Mersenne primes (it also follows from the Extended Riemann Hypothesis for Dirichlet L-functions by unpublished work of Pomerance). Schinzel and Sierpiński deduce from Hypothesis H (**J1**, C_8) a stronger result: for every k, there are integers m for which simultaneously $A(m) \geqslant k$ and $B(m) \geqslant k$.

More information about the arithmetic function problems investigated in **G1**–**G6**, **J1** and **J2**, including additional references to related work, may be found in Richard Guy's book [16], especially sections B13, B36, B38, B39, B41 and B42.

References

[1] L. Alaoglu, P. Erdős, *A conjecture in elementary number theory*. Bull. Amer. Math. Soc. 50 (1944), 881–882.

[2] E. Alkan, K. Ford, A. Zaharescu, *Diophantine approximation with arithmetic functions*. Preprint.

[3] R. C. Baker, G. Harman, *Shifted primes without large prime factors*. Acta Arith. 83 (1998), 331–361.

[4] R. D. Carmichael, *On Euler's ϕ-function*. Bull. Amer. Math. Soc. 13 (1907), 241–243.

[5] —, *Note on Euler's φ-function*. Bull. Amer. Math. Soc. 28 (1922), 109–110.

[6] P. Erdős, *On the normal number of prime factors of $p-1$ and some related problems concerning Euler's ϕ-function*. Quart. J. Math. Oxford Ser. 6 (1935), 205–213.

[7] —, *On integers of the form $2^k + p$ and some related problems*. Summa Brasil. Math. 2 (1950), 113–123.

[8] —, *Some remarks on Euler's φ-function*. Acta Arith. 4 (1958), 10–19.

[9] —, *Über die Zahlen der Form $\sigma(n) - n$ und $n - \varphi(n)$*. Elem. Math. 28 (1973), 83–86.

[10] A. Flammenkamp, F. Luca, *Infinite families of noncototients*. Colloq. Math. 86 (2000), 37–41.

[11] K. Ford, *The distribution of totients*. The Ramanujan J. 2 (1998), 67–151.

[12] —, *The number of solutions of $\phi(x) = m$*. Ann. of Math. (2) 150 (1999), 283–311.

[13] —, *An explicit sieve bound and small values of $\sigma(\phi(m))$*. Period. Math. Hungar. 43 (2001), 15–29.

[14] K. Ford, S. Konyagin, *On two conjectures of Sierpiński concerning the arithmetic functions σ and ϕ*. In: Number Theory in Progress, Vol. 2 (Zakopane–Kościelisko, 1997), de Gruyter, Berlin 1999, 795–803.

[15] S. W. Graham, J. J. Holt, C. Pomerance, *On the solutions to $\phi(n) = \phi(n+k)$*. In: Number Theory in Progress, Vol. 2 (Zakopane–Kościelisko, 1997), de Gruyter, Berlin 1999, 867–882.

[16] R. K. Guy, *Unsolved Problems in Number Theory*, third edition. Problem Books in Math., Springer, New York 2004.

[17] F. Luca, C. Pomerance, *On some problems of Mąkowski–Schinzel and Erdős concerning the arithmetical functions ϕ and σ*. Colloq. Math. 92 (2002), 111–130.

[18] S. S. Pillai, *On some functions connected with $\phi(n)$*. Bull. Amer. Math. Soc. 35 (1929), 832–836.

[19] C. Pomerance, *On the composition of the arithmetic functions σ and φ*. Colloq. Math. 58 (1989), 11–15.

[20] A. Schinzel, *Quelques théorèmes sur les fonctions $\varphi(n)$ et $\sigma(n)$*. Bull. Acad. Polon. Sci. Cl. III 2 (1954), 467–469.

[21] —, *Generalization of a theorem of B. S. K. R. Somayajulu on the Euler's function $\varphi(n)$*. Ganita 5 (1954), 123–128.

[22] —, *Sur l'équation $\varphi(x + k) = \varphi(x)$*. Acta Arith. 4 (1958), 181–184.

[23] A. Schinzel, W. Sierpiński, *Sur quelques propriétés des fonctions $\varphi(n)$ et $\sigma(n)$*. Bull. Acad. Polon. Sci. Cl. III 2 (1954), 463–466.

[24] A. Schinzel, A. Wakulicz, *Sur l'équation $\varphi(x + k) = \varphi(x)$*, II. Acta Arith. 5 (1959), 425–426.

[25] W. Sierpiński, *Sur une propriété de la fonction $\phi(n)$*. Publ. Math. Debrecen 4 (1956), 184–185.

[26] —, *Teoria liczb*, część 2 (*Number Theory*, Part II). Monografie Matematyczne 38, PWN, Warszawa 1959 (Polish).

[27] B. S. K. R. Somayajulu, *The Euler's totient function $\varphi(n)$*. Math. Student 18 (1950), 31–32.

Originally published in
Bulletin de l'Académie Polonaise des Sciences
Cl. III 3 (1955), 415–419

On functions $\varphi(n)$ and $\sigma(n)$

The object of the present note is to prove the following two theorems:

Theorem 1. *For every finite sequence of positive numbers $a_1, a_2, \dots, a_k$ there exists an increasing infinite sequence of natural numbers $n_1, n_2, \dots$ such that*

$$\lim_{k\to\infty} \frac{\varphi(n_k+i)}{\varphi(n_k+i-1)} = a_i \quad \text{for} \quad i = 1, 2, \dots, h.$$

Theorem 2 *is obtained from Theorem* 1 *by replacing the letter φ by σ.*

Lemma 1. *Let u_n $(n = 1, 2, \dots)$ denote an infinite sequence of real numbers such that*

$$\lim_{n\to\infty} u_n = +\infty, \quad \lim_{n\to\infty} \frac{u_{n+1}}{u_n} = 1.$$

Then, for every real number $C > 1$ and for every increasing infinite sequence of natural numbers n_k, there exists an infinite sequence of natural numbers l_k such that

$$\lim_{k\to\infty} \frac{u_{l_k}}{u_{n_k}} = C.$$

Proof. Let n_k $(k = 1, 2, \dots)$ denote a given increasing infinite sequence of natural numbers. For every natural number k let us denote by l_k the least natural number for which

$$\frac{u_{l_k}}{u_{n_k}} > C;$$

such a number exists, since

$$\lim_{l\to\infty} u_l = +\infty.$$

Thus we have

$$\frac{u_{l_k}}{u_{n_k}} > C \geqslant \frac{u_{l_k-1}}{u_{n_k}},$$

whence

$$1 > C : \frac{u_{l_k}}{u_{n_k}} \geqslant \frac{u_{l_k-1}}{u_{l_k}}$$

Presented by W. Sierpiński on June 21, 1955

and, in view of

$$\lim_{k\to\infty}\frac{u_{l_k-1}}{u_{l_k}}=1,$$
$$\lim_{k\to\infty}\frac{u_{l_k}}{u_{n_k}}=C. \qquad \square$$

Lemma 2. *If g is a natural number, and $A_0, A_1, \ldots, A_g$ are natural numbers >1 relatively prime in pairs, then there exists a natural number m such that, for $i=0,1,\ldots,g$,*

$$A_i \mid m+i, \quad \left(A_i, \frac{m+i}{A_i}\right)=1, \quad (A_0A_1\cdots A_g)^2 > m+i.$$

Proof. In virtue of so-called Chinese remainder theorem there exists a natural number m_1 such that

$$m_1+i \equiv A_i \pmod{A_i^2} \quad \text{for} \quad i=0,1,\ldots,g.$$

Let $m = m_1 - A_0^2A_1^2\cdots A_g^2\left[\frac{m_1+g}{A_0^2A_1^2\cdots A_g^2}\right]$. We shall have $A_i \mid m+i$ and $\left(A_i, \frac{m+i}{A_i}\right)=1$, since

$$A_i \mid m_1+i, \quad \frac{m+i}{A_i} \equiv \frac{m_1+i}{A_i} \equiv 1 \pmod{A_i} \quad \text{for} \quad i=0,1,\ldots,g.$$

We shall also have $-g \leqslant m < (A_0A_1\cdots A_g)^2 - g$.

If we had $m \leqslant 0$, we should have for $i=-m$, $0 \leqslant i \leqslant g$ and $A_i^2 \mid m+i$, which is impossible, since $A_i > 1$. Thus m is an integer such that for $i=0,1,\ldots,g$

$$(A_0A_1\cdots A_g)^2 > m+i > 0. \qquad \square$$

Lemma 3a. *For every finite sequence of real numbers, $b_1, b_2, \ldots, b_g$, satisfying the inequality*

$$\frac{\varphi(i)}{i} > b_i > 0 \quad \textit{for} \quad i=1,2,\ldots,g,$$

there exists a sequence m_k such that

$$\lim_{k\to\infty}\frac{\varphi(m_k+i)}{m_k+i}=b_i, \quad i=1,2,\ldots,g.$$

Proof. Assume in Lemma 1 that

$$u_n=\prod_{i=1}^{n}\left(\frac{1}{1-1/p_i}\right)$$

(where p_i is the i-th prime number) and that

$$C_i=\frac{1}{b_i}\,\frac{\varphi(i)}{i},$$

and for $k \geqslant g$, $i=1,2,\ldots,g$, let

$$A_{0,k}=g!\,p_1\cdot p_2\cdots p_k, \quad A_{i,k}=p_{l_{i-1,k}+1}\cdots p_{l_{i,k}},$$

where $l_{0,k} = k$ and $l_{i,k}$ is the number l_k from Lemma 1 suitably chosen for the number C_i and the sequence $l_{i-1,k}$.

In virtue of Lemma 2 there exists a number m_k such that

$$A_{i,k} \mid m_k + i, \quad \left(\frac{m_k + i}{A_{i,k}}, A_{i,k}\right) = 1, \quad (A_{0,k} A_{1,k} \cdots A_{g,k})^2 > m_k + i > 0$$

for $i = 0, 1, \ldots, g$.

Moreover, for $i, j > 0$

$$(A_{0,k}, m_k + i) = (A_{0,k}, i) = i \tag{1}$$

$$\left(p_1 p_2 \cdots p_k, \frac{m_k + i}{i}\right) \Big| \left(\frac{A_{0,k}}{i}, \frac{m_k + i}{i}\right) = 1 \tag{2}$$

$$(A_{j,k}, m_k + i) = (A_{j,k}, i - j) = 1 \tag{3}$$

for $i \neq j$, because $k \geqslant g$.

Accordingly, for $i = 1, 2, \ldots, g$,

$$m_k + i = i A_{i,k} q_{i,1}^{\alpha_{i,1}} q_{i,2}^{\alpha_{i,2}} \cdots q_{i,s_i}^{\alpha_{i,s_i}},$$

where

$$p_{l_{g,k}} < q_{i,1} < q_{i,2} < \ldots < q_{i,s_i}$$

are prime numbers and, of course, $s_i < 2l_{g,k}$. Hence,

$$\frac{\varphi(i)}{i} \cdot \frac{\varphi(A_{i,k})}{A_{i,k}} > \frac{\varphi(m_k + i)}{m_k + i} = \frac{\varphi(i)}{i} \cdot \frac{\varphi(A_{i,k})}{A_{i,k}} \prod_{j=1}^{s_i} \left(1 - \frac{1}{q_{i,j}}\right)$$

$$> \frac{\varphi(i)}{i} \cdot \frac{\varphi(A_{i,k})}{A_{i,k}} \cdot \prod_{j=1}^{s_1} \left(1 - \frac{1}{p_{l_{g,k}} + j}\right) > \frac{\varphi(i)}{i} \cdot \frac{\varphi(A_{i,k})}{A_{i,k}} \cdot \frac{p_{l_{g,k}}}{p_{l_{g,k}} + 2l_{g,k}}$$

and, in virtue of the formulas

$$\lim_{k \to \infty} \frac{u_{l_{i-1,k}}}{u_{l_{i,k}}} = b_i \cdot \frac{i}{\varphi(i)}, \quad \lim_{k \to \infty} \frac{p_{l_{g,k}}}{p_{l_{g,k}} + 2l_{g,k}} = 1,$$

we have

$$\lim_{k \to \infty} \frac{\varphi(m_k + i)}{m_k + i} = b_i. \qquad \square$$

Lemma 3b. *For every finite sequence of real numbers, $b_1, b_2, \ldots, b_g$, satisfying the inequality*

$$b_i > \frac{\sigma(i)}{i} \quad \textit{for} \quad i = 1, 2, \ldots, g,$$

there exists a sequence m_k such that

$$\lim_{k \to \infty} \frac{\sigma(m_k + i)}{m_k + i} = b_i, \quad i = 1, 2, \ldots, g.$$

Proof. Assume in Lemma 1 that

$$u_n = \prod_{i=1}^{n}\Big(1+\frac{1}{p_i}\Big)$$

(where p_i is the i-th prime number) and that $C_i = b_i \cdot i/\sigma(i)$, and, for $k \geqslant g$, $i = 1, 2, \ldots, g$, let

$$A_{0,k} = g!\, p_1 \cdot p_2 \cdots p_k, \quad A_{i,k} = p_{l_{i-1,k}+1} \cdots p_{l_{i,k}},$$

where $l_{i,k}$ are the numbers from Lemma 1 (on the whole different from those in Lemma 3a).

Analogously to the proof of Lemma 3a, we prove the existence of a number m_k such that, for $i = 1, 2, \ldots, g$,

$$m_k + i = i A_{i,k} q_{i,1}^{\alpha_{i,1}} q_{i,2}^{\alpha_{i,2}} \cdots q_{i,s_i}^{\alpha_{i,s_i}},$$

where

$$p_{l_{g,k}} < q_{i,1} < q_{i,2} < \ldots < q_{i,s_i}$$

are prime numbers (on the whole different from those in Lemma 3a) and $s_i < 2l_{g,k}$. Hence,

$$\frac{\sigma(i)}{i}\cdot\frac{\sigma(A_{i,k})}{A_{i,k}} < \frac{\sigma(m_k+i)}{m_k+i} < \frac{\sigma(i)}{i}\cdot\frac{\sigma(A_{i,k})}{A_{i,k}}\prod_{j=1}^{s_i}\Big(\frac{q_{i,j}}{q_{i,j}-1}\Big)$$

$$< \frac{\sigma(i)}{i}\cdot\frac{\sigma(A_{i,k})}{A_{i,k}}\cdot\prod_{j=1}^{s_i}\frac{p_{l_{g,k}}+j}{p_{l_{g,k}}+j-1} < \frac{\sigma(i)}{i}\cdot\frac{\sigma(A_{i,k})}{A_{i,k}}\cdot\frac{p_{l_{g,k}}+2l_{g,k}}{p_{l_{g,k}}},$$

whence, as in Lemma 3a,

$$\lim_{k\to\infty}\frac{\sigma(m_k+i)}{m_k+i} = \frac{\sigma(i)}{i}, \quad \lim_{k\to\infty}\frac{\sigma(A_{i,k})}{A_{i,k}} = b_i. \qquad \square$$

Remark. In the case of $g = 1$ Lemmas 3a and 3b imply W. Sierpiński's theorems on the density of the sets

$$\Big\{\frac{\varphi(m)}{m}\Big\}_{m=1,2,\ldots} \text{ in } [0,1] \quad \text{and} \quad \Big\{\frac{\sigma(m)}{m}\Big\}_{m=1,2,\ldots} \text{ in } [1,\infty].$$

Proof of Theorem 1. Assume in Lemma 3a that $g = h+1$ and that $b_{1+i} = b_1 a_1 \cdots a_i$ $(i = 1, \ldots, h)$, where b_1 is so small that

$$b_{1+i} < \frac{\varphi(i+1)}{i+1} \quad \text{for} \quad i = 0, 1, \ldots, h.$$

Thus there exists a sequence n_k such that

$$\lim_{k\to\infty}\frac{\varphi(n_k+i)}{n_k+i} = b_{1+i} \quad \text{for} \quad i = 0, 1, \ldots, h.$$

Hence

$$\lim_{k\to\infty}\frac{\varphi(n_k+i)}{\varphi(n_k+i-1)} = \frac{b_{1+i}}{b_i} = a_i \quad \text{for} \quad i = 0, 1, \ldots, h. \qquad \square$$

I have been informed that the proof of this theorem, based on Brun's method, has also been given by Y. Wang; the proof has not yet appeared in print.

The proof of Theorem 2 is analogous to the preceding one but based on Lemma 3b.

Conclusions. In Theorems 1 and 2 we can, of course, take 0 or ∞ for a_i ($i = 1, 2, \ldots, h$).

Remark. Setting $h = 1$ in Theorems 1 and 2 we obtain the theorems on the density of sets

$$\left\{\frac{\varphi(n+1)}{\varphi(n)}\right\}_{n=1,2,\ldots} \quad \text{and} \quad \left\{\frac{\sigma(n+1)}{\sigma(n)}\right\}_{n=1,2,\ldots} \quad \text{in } [0,\infty] \quad [1].$$

Setting $h = 2$, $a_1 = \infty$, $a_2 = 0$; $a_1 = 0$, $a_2 = \infty$; $a_1 = \infty$, $a_2 = \infty$; $a_1 = 0$, $a_2 = 0$, we obtain a theorem from W. Sierpiński's and my note [2]; setting $a_1 = a_2 = \ldots = a_h = \infty$ and $a_1 = a_2 = \ldots = a_h = 0$, we obtain a theorem from another note of mine [3].

The case of $h = 1$, $a_1 = \infty$ and $a_1 = 0$ gives a theorem of B. S. K. R. Somayajulu [4].

References

[1] A. Schinzel, *Generalization of a theorem of B. S. K. R. Somayajulu on the Euler's function* $\varphi(n)$. Ganita 5 (1954), 123–128.

[2] A. Schinzel, W. Sierpiński, *Sur quelques propriétés des fonctions* $\varphi(n)$ *et* $\sigma(n)$. Bull. Acad. Polon. Sci. Cl. III 2 (1954), 463–466.

[3] A. Schinzel, *Quelques théorèmes sur les fonctions* $\varphi(n)$ *et* $\sigma(n)$. Bull. Acad. Polon. Sci. Cl. III 2 (1954), 467–469.

[4] B. S. K. R. Somayajulu, *The Euler's totient function* $\varphi(n)$. Math. Student 18 (1950), 31–32.

Andrzej Schinzel
Selecta

Originally published in
Elemente der Mathematik.
Revue de mathématiques élémentaires
11 (1956), 75–78

Sur l'équation $\varphi(x) = m$

L'équation $\varphi(x) = m$, où m est un nombre naturel donné et $\varphi(x)$ est la fonction connue de Euler–Gauss (qui exprime le nombre de nombres naturels $\leqslant x$ et premiers avec x) a été étudiée par plusieurs auteurs. En particulier on a examiné combien de solutions peut admettre cette équation pour m donnés.

M. M. G. Beumer a posé le problème de démontrer qu'il existe une infinité de nombres naturels pairs m pour lesquels l'équation $\varphi(x) = m$ n'a pas de solutions ([1]). M. W. Sierpiński a demontré ([2]) que tels sont par exemple les nombres $2 \cdot 5^{2n}$, où $n = 1, 2, \ldots$, et aussi les nombres $m = 2p$, où p est un nombre premier $\equiv 1 \pmod 3$, et que, dans l'état actuel de la science nous ne savons pas résoudre le problème s'il existe une infinité de nombres premiers p pour lesquels l'équation $\varphi(x) = 2p$ a des solutions.

Or, je démontrerai un théorème qui résout une généralisation du problème de M. G. Beumer.

Théorème 1. *Quel que soit le nombre naturel n, il existe une infinité de nombres naturels m qui sont des multiples de n, tels que l'équation $\varphi(x) = m$ n'a pas de solutions.*

Démonstration. Soit n un nombre naturel, $d_1, d_2, \ldots, d_s$ tous les diviseurs naturels de n. D'après le théorème connu de Lejeune–Dirichlet il existe une infinité de nombres premiers p tels que

$$p \equiv 1 \pmod{d_i + 1} \quad (i = 1, 2, \ldots, s). \tag{1}$$

Soit p un de ces nombres premiers et supposons que le nombre naturel x satisfait à l'équation $\varphi(x) = p^k n$, où k est un nombre naturel. S'il était $p \mid x$, on aurait $p - 1 \mid \varphi(x)$, d'où, d'après notre équation, $p - 1 \mid n$, ce qui est impossible, vu que d'après (1) on a $p \equiv 1 \pmod{n+1}$. On a donc $(x, p) = 1$. Soit $x = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_r^{\alpha_r}$ le développement du nombre x en facteurs premiers. On a donc

$$q_1^{\alpha_1 - 1}(q_1 - 1) q_2^{\alpha_2 - 1}(q_2 - 1) \cdots q_r^{\alpha_r - 1}(q_r - 1) = p^k n$$

et, comme $(x, p) = 1$, il existe un indice $i \leqslant r$ tel que $p \mid q_i - 1$, d'où $q_i - 1 = p^l d_j$, où $l \geqslant 1$ et d_j est un diviseur du nombre n. On a donc, d'après (1),

$$q_i = p^l d_j + 1 \equiv 1 \cdot d_j + 1 \equiv 0 \pmod{d_j + 1}$$

et, comme $q_i = p^l d_j + 1 > d_j + 1$ et q_i est un nombre premier, on aboutit à une

([1]) *Elem. Math.* 10 (1955), 22, problème 230.
([2]) Voir solution du problème 230, *Elem. Math.* 11 (1956), 37.

contradiction. k pouvant être un nombre naturel quelconque, le théorème 1 se trouve démontré. □

Si $n = 2$, $p = 7$, on a $d_1 = 1$, $d_2 = 2$, $s = 2$ et la formule (1) est vérifiée, d'où il résulte (d'après notre démonstration) que l'équation $\varphi(x) = 2 \cdot 7^k$ n'a pas de solutions pour k naturels. Or, comme on sait, pour $k = 0$ cette équation n'a que trois solutions : $x = 3$, 4 ou 6. On a ainsi ce

Corollaire 1. *L'équation* $\varphi(x) = 2 \cdot 7^k$ *a des solutions seulement si* $k = 0$ (*et alors* $x = 3$, 4 *ou* 6).

On connait l'hypothèse de R. D. Carmichael qu'il n'existe aucun nombre naturel m pour lequel l'équation $\varphi(x) = m$ aurait une et une seule solution, ce qui a été vérifié par V. L. Klee jr. pour $m \leqslant 10^{400}$ [1]. Or, M. W. Sierpiński a démontré qu'il existe une infinité de nombres naturels m pour lesquels l'équation $\varphi(x) = m$ a précisément deux solutions : tels sont par exemple les nombres $m = 2 \cdot 3^{6k+1}$ ($k = 1, 2, \dots$). Or, je démontrerai la généralisation suivante de cette proposition :

Théorème 2. *Si* p *est un nombre premier de la forme* $4t + 3$ *et si* k *est un nombre naturel, l'équation* $\varphi(x) = p^{6k+1}(p-1)$ *a seulement deux solutions :* $x = p^{6k+2}$ *et* $x = 2p^{6k+2}$.

Démonstration. Soit k un nombre naturel donné et p un nombre premier de la forme $4t+3$. On vérifie sans peine que les nombres $x = p^{6k+2}$ et $x = 2p^{6k+2}$ satisfont à l'équation $\varphi(x) = p^{6k+1}(p-1)$. Supposons maintenant que x est un nombre naturel tel que

$$\varphi(x) = p^{6k+1}(p-1), \quad x \neq p^{6k+2} \quad \text{et} \quad x \neq 2p^{6k+2}. \tag{2}$$

S'il était $x = 2^\alpha$, où α est un nombre naturel, on aurait $p^{6k+1}(p-1) = \varphi(x) = 2^{\alpha-1}$, ce qui est impossible, puisque $p \neq 2$. On a donc $x = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, où r est un nombre naturel, $p_1, p_2, \dots, p_r$ sont des nombres premiers, $2 < p_1 < p_2 < \dots < p_r$, $\alpha \geqslant 0$, $\alpha_i > 0$ ($i = 1, 2, \dots, r$), ce qui donne

$$\varphi(x) = \varphi(2^\alpha) p_1^{\alpha_1 - 1}(p_1 - 1) p_2^{\alpha_2 - 1}(p_2 - 1) \cdots p_r^{\alpha_r - 1}(p_r - 1)$$

et, comme $2 \mid p_i - 1$ ($i = 1, 2, \dots, r$) on trouve $\varphi(2^\alpha) 2^r \mid \varphi(x) = p^{6k+1}(p-1)$, d'où $\alpha \leqslant 1$, $r = 1$, donc $x = 2^\alpha p_1^{\alpha_1}$ et $\varphi(x) = p_1^{\alpha_1 - 1}(p_1 - 1) = p^{6k+1}(p-1)$. S'il était $p_1 = p$, on aurait $\alpha_1 - 1 = 6k + 1$ et $x = 2^\alpha p^{6k+2}$, où $\alpha = 0$ ou $\alpha = 1$, contrairement à (2). On a donc $p_1 \neq p$. S'il était $\alpha_1 > 1$, on aurait donc $p_1 \mid p - 1$ et $p \mid p_1 - 1$, ce qui est impossible. On a donc $\alpha_1 = 1$, d'où $p_1 - 1 = p^{6k+1}(p-1)$ et

$$p_1 = p^{6k+1}(p-1) + 1 > p^2 + 1 > p^2 - p + 1,$$

et comme, d'autre part

$$p_1 = p^{6k+2} - p^{6k+1} + 1 = p^{6k}(p^2 - p + 1) - (p^{6k} - 1),$$
$$p^6 - 1 \mid p^{6k} - 1, \quad p^6 - 1 = (p^3 - 1)(p+1)(p^2 - p + 1),$$

on a $1 < (p^2 - p + 1) \mid p_1$, ce qui est impossible, vu que le nombre p_1 est premier.

Le théorème 2 se trouve ainsi démontré. □

Il en résulte immédiatement ce

Corollaire 2. *L'équation $\varphi(x) = 6 \cdot 7^{12k+1}$, où k est un nombre naturel, a précisément deux solutions : $x = 7^{12k+2}$ et $x = 2 \cdot 7^{12k+2}$.*

Théorème 3. *Il existe une infinité de nombres naturels m pour lesquels l'équation $\varphi(x) = m$ a précisément trois solutions. Tels sont, par exemple, les nombres $m = 12 \cdot 7^{12k+1}$ où $k = 1, 2, \ldots$.*

Démonstration. Soit k un nombre naturel et $m = 12 \cdot 7^{12k+1}$. On vérifie sans peine que

$$m = \varphi(3 \cdot 7^{12k+2}) = \varphi(4 \cdot 7^{12k+2}) = \varphi(6 \cdot 7^{12k+2}).$$

Supposons maintenant que

$$\varphi(x) = m, \quad x \neq 3 \cdot 7^{12k+2}, \quad x \neq 4 \cdot 7^{12k+2} \quad \text{et} \quad x \neq 6 \cdot 7^{12k+2}. \tag{3}$$

D'après $\varphi(x) = m$ il ne peut pas être $x = 2^\alpha$, où α est un entier $\geqslant 0$.

S'il était $x = 2^\alpha y$, où $\alpha \geqslant 2$ et $(y, 2) = 1$, on aurait

$$\varphi(x) = 2^{\alpha-1}\varphi(y) = 12 \cdot 7^{12k+1}, \quad \text{donc} \quad \alpha = 2 \quad \text{et} \quad \varphi(y) = 6 \cdot 7^{12k+1},$$

et, d'après le corollaire 2 on aurait $y = 7^{12k+2}$ [puisque $(y, 2) = 1$], d'où

$$x = 4y = 4 \cdot 7^{12k+2},$$

contrairement à (3).

Donc, le nombre x n'est pas divisible par 4 et on a $x = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ où r est un nombre naturel, $p_1, p_2, \ldots, p_r$ sont des nombres premiers impairs distincts, $\alpha \leqslant 1$ et $\alpha_i \geqslant 1$ $(i = 1, 2, \ldots, r)$. On a donc

$$\varphi(x) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_r^{\alpha_r}) = 12 \cdot 7^{12k+1}.$$

S'il était $r \geqslant 3$, on aurait $8 \mid \varphi(x) = 12 \cdot 7^{12k+1}$, ce qui est impossible. On a donc $r \geqslant 2$.

S'il était $r = 2$ alors, les nombres $\varphi(p_1^{\alpha_1})$ et $\varphi(p_2^{\alpha_2})$ étant pairs, un d'eux, soit $\varphi(p_1^{\alpha_1})$ serait égal à $2 \cdot 7^l$, où l est un entier $\geqslant 0$, d'où, d'après le corollaire 1, $l = 0$ et $p_1^{\alpha_1} = 3$, donc $\varphi(p_1^{\alpha_1}) = 2$ et $\varphi(p_2^{\alpha_2}) = 6 \cdot 7^{12k+1}$ et, d'après le corollaire 2 on aurait $p_2^{\alpha_2} = 7^{12k+2}$, d'où $x = 2^\alpha \cdot 3 \cdot 7^{12k+2}$, contrairement à (3).

On a donc $r = 1$ et $\varphi(x) = \varphi(p_1^{\alpha_1}) = 12 \cdot 7^{12k+1}$ et évidemment on a $p_1 \neq 3$ et $p_1 \neq 7$, donc $\alpha_1 = 1$ et $p_1 - 1 = 12 \cdot 7^{12k+1}$, d'où $p_1 = 12 \cdot 7^{12k+1} + 1 > 5$, ce qui est impossible, vu que le nombre $12 \cdot 7^{12k+1} + 1$ est divisible par 5 (puisque $7^4 = 5t + 1$ et $12 \cdot 7 = 5u - 1$).

Nous avons ainsi démontré que l'équation $\varphi(x) = m$ a précisément trois solutions. Le théorème 3 est ainsi démontré. □

M. W. Sierpiński a exprimé l'hypothèse que, quel que soit le nombre naturel $s > 1$, il existe une infinité de nombres naturels m pour lesquels l'équation $\varphi(x) = m$ a précisément s solutions. Or, nous ne savons pas démontrer même que pour tout nombre naturel $s > 1$ il existe au moins un nombre naturel m tel que l'équation $\varphi(x) = m$ a précisément s solutions.

Il est encore à remarquer que dans une communication présentée au Congrès des mathématiciens tchécoslovaques à Prague en 1955 ([3]) j'ai démontré d'une façon tout-à-fait élémentaire que, quel que soit le nombre naturel m tel que l'équation $\varphi(x) = m$ a plus que s solutions. Tel est, par exemple, le nombre $m = (p_1 - 1)(p_2 - 1) \cdots (p_s - 1)$, où p_i désigne le i-ème nombre premier. (L'équation $\varphi(x) = m$ est ici vérifiée par les nombres

$$x_0 = p_1 p_2 \cdots p_s \quad \text{et} \quad x_i = x_0 \frac{p_i - 1}{p_i} .$$

où $i = 1, 2, \ldots, s$.)

Bibliographie

[1] V. L. Klee, jr., *On a conjecture of Carmichael*. Bull. Amer. Math. Soc. 53 (1947), 1183–1186.

([3]) Voir G3, p. 875–876.

Andrzej Schinzel
Selecta

Originally published in
Czechoslovak Mathematical Journal
6 (1956), 164–165

Sur un problème concernant la fonction $\varphi(n)$

Récemment M. W. Sierpiński m'a posé le problème suivant : *k étant un nombre naturel quelconque, existe-t-il toujours un nombre naturel m tel que l'équation $\varphi(x) = m$ ait plus que k solutions* (en nombres naturels x) ?

($\varphi(n)$ désigne ici le nombre de nombres naturels $\leqslant n$ et premiers avec n).

Le but de cette communication est de démontrer que *la réponse à ce problème est positive*.

Soit k un nombre naturel donné, p_i — le i-ème nombre premier. Posons

$$m = (p_1 - 1)(p_2 - 1)\cdots(p_k - 1), \tag{1}$$

$$x_i = p_1 p_2 \cdots p_{i-1}(p_i - 1)p_{i+1}\cdots p_k \quad \text{pour} \quad i = 1, 2, \ldots, k, \tag{2}$$

$$x_{k+1} = p_1 p_2 \cdots p_k. \tag{3}$$

Les nombres $x_1, x_2, \ldots, x_k, x_{k+1}$ sont évidemment naturels et distincts deux à deux.

Soit maintenant i un des nombres $1, 2, \ldots, k$. Le nombre $p_i - 1$ évidemment n'est pas divisible par aucun nombre premier $> p_{i-1}$:

$$p_i - 1 = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_{i-1}^{\gamma_{i-1}} \tag{4}$$

où $\gamma_1, \gamma_2, \ldots, \gamma_{i-1}$ sont des entiers $\geqslant 0$. D'après (2) on a donc

$$x_i = p_1^{\gamma_1+1} p_2^{\gamma_2+1} \cdots p_{i-1}^{\gamma_{i-1}+1} p_{i+1} p_{i+2} \cdots p_k,$$

d'où

$$\varphi(x_i) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_{i-1}^{\gamma_{i-1}} (p_1 - 1)\cdots(p_{i-1} - 1)(p_{i+1} - 1)\cdots(p_k - 1)$$

et, d'après (4) et (1) on trouve $\varphi(x_i) = m$.

Or, d'après (3) et (1) on a évidemment $\varphi(x_{k+1}) = m$.

Les $k + 1$ nombres naturels distincts $x_1, x_2, \ldots, x_{k+1}$ satisfont donc à l'équation $\varphi(x) = m$ et notre assertion se trouve démontrée.

En ce qui concerne l'équation $\varphi(x) = m$ il est encore à remarquer que R. D. Carmichael suppose qu'il n'existe aucun nombre naturel m pour lequel elle ait précisément une solution [1] ; comme l'a démontré V. L. Klee jr., cela est vrai pour $m \leqslant 10^{400}$ [2]. Or, M. W. Sierpiński a récemment démontré qu'il existe une infinité de nombres naturels m pour lesquels l'équation $\varphi(x) = m$ a précisément deux solutions : tels sont, par exemple,

---

Communication présentée le 2 septembre 1955 au Congrès des mathématiciens tchécoslovaques à Prague par M. W. Sierpiński.

les nombres $m = 2 \cdot 3^{6k+1}$, où $k = 1, 2, \ldots$. (Ces deux solutions sont ici $x = 3^{6k+2}$ et $x = 2 \cdot 3^{6k+2}$).

Après avoir pris connaissance avec la communication de A. Schinzel, M. P. Erdős a remarqué que S. Pillai a prouvé que le nombre des entiers $m \leqslant x$ pour lesquels l'équation $\varphi(y) = m$ a des solutions est d'ordre $o(x)$.

En 1935 P. Erdős a démontré (dans le *Quarterly Journal of Mathematics*) l'existence d'une suite infinie croissante d'entiers n_k ($k = 1, 2, \ldots$) telle que le nombre de solutions de l'équation $\varphi(y) = n_k$ est plus grand que n_k^c où c est un nombre fixe positif, et il énonce l'hypothèse que pour tout $\varepsilon > 0$ il existe un tel $c > 1 - \varepsilon$.

Quant à la démonstration de A. Schinzel, M. P. Erdős la considére comme la plus simple de toutes qui lui sont connues.

Travaux cités

[1] R. D. Carmichael, *Note on Euler's φ-function*. Bull. Amer. Math. Soc. 28 (1922), 109–110.

[2] V. L. Klee, jr., *On a conjecture of Carmichael*. Bull. Amer. Math. Soc. 53 (1947), 1183–1186.

Originally published in
Acta Arithmetica VI (1961), 473–485

Distributions of the values of some arithmetical functions

with P. Erdős (*Budapest*)

1.

Y. Wang and A. Schinzel proved, by Brun's method, the following theorem ([3]):

For any given sequence of h non-negative numbers $a_1, a_2, \dots, a_h$ and $\varepsilon > 0$, there exist positive constants $c = c(a, \varepsilon)$ and $x_0 = x_0(a, \varepsilon)$ such that the number of positive integers $n \leqslant x$ satisfying

$$\left|\frac{\varphi(n+i)}{\varphi(n+i-1)} - a_i\right| < \varepsilon \quad (1 \leqslant i \leqslant h)$$

is greater than $cx/\log^{h+1} x$, whenever $x > x_0$.

They also proved the analogous theorem for the function σ.

Shao Pin Tsung, also using Brun's method, extended this result to all multiplicative positive functions $f_s(n)$ satisfying the following conditions ([4]):

I. *For any positive integer l and prime number p:*

$$\lim_{p\to\infty}\left(f_s(p^l)/p^{ls}\right) = 1 \quad (p \text{ denotes primes}).$$

II. *There exists an interval $\langle a, b\rangle$, $a = 0$ or $b = \infty$, such that for any integer $M > 0$ the set of numbers $f_s(N)/N^s$, where $(N, M) = 1$, is dense in $\langle a, b\rangle$.*

(This formulation is not the same but equivalent to the original one.)

In this paper we shall show without using Brun's method that *if we replace the condition* I *by the condition*

$$\sum \frac{\left(f_s(p) - p^s\right)^2}{p^{2s+1}} < \infty$$

(*but preserving condition* II) *then there exists more than $C(a, \varepsilon)x$ positive integers $n \leqslant x$ for which*

$$\left|\frac{f_s(n+i)}{f_s(n+i-1)} - a_i\right| < \varepsilon \quad (i = 1, 2, \dots, h).$$

This theorem follows easily from the following stronger theorem.

Theorem 1. *Let $f(n)$ be an additive function, satisfying the following conditions*

1. $\sum_p \left(\|f(p)\|^2/p\right)$ *is convergent, where* $\|f\|$ *denotes* $f(p)$ *for* $|f(p)| \leqslant 1$ *and* 1 *for* $|f(p)| > 1$.
2. *There exists a number c_1 such that, for any integer $M > 0$, the set of numbers $f(N)$, where $(N, M) = 1$, is dense in (c_1, ∞).*

Then, for any given sequence of h real numbers $a_1, a_2, \ldots, a_h$ and $\varepsilon > 0$, there exist more than $C(a, \varepsilon)x$ positive integers $n \leqslant x$ for which

$$\left|f(n+i) - f(n+i-1) - a_i\right| < \varepsilon \quad (i = 1, 2, \ldots, h); \tag{1}$$

$C(a, \varepsilon)$ is a positive constant, depending on ε and a_i.

Lemma. *There exists an absolute constant c such that the number of integers of the form $pq > x$ for which one can find $n \leqslant x$ satisfying $n \equiv b \pmod a$, $n \equiv 0 \pmod p$ and $n + 1 \equiv 0 \pmod q$ is for $x > x_0(a)$ less than cx/a.*

Proof. Let $c_1, c_2, \ldots$ denote absolute constants. Assume $p > x^{1/2}$ ($q > x^{1/2}$ can be dealt similarly). Denote by $A_l(x)$ the number of integers of the form pq satisfying

$$pq > x, \quad x^{1-1/2^l} \leqslant p < x^{1-1/2^{l+1}}, \quad n \equiv b \pmod a, \quad p \mid n,\ q \mid n+1,$$
$$\text{for some } n, \quad 1 \leqslant n \leqslant x,$$

and by $A'_l(x)$ the number of integers pq for which

$$x^{1-1/2^l} \leqslant p < x^{1-1/2^{l+1}}, \quad q > x^{1/2^{l+1}}, \quad n \equiv b \pmod a, \quad p \mid n,\ q \mid n+1,$$
$$\text{for some } n, \quad 1 \leqslant n \leqslant x,$$

Clearly $A'_l(x) \geqslant A_l(x)$ and it will suffice to prove that for $x > x_0(a)$, $\sum_{l=1}^{\infty} A'_l(x) < cx/a$.

Define positive integer l_x by the inequality

$$2^{l_x} \geqslant \log\log x > 2^{l_x - 1}.$$

The number k of integers n satisfying

$$n \leqslant x, \quad n \equiv b \pmod a, \quad n \equiv 0 \pmod p, \quad x^{1-1/2^l} < p < x^{1-1/2^{l+1}} \tag{2}$$

for an $l \geqslant l_x$ does not exceed $\sum_{x \geqslant p > x^{1-2^{-l_x}}} \left(\left[\frac{x}{pa}\right] + 1\right)$, thus by theorems of Mertens and Chebyshev

$$k < \frac{c_1 x}{a \cdot 2^{l_x}} + \frac{c_2 x}{\log x}$$

and by the definition of l_x

$$k < \frac{c_3 x}{a \log\log x} \quad \text{for } x > x_1(a).$$

c Denote the numbers satisfying (2) for an $l \geqslant l_x$ and satisfying $\nu(n+1) \leqslant 10 \log\log x$ by $a_1 < a_2 < \ldots < a_h \leqslant x$ and denote the numbers satisfying (2) for an $l \geqslant l_x$ and satisfying $\nu(n+1) > 10 \log\log x$ by $b_1 < b_2 < \ldots < b_j \leqslant x$. Since

$$\sum_{n \leqslant x} 2^{\nu(n+1)} \leqslant \sum_{n \leqslant x} d(n+1) = O(x \log x)$$

we have

$$j < \frac{c_4 x}{\log^5 x}.$$

Clearly $h \leqslant k$ and $\nu(n+1) \leqslant 2\log(n+1) \leqslant 3 \log x$ for all $n \leqslant x$, thus

$$\sum_{l \geqslant l_x} A_l'(x) \leqslant \sum_{i=1}^{h} \nu(a_i + 1) + \sum_{i=1}^{j} \nu(b_i + 1) \leqslant 10k \log\log x + 3j \log x < \frac{c_5 x}{a} \tag{3}$$

for $x > x_2(a)$.

For $l < l_x$ denote numbers satisfying (2) by $a_1^{(l)} < a_2^{(l)} < \ldots < a_{k_l}^{(l)}$. For the same c reason as for k we have for k_l the inequality

$$k_l < \frac{c_6 x}{a \cdot 2^{l+1}} + \frac{c_2 x}{\log x}$$

hence by $l < l_x$

$$k_l < \frac{c_7 x}{a \cdot 2^l} \quad \text{for} \quad x > x_3(a). \tag{4}$$

We shall prove that for $l < l_x$ and sufficiently large x

$$A_l'(x) = \sum_{i=1}^{k_l} \nu_l(a_i^{(l)} + 1) < \frac{c_8 x}{a \cdot l^2} \tag{5}$$

where $\nu_l(m)$ denotes the number of prime factors $> x^{1/2^{l+1}}$ of m.

For this purpose, we split the summands of the sum (5) into two classes. In the first class are the integers $a_i^{(l)}$ for which $\nu_l(a_i^{(l)} + 1) \leqslant 2^l/l^2$. From (4) it follows that the contribution of these integers $a_i^{(l)}$ to (5) is less than $c_7 x/al^2$. The integers in the second class satisfy $\nu_l(a_i^{(l)} + 1) > 2^l/l^2$. Thus these integers are divisible by more than $2^l/l^2$ primes $q > x^{1/2^{l+1}}$.

c Let $g = [2^l/l^2]$. Given distinct primes $q_1, q_2, \ldots, q_g$ greater than $x^{1/2^{l+1}}$ with $q_1 q_2 \cdots q_g \leqslant x + 1$, the number of integers $n \leqslant x$ satisfying $n \equiv a \pmod b$ and $q_1 \cdots q_g \mid n+1$ is at most $\dfrac{x}{aq_1 \cdots q_g} + 1$. Thus, by theorems of Chebyshev and Mertens,

the number of integers of the second class is less than

$$\frac{x}{ag!}\Big(\sum_{x^{1/2^{l+1}}<q\leqslant x}\frac{1}{q}\Big)^g + O\Big(\sum_{q_1,\dots,q_{g-1}}\frac{x}{gq_1\cdots q_{g-1}\log(x/q_1\cdots q_{g-1})}\Big)$$

$$< \frac{x(c_9 l)^g}{ag!} + O\Big(\frac{2^{l+1}(c_9 l)^{g-1}x}{g!\log x}\Big) < \frac{x}{a\cdot 4^l}$$

for $l > c_{10}$, $x > x_4(a)$. By definition, $\nu_l(a_i^{(l)}+1) < 2^{l+1}$. Thus, for $l > c_{10}$, the contribution of the numbers of the second class to (5) is $< x/a\cdot 2^{l-1}$; for $l \leqslant c_{10}$ the contribution is clearly $< 2^{c_{10}+1}x$. Thus, for $l < l_x$, $x > x_4(a)$,

$$A_l'(x) < c_8 x/al^2$$

and in view of (3) we have for $x > x_0(a)$

$$\sum_{l=1}^{\infty} A_l'(x) < \frac{c_5 x}{a} + \sum_{l<l_x}\frac{c_8 x}{al^2} < \frac{cx}{a}$$

which proves the lemma. □

Proof of the theorem. Let ε be a positive number and let a sequence a_i $(i = 1, 2, \dots, h)$ be given.

By condition 2 we can find positive integers $N_0, N_1, \dots, N_h$ such that

$$(N_i, (h+1)!) = 1 \ (i = 0, 1, \dots, h), \quad (N_i, N_j) = 1 \ (0 \leqslant i < j \leqslant h), \tag{6}$$

$$f(N_0) > c_1 + \max_{1\leqslant i\leqslant h}\Big\{f(i+1) - \sum_{j=1}^{i} a_j\Big\}$$

and

$$\Big|f(N_i) - \Big\{f(N_0) - f(i+1) + \sum_{j=1}^{i} a_j\Big\}\Big| < \tfrac{1}{4}\varepsilon \quad (1 \leqslant i \leqslant h);$$

hence

$$\big|f\big((i+1)N_i\big) - f(iN_{i-1}) - a_i\big| < \tfrac{1}{2}\varepsilon \quad (1 \leqslant i \leqslant h). \tag{7}$$

Let k_1 be the greatest prime factor of $N_0N_1\cdots N_h$ or h if $N_0N_1\cdots N_h = 1$. Put $\mu = \varepsilon/\sqrt{96hc}$ (c is the constant of the Lemma). By condition 1, $\sum_{|f(p)|\geqslant\mu}(1/p)$ is convergent. Since $\sum_p (1/p^2)$ is also convergent, there exists a k_2 such that

$$\sum_{\substack{|f(p)|\geqslant\mu\\ p>k_2}}\frac{1}{p} + \sum_{p>k_2}\frac{1}{p^2} < \frac{1}{3(h+1)}\,. \tag{8}$$

Finally by condition 1 there exists a k_3 such that

$$\sum_{\substack{|f(p)|<\mu \\ p>k_3}} \frac{f(p)^2}{p} < \frac{\varepsilon^2}{48h}. \tag{9}$$

Let us put

$$k = \max(k_1, k_2, k_3), \quad N = N_1 N_2 \cdots N_h, \quad P = \prod_{p \leqslant k,\ p \nmid N} p, \quad Q = (h+1)!\, N^2 P$$

and let us consider the following system of congruences

$$n \equiv 1 \pmod{(h+1)!\,P}, \quad n \equiv -i + N_i \pmod{N_i^2}, \quad 0 \leqslant i \leqslant h.$$

By (6) and the Chinese Remainder Theorem there exists a number n_0 satisfying these congruences.

It is easy to see that

(10) *for every integer t the numbers $(Qt+n_0+i)/(i+1)N_i$ $(i = 1, 2, \ldots, h)$ are integers which are not divisible by any prime $\leqslant k$;*

(11) *the number of terms not exceeding x of the arithmetical progression $Qt + n_0$ is $x/Q + O(1)$.*

In order to prove Theorem 1 we shall estimate the number of integers n of the progression $Qt + n_0$ which satisfy the inequalities

$$n \leqslant x, \quad \sum_{i=1}^{h} \Big(f(n+i) - f(n+i-1) - f\big((i+1)N_i\big) + f(iN_{i-1}) \Big)^2 > \tfrac{1}{4}\varepsilon^2. \tag{12}$$

We divide the set of integers $n \equiv n_0 \pmod{Q}$ for which the inequalities (12) hold into two classes. Integers n such that $n(n+1)\cdots(n+h)$ is divisible by a prime $p > k$ with $|f(p)| \geqslant \mu$, or by p^2, $p > k$, are in the first class and all other integers are in the second class.

(13) *The number of integers $n \leqslant x$, $n \equiv r \pmod{Q}$ which are divisible by a given integer $d > 0$ is equal to $x/dQ + O(1)$ for $(d, Q) = 1$,*

hence the number of integers $n \leqslant x$, $n \equiv n_0 \pmod{Q}$ of the first class is less than

$$(h+1)\,\frac{x}{Q}\Big(\sum_{\substack{p>k \\ |f(p)|\geqslant\mu}} \frac{1}{p} + \sum_{p>k} \frac{1}{p^2} \Big) + O\Big(\sum_{p \leqslant x+h} 1 + \sum_{p^2 \leqslant x+h} 1 \Big).$$

By the inequality (8) and the definition of k this number is less than $\frac{1}{3}x/Q + o(x)$.

For the integers of the second class, by remark (10) we have

$$\sum_n{}'' \sum_{i=1}^{h}\Big(f(n+i)-f(n+i-1)-f\big((i+1)N_i\big)+f(iN_{i-1})\Big)^2$$
$$= S = \sum_n{}'' \sum_{i=1}^{h}\Big\{\sum_{\substack{p\mid n+i\\ p>k}} f(p) - \sum_{\substack{p\mid n+i-1\\ p>k}} f(p)\Big\}^2,$$

where $\sum''$ means that the summation runs through the integers of the second class. In view of remark (13), since $(Q, p) = 1$ we have

$$\begin{aligned} S &\leqslant \sum_{\substack{n\equiv n_0 \pmod Q\\ n\leqslant x}} \sum_{i=1}^{h}\Big\{\sum_{\substack{p\mid n+i\\ p>k,\ |f(p)|<\mu}} f(p) - \sum_{\substack{p\mid n+i-1\\ p>k,\ |f(p)|<\mu}} f(p)\Big\}^2 \\ &= \sum_{\substack{x+h\geqslant p>k\\ |f(p)|<\mu}} f^2(p)\Big(\frac{2hx}{Qp}+O(1)\Big) \\ &\quad + \sum_{\substack{n\equiv n_0 \pmod Q\\ n\leqslant x}} \sum_{i=1}^{h}\Big\{2\sum_{\substack{pq\mid n+i,\ q>p>k\\ |f(p)|<\mu,\ |f(q)|<\mu}} f(p)f(q) \\ &\qquad + 2\sum_{\substack{pq\mid n+i-1,\ q>p>k\\ |f(p)|<\mu,\ |f(q)|<\mu}} f(p)f(q) - 2\sum_{\substack{p\mid n+i,\ q\mid n+i-1,\ q>k\\ p>k,\ |f(p)|<\mu,\ |f(q)|<\mu}} f(p)f(q)\Big\} \\ &\leqslant \frac{2hx}{Q}\sum_{p>k,\ |f(p)|<\mu}\frac{f^2(p)}{p} + \sum_{\substack{n\equiv n_0 \pmod Q\\ n\leqslant x}} \sum_{i=1}^{h} 2\sum_{\substack{p\mid n+i,\ q\mid n+i-1\\ pq\geqslant x,\ p>k,\ q>k\\ |f(p)|<\mu,\ |f(q)|<\mu}} |f(p)f(q)| \\ &\qquad + O\Big(\sum_{\substack{p\leqslant x+h\\ |f(p)|<\mu}} f^2(p) + \sum_{\substack{p>q>k,\ pq\leqslant x+h\\ |f(p)|<\mu,\ |f(q)|<\mu}} |f(p)f(q)|\Big). \end{aligned}$$

Thus finally from (9), Lemma, the equality $\mu^2 = \varepsilon^2/96hc$ and from the fact that the number of integers of the form pq not exceeding $x + h$ is $o(x)$, we get

$$S < \frac{\varepsilon^2}{12}\cdot\frac{x}{Q} + o(x).$$

Thus the number of integers of the second class is less than $\frac{1}{3}x/Q + o(x)$.

Hence there exist less than $\frac{2}{3}x/Q + o(x)$ positive integers $n \leqslant x$, $n \equiv n_0 \pmod Q$ for which

$$\sum_{i=1}^{h}\big(f(n+i)-f(n+i-1)-f((i+1)N_i)+f(iN_{i-1})\big)^2 > \tfrac{1}{4}\varepsilon^2.$$

Therefore by (11) there exist more than $\frac{1}{3}x/Q + o(x)$ positive integers $n \leqslant x$ for which

$$\sum_{i=1}^{h}\big(f(n+i) - f(n+i-1) - f((i+1)N_i) + f(iN_{i-1})\big)^2 \leqslant \tfrac{1}{4}\varepsilon^2$$

and then

$$\big|\big(f(n+i) - f(n+i-1) - f((i+1)N_i) + f(iN_{i-1})\big| \leqslant \tfrac{1}{2}\varepsilon \quad (i = 1, 2, \ldots, h).$$

In view of (7), the proof is complete. □

Theorem 2. *Let $f(n)$ be an additive function satisfying the conditions of Theorem* 1 *and such that partial sums of $\sum\big(\|f(p)\|/p\big)$ are bounded*:

$$A > |S_k|, \quad S_k = \sum_{p\leqslant k}\frac{\|f(p)\|}{p}. \tag{14}$$

Then for any given natural number h there exists a number c_h such that for any $\varepsilon > 0$ and every sequence of h numbers: $a_1, a_2, \ldots, a_h \geqslant c_h$, there exist more than $C(a,\varepsilon)x$ positive integers $n \leqslant x$ for which

$$|f(n+i) - a_i| < \varepsilon \quad (i = 1, 2, \ldots, h). \tag{15}$$

$C(a,\varepsilon)$ is a positive constant, depending on ε and a_i.

Proof. Let ε be a positive number, $c_h = c_1 + \max\limits_{1\leqslant i\leqslant h} f(i)$ and let a sequence $a_i \geqslant c_h$ $(i = 1, 2, \ldots, h)$ be given.

By condition 2 we can find positive integers $N_1, N_2, \ldots, N_h$ such that

$$(N_i, h!) = 1 \ (i = 1, 2, \ldots, h), \quad (N_i, N_j) = 1 \ (1 \leqslant i < j \leqslant h) \tag{16}$$

and

$$|f(N_i) - a_i + f(i)| < \tfrac{1}{2}\varepsilon \quad (i = 1, 2, \ldots, h). \tag{17}$$

Let k_1 be the greatest prime factor of $N_1N_2\cdots N_h$ or h if $N_0N_1\cdots N_h = 1$. Let C be an absolute constant such that

$$\sum_{y\leqslant p<z}\frac{1}{p} < C\log\frac{\log z}{\log y} \quad \text{for all} \quad z > 2y \geqslant 2.$$

Put $\mu = \varepsilon/20C\sqrt{h}$. By condition 1, $\sum\limits_{|f(p)|\geqslant\mu}(1/p)$ is convergent. Since $\sum(1/p^2)$ is also convergent, there exists a k_2 such that

$$\sum_{|f(p)|\geqslant\mu,\ p>k_2}\frac{1}{p} + \sum_{p>k_2}\frac{1}{p^2} < \frac{1}{3h}. \tag{18}$$

By condition 1 there exists also a k_3 such that

$$\sum_{p>k_3,\ |f(p)|<\mu}\frac{f(p)^2}{p} < \frac{\varepsilon^2}{24h}. \tag{19}$$

Put $\eta = \varepsilon/\sqrt{96h}$, $A' = \sum_{|f(p)|\geqslant\mu} (1/p)$, $B = A + \eta A'$ and denote by I_ν the interval

$$\left[\nu\eta - \tfrac{1}{2}\eta, \nu\eta + \tfrac{1}{2}\eta\right], \quad \nu = 0, \pm1, \pm2, \ldots, \pm[B/\eta + 1]$$

and let k_ν be the least integer $k > \max\{k_1, k_2, k_3\}$ such that $\sum_{p\leqslant k,\, |f(p)|<\mu} \big(f(p)/p\big) \in I_\nu$ if such integers k exist, otherwise let $k_\nu = 1$.

Now if $\sum_{p\leqslant x+h,\, |f(p)|<\mu} \big(f(p)/p\big) \in I_{\nu_x}$—by the condition (14) and by (18) such ν_x certainly exists—we put $k_{\nu_x} = k$ and then we get

$$\left|\sum_{x+h\geqslant p>k,\, |f(p)|<\mu} \frac{f(p)}{p}\right| < \eta, \quad k \leqslant \max_{|\nu|\leqslant[B/\eta]+1} k_\nu = \bar{k}. \tag{20}$$

Let $\sum'$ denote that the summation runs through all primes p, q satisfying conditions $p > q > k$, $pq \leqslant x + h$, $|f(p)| < \mu$, $|f(q)| < \mu$. From (20) we get

$$\begin{aligned} 2\sum{}' \frac{f(p)f(q)}{pq} &\leqslant \Bigg(\sum_{\substack{x+h\geqslant p>k\\ |f(p)|<\mu}} \frac{f(p)}{p}\Bigg)^2 + 2\sum_{x+h\geqslant p>\sqrt{x+h}} \frac{\mu}{p} \sum_{x+h\geqslant q>(x+h)/p} \frac{\mu}{q} \\ &\leqslant \frac{\varepsilon^2}{96h} + 2\sum_{l=2}^{\infty} \sum_{\substack{(x+h)^{1-1/2^l}\geqslant p>(x+h)^{1-1/2^{l-1}}\\ p\leqslant(x+h)/4}} \frac{\mu}{p} \sum_{x+h\geqslant q>(x+h)/p} \frac{\mu}{q} \\ &\quad + 2\sum_{x+h\geqslant p>(x+h)/4} \frac{\mu}{p} \sum_{x+h\geqslant q} \frac{\mu}{q} \\ &\leqslant \frac{\varepsilon^2}{96h} + 2\mu^2C^2\sum_{l=2}^{\infty} \frac{l\log 2}{2^l - 2} + O\left(\frac{\mu^2\log\log x}{\log x}\right) < \frac{\varepsilon^2}{24h}. \end{aligned} \tag{21}$$

Let us put $N = N_1N_2\cdots N_h$, $P = \prod_{p\leqslant k,\, p\nmid N} p$,

$$Q = h!\,N^2P \leqslant h!\,N^2 \prod_{p\leqslant k,\, p\nmid N} p = \overline{Q} \tag{22}$$

and let us consider the following system of congruences:

$$n \equiv 0 \pmod{h!\,P}, \quad n \equiv -i + N_i \pmod{N_i^2}.$$

By (16) and the Chinese Remainder Theorem there exists a number n_0 satisfying these congruences.

It is easy to see that

(23) *for every integer t the numbers* $\dfrac{Qt + n_0 + i}{iN_i}$ $(i = 1, 2, \ldots, h)$ *are integers which are not divisible by any prime* $\leqslant k$.

Analogously, as in the proof of Theorem 1, we shall estimate the number of integers n of

the progression $Qt + n_0$ which satisfy the inequalities

$$n \leqslant x, \quad \sum_{i=1}^{h} \big(f(n+i) - f(iN_i)\big)^2 > \tfrac{1}{4}\varepsilon^2. \tag{24}$$

We divide the set of integers $n \equiv n_0 \pmod{Q}$ for which the inequalities (24) hold into two classes. Integers n such that $(n+1)(n+2)\cdots(n+h)$ is divisible by a prime $p > k$ with $|f(p)| \geqslant \mu$ or by p^2, $p > k$, are in the first class and all other integers are in the second class.

By remark (13) the number of integers $n \leqslant x$, $n \equiv n_0 \pmod{Q}$ of the first class is less than

$$h\,\frac{x}{Q}\Big(\sum_{p>k,\ |f(p)|\geqslant\mu} \frac{1}{p} + \sum_{p>k} \frac{1}{p^2}\Big) + O\Big(\sum_{p\leqslant x+h} 1 + \sum_{p^2\leqslant x+h} 1\Big).$$

By the inequality (18) and the definition of k this number is less than $\frac{1}{3}x/Q + o(x)$.

For the integers of the second class, by remark (23), we have

$$\sum_{i=1}^{h} \big(f(n+i) - f(iN_i)\big)^2 = \sum_{i=1}^{h} \Big(\sum_{\substack{p\mid n+i,\ p>k\\ |f(p)|<\mu}} f(p)\Big)^2$$

and

$$\sum_{n}{}'' \sum_{i=1}^{h} \big(f(n+i) - f(iN_i)\big)^2 = \sum_{n}{}'' \sum_{i=1}^{h} \Big(\sum_{\substack{p\mid n+i,\ p>k\\ |f(p)|<\mu}} f(p)\Big)^2,$$

where $\sum_n{}''$ means that the summation runs through the integers of the second class. In view of remark (13), we have

$$\sum_{n}{}'' \sum_{i=1}^{h} \big(f(n+i) - f(iN_i)\big)^2 \leqslant \sum_{\substack{n\equiv n_0 \pmod{Q}\\ n\leqslant x}} \sum_{i=1}^{h} \Big(\sum_{\substack{p\mid n+i,\ p>k\\ |f(p)|<\mu}} f(p)\Big)^2$$

$$= \sum_{\substack{x+h\geqslant p>k\\ |f(p)|<\mu}} f^2(p)\Big(\frac{hx}{Qp} + O(1)\Big) + 2\sum{}' f(p)f(q)\Big(\frac{hx}{Qpq} + O(1)\Big)$$

$$\leqslant \frac{hx}{Q}\Big(\sum_{p>k,\ |f(p)|<\mu} \frac{f^2(p)}{p} + 2\sum{}' \frac{f(p)f(q)}{pq}\Big) + O\Big(\sum_{\substack{p\leqslant x+h\\ |f(p)|<\mu}} f^2(p) + \sum{}' \big|f(p)f(q)\big|\Big).$$

Thus, finally from (19), (21) and from the fact that the number of integers of the form

pq not exceeding $x+h$ is $o(x)$ we get

$$\sum{}'' \sum_{i=1}^{h} \big(f(n+i) - f(iN_i)\big)^2 < \frac{\varepsilon^2}{12} \cdot \frac{x}{Q} + o(x).$$

Thus the number of integers of the second class is less than $\frac{1}{3}x/Q + o(x)$.

Hence, there exist less than $\frac{2}{3}x/Q + o(x)$ positive integers $n \leqslant x$, $n \equiv n_0 \pmod{Q}$, for which

$$\sum_{i=1}^{h} \big(f(n+i) - f(iN_i)\big)^2 > \tfrac{1}{4}\varepsilon^2.$$

By (11) and (22) there exist, therefore, more than $\frac{1}{3}x/Q + o(x)$ positive integers $n \leqslant x$ for which

$$\sum_{i=1}^{h} \big(f(n+i) - f(iN_i)\big)^2 \leqslant \tfrac{1}{4}\varepsilon^2,$$

and then

$$\big|f(n+i) - f(iN_i)\big| \leqslant \tfrac{1}{2}\varepsilon \quad (i = 1, 2, \ldots, h).$$

In view of (16) and (17), this completes the proof. □

Theorem 2 is best possible. Assume only that there exists an a and a $c > 0$ so that the number of integers $n \leqslant x$ satisfying $|f(n)| < a$ is greater than cx.

Then $\sum \dfrac{\|f(p)\|^2}{p}$ *converges and* $\sum \dfrac{\|f(p)\|}{p}$ *has bounded partial sums.*

In the paper [2], P. Erdős proved [1] the following theorem:

If there exist two constants c_1 and c_2 and an infinite sequence $x_k \to \infty$ so that for every x_k there are at least $c_1 x_k$ integers:

$$1 \leqslant a_1 < a_2 < \ldots < a_l \leqslant x_k, \quad l \geqslant c_1 x_k,$$

for which

$$|f(a_i) - f(a_j)| < c_2, \quad 1 \leqslant i < j \leqslant l,$$

then

$$f(n) = \alpha \log n + g(n), \quad \textit{where} \quad \sum \frac{\|g(p)\|^2}{p} < \infty.$$

In our case the conditions of this theorem are clearly satisfied and, in fact, we clearly

[1] The proof of Lemma 8 [2] is not clear and on p. 15 needs more details similar to these given above.

must have $\alpha = 0$. This implies that

$$\sum \frac{\|f(p)\|^2}{p} < \infty.$$

Assume now that $\sum\big(\|f(p)\|/p\big)$ does not have bounded partial sums. Let e.g. $\sum_{p<x}\big(\|f(p)\|/p\big) = A$, A large. Then by the method of Turán ([5], cf. also [2]) we obtain

$$\sum_{n=1}^{x}\big(f(n) - A\big)^2 < c_3 x$$

which implies that $|f(n)-A| < A-a$ for all but ηx integers $n \leqslant x$, where $\eta = c_3/(A-a)^2$. For sufficiently large A, it contradicts the assumption that $|f(n)| < a$ has cx solutions $n \leqslant x$, thus the proof is complete.

[c] [According to a remark of P. Erdős made without proof in his letter to A. Schinzel of August 17, 1961, also the condition 2 of Theorem 1 follows from the conclusion of Theorem 2.]

In Theorem 1 one can replace $\sum\big(\|f(p)\|^2/p\big) < \infty$ by: *there is an α so that if we put $f(n) - \alpha \log n = g(n)$ then* $\sum\big(\|g(p)\|^2/p\big) < \infty$. We think that here we again have a necessary and sufficient condition, but we cannot prove this. In fact, we conjecture that if there exist an a and a $c > 0$ such that the number of integers $n \leqslant x$ satisfying $|f(n+1) - f(n)| < a$ is $> cx$, then

$$f(n) = \alpha \log n + g(n) \quad \text{with} \quad \sum \frac{\|g(p)\|^2}{p} < \infty.$$

2.

The proof of Theorem 2 is very similar to the proof of Lemma 1 of P. Erdős' paper [1]. Using ideas and results from that paper we can prove the following theorem.

Theorem 3. *Let $f(n)$ be an additive function satisfying condition* 1 *of Theorem* 1 *and let $\sum_{f(p)\neq 0}(1/p)$ be divergent, $\sum\big(\|f(p)\|/p\big)$ convergent, then the distribution function of h-tuples $\big\{f(m+1), f(m+2), \ldots, f(m+h)\big\}$ exists, and it is a continuous function.*

Proof. We denote by $N(f; c_1, c_2, \ldots, c_h)$ the number of positive integers m not exceeding n for which

$$f(m+i) \geqslant c_i, \quad i = 1, 2, \ldots, h,$$

where c_i are given constants.

It is sufficient to consider, as in [1], the special case in which, for any α, $f(p^\alpha) = f(p)$, so that

$$f(m) = \sum_{p|m} f(p).$$

Let us also consider the function $f_k(m) = \sum_{p|m,\, p\leqslant k} f(p)$. We are going to show that the sequence $N(f_k; c_1, c_2, \ldots, c_h)/n$ is convergent. Since $f_k(m + A) = f_k(m)$, where $A = \prod_{p\leqslant k} p$, we can see that the integers m for which

$$f_k(m + i) \geqslant c_i \quad (i = 1, 2, \ldots, h)$$

are distributed periodically with the period A. Hence $N(f_k; c_1, c_2, \ldots, c_h)/n$ has a limit.

To prove the existence of a limit of $N(f; c_1, c_2, \ldots, c_h)/n$ it is sufficient to show that for arbitrary $\varepsilon > 0$ there exists k_0 such that for every $k > k_0$ and $n > n(\varepsilon)$

$$\big|N(f; c_1, c_2, \ldots, c_h) - N(f_k; c_1, c_2, \ldots, c_h)\big|/n < \varepsilon.$$

To show this, it is enough to prove that the number of integers $m \leqslant n$ for which there exists $i \leqslant h$ such that $f_k(m + i) < c_i$ and $f(m + i) \geqslant c_i$ or $f_k(m + i) \geqslant c_i$ and $f(m + i) < c_i$ is less that εhn. But it is an immediate consequence of the analogous theorem for $h = 1$ proved in [1], p. 123.

In order to prove that the distribution function is continuous we must show that for every $\varepsilon > 0$, there exists a $\delta > 0$ such that

$$\Delta = N(f; c_1 - \delta, c_2 - \delta, \ldots, c_h - \delta) - N(f; c_1 + \delta, c_2 + \delta, \ldots, c_h + \delta) < \varepsilon.$$

Now

$$\Delta = \sum_{i=1}^{h} \big\{ N(f; c_1 + \delta, \ldots, c_{i-1} + \delta, c_i - \delta, \ldots, c_h - \delta) - N(f; c_1 + \delta, \ldots, c_i + \delta, c_{i+1} - \delta, \ldots, c_h - \delta) \big\}$$

and by Lemma 2 of [1] each term of this sum is less than ε/h for suitably chosen δ. This completes the proof. □

We conclude from Theorems 2 and 3 that if an additive function f satisfies conditions 1, 2, $\sum_{f(p)\neq 0} (1/p)$ is divergent and $\sum\big(\|f(p)\|/p\big)$ convergent, then the distribution function of $\{f(m + 1), \ldots, f(m + h)\}$ exists, is continuous and strictly decreasing on some half straight-line, thus the sequence of integers n for which inequality (15) holds has a positive density. Similarly we can prove the following:

Theorem 4. *Assume that* $\sum_{f(p)\neq 0} \frac{1}{p} = \infty$ *and that* $\sum \frac{\|f(p)\|^2}{p} < \infty$ *then* $\big\{f(n + 1) - f(n), f(n + 2) - f(n + 1), \ldots, f(n + k) - f(n + k - 1)\big\}$ *has a continuous distribution function.*

It is easy to see that condition 2 can be replaced by the conditions

$$\lim_{p\to\infty} f(p) = 0 \quad \text{and} \quad \sum_{p} |f(p)| = \infty.$$

3.

Y. Wang proved in [6] that the number N of primes $p < x$ satisfying

$$\left|\frac{\varphi(p+\nu+1)}{\varphi(p+\nu)} - a_\nu\right| < \varepsilon, \quad 1 \leqslant \nu \leqslant k,$$

is greater than

$$c(a,\varepsilon)\frac{x}{(\log x)^{k+2}\log\log x}.$$

By our methods we can obtain in that case

$$N > c_1(a,\varepsilon)\frac{x}{\log x}.$$

After having passed to the additive function $\log\bigl(\varphi(n)/n\bigr)$ the proof is similar to the proof of Theorem 1. We use the fact that $\log\bigl(\varphi(n)/n\bigr)$ is always negative, and apply the asymptotic formula for the number of primes in arithmetical progression instead of (11) and the Brun–Titchmarsh theorem instead of (13).

We can also prove that there exists distribution function $N(c_1, c_2, \ldots, c_k)$ defined as

$$\lim_{x\to\infty}\frac{1}{\pi(x)}N\Bigl(p < x;\ \frac{\varphi(p+\nu)}{p+\nu} \geqslant c_\nu,\ \nu = 1,2,\ldots,k\Bigr).$$

References

[1] P. Erdős, *On the density of some sequences of numbers* III. J. London Math. Soc. 13 (1938), 119–127.

[2] —, *On the distribution function of additive functions*. Ann. of Math. (2) 47 (1946), 1–20.

[3] A. Schinzel, Y. Wang, *A note on some properties of the functions $\varphi(n)$, $\sigma(n)$ and $\theta(n)$*. Bull. Acad. Polon. Sci. Cl. III 4 (1956), 207–209; Ann. Polon. Math. 4 (1958), 201–213; *Corrigendum*, ibid. 19 (1967), 115.

[4] P. T. Shao, *On the distribution of the values of a class of arithmetical functions*. Bull. Acad. Polon. Sci. Cl. III 4 (1956), 569–572.

[5] P. Turán, *On a theorem of Hardy and Ramajunan*. J. London Math. Soc. 9 (1934), 274–276.

[6] Y. Wang, *A note on some properties of the arithmetical functions $\varphi(n)$, $\sigma(n)$ and $d(n)$*. Acta Math. Sinica 8 (1958), 1–11.

Originally published in
Colloquium Mathematicum XIII (1964), 95–99

On the functions $\varphi(n)$ and $\sigma(n)$

with A. Mąkowski (Warsaw)

In this paper $\varphi(n)$ and $\sigma(n)$ denote the Euler function and the sum of the divisors of n, respectively, p denotes odd primes, p_i the i-th prime.

It has been asked in [5] whether the inequality

$$\liminf \frac{\overbrace{\sigma \ldots \sigma}^{k \text{ times}}(n)}{n} < \infty$$

holds for every k and it has been remarked that for $k = 2$ the affirmative answer follows from a certain deep theorem of Rényi [4]. The aim of this paper is to give an elementary proof of the equality

$$\liminf \frac{\sigma\sigma(n)}{n} = 1$$

and to evaluate other similar limits.

Theorem. *The following formulae hold*:

$$\liminf \frac{\sigma\sigma(n)}{n} = 1, \tag{1}$$

$$\limsup \frac{\varphi\sigma(n)}{n} = \infty, \tag{2}$$

$$\limsup \frac{\varphi\varphi(n)}{n} = \frac{1}{2}, \tag{3}$$

$$\liminf \frac{\sigma\varphi(n)}{n} \leqslant \inf_{4|m} \frac{\sigma\varphi(m)}{m} \leqslant \frac{1}{2} + \frac{1}{2^{34} - 4}. \tag{4}$$

The proof is based on two lemmata. The first is a generalization of a result of Bojanić [2] and is elementary, the second is related to a theorem of Rényi and is used only to show (3) and (4).

Lemma 1. *If a is an integer > 1 and $N(a, p) = (a^p - 1)/(a - 1)$, then*

$$\lim_{p\to\infty} \frac{\varphi\big(N(a, p)\big)}{N(a, p)} = \lim_{p\to\infty} \frac{\sigma\big(N(a, p)\big)}{N(a, p)} = 1.$$

Proof. Put $N(a, p) = N = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_s^{\alpha_s}$, where q_i $(1 \leqslant i \leqslant s)$ are different primes, $\alpha_i \geqslant 1$. Clearly

$$\prod_{i=1}^{s}\Big(1-\frac{1}{q_i}\Big)^{-1} \geqslant \frac{\sigma(N)}{N} \geqslant 1 \geqslant \frac{\varphi(N)}{N} \geqslant \prod_{i=1}^{s}\Big(1-\frac{1}{q_i}\Big). \tag{5}$$

For $p > a+1$, we have $p \nmid a-1$, thus $q_i \equiv 1 \pmod p$ (cf. [3], p. 381) and $q_i > p$ $(i = 1, 2, \ldots, s)$. It follows that

$$N \geqslant p^{\alpha_1+\ldots+\alpha_s} \geqslant p^s$$

and

$$s \leqslant \frac{\log N}{\log p} = \frac{\log\Big(\dfrac{a^p-1}{a-1}\Big)}{\log p} < \frac{\log a^p}{\log p} = \frac{p\log a}{\log p}\,.$$

Hence

$$\prod_{i=1}^{s}\Big(1-\frac{1}{q_i}\Big) \geqslant \Big(1-\frac{1}{p}\Big)^s > \Big(1-\frac{1}{p}\Big)^{p\log a/\log p} \to 1. \tag{6}$$

The lemma follows from (5) and (6). □

Lemma 2. *The following formula holds*:

$$\limsup \frac{\varphi\big(\frac12(p-1)\big)}{\frac12(p-1)} = \liminf \frac{\sigma\big(\frac12(p-1)\big)}{\frac12(p-1)} = 1.$$

Proof. Clearly

$$\frac{\varphi\big(\frac12(p-1)\big)}{\frac12(p-1)} \leqslant 1 \leqslant \frac{\sigma\big(\frac12(p-1)\big)}{\frac12(p-1)}\,. \tag{7}$$

On the other hand, it has been proved by Wang ([6], Appendix, formulae (7) and (8)) that

$$P_\omega(x, q, x^{1/6.5q}) > 12.9\eta\,\frac{c_q(x)}{\varphi(q)\log^2 x} + O\Big(\frac{c_q x}{\log^3 x}\Big).$$

Here, $P_\omega(x, q, \xi)$ is the number of primes p satisfying $p \leqslant x$, $p \equiv a \pmod q$, $p \not\equiv a_i \pmod{p_i'}$ $(i = 1, \ldots, r)$, where $\omega = \langle a, q, a_i\ (1 \leqslant i \leqslant r)\rangle$ is a sequence of integers such that $q \leqslant x$, $(a, q) = 1$, $a_i \not\equiv 0 \pmod{p_i'}$ and p_i' are all primes $\leqslant \xi$ not dividing $2q$; c_q is a certain positive constant (cf. [6], formula (6)), $\eta = \delta/(\delta-1)$, where as stated on p. 1054 one can take $\delta = 1.5$. It follows after the substitution $\omega = \langle 3, 4, \overbrace{1, \ldots, 1}^{r \text{ times}}\rangle$ that there exist infinitely many primes p such that every prime factor of $(p-1)/2$ is greater than $p^{1/20}$. Let ε be any number > 0 and take p of the above kind greater than $20^{20}\varepsilon^{-20}$. Let

$$\tfrac12(p-1) = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_s^{\alpha_s},$$

where q_i $(1 \leqslant i \leqslant s)$ are different primes and $\alpha_i \geqslant 1$. Clearly $s < 20$, and

$$\prod_{i=1}^{s}\Big(1 - \frac{1}{q_i}\Big) > \Big(1 - \frac{1}{p^{1/20}}\Big)^{20} > 1 - \frac{20}{p^{1/20}} > 1 - \varepsilon.$$

On the other hand,

$$\prod_{i=1}^{s}\Big(1 - \frac{1}{q_i}\Big)^{-1} \geqslant \frac{\sigma\big(\frac{1}{2}(p-1)\big)}{\frac{1}{2}(p-1)} \geqslant \frac{\varphi\big(\frac{1}{2}(p-1)\big)}{\frac{1}{2}(p-1)} \geqslant \prod_{i=1}^{s}\Big(1 - \frac{1}{q_i}\Big).$$

It follows that

$$(1-\varepsilon)^{-1} > \frac{\sigma\big(\frac{1}{2}(p-1)\big)}{\frac{1}{2}(p-1)} \geqslant \frac{\varphi\big(\frac{1}{2}(p-1)\big)}{\frac{1}{2}(p-1)} > 1 - \varepsilon.$$

In view of (7), this completes the proof. □

Proof of the Theorem. We begin with formula (1). For any $\varepsilon > 0$ we take a prime $r > 1 + \varepsilon^{-1}$ and put $a = r$ in Lemma 1. We have $N(r, p) = \sigma(r^{p-1})$. Hence

$$\lim_{p\to\infty} \frac{\sigma\sigma(r^{p-1})}{r^{p-1}} = \lim_{p\to\infty} \frac{\sigma\sigma(r^{p-1})}{\sigma(r^{p-1})} \cdot \frac{\sigma(r^{p-1})}{r^{p-1}}$$
$$= \lim_{p\to\infty} \frac{\sigma\big(N(r,p)\big)}{N(r,p)} \cdot \lim_{p\to\infty} \frac{\sigma(r^{p-1})}{r^{p-1}} = \frac{r}{r-1} < 1 + \varepsilon.$$

Since $\sigma\sigma(n)/n \geqslant 1$ for all n, formula (1) is proved.

Proof of formula (2) is similar. For any M we take a number t such that

$$\prod_{i=1}^{t} \frac{p_i}{p_i - 1} > M$$

and put successively $a = p_1, p_2, \ldots, p_t$ in Lemma 1. We have

$$\sigma\Big(\prod_{i=1}^{t} p_i^{p-1}\Big) = \prod_{i=1}^{t} N(p_i, p).$$

Hence

$$\limsup_{p\to\infty} \frac{\varphi\sigma\Big(\prod_{i=1}^{t} p_i^{p-1}\Big)}{\prod_{i=1}^{t} p_i^{p-1}} = \limsup_{p\to\infty} \frac{\varphi\Big(\prod_{i=1}^{t} N(p_i,p)\Big)}{\prod_{i=1}^{t} p_i^{p-1}} \geqslant \limsup_{p\to\infty} \prod_{i=1}^{t} \frac{\varphi\big(N(p_i,p)\big)}{p_i^{p-1}}$$
$$= \prod_{i=1}^{t} \lim_{p\to\infty} \frac{\varphi\big(N(p_i,p)\big)}{N(p_i,p)} \cdot \prod_{i=1}^{t} \lim_{p\to\infty} \frac{N(p_i,p)}{p_i^{p-1}} = \prod_{i=1}^{t} \frac{p_i}{p_i - 1} > M.$$

This completes the proof of (2).

Formula (3) follows at once from Lemma 2, since

$$\limsup_{p\to\infty}\frac{\varphi\varphi(p)}{p}=\limsup_{p\to\infty}\frac{\varphi(p-1)}{p}\geqslant\limsup_{p\to\infty}\frac{\varphi\left(\frac{1}{2}(p-1)\right)}{\frac{1}{2}(p-1)}\cdot\frac{p-1}{2p},$$

and, on the other hand, $\varphi\varphi(n)/n\leqslant\frac{1}{2}$ for all $n>1$.

In order to prove formula (4) assume that m is any positive integer divisible by 4. By Lemma 2

$$\liminf_{p\to\infty}\frac{\sigma\varphi\left(\frac{1}{2}mp\right)}{\frac{1}{2}mp}\leqslant\liminf_{p\to\infty}\frac{\sigma\left(2\varphi(\frac{1}{2}m)\right)\sigma\left(\frac{1}{2}(p-1)\right)}{\frac{1}{2}mp}$$
$$=\frac{\sigma\varphi(m)}{m}\cdot\liminf_{p\to\infty}\frac{\sigma\left(\frac{1}{2}(p-1)\right)}{\frac{1}{2}p}=\frac{\sigma\varphi(m)}{m}.$$

Since

$$\frac{\sigma\varphi(2^{34}-4)}{2^{34}-4}=\frac{2^{33}-1}{2^{34}-4}=\frac{1}{2}+\frac{1}{2^{34}-4},$$

the proof of the theorem is complete. □

The following equalities supplement the theorem:

$$\limsup\frac{\sigma\sigma(n)}{n}=\infty, \tag{8}$$

$$\liminf\frac{\varphi\sigma(n)}{n}=0, \tag{9}$$

$$\liminf\frac{\varphi\varphi(n)}{n}=0, \tag{10}$$

$$\limsup\frac{\sigma\varphi(n)}{n}=\infty. \tag{11}$$

Equalities (8) and (10) are trivial, equalities (9) and (11) have been proved by Alaoglu and Erdős [1]. In that paper the following conjecture has been announced: *for sufficiently large n the sequence*

$$\sigma(n),\sigma\sigma(n),\varphi\sigma\sigma(n),\sigma\varphi\sigma\sigma(n),\ldots$$

tends to infinity. We remark that this conjecture implies the finiteness of the set of Mersenne primes. Indeed, if 2^p-1 is a prime, then

$$\varphi\sigma\sigma(2^{p-1})=\varphi\sigma(2^p-1)=\varphi(2^p)=2^{p-1},$$

and the sequence in question is periodical.

It seems a natural question to ask whether formula (4) can be improved. Mrs. K. Kuhn has investigated the quotient $\sigma\varphi(n)/n$ for n having at most 6 prime factors and has found that $\sigma\varphi(n)/n\geqslant\frac{1}{2}$ for such n's, the equality being realized only if $n=2^{2^i+1}-2$ $(0\leqslant i\leqslant 5)$. This suggests a problem

P486. Is the inequality $\sigma\varphi(n)/n\geqslant\frac{1}{2}$ true for all n ?

Remark. Even the weaker inequality $\inf \sigma\varphi(n)/n > 0$ remains still unproved.

References

[1] L. Alaoglu, P. Erdős, *A conjecture in elementary number theory*. Bull. Amer. Math. Soc. 50 (1944), 881–882.

[2] R. Bojanić, *Solution to problem 4590*. Amer. Math. Monthly 62 (1955), 498–499.

[3] L. E. Dickson, *History of the Theory of Numbers*, vol. I. Chelsea, New York 1952.

[4] A. Rényi, *On the representation of an even number as the sum of a prime and of an almost prime*. Izv. Akad. Nauk SSSR Ser. Mat. 12 (1948), 57–78 (Russian); English transl.: Amer. Math. Soc. Transl. (2), 19 (1962), 299–321.

[5] A. Schinzel, *Ungelöste Probleme, Nr. 30*. Elem. Math. 14 (1959), 60–61.

[6] Y. Wang, *On the representation of large integer as a sum of prime and an almost prime*. Sci. Sinica 11 (1962), 1033–1054.

Originally published in
Colloquium Mathematicum LXVIII (1995), 55–58

On integers not of the form $n - \varphi(n)$

with J. Browkin (Warszawa)

W. Sierpiński asked in 1959 (see [4], pp. 200–201, cf. [2]) whether there exist infinitely many positive integers not of the form $n - \varphi(n)$, where φ is the Euler function. We answer this question in the affirmative by proving

Theorem. *None of the numbers* $2^k \cdot 509203$ $(k = 1, 2, \dots)$ *is of the form* $n - \varphi(n)$.

Lemma 1. *The number* 1018406 *is not of the form* $n - \varphi(n)$.

Proof. Suppose that

$$10108406 = n - \varphi(n) \tag{1}$$

and let

$$n = \prod_{i=1}^{j} q_i^{\alpha_i} \quad (q_1 < q_2 < \ldots < q_j \text{ primes}). \tag{2}$$

If for any $i \leqslant j$ we have $\alpha_i > 1$ it follows that $q_i \mid 2 \cdot 509203$, and since 509203 is a prime, either $q_i = 2$ or $q_i = 509203$. In the former case $n - \varphi(n) \equiv 0 \not\equiv 10108406 \pmod 4$, in the latter case $n - \varphi(n) > 1018406$, hence

$$\alpha_i = 1 \quad (1 \leqslant i \leqslant j). \tag{3}$$

Since $n > 2$ we have $\varphi(n) \equiv 0 \pmod 2$, hence $n \equiv 0 \pmod 2$. However, $n/2$ cannot be a prime since 1018405 is composite. Hence $\varphi(n) \equiv 0 \pmod 4$ and $n \equiv 2 \pmod 4$. Moreover, $n \equiv 1 \pmod 3$ would imply $\varphi(n) \equiv n - 1018406 \equiv 2 \pmod 3$, which is impossible, since

$$\varphi(n) \equiv \begin{cases} 0 \pmod 3 & \text{if at least one } q_i \equiv 1 \pmod 3, \\ 1 \pmod 3 & \text{otherwise.} \end{cases}$$

Hence $n \equiv 2 \pmod{12}$ or $n \equiv 6 \pmod{12}$ and

$$n - \varphi(n) > \frac{1}{2} n. \tag{4}$$

Let p_i denote the ith prime and consider first the case $n = 12k + 2$. We have $q_1 = 2$, $q_i \geqslant p_{i+1}$ $(i \geqslant 2)$. Since

$$\prod_{i=2}^{7} p_{i+1} > 1018406, \tag{5}$$

it follows from (1)–(4) that $j \leqslant 6$ and

$$\frac{1}{2}\prod_{i=2}^{6}\Big(1 - \frac{1}{p_{i+1}}\Big) \leqslant \frac{\varphi(n)}{n} \leqslant \begin{cases} 2/5 & \text{if } n \equiv 0 \pmod 5, \\ 1/2 & \text{otherwise.} \end{cases}$$

Hence if $n = 12k + 2$ satisfies (1) we have either $116381 < k < 141446$ or $141446 \leqslant k < 169735$ and $k \not\equiv 4 \pmod 5$.

Consider now $n = 12k + 6$. Here $q_1 = 2$, $q_2 = 3$, $q_i \geqslant p_i$. By (1)–(5), $j \leqslant 7$ and

$$\prod_{i=1}^{7}\Big(1 - \frac{1}{p_i}\Big) \leqslant \frac{\varphi(n)}{n} \leqslant \frac{1}{3}.$$

Hence if $n = 12k + 6$ satisfies (1) we have

$$103561 < k < 127301.$$

The computation performed on the computer SUN/SPARC of the Institute of Applied Mathematics and Mechanics of the University of Warsaw using the program GP/PARI has shown that no n corresponding to k in the indicated range satisfies (1). □

Lemma 2. *All the numbers* $2^k \cdot 509203 - 1$ $(k = 1, 2, \dots)$ *are composite.*

Proof. We have

$$509203 \equiv 2^{a_i} \pmod{q_i},$$

where $\langle q_i, a_i\rangle$ is given by $\langle 3, 0\rangle$, $\langle 5, 3\rangle$, $\langle 7, 1\rangle$, $\langle 13, 5\rangle$, $\langle 17, 1\rangle$ and $\langle 241, 21\rangle$ for $i = 1, 2, \dots, 6$, respectively. Now, 2 belongs mod q_i to the exponent m_i, where $m_i = 2, 4, 3, 12, 8$ and 24 for $i = 1, 2, \dots, 6$, respectively.

It is easy to verify that every integer n satisfies one of the congruences

$$n \equiv -a_i \pmod{m_i} \quad (1 \leqslant i \leqslant 6).$$

If $k \equiv -a_j \pmod{m_j}$ we have

$$2^k \cdot 509203 \equiv 2^{a_j - a_j} \equiv 1 \pmod{q_j},$$

and since $2^k \cdot 509203 - 1 > q_j$ the number $2^k \cdot 509203 - 1$ is composite. □

Remark 1. Lemma 2 was proved by H. Riesel, already in 1956 (see [3], Anhang).

The following problem, implicit in [1], suggests itself.

Problem 1. What is the least positive integer n such that all integers $2^k n - 1$ $(k = 1, 2, \dots)$ are composite?

Proof of the theorem. We shall prove that $n - \varphi(n) \neq 2^k \cdot 509203$ by induction on k. For $k = 1$ this holds by virtue of Lemma 1. Assume that this holds with k replaced by $k - 1$ ($k \geqslant 2$) and that

$$n - \varphi(n) = 2^k \cdot 509203. \tag{6}$$

If $\varphi(n) \equiv 0 \pmod 4$ we have $n \equiv 0 \pmod 4$ and

$$\frac{n}{2} - \varphi\Big(\frac{n}{2}\Big) = 2^{k-1} \cdot 509203,$$

contrary to the inductive assumption. Thus $\varphi(n) \equiv 2 \pmod 4$ and $n = 2p^\alpha$, where p is an odd prime. From (6) we obtain

$$p^{\alpha-1}(p+1) = 2^k \cdot 509203.$$

By Lemma 2, $\alpha = 1$ is impossible. If $\alpha > 1$ we have

$$p \mid 2^k \cdot 509203,$$

and since 509203 is a prime, $p = 509203$, $\alpha = 2$ and

$$509204 = 2^k,$$

which is impossible. The inductive proof is complete. □

Remark 2. D. H. Lehmer on the request of one of us has kindly computed the table of all numbers not of the form $n - \varphi(n)$ up to 50 000. This table and its prolongation up to 100 000 seems to indicate that the numbers not of the form $n - \varphi(n)$ have a positive density, about 1/10.

This suggests

Problem 2. Have the integers not of the form $n - \varphi(n)$ a positive lower density?

Added in proof (November 1994). A computation performed by A. Odlyzko has shown that there are 561 850 positive integers less than 5 000 000 not of the form $n - \varphi(n)$.

References

[1] A. Aigner, *Folgen der Art $ar^n + b$, welche nur teilbare Zahlen liefern*. Math. Nachr. 23 (1961), 259–264.

[2] P. Erdős, *Über die Zahlen der Form $\sigma(n) - n$ und $n - \varphi(n)$*. Elem. Math. 28 (1973), 83–86.

[3] W. Keller, *Woher kommen die größten derzeit bekannten Primzahlen?* Mitt. Math. Ges. Hamburg 12 (1991), 211–229.

[4] W. Sierpiński, *Teoria liczb*, część 2 (*Number Theory*, Part II). Monografie Matematyczne 38, PWN, Warszawa 1959.

Part H

Divisibility and congruences

Commentary on H: Divisibility and congruences

by H. W. Lenstra jr.

The eleven papers in Section H are naturally divided in two categories: four papers in elementary number theory, and seven papers on local-global results concerning exponential equations.

The four papers **H1**, **H3**, **H6**, **H8** in the first category show Schinzel's resourcefulness in elementary arithmetic. Problem **P217**, formulated in **H1**, has been studied by E. Burkacka and J. Piekarczyk in their master dissertations at the University of Warsaw; see *Colloq. Math.* 10 (1963), 365. The joint paper **H6** with G. Baron, which has a combinatorial flavour, has applications in ring theory. An algebraic proof of the main result of this paper was obtained by M. Van Den Bergh and M. Van Gastel [5]. Especially noteworthy is the joint paper **H8** with J. Wójcik, which was suggested by work in group theory. The theme of the paper is reminiscent of the local-global results discussed below, but the tools used are quite different and more elementary. A negative answer to the question posed at the end of the paper was given by J. Wójcik [7].

The seven papers **H2**, **H4**, **H5**, **H7**, **H9**, **H10**, **H11** in the second category address fundamental issues related to exponential diophantine equations, the emphasis being on local-global results such as the following Theorem 2 from **H4**: *if H is a finitely generated subgroup of the multiplicative group of an algebraic number field K, and a non-zero element $b \in K$ has the property that for almost all primes $\mathfrak{p}$ of K the element $b \bmod \mathfrak{p}$ belongs to $H \bmod \mathfrak{p}$, then b belongs to H*. The result admits numerous variations and applications, and Schinzel investigated many of them. His work helped inspire a development in which the role of the multiplicative group is played by general algebraic groups. A good discussion and a substantial bibliography can be found in a paper by E. Kowalski [1].

The technique used by Schinzel in most papers in the second category, consists of combining density theorems from algebraic number theory with information on Galois groups of field extensions obtained by adjoining radicals. Several of Schinzel's auxiliary results on such Galois groups are new. The most notable one (**H5**, Theorem 2) asserts the following. *Let K be a field, n a positive integer not divisible by the characteristic of K, and w the number of nth roots of unity in K. Then, for $a \in K$, the Galois group of $X^n - a$ over K is abelian if and only if there exists $b \in K$ with $a^w = b^n$*. This basic result has been finding its way into the field-theoretic literature as *Schinzel's theorem*. It is important in the context of Stark's conjectures (J. Tate, [4]; see Chapitre IV, Exercice 1.4).

One also encounters Schinzel's theorem when one attempts to describe, for any field K with algebraic closure $\bar{K}$, the Galois group of the "maximal radical extension" of K, which one obtains by adjoining all $\alpha \in \bar{K}$ for which there exists an integer n not divisible by the characteristic of K with $\alpha^n \in K$.

P. Stevenhagen ([3], cf. [6]) gave a proof of Schinzel's theorem that is so elegant that it deserves to be included here. We may assume $a \neq 0$. Denote by L the splitting field of $X^n - a$ over K, and generally by ζ_m a primitive mth root of unity. First suppose $a^w = b^n$ with $b \in K$. Then L is contained in the composite of the Kummer extension $K(b^{1/w})$ and the cyclotomic extension $K(\zeta_{wn})$ of K. Both of these extensions are abelian, and therefore so is L. For the converse, suppose L has an abelian Galois group G. We fix an nth root α of a in L. For each $\sigma \in G$, one has $\sigma(\alpha)/\alpha = \zeta_\sigma \in \langle \zeta_n \rangle$, and $\sigma(\zeta_n) = \zeta_n^{c(\sigma)}$ with $c(\sigma) \in \mathbb{Z}$. For any $\sigma, \tau \in G$ one has $\tau(\alpha^{c(\sigma)})/\alpha^{c(\sigma)} = \zeta_\tau^{c(\sigma)} = \sigma(\tau(\alpha)/\alpha) = \tau\sigma(\alpha)/\sigma(\alpha)$; hence $\alpha^{c(\sigma)}/\sigma(\alpha)$ is fixed by all τ so belongs to K, and taking the nth power one sees that $a^{c(\sigma)-1} \in K^{*n}$. Thus, if v denotes the gcd of n and all numbers $c(\sigma) - 1$ (for $\sigma \in G$), then one has $a^v \in K^{*n}$. To finish the proof it suffices to show $v = w$. A divisor d of n divides v if and only if d divides all numbers $c(\sigma) - 1$, if and only if all elements $\sigma(\zeta_d)/\zeta_d = \zeta_d^{c(\sigma)-1}$ are 1, if and only if $\zeta_d \in K$, and if and only if d divides w. Therefore we have $v = w$, as required.

The Corollary to Theorem 5 in **H5** has the condition $a \neq d^3 + 3d$. Schinzel himself proved that this condition can be omitted [2].

References

[1] E. Kowalski, *Some local-global applications of Kummer theory*. Manuscripta Math. 111 (2003), 105–139.

[2] A. Schinzel, *On the congruence* $u_n \equiv c \pmod{\mathfrak{p}}$*, where* u_n *is a recurring sequence of the second order*. Acta Acad. Paedagog. Agriensis Sect. Mat. (N.S.) 30 (2003), 147–165.

[3] P. Stevenhagen, *Ray class groups and governing fields*. Thesis, Universiteit van Amsterdam, 1989.

[4] J. Tate, *Les conjectures de Stark sur les fonctions L d'Artin en* $s = 0$. Progr. Math. 47, Birkhäuser, Boston 1984.

[5] M. Van Den Bergh, M. Van Gastel, *On the structure of non-commutative regular local rings of dimension two*. Comm. Algebra 30 (2002), 4575–4588.

[6] J. Wójcik, *Criterion for a field to be abelian*. Colloq. Math. 68 (1995), 187–191.

[7] —, *On a problem in algebraic number theory*. Math. Proc. Cambridge Philos. Soc. 119 (1996), 191–200.

Originally published in
Colloquium Mathematicum V (1958), 198–204

Sur un problème de P. Erdős

Désignons pour k naturels et n entiers par $H_{k,n}$ la proposition suivante :

$H_{k,n}$: *il existe un entier* i *tel que* $0 \leqslant i < k$ *et* $n - i \mid \binom{n}{k}$.

P. Erdős a posé le problème, *si* $H_{k,n}$ *subsiste pour tous les nombres naturels* k *et* $n \geqslant 2k$. La réponse à ce problème est négative, comme le prouve l'exemple $k = 15, n = 99215$. En effet, les décompositions en facteurs premiers

$$99215 = 5 \cdot 19843, \quad 99214 = 2 \cdot 113 \cdot 439, \quad 99213 = 3 \cdot 33071,$$
$$99212 = 2^2 \cdot 17 \cdot 1459, \quad 99211 = 7 \cdot 14173, \quad 99210 = 2 \cdot 3 \cdot 5 \cdot 3307,$$
$$99209 = 11 \cdot 29 \cdot 311, \quad 99208 = 2^3 \cdot 12401, \quad 99207 = 3^2 \cdot 73 \cdot 151,$$
$$99206 = 2 \cdot 49603, \quad 99205 = 5 \cdot 19841, \quad 99204 = 2^2 \cdot 3 \cdot 7 \cdot 1181,$$
$$99203 = 13^2 \cdot 587, \quad 99202 = 2 \cdot 193 \cdot 257, \quad 99201 = 3 \cdot 43 \cdot 769$$

entraînent que

1° $\binom{n}{k} = 13P$, où $(P, 15!) = 1$,
2° chacun des nombres $n - i$ $(0 \leqslant i < k)$ a un diviseur premier $p_i < 15$.

Donc, si l'on avait $n - i \mid \binom{n}{k}$ pour un i, où $0 \leqslant i < k$, on aurait $p_i \mid \binom{n}{k} = 13P$, donc

$$p_i = 13 \mid n - i, \quad n - i = 99203, \quad 13^2 \mid n - i \mid \binom{n}{k} = 13P, \quad 13 \mid P,$$

ce qui implique une contradiction.

On peut démontrer que la proposition $H_{k,n}$ est vraie pour $k < 15$, $n \geqslant 2k$ et pour $k = 15$, $30 \leqslant n < 99215$.

En omettant la démonstration assez pénible de ce dernier fait, j'indiquerai plus loin certaines méthodes d'examiner si pour un k fixé, il existe un n pour lequel $H_{k,n}$ est un défaut.

Je commencerai par les remarques suivantes.

1. Soit $n_1 \equiv n_2 \pmod{k!}$. Alors on l'équivalence $H_{n_1,k} \equiv H_{n_2,k}$.

En effet, on a

$$n_1 - i \mid \binom{n_1}{k}$$

dans ce et seulement dans ce cas $n_1 \cdots (n_1 - i + 1)(n_1 - i - 1) \cdots (n_1 - k + 1) \equiv 0 \pmod{k!}$, c'est-à-dire, si $n_2 \cdots (n_2 - i + 1)(n_2 - i - 1) \cdots (n_2 - k + 1) \equiv 0 \pmod{k!}$, ce

qui équivaut à

$$n_2 - i \mid \binom{n_2}{k}.$$

Il en résulte que si pour un nombre naturel k donné il existe un nombre naturel $n \geqslant 2k$ tel que la proposition $H_{k,n}$ est fausse, il existe une infinité de tels nombres naturels n.

2. On a l'équivalence $H_{k,n} \equiv H_{k,-n+k-1}$.

En effet, vu l'identité

$$\binom{n}{k} = (-1)^k \binom{-n+k-1}{k},$$

on a la formule $n - i \mid \binom{n}{k}$, où $0 \leqslant i < k$, dans ce et seulement dans ce cas, si

$$(-n+k-1) - j \mid \binom{-n+k-1}{k}, \quad \text{où} \quad 0 \leqslant j = k - i - 1 < k.$$

La proposition $H_{k,n}$ étant vraie pour $0 \leqslant n < 2k$ (ce qu'on déduit sans peine du théorème de Tchebycheff), il résulte de la remarque 2 que si $H_{k,n}$ est vraie pour le nombre naturel k et pour les entiers $n \geqslant 2k$, elle est vraie pour n entier quelconque.

Désignons par H_k la proposition affirmant que $H_{k,n}$ subsiste pour tout entier n.

Lemme 1. *S'il existe pour k et n donnés un i tel que $0 \leqslant i < k$, $\left(n - i, \binom{k}{i}(k-i)\right) = 1$, la proposition $H_{k,n}$ est vraie.*

Démonstration. On a l'identité

$$\binom{n}{k}\binom{k}{i}(k-i) = \binom{n}{i}\binom{n-i-1}{k-i-1}(n-i).$$

Donc, si pour un i, $0 \leqslant i < k$, $\left(n - i, \binom{k}{i}(k-i)\right) = 1$, on a $n - i \mid \binom{n}{k}$. □

Théorème 1. *La proposition H_k est vraie pour $k = p^\alpha$, où p est un nombre premier et α un entier $\geqslant 0$.*

Démonstration. Si $(n, p) = 1$, on a

$$\left(n - 0, \binom{k}{0}(k-0)\right) = (n, k) = (n, p^\alpha) = 1.$$

Or, si $(n, p) > 1$, on a $p \mid n$ donc $(n+1, p) = 1$ et

$$\left(n - (k-1), \binom{k}{k-1}(k-(k-1))\right) = (n-k+1, k) = (n+1, k) = (n+1, p^\alpha) = 1.$$

Dans tous les deux cas $H_{k,n}$ est vraie d'après le Lemme 1. □

Théorème 2. *La proposition H_k est vraie pour $k = 6, 10, 12, 14, 18, 20, 24, 26, 28, 30$.*

Démonstration. À titre d'exemple nous donnerons la démonstration pour $k = 30$. Pour les autres k la démonstration est analogue.

Supposons d'abord que $n \equiv 0 \pmod 2$. La vérité de $H_{k,n}$ résulte alors du Lemme 1 dans lequel selon les restes de n de la division par 3, 5, 29, 7, 13, 23 et 11 on substitue les valeurs envisagées dans la table suivante, pour lesquels on a $\left(n-i, \binom{30}{i}(30-i)\right) = 1$:

le reste de la division de n par					
3	5	29	7	13	i
$n \not\equiv 2$	$n \not\equiv 4$				29
0	4	$n \not\equiv 1$			1
0	4	1	$n \not\equiv 4$	$n \not\equiv 12$	25
0	4	1	$n \not\equiv 5$	12	5
0	4	1	5	12	23
0	4	1	4	$n \not\equiv 5$	5
0	4	1	4	5	23
1	4	$n \not\equiv 27$	$n \not\equiv 6$		27
1	4	$n \not\equiv 3$	6		3
1	4	3	6	$n \not\equiv 5$	5
1	4	3	6	5	23
1	4	27	$n \not\equiv 3$		3
1	4	27	3	$n \not\equiv 5$	5
1	4	27	3	5	23
2	$n \not\equiv 1$	$n \not\equiv 1$			1
2	$n \not\equiv 2$	1	$n \not\equiv 6$		27
2	$n \not\equiv 3$	1	6		3
2	1	$n \not\equiv 27$	$n \not\equiv 6$		27
2	1	$n \not\equiv 3$	6		3
2	1	3	6	$n \not\equiv 12$	25

le reste de la division de n par							
3	5	29	7	13	23	11	i
2	1	3	6	12	$n \not\equiv 7$		7
2	1	3	6	12	7	$n \not\equiv 9$	9
2	1	3	6	12	7	9	19
2	1	27	$n \not\equiv 3$				3
2	1	27	3	$n \not\equiv 12$			25
2	1	27	3	12	$n \not\equiv 7$		7
2	1	27	3	12	7	$n \not\equiv 9$	9
2	1	27	3	12	7	9	19
2	2	1	$n \not\equiv 3$				3
2	2	1	3	$n \not\equiv 12$			25
2	2	1	3	12	$n \not\equiv 21$	$n \not\equiv 10$	21
2	2	1	3	12	$n \not\equiv 9$	10	9
2	2	1	3	12	9	10	19
2	2	1	3	12	21	$n \not\equiv 9$	9
2	2	1	3	12	21	9	19
2	3	1	6	$n \not\equiv 12$			25
2	3	1	6	12	$n \not\equiv 7$		7
2	3	1	6	12	7	$n \not\equiv 10$	21
2	3	1	6	12	7	10	9

Le cas $n \equiv 1 \pmod 2$ qui reste à examiner se réduit au précédant d'après la remarque 2 et la congruence $-n + k - 1 \equiv -n + 29 \equiv 0 \pmod 2$. □

Lemme 2. *Soient* $2 = p_1 < p_2 < \ldots < p_l \leqslant k$ *tous les nombres premiers* $\leqslant k$. *S'il existe un système des entiers* $a(p_1), a(p_2), \ldots, a(p_l)$ *tel que*

1° *tout entier* i, $0 \leqslant i < k$, *satisfait à une des congruences* $i \equiv a(p_j) \pmod{p_j}$ $(1 \leqslant j \leqslant l)$,

2° *quel que soit le nombre naturel* $j \leqslant l$, *on a*

$$\left[\frac{k}{p_j}\right] + \left[\frac{a(p_j) - k}{p_j}\right] = \left[\frac{a(p_j)}{p_j}\right],$$

alors H_k *est en défaut.*

Démonstration. Supposons que le système $a(p_j)$ $(1 \leqslant j \leqslant l)$ satisfait aux conditions 1°–2°. Posons

$$\alpha_j = \left[\frac{\ln k}{\ln p_j}\right] + 1, \quad \bar{a}(p_j) = a(p_j) - \left[\frac{a(p_j)}{p_j}\right] p_j.$$

D'après 2° on a pour $j \leqslant l$

$$\left[\frac{k}{p_j}\right] + \left[\frac{\bar{a}(p_j) - k}{p_j}\right] = \left[\frac{\bar{a}(p_j)}{p_j}\right] = 0. \tag{1}$$

D'après le théorème chinois sur les restes il existe un entier n tel que

$$n \equiv \bar{a}(p_j) - p_j \pmod{p_j^{\alpha_j}} \quad (1 \leqslant j \leqslant l). \tag{2}$$

Admettons que, pour un certain i_0, $0 \leqslant i_0 < k$ et

$$n - i_0 \mid \binom{n}{k}. \tag{3}$$

D'après la condition 1° il existe un $j_0 \leqslant l$ tel que $i_0 \equiv \bar{a}(p_{j_0}) \pmod{p_{j_0}}$, d'où, d'après (2), $n - i_0 \equiv 0 \pmod{p_{j_0}}$ et d'après (3)

$$p_{j_0} \mid \binom{n}{k}. \tag{4}$$

D'autre part, parmi les nombres $n - i$ $(0 \leqslant i < k)$ les seuls nombres divisibles par p_{j_0} sont, d'après (2), les nombres $n - i(t)$, où

$$i(t) = \bar{a}(p_{j_0}) + tp_{j_0}, \quad 0 \leqslant t \leqslant -\left[\frac{\bar{a}(p_{j_0}) - k}{p_{j_0}}\right] - 1.$$

Or, d'après (1),

$$\left[\frac{\bar{a}(p_{j_0}) - k}{p_{j_0}}\right] = -\left[\frac{k}{p_{j_0}}\right],$$

donc $i(t) \leqslant \bar{a}(p_{j_0}) + [k/p_{j_0}]p_{j_0} - p_{j_0}$, d'où $0 < -\bar{a}(p_{j_0}) + p_{j_0} + i(t) \leqslant k < p_{j_0}^{\alpha_{j_0}}$.

D'autre part, d'après (2), $-\bar{a}(p_{j_0}) + p_{j_0} + i(t) \equiv -[n - i(t)] \pmod{p_{j_0}^{\alpha_{j_0}}}$. Donc p_{j_0} figure dans le développement de $-\bar{a}(p_{j_0}) + p_{j_0} + i(t)$ en facteurs premiers avec le même exposant que dans le développement de $n - i(t)$.

On a donc $\left(p_{j_0}, \binom{n}{k}\right) = 1$, contrairement à la formule (4), ce qui achève la démonstration. □

Théorème 3. *S'il existe un système de nombres premiers* $\leqslant k$,

$$Q(k) = \{q_1, q_2, \ldots, q_m\}$$

tel que pour tout nombre $s = q_1^{\beta_1} q_2^{\beta_2} \cdots q_m^{\beta_m} \leqslant k$, *où* $\beta_1, \beta_2, \ldots, \beta_m \geqslant 0$, *on a* $(k + 1 - s, q_1 q_2 \cdots q_m) > 1$, *alors* H_k *est en défaut.*

Démonstration. Soient $r_1, r_2, \ldots, r_{l-m}$ tous les nombres premiers $\leqslant k$ qui n'appartiennent pas à $Q(k)$ et posons $a(q_j) = -1, a(r_j) = k$. Nous prouverons que le système des nombres a ainsi défini remplit les conditions 1° et 2° du Lemme 2.

1° Pour tout nombre i, $0 \leqslant i < k$, on a

$$k - i = q_1^{\beta_1} q_2^{\beta_2} \cdots q_m^{\beta_m} \cdot r_1^{\gamma_1} r_2^{\gamma_2} \cdots r_{l-m}^{\gamma_{l-m}}, \quad \text{où} \quad \beta_1, \ldots, \beta_m, \gamma_1, \ldots, \gamma_{l-m} \geqslant 0.$$

Donc $(k - i, r_1 r_2 \cdots r_{l-m}) > 1$ ou bien $k - i = q_1^{\beta_1} \cdots q_m^{\beta_m}$.

Dans le premier cas il existe un $j \leqslant l-m$ tel que $i \equiv k = a(r_j) \pmod{r_j}$, et dans le second cas, en posant $s = k-i$, nous obtenons d'après l'hypothèse $(i+1, q_1 q_2 \cdots q_m) > 1$, d'où, pour un certain $j \leqslant m$, $i \equiv -1 = a(q_j) \pmod{q_j}$.

2° Il faut vérifier que

$$\left[\frac{-1-k}{q_j}\right] + \left[\frac{k}{q_j}\right] = -1 \quad (1 \leqslant j \leqslant m)$$

et que

$$\left[\frac{k-k}{r_j}\right] + \left[\frac{k}{r_j}\right] = \left[\frac{k}{r_j}\right] \quad (1 \leqslant j \leqslant l-m).$$

La deuxième de ces égalités est évidente et on obtient la première en changeant le signe dans l'inégalité

$$\left[\frac{k}{q_j}\right] + 1 \geqslant \frac{1+k}{q_j} > \left[\frac{k}{q_j}\right]. \qquad \square$$

Corollaire 1. *La proposition H_k est fausse pour $k = 15, 21, 33, 35, 45, 55, 63, 65, 69, 75, 77, 85, 87, 91, 93, 95, 99$.*

La démonstration résulte du Théorème 3 dans lequel il faut prendre comme $Q(k)$ les systèmes suivants des nombres premiers :

$$Q(15) = \{5, 11\}, \qquad Q(21) = \{5, 7, 17\},$$
$$Q(33) = \{11, 23\}, \qquad Q(35) = \{7, 29\},$$
$$Q(45) = \{3, 19, 37, 43\}, \qquad Q(55) = \{5, 13, 17, 31, 43\},$$
$$Q(63) = \{3, 11, 31, 37, 53, 61\}, \qquad Q(65) = \{13, 53\},$$
$$Q(69) = \{23, 47\}, \qquad Q(75) = \{5, 17, 59, 71\},$$
$$Q(77) = \{11, 67\}, \qquad Q(85) = \{7, 17, 23, 37, 79\},$$
$$Q(87) = \{29, 59\}, \qquad Q(91) = \{13, 79\},$$
$$Q(93) = \{5, 7, 23, 29, 31, 59, 71, 89\}, \qquad Q(95) = \{11, 17, 19, 79\},$$
$$Q(99) = \{11, 89\}.$$

Comme on voit, pour $k = 15, 33, 35, 65, 69, 77, 87, 91, 99$ le système $Q(k)$ est formé de deux nombres. Comme on le vérifie aisément, cela a lieu dans ce et seulement dans ce cas si $k = aq_1$, où les nombres $q_1 > a > 1$ et $q_2 = (a-1)q_1 + 1$ sont tous les deux premiers, donc, par exemple, si $k = 3q_1$, où les nombres $q_1 > 3$ et $2q_1 + 1$ sont tous les deux premiers. Grâce à ce fait, la réponse positive au problème suivant est très probable :

P216. Existe-t-il une infinité de nombres k pour lesquels H_k est fausse ?

Théorème 4. *La proposition H_k est fausse pour $k = 22$.*

La démonstration résulte du Lemme 2 où l'on pose $a(2) = 0$, $a(3) = 1$, $a(5) = 4$, $a(7) = 3$, $a(11) = 10$, $a(13) = 11$, $a(17) = 5$, $a(19) = 15$.

Des théorèmes 1, 2 et 4 et du corollaire 1 il résulte le

Corollaire 2. *La proposition H_k est vraie pour tous les nombres $k \leqslant 33$ sauf pour les nombres $k = 15, 21, 22$ et 33.*

Il se pose ici le problème suivant :

P217. Est-ce que la proposition H_k est vraie pour une infinité de nombres $k \neq p^\alpha$, où p est un nombre premier et α un entier $\geqslant 0$?

Je suppose que la réponse est négative.

Ajouté pendant la correction des épreuves. P. Erdős a demontré que la réponse au Problème P216 est positive. Voici l'esquisse de sa démonstration — l'extrait de sa lettre à l'auteur du 5 février 1957 :

"Let q be a large prime. I want to find an $n = aq$ so that H_n is false. Let $p \equiv 1 \pmod q$, $p = (a_1 - 1)q + 1$, $n_1 = a_1 q$, $p < e^{\sqrt{q}}$ but p so large that the number of primes $\equiv 1 \pmod q$ which are $\leqslant p$ is

$$\big(1 + o(1)\big)\,\frac{p}{q \log p}$$

(such a p exists by Page–Walfisz–Siegel theorem).

Choose $a(q) = 0$, $a(r) = -1$ (r prime) except for a "few" primes p_i which I define now, $a(p) = q - 1$. All the primes p_i for which $a(p_i) \neq -1$ will satisfy $p_i \equiv 1 \pmod q$, $p_i > n/2$. Thus the only numbers $\leqslant n$ which are not yet eliminated by our congruences are $q^2 - 1, q^3 - 1, \ldots, q^k - 1$ ($q^k - 1 < n_1 \leqslant q^{k+1} - 1$).

If there are at least l primes $p_i \equiv 1 \pmod q$ in $(n_1, n_1 - q^l + 1)$ for every $l \geqslant 2$, we successively eliminate these integers by the primes p_i and avoid contradiction against Lemma 2. If not, then for some l there are fewer than l primes $p_i \equiv 1 \pmod q$ in $(n_1 - q^l + 1, n_1)$. Consider then the greatest prime $p_2 \equiv 1 \pmod q$, $p_2 < n_1 - q^l + 1$, put $p_2 = (a_2 - 1)q + 1$, $n_2 = a_2 q$ and repeat the same argument until $n_k < n_1/2$. But then the number of primes $\equiv 1 \pmod q$ in $(n_1/2, n_1)$ is $< n_1/q^2$, but since q was "small" compared with n_1, by Page–Walfisz, the number of these primes is

$$\big(1 + o(1)\big)\frac{n_1}{2q \log n_1} > \frac{n_1}{q^2}$$

if $n_1 < e^{\sqrt{q}}$.

This contradiction shows that before n_k becomes $< n_1/2$, we have that for every $l \geqslant 2$, $(n_k - q^l + 1, n_k)$, where $n_k = a_k q$, $(a_k - 1)q + 1$ is a prime, contains at least l primes $p \equiv 1 \pmod q$ and H_{n_k} is false."

Originally published in
Bulletin de l'Académie Polonaise des Sciences
Série des sci. math., astr. et phys.
VIII (1960), 307–309

On the congruence $a^x \equiv b \pmod{p}$

The aim of this paper is to prove the following theorem signalled in [1].

Theorem. *If a, b are rational integers, $a > 0$ and $b \neq a^k$ (k—rational integer), then there exist an infinite number of rational primes, p, for which the congruence $a^x \equiv b \pmod{p}$ has no solutions in rational integers x.*

Lemma. *Let l be an arbitrary rational prime, ζ_l—a primitive root of unity of order l, $k = \Gamma(\zeta_l)$—the field obtained by adjoining ζ_l to the field Γ of rational numbers. If a system of rational integers $\gamma_1, \gamma_2, \ldots, \gamma_t$ has the property that $\gamma_1^{m_1}\gamma_2^{m_2}\cdots\gamma_t^{m_t}$ is an l-th power of a rational integer only when $l \mid m_i$ $(i = 1, \ldots, t)$, then for arbitrary rational integers $c_1, c_2, \ldots, c_t$ there exists an infinite number of prime ideals $\mathfrak{p}$ of the field k whose degree is 1, and for which*

$$\left(\frac{\gamma_i}{\mathfrak{p}}\right) = \zeta_l^{c_i} \quad (i = 1, 2, \ldots, t).$$

Proof. If the number $\gamma_1^{m_1}\gamma_2^{m_2}\cdots\gamma_t^{m_t}$ is not an l-th power of a rational integer, then the polynomial $x^l - \gamma_1^{m_1}\gamma_2^{m_2}\cdots\gamma_t^{m_t}$ is irreducible over Γ. On the basis of a well known theorem ([2], p. 298, Th. 16) the polynomial remains irreducible over the field $\Gamma(\zeta_l)$, therefore $\gamma_1^{m_1}\gamma_2^{m_2}\cdots\gamma_t^{m_t}$ is not an l-th power of the integer of the field k. The thesis of the lemma follows from this directly, in view of Chebotarev's improvement of a Hilbert's theorem ([3], cf. [4], p. 276, Th. 152). □

Proof of the Theorem. The cases $a = 1$ and $b = 0$ are trivial. Assume that $a > 1$, $b \neq 0$, hence $|ab| > 1$ and let $q_1, q_2, \ldots, q_s$ be all the prime factors of ab.

Let further

$$a = q_1^{\alpha_1}q_2^{\alpha_2}\cdots q_s^{\alpha_s}, \quad b = \pm q_1^{\beta_1}q_2^{\beta_2}\cdots q_s^{\beta_s} \quad (\alpha_i, \beta_i \geqslant 0).$$

If $b < 0$, we observe that the numbers $l = 2$, $t = s + 1$, $\gamma_i = q_i$ $(i = 1, 2, \ldots, s)$, $\gamma_{s+1} = -1$ satisfy the conditions of our Lemma. Then there exists an infinite number of prime ideals $\mathfrak{p}$ of the field $\Gamma(-1)$ (i.e., simply rational primes) for which we have

$$\left(\frac{q_i}{\mathfrak{p}}\right) = 1, \quad \left(\frac{-1}{\mathfrak{p}}\right) = -1,$$

Presented by W. Sierpiński on March 17, 1960

whence

$$\left(\frac{a}{\mathfrak{p}}\right) = 1, \quad \left(\frac{b}{\mathfrak{p}}\right) = -1.$$

Assume now that $b > 0$ and that for some indices $i, j \leqslant s$ we have $\alpha_i\beta_j - \beta_i\alpha_j \neq 0$. Choose a rational prime $l > |\alpha_i\beta_j - \beta_i\alpha_j|$.

The numbers $\gamma_i = q_i$ $(i = 1, 2, \ldots, s)$, as different rational primes and the number l satisfy the conditions of the Lemma. Then there exists an infinite number of prime ideals $\mathfrak{p}$ of the field $\Gamma(\zeta_l)$, the degree of which is 1 and for which we have

$$\left(\frac{q_v}{\mathfrak{p}}\right) = 1 \ (v \neq i, j), \quad \left(\frac{q_i}{\mathfrak{p}}\right) = \zeta_l^{-\alpha_j}, \quad \left(\frac{q_j}{\mathfrak{p}}\right) = \zeta_l^{\alpha_i},$$

whence

$$\left(\frac{a}{\mathfrak{p}}\right) = 1, \quad \left(\frac{b}{\mathfrak{p}}\right) = \zeta_l^{\alpha_i\beta_j - \beta_i\alpha_j} \neq 1.$$

In both considered cases, therefore, there exists such a rational prime l that the field $\Gamma(\zeta_l)$ contains infinitely many prime ideals $\mathfrak{p}$, of the degree 1, for which $\left(\frac{b}{\mathfrak{p}}\right) \neq 1$, but $\left(\frac{a}{\mathfrak{p}}\right) = 1$, whence $\left(\frac{a^x}{\mathfrak{p}}\right) = 1$, then the congruence $a^x \equiv b \pmod{\mathfrak{p}}$ is insoluble.

The same property has, of course, the congruence $a^x \equiv b \pmod{p}$, where the rational prime p is the norm of the ideal $\mathfrak{p}$. As a prime p can be a norm of only a finite $\leqslant l$ number of prime ideals, there exists in the considered cases an infinite number of rational primes for which the congruence $a^x \equiv b \pmod{p}$ is insoluble.

We have still to examine the case, when $b > 0$ and when for all $i, j \leqslant s$: $\alpha_i\beta_j - \alpha_j\beta_i = 0$. As $\alpha_i + \beta_i > 0$ $(i = 1, 2, \ldots, s)$ and not all α_i are $= 0$, it follows from the last formula that all α_i are $\neq 0$ and that, for $i \leqslant s$, $\dfrac{\beta_i}{\alpha_i} = \dfrac{\beta_1}{\alpha_1}$ holds.

Let

$$\frac{\alpha_1}{(\alpha_1, \beta_1)} = \alpha, \quad \frac{\beta_1}{(\alpha_1, \beta_1)} = \beta.$$

As $(\alpha, \beta) = 1$, $\dfrac{\beta_i}{\alpha_i} = \dfrac{\beta}{\alpha}$ $(i \leqslant s)$, we have $\alpha_i = \alpha\delta_i$, $\beta_i = \beta\delta_i$, where δ_i are positive integers.

Putting $c = \gamma_1^{\delta_1}\gamma_2^{\delta_2}\cdots\gamma_s^{\delta_s}$ we get $a = c^\alpha$, $b = c^\beta$.

If $\alpha = 1$, one obtains $b = a^\beta$, in spite of the conditions assumed. Hence, $\alpha > 1$ and there exists a rational prime $l \mid \alpha$. Choose a positive integer h so that $l^h \nmid 2(\delta_1, \delta_2, \ldots, \delta_s)$. As the numbers q_i are primes, it follows from the last formula that c is neither of the form n^{l^h} nor of the form $2^{l^h/2}n^{l^h}$, where n is a rational integer. By Trost's theorem ([5]) there exists, therefore, an infinite set P of rational primes p, for which c is not a residue of l^h-th degree.

As $l \mid \alpha$, $l \nmid \beta$ for any rational integer x: $l \nmid \alpha x - \beta$. Hence, for all $p \in P$, for all x: $c^{\alpha x - \beta}$ is not a residue of l^h-th degree, then the congruence $c^{\alpha x} \equiv c^\beta \pmod{p}$, i.e. the congruence $a^x \equiv b \pmod{p}$ is impossible.

This completes the proof. □

c *Remark.* The Theorem remains true, if $a > 0$ is not assumed, but the proof is longer.

References

[1] A. Schinzel, W. Sierpiński, *Sur les congruences* $x^x \equiv c \pmod{m}$ *et* $a^x \equiv b \pmod{p}$. Collect. Math. 11 (1959), 153–164.

[2] N. Tschebotaröw [Chebotarev], *Grundzüge der Galoisschen Theorie*. Übersetzt und bearbeitet von H. Schwerdtfeger, Noordhoff, Groningen–Djakarta 1950.

[3] N. Chebotarev, *Über einen Satz von Hilbert*. Vestnik Ukr. Akad. Nauk, 1923, 3–7; Sobranie Sochineniĭ I, Izd. Akad. Nauk SSSR, Moscow–Leningrad 1949–50, 14–17.

[4] D. Hilbert, *Die Theorie der algebraischen Zahlkörper*. In: Ges. Abhandlungen I, Berlin 1932, 63–363.

[5] E. Trost, *Zur Theorie von Potenzresten*. Nieuw Arch. Wisk. 18 (1934), 58–61.

Originally published in
Nordisk Matematisk Tidskrift 10 (1962), 8–10

On the composite integers of the form $c(ak+b)! \pm 1$

Summary. The author raises the problem whether there exist infinitely many composite integers of the form $c(ak+b)! \pm 1$. An affirmative answer in many cases when $c = 1$ follows immediately from Wilson's theorem; other cases are answered in the Theorem.

It follows immediately from the theorems of Wilson ([1]) and Leibniz ([2]) that there exist infinitely many composite integers of the forms $(ak+b)! + 1$ and $(ak+b)! - 1$ if $a > 0$ and $(a, b+1) = 1$ or $(a, b+2) = 1$ respectively. This suggests the problem whether for arbitrary integers $a > b \geqslant 0$ and rational $c > 0$ there exist infinitely many composite integers of the form $c(ak+b)! \pm 1$. All the cases, except the two mentioned above, for which I have found a positive answer to this problem are given by the following

Theorem. *There exist infinitely many composite integers of each of the forms*

1) $c(4k)! + 1,\ c(4k+2)! + 1,\ c(6k)! + 1,\ c(6k+2)! + 1,\ c(6k+4)! + 1;$
2) $c(2k)! - 1,\ c(2k+1)! + 1,\ c(2k+1)! - 1;$
3) $[b(2k+1)]! + 1.$

Here b is a positive odd integer and c a positive rational number.

Proof. An immediate generalisation of the theorem of Wilson gives

$$(p-i-1)!\,i! \equiv (-1)^{i+1} \pmod{p}, \quad p \text{ prime},\ 0 \leqslant i \leqslant p-1.$$

c Hence for arbitrary $c = d/n$ (d, n positive integers):

$$p \mid ni! + \varepsilon(-1)^{i+1}d \quad \text{implies} \quad p \mid d(p-i-1)! + \varepsilon n \tag{1}$$
$$(0 \leqslant i \leqslant p-1,\ \varepsilon = \pm 1).$$

Let now $a = 4$ or 6, b even. For sufficiently large l we have $\dfrac{(al-b-2)!}{c} \equiv 0 \pmod{a}$, therefore

$$\frac{(al-b-2)!}{c} - 1 \equiv -1 \pmod{a},$$

([1]) $(p-1)! \equiv -1 \pmod{p}$.
([2]) $(p-2)! \equiv +1 \pmod{p}$.

and since positive integers of the form $4t-1$ resp. $6t-1$ have a prime factor of the same form, $\dfrac{(al-b-2)!}{c}-1$ has a prime factor $p_l \equiv -1 \pmod a$. For sufficiently large l, p_l must be $> al-b-2 > n$, and in view of (1):

$$p_l \mid d(p_l - al + b + 1)! + n. \tag{2}$$

It follows that $d(p_l - al + b + 1)! + n \geqslant p_l > al - b - 2$, whence

$$\lim_{l\to\infty} (p_l - al + b + 1) = \infty,$$

and for l large enough, $c(p_l - al + b + 1)! \equiv 0 \pmod a$. Since $p_l \equiv -1 \pmod a$ we have $p_l \neq c(p_l - al + b + 1)! + 1$, and the number $c(p_l - al + b + 1)! + 1$ is composite, because by (2)

$$p_l \mid c(p_l - al + b + 1)! + 1.$$

Since $p_l - al + b + 1 \equiv b \pmod a$, the proof of part 1 of the theorem is complete.

To prove part 2, let us assume $a = 2$, $b = 0$ or 1, $\varepsilon = \pm 1$, and if $2l - b \geqslant d$ denote by p_l the greatest prime factor of $\dfrac{(2l-b)!}{c} + \varepsilon(-1)^{b+1}$. For l large enough, each prime factor p of the above number is $> 2l - b > n$, thus in view of (1):

$$p \mid d(p - 2l + b - 1)! + \varepsilon n.$$

It follows hence that $d(p - 2l + b - 1)! + \varepsilon n \geqslant p > 2l - b$. For sufficiently large l we have $n \mid (p - 2l + b - 1)!$ and thus

$$p \mid c(p - 2l + b - 1)! + \varepsilon. \tag{3}$$

In particular

$$p_l \mid c(p_l - 2l + b - 1)! + \varepsilon. \tag{4}$$

Suppose that

$$p_l = c(p_l - 2l + b - 1)! + \varepsilon. \tag{5}$$

If $\dfrac{(2l-b)!}{c} + \varepsilon(-1)^{b+1}$ has any prime factor $p < p_l$, we have

$$p \leqslant c(p - 2l + b - 1)! + \varepsilon$$

in view of (3), and therefore for sufficiently large l:

$$\begin{aligned} p_l - p &\geqslant c(p_l - 2l + b - 1)! + \varepsilon - c(p - 2l + b - 1)! - \varepsilon \\ &= c(p - 2l + b - 1)!\big[(p_l - 2l + b - 1)\cdots(p - 2l + b) - 1\big] \\ &\geqslant (p - \varepsilon)(p_l - p - 1) \geqslant (2l - b)(p_l - p - 1) > p_l - p, \end{aligned}$$

which is impossible. Equality (5) implies therefore

$$\frac{(2l-b)!}{c} + \varepsilon(-1)^{b+1} = p_l^{\alpha}. \tag{6}$$

For sufficiently large l we have further

$$6 \mid c(p_l - 2l + b - 1)! = p_l - \varepsilon,$$
$$2l - b \geqslant \frac{p_l - \varepsilon}{2} > \frac{p_l - \varepsilon}{3} > 6d,$$

thus $d(p_l - \varepsilon)^2 \mid (2l - b)!$ and in view of (6):

$$(p_l - \varepsilon)^2 \mid p_l^\alpha - \varepsilon(-1)^{b+1}.$$

Hence

$$(p_l - \varepsilon)^2 \mid \alpha(p_l - \varepsilon)\varepsilon^{\alpha-1} + \varepsilon^\alpha - \varepsilon(-1)^{b+1}, \quad (p_l - \varepsilon) \mid \alpha,$$

and we get

$$\frac{(2l - b)!}{c} + \varepsilon(-1)^{b+1} = p_l^\alpha \geqslant p_l^{p_l - \varepsilon} > (2l - b)^{2l-b},$$

which for l large enough gives a contradiction. We must therefore have $p_l \neq c(p_l - 2l + b - 1)! + \varepsilon$, and in view of (4) the number $c(p_l - 2l + b - 1)! + \varepsilon$ is composite. Since $p_l \equiv 1 \pmod 2$,

$$p_l - 2l + b - 1 \equiv b \pmod 2,$$

which proves part 2 of the theorem.

In order to prove part 3, we shall show that if b is odd and $b(2l + 1) > 3$, at least one of the numbers $[b(2l + 1)]! + 1$ and $\{[b(2l + 1)]! - b(2l + 1)\}! + 1$ is composite. In fact, suppose that $[b(2l + 1)]! + 1$ is a prime p. Then, in view of (1):

$$p \mid \{[b(2l + 1)]! - b(2l + 1)\}! + 1,$$

and if $\{[b(2l + 1)]! - b(2l + 1)\}! + 1$ is not composite, we have

$$\{[b(2l + 1)]! - b(2l + 1)\}! + 1 = p = [b(2l + 1)]! + 1,$$
$$[b(2l + 1)]! - b(2l + 1) = b(2l + 1),$$
$$[b(2l + 1) - 1]! = 2, \quad b(2l + 1) = 3,$$

against the assumption. On the other hand, both numbers $b(2l + 1)$ and $[b(2l + 1)]! - b(2l + 1)$ are of the form $b(2k + 1)$, which completes the proof.

Originally published in
Acta Arithmetica XXVII (1975), 397–420

On power residues and exponential congruences

In memory of Yu. V. Linnik

The main aim of this paper is to extend the results of [6] to algebraic number fields. We shall prove

Theorem 1. *Let K be an algebraic number field, ζ_q a primitive qth root of unity and τ the greatest integer such that $\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} \in K$. Let $n_1, \dots, n_k, n$ be positive integers, $n_i \mid n$; $\alpha_1, \dots, \alpha_k, \beta$ be non-zero elements of K. The solubility of the k congruences $x^{n_i} \equiv \alpha_i \bmod \mathfrak{p}$ $(1 \leqslant i \leqslant k)$ implies the solubility of the congruence $x^n \equiv \beta \bmod \mathfrak{p}$ for almost all prime ideals $\mathfrak{p}$ of K if and only if at least one of the following four conditions is satisfied for suitable rational integers $l_1, \dots, l_k, m_1, \dots, m_k$ and suitable $\gamma, \delta \in K$:*

(i) $\beta \prod_{i=1}^{k} \alpha_i^{nm_i/n_i} = \gamma^n$;

(ii) $n \not\equiv 0 \bmod 2^\tau$, $\prod_{2 \mid n_i} \alpha_i^{l_i} = -\delta^2$ *and* $\beta \prod_{i=1}^{k} \alpha_i^{nm_i/n_i} = -\gamma^n$;

(iii) $n \equiv 2^\tau \bmod 2^{\tau+1}$, $\prod_{2 \mid n_i} \alpha_i^{l_i} = -\delta^2$ *and*

$$\beta \prod_{i=1}^{k} \alpha_i^{nm_i/n_i} = -\left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{n/2} \gamma^n;$$

(iv) $n \equiv 0 \bmod 2^{\tau+1}$ *and* $\beta \prod_{i=1}^{k} \alpha_i^{nm_i/n_i} = \left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{n/2} \gamma^n$.

If $\zeta_4 \in K$, the conditions (ii), (iii), (iv) *imply* (i); *if $\tau = 2$,* (ii) *implies* (i) *for not necessarily the same $m_1, \dots, m_k$ and γ.*

Almost all prime ideals means all but for a set of Dirichlet density zero or all but finitely many. In this context it comes to the same in virtue of Frobenius density theorem.

Corollary 1. *If each of the fields $K(\xi_1, \xi_2, \dots, \xi_k)$, where $\xi_i^{n_i} = \alpha_i$, contains at least one η satisfying $\eta^n = \beta$ then at least one of the conditions* (i)–(iv) *holds.*

This corollary may be regarded as a generalization of the well known result concerning Kummer fields (see [3], p. 42). As one can see from Lemmata 6 and 7 below it holds for arbitrary fields K of characteristic not dividing n (with $\tau = \infty$, if necessary).

Corollary 2. *The congruences* $x^n \equiv \alpha \bmod \mathfrak{p}$ *and* $x^n \equiv \beta \bmod \mathfrak{p}$ *are simultaneously soluble or insoluble for almost all prime ideals* $\mathfrak{p}$ *of* K *if and only if either*

$$\beta\alpha^u = \gamma^n,$$

or $n \equiv 0 \bmod 2^{\tau+1}$ *and*

$$\beta\alpha^u = \left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{n/2}\gamma^n$$

where $(u, n) = 1$ *and* $\gamma \in K$.

This is a simultaneous refinement of the theorems of Flanders [1] and Gerst [2] concerning $\alpha = 1$ and $K = \mathbb{Q}$, respectively.

We shall prove further

Theorem 2. *If* $\alpha_1, \ldots, \alpha_k, \beta$ *are non-zero elements of* K *and the congruence*

$$\alpha_1^{x_1}\alpha_2^{x_2}\cdots\alpha_k^{x_k} \equiv \beta \bmod \mathfrak{p}$$

is soluble for almost all prime ideals $\mathfrak{p}$ *of* K *then the corresponding equation is soluble in rational integers.*

This is a refinement of a theorem of Skolem [7], in which he assumes that the congruence is soluble for all moduli (also composite). Skolem's proof is defective but it can be amended.

On the lines indicated by Skolem we prove

Theorem 3. *Let* α_{ij}, β_i $(i = 1, \ldots, h,\ j = 1, \ldots, k)$ *be non-zero elements of* K, D *a positive integer. If the system of congruences*

$$\prod_{j=1}^{k} \alpha_{ij}^{x_j} \equiv \beta_i \bmod \mathfrak{m} \quad (i = 1, \ldots, h)$$

is soluble for all moduli $\mathfrak{m}$ *prime to* D *then the corresponding system of equations is soluble in integers.*

We show on an example that already for $h = 2$, $k = 3$ one cannot replace here "all moduli prime to D" by "all prime moduli".

On the other hand, the present approach gives no clue to Skolem's very interesting conjecture:

If the congruence

$$\sum_{i=1}^{h} \alpha_{i0}\alpha_{i1}^{x_1}\cdots\alpha_{ik}^{x_k} \equiv 0 \bmod \mathfrak{m}$$

is soluble for all moduli $\mathfrak{m}$ *then the corresponding equation is soluble in rational integers.*

The proof of Theorem 1 is based on nine lemmata. In formulating and proving them we use as much as possible the matrix notation. Integral matrices are denoted by bold face capital letters, integral vectors are treated as matrices with one row and denoted by

bold face lower case letters. $\boldsymbol{A}^T$ is the transpose of $\boldsymbol{A}$. A congruence $\boldsymbol{a} \equiv \boldsymbol{b} \bmod \boldsymbol{M}$ or $\boldsymbol{a}^T \equiv \boldsymbol{b}^T \bmod \boldsymbol{M}$ means that for a certain $\boldsymbol{x}$, $\boldsymbol{a}-\boldsymbol{b} = \boldsymbol{x}\boldsymbol{M}$, a congruence $\boldsymbol{a} \equiv \boldsymbol{b} \bmod (\boldsymbol{M}, \boldsymbol{N})$ means that $\boldsymbol{a}-\boldsymbol{b} = \boldsymbol{x}\boldsymbol{M}+\boldsymbol{y}\boldsymbol{N}$. Instead of $\bmod n\boldsymbol{I}$ or $\bmod (n\boldsymbol{I}, \boldsymbol{N})$, where $\boldsymbol{I}$ is the identity matrix, we write $\bmod n$ or $\bmod (n, \boldsymbol{N})$, respectively. The congruence $\boldsymbol{a} \equiv \boldsymbol{b} \bmod (n, \boldsymbol{N})$ implies $\boldsymbol{a}\boldsymbol{R} \equiv \boldsymbol{b}\boldsymbol{R} \bmod (n, \boldsymbol{N}\boldsymbol{R})$ for any $\boldsymbol{R}$ and $\boldsymbol{a} \equiv \boldsymbol{b} \bmod (n, \boldsymbol{R}\boldsymbol{N})$ for any unimodular $\boldsymbol{R}$.

Lemma 1. *For every integral matrix $\boldsymbol{A}$ there exist two unimodular matrices $\boldsymbol{P}$ and $\boldsymbol{Q}$ such that all elements of $\boldsymbol{P}\boldsymbol{A}\boldsymbol{Q}$ outside the diagonal are zero.*

Proof. See [8], p. 13. □

Lemma 2. *Let $\boldsymbol{A}$ be an integral matrix, $\boldsymbol{b}$ an integral vector. If for all integral vectors $\boldsymbol{x}$ the congruence $\boldsymbol{x}\boldsymbol{A} \equiv \boldsymbol{0} \bmod n$ implies $\boldsymbol{x}\boldsymbol{b}^T \equiv 0 \bmod n$ then $\boldsymbol{b}^T \equiv \boldsymbol{A}\boldsymbol{c}^T \bmod n$ for an integral vector $\boldsymbol{c}$.*

Proof. Let $\boldsymbol{A} = [a_{ij}]_{\substack{i \leqslant r \\ j \leqslant s}}$, $\boldsymbol{b} = [b_1, \ldots, b_r]$. If $a_{ij} = 0$ for $i \neq j$ then the congruence $\boldsymbol{x}\boldsymbol{A} \equiv \boldsymbol{0} \bmod n$ is satisfied by

$$\boldsymbol{x}_i = \begin{cases} \Big(\underbrace{0, \ldots, 0, \frac{n}{(n, a_{ii})}}_{i}, 0, \ldots, 0\Big) & (1 \leqslant i \leqslant q = \min(r, s)), \\ (\underbrace{0, \ldots, 0, 1}_{i}, 0, \ldots, 0) & (q < i \leqslant r). \end{cases}$$

It follows that $\boldsymbol{x}_i\boldsymbol{b}^T \equiv 0 \bmod n$ $(1 \leqslant i \leqslant r)$ and hence

$$b_i \equiv \begin{cases} 0 \bmod (n, a_{ii}) & (1 \leqslant i \leqslant q), \\ 0 \bmod n & (q < i \leqslant r). \end{cases}$$

Thus $b_i \equiv a_{ii}c_i \bmod n$ for suitable c_i $(1 \leqslant i \leqslant q)$ and setting $\boldsymbol{c} = [c_1, \ldots, c_q, 0, \ldots, 0]$ we get $\boldsymbol{b}^T \equiv \boldsymbol{A}\boldsymbol{c}^T \bmod n$.

In the general case let $\boldsymbol{P}, \boldsymbol{Q}$ have the property asserted in Lemma 1. If $\boldsymbol{x}\boldsymbol{P}\boldsymbol{A}\boldsymbol{Q} \equiv 0 \bmod n$ then $\boldsymbol{x}\boldsymbol{P}\boldsymbol{A} \equiv \boldsymbol{0} \bmod n$ hence $\boldsymbol{x}\boldsymbol{P}\boldsymbol{b}^T \equiv 0 \bmod n$. By the already proved case of our lemma $\boldsymbol{P}\boldsymbol{b}^T \equiv \boldsymbol{P}\boldsymbol{A}\boldsymbol{Q}\boldsymbol{d}^T \bmod n$ for a suitable integral $\boldsymbol{d}$ and since $\boldsymbol{P}$ is unimodular $\boldsymbol{b}^T \equiv \boldsymbol{A}\boldsymbol{Q}\boldsymbol{d}^T \bmod n$. Thus we can take $\boldsymbol{c} = \boldsymbol{d}\boldsymbol{Q}^T$. □

Lemma 3. *Let $\boldsymbol{A}$ and $\boldsymbol{b}$ satisfy the assumptions of Lemma 2, let besides $\boldsymbol{a} \equiv \boldsymbol{0} \bmod np^{-1}$ and $\boldsymbol{b} \equiv \boldsymbol{0} \bmod np^{-1}$, where p is a prime and $p \parallel n$. If for all integral vectors $\boldsymbol{x}$ the congruence $\boldsymbol{x}\boldsymbol{A} \equiv \boldsymbol{a} \bmod n$ implies $\boldsymbol{x}\boldsymbol{b}^T \equiv b \bmod n$ then*

$$\boldsymbol{b}^T \equiv \boldsymbol{A}\boldsymbol{d}^T \bmod n \quad \textit{and} \quad b \equiv \boldsymbol{a}\boldsymbol{d}^T \bmod n$$

for an integral vector $\boldsymbol{d}$.

Proof. Let $\boldsymbol{A} = [a_{ij}]_{\substack{i \leqslant r, \\ j \leqslant s}}$, $\boldsymbol{a} = (a_{01}, \ldots, a_{0s})$. As in the proof of Lemma 2 it is enough to consider the case where $a_{ij} = 0$ for $i \neq 0, j$. In virtue of that lemma we have $\boldsymbol{b}^T \equiv \boldsymbol{A}\boldsymbol{c}^T \bmod n$, for a certain $\boldsymbol{c}$.

If the congruence $\boldsymbol{x}\boldsymbol{A} \equiv \boldsymbol{a} \bmod n$ is soluble then we take $\boldsymbol{d} = \boldsymbol{c}$. Indeed, we have for a suitable $\boldsymbol{x}_0$

$$b \equiv \boldsymbol{x}_0\boldsymbol{b}^T \equiv \boldsymbol{x}_0\boldsymbol{A}\boldsymbol{c}^T \equiv \boldsymbol{a}\boldsymbol{c}^T \bmod n.$$

If the congruence $\boldsymbol{x}\boldsymbol{A} \equiv \boldsymbol{a} \bmod n$ is insoluble we have, for a certain $j \leqslant \min(r, s)$, $(n, a_{jj}) \nmid a_{0j}$, hence in view of $a_{0j} \equiv 0 \bmod np^{-1}$

$$p \mid a_{jj} \quad \text{and} \quad p \nmid a_{0j}. \tag{1}$$

We determine d from the system of congruences

$$d \equiv 0 \bmod np^{-1}, \tag{2}$$

$$a_{0j}d \equiv (b - \boldsymbol{a}\boldsymbol{c}^T) \bmod p \tag{3}$$

and set $\boldsymbol{d} = \boldsymbol{c} + (\underbrace{0, \ldots, 0, d}_{j}, 0, \ldots, 0)$.

It follows from (1) and (2) that $\boldsymbol{A}\boldsymbol{d}^T \equiv \boldsymbol{A}\boldsymbol{c}^T \equiv \boldsymbol{b}^T \bmod n$ and by (3) $\boldsymbol{a}\boldsymbol{d}^T \equiv b \bmod n$.

Lemma 4. *Let $\mathscr{A}_n$ be a subgroup of the multiplicative group of residues* $\bmod n$ *and B the set of all integers $b \equiv 1 \bmod (4, n)$ the residues of which belong to $\mathscr{A}_n$. Let d be the greatest common factor of all numbers $b - 1$, where $b \in B$; $n = n_1n_2$, where each prime factor of n_1 divides d and $(n_2, d) = 1$. If an integer valued function h on B satisfies the congruences*

$$h(ab) \equiv ah(b) + h(a) \bmod n, \tag{4}$$

$$h(b) \equiv 0 \bmod n_1 \quad \textit{if} \quad b \equiv 1 \bmod n_1 \tag{5}$$

then

$$h(b) \equiv c(b - 1) \bmod n$$

for a suitable c and all $b \in B$.

Proof. Let $n = p_1^{\nu_1}p_2^{\nu_2}\cdots p_s^{\nu_s}$ be the factorization of n into primes. Assume that $p_i \mid n_1$ for $i \leqslant r$, $p_i \mid n_2$ for $i > r$. Let b_i be an element of B such that $\operatorname{ord}_{p_i}(b_i - 1)$ is minimal, equal to, say μ_i. We have

$$d = p_1^{\mu_1}p_2^{\mu_2}\cdots p_r^{\mu_r}, \quad 1 \leqslant \mu_i \leqslant \nu_i \ (i \leqslant r), \quad \mu_i = 0 \ (i > r).$$

For $i \leqslant r$ let g_i be a primitive root $\bmod p_i^{\nu_i+1}$ or if $p_i = 2$, $\nu_i \geqslant 2$ then $g_i = 5$. Let, for $a \not\equiv 0 \bmod p_i$, $a \equiv 1 \bmod 4$, if $p_i = 2$, $\nu_i \geqslant 2$, $\operatorname{ind}_i a$ be defined by the congruence

$$g_i^{\operatorname{ind}_i a} \equiv a \bmod p_i^{\nu_i+1}$$

and set

$$\varphi'(p^\nu) = \begin{cases} 2^{\nu-2} & \text{if } p = 2, \ \nu \geqslant 2, \\ p^{\nu-1}(p-1) & \text{otherwise.} \end{cases} \tag{6}$$

$\operatorname{ind}_i a$ is determined $\bmod \varphi'(p_i^{\nu_i+1})$, moreover for $\mu \leqslant \nu_i + 1$

c (7) $$a \equiv 1 \bmod p_i^{\mu} \quad \text{if and only if} \quad \operatorname{ind}_i a \equiv 0 \bmod \varphi'(p_i^{\mu}).$$

Since $\operatorname{ind}_i a^{\nu} \equiv \nu \operatorname{ind}_i a \bmod \varphi'(p_i^{\nu_i+1})$ it follows from (6) and (7) that

$$\min\bigl(\nu_i + 1, \operatorname{ord}_{p_i}(a^{\nu} - 1)\bigr) = \min\bigl(\nu_i + 1, \operatorname{ord}_{p_i} \nu + \operatorname{ord}_{p_i}(a - 1)\bigr)$$

and since ν_i can be arbitrarily large

(8) $$\operatorname{ord}_{p_i}(a^{\nu} - 1) = \operatorname{ord}_{p_i} \nu + \operatorname{ord}_{p_i}(a - 1),$$

c provided $p_i > 2, a \equiv 1 \bmod p_i$ or $p_i = 2, a \equiv 1 \bmod 4$ or $p_i = 2, a\nu$ odd.

Since for all $a \in B$

(9) $$\operatorname{ord}_{p_j}(a - 1) \geqslant \mu_j,$$

we have in particular

$$\operatorname{ord}_{p_j}(b_i^{n_1 d^{-1}} - 1) \geqslant \nu_j \quad (1 \leqslant j \leqslant r)$$

and hence $b_i^{n_1 d^{-1}} \equiv 1 \bmod n_1$. By (5)

(10) $$h(b_i^{n_1 d^{-1}}) \equiv 0 \bmod n_1.$$

c On the other hand, by (4)

(11) $$h(b^e) \equiv \frac{b^e - 1}{b - 1} h(b) \bmod n.$$

The formula (8) gives $\operatorname{ord}_{p_i}(b_i^{n_i d^{-1}} - 1) = \nu_i$ and we infer from (10) and (11) that $p_i^{\mu_i} \mid h(b_i)$ for all $i \leqslant r$. The same holds clearly for $i > r$. We now choose c to satisfy the system of congruences

(12) $$c \equiv \frac{h(b_i) p_i^{-\mu_i}}{(b_i - 1) p_i^{-\mu_i}} \bmod p_i^{\nu_i} \quad (1 \leqslant i \leqslant s).$$

c For every $b \in B$ and $i \leqslant r$ we have by (6), (7) and (9)

$$\bigl(\operatorname{ind}_i b_i, \varphi'(p_i^{\nu_i})\bigr) \mid \operatorname{ind}_i b.$$

Choosing x_i so that

$$x_i \operatorname{ind}_i b_i + \operatorname{ind}_i b \equiv 0 \bmod \varphi'(p_i^{\nu_i})$$

we get

(13) $$b_i^{x_i} b \equiv 1 \bmod p_i^{\nu_i}.$$

It follows from (8) and (9) with $a = b_i^{x_i} b$ that

$$\operatorname{ord}_{p_j}\bigl((b_i^{x_i} b)^{n_1 p_i^{-\nu_i}} - 1\bigr) \geqslant \nu_j \quad (1 \leqslant j \leqslant r)$$

and thus

$$(b_i^{x_i} b)^{n_1 p_i^{-v_i}} \equiv 1 \bmod n_1.$$

c Hence by (5) and (11)

$$h\big((b_i^{x_i} b)^{n_1 p_i^{-v_i}}\big) \equiv \frac{(b_i^{x_i} b)^{n_1 p_i^{-v_i}} - 1}{b_i^{x_i} b - 1}\, h(b_i^{x_i} b) \equiv 0 \bmod n_1.$$

However by (8) the cofactor of $h(b_i^{x_i} b)$ above is prime to p_i, thus

$$h(b_i^{x_i} b) \equiv b\,\frac{b_i^{x_i} - 1}{b_i - 1}\, h(b_i) + h(b) \equiv 0 \bmod p_i^{v_i}$$

and by (12) and (13)

$$h(b) \equiv c(b-1) \bmod p_i^{v_i} \quad (1 \leqslant i \leqslant r). \tag{14}$$

On the other hand, for $i > r$ we have by (4)

$$h(bb_i) \equiv bh(b_i) + h(b) \equiv b_i h(b) + h(b_i) \bmod p_i^{v_i},$$

hence by (12)

$$h(b) \equiv \frac{h(b_i)}{b_i - 1}\,(b-1) \equiv c(b-1) \bmod p_i^{v_i} \quad (r < i \leqslant s), \tag{15}$$

and the lemma follows from (14) and (15). □

Lemma 5. *Let $\mathscr{A}_n$ be a subgroup of the multiplicative group of residues* mod n *and A the set of all integers the residues of which belong to $\mathscr{A}_n$. Let $\boldsymbol{M}$ be a non-singular square matrix such that $n\boldsymbol{M}^{-1}$ is integral. Let $\boldsymbol{f}$ and g be functions on A into set of integral vectors or integers respectively, satisfying the conditions*

$$\boldsymbol{f}(a) \equiv \boldsymbol{f}(b), \quad g(a) \equiv g(b) \bmod n \quad \text{if} \quad a \equiv b \bmod n, \tag{16}$$

$$\boldsymbol{f}(ab) \equiv a\,\boldsymbol{f}(b) + \boldsymbol{f}(a) \bmod \boldsymbol{M}, \tag{17}$$

$$g(ab) \equiv ag(b) + g(a) \bmod n. \tag{18}$$

If for all $a \in A$ the congruence

$$\boldsymbol{f}(a) \equiv 0 \bmod (a-1, \boldsymbol{M})$$

implies the congruence

$$g(a) \equiv 0 \bmod (a-1, n)$$

c *then there exist vectors $\boldsymbol{u}_1$ and $\boldsymbol{u}_2$ and an integer c such that for all $a \in A$, $a \equiv 1 \bmod (4, n)$*

$$g(a) \equiv c(a-1) + \boldsymbol{f}(a) n \boldsymbol{M}^{-1} \boldsymbol{u}_1^T \bmod n$$

and for all $a \in A$

$$g(a) \equiv \boldsymbol{f}(a)\boldsymbol{u}_2^T \bmod (2, n), \quad \boldsymbol{M}\boldsymbol{u}_2^T \equiv \boldsymbol{0} \bmod (2, n).$$

Proof. By Lemma 1 there exist unimodular matrices $\boldsymbol{P}$ and $\boldsymbol{Q}$ such that

$$\boldsymbol{P}\boldsymbol{M}\boldsymbol{Q} = \begin{bmatrix} e_1 & 0 & \dots & 0 \\ 0 & e_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & e_k \end{bmatrix}. \tag{19}$$

Since $\boldsymbol{M}$ is non-singular the entries e_i are non-zero and since $n\boldsymbol{M}^{-1}$ is integral we have $e_i \mid n$ $(1 \leqslant i \leqslant k)$. Any congruence $\boldsymbol{x} \equiv \boldsymbol{0} \bmod (m, \boldsymbol{P}\boldsymbol{M}\boldsymbol{Q})$ where $\boldsymbol{x} = [x_1, \dots, x_k]$ is equivalent to the system of congruences $x_i \equiv 0 \bmod (m, e_i)$ $(1 \leqslant i \leqslant k)$, which will be frequently used in the sequel.

Let n_1, n_2 have the meaning defined in Lemma 4.

For each prime $p_i \mid n_2$ there exists $b_i \in A$ such that $b_i \not\equiv 1 \bmod p_i$.

If $p_i^{\nu_i} \parallel n_2$ we get by (17) for all $a \in A$

$$\begin{gathered} \boldsymbol{f}(a)(b_i - 1) \equiv \boldsymbol{f}(b_i)(a - 1) \bmod \boldsymbol{M}, \\ \boldsymbol{f}(a)(b_i - 1)\boldsymbol{Q} \equiv \boldsymbol{0} \bmod (a - 1, \boldsymbol{P}\boldsymbol{M}\boldsymbol{Q}), \\ \boldsymbol{f}(a)\boldsymbol{Q} \equiv \boldsymbol{0} \bmod \big((a - 1, p_i^{\nu_i}), \boldsymbol{P}\boldsymbol{M}\boldsymbol{Q}\big), \\ \boldsymbol{f}(a)\boldsymbol{Q} \equiv \boldsymbol{0} \bmod \big((a - 1, n_2), \boldsymbol{P}\boldsymbol{M}\boldsymbol{Q}\big). \end{gathered} \tag{20}$$

Let $a_1, \dots, a_r$ represent all residue classes of $\mathscr{A}_n$ congruent to $1 \bmod n_1$.

If $x_1, \dots, x_r$ are integers not necessarily positive and

$$a \equiv a_1^{x_1} \cdots a_r^{x_r} \bmod n$$

we have by (16), (17) and (18)

$$\boldsymbol{f}(a) \equiv x_1\boldsymbol{f}(a_1) + \dots + x_r\boldsymbol{f}(a_r) \bmod (n_1, \boldsymbol{M}), \tag{21}$$

$$g(a) \equiv x_1 g(a_1) + \dots + x_r g(a_r) \bmod n_1. \tag{22}$$

Let us set

$$\boldsymbol{F} = \begin{bmatrix} \boldsymbol{f}(a_1) \\ \boldsymbol{f}(a_2) \\ \vdots \\ \boldsymbol{f}(a_r) \end{bmatrix}, \quad \boldsymbol{g} = [g(a_1), \dots, g(a_r)].$$

By (21)

$$\boldsymbol{f}(a) \equiv \boldsymbol{x}\boldsymbol{F} \bmod (n_1, \boldsymbol{P}\boldsymbol{M})$$

and

$$\boldsymbol{f}(a)\boldsymbol{Q} \equiv \boldsymbol{x}\boldsymbol{F}\boldsymbol{Q} \bmod (n_1, \boldsymbol{P}\boldsymbol{M}\boldsymbol{Q}). \tag{23}$$

Now suppose that for a vector $\boldsymbol{x}$ we have

$$\boldsymbol{x}\boldsymbol{F}n\boldsymbol{M}^{-1} \equiv \boldsymbol{0} \bmod n_1. \tag{24}$$

Then

$$n_2\boldsymbol{x}\boldsymbol{F}\boldsymbol{Q} \equiv \boldsymbol{0} \bmod \boldsymbol{P}\boldsymbol{M}\boldsymbol{Q}$$

and in view of (19)

$$\boldsymbol{x}\boldsymbol{F}\boldsymbol{Q} \equiv \boldsymbol{0} \bmod (n_1, \boldsymbol{P}\boldsymbol{M}\boldsymbol{Q}).$$

By (23) we can write the above congruence in the form

$$\boldsymbol{f}(a)\boldsymbol{Q} \equiv \boldsymbol{0} \bmod (n_1, \boldsymbol{P}\boldsymbol{M}\boldsymbol{Q}).$$

This together with (20) gives

$$\boldsymbol{f}(a)\boldsymbol{Q} \equiv \boldsymbol{0} \bmod \big((a-1, n), \boldsymbol{P}\boldsymbol{M}\boldsymbol{Q}\big)$$

and since $e_i \mid n$ we infer that

$$\boldsymbol{f}(a)\boldsymbol{Q} \equiv \boldsymbol{0} \bmod (a-1, \boldsymbol{P}\boldsymbol{M}\boldsymbol{Q}),$$
$$\boldsymbol{f}(a) \equiv \boldsymbol{0} \bmod (a-1, \boldsymbol{M}).$$

By the assumption

$$g(a) \equiv 0 \bmod (a-1, n)$$

and by (22)

$$\boldsymbol{x}\boldsymbol{g}^T \equiv 0 \bmod n_1. \tag{25}$$

Thus (24) implies (25) and by Lemma 2 we get

$$\boldsymbol{g}^T \equiv \boldsymbol{F}n\boldsymbol{M}^{-1}\boldsymbol{u}_1^T \bmod n_1$$

for a suitable $\boldsymbol{u}_1$. On comparing the components it follows

$$g(a_i) \equiv \boldsymbol{f}(a_i)n\boldsymbol{M}^{-1}\boldsymbol{u}_1^T \bmod n_1 \quad (1 \leqslant i \leqslant r).$$

However every $a \equiv 1 \bmod n_1$ satisfies $a \equiv a_i \bmod n$ for a suitable $i \leqslant r$, thus by (16) the function

$$h(a) = g(a) - \boldsymbol{f}(a)n\boldsymbol{M}^{-1}\boldsymbol{u}_1^T$$

satisfies $h(a) \equiv 0 \bmod n_1$ for all $a \equiv 1 \bmod n_1$. By (17) and (18) it satisfies also
c $h(ab) \equiv ah(b)+h(a) \bmod n$ and by Lemma 4 we infer that for all $a \in A, a \equiv 1 \bmod (4, n)$,

$$h(a) \equiv c(a-1) \bmod n$$

for suitable c. This gives the first assertion of the lemma.

In order to prove the second one it is enough to consider the case where $4 \mid n$ and A contains an integer $\bar{a}_0 \equiv -1 \bmod 4$. Let n_0 be the greatest odd factor of n_1 and $a_0 = \bar{a}_0^{n_0}$. Clearly $a_0 \equiv -1 \bmod 4$ and by (8)

$$a_0 \equiv 1 \bmod n_0(\bar{a}_0 - 1).$$

Hence by (17) and (18)

$$\boldsymbol{f}(a_0) \equiv \frac{a_0-1}{\bar{a}_0-1}\,\boldsymbol{f}(\bar{a}_0) \equiv \boldsymbol{0} \bmod (n_0, \boldsymbol{M}), \tag{26}$$

$$g(a_0) \equiv \frac{a_0-1}{\bar{a}_0-1}\,g(\bar{a}_0) \equiv 0 \bmod n_0. \tag{27}$$

Let $a_1, \ldots, a_s$ represent all residue classes of A congruent to 1 mod $4n_0$. If

$$a \equiv a_0 a_1^{x_1} \cdots a_s^{x_s} \bmod n \tag{28}$$

we have by (16), (17) and (18)

$$\begin{aligned} \boldsymbol{f}(a) &\equiv \boldsymbol{f}(a_0) + \boldsymbol{f}(a_1^{x_1} \cdots a_s^{x_s}) \\ &\equiv \boldsymbol{f}(a_0) + x_1 \boldsymbol{f}(a_1) + \ldots + x_s \boldsymbol{f}(a_s) \bmod (4n_0, \boldsymbol{M}), \end{aligned} \tag{29}$$

$$g(a) \equiv g(a_0) + g(a_1^{x_1} \cdots a_s^{x_s}) \equiv g(a_0) + x_1 g(a_1) + \ldots + x_s g(a_s) \bmod 4n_0. \tag{30}$$

Let us set

$$\boldsymbol{F}_0 = \begin{bmatrix} \boldsymbol{f}(a_1) \\ \vdots \\ \boldsymbol{f}(a_s) \end{bmatrix}, \quad \boldsymbol{g}_0 = [g(a_1), \ldots, g(a_s)].$$

By (29)

$$\boldsymbol{f}(a) \equiv \boldsymbol{f}(a_0) + \boldsymbol{x}\boldsymbol{F}_0 \bmod (4n_0, \boldsymbol{P}\boldsymbol{M})$$

and

$$\boldsymbol{f}(a)\boldsymbol{Q} \equiv \boldsymbol{f}(a_0)\boldsymbol{Q} + \boldsymbol{x}\boldsymbol{F}_0\boldsymbol{Q} \bmod (4n_0, \boldsymbol{P}\boldsymbol{M}\boldsymbol{Q}). \tag{$*$}$$

Now suppose that for a vector $\boldsymbol{x}$ we have

$$\boldsymbol{x}\boldsymbol{F}_0\boldsymbol{R} + \boldsymbol{f}(a_0)\boldsymbol{R} \equiv \boldsymbol{0} \bmod 2n_0, \tag{31}$$

where

$$\boldsymbol{R} = \boldsymbol{Q} \begin{bmatrix} \dfrac{2n_0}{(2n_0, e_1)} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \dfrac{2n_0}{(2n_0, e_k)} \end{bmatrix}.$$

Then

$$\boldsymbol{x}\boldsymbol{F}_0\boldsymbol{Q} + \boldsymbol{f}(a_0)\boldsymbol{Q} \equiv \boldsymbol{0} \bmod (2n_0, \boldsymbol{P}\boldsymbol{M}\boldsymbol{Q})$$

and since by (28) $(2n_0, e_i) = (a - 1, n_1, e_i)$ we have by $(*)$

$$\boldsymbol{f}(a)\boldsymbol{Q} \equiv \boldsymbol{0} \bmod \big((a-1, n_1), \boldsymbol{P}\boldsymbol{M}\boldsymbol{Q}\big).$$

This together with (20) gives

$$\begin{aligned} \boldsymbol{f}(a)\boldsymbol{Q} &\equiv \boldsymbol{0} \bmod (a-1, \boldsymbol{P}\boldsymbol{M}\boldsymbol{Q}), \\ \boldsymbol{f}(a) &\equiv \boldsymbol{0} \bmod (a-1, \boldsymbol{M}). \end{aligned}$$

By the assumption

$$g(a) \equiv 0 \bmod (a-1, n)$$

and by (30)

$$\boldsymbol{x}\boldsymbol{g}_0^T + g(a_0) \equiv 0 \bmod 2n_0. \tag{32}$$

Thus (31) implies (32). On the other hand, by the already proved part of the lemma and since $a - 1 \equiv 0 \bmod 2n_0$,

$$\boldsymbol{g}_0^T \equiv \boldsymbol{F}_0 n \boldsymbol{M}^{-1} \boldsymbol{u}_1^T \bmod 2n_0.$$

Also

$$n\boldsymbol{M}^{-1} = \boldsymbol{R} \begin{bmatrix} \dfrac{n(2n_0, e_1)}{2n_0 e_1} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \dfrac{n(2n_0, e_k)}{2n_0 e_k} \end{bmatrix} \boldsymbol{P}$$

and finally by (26) and (27)

$$\boldsymbol{f}(a_0)\boldsymbol{R} \equiv \boldsymbol{0} \bmod n_0, \quad g(a_0) \equiv 0 \bmod n_0.$$

The assumptions of Lemma 3 are satisfied with $p = 2$ and we infer that for a suitable vector $\boldsymbol{d}$

$$\boldsymbol{g}_0^T \equiv \boldsymbol{F}_0 \boldsymbol{R} \boldsymbol{d}^T \bmod 2n_0, \quad g(a_0) \equiv \boldsymbol{f}(a_0)\boldsymbol{R}\boldsymbol{d}^T \bmod 2n_0.$$

Setting $\boldsymbol{u}_2 = \boldsymbol{d}\boldsymbol{R}^T$ we get

$$\boldsymbol{M}\boldsymbol{u}_2^T = \boldsymbol{M}\boldsymbol{R}\boldsymbol{d}^T = \boldsymbol{P}^{-1} \begin{bmatrix} \dfrac{2n_0 e_1}{(2n_0, e_1)} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \dfrac{2n_0 e_k}{(2n_0, e_k)} \end{bmatrix} \boldsymbol{d}^T \equiv \boldsymbol{0} \bmod 2. \tag{33}$$

On the other hand, for each $i \leqslant s$

$$g(a_i) \equiv \boldsymbol{f}(a_i)\boldsymbol{u}_2^T \bmod 2n_0$$

and since every $a \in A$, $a \equiv 1 \bmod 2n_0$ is congruent to a_i or to $a_0 a_i \bmod n$ we infer from (16), (29) and (30) that

$$g(a) \equiv \boldsymbol{f}(a)\boldsymbol{u}_2^T \bmod 2n_0$$

for all $a \in A$, $a \equiv 1 \bmod 2n_0$. By (8) for any $a \in A$, $a^{n_0} \equiv 1 \bmod n_0$ and hence

$$g(a^{n_0}) - \boldsymbol{f}(a^{n_0})\boldsymbol{u}_2^T \equiv 0 \bmod 2n_0.$$

On the other hand by (17), (18) and (33)

$$g(a^{n_0}) - \boldsymbol{f}(a^{n_0})\boldsymbol{u}_2^T \equiv \frac{a^{n_0} - 1}{a - 1}\left(g(a) - \boldsymbol{f}(a)\boldsymbol{u}_2^T\right) \bmod 2$$

and since $\dfrac{a^{n_0} - 1}{a - 1}$ is odd

$$g(a) \equiv \boldsymbol{f}(a)\boldsymbol{u}_2^T \bmod 2. \qquad \square$$

Lemma 6. *Let K be an arbitrary field, n a positive integer not divisible by the characteristic of K, n_i divisors of n and $\alpha_1, \dots, \alpha_k, \beta$ non-zero elements of K. Let $\mathscr{G}$ be the Galois*

group of the field $K(\zeta_n, \sqrt[n_1]{a_1}, \ldots, \sqrt[n_k]{a_k})$ *and assume that every element of* $\mathscr{G}$ *which fixes one of the fields* $K(\xi_1, \ldots, \xi_k)$, *where* $\xi_i^{n_i} = \alpha_i$, *fixes at least one* η *with* $\eta^n = \beta$. *Then for any choice of numbers* ξ_i *and* η *and for suitable exponents* $m_0, m_1, \ldots, m_k, q_1, \ldots, q_k$

$$\zeta_n^{m_0} \eta \xi_1^{m_1} \cdots \xi_k^{m_k} \in K(\zeta_4),$$

and if $n \equiv 0 \bmod 2$,

$$\eta^{n/2} \xi_1^{q_1} \cdots \xi_k^{q_k} \in K, \quad 2q_i \equiv 0 \bmod n_i \quad (1 \leqslant i \leqslant k).$$

Proof. Let us choose some ξ_i and η. It is clear that

$$\eta \in K(\zeta_m, \xi_1, \ldots, \xi_k) = L.$$

The elements σ of $\mathscr{G}$ act on L in the following way

$$\sigma(\zeta_n) = \zeta_n^{\alpha}, \quad \sigma(\xi_i) = \zeta_{n_i}^{t_i} \xi_i.$$

$\mathscr{G}$ contains a normal subgroup $\mathscr{H} = \{\sigma : \sigma(\zeta_n) = \zeta_n\}$. The vectors $[t_1, \ldots, t_k]$ such that for a $\sigma \in \mathscr{H}$

$$\sigma(\xi_i) = \zeta_{n_i}^{t_i} \xi_i \quad (1 \leqslant i \leqslant k)$$

constitute a lattice Λ. The fundamental vectors of Λ written horizontally form a matrix, say $\boldsymbol{M}$. Since the vectors $[n_1, 0, \ldots, 0]$, $[0, n_2, 0, \ldots, 0]$, ..., $[0, \ldots, 0, n_k]$ belong to Λ, $\boldsymbol{M}$ is non-singular and

$$n\boldsymbol{M}^{-1} = \boldsymbol{S}\boldsymbol{N} \quad \text{for} \quad \boldsymbol{S} = \begin{bmatrix} n/n_1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & n/n_k \end{bmatrix} \tag{34}$$

and a certain integral matrix $\boldsymbol{N}$.

Let A be the set of all integers a such that for a $\sigma \in \mathscr{G}$: $\sigma(\zeta_n) = \zeta_n^a$. The residues of $a \in A \bmod n$ form a subgroup $\mathscr{A}_n$ of the multiplicative group of residues $\bmod n$, isomorphic to $\mathscr{G}/\mathscr{H}$, and every integer the residue of which belongs to $\mathscr{A}_n$ is in A. Let $\boldsymbol{f}(1) = \boldsymbol{0}$, for an $a \in A$, $1 < a < n$, $\boldsymbol{f}(a) = [f_1(a), \ldots, f_k(a)]$ be any vector such that for a $\sigma \in \mathscr{G}$:

$$\sigma(\zeta_n) = \zeta_n^a, \quad \sigma(\xi_i) = \zeta_{n_i}^{f_i(a)} \xi_i \quad (1 \leqslant i \leqslant k)$$

and for all the other a let $\boldsymbol{f}(a) = \boldsymbol{f}\left(a - n\left[\frac{a}{n}\right]\right)$. Thus $\boldsymbol{f}(a) = \boldsymbol{f}(b)$ for $a \equiv b \bmod n$. On the other hand, for every $\sigma \in \mathscr{G}$ we have

$$\sigma(\zeta_n) = \zeta_n^a, \quad \sigma(\xi_i) = \zeta_{n_i}^{f_i(a)+t_i} \xi_i \tag{35}$$

for a suitable $a \in A$ and a suitable $[t_1, \ldots, t_k] \equiv \boldsymbol{0} \bmod \boldsymbol{M}$. Since $\mathscr{G}$ is a group with respect to superposition we get for all $a, b \in A$

$$\boldsymbol{f}(ab) \equiv a\boldsymbol{f}(b) + \boldsymbol{f}(a) \bmod \boldsymbol{M}.$$

Now for every pair $a, \boldsymbol{t}$ where $a \in A$, $\boldsymbol{t} \equiv \boldsymbol{0} \bmod \boldsymbol{M}$ we define σ by (35) and $\varphi(a, \boldsymbol{t})$ by the condition

$$\sigma(\eta) = \zeta_n^{\varphi(a,\boldsymbol{t})} \eta, \quad 0 \leqslant \varphi(a, \boldsymbol{t}) < n. \tag{36}$$

Since $\sigma_2\sigma_1(\eta) = \sigma_2\big(\sigma_1(\eta)\big)$ we get

$$\varphi\big(a_1a_2, a_2\big(\boldsymbol{t}_1 + \boldsymbol{f}(a_1)\big) + \boldsymbol{t}_2 + \boldsymbol{f}(a_2) - \boldsymbol{f}(a_1a_2)\big) \equiv a_2\varphi(a_1, \boldsymbol{t}_1) + \varphi(a_2, \boldsymbol{t}_2) \bmod n \tag{37}$$

and in particular

$$\varphi(1, \boldsymbol{t}_1 + \boldsymbol{t}_2) \equiv \varphi(1, \boldsymbol{t}_1) + \varphi(1, \boldsymbol{t}_2) \bmod n \quad \text{for} \quad \boldsymbol{t}_1 \equiv \boldsymbol{t}_2 \equiv \boldsymbol{0} \bmod \boldsymbol{M}.$$

c It follows that $\varphi(1, \boldsymbol{0}) = 0$ and if $\boldsymbol{t} = \boldsymbol{x}\boldsymbol{M}$,

$$\boldsymbol{M} = \begin{bmatrix} \boldsymbol{m}_1 \\ \boldsymbol{m}_2 \\ \vdots \\ \boldsymbol{m}_k \end{bmatrix}$$

then

c $$\varphi(1, \boldsymbol{t}) \equiv x_1\varphi(1, \boldsymbol{m}_1) + \ldots + x_k\varphi(1, \boldsymbol{m}_k) \bmod n.$$

c Since $\boldsymbol{t}\boldsymbol{S} \equiv \boldsymbol{0} \bmod n$ implies $\varphi(1, \boldsymbol{t}) = \varphi(1, \boldsymbol{0}) = 0$ we infer by Lemma 2 that for an integral vector $\boldsymbol{c}$

$$\begin{bmatrix} \varphi(1, \boldsymbol{m}_1) \\ \vdots \\ \varphi(1, \boldsymbol{m}_k) \end{bmatrix} \equiv \boldsymbol{M}\boldsymbol{S}\boldsymbol{c}^T \bmod n$$

and thus $\varphi(1, \boldsymbol{t}) \equiv \boldsymbol{t}\boldsymbol{S}\boldsymbol{c}^T \bmod n$. Hence by (37) with $a_2 = 1, \boldsymbol{t}_1 = \boldsymbol{0}$

$$\varphi(a, \boldsymbol{t}) \equiv \varphi(a, \boldsymbol{0}) + \boldsymbol{t}\boldsymbol{S}\boldsymbol{c}^T \bmod n. \tag{38}$$

The condition (37) takes the form

$$\varphi(a_1a_2, \boldsymbol{0}) + (a_2\boldsymbol{t}_1 + \boldsymbol{t}_2)\boldsymbol{S}\boldsymbol{c}^T + \big(a_2\boldsymbol{f}(a_1) + \boldsymbol{f}(a_2) - \boldsymbol{f}(a_1a_2)\big)\boldsymbol{S}\boldsymbol{c}^T \equiv a_2\varphi(a_1, \boldsymbol{0}) + a_2\boldsymbol{t}_1\boldsymbol{S}\boldsymbol{c}^T + \varphi(a_2, \boldsymbol{0}) + \boldsymbol{t}_2\boldsymbol{S}\boldsymbol{c}^T \bmod n.$$

It follows that the function

$$g(a) = \varphi(a, \boldsymbol{0}) - \boldsymbol{f}(a)\boldsymbol{S}\boldsymbol{c}^T \tag{39}$$

satisfies the conditions $g(a) \equiv g(b) \bmod n$ for $a \equiv b \bmod n$ and

$$g(ab) \equiv ag(b) + g(a) \bmod n.$$

Now suppose that for an $a \in A$ we have

$$\boldsymbol{f}(a) \equiv \boldsymbol{0} \bmod (a - 1, \boldsymbol{M}). \tag{40}$$

It follows that for a suitable $\boldsymbol{v} = [v_1, \ldots, v_k]$

$$\boldsymbol{f}(a) - (a - 1)\boldsymbol{v} \equiv \boldsymbol{0} \bmod \boldsymbol{M}$$

and $\mathscr{G}$ contains σ such that

c $$\sigma(\zeta_n) = \zeta_n^a, \quad \sigma(\xi_i) = \zeta_{n_i}^{(a-1)v_i}\xi_i \quad (1 \leqslant i \leqslant k).$$

We have

$$\sigma(\zeta_{n_i}^{-v_i}\xi_i) = \zeta_{n_i}^{-v_i}\xi_i \quad (1 \leqslant i \leqslant k),$$

thus by the assumption

$$\sigma(\zeta_n^{-v_0}\eta) = \zeta_n^{-v_0}\eta$$

for a suitable v_0. We obtain from (36), (38) and (39)

$$\begin{aligned} -v_0 a + \varphi\big(a, (a-1)\boldsymbol{v} - \boldsymbol{f}(a)\big) &\equiv -v_0 \bmod n, \\ \varphi(a, \boldsymbol{0}) + \big((a-1)\boldsymbol{v} - \boldsymbol{f}(a)\big)\boldsymbol{S}\boldsymbol{c}^T &\equiv (a-1)v_0 \bmod n, \\ g(a) &\equiv 0 \bmod (a-1, n). \end{aligned} \tag{41}$$

c Thus (40) implies (41) and we infer by Lemma 5 that for all $a \in A$, $a \equiv 1 \bmod (4, n)$

$$g(a) \equiv -m_0(a-1) + \boldsymbol{f}(a)n\boldsymbol{M}^{-1}\boldsymbol{u}_1^T \bmod n \tag{42}$$

c and for all $a \in A$

$$g(a) \equiv \boldsymbol{f}(a)\boldsymbol{u}_2^T \bmod (2, n), \quad \boldsymbol{M}\boldsymbol{u}_2^T \equiv \boldsymbol{0} \bmod (2, n). \tag{43}$$

Set $\boldsymbol{m} = [m_1, \ldots, m_k] = -\boldsymbol{c} - \boldsymbol{u}_1\boldsymbol{N}^T$, where $\boldsymbol{N}$ is defined by (34). If σ is defined by (35) and $a \equiv 1 \bmod (4, n)$ we get

$$\sigma(\zeta_n^{m_0}\eta\xi_1^{m_1}\cdots\xi_k^{m_k}) = \zeta_n^{e_1}\eta\xi_1^{m_1}\cdots\xi_k^{m_k},$$

where by (36), (38), (39) and (42)

$$\begin{aligned} e_1 &= am_0 + \varphi(a, \boldsymbol{t}) + \big(\boldsymbol{f}(a) + \boldsymbol{t}\big)\boldsymbol{S}\boldsymbol{m}^T \\ &\equiv am_0 + g(a) + \big(\boldsymbol{f}(a) + \boldsymbol{t}\big)\boldsymbol{S}\boldsymbol{c}^T + \big(\boldsymbol{f}(a) + \boldsymbol{t}\big)\boldsymbol{S}\boldsymbol{m}^T \\ &\equiv am_0 - m_0(a-1) + \boldsymbol{f}(a)n\boldsymbol{M}^{-1}\boldsymbol{u}_1^T - \big(\boldsymbol{f}(a) + \boldsymbol{t}\big)\boldsymbol{S}\boldsymbol{N}\boldsymbol{u}_1^T \\ &\equiv m_0 - \boldsymbol{t}n\boldsymbol{M}^{-1}\boldsymbol{u}_1^T \equiv m_0 \bmod n. \end{aligned}$$

Thus $\sigma(\zeta_4) = \zeta_4$ implies

$$\sigma(\zeta_n^{m_0}\eta\xi_1^{m_1}\cdots\xi_k^{m_k}) = \zeta_n^{m_0}\eta\xi_1^{m_1}\cdots\xi_k^{m_k}$$

and the first assertion of the lemma follows. In order to prove the second one assume $2 \mid n$ and set

$$\boldsymbol{q} = [q_1, \ldots, q_k] = \frac{n}{2}\,\boldsymbol{c} + \frac{n}{2}\,\boldsymbol{u}_2\boldsymbol{S}^{-1}. \tag{44}$$

$\boldsymbol{q}$ is integral since by (34) and (43)

$$(n\boldsymbol{u}_2\boldsymbol{S}^{-1})^T = n\boldsymbol{S}^{-1}\boldsymbol{u}_2^T = \boldsymbol{N}\boldsymbol{M}\boldsymbol{u}_2^T \equiv \boldsymbol{0} \bmod 2.$$

If σ is defined by (35) we get

$$\sigma(\eta^{n/2}\xi_1^{q_1}\cdots\xi_k^{q_k}) = \zeta_n^{e_2}\eta^{n/2}\xi_1^{q_1}\cdots\xi_k^{q_k},$$

where by (36), (38), (39) and (43)

$$e_2 = \frac{n}{2}\varphi(a, \boldsymbol{t}) + \big(\boldsymbol{f}(a) + t\big)\boldsymbol{S}\boldsymbol{q}^T$$
$$\equiv \frac{n}{2}\, g(a) + \frac{n}{2}\big(\boldsymbol{f}(a) + \boldsymbol{t}\big)\boldsymbol{S}\boldsymbol{c}^T + \big(\boldsymbol{f}(a) + \boldsymbol{t}\big)\frac{n}{2}\,\boldsymbol{S}\boldsymbol{c}^T + \big(\boldsymbol{f}(a) + \boldsymbol{t}\big)\frac{n}{2}\,\boldsymbol{u}_2^T \equiv 0 \bmod n.$$

It follows that

$$\eta^{n/2}\xi_1^{q_1}\cdots\xi_k^{q_k} \in K.$$

Also, by (44), $2q_i \equiv 0 \bmod n_i$. □

Lemma 7. *Let K be an arbitrary field of characteristic different from 2 and τ the greatest integer such that $\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} \in K$ if there are only finitely many of them, otherwise $\tau = \infty$. If $\vartheta \in K(\zeta_4)$, $\vartheta^n \in K$, then at least one of the following four conditions is satisfied for a suitable $\gamma \in K$:*

(i) $\vartheta^n = \gamma^n$,
(ii) $n \not\equiv 0 \bmod 2^\tau$, $\vartheta^n = -\gamma^n$,
(iii) $n \equiv 2^\tau \bmod 2^{\tau+1}$, $\vartheta^n = -\big(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\big)^{n/2}\gamma^n$,
(iv) $n \equiv 0 \bmod 2^{\tau+1}$, $\vartheta^n = \big(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\big)^{n/2}\gamma^n$.

Remark. If n is a power of 2 the lemma is contained in Satz 2 of [4].

Proof. Set $\zeta_4 = i$, $\vartheta = \alpha + \beta i$, $\alpha, \beta \in K$. If $i \in K$ we have (i); if $i \notin K$ then $(\alpha + \beta i)^n = \kappa \in K$ implies $(\alpha - \beta i)^n = \kappa$ hence

$$\alpha + \beta i = \zeta_n^\nu(\alpha - \beta i), \tag{45}$$
$$\zeta_n^\nu + \zeta_n^{-\nu} = \frac{\alpha + \beta i}{\alpha - \beta i} + \frac{\alpha - \beta i}{\alpha + \beta i} = \frac{2(\alpha^2 - \beta^2)}{\alpha^2 + \beta^2} \in K.$$

It follows that the only conjugate of ζ_n^ν over K is $\zeta_n^{-\nu}$ and the only possible conjugates of ζ_{2n}^ν are

$$\varepsilon_1\zeta_{2n}^{\varepsilon_2\nu} \quad (\varepsilon_1 = \pm 1,\ \varepsilon_2 = \pm 1).$$

(ζ_{2n} is chosen so that $\zeta_{2n}^2 = \zeta_n$.)

Let

$$\mu = \operatorname{ord}_2 2n/(2n, \nu). \tag{46}$$

Then

$$\zeta_{2^\mu} = \zeta_{2n}^{\nu\varrho}, \quad \varrho \equiv 1 \bmod 2. \tag{47}$$

If σ is an automorphism of $K(\zeta_{2n}^\nu)$ and

$$\sigma(\zeta_{2n}^\nu) = \varepsilon_1\zeta_{2n}^{\varepsilon_2\nu} \tag{48}$$

we get

$$\sigma(\zeta_{2^\mu}) = \varepsilon_1\zeta_{2^\mu}^{\varepsilon_2}. \tag{49}$$

If $\mu = 2$ we have $\zeta_n^\nu \neq 1$, by (45)

$$\alpha = \beta i \, \frac{\zeta_n^\nu + 1}{\zeta_n^\nu - 1},$$

$$\vartheta^n = \beta^n \left(\frac{2i}{\zeta_n^\nu - 1} \right)^n = \beta^n (-1)^\nu \left(\frac{2i}{\zeta_{2n}^\nu - \zeta_{2n}^{-\nu}} \right)^n \tag{50}$$

and by (48) and (49) for all automorphisms σ of $K(\zeta_{2n}^\nu)$ over K

$$\sigma\left(\frac{2i}{\zeta_{2n}^\nu - \zeta_{2n}^{-\nu}} \right) = \frac{2i}{\zeta_{2n}^\nu - \zeta_{2n}^{-\nu}}.$$

Thus $\dfrac{2i}{\zeta_{2n}^\nu - \zeta_{2n}^{-\nu}} \in K$ and by (46) and (50) we get (i) if ν is even and (ii) if ν is odd.

If $\mu \neq 2$, $\zeta_n^\nu \neq -1$ and by (45)

$$\beta i = \alpha \, \frac{\zeta_n^\nu - 1}{\zeta_n^\nu + 1},$$

$$\vartheta^n = \alpha^n \left(\frac{2}{\zeta_n^\nu + 1} \right)^n = \alpha^n (-1)^\nu \left(\frac{2}{\zeta_{2n}^\nu + \zeta_{2n}^{-\nu}} \right)^n. \tag{51}$$

If σ is an automorphism of $K(\zeta_{2n}^\nu)$,

$$\delta = (\zeta_{2n}^\nu + \zeta_{2n}^{-\nu})(\zeta_{2^\mu} + \zeta_{2^\mu}^{-1})$$

we have by (48) and (49)

$$\sigma(\delta) = \delta.$$

Thus $\delta \in K$ and since $\zeta_{2^\mu} + \zeta_{2^\mu}^{-1} \neq 0$ we get from (51)

$$\vartheta^n = (-1)^\nu (\zeta_{2^\mu} + \zeta_{2^\mu}^{-1})^n \left(\frac{2\alpha}{\delta} \right)^n. \tag{52}$$

On the other hand, $\mu \leqslant \tau + 1$. This is clear if $\mu = 0$ and if $\mu > 0$ it follows from (47) that

$$\zeta_{2^{\mu-1}} + \zeta_{2^{\mu-1}}^{-1} = \zeta_n^{\nu\varrho} + \zeta_n^{-\nu\varrho} = \left(\frac{\alpha + \beta i}{\alpha - \beta i} \right)^\varrho + \left(\frac{\alpha - \beta i}{\alpha + \beta i} \right)^\varrho \in K$$

thus $\mu - 1 \leqslant \tau$.

Denoting by γ a suitable element of K we can draw from (46) and (52) the following conclusions:

If $\mu \leqslant \tau$, $\nu \equiv 0 \bmod 2$ then $\vartheta^n = \gamma^n$;

if $\mu \leqslant \tau$, $\nu \equiv 1 \bmod 2$ then $\vartheta^n = -\gamma^n$; $n \not\equiv 0 \bmod 2^\tau$;

if $\mu = \tau + 1$, $\nu \equiv 1 \bmod 2$, then $\vartheta^n = -\left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{n/2} \gamma^n$ and $n \equiv 2^\tau \bmod 2^{\tau+1}$;

if $\mu = \tau + 1$, $\nu \equiv 0 \bmod 2$, then $\vartheta^n = \left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{n/2} \gamma^n$,

which correspond to the conditions (i), (ii), (iii), (iv), respectively. □

Lemma 8. *Let K be an algebraic number field, $f_i(x)$ polynomials over K with integral coefficients and discriminants D_i and $\mathfrak{p}$ a prime ideal of K not dividing $D_1 \cdots D_k$. The k*

congruences $f_i(x) \equiv 0 \bmod \mathfrak{p}$ $(1 \leqslant i \leqslant k)$ *are soluble* $\bmod \mathfrak{p}$ *if and only if* $\mathfrak{p}$ *has a prime factor of degree one in at least one field* $K(\xi_1, \ldots, \xi_k)$, *where* $f_i(\xi_i) = 0$.

Proof. The sufficiency of the condition is obvious. In order to prove the necessity we proceed by induction. For $k = 1$ the condition follows from Dedekind's theorem applied to a suitable irreducible factor of f. Suppose that the condition holds for less than k polynomials and that the k congruences $f_i(x) \equiv 0 \bmod \mathfrak{p}$ are soluble. Then $\mathfrak{p}$ has a prime factor $\mathfrak{P}$ of degree one in $K(\xi_1, \ldots, \xi_{k-1})$, where ξ_i is a certain zero of $f_i(x)$. The congruence $f_k(x) \equiv 0 \bmod \mathfrak{P}$ being soluble it follows by Dedekind's theorem that $\mathfrak{P}$ has a prime factor of relative degree one in at least one field $K(\xi_1, \ldots, \xi_k)$ where $f_k(\xi_k) = 0$. This factor is of degree one over K, which completes the proof. □

Lemma 9. *If* K *is an algebraic number field,* τ *is defined as in Theorem* 1 *and* $\nu > \tau$ *then the congruence* $x^{2^\nu} \equiv (\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{2^{\nu-1}} \bmod \mathfrak{p}$ *is soluble for all prime ideals* $\mathfrak{p}$ *of* K.

Proof. See [5], p. 156. □

Proof of Theorem 1. *Necessity.* Suppose that the Galois group $\mathscr{G}$ of the extension $L = K\left(\zeta_n, \sqrt[n_1]{\alpha_1}, \ldots, \sqrt[n_k]{\alpha_k}\right)$ of K contains an element σ which fixes one of the fields $K(\xi_1, \ldots, \xi_k)$, where $\zeta_i^{n_i} = \alpha_i$, but does not fix any η with $\eta^n = \beta$. By Frobenius density theorem prime ideals $\mathfrak{p}$ of K belonging to the division of σ in $\mathscr{G}$ have a positive density. Every such prime ideal $\mathfrak{p}$ has a prime factor of degree one in $K(\xi_1, \ldots, \xi_k)$ $(1 \leqslant i \leqslant k)$ where $\xi_1, \ldots, \xi_k$ are suitably chosen roots of $\xi_i^{n_i} = \alpha_i$, but it has no prime factor of degree one in any of the fields $K(\eta)$, where $\eta^n = \beta$. By Lemma 8, for almost all $\mathfrak{p}$'s the congruences $x^{n_i} \equiv \alpha_i \bmod \mathfrak{p}$ are soluble and the congruence $x^n \equiv \beta \bmod \mathfrak{p}$ is insoluble. The obtained contradiction shows that the assumptions of Lemma 6 are satisfied. Let us choose some values of $\xi_1, \ldots, \xi_k$ and η. By Lemma 6 there exist integers $m_0, m_1, \ldots, m_k$, $q_1, \ldots, q_k$ such that

$$\vartheta = \zeta_n^{m_0} \eta \xi_1^{m_1} \cdots \xi_k^{m_k} \in K(\zeta_4)$$

and if $n \equiv 0 \bmod 2$

$$\kappa = \eta^{n/2} \xi_1^{q_1} \cdots \xi_k^{q_k} \in K, \quad 2q_i \equiv 0 \bmod n_i \quad (1 \leqslant i \leqslant k). \tag{53}$$

Since

$$\vartheta^n = \beta \prod_{i=1}^{k} \alpha_i^{nm_i/n_i} \in K$$

we have by Lemma 7 for a suitable $\gamma \in K$ either

$$\beta \prod_{i=1}^{k} \alpha_i^{nm_i/n_i} = \gamma^n, \tag{54}$$

or $n \not\equiv 0 \bmod 2^\tau$

$$\beta \prod_{i=1}^{k} \alpha_i^{nm_i/n_i} = -\gamma^n \tag{55}$$

or $n \equiv 2^\tau \bmod 2^{\tau+1}$

$$\beta \prod_{i=1}^{k} \alpha_i^{nm_i/n_i} = -\left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{n/2} \gamma^n \tag{56}$$

or $n \equiv 0 \bmod 2^{\tau+1}$

$$\beta \prod_{i=1}^{k} \alpha_i^{nm_i/n_i} = \left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{n/2} \gamma^n. \tag{57}$$

(54) and (57) correspond to the conditions (i) and (iv), respectively.

If $n \not\equiv 0 \bmod 2$, (55) reduces to (54). If $n \equiv 0 \bmod 2$ we get from (53)

$$\beta \prod_{i=1}^{k} \alpha_i^{2q_i/n_i} = \kappa^2, \quad \kappa \in K.$$

This together with (55) and (56) gives on division

$$\prod_{i=1}^{k} \alpha_i^{l_i} = -\lambda^2, \quad \text{where} \quad l_i = \frac{nm_i - 2q_i}{n_i}, \ \lambda \in K.$$

However if n_i is odd, l_i is even, thus

$$\prod_{n_i \text{ even}} \alpha_i^{l_i} = -\delta^2, \quad \delta \in K.$$

Sufficiency. The sufficiency of the condition (i) is obvious. To show that (ii) and (iii) are sufficient we argue as follows. The equality

$$\prod_{n_i \text{ even}} \alpha_i^{l_i} = -\delta^2$$

implies that for any choice of ξ_i satisfying $\xi_i^{n_i} = \alpha_i$

$$\zeta_4 \in K(\xi_1, \ldots, \xi_k).$$

Since

$$\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} \in K, \quad 2\zeta_{2^\tau} = \zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + \zeta_4\left(\zeta_{2^\tau}^{1-2^{\tau-2}} + \zeta_{2^\tau}^{-1+2^{\tau-2}}\right)$$

we have $K(\zeta_4) = K(\zeta_{2^\tau})$. Hence $\zeta_{2^\tau} \in K(\xi_1, \ldots, \xi_k)$.

Let $\nu = \operatorname{ord}_2 n$. The conditions

$$\beta \prod_{i=1}^{k} \alpha_i^{nm_i/n_i} = -\gamma^n, \quad \nu < \tau,$$

and

$$\beta \prod_{i=1}^{k} \alpha_i^{nm_i/n_i} = -\left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{n/2} \gamma^n, \quad \nu = \tau,$$

can be rewritten for a suitable η and ϱ as

$$\eta \prod_{i=1}^{k} \xi_i^{m_i} = \zeta_{2^\tau}^{\varrho} \gamma \quad \text{and} \quad \eta \prod_{i=1}^{k} \xi_i^{m_i} = (\zeta_{2^\tau} + 1)\gamma,$$

respectively.

It follows that $\eta \in K(\xi_1, \ldots, \xi_k)$ and any ideal $\mathfrak{p}$ which has a prime factor of degree one in $K(\xi_1, \ldots, \xi_k)$ has a prime factor of degree one in $K(\eta)$. Since this is valid for any choice of ξ_i and a suitable η, we infer by Lemma 8 that the solubility of $x^n \equiv \alpha_i$ $(1 \leqslant i \leqslant k)$ implies the solubility of $x^n \equiv \beta \bmod \mathfrak{p}$.

The sufficiency of condition (iv) follows from Lemma 9, since the solubility of the congruence

$$x^{2^\nu} \equiv \left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{2^{\nu-1}} \bmod \mathfrak{p}$$

clearly implies the solubility of the congruence

$$x^n \equiv \left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{n/2} \bmod \mathfrak{p}.$$

If $\zeta_4 \in K$ then $\zeta_{2^\tau} \in K$ and the equalities

$$-1 = \zeta_{2^{\nu+1}}^{n} \quad \text{if} \quad \nu < \tau,$$

$$(-1)^{n/2^\tau} \left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{n/2} = \left(\zeta_{2^\tau} + 1\right)^n, \quad \text{if} \quad \nu \geqslant \tau$$

show that the conditions (ii), (iii), (iv) imply (i).

If $\tau = 2$ and $n \not\equiv 0 \bmod 2^\tau$ we have either $n \equiv 1 \bmod 2$ in which case $-\gamma^n = (-\gamma)^n$ or $n \equiv 2 \bmod 4$. In the latter case we get from (ii)

$$\beta \prod_{i=1}^{k} \alpha_i^{nm_i/n_i} \prod_{n_i \text{ even}} \alpha_i^{l_i n/2} = (\gamma\delta)^n,$$

which leads to (i). The proof is complete. □

Proof of Corollary 1 follows at once from Lemma 8. □

Proof of Corollary 2. If the congruences $x^n \equiv \alpha \bmod \mathfrak{p}$ and $x^n \equiv \beta \bmod \mathfrak{p}$ are for almost all $\mathfrak{p}$ simultaneously soluble or insoluble, we have by Theorem 1 the following seven possibilities:

$$\alpha \overset{n}{=} \beta^t, \quad \beta \overset{n}{=} \alpha^s; \tag{58}$$

$$n \not\equiv 0 \bmod 2^\tau, \quad \alpha \overset{n}{=} \beta^t = -\delta^2, \quad \beta \overset{n}{=} -\alpha^s; \tag{59}$$

$$n \equiv 2^\tau \bmod 2^{\tau+1}, \quad \alpha \overset{n}{=} \beta^t = -\delta^2, \quad \beta \overset{n}{=} -\omega\alpha^s; \tag{60}$$

$$n \equiv 0 \bmod 2^{\tau+1}, \quad \alpha \overset{n}{=} \beta^t, \quad \beta \overset{n}{=} \omega\alpha^s; \tag{61}$$

$$n \not\equiv 0 \bmod 2^\tau, \quad \alpha \overset{n}{=} -\beta^t = -\delta_1^2, \quad \beta \overset{n}{=} -\alpha^s = -\delta_2^2; \tag{62}$$

$$n \equiv 2^\tau \bmod 2^{\tau+1}, \quad \alpha \overset{n}{=} -\omega\beta^t = -\delta_1^2, \quad \beta \overset{n}{=} -\omega\alpha^s = -\delta_2^2; \tag{63}$$

$$n \equiv 0 \bmod 2^{\tau+1}, \quad \alpha \overset{n}{=} \omega\beta^t, \quad \beta \overset{n}{=} \omega\alpha^s \tag{64}$$

and three other possibilities obtained by the permutation of α and β in (59), (60) and (61). Here $\gamma \overset{n}{=} \delta$ means that γ/δ is an nth power in K and $\omega = \left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{n/2}$. Moreover, in (59) to (64) it is assumed that $\zeta_4 \notin K$. Let us choose an integer x such that $u = s + (st-1)x$ is prime to n. If s is even or t is odd x will be chosen odd, which is possible because then $\big(s + st - 1, 2(st-1)\big) = 1$.

Now, (58) gives $\alpha \overset{n}{=} \alpha^{st}$, $\alpha^{st-1} \overset{n}{=} 1$, $\beta \overset{n}{=} \alpha^u$;

(59) gives $t \equiv 1 \bmod 2$, $\alpha \overset{n}{=} -\alpha^{st}$, $\alpha^{st-1} \overset{n}{=} -1$, $\beta \overset{n}{=} \alpha^u$;

(60) gives $t \equiv 1 \bmod 2$, $\alpha \overset{n}{=} -\omega\alpha^{st}$, $\alpha^{st-1} \overset{n}{=} -\omega$, $\beta \overset{n}{=} \alpha^u$;

(61) gives $\alpha \overset{n}{=} \omega^t\alpha^{st}$, $\alpha^{st-1} \overset{n}{=} \omega^t$, $\beta \overset{n}{=} \omega^{t+1}\alpha^u$;

(62) gives $s \equiv t \equiv 0 \bmod 2$. Indeed, if for instance $t \equiv 1 \bmod 2$ then $-\delta_1^2 = -\beta^t = \delta_2^{2t}$ and $\zeta_4 \in K$. If $s \equiv t \equiv 0 \bmod 2$ then $\alpha \overset{n}{=} -\alpha^{st}$, $\alpha^{st-1} \overset{n}{=} -1$, $\beta \overset{n}{=} \alpha^u$.

(63) gives like (62) that $s \equiv t \equiv 0 \bmod 2$. In that case $\alpha \overset{n}{=} -\omega\alpha^{st}$, $\alpha^{st-1} \overset{n}{=} -\omega$, $\beta \overset{n}{=} \alpha^u$.

Finally (64) gives $\alpha \overset{n}{=} \omega^{t+1}\alpha^{st}$, $\alpha^{st-1} \overset{n}{=} \omega^{t+1}$, $\beta \overset{n}{=} \omega^{t+x+1}\alpha^u$.

On the other hand, if $\beta \overset{n}{=} \alpha^u$ or $n \equiv 0 \bmod 2^{\tau+1}$ and $\beta \overset{n}{=} \omega\alpha^u$, where $(u, n) = 1$ then also $\alpha \overset{n}{=} \beta^v$ or $\alpha \overset{n}{=} \omega\beta^v$, respectively and by Theorem 1 the congruences $x^n \equiv \alpha \bmod \mathfrak{p}$ and $x^n \equiv \beta \bmod \mathfrak{p}$ are simultaneously soluble or insoluble for almost all prime ideals $\mathfrak{p}$ of K. □

To prove Theorem 2 we need two lemmata both due to Skolem.

Lemma 10. *In every algebraic number field K there exists an infinite sequence of elements π_j such that every element of K is represented uniquely in the form $\zeta \prod_{j=1}^{l} \pi_j^{d_j}$, where ζ is a root of unity and d_j are rational integers.*

Proof. See [9]. □

Lemma 11. *If a system of linear congruences is soluble for all moduli, then the corresponding system of equations is soluble in rational integers.*

Proof. See [7]. □

Proof of Theorem 2. Let

$$\alpha_i = \zeta_w^{a_{i0}} \prod_{j=1}^{l} \pi_j^{a_{ij}}, \quad \beta = \zeta_w^{b_0} \prod_{j=1}^{l} \pi_j^{b_j},$$

where w is the number of roots of unity contained in K, π_j have the property asserted in Lemma 10 and a_{ij}, b_j are rational integers. If the congruence

$$\alpha_1^{x_1} \cdots \alpha_k^{x_k} \equiv \beta \bmod \mathfrak{p}$$

is soluble for almost all $\mathfrak{p}$ then for every positive integer n the solubility of the k congruences $x^n \equiv \alpha_i \bmod \mathfrak{p}$ $(1 \leqslant i \leqslant k)$ implies the solubility of $x^n \equiv \beta \bmod \mathfrak{p}$. It follows hence by Theorem 1 with $n = 2^{\tau+1}m$ that for every positive integer n there exist $\gamma \in K$ and rational integers $m_1, \ldots, m_k$ such that

$$\beta \alpha_1^{m_1} \cdots \alpha_k^{m_k} = \gamma^m.$$

By Lemma 10 the last equality implies for a suitable m_0

$$b_0 + \sum_{i=1}^{k} a_{i0} m_i + w m_0 \equiv 0 \bmod m,$$

$$b_j + \sum_{i=1}^{k} a_{ij} m_i \equiv 0 \bmod m \quad (1 \leqslant j \leqslant l).$$

By Lemma 11 there exist rational integers $m_0, \ldots, m_k$ such that

$$b_0 + \sum_{i=1}^{k} a_{i0} m_i + w m_0 = 0,$$

$$b_j + \sum_{i=1}^{k} a_{ij} m_i = 0 \quad (1 \leqslant j \leqslant l)$$

and this gives

$$\beta = \prod_{i=1}^{k} \alpha_i^{m_i}. \qquad \square$$

The above proof is modelled on Skolem's proof ([7]) of his theorem that the solubility of the congruence $\alpha_1^{x_1} \cdots \alpha_k^{x_k} \equiv \beta \bmod \mathfrak{m}$ for all moduli implies the solubility of the corresponding equation. That proof uses instead of Theorem 1 the case $D = 1$ of the following

Lemma 12. *Let $\xi_0 = \zeta_w, \xi_1, \ldots, \xi_t$ be any t distinct terms of the sequence π_j. For any positive integer m there exists $\mu \in K$ prime to D such that the congruence*

$$\xi_0^{y_0} \xi_1^{y_1} \cdots \xi_t^{y_t} \equiv 1 \bmod \mu$$

implies $y_0 \equiv 0 \bmod w$, $y_1 \equiv \ldots \equiv y_t \equiv 0 \bmod m$.

Skolem's proof of the above lemma given only in the case of fields with class number one is defective because he claims the existence of prime ideals $\mathfrak{p}_0, \ldots, \mathfrak{p}_l$ of K such that $x^m \equiv \xi_r \bmod \mathfrak{p}_s$ is soluble for $r \neq s$ and $x^m \equiv \xi_r^j \bmod \mathfrak{p}_r$ is insoluble for $j \not\equiv 0 \bmod m$,

$_c$ $r \neq 0$ and $j \not\equiv 0 \bmod (m, w)$, $r = 0$. The assertion is false for $K = \mathbb{Q}$, $t = 1$, $\xi_1 = 2$, $m = 4$.

Proof of Lemma 12. We can assume without loss of generality that $m \equiv 0 \bmod 2^{\tau+1} w$. For every $p \mid m$ set $n = m(p, 2)$. Suppose that the solubility of

$$x^n \equiv \xi_i \bmod \mathfrak{p} \quad (i \neq r \neq 0) \tag{65}$$

implies the solubility of

$$x^n \equiv \xi_r^{m/p} \bmod \mathfrak{p} \tag{66}$$

for almost all $\mathfrak{p}$. Then by Theorem 1

$$\xi_r^{m/p} \prod_{i \neq r} \xi_i^{m_i} = \gamma^{n/2}$$

for suitable $\gamma \in K$ and suitable exponents m_i. We get

$$\frac{m}{p} \equiv 0 \bmod \frac{n}{2}, \quad \frac{m}{p} \equiv 0 \bmod \frac{m(p,2)}{2},$$

which is impossible.

The obtained contradiction shows that for a certain prime ideal $\mathfrak{p}$ prime to D the congruences (65) are soluble, but (66) is insoluble. Denoting this prime ideal by $\mathfrak{p}_{p,r}$ we infer from

$$\xi_0^{x_0} \xi_1^{x_1} \cdots \xi_t^{x_t} \equiv 1 \bmod \mathfrak{p}_{p,r}$$

that

$$\big(m(p,2), x_r\big) \nmid \frac{m}{p},$$

hence

$$\operatorname{ord}_p x_r \geqslant \operatorname{ord}_p m.$$

If $p \mid w$, suppose that the solubility of the congruences

$$x^n \equiv \xi_i \bmod \mathfrak{p} \quad (1 \leqslant i \leqslant t) \tag{67}$$

implies the solubility of the congruence

$$x^n \equiv \zeta_p \bmod \mathfrak{p} \tag{68}$$

for almost all $\mathfrak{p}$. Then by Theorem 1

$$\zeta_p \prod_{i=1}^{t} \xi_i^{m_i} = \gamma^{n/2}$$

for suitable $\gamma \in K$ and suitable exponents m_i. We get

$$\frac{w}{p} \equiv 0 \bmod \Big(\frac{n}{2}, w\Big), \quad \frac{w}{p} \equiv 0 \bmod \frac{w(p,2)}{2}.$$

The obtained contradiction shows that for a certain prime ideal $\mathfrak{p}$ prime to D the congruences (67) are soluble, but (68) is insoluble. Denoting this prime ideal by $\mathfrak{p}_{p,0}$ we infer from

$$\xi_0^{x_0}\xi_1^{x_1}\cdots\xi_t^{x_t} \equiv 1 \bmod \mathfrak{p}_{p,0}$$

that

$$(x_0, w) \nmid \frac{w}{p}$$

hence $\operatorname{ord}_p x_0 \geqslant \operatorname{ord}_p w$.

For μ we can choose any number prime to D divisible by

$$\prod_{p|m}\prod_{r=1}^{k}\mathfrak{p}_{p,r}\prod_{p|w}\mathfrak{p}_{p,0}. \qquad \square$$

Proof of Theorem 3. Let for $i \leqslant h$, $j \leqslant k$

$$\alpha_{ij} = \prod_{s=0}^{t}\xi_s^{a_{ijs}}, \quad \beta_i = \prod_{s=0}^{t}\xi_s^{a_{i0s}}$$

in the notation of Lemma 12 and let m, D be positive integers.

Let μ be a modulus with the property asserted in Lemma 12. Then the congruences

$$\prod_{j=1}^{k}\alpha_{ij}^{x_j} \equiv \beta_i \bmod \mu \quad (i = 1, \ldots, h)$$

imply

$$\sum_{j=1}^{k} a_{ij0}x_j \equiv a_{i00} \bmod w \quad (i = 1, \ldots, h),$$

$$\sum_{j=1}^{k} a_{ijs}x_j \equiv a_{i0s} \bmod m \quad (i = 1, \ldots, h;\ s = 1, \ldots, t)$$

and by Lemma 11 there exist rational integers x_j $(j = 1, \ldots, k)$, y_i $(i = 1, \ldots, h)$ satisfying the system of equations

$$\sum_{j=1}^{k} a_{ij0}x_j = a_{i00} + wy_i \quad (i = 1, \ldots, h),$$

$$\sum_{j=1}^{k} a_{ijs}x_j = a_{i0s} \quad (i = 1, \ldots, h;\ s = 1, \ldots, t).$$

Hence

$$\prod_{j=1}^{k} \alpha_{ij}^{x_j} = \beta_i \quad (i = 1, \ldots, h).$$

The proof is complete. □

We proceed to the example showing that Theorem 3 is no longer valid if the solubility for all moduli prime to D is replaced by the solubility for all prime moduli.

Let us consider the system

$$\begin{aligned} 2^x 3^y &\equiv 1 \bmod p, \\ 2^y 3^z &\equiv 4 \bmod p. \end{aligned} \tag{69}$$

For $p = 2, 3$ it has the solution $(x, y, z) = (0, 1, 0), (0, 0, 0)$, respectively. For other p it is equivalent to the system

$$\begin{aligned} x \operatorname{ind} 2 + y \operatorname{ind} 3 &\equiv 0 \bmod p - 1, \\ y \operatorname{ind} 2 + z \operatorname{ind} 3 &\equiv 2 \operatorname{ind} 2 \bmod p - 1, \end{aligned} \tag{70}$$

where indices are taken with respect to a fixed primitive root $\bmod p$. Now

$$\left((\operatorname{ind} 2)^2, (\operatorname{ind} 3)^2\right) \mid \operatorname{ind} 2 \operatorname{ind} 3.$$

Hence

$$\left(\frac{(\operatorname{ind} 2)^2}{(\operatorname{ind} 2, \operatorname{ind} 3)}, \operatorname{ind} 3\right) \Big| \operatorname{ind} 2$$

and the equation

$$t \frac{(\operatorname{ind} 2)^2}{(\operatorname{ind} 2, \operatorname{ind} 3)} + z \operatorname{ind} 3 = 2 \operatorname{ind} 2$$

is soluble in integers. The numbers $x = \dfrac{-t \operatorname{ind} 3}{(\operatorname{ind} 2, \operatorname{ind} 3)}$, $y = \dfrac{t \operatorname{ind} 2}{(\operatorname{ind} 2, \operatorname{ind} 3)}$ and z satisfy the system (70) and hence also (69).

References

[1] H. Flanders, *Generalization of a theorem of Ankeny and Rogers*. Ann. of Math. (2) 57 (1953), 392–400.

[2] I. Gerst, *On the theory of n-th power residues and a conjecture of Kronecker*. Acta Arith. 17 (1970), 121–139.

[3] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper* II. Jahresber. der Deutschen Mathematiker-Vereinigung 6 (1930); reprint: Physica-Verlag, Würzburg–Wien 1965.

[4] —, *Zum Existenzsatz von Grunwald in der Klassenkörpertheorie*. J. Reine Angew. Math. 188 (1950), 40–64.

[5] H. B. Mann, *Introduction to Algebraic Number Theory*. The Ohio Univ. Press, Columbus 1955.

[6] A. Schinzel, *A refinement of a theorem of Gerst on power residues*. Acta Arith. 17 (1970), 161–168.

[7] Th. Skolem, *Anwendung exponentieller Kongruenzen zum Beweis der Unlösbarkeit gewisser diophantischer Gleichungen*. Vid. Akad. Avh. Oslo I 1937 nr. 12.

[8] —, *Diophantische Gleichungen*. Berlin, 1938.

[9] —, *On the existence of a multiplicative basis for an arbitrary algebraic field*. Norske Vid. Selsk. Forh. (Trondheim) 20 (1947), no. 2, 4–7.

Andrzej Schinzel
Selecta

Originally published in
Acta Arithmetica XXXII (1977), 245–274

Abelian binomials, power residues and exponential congruences*

In memory of Marceli Stark

This paper supplements the results of [6] concerning power residues and extends those pertaining to exponential congruences. We begin however with the study of binomials. G. Darbi [1] and E. Bessel-Hagen (cf. [10], p. 302) have found all binomials $x^n - a$ normal over the rational field $\mathbb{Q}$. (Their argument extends to fields K such that a primitive n-th root of unity ζ_n is of degree $\varphi(n)$ over K.) We shall do the same for an arbitrary field and n equal to a prime power. In fact, we shall prove

Theorem 1. *Let K be a field, p a prime different from the characteristic of K. A binomial $x^{p^\nu} - \alpha$ is the product of factors normal over K if and only if at least one of the following conditions is satisfied for a suitable integer λ and a suitable $\gamma \in K$:*

(i) $\alpha^{p^{\min(\omega,\nu)}} = \gamma^{p^\nu}$;

(ii) $p = 2$, $\omega = 1$, $\nu \leqslant \tau$, $\alpha = -\gamma^2$;

(iii) $p = 2$, $\omega = 1$, $\nu = \tau + 1$, $\alpha = -\gamma^2$, $\sqrt{-\left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)} \in K$;

(iv) $p = 2$, $\omega = 1$, $\nu = \tau + 1$, $\alpha = -\left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{2^\lambda} \gamma^{2^{\lambda+1}}$, $1 \leqslant \lambda \leqslant \tau - 2$;

(v) $p = 2$, $\omega = 1$, $\nu \geqslant \tau + 2$, $\alpha = -\left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{2^{\nu-2}} \gamma^{2^{\nu-1}}$.

Here ω is the greatest integer such that $\zeta_{p^\omega} \in K$ if there are only finitely many of them, $\omega = \infty$ otherwise; τ is the greatest integer such that $\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} \in K$ if there are only finitely many of them, $\tau = \infty$ otherwise.

If the binomial in question is irreducible (iv) *implies* $\sqrt{-\left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)} \notin K$, $\lambda = 1$, $\tau \geqslant 3$; (v) *implies* $\tau = 2$.

Theorem 2. *Let n be a positive integer not divisible by the characteristic of K. A binomial $x^n - \alpha$ has over K an abelian Galois group if and only if $\alpha^{w_n} = \gamma^n$, where $\gamma \in K$ and w_n is the number of n-th roots of unity contained in K. When a binomial satisfying this condition is irreducible then its group is cyclic if $n \not\equiv 0 \bmod 4$ or $\zeta_4 \in K$ and the product of cyclic groups of order 2 and $n/2$ otherwise.*

From Theorem 2 and a result of Hasse [2] concerning the case $n = p^\nu$ we shall deduce

Addendum and corrigendum, Acta Arith. 36 (1980), 101–104.

* Written within the Research Program I.1.

Theorem 3. *Let n be a positive integer not divisible by the characteristic of K. If*

$$\alpha = \vartheta^n, \quad \vartheta \in K(\zeta_n)$$

then

$$\alpha^\sigma = \gamma^n, \quad \gamma \in K,$$

where

(vi) $$\sigma = \Big(w_n, \quad \underset{\substack{q \mid n \\ q \text{ prime or } q=4}}{\text{l.c.m.}} \quad [K(\zeta_q) : K]\Big).$$

Moreover if for a certain m prime to n

(vii) $$\begin{cases} \text{either } \zeta_{(4,n)} \in K \text{ and } nm \equiv 0 \bmod w_n \underset{\substack{q \mid n \\ q \text{ prime}}}{\text{l.c.m.}} [K(\zeta_q) : K] \\ \text{or } \zeta_{(4,n)} \notin K,\ \tau < \infty \text{ and } nm \equiv 0 \bmod 2^\tau w_n \underset{\substack{q \mid n \\ q \text{ prime}}}{\text{l.c.m.}} [K(\zeta_q) : K] \end{cases}$$

then

$$\alpha = \gamma^{n/\sigma}, \quad \gamma \in K.$$

Next we shall assume that K is an algebraic number field and prove the following extension of Kummer's theorem (see [3], Satz 152) on power residues.

Theorem 4. *Let K be an algebraic number field, w the number of roots of unity contained in K, σ given by* (vi). *If $\alpha_1, \ldots, \alpha_k \in K^*$ are such that*

(viii) $$\alpha_1^{\sigma x_1} \cdots \alpha_k^{\sigma x_k} = \gamma^n, \quad \gamma \in K \text{ implies } x_1 \equiv x_2 \equiv \ldots \equiv x_k \bmod n/\sigma$$

then for any integers $c_1, \ldots, c_k \equiv 0 \bmod \sigma$ there exist infinitely many prime ideals $\mathfrak{p}$ of $K(\zeta_n)$ such that

$$\left(\frac{\alpha_i}{\mathfrak{p}}\right)_n = \zeta_n^{c_i}.$$

If $\alpha_1, \ldots, \alpha_k$ satisfy the stronger condition that

(ix) $$\zeta_w^{x_0} \alpha_1^{x_1} \cdots \alpha_k^{x_k} = \gamma^{n/\sigma} \text{ implies } x_1 \equiv x_2 \equiv \ldots \equiv x_k \equiv 0 \bmod n/\sigma$$

and n satisfies the condition (vii) *of Theorem* 3 *then for any integers $c_1, \ldots, c_k \equiv 0 \bmod \sigma$ and any c_0 there exist infinitely many prime ideals $\mathfrak{p}$ of $K(\zeta_n)$ such that*

$$\left(\frac{\zeta_w}{\mathfrak{p}}\right)_n = \zeta_{(w,n)}^{c_0}, \quad \left(\frac{\alpha_i}{\mathfrak{p}}\right)_n = \zeta_n^{c_i}.$$

If $n = p^\nu$, p prime and $p > 2$ or $\nu = 1$ or $w \equiv 0 \bmod 4$ then the assertion holds without any restriction on c_i. Thus, for $n = p$, $\nu = 1$ we obtain Chebotarev's refinement [9] of Kummer's theorem. For $K = \mathbb{Q}$ and n arbitrary a more precise result has been obtained by Mills [5].

We shall use Theorem 4 to prove two theorems on exponential congruences.

Theorem 5. *Let $f(x)$ be a polynomial of degree g over K, $\alpha_1, \ldots, \alpha_k \in K^*$. If the congruence*

$$f(\alpha_1^{x_1} \cdots \alpha_k^{x_k}) \equiv 0 \bmod \mathfrak{p}$$

is soluble for almost all prime ideals $\mathfrak{p}$ of K then the equation $f(\alpha_1^{x_1} \cdots \alpha_k^{x_k}) = 0$ is soluble in rational numbers $x_1, \ldots, x_k$ with the least common denominator not exceeding $\max\{1, g-1\}$.

This is a generalization of Theorem 2 of [6] and the examples which we give further show that it is essentially best possible.

Corollary. *Let a sequence u_n of rational integers satisfy the recurrence relation $u_{n+1} = au_n + bu_{n-1}$, where $a^2 + 4b \neq 0$. If the congruence $u_n \equiv c \bmod p$ is soluble for almost all primes p and either $b = 0, -1$ or $b = 1$, $a \neq d^3 + 3d$ (d integer), then $c = u_m$ for an integer m.*

Here as in Theorem 5 almost all means all except a set of density zero.

It is conjectured that the Corollary holds for all recurring sequences of the second order satisfying $a^2 + 4b \neq 0$.

Theorem 6. *Let α_{hij}, β_{hi} be non-zero elements of K, D a positive integer. If the system of congruences*

$$\prod_{h=1}^{g_i}\left(\prod_{j=1}^{k} \alpha_{hij}^{x_j} - \beta_{hi}\right) \equiv 0 \bmod \mathfrak{m} \quad (i = 1, 2, \ldots, l)$$

is soluble for all moduli prime to D then the corresponding system of equations is soluble in integers.

This is a generalization of Theorem 3 of [6]. According to Skolem's conjecture Theorem 6 with $D = 1$ remains valid if

$$\prod_{h=1}^{g_i}\left(\prod_{j=1}^{k} \alpha_{hij}^{x_j} - \beta_{hi}\right)$$

is replaced by

$$\sum_{h=1}^{g_i} \beta_{hi} \prod_{j=1}^{k} \alpha_{hij}^{x_j},$$

but that we cannot prove.

Lemma 1. *If p is a prime different from the characteristic of K, $\zeta_p \in K$, $\xi^{p^\mu} \in K^*$, $\eta^{p^\nu} \in K^*\langle\xi\rangle$ and $\eta \in K(\xi)$ then either $\eta \in K^*\langle\xi\rangle$ or $p = 2$, $\zeta_4 \notin K$ and $\zeta_4 \in K^*\langle\xi\rangle$. Here $K^*\langle\xi\rangle$ is the multiplicative group generated by K^* and ξ.*

Proof. For $p > 2$ this is an easy consequence of a theorem of Kneser [4], since however for $p = 2$ we have to go through Kneser's proof all over again, we can cover at once the general case. The proof is by induction with respect to μ and ν. If $\mu = 0$ or $\nu = 0$ the lemma is obvious. Assume it is true for $\mu = m - 1$ and all ν. We prove it first for $\mu = m$, $\nu = 1$.

Suppose that $\xi \in K(\xi^p)$. Then using the inductive assumption with $\xi_1 = \xi^p$, $\eta_1 = \xi$, $\nu_1 = 1$ we get either $\xi \in K^*\langle\xi^p\rangle$ or $p = 2$, $\zeta_4 \notin K$ and $\zeta_4 \in K^*\langle\xi^2\rangle$. The former possibility gives $\xi \in K$, the latter $\zeta_4 \in K^*\langle\xi\rangle$, thus in this case lemma holds.

Suppose now that $\xi \notin K(\xi^p)$. Then also $\xi\zeta_p \notin K(\xi^p)$, ξ satisfies over $K(\xi^p)$ the irreducible equation $x^p - \xi^p = 0$ and denoting by N the norm from $K(\xi)$ to $K(\xi^p)$ we have

$$N\xi = (-1)^{p-1}\xi^p.$$

On the other hand, $\eta^p \in K^*\langle\xi\rangle$, hence $\eta^p = a\xi^{pk+q}$, where $0 \leqslant q < p$, $a \in K^*$. Consider first the case $q > 0$. Taking the norms of both sides we get

$$\left((-1)^{p-1}\xi^p\right)^q = (N\eta)^p a^{-p}\xi^{-p^2k}.$$

For $p > 2$ it follows that $\xi^p \in K(\xi^p)^p$ and $\xi \in K(\xi^p)$ which has been excluded. For $p = 2$ we get

$$-\xi^2 = (N\eta)^2 a^{-2}\xi^{-4k}, \quad \zeta_4\xi \in K(\xi^2), \quad \eta^2 = \pm\zeta_4 N(\eta),$$

hence $\zeta_4 \in K(\xi)$, $\zeta_4 \notin K(\xi^2)$. Writing $\eta = g + \zeta_4 h$ with $g, h \in K(\xi^2)$ we obtain $g^2 = h^2$, $\eta = (1 \pm \zeta_4)g$. Hence $g^4 = -\eta^4/4 \in K^*\langle\xi^2\rangle$ and by the inductive assumption with $\xi_1 = \xi^2$, $\eta_1 = g$, $\nu_1 = 2$ we infer that $g \in K^*\langle\xi^2\rangle$, $\zeta_4 = \pm\frac{1}{2}\eta^2 g^{-2} \in K^*\langle\xi\rangle$.

Consider now the case $q = 0$. Let S be an automorphism of the normal closure of $K(\xi)$ over $K(\xi^p)$ such that $S\xi = \xi\zeta_p$. From $q = 0$ we infer that $\eta^p \in K(\xi^p)$, $S\eta^p = \eta^p$, $S\eta = \zeta_p^r\eta$. It follows that $S(\eta\xi^{-r}) = \eta\xi^{-r}$, $\eta\xi^{-r} \in K(\xi^p)$. Since $\eta^p\xi^{-rp} \in K^*\langle\xi^p\rangle$, we apply the inductive assumption with $\xi_1 = \xi^p$, $\eta_1 = \eta\xi^{-r}$, $\nu_1 = 1$ and obtain that $\eta\xi^{-r} \in K^*\langle\xi^p\rangle$ or $p = 2$, $\zeta_4 \notin K$, $\zeta_4 \in K^*\langle\xi^2\rangle$. The former possibility gives $\eta \in K^*\langle\xi\rangle$ and the proof for $\mu = m$, $\nu = 1$ is complete. Assume now that $n \geqslant 2$, the lemma holds for $\mu = m$, $\nu < n$ and that $\eta^{p^n} \in K^*\langle\xi\rangle$. Using the inductive assumption with $\eta_1 = \eta^p$, $\nu_1 = n - 1$, we get $\eta^p \in K^*\langle\xi\rangle$, or $p = 2$, $\zeta_4 \notin K$ and $\zeta_4 \in K^*\langle\xi\rangle$. In the former case we use the inductive assumption with $\nu_1 = 1$ and obtain $\eta \in K^*\langle\xi\rangle$, which completes the inductive proof. □

Lemma 2. *Let K be a field of characteristic different from 2. If $\vartheta \in K(\zeta_4)$, $\vartheta^{2^\nu} \in K$ then at least one of the following four conditions is satisfied for a suitable $\gamma \in K$:*

$$\vartheta^{2^\nu} = \gamma^{2^\nu}; \tag{1}$$

$$\nu < \tau, \quad \vartheta^{2^\nu} = -\gamma^{2^\nu}; \tag{2}$$

$$\nu = \tau, \quad \vartheta^{2^\nu} = -\left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{2^{\nu-1}}\gamma^{2^\nu}; \tag{3}$$

$$\nu > \tau, \quad \vartheta^{2^\nu} = \left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{2^{\nu-1}}\gamma^{2^\nu}. \tag{4}$$

Proof. This is a special case, $n = 2^\nu$ of Lemma 7 of [6]. Let us remark that the conditions (3) and (4) do not depend upon the choice of ζ_{2^τ}. Indeed, for any odd j

$$\left(\zeta_{2^{\tau+1}}^{j} + \zeta_{2^{\tau+1}}^{-j}\right)\left(\zeta_{2^{\tau+1}} + \zeta_{2^{\tau+1}}^{-1}\right)^{-1} \in K,$$

hence

$$\left(\zeta_{2^\tau}^{j} + \zeta_{2^\tau}^{-j} + 2\right)^{2^{\nu-1}}\left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{-2^{\nu-1}} \in K^{2^\nu}.$$

(The same remark applies to the general case.) □

Lemma 3. *Let τ_1 be the greatest integer such that $\zeta_{2^{\tau_1}} \in K(\zeta_4)$, if there are only finitely many of them, $\tau_1 = \infty$ otherwise. Then*

$$\tau_1 = \begin{cases} \tau + 1 & \text{if } \tau < \infty \text{ and } \sqrt{-\left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)} \in K, \\ \tau & \text{otherwise.} \end{cases}$$

Proof. We have for all $\sigma \geqslant 2$

$$2\zeta_{2^\sigma} = \left(\zeta_{2^\sigma} + \zeta_{2^\sigma}^{-1}\right) + \zeta_4\left(\zeta_{2^\sigma}^{1-2^{\sigma-2}} + \zeta_{2^\sigma}^{-1+2^{\sigma-2}}\right)$$

which implies $\tau_1 \geqslant \tau$. If we had $\tau < \infty$ and $\zeta_{2^{\tau+2}} \in K(\zeta_4)$ it would follow by Lemma 2 that

$$-1 = \zeta_{2^{\tau+2}}^{2^{\tau+1}} = \gamma^{2^{\tau+1}} \quad \text{or} \quad \left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{2^\tau}\gamma^{2^{\tau+1}}, \quad \gamma \in K,$$

hence $\zeta_4 \in K$ and $\zeta_{2^{\tau+2}} \in K$, $\zeta_{2^{\tau+2}} + \zeta_{2^{\tau+2}}^{-1} \in K$ contrary to the definition of τ. This proves $\tau_1 < \tau + 2$.

If $\zeta_{2^{\tau+1}} \in K(\zeta_4)$, then $\zeta_4 \notin K$ and ζ_{2^τ} is conjugate over K to $\zeta_{2^\tau}^{-1}$. Hence $\zeta_4\zeta_{2^{\tau+1}}$ is conjugate over K either to $\zeta_4\zeta_{2^{\tau+1}}^{-1}$ or to $-\zeta_4\zeta_{2^{\tau+1}}^{-1}$. However the latter possibility gives $\zeta_{2^{\tau+1}}^{1+2^{\tau-1}} + \zeta_{2^{\tau+1}}^{-1-2^{\tau-1}} \in K$ contrary to the definition of τ. Thus the former possibility holds and $\zeta_4\zeta_{2^{\tau+1}} + \zeta_4\zeta_{2^{\tau+1}}^{-1} \in K$, $\sqrt{-\left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)} \in K$. Conversely if $\sqrt{-\left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)} \in K$ then

$$\zeta_{2^{\tau+1}} + \zeta_{2^{\tau+1}}^{-1} \in K(\zeta_4) \quad \text{and} \quad \zeta_{2^{\tau+1}} = \frac{\zeta_{2^\tau} + 1}{\zeta_{2^{\tau+1}} + \zeta_{2^{\tau+1}}^{-1}} \in K(\zeta_4).$$

This proves the lemma. □

Lemma 4. *If $\xi^{p^\mu} = \beta \in K$, $\zeta_{p^\mu} \in K(\xi)$ and either $p > 2$, $\zeta_p \in K$ or $p = 2$, $\zeta_4 \in K$ then*

$$\beta = \zeta_{p^\kappa}^{j}\gamma^{p^{\mu-\kappa}}, \quad 0 \leqslant \kappa \leqslant \min(\mu, \omega), \quad (j, p) = 1, \quad \gamma \in K.$$

Proof. By Lemma 1 we have in any case

$$\zeta_{p^\mu} \in K^*\langle\xi\rangle,$$

$$\zeta_{p^\mu} = \delta\xi^i, \quad \delta \in K^*, \quad 1 \leqslant i \leqslant p^\mu. \tag{5}$$

Let

$$i = p^{\kappa}h, \quad (h, p) = 1, \quad hj \equiv 1 \bmod p^{\mu-\kappa}.$$

Raising both sides of (5) to the power $p^{\mu-\kappa}j$ we get

$$\zeta_{p^{\kappa}}^{j} = \delta^{p^{\mu-\kappa}j}\beta^{hj},$$

hence $\kappa \leqslant \omega$ and the lemma holds with $\gamma = \beta^{(1-hj)p^{\kappa-\mu}}\delta^{-j}$. □

Proof of Theorem 1. *Necessity.* Assume that $x^{p^{\nu}} - \alpha$ is the product of normal factors. Let μ be the least nonnegative integer such that

$$\alpha = \beta^{p^{\nu-\mu}}, \quad \beta \in K.$$

If $\mu = 0$ then the theorem holds with $\gamma = \beta^{\min(\nu,\omega)}$. If $\mu > 0$ then

$$\beta \neq \zeta_{p^{\nu-\mu}}^{j}\delta^{p}, \quad \delta \in K. \tag{6}$$

Hence if $p > 2$ or $p = 2$, $\zeta_4 \in K$, then $x^{p^{\mu}} - \beta$ is irreducible and by the assumption normal. Denoting any of its zeros by ξ we get

$$\zeta_{p^{\mu}} \in K(\xi), \quad \zeta_p \in K(\xi) \tag{7}$$

and since $[K(\xi) : K] = p^{\mu}$, $[K(\zeta_p) : K] \mid p - 1$, it follows that $\zeta_p \in K$. By Lemma 4 we have

$$\beta = \zeta_{p^{\kappa}}^{j}\gamma^{p^{\mu-\kappa}}; \quad 0 \leqslant \kappa \leqslant \min(\mu, \omega) \tag{8}$$

and $\alpha^{p^{\kappa}} = \gamma^{p^{\nu}}$, which proves (i).

Assume now that $p = 2$, $\zeta_4 \notin K$. Then either $x^{2^{\mu}} - \beta$ is irreducible or $\mu \geqslant 2$, $\beta = -4\delta^4$, $\delta \in K$. In the former case we get again (7) for any zero ξ of $x^{2^{\mu}} - \beta$, in the latter case let ϱ be the least nonnegative integer such that

$$(1 + \zeta_4)\delta = \eta^{2^{\mu-2-\varrho}}, \quad \eta \in K(\zeta_4).$$

The binomial $x^{2^{\varrho}} - \eta$ is irreducible over $K(\zeta_4)$, hence

$$f(x) = N_{K(\zeta_4)/K}(x^{2^{\varrho}} - \eta)$$

is irreducible over K. The polynomial $f(x)$ is a factor of

$$N_{K(\zeta_4)/K}\left(x^{2^{\mu-2}} - \eta^{2^{\mu-2-\varrho}}\right) = x^{2^{\mu-1}} + 2\delta x^{2^{\mu-2}} + 2\delta^2 \mid x^{2^{\mu}} + 4\delta^4,$$

hence it is normal. Let ξ be a zero of $x^{2^{\varrho}} - \eta$, ξ' a zero of $x^{2^{\varrho}} - \eta'$, where η' is conjugate to η over K. We have

$$\frac{\xi'}{\xi} \in K(\xi), \tag{9}$$

on the other hand

$$\left(\frac{\xi'}{\xi}\right)^{2^{\mu-2}} = \left(\frac{\eta'}{\eta}\right)^{2^{\mu-2-\varrho}} = \frac{(1 - \zeta_4)\delta}{(1 + \zeta_4)\delta} = -\zeta_4,$$

hence $\xi'/\xi = \zeta_{2^\mu}^j$, $(j,2)=1$ and from (9) we get again (7). Using now Lemma 1 we get $\zeta_4 \in K^*\langle\xi\rangle$. Hence

$$\zeta_4 = \delta\xi^i, \quad \delta \in K, \tag{10}$$

$$2 = [K^*\langle\zeta_4\rangle : K^*] = [K^*\langle\xi^i\rangle : K^*] = 2^{\mu-\operatorname{ord}_2 i}, \quad i = 2^{\mu-1}j, \quad (j,2)=1$$

and on squaring both sides of (10) we get

$$-1 = \delta^2\beta^j, \quad \beta = -\gamma^2.$$

It follows from (6) that $\mu = \nu$

$$\alpha = \beta = -\gamma^2. \tag{11}$$

On the other hand, applying Lemma 4 to the field $K(\zeta_4)$ we get

$$\alpha = \zeta_{2^\sigma}\vartheta^{2^{\nu-\sigma}}, \quad 0 \leqslant \sigma \leqslant \min(\nu, \tau_1), \quad \vartheta \in K(\zeta_4).$$

If $\nu \leqslant \tau_1$, then by (11) and Lemma 3 we have (ii) or (iii). If $\nu > \tau_1$ then, since $\zeta_4 \notin K$ by (11) and Lemma 2, $\sigma = 0$ is impossible. We get

$$\alpha^{2^{\sigma-1}} = -\vartheta^{2^{\nu-1}}$$

and by Lemma 2 either

$$\alpha^{2^{\sigma-1}} = -\gamma^{2^{\nu-1}}, \quad \gamma \in K \tag{12}$$

or

$$\nu - 1 = \tau = \tau_1, \quad \alpha^{2^{\sigma-1}} = \left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{2^{\tau-1}}\gamma^{2^\tau} \tag{13}$$

or

$$\nu - 1 > \tau, \quad \alpha^{2^{\sigma-1}} = -\left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{2^{\nu-2}}\gamma^{2^{\nu-1}} \tag{14}$$

Since $\zeta_4 \notin K$, (12) and (14) imply $\sigma = 1$ and then we get (i) or (v) respectively. Finally (13) in view of (11) implies $\sigma > 1$

$$\alpha = \pm\left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{2^{\tau-\sigma}}\gamma^{2^{\tau-\sigma+1}},$$

again by (11) and Lemma 3, $\sigma < \tau$ and the upper sign is excluded. This gives (iv).

Sufficiency. To prove the sufficiency of (i) we proceed by induction with respect to ν. The case $\nu \leqslant \omega$ is trivial. If $\nu > \omega$ (i) gives

$$\alpha = \zeta_{p^\kappa}\gamma^{p^{\nu-\omega}}, \quad 0 \leqslant \kappa \leqslant \omega. \tag{15}$$

If $\kappa < \omega$ we have

$$x^{p^\nu} - \alpha = \prod_{j=0}^{p-1}\left(x^{p^{\nu-1}} - \zeta_p^j\zeta_{p^{\kappa+1}}\gamma^{p^{\nu-\omega-1}}\right).$$

Each of the factors on the right hand side is by the inductive assumption the product of normal factors, hence the same holds for $x^{p^\nu} - \alpha$. If $\kappa = \omega = 0$ we have

$$x^{p^\nu} - \alpha = \alpha \prod_{\mu=0}^{\nu} X_{p^\mu}\Big(\frac{x}{\gamma}\Big),$$

where $X_n(x)$ is the nth cyclotomic polynomial. Every zero of $X_n\Big(\frac{x}{\gamma}\Big)$ generates over K all the other zeros, hence the desired result.

Finally if $\kappa = \omega > 0$ let ξ denote as in the sequel any zero of $x^{p^\nu} - \alpha$.

We have by (15)

$$\big(\xi^{p^\omega}\gamma^{-1}\big)^{p^{\nu-\omega}} = \zeta_{p^\omega}$$

[c] hence for an integer j

$$\zeta_{p^\nu} = \big(\xi^{p^\omega}\gamma^{-1}\big)^j.$$

If (ii) or (iii) holds then

$$\zeta_4 = \pm\xi^{2^{\nu-1}}\gamma^{-1}.$$

Since, by Lemma 3, $\nu \leqslant \tau_1$ and by definition $\zeta_{2^{\tau_1}} \in K(\zeta_4)$, it follows that

$$\zeta_{2^\nu} \in K(\xi).$$

If (iv) holds then

$$\xi^{2^{\tau-\lambda}} = \zeta_{2^{\lambda+2}}^j \gamma\big(\zeta_{2^{\tau+1}} + \zeta_{2^{\tau+1}}^{-1}\big), \quad (j,2) = 1,$$

thus

$$\xi^{2^{\tau-\lambda}}\zeta_{2^{\tau+1}} \in K(\zeta_{2^\tau}), \quad \zeta_4 \in K(\xi^{2^\tau}).$$

Since, by Lemma 3, $K(\zeta_{2^\tau}) = K(\zeta_4)$ it follows that

$$\xi^{2^{\tau-\lambda}}\zeta_{2^{\tau+1}} \in K(\xi^{2^\tau})$$

and

$$\zeta_{2^{\tau+1}} \in K(\xi).$$

If (v) holds then

$$\xi^2 = \zeta_{2^\nu}^j\big(\zeta_{2^{\tau+1}} + \zeta_{2^{\tau+1}}^{-1}\big)\gamma, \quad (j,2) = 1,$$

thus $\xi^2 \in K(\zeta_{2^\nu})$. We shall show that ξ^2 has as many distinct conjugates over K as ζ_{2^ν}. Indeed, if S is an automorphism of $K(\zeta_{2^\nu})$ over K then

$$S\big(\zeta_{2^{\tau+1}} + \zeta_{2^{\tau+1}}^{-1}\big) = \pm\big(\zeta_{2^{\tau+1}} + \zeta_{2^{\tau+1}}^{-1}\big).$$

Hence $S\xi^2 = \xi^2$ implies $S\zeta_{2^\nu}^j = \zeta_{2^\nu}^j$, $S\zeta_{2^\nu} = \zeta_{2^\nu}$ or

$$S\zeta_{2^\nu}^j = -\zeta_{2^\nu}^j, \quad S\big(\zeta_{2^{\tau+1}} + \zeta_{2^{\tau+1}}^{-1}\big) = -\big(\zeta_{2^{\tau+1}} + \zeta_{2^{\tau+1}}^{-1}\big).$$

The latter case is however impossible, since $S\zeta_{2^{\tau+1}} = S(\zeta_{2^\nu})^{2^{\nu-\tau-1}}$. It follows that

$$\zeta_{2^\nu} \in K(\xi^2).$$

If the binomial $x^{p^\nu} - \alpha$ is irreducible, then for $p = 2$, $\nu \geqslant 2$ we have $\alpha \neq -4\gamma^4$, hence for $\tau \geqslant 3$, $\alpha \neq -\gamma^4$, $\gamma \in K$. Thus (iv) implies $\tau \geqslant 3$, $\sqrt{-\left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)} \notin K$, $\lambda = 1$; (v) implies $\tau = 2$. □

c *Remark.* Note that in case (i) if $\kappa = \omega > 0$ and in cases (ii)–(v) every root of $x^{p^\nu} - \alpha$ generates all the others.

Lemma 5. *If a binomial $x^{p^\nu} - \alpha$ satisfies condition* (i) *then its Galois group G over K is abelian. If it is irreducible then G is cyclic unless $p = 2$, $\nu \geqslant 2$, $\omega = 1$, in which case G is of type* $(2, 2^{\nu-1})$.

If λ is the least nonnegative integer such that

$$\alpha = \zeta_{p^\kappa}\gamma^{p^{\nu-\lambda}}, \quad 0 \leqslant \kappa \leqslant \lambda \leqslant \omega, \quad \gamma \in K,$$

then the Galois group of each irreducible factor of $x^{p^\nu} - \alpha$ contains an element of order p^λ and besides an element of order

$$p^{\nu-\omega+\kappa} \quad \text{if} \quad \langle p, \omega\rangle \neq \langle 2, 1\rangle \ \text{and}\ \kappa > \max\{0, \omega - \nu + \lambda\},$$
$$p^{\nu-\tau+1} \quad \text{if} \quad \langle p, \omega\rangle = \langle 2, 1\rangle \ \text{and}\ \kappa = \lambda = 1 > \tau - \nu + 1.$$

Proof. We start by proving that an irreducible binomial satisfying (i) has a cyclic group G unless $p = 2, \nu \geqslant 2, \omega = 1$. Since it is irreducible we have either $\nu - \lambda = 0$ or $\kappa = \omega = \lambda$. In the former case $\nu \leqslant \omega$; if ξ is any zero of $x^{p^\nu} - \alpha$ and S the substitution $\xi \to \zeta_{p^\nu}\xi$ we have $S^j(\xi) = \zeta_{p^\nu}^j\xi$ hence G is cyclic, generated by S. In the latter case let ξ be any zero of $x^{p^\nu} - \alpha$ satisfying

$$\xi^{p^\omega} = \zeta_{p^\nu}\gamma$$

and consider the substitution $S : \xi \to \zeta_{p^\nu}\xi$. We have

$$S(\zeta_{p^\nu}) = \zeta_{p^\nu}^{p^\omega+1}, \quad S^j(\xi) = \zeta_{p^\nu}^{\sum_{i=0}^{j-1}(p^\omega+1)^i}\xi.$$

The order of S is the least j such that

$$\sum_{i=0}^{j-1}(p^\omega + 1)^i = \frac{(p^\omega + 1)^j - 1}{p^\omega} \equiv 0 \bmod p^\nu. \tag{16}$$

However if $p > 2$, $a \equiv 1 \bmod p$ or $p = 2$, $a \equiv 1 \bmod 4$ we have

$$\operatorname{ord}_p(a^j - 1) = \operatorname{ord}_p j + \operatorname{ord}_p(a - 1) \tag{17}$$

(see [6], p. 401 ([1]), formula (8)). Hence if $p > 2$ or $p = 2$, $\omega \geqslant 2$, (16) implies

$$\operatorname{ord}_p j \geqslant \nu$$

([1]) Page 919 in this volume.

and S is of order p^ν. The same is clearly true for $p^\nu = 2$.

The remaining assertions of the lemma are trivial for $\lambda = 0$. If $\lambda > 0$ we consider first the case $p > 2$ or $p = 2, \omega \geqslant 2$. If $\kappa > \max\{0, \omega - \nu + \lambda\}$ we have the factorization

$$x^{p^\nu} - \alpha = \prod_{j=0}^{p^{\omega-\kappa}-1} \left(x^{p^{\nu-\omega+\kappa}} - \zeta_{p^{\omega-\kappa}}^{j} \zeta_{p^\omega} \gamma^{p^{\nu-\lambda-\omega+\kappa}}\right)$$

and the factors are irreducible since $\zeta_{p^{\omega+1}} \notin K$. By the fact already established the Galois groups are cyclic of order $p^{\nu-\omega+\kappa}$ and since $\nu - \omega + \kappa > \lambda$ contain also an element of order p^λ.

If $\kappa \leqslant \omega - \nu + \lambda$ then

$$\alpha = \gamma_1^{p^{\nu-\lambda}}, \quad \gamma_1 = \zeta_{p^{\kappa+\nu-\lambda}} \gamma \in K.$$

We have the factorization

$$x^{p^\nu} - \alpha = \prod_{j=0}^{p^{\nu-\lambda}-1} \left(x^{p^\lambda} - \zeta_{p^{\nu-\lambda}}^{j} \gamma_1\right)$$

and the factors are irreducible, since $\zeta_{p^{\nu-\lambda}}^{j} \gamma_1 = \gamma_2^p$, $\gamma_2 \in K$ would imply

$$\alpha^{p^{\lambda-1}} = \gamma_2^{p^\nu}$$

contrary to the choice of λ. The Galois groups are cyclic of order p^λ.

If $\kappa = 0 > \omega - \nu + \lambda$ we have the factorization

$$x^{p^\nu} - \alpha = \prod_{j=0}^{p^\omega-1} \left(x^{p^\lambda} - \zeta_{p^\omega}^{j} \gamma\right) \prod_{\mu=\lambda+1}^{\nu-\omega} \prod_{\substack{j=0 \\ (j,p)=1}}^{p^\omega-1} \left(x^{p^\mu} - \zeta_{p^\omega}^{j} \gamma^{p^{\mu-\lambda}}\right).$$

The factors of the first product are irreducible for the same reason as before, the other factors are irreducible since $\zeta_{p^{\omega+1}} \notin K$. The Galois groups are cyclic of order p^μ $(\lambda \leqslant \mu \leqslant \nu - \omega)$.

Consider now the case $p = 2, \omega = \lambda = 1$. Let τ_1 have the meaning of Lemma 3.

If $\kappa = 1 > \tau - \nu + 1$ we have $\nu \geqslant \tau + 1 \geqslant \tau_1$ and the factorization

$$x^{2^\nu} - \alpha = \prod_{\substack{j=1 \\ j \equiv 1 \bmod 4}}^{2^{\tau_1}-1} N_{K(\zeta_4)/K}\left(x^{2^{\nu-\tau_1+1}} - \zeta_{2^{\tau_1}}^{j} \gamma^{2^{\nu-\tau_1}}\right).$$

If $f_j(x) = x^{2^{\nu-\tau_1+1}} - \zeta_{2^{\tau_1}}^{j} \gamma^{2^{\nu-\tau_1}}$ were reducible over $K(\zeta_4)$, then since $\zeta_{2^{\tau_1+1}} \notin K(\zeta_4)$ we should have $\nu = \tau_1 = \tau + 1$ and

$$\zeta_{2^{\tau_1}}^{j} \gamma = \vartheta^2, \quad \vartheta \in K(\zeta_4),$$

whence $-\gamma^{2^\tau} = \vartheta^{2^{\tau+1}}$ contrary to Lemma 2. Thus $f_j(x)$ is irreducible over $K(\zeta_4)$ and $N_{K(\zeta_4)/K} f_j(x) = f_j(x) f_j'(x)$ is irreducible over K.

In order to determine the Galois group of $f_j f_j'$ it is necessary to distinguish between the cases $\tau_1 = \tau + 1$ and $\tau_1 = \tau$.

Let ξ be a zero of $f_j(x)$ satisfying

c (18) $$\xi^2 = \zeta_{2^\nu}^j \gamma.$$

If $\tau_1 = \tau + 1$ then $-\zeta_{2^{\tau_1}}^{-j}$ is conjugate over K to $\zeta_{2^{\tau_1}}^j$ hence $\zeta_{2^\nu}^{-j(1+2^{\tau-1})}\xi$ is a zero of $f_j'(x)$. Let S be the substitution

$$\xi \to \zeta_{2^\nu}^{-j(1+2^{\tau-1})}\xi.$$

We have by (18)

$$S(\zeta_{2^\nu}^j) = \zeta_{2^\nu}^{-j(1+2^\tau)}$$

hence

$$S^r(\xi) = \zeta_{2^\nu}^{-j(1+2^{\tau-1})\sum_{i=0}^{r-1}(-1-2^\tau)^i}\xi.$$

The order of S is the least r such that

$$-j(1+2^{\tau-1})\sum_{i=0}^{r-1}(-1-2^\tau)^i = j\,\frac{(-1-2^\tau)^r - 1}{2} \equiv 0 \bmod 2^\nu.$$

Clearly r must be even and since by (17)

c $$\operatorname{ord}_2\big((1+2^\tau)^r - 1\big) = \operatorname{ord}_2 r + \tau$$

we get $r \equiv 0 \bmod 2^{\nu-\tau+1}$. The order of S is thus equal to the degree of $f_j f_j'$ and since the latter polynomial is normal, its group is cyclic of order $2^{\nu-\tau+1}$.

If $\tau_1 = \tau$ then $\zeta_{2^{\tau_1}}^{-j}$ is conjugate over K to $\zeta_{2^{\tau_1}}^j$ hence $\zeta_{2^\nu}^{-j}\xi$ is a zero of $f_j'(x)$. Let S be the substitution $\xi \to \zeta_{2^\nu}^{-j}\xi$ and T the substitution $\xi \to \zeta_{2^{\nu-\tau+1}}^j\xi$. We have by (18)

$$S(\zeta_{2^\nu}^j) = \zeta_{2^\nu}^{-j}, \quad S^2(\xi) = \xi;$$
$$T(\zeta_{2^\nu}^j) = \zeta_{2^\nu}^{j(1+2^\tau)}, \quad T^r(\xi) = \zeta_{2^{\nu-\tau+1}}^{j\sum_{i=0}^{r-1}(1+2^\tau)^i}\xi.$$

Using (17) we infer that T is of order $2^{\nu-\tau+1}$, moreover $-j \not\equiv 0 \bmod 2^{\tau-1}$, hence $S \neq T^r$. However

$$ST(\xi) = S(\zeta_{2^{\nu-\tau+1}}^j)S(\xi) = \zeta_{2^{\nu-\tau+1}}^{-j}\zeta_{2^\nu}^{-j}\xi = \zeta_{2^\nu}^{-j(1+2^{\tau-1})}\xi,$$
$$TS(\xi) = T(\zeta_{2^\nu}^{-j})T(\xi) = \zeta_{2^\nu}^{-j(1+2^\tau)}\zeta_{2^{\nu-\tau+1}}^j\xi = \zeta_{2^\nu}^{-j(1+2^{\tau-1})}\xi,$$

thus $ST(\xi) = TS(\xi)$ and the group of $f_j f_j'$ being of order $2^{\nu-\tau+2}$ must be abelian of type $(2, 2^{\nu-\tau+1})$.

In particular, if $x^{2^\nu} - \alpha$ is irreducible, we have $\tau_1 = \tau = 2$ and the group is abelian of type $(2, 2^{\nu-1})$.

Consider now the case $\kappa = 1 \leqslant \tau - \nu + 1$. We have the factorization

$$x^{2^\nu} - \alpha = \prod_{\substack{j=1 \\ j \equiv 1 \bmod 4}}^{2^\nu - 1} N_{K(\zeta_4)/K}(x^2 - \zeta_{2^\nu}^j \gamma).$$

The factors that are not irreducible are products of two quadratic factors and hence satisfy the condition of the lemma. The irreducible factors have groups abelian of type $(2, 2)$ generated by the substitutions $(\xi \to -\xi)$ and $(\xi \to \zeta_{2^\nu}^{-j}\xi)$, where ξ is a zero of $x^2 - \zeta_{2^\nu}^j \gamma$.

In particular this applies to the case of an irreducible binomial $x^4 + \gamma^2$.

It remains to consider the case $\kappa = 0$. Then the assertions of the lemma follow by induction with respect to ν. They are true for $\nu = 1$. For $\nu > 1$ we have the factorization

$$x^{2^\nu} - \gamma^{2^{\nu-1}} = \left(x^{2^{\nu-1}} - \gamma^{2^{\nu-2}}\right)\left(x^{2^{\nu-1}} + \gamma^{2^{\nu-2}}\right).$$

The first factor on the right hand side has an abelian Galois group and all its irreducible factors are of even degree by the inductive assumption, the second factor has this property by the already considered case $\kappa = 1$ of the lemma. □

Proof of Theorem 2. *Necessity.* Assume that the splitting field of $x^n - \alpha$ is abelian over K. Then also the splitting field of $x^{p^\nu} - \alpha$ is abelian over K for any $p^\nu \mid n$ and since every subgroup of an abelian group is normal $x^{p^\nu} - \alpha$ is the product of normal factors. Thus we have one of the conditions (i)–(v) listed in Theorem 1. We shall show that under our assumption (ii)–(v) lead to (i). Consider first (ii), (iii) or (iv).

Let μ be the least nonnegative integer such that

$$\alpha = -\gamma_1^{2^{\nu-\mu}}, \quad \gamma_1 \in K.$$

Clearly $\mu < \nu$. If $\mu \leqslant 1$ we have (i). If $\mu > 1$ then $\nu - \mu + 2 \leqslant \tau$, unless $\nu = \tau + 1$, $\mu = 2$, in which case by (iii) or (iv) and, by Lemma 3, $\nu - \mu + 2 \leqslant \tau_1$. Thus

$$\zeta_{2^{\nu-\mu+2}} \in K(\zeta_4). \tag{19}$$

$x^{2^\nu} - \alpha$ has over $K(\zeta_4)$ the factor

$$f(x) = x^{2^\mu} - \zeta_{2^{\nu-\mu+1}}\gamma_1.$$

Now

$$\zeta_{2^{\nu-\mu+1}}\gamma_1 \neq \vartheta^2, \quad \vartheta \in K(\zeta_4),$$

since otherwise, by (19) $\gamma_1 = \vartheta_1^2$, $\gamma_1 \in K(\zeta_4)$ and by Lemma 2

$$\gamma_1 = \pm\gamma_2^2, \quad \gamma_2 \in K; \quad \alpha = -\gamma_2^{2^{\nu-\mu+1}}$$

contrary to the choice of μ. Thus $f(x)$ is irreducible over $K(\zeta_4)$ and $N_{K(\zeta_4)/K} f(x) = f(x) f'(x)$ is irreducible over K. By the assumption the latter polynomial is normal over K. Let ξ be any zero of $f(x)$,

$$\xi_1 = \zeta_{2^\nu}^{-1}\xi, \quad \xi_2 = \zeta_{2^\nu}^{-1-2^{\nu-\mu}}\xi.$$

ξ_1, ξ_2 are zeros of $f'(x)$. Let S_i be the automorphism of the Galois group of ff' over K such that

$$S_i\xi = \xi_i \quad (i = 1, 2).$$

We have $S_i\zeta_{2^{\nu-\mu+1}} = \zeta_{2^{\nu-\mu+1}}^{-1}$ hence $S_i\zeta_{2^\nu} = \varepsilon_i\zeta_{2^\nu}^{-1}$ ($\varepsilon_i = \pm 1$). It follows that

$$S_1S_2\xi = S_1\xi_2 = S_1(\zeta_{2^\nu}^{-1-2^{\nu-\mu}})S_1\xi = \varepsilon_1\zeta_{2^\mu}\xi,$$
$$S_2S_1\xi = S_2\xi_1 = S_2(\zeta_{2^\nu}^{-1})S_2\xi = \varepsilon_2\zeta_{2^\mu}^{-1}\xi.$$

c By Lemma 3 we have $\varepsilon_1 = \varepsilon_2$ unless $\nu = \tau + 1$ and $\sqrt{-\left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)} \notin K$. In the
c latter case by (iv) $\mu = \nu - \lambda \geqslant 3$, thus in both cases $S_1S_2\xi \neq S_2S_1\xi$ and the group in question is not abelian.

Consider now the case (v). If $\sqrt{-\left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)} \in K$ then we get (i). If $\sqrt{-\left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)} \notin K$ then by Lemma 3

$$\zeta_{2^{\tau+1}} \notin K(\zeta_4). \tag{20}$$

c $x^{2^\nu} - \alpha$ has over $K(\zeta_4)$ the factor

$$f(x) = x^{2^{\nu-\tau+1}} - \zeta_{2^\tau}\left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{2^{\nu-\tau-1}}\gamma^{2^{\nu-\tau}}.$$

c By (20) and the inequality $\nu \geqslant \tau + 2$, $f(x)$ is irreducible over $K(\zeta_4)$. Hence
c $N_{K(\zeta_4)/K} f(x) = f(x)f'(x)$ is irreducible over K and by the assumption normal.

Let ξ be a zero of $f(x)$ satisfying

$$\xi^2 = \zeta_{2^\nu}\left(\zeta_{2^{\tau+1}} + \zeta_{2^{\tau+1}}^{-1}\right)\gamma \tag{21}$$

and let

$$\xi_1 = \zeta_{2^\nu}^{-1}\xi, \quad \xi_2 = \zeta_{2^\nu}^{-1-2^{\tau-1}}\xi.$$

ξ_1 and ξ_2 are zeros of $f'(x)$. Let S_i ($i = 1, 2$) be the automorphism of the Galois group of ff' over K such that

$$S_i\xi = \xi_i \quad (i = 1, 2).$$

We have for a suitable $\varepsilon_i = \pm 1$

$$S_i\left(\zeta_{2^{\tau+1}} + \zeta_{2^{\tau+1}}^{-1}\right) = \varepsilon_1\left(\zeta_{2^{\tau+1}} + \zeta_{2^{\tau+1}}^{-1}\right);$$

then by (21)

$$S_1\zeta_{2^\nu} = \varepsilon_1\zeta_{2^\nu}^{-1}, \quad S_2\zeta_{2^\nu} = \varepsilon_2\zeta_{2^\nu}^{-1-2^\tau} \tag{22}$$

hence

$$S_1\left(\zeta_{2^{\tau+1}} + \zeta_{2^{\tau+1}}^{-1}\right) = \left(\varepsilon_1\zeta_{2^\nu}^{-1}\right)^{2^{\nu-\tau-1}} + \left(\varepsilon_1\zeta_{2^\nu}\right)^{2^{\nu-\tau-1}} = \zeta_{2^{\tau+1}} + \zeta_{2^{\tau+1}}^{-1},$$
$$S_2\left(\zeta_{2^{\tau+1}} + \zeta_{2^{\tau+1}}^{-1}\right) = \left(\varepsilon_2\zeta_{2^\nu}^{-1-2^\tau}\right)^{2^{\nu-\tau-1}} + \left(\varepsilon_2\zeta_{2^\nu}^{1+2^\tau}\right)^{2^{\nu-\tau-1}} = -\zeta_{2^{\tau+1}} - \zeta_{2^{\tau+1}}^{-1}.$$

Thus $\varepsilon_1 = 1$, $\varepsilon_2 = -1$ and (22) implies

$$S_1 S_2 \xi = S_1 \xi_2 = S_1\big(\zeta_{2^\nu}^{-1-2^{\tau-1}}\big) S_1 \xi = \zeta_{2^{\nu-\tau+1}} \xi,$$
$$S_2 S_1 \xi = S_2 \xi_1 = S_2\big(\zeta_{2^\nu}^{-1}\big) S_2 \xi = -\zeta_{2^{\nu-\tau+1}} \xi.$$

Hence $S_1 S_2 \xi \neq S_2 S_1 \xi$ and the group in question is not abelian. Therefore, if $n = \prod_{i=1}^{k} p_i^{\nu_i}$ is the canonical factorization of n we get for each $i \leqslant k$

$$\alpha^{w^i} = \gamma_i^{p_i^{\nu_i}}, \quad \gamma_i \in K,$$

where we have put for abbreviation $w^i = w_{p_i^{\nu_i}}$. It follows that

$$\alpha^{n w_n / p_i^{\nu_i}} = \gamma_i^{n w_n / w^i}.$$

If now

$$\frac{1}{n} = \sum_{i=1}^{k} \frac{r_i}{p_i^{\nu_i}} \tag{23}$$

we obtain

$$\alpha^{w_n} = \left(\prod_{i=1}^{k} \gamma_i^{r_i w_n / w^i} \right)^n$$

and the proof is complete.

Sufficiency. Assume that

$$\alpha^{w_n} = \gamma^n, \quad \gamma \in K,$$

and let again $n = \prod_{i=1}^{k} p_i^{\nu_i}$, $w^i = w_{p_i^{\nu_i}}$.

Since $\left(\frac{w_n}{w^i}, p_i^{\nu_i} \right) = 1$ we have

$$\alpha^{w^i} = \gamma_i^{p_i^{\nu_i}}. \tag{24}$$

Thus α satisfies the assumptions of Lemma 5 for all p_i and by that lemma the Galois groups over K of all binomials

$$x^{p_i^{\nu_i}} - \alpha \quad (1 \leqslant i \leqslant k) \tag{25}$$

are abelian. If ξ is any zero of $x^n - \alpha$ then $\xi^{n/p_i^{\nu_i}}$ is a zero of (25) and defining r_i by (23) we get

$$\xi = \prod_{i=1}^{k} \big(\xi^{n/p_i^{\nu_i}}\big)^{r_i}.$$

Hence the splitting field of $x^n - \alpha$ as the composite of the splitting fields of (25) is abelian.

Moreover if $x^n - \alpha$ is irreducible then also the binomials (25) are irreducible and their groups are cyclic of order $p_i^{\nu_i}$ unless $p_i^{\nu_i} \equiv 0 \bmod 4$ and $\zeta_4 \notin K$ in which case the group

of (25) has a cyclic factor of order 2^{ν_i-1}. Since the direct product of cyclic groups of orders prime in pairs is again cyclic we get all assertions of the theorem. □

Lemma 6 (Hasse). *If $\alpha = \eta^{p^\nu}$, $\eta \in K(\zeta_{p^\nu})$, then at least one of the following conditions is satisfied for a suitable $\gamma \in K$:*

$$\alpha = \gamma^{p^\nu}; \tag{26}$$

$$p = 2,\ \omega = 1,\ 1 < \nu < \tau,\ \alpha = -\gamma^{2^\nu};$$

$$p = 2,\ \omega = 1,\ \nu = \tau,\ \alpha = -\left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{2^{\tau-1}} \gamma^{2^\tau};$$

$$p = 2,\ \omega = 1,\ \nu > \tau,\ \alpha = \left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{2^{\nu-1}} \gamma^{2^\nu},$$

where ω and τ have the meaning of Theorem 1, $p \neq \operatorname{char} K$.

Proof which we give is based on the previous results and therefore much shorter than the original Hasse's proof ([2], for char $K = 0$).

Since all the subextensions of $K(\zeta_{p^\nu})$ are normal over K the binomial $x^{p^\nu} - \alpha$ satisfies the conditions of Theorem 1. Hence we have either (26) or $\omega \geqslant 1$. In the latter case Lemma 1 applies with $\xi = \zeta_{p^\nu}$, and we get either

$$\eta \in K^* \langle \zeta_{p^\nu} \rangle; \quad \eta = \gamma \zeta_{p^\nu}^j, \quad \gamma \in K^* \tag{27}$$

or $p = 2$, $\zeta_4 \notin K$. (27) gives at once (26). To settle the case $p = 2$ we apply the already proved case of our lemma for the field $K(\zeta_4)$ and get

$$\alpha = \vartheta^{2^\nu}, \quad \vartheta \in K(\zeta_4).$$

Now Lemma 6 follows immediately from Lemma 2. □

Proof of Theorem 3. We start by estimating for each $p^\nu \parallel n$ the greatest exponent μ_p such that p^{μ_p} divides the order of an element in $\operatorname{Gal}\left(K(\zeta_{np^{-\nu}})/K\right)$. Since $K(\zeta_{np^{-\nu}})$ is the composite of $K(\zeta_{q^s})$, where $q \neq p$ is a prime and $q^s \parallel n$, we have

$$\mu_p \leqslant \max_{\substack{q^s \parallel n \\ q \neq p}} \operatorname{ord}_p [K(\zeta_{q^s}) : K]. \tag{\#}$$

Let r be the largest integer such that $\zeta_{q^r} \in K(\zeta_q)$. Then for $q^s > 2$

$$[K(\zeta_{q^s}) : K] = \begin{cases} q^{\max(0, s-r)} [K(\zeta_q) : K] & \text{if } (q, r) \neq (2, 1), \\ 2^{\max(0, s-\tau_1)} [K(\zeta_4) : K] & \text{if } (q, r) = (2, 1). \end{cases}$$

This gives

$$\mu_p \leqslant \max_{\substack{q \mid n \\ q \text{ prime}}} \operatorname{ord}_p [K(\zeta_q) : K]. \tag{28}$$

(Actually we have here the equality [2].)

[2] See *Addendum*, p. 967.

Assume now that

$$\alpha = \vartheta^n, \quad \vartheta \in K(\zeta_n). \tag{29}$$

Then for each $p^\nu \parallel n$, the binomial $x^{p^\nu} - \alpha$ is abelian over K and by Theorem 2

$$\alpha = \zeta_{p^\kappa} \gamma_p^{p^{\nu-\lambda}}; \quad \kappa \leqslant \lambda \leqslant \min(\nu, \omega), \quad \gamma_p \in K. \tag{30}$$

where ω has the meaning of Theorem 1.

Suppose first $p^\nu \not\equiv 0 \bmod 4$ or $\zeta_4 \in K$. Then by Lemma 6 it follows from (29) that

$$\alpha = \vartheta_1^{p^\nu}, \quad \vartheta_1 \in K(\zeta_{np^{-\nu}}). \tag{31}$$

By Lemma 5 $\mathrm{Gal}\big(K(\vartheta_1)/K\big)$ contains an element of order p^λ hence $\mathrm{Gal}\big(K(\zeta_{np^{-\nu}})/K\big)$ contains such an element and by (28) we have

$$\lambda \leqslant \mu_p \leqslant \max_{\substack{q \mid n \\ q \text{ prime}}} \operatorname{ord}_p [K(\zeta_q) : K].$$

By (30) we have also

$$\lambda \leqslant \operatorname{ord}_p w_n \tag{32}$$

hence $\lambda \leqslant \operatorname{ord}_p \sigma$.

The same inequality follows directly from (32) if $p^\nu \equiv 0 \bmod 4$, $\zeta_4 \notin K$. Thus, by (30), for each p we have

$$\alpha^\sigma = \delta_p^{p^\nu}, \quad \delta_p \in K,$$

whence by the standard argument (see the proof of Theorem 2)

$$\alpha^\sigma = \gamma^n, \quad \gamma \in K.$$

Assume now in addition to (29) that for a certain m prime to n

$$\begin{cases} \text{either } \zeta_{(4,n)} \in K \text{ and } nm \equiv 0 \bmod w_n \operatorname{l.c.m.}_{\substack{q \mid n \\ q \text{ prime}}} [K(\zeta_q) : K] \\ \text{or } \zeta_{(4,n)} \notin K \text{ and } nm \equiv 0 \bmod 2^\tau w_n \operatorname{l.c.m.}_{\substack{q \mid n \\ q \text{ prime}}} [K(\zeta_q) : K] \end{cases} \tag{33}$$

and consider again (30) for any $p^\nu \parallel n$.

If $\nu \leqslant \omega$ then from (30) we get immediately

$$\alpha = \delta_p^{p^{\nu-\lambda}}, \quad \delta_p \in K. \tag{34}$$

If $\nu > \omega$ and either $p > 2$ or $\zeta_4 \in K$ we get from (28) and (33),

$$\nu \geqslant \omega + \mu_p, \tag{35}$$

hence in particular

$$\omega - \nu + \lambda \leqslant -\mu_p + \operatorname{ord}_p \sigma \leqslant 0. \tag{\#\#}$$

Thus if (30) holds with $\kappa > 0$ we get by Lemma 5 and (31)

$$\nu - \omega + 1 \leqslant \mu_p,$$

which contradicts (35). If $\nu > \omega = 1$ and $p = 2$ we get from (33)

$$\nu \geqslant \tau + 1 + \mu_2 > \tau. \tag{36}$$

Let τ_2 be the greatest integer such that

$$\zeta_{2^{\tau_2}} + \zeta_{2^{\tau_2}}^{-1} \in K\big(\zeta_{n2^{-\nu}}\big).$$

Since $K\big(\zeta_{2^{\tau_2}} + \zeta_{2^{\tau_2}}^{-1}\big)$ is over K cyclic of degree $2^{\tau_2 - \tau}$ we have

$$\tau_2 - \tau \leqslant \mu_2$$

and by (36)

$$\nu \geqslant \tau_2 + 1.$$

Hence by (29) and Lemma 6

$$\alpha = \vartheta_1^{2^{\nu-1}}, \quad \vartheta_1 \in K\big(\zeta_{n2^{-\nu}}\big).$$

Thus if (30) holds with $\kappa > 0$ we get by Lemma 5 that $\mathrm{Gal}(K(\vartheta_1)/K)$ contains an element of order $2^{\nu-\tau}$, hence

$$\nu - \tau \leqslant \mu_2$$

contrary to (36). Therefore (34) holds in any case and by the standard argument

$$\alpha = \gamma^{n/\sigma}, \quad \gamma \in K. \qquad \square$$

Remark ([3]). If $(w_n, n/w_n) = 1$ the number σ occurring in Theorem 3 is the least integer with the required property. Indeed, by the definition of σ there exists a character $\chi \bmod n$ belonging to exponent σ on the group $G = \mathrm{Gal}\big(K(\zeta_n)/K\big)$.

Let $\tau(\chi, \zeta_n)$ be the corresponding Gauss sum. Clearly $\tau(\chi) \in K(\zeta_n)$. Suppose that $\tau(\chi)^{n\varrho} = \gamma^n$, $\gamma \in K$, $0 < \varrho < \sigma$. Then $\tau(\chi)^\varrho = \zeta_n^\alpha \gamma$ and applying an automorphism

$$\zeta_n \to \zeta_n^j \tag{$*$}$$

from G we get $\overline{\chi}(j)^\varrho = \zeta_n^{a(j-1)}$. It follows that

$$\zeta_n^{a(j^2-1)} = \overline{\chi}(j^2)^\varrho = \overline{\chi}(j)^{2\varrho} = \zeta_n^{2a(j-1)}; \quad \zeta_n^{a(j-1)^2} = 1,$$

$a(j-1)^2 \equiv 0 \bmod n$ and since this holds for all automorphisms $(*)$ from G, $aw_n^2 \equiv 0 \bmod n$. Since $(w_n, n/w_n) = 1$ we get

$$a \equiv 0 \bmod \frac{n}{w_n}, \quad a(j-1) \equiv 0 \bmod n \quad \text{and} \quad \overline{\chi}(j)^\varrho = 1$$

contrary to the choice of χ.

([3]) See *Addendum*, p. 967.

Lemma 7. *Under the assumption* (viii) *of Theorem* 4 *the group*

$$G_0 = \mathrm{Gal}\big(K(\zeta_n, \sqrt[n]{\alpha_1}, \ldots, \sqrt[n]{\alpha_k})/K(\zeta_n)\big)$$

contains the substitution

$$\sqrt[n]{\alpha_i} \to \zeta_n^{c_i} \sqrt[n]{\alpha_i} \quad (1 \leqslant i \leqslant k),$$

under the assumptions (vii) *and* (ix) *the group*

$$G_1 = \mathrm{Gal}\big(K(\zeta_n, \sqrt[n]{\zeta_w}, \sqrt[n]{\alpha_1}, \ldots, \sqrt[n]{\alpha_k})/K(\zeta_n)\big)$$

contains the substitution

$$\sqrt[n]{\zeta_w} \to \zeta_{(w,n)}^{c_0} \sqrt[n]{\zeta_w}, \quad \sqrt[n]{\alpha_i} \to \zeta_n^{c_i} \sqrt[n]{\alpha_i} \quad (1 \leqslant i \leqslant k)$$

for any c_0 *and any* $c_i \equiv 0 \bmod \sigma$ $(1 \leqslant i \leqslant k)$.

Proof. Let us denote any value of $\sqrt[n]{\alpha_i}$ by ξ_i $(1 \leqslant i \leqslant k)$ and of $\sqrt[n]{\zeta_w}$ by ξ_0. To prove the first part of the lemma it is clearly sufficient to prove that G_0 contains each of the substitutions $(1 \leqslant i \leqslant k)$

$$\xi_j \to \xi_j \ (1 \leqslant j \leqslant k,\ j \neq i), \quad \xi_i \to \zeta_n^{\sigma} \xi_i. \tag{37}$$

If (37) were not contained in G_0, we should have

$$d_i = \mathrm{Gal}\big(K(\zeta_n, \xi_1, \ldots, \xi_k)/K(\zeta_n, \xi_1, \ldots, \xi_{i-1}, \xi_{i+1}, \ldots, \xi_k) \not\equiv 0 \bmod \frac{n}{\sigma}. \tag{38}$$

Now by Kneser's theorem

$$d_i = \big[K(\zeta_n)^*\langle \xi_1, \ldots, \xi_k\rangle : K(\zeta_n)^*\langle \xi_1, \ldots, \xi_{i-1}, \xi_{i+1}, \ldots, \xi_k\rangle\big]$$

hence d_i is the least exponent such that

$$\xi_i^{d_i} = \vartheta \xi_1^{x_1} \cdots \xi_{i-1}^{x_{i-1}} \xi_{i+1}^{x_{i+1}} \cdots \xi_k^{x_k}, \quad \vartheta \in K(\zeta_n). \tag{39}$$

By raising (39) to nth power we get that

$$\alpha_i^{d_i} = \vartheta^n \alpha_1^{x_1} \cdots \alpha_{i-1}^{x_{i-1}} \alpha_{i+1}^{x_{i+1}} \cdots \alpha_k^{x_k},$$

$\vartheta^n \in K$ and, by Theorem 3, $\vartheta^{n\sigma} = \gamma^n$; $\gamma \in K$,

$$\alpha_1^{-\sigma x_1} \cdots \alpha_i^{d_i \sigma} \cdots \alpha_k^{-\sigma x_k} = \gamma^n.$$

By the assumption $d_i \sigma \equiv 0 \bmod n$, contrary to (38).

To prove the second part of the lemma we have similarly to prove that G_1 contains each of the substitutions $(1 \leqslant i \leqslant k)$

$$\xi_0 \to \zeta_{(n,w)} \xi_0, \quad \xi_j \to \xi_j \quad (1 \leqslant j \leqslant k);$$
$$\xi_0 \to \xi_0, \quad \xi_j \to \xi_j \quad (1 \leqslant j \leqslant k,\ j \neq i), \quad \xi_i \to \zeta_n^{\sigma} \xi_i.$$

This reduces to proving that the least exponents e_i $(0 \leqslant i \leqslant k)$ such that

$$\xi_i^{e_i} \in K(\zeta_n)\langle \xi_0, \ldots, \xi_{i-1}, \xi_{i+1}, \ldots, \xi_k\rangle \tag{40}$$

satisfy $e_0 \equiv 0 \bmod (n, w)$, $e_i \equiv 0 \bmod n/\sigma$. Now (40) implies for $i = 0$

$$\zeta_w^{e_0} = \vartheta^n \alpha_1^{x_1} \cdots \alpha_k^{x_k}, \quad \vartheta \in K(\zeta_n);$$

c hence by (vii) and (ix)

$$\zeta_w^{e_0} \alpha_1^{-x_1} \cdots \alpha_k^{-x_k} = \gamma^{n/\sigma}, \quad \gamma \in K; \quad x_i \equiv 0 \bmod n/\sigma;$$
$$\zeta_w^{e_0} = \gamma^{n/\sigma} \alpha_1^{y_1 n/\sigma} \cdots \alpha_k^{y_k n/\sigma} = \gamma_1^{n/\sigma}.$$

γ_1 must be a root of unity contained in K; $\gamma_1 = \zeta_w^j$ and so we get $e_0 \equiv 0 \bmod (w, n/\sigma)$.
c However by the condition (vii) $n/\sigma \equiv 0 \bmod (w, n)$ and thus $e_0 \equiv 0 \bmod (w, n)$.

For $i > 0$, (40) implies

$$\alpha_i^{e_i} = \vartheta^n \zeta_w^{x_0} \alpha_1^{x_1} \cdots \alpha_{i-1}^{x_{i-1}} \alpha_{i+1}^{x_{i+1}} \cdots \alpha_k^{x_k}, \quad \vartheta \in K(\zeta_n);$$
$$\zeta_w^{-x_0} \alpha_1^{-x_1} \cdots \alpha_i^{e_i} \cdots \alpha_k^{-x_k} = \gamma^{n/\sigma}, \quad \gamma \in K; \quad e_i \equiv 0 \bmod n/\sigma. \qquad \square$$

Proof of Theorem 4. We use Chebotarev's density theorem and get the existence of infinitely many prime ideals $\mathfrak{P}$ of $L_0 = K(\zeta_n, \xi_1, \ldots, \xi_k)$ or $L_1 = K(\zeta_n, \xi_0, \ldots, \xi_k)$ dividing $\mathfrak{p}$ in $K(\zeta_n)$ such that for all $\eta \in L_0$ or L_1 respectively

$$\eta^{N\mathfrak{p}} \equiv S\eta \bmod \mathfrak{P},$$

where S is the automorphism described in Lemma 7, $\xi_0^n = \zeta_w$, $\xi_i^n = \alpha_i$. Setting $\eta = \xi_i$ we get

$$\xi_i^{N\mathfrak{p}} \equiv \xi_i \zeta_n^{c_i} \bmod \mathfrak{P} \quad (i > 0),$$
$$\xi_0^{N\mathfrak{p}} \equiv \xi_0 \zeta_{(w,n)}^{c_0} \bmod \mathfrak{P},$$

consequently

$$\alpha_i^{(N\mathfrak{p}-1)/n} \equiv \zeta_n^{c_i} \bmod \mathfrak{P},$$
$$\zeta_w^{(N\mathfrak{p}-1)/n} \equiv \zeta_{(w,n)}^{c_0} \bmod \mathfrak{P}$$

and the same $\bmod \mathfrak{p}$. One has only to remark that $N\mathfrak{p} \equiv 1 \bmod n$. $\square$

Remark. If $(w_n, n/w_n) = 1$ the number σ occurring in the first part of Theorem 4 is the least integer with the required property. This follows from the Remark after Theorem 3 on taking $k = 1$, $\alpha = \tau(\chi)^\sigma$. If $(w_n, n/w_n) > 1$ σ need not be best possible. In particular, if $\zeta_4 \notin K$, $n \not\equiv 0 \bmod 2^{\tau+1}$, σ can be replaced by $\big(w_n, \underset{q\,|\,n,\ q \text{ prime}}{\text{l.c.m.}} [K(\zeta_q) : K]\big)$.

Lemma 8. *If every integral vector* $[t_0, t_1, \ldots, t_r]$ *satisfies at least one of the congruences*

$$\sum_{s=0}^{r} a_{hs} t_s \equiv 0 \bmod m \quad (1 \leqslant h \leqslant g) \tag{41}$$

then for at least one h *we have*

$$a_{h0} \equiv 0 \bmod (a_{h1}, \ldots, a_{hr}, m)$$

and

$$\frac{m}{(a_{h1}, \ldots, a_{hr}, m)} \leqslant \max(g-1, 1). \tag{42}$$

Proof. Let us choose in $\{1, 2, \ldots, g\}$ a minimal subset M with the property that every integral vector $[1, t_1, \ldots, t_r]$ satisfies at least one congruence (41) with $h \in M$.

Put $d_h = (a_{h1}, \ldots, a_{hr}, m)$. For $h \in M$ we have $a_{h0} \equiv 0 \bmod d_h$, since otherwise the congruence

$$a_{h0} + \sum_{s=1}^{r} a_{hs} t_s \equiv 0 \bmod m \tag{43}$$

would not be satisfied by any $[t_1, \ldots, t_r]$.

Hence, by a theorem of Frobenius the congruence (43) has $d_h m^{r-1}$ solutions $\bmod m$. If for a certain $h \in M$ we have $m/d_h < g$ (42) follows. If for all $h \in M$, $m/d_h \geqslant g$ then either

$$\sum_{h \in M} \frac{d_h}{m} < 1$$

or $|M| = g$ and $d_h = m/g$ $(1 \leqslant h \leqslant g)$. The former case is impossible since then the alternative of congruences (43) for $h \in M$ would have $m^r \sum d_h/m < m^r$ solutions $\bmod m$, contrary to the choice of M. In the latter case, we consider the system of congruences

$$\sum_{s=1}^{r} a_{hs} t_s \equiv 0 \bmod m$$

obtained from (41) by the substitution $t_0 = 0$. Since every integral vector $[t_1, \ldots, t_r]$ satisfies at least one of these congruences and $\sum_{h=1}^{g} d_h/m = 1$, every vector must satisfy exactly one congruence. However, vector $[0, \ldots, 0]$ satisfies them all. This is a contradiction unless $g = 1$, $m = d_1$. □

Lemma 9. *In any number field K there exists a multiplicative basis, i.e. such a sequence $\pi_1, \pi_2, \ldots$ that any non-zero element of K is represented uniquely as $\zeta \prod_{s=1}^{t} \pi_s^{x_s}$, where x_s are rational integers and ζ is a root of unity contained in K.*

Proof. See Skolem [8]. □

Proof of Theorem 5. Let $\beta_1, \ldots, \beta_g$ be the zeros of f_i. We assume without loss of generality that $\beta_i \neq 0$ and put $K_1 = K(\beta_1, \ldots, \beta_g)$. Let in K_1

$$\alpha_j = \zeta_w^{a_{j0}} \prod_{s=1}^{t} \pi_s^{a_{js}} \qquad (1 \leqslant j \leqslant k),$$

$$\beta_h = \zeta_w^{b_{h0}} \prod_{s=1}^{t} \pi_s^{b_{hs}} \qquad (1 \leqslant h \leqslant g),$$

where w is the number of roots of unity contained in K_1 and π_s are elements of the multiplicative basis described in Lemma 9. Let $\boldsymbol{A} = [a_{js}]_{\substack{1\leqslant j\leqslant k\\ 1\leqslant s\leqslant t}}$ and let $\boldsymbol{P}$ and $\boldsymbol{Q}$ be unimodular matrices such that

$$\boldsymbol{P}\boldsymbol{A}\boldsymbol{Q} = \begin{bmatrix} e_1 & & & & \\ & e_2 & & & \\ & & \ddots & & \\ & & & e_r & \\ & & & & \ddots \end{bmatrix},$$

where all the elements outside the principal diagonal are zero, on the diagonal precisely $e_1, \dots, e_r$ are non-zero and $e_i \mid e_{i+1}$. Let

$$\boldsymbol{P}\begin{bmatrix} a_{10} \\ \vdots \\ a_{k0} \end{bmatrix} = \begin{bmatrix} c_1 \\ \vdots \\ c_k \end{bmatrix}, \quad [b_{h1}, \dots, b_{ht}]\boldsymbol{Q} = [d_{h1}, d_{h2}, \dots, d_{ht}].$$

We choose integers $\eta_{r+1}, \dots, \eta_t$ divisible by w so that for all $h \leqslant g$

$$\sum_{s=r+1}^{t} d_{hs}\eta_s = 0 \quad \text{implies} \quad d_{hs} = 0 \quad (r < s \leqslant t)$$

and set

$$m = \max_{1\leqslant h\leqslant g}\left|\sum_{s=r+1}^{t} d_{hs}\eta_s\right| + 1.$$

Further we set

$$n = 2^{\tau} wme_r \operatorname*{l.c.m.}_{\substack{q\leqslant m+e_r\\ q \text{ prime}}} (q-1), \quad \eta_s = (w, c_{r+1}, \dots, c_k)\frac{n}{e_s w}t_s + c_s\frac{n}{e_s w}t_0,$$

$$(1 \leqslant s \leqslant r)$$

where τ is the relevant parameter of the field K_1,

$$\varepsilon_0 = -t_0, \quad \begin{bmatrix} \varepsilon_1 \\ \vdots \\ \varepsilon_t \end{bmatrix} = \boldsymbol{Q}\begin{bmatrix} \eta_1 \\ \vdots \\ \eta_t \end{bmatrix}.$$

By Theorem 4 there exist infinitely many prime ideals $\mathfrak{p}$ of $K_1(\zeta_n)$ such that

$$\left(\frac{\zeta_w}{\mathfrak{p}}\right)_n = \zeta_w^{\varepsilon_0}, \quad \left(\frac{\pi_s}{\mathfrak{p}}\right)_n = \zeta_n^{\varepsilon_s} \quad (1 \leqslant s \leqslant t).$$

The congruence

$$f\left(\alpha_1^{x_1}\cdots\alpha_k^{x_k}\right) \equiv 0 \bmod \mathfrak{p}$$

gives for a suitable $h \leqslant g$

$$\left(\frac{\alpha_1^{x_1} \cdots \alpha_k^{x_k}}{\mathfrak{p}}\right)_n = \left(\frac{\beta_h}{\mathfrak{p}}\right)_n$$

hence

$$\sum_{j=1}^{k} x_j \left(\frac{n}{w}\, a_{j0}\varepsilon_0 + \sum_{s=1}^{t} a_{js}\varepsilon_s\right) \equiv \frac{n}{w}\, b_{h0}\varepsilon_0 + \sum_{s=1}^{t} b_{hs}\varepsilon_s \bmod n.$$

Setting $[y_1, \ldots, y_k] = [x_1, \ldots, x_k]\boldsymbol{P}^{-1}$ we get

$$\sum_{j=1}^{k} y_j \left(\frac{n}{w}\, c_j\varepsilon_0 + e_j\eta_j\right) \equiv \frac{n}{w}\, b_{h0}\varepsilon_0 + \sum_{s=1}^{t} d_{hs}\eta_s \bmod n,$$

where $e_j = 0$ for $j > r$, hence

$$\frac{n}{w}\left(\sum_{j=1}^{r} y_j(w, c_{r+1}, \ldots, c_k)t_j - \sum_{j=r+1}^{k} y_j c_j t_0\right)$$
$$\equiv -\frac{n}{w}\, b_{h0}t_0 + \frac{n}{w}\sum_{s=1}^{r} d_{hs}\left(\frac{(w, c_{r+1}, \ldots, c_k)}{e_s}\, t_s + \frac{c_s}{e_s}\, t_0\right) + \sum_{s=r+1}^{t} d_{hs}\eta_s \bmod n.$$

It follows that

$$\sum_{s=r+1}^{t} d_{hs}\eta_s \equiv 0 \bmod m, \qquad \sum_{s=r+1}^{t} d_{hs}\eta_s = 0$$

and by the choice of $\eta_{r+1}, \ldots, \eta_s$: $d_{hs} = 0$ $(r < s \leqslant t)$.

Hence all integer vectors $[t_0, \ldots, t_r]$ satisfy at least one congruence

$$\sum_{s=1}^{r} \frac{nd_{hs}}{we_s}(w, c_{r+1}, \ldots, c_k)t_s + t_0\left(\sum_{s=1}^{r} \frac{nc_s d_{hs}}{we_s} - \frac{n}{w}\, b_{h0}\right) \equiv 0 \bmod \frac{n}{w}(w, c_{r+1}, \ldots, c_k),$$

such that $d_{hs} = 0$ $(r < s \leqslant t)$.

It follows by Lemma 8 that for a certain h

$$q = \frac{n/w}{\left(\dfrac{n}{w}, \underset{1 \leqslant s \leqslant r}{\text{g.c.d.}} \dfrac{n}{w}\, \dfrac{d_{hs}}{e_s}\right)} \leqslant \max(g - 1, 1), \quad d_{hs} = 0 \quad (r < s \leqslant t) \tag{44}$$

and

$$\sum_{s=1}^{r} \frac{n}{w}\, \frac{c_s d_{hs}}{e_s} - \frac{n}{w}\, b_{h0} \equiv 0 \bmod \frac{n}{wq}(w, c_{r+1}, \ldots, c_k). \tag{45}$$

For h satisfying (44) we have

$$\frac{d_{hs}}{e_s} = \frac{p_s}{q}, \quad p_s \text{ integer} \quad (1 \leqslant s \leqslant r), \quad (p_1, \ldots, p_r, q) = 1$$

and by (45) there exist integers $u_1, \dots, u_k$ such that

$$\sum_{s=1}^{r} \frac{n}{w} \frac{c_s d_{hs}}{e_s} - \frac{n}{w} b_{h0} + \sum_{s=1}^{r} n \frac{d_{hs}}{e_s} u_s + \sum_{s=r+1}^{k} \frac{n}{wq} c_s u_s \equiv 0 \bmod n. \tag{46}$$

Let us fix any values of $\log \pi_s$ $(1 \leqslant s \leqslant t)$ and set $\log \zeta_w = \dfrac{2\pi i}{w}$. The function α_j^x is many valued and $\prod_{j=1}^{k} \alpha_j^{x_j}$ can take any value

$$V = \exp\left[\frac{2\pi i}{w} \sum_{j=1}^{k} a_{j0} x_j + \sum_{s=1}^{t} \log \pi_s \sum_{j=1}^{k} a_{js} x_j + 2\pi i \sum_{j=1}^{k} v_j x_j\right],$$

where $[v_1, \dots, v_k]$ is an integral vector. Taking

$$[v_1, \dots, v_k] = [u_1, \dots, u_r, 0, \dots, 0](\boldsymbol{P}^{-1})^T,$$
$$[x_1, \dots, x_k] = \left[\frac{d_{h1}}{e_1}, \dots, \frac{d_{hr}}{e_r}, \frac{u_{r+1}}{q}, \dots, \frac{u_k}{q}\right]\boldsymbol{P}$$

we get

$$V = \exp\left[\frac{2\pi i}{w}\left(\sum_{j=1}^{r} \frac{d_{hj}}{e_j} c_j + \sum_{j=r+1}^{k} \frac{u_j}{q} c_j\right) + \sum_{s=1}^{t} b_{hs} \log \pi_s + 2\pi i \sum_{j=1}^{r} \frac{d_{hj}}{e_j} u_j\right].$$

By (46) $V = \beta_h$, hence $f(V) = 0$. □

Remark. Theorem 5 is essentially best possible, as the following example shows:

$$f(t) = (t - \beta_1) \prod_{j=0}^{q-1} \left(t - \beta_1^j \beta_2\right),$$

where q is a prime and β_1, β_2 are integers of K multiplicatively independent.

The congruence

$$f\left(\alpha_1^{x_1} \alpha_2^{x_2}\right) \equiv 0 \bmod \mathfrak{p}, \quad \text{where} \quad \alpha_1 = \beta_1^q,\ \alpha_2 = \beta_2^q,$$

is soluble for every prime ideal $\mathfrak{p}$. Indeed, let γ be a primitive root $\bmod \mathfrak{p}$.

If $\operatorname{ord}_q \operatorname{ind}_\gamma \beta_1 > \operatorname{ord}_q \operatorname{ind}_\gamma \beta_2$ then the equation

$$q x_1 \operatorname{ind}_\gamma \beta_1 + q x_2 \operatorname{ind}_\gamma \beta_2 = \operatorname{ind}_\gamma \beta_1$$

is soluble and so is the congruence

$$\alpha_1^{x_1} \alpha_2^{x_2} \equiv \beta_1 \bmod \mathfrak{p}.$$

If on the other hand, $\operatorname{ord}_q \operatorname{ind}_\gamma \beta_1 \leqslant \operatorname{ord}_q \operatorname{ind}_\gamma \beta_2$ then there is a $j < q$ such that

$$\operatorname{ord}_q\left(j \operatorname{ind}_\gamma \beta_1 + \operatorname{ind}_\gamma \beta_2\right) > \operatorname{ord}_q \operatorname{ind}_\gamma \beta_1.$$

This implies the solubility of the equation

$$qx_1 \operatorname{ind}_\gamma \beta_1 + qx_2 \operatorname{ind}_\gamma \beta_2 = j \operatorname{ind}_\gamma \beta_1 + \operatorname{ind}_\gamma \beta_2$$

and of the congruence

$$\alpha_1^{x_1}\alpha_2^{x_2} \equiv \beta_1^j \beta_2 \bmod \mathfrak{p}.$$

c The solubility of $f\left(\alpha_1^{x_1}\alpha_2^{x_2}\right) \equiv 0 \bmod \mathfrak{p}$ if $\mathfrak{p} \mid \alpha_1\alpha_2$ is trivial. On the other hand, the equation $f\left(\alpha_1^{x_1}\alpha_2^{x_2}\right) = 0$ has only the solutions $(x_1, x_2) = \left(\frac{1}{q}, 0\right), \left(\frac{j}{q}, \frac{1}{q}\right)$ $(0 \leqslant j \leqslant q)$.

For $\beta_1 = \zeta_q$, β_2 different from a root of unity we get an example with $k = 1$.

Let us note further that Theorem 5 does not extend to all exponential congruences even in one variable, e.g. the congruence

$$(\alpha^x + \alpha)\left((-\alpha)^x - \alpha\right) \equiv 0 \bmod \mathfrak{p}$$

is soluble for all prime ideals $\mathfrak{p}$, but the corresponding equation has no rational solutions if α is not a root of unity.

Proof of the Corollary. For $b = 0$ it suffices to put in Theorem 5

$$f(t) = u_1 t - c, \quad k = 1, \quad \alpha_1 = a.$$

For $b = -1$, we have $t^2 - at - b = (t - \alpha)(t - \alpha^{-1})$ with $\alpha \neq \pm 1$ since $a^2 - 4 \neq 0$. It c is well known that $u_n = \lambda_1\alpha^n + \lambda_2\alpha^{-n}$ and it suffices to put in Theorem 5

$$f(t) = \lambda_1 t^2 - ct + \lambda_2, \quad k = 1, \quad \alpha_1 = \alpha.$$

For $b = 1$ we have $t^2 - at - b = (t - \alpha)(t + \alpha^{-1})$ with $\alpha \neq \pm 1$ since $a \neq 0$. Now $u_n = \lambda_1\alpha^n + \lambda_2(-\alpha)^{-n}$, where λ_1, λ_2 are conjugate in the field $\mathbb{Q}(\alpha)$. If $c = 0$, we set in Theorem 5

$$f(t) = \lambda_1 t + \lambda_2, \quad k = 1, \quad \alpha_1 = -\alpha^2.$$

If $c \neq 0$, we set

$$f(t) = (\lambda_1 t^2 - ct + \lambda_2)(\lambda_1 t^2 - ct - \lambda_2), \quad k = 1, \quad \alpha_1 = \alpha,$$

where α is chosen negative (one of the numbers α, $-\alpha^{-1}$ is always negative). We infer that the equation $f(\alpha^x) = 0$ has a solution $x = m/q$, where $(m, q) = 1$, $q \leqslant 3$. If $q = 1$ and

$$\lambda_1\alpha^{2m} - c\alpha^m + (-1)^m\lambda_2 = 0$$

we get $c = u_m$. If $q = 1$ and

$$\lambda_1\alpha^{2m} - c\alpha^m - (-1)^m\lambda_2 = 0 \tag{47}$$

we get a contradiction. Indeed, since

$$\lambda_1\alpha^{2m} - u_m\alpha^m + (-1)^m\lambda_2 = 0$$

we obtain

$$2\lambda_1\alpha^{2m} - (c + u_m)\alpha^m = 0, \quad \lambda_1 = \tfrac{1}{2}(c + u_m)\alpha^{-m}, \quad \lambda_2 = \tfrac{1}{2}(c + u_m)(-\alpha)^{-m}$$

and from (47) $c = 0$.

$q = 2$ is impossible since then both numbers $\lambda_1\alpha^{2x} - c\alpha^x \pm \lambda_2$ have a non-zero imaginary part.

Finally $q = 3$ is impossible for the following reason. If $\alpha \neq \beta^3$, $\beta \in \mathbb{Q}(\alpha)$ then $\alpha^{m/3}$ is of degree 3 over $\mathbb{Q}(\alpha)$ and cannot satisfy the equation $\lambda_1 t^2 - ct \pm \lambda_2 = 0$ for any choice of sign. If $\alpha = \beta^3$, $\beta \in \mathbb{Q}(\alpha)$ then β satisfies an equation $t^2 - dt - 1 = 0$, d integer, and we get $a = \operatorname{Tr}\beta^3 = d^3 + 3d$, contrary to the assumption. □

Lemma 10. *If every integral vector* $[t_1, \ldots, t_k]$ *satisfies at least one congruence of the set* S:

$$a_{h0} + \sum_{j=1}^{k} a_{hj} t_j \equiv 0 \bmod m \quad (1 \leqslant h \leqslant g) \tag{48}$$

and no proper subset of S *has the same property then for all* h, j

$$M(g) a_{hj} \equiv 0 \bmod m,$$

where

$$M(g) = \prod_{\substack{p \leqslant g \\ p \text{ prime}}} p^{[(g-1)/(p-1)]}.$$

Proof. Let $d_h = (a_{h1}, a_{h2}, \ldots, a_{hk}, m)$. If $d_h \nmid a_{h0}$ the congruence

$$\sum_{j=1}^{k} a_{hj} t_j + a_{h0} \equiv 0 \bmod m$$

is never satisfied contrary to the minimal property of S. Hence for all h

$$a_{h0} \equiv 0 \bmod d_h \tag{49}$$

and the congruences (48) take the form

$$\sum_{j=1}^{k} \frac{a_{hj}}{d_h} t_j + \frac{a_{h0}}{d_h} \equiv 0 \bmod \frac{m}{d_h} \quad (1 \leqslant h \leqslant g). \tag{50}$$

For a given prime p let n_r be the number of indices $h \leqslant g$ such that $p^r \parallel \dfrac{m}{d_h}$ and let s be the largest r with $n_r \neq 0$. We have

$$\frac{n_r}{p} + \frac{n_{r+1}}{p^2} + \ldots + \frac{n_s}{p^{s-r+1}} \geqslant 1 \quad (1 \leqslant r \leqslant s). \tag{51}$$

In order to prove this assume that for a certain $r \leqslant s$

$$\frac{n_r}{p} + \frac{n_{r+1}}{p^2} + \ldots + \frac{n_s}{p^{s-r+1}} < 1. \tag{52}$$

The congruences (48) with $p^r \nmid \dfrac{m}{d_h}$ form a proper subset of the set S and by the assumption there is a vector $\boldsymbol{t}^0$ which does not satisfy any of them.

On the other hand, a congruence (50) with $p^q \parallel \frac{m}{d_h}$ $(q \geqslant r)$ is in virtue of Frobenius's theorem (used in proof of Lemma 8) satisfied by at most

$$\Big(\frac{a_{h1}}{d_h}, \ldots, \frac{a_{hk}}{d_h}, p^{q-r+1}\Big) p^{(q-r+1)(k-1)} = p^{(q-r+1)(k-1)}$$

integral vectors $\boldsymbol{t}$ mod p^q satisfying

$$\boldsymbol{t} \equiv \boldsymbol{t}^0 \bmod p^{r-1}. \tag{53}$$

The alternative of all congruences in question is satisfied by at most

$$\sum_{q=r}^{s} \frac{n_q}{p^{q-r+1}} p^{(s-r+1)k}$$

integral vectors $\boldsymbol{t}$ mod p^s satisfying (53). Since the number of all integral vectors $\boldsymbol{t}$ mod p^s satisfying (53) is $p^{(s-r+1)k}$, (52) implies the existence of a vector $\boldsymbol{t}_1 \equiv \boldsymbol{t}_0 \bmod p^{r-1}$ which satisfies no congruence (50) and consequently no congruence (48) with $p^r \mid \frac{m}{d_h}$. By the Chinese remainder theorem there exists a vector $\boldsymbol{t}$ such that

$$\boldsymbol{t} \equiv \boldsymbol{t}_0 \bmod \operatorname*{l.c.m.}_{p^r \nmid m/d_h} \frac{m}{d_h},$$
$$\boldsymbol{t} \equiv \boldsymbol{t}_1 \bmod p^s.$$

This vector satisfies no congruence (48). The obtained contradiction proves (51).

Consider the lower bound of the function $n_1 + n_2 + \ldots + n_s = f(n_1, \ldots, n_s)$ under the condition (51), where now $n_1, \ldots, n_s$ are nonnegative real numbers. Since $f(n_1, n_2, \ldots, n_s) \geqslant \max\limits_{1 \leqslant r \leqslant s} n_r$ the lower bound is attained.

Let $(n_1^{(0)}, \ldots, n_s^{(0)})$ be a point in which it is attained. We shall show by induction with respect to $s - r$

$$n_r^{(0)} = p - 1 \quad (1 \leqslant r < s), \quad n_s^{(0)} = p. \tag{54}$$

Indeed, (51) for $r = s$ gives $n_s^{(0)} \geqslant p$. If $n_s^{(0)} > p$, we set $n_r^{(1)} = n_r^{(0)}$ for $r < s-1, n_{s-1}^{(1)} = n_{s-1}^{(0)} + \frac{1}{p}(n_s^{(0)} - p), n_s^{(1)} = p$, verify (51) and find $f(n_1^{(1)}, \ldots, n_s^{(1)}) < f(n_1^{(0)}, \ldots, n_s^{(0)})$ which is impossible. Assume now that (54) holds for $s - r < s - q$, i.e. $r > q$. The condition (51) for $r = q$ gives

$$\frac{n_q^{(0)}}{p} \geqslant 1 - \sum_{q=r+1}^{s-1} \frac{p-1}{p^{q-r+1}} - \frac{p}{p^{s-r+1}} \frac{p-1}{p}; \quad n_q^{(0)} \geqslant p - 1.$$

If $n_q^{(0)} > p - 1$, we set

$$n_r^{(1)} = n_r^{(0)} \quad \text{for} \quad r \neq q-1, q;$$
$$n_{q-1}^{(1)} = n_{q-1}^{(0)} + \frac{1}{p}(n_q^{(0)} - p + 1), \quad n_q^{(1)} = p - 1,$$

verify (51) and find again

$$f(n_1^{(1)}, \ldots, n_s^{(1)}) < f(n_1^{(0)}, \ldots, n_s^{(0)}),$$

which is impossible.

Since $n_1^{(0)} + \ldots + n_s^{(0)} \leqslant g$ it follows from (54) that

$$s(p-1) + 1 \leqslant g, \quad s \leqslant \left[\frac{g-1}{p-1}\right]$$

and thus for all $h \leqslant g$, $\dfrac{m}{d_h} \mid M(g)$.

This together with (49) gives the lemma. □

Lemma 11. *If every integral vector* $[t_1, \ldots, t_r]$ *satisfies at least one of the congruences*

$$a_{h0} + \sum_{s=1}^{r} a_{hs} t_s \equiv 0 \bmod m \tag{55}$$

$(1 \leqslant h \leqslant g)$ *then for at least one* h

$$a_{h0} \equiv 0 \bmod m \quad \textit{and} \quad M(g) a_{hs} \equiv 0 \bmod m \quad (1 \leqslant s \leqslant r), \tag{56}$$

where $M(g)$ *has the meaning of Lemma* 10.

Proof. Choose in $\{1, 2, \ldots, g\}$ a minimal subset M with the property that every integral vector satisfies at least one congruence (55) with $h \in M$. To the set of these congruences Lemma 10 applies. The congruence satisfied by the vector $[0, 0, \ldots, 0]$ satisfies also the conditions (56). □

Remark. $M(g)$ is the least number with the property formulated in Lemmata 10 and 11, as the following example shows already in dimension one: $m = p^{[(g-1)/(p-1)]}$ (p prime), $a_{11} = 1$, $a_{10} = 0$ and for $h = (p-1)q + r + 1$, $1 \leqslant r \leqslant p-1$, $2 \leqslant h \leqslant g$, $a_{h1} = p^q$, $a_{h0} = \dfrac{m}{p} r$.

c For $k = 1$ Lemma 10 is contained in a stronger result of S. Znám [11], however his proof does not extend to $k > 1$.

Lemma 12. *Let* H, I *be two finite sets and let* M_{hi} $(h \in H, i \in I)$ *be inhomogeneous linear forms with integral coefficients. If for every positive integer* m *and a suitable* $h \in H$ *the system of congruences*

$$M_{hi}(x) \equiv 0 \bmod m \quad (i \in I) \tag{57}$$

is soluble then for a suitable $h \in H$ *the system of equations*

$$M_{hi}(x) = 0 \quad (i \in I) \tag{58}$$

is soluble in integers.

Proof. Suppose that no system (58) is soluble in integers. Then by Lemma 9 of [6] for each $h \in H$ there exists an m_h such that the system (57) is insoluble for $m = m_h$. Taking

$m = \prod_{h \in H} m_h$ we infer that the system (57) is insoluble for any $h \in H$ contrary to the assumption. □

Proof of Theorem 6. Let us set

$$\alpha_{hij} = \zeta_w^{a_{hij0}} \prod_{s=1}^{r} \pi_s^{a_{hijs}}, \quad \beta_{hi} = \zeta_w^{b_{hi0}} \prod_{s=1}^{r} \pi_s^{b_{his}}, \tag{59}$$

where w is the number of roots of unity contained in K and π_s are elements of the multiplicative basis described in Lemma 9. Consider the linear forms

$$\begin{aligned} L_{hi0} &= wx_0 + \sum_{j=1}^{k} a_{hij0} x_j - b_{hi0}, \\ L_{his} &= \sum_{j=1}^{k} a_{hijs} x_j - b_{his} \quad (1 \leqslant s \leqslant r) \end{aligned} \tag{60}$$

and let H be the set of all vectors $\boldsymbol{h} = [h_1, h_2, \ldots, h_l]$ with $1 \leqslant h_i \leqslant g_i$ $(1 \leqslant i \leqslant l)$, I be the set of all vectors $\boldsymbol{i} = [i, s]$ with $1 \leqslant i \leqslant l$, $0 \leqslant s \leqslant r$.

For any $\boldsymbol{h} \in H$, $\boldsymbol{i} = [i, s] \in I$ we put

$$M_{\boldsymbol{hi}} = L_{h_i is}. \tag{61}$$

We assert that for any positive integer m there exists an $\boldsymbol{h} \in H$ such that the system of congruences

$$M_{\boldsymbol{hi}}(x_0, x_1, \ldots, x_k) \equiv 0 \bmod m \quad (\boldsymbol{i} \in I) \tag{62}$$

is soluble.

Let us take $n = 2^\tau w M(\max g_i) m \operatorname{l.c.m.}_{\substack{q \leqslant m + \max g_i \\ q \text{ prime}}} (q-1)$, where τ is the relevant parameter of K.

By Theorem 4 for any choice of $t_1, \ldots, t_r \bmod n/w$ there exists a prime ideal $\mathfrak{p}$ of $K(\zeta_n)$ prime to D such that

$$\left(\frac{\zeta_w}{\mathfrak{p}}\right)_n = \zeta_w, \quad \left(\frac{\pi_s}{\mathfrak{p}}\right)_n = \zeta_n^{w t_s} \quad (1 \leqslant s \leqslant r). \tag{63}$$

Let $\mathfrak{m}$ be the product of all these prime ideals $\mathfrak{p}$.

The solubility of the system of congruences

$$\prod_{h=1}^{g_i} \left(\prod_{j=1}^{k} \alpha_{hij}^{x_j} - \beta_{hi} \right) \equiv 0 \bmod \mathfrak{m} \quad (i = 1, \ldots, l)$$

implies that for any vector $[t_1, \ldots, t_r]$ and any $i \leqslant l$ there is an $h \leqslant g_i$ such that

$$\prod_{j=1}^{k} \alpha_{hij}^{x_j} \equiv \beta_{hi} \bmod \mathfrak{p}, \quad \prod_{j=1}^{k} \left(\frac{\alpha_{hij}}{\mathfrak{p}} \right)_n^{x_j} = \left(\frac{\beta_{hi}}{\mathfrak{p}} \right)_n$$

for some $\mathfrak{p}$ satisfying (63). This implies by (59) that

$$\sum_{j=1}^{k}\left(\frac{n}{w}\,a_{hij0}+\sum_{s=1}^{r} wt_s a_{hijs}\right)x_j \equiv \frac{n}{w}\,b_{hi0}+\sum_{s=1}^{r} wt_s b_{his} \bmod n,$$

whence

$$\frac{n}{w}\left(\sum_{j=1}^{k} a_{hij0}x_j - b_{hi0}\right)+w\sum_{s=1}^{r} t_s\left(\sum_{j=1}^{k} a_{hijs}x_j - b_{his}\right)\equiv 0 \bmod n.$$

Using now Lemma 11 we get that for any $i \leqslant l$ and a certain $h_i \leqslant g_i$

$$\sum_{j=1}^{k} a_{h_i ij0}x_j - b_{h_i i0} \equiv 0 \bmod w,$$

$$\sum_{j=1}^{k} a_{h_i ijs}x_j - b_{h_i is} \equiv 0 \bmod m \quad (1 \leqslant s \leqslant r).$$

c

In virtue of (60) and (61) this is equivalent for a suitable x_0 to the system (62) in which $\boldsymbol{h} = [h_1, \ldots, h_l]$. Therefore, by Lemma 12 there exists a vector $\boldsymbol{h}^0 = [h_1^0, \ldots, h_l^0]$ such that the system of equations

$$M_{\boldsymbol{h}^0\boldsymbol{i}}(x_0, x_1, \ldots, x_k) = 0 \quad (\boldsymbol{i} \in I)$$

is soluble in integers. Denoting a solution by $[x_0^0, x_1^0, \ldots, x_k^0]$ we get from (60) and (61) for all $i \leqslant l$

$$wx_0^0 + \sum_{j=1}^{k} a_{h_i^0 ij0}x_j^0 - b_{h_i^0 i0} = 0,$$

$$\sum_{j=1}^{k} a_{h_i^0 ijs}x_j^0 - b_{h_i^0 is} = 0 \quad (1 \leqslant s \leqslant r)$$

hence by (59)

$$\prod_{h=1}^{g_i}\left(\prod_{j=1}^{h}\alpha_{hij}^{x_j^0} - \beta_{hi}\right) = 0 \quad (1 \leqslant i \leqslant l). \qquad \square$$

Addendum

1. Dr. J. Wójcik has pointed out that the equality in formula (28) which is only said to hold but not proved is actually used in the formula (##) on p. 954. The equality in question follows from the formula (#) on p. 953, where also $\leqslant$ can be replaced by $=$. The latter is a consequence of the fact that for $q > 2$ the extension $K(\zeta_{q^s})/K$ is cyclic and for $q = 2$, $p \neq 2$ we have $\operatorname{ord}_p[K(\zeta_{q^s}) : K] = 0$.

2. The remark made on p. 955 has not been proved rigorously, since it is not clear why $\tau(\chi) \neq 0$. Therefore, we return to the question and we shall prove more than was asserted

namely that the number σ occurring in Theorem 3 is the least integer with the required property, provided $(\sigma, n/w_n) = 1$.

By the definition of σ there exists a character χ belonging to the exponent σ on the group $G = \mathrm{Gal}\big(K(\zeta_n)/K\big)$ represented as a multiplicative group of residue classes mod n. Let

$$\tau_y = \sum_{x \in G} \chi(x)\zeta_n^{xy}.$$

Since $\chi(x)$ are non-zero and the Vandermonde determinant $|\zeta_n^{xy}|_{\substack{x\in G \\ y=1,2,\ldots,|G|}}$ is non-zero there exists a y such that $\tau_y \neq 0$. Let us fix such a y and denote the corresponding τ_y by $\tau(\chi) \neq 0$. Since $\chi(x) \in K$, $\chi(x)^\sigma = 1$ we have $\tau(\chi) \in K(\zeta_n)$, $\tau(\chi)^\sigma \in K$, $\tau(\chi)^{n\sigma} \in K^n$. Suppose that $\tau(\chi)^{n\sigma} = \gamma^n$, $\gamma \in K$. Then

$$\tau(\chi)^{(n/w_n)\varrho} = \zeta_{w_n}^{\alpha}\gamma \in K$$

and applying an automorphism $\zeta_n \to \zeta_n^j$ with $j \in G$ we get

$$\tau(\chi)^{(n/w_n)\varrho}\,\overline{\chi}(j)^{(n/w_n)\varrho} = \tau(\chi)^{(n/w_n)\varrho}.$$

Since $\tau(\chi) \neq 0$ it follows that

$$\chi(j)^{(n/w_n)\varrho} = 1$$

and by the choice of χ

$$\sigma \;\Big|\; \frac{n}{w_n}\varrho.$$

Hence if $(\sigma, n/w_n) = 1$ we get $\sigma \mid \varrho$. If $(\sigma, n/w_n) \neq 1$ σ need not be the least integer with the property asserted in Theorem 3. In particular if $\zeta_4 \notin K$, $n \equiv 0 \bmod 2^{\tau+1}$, $\sqrt{-\big(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\big)} \in K$, σ can be replaced by $(w_n, \underset{q\mid n,\, q \text{ prime}}{\text{l.c.m.}} [K(\zeta_q) : K])$.

The remark on p. 957 remains valid on replacing $(w_n, n/w_n)$ by $(\sigma, n/w_n)$ which makes it stronger.

3. Theorem 6 has the following equivalent form much more useful in applications.

Theorem 7. *Let $f_r(z_1, \ldots, z_p)$ $(1 \leqslant r \leqslant s)$ be polynomials with coefficients in an algebraic number field K and α_{ij} $(1 \leqslant i \leqslant p,\ 1 \leqslant j \leqslant q)$ non-zero elements of K, M a positive integer. If the system of equations*

$$f_r(z_1, \ldots, z_p) = 0 \quad (1 \leqslant r \leqslant s) \tag{A1}$$

has only finitely many solutions in the complex field and the system of congruences

$$f_r\left(\prod_{j=1}^{q} \alpha_{1j}^{x_j}, \ldots, \prod_{j=1}^{q} \alpha_{pj}^{x_j}\right) \equiv 0 \bmod m \quad (1 \leqslant r \leqslant s) \tag{A2}$$

is soluble for all moduli m prime to M then the system of equations

$$f_r\Big(\prod_{j=1}^{q}\alpha_{1j}^{x_j},\ldots,\prod_{j=1}^{q}\alpha_{pj}^{x_j}\Big)=0\quad(1\leqslant r\leqslant s) \tag{A3}$$

is soluble in rational integers x_j.

Proof. Since the system (A1) has only finitely many solutions they all lie in a finite extension K_1 of K. Let them be $(\beta_{h1},\ldots,\beta_{hp})$ $(1\leqslant h\leqslant g)$. Thus we have the equivalence

$$\bigwedge_{r\leqslant s} f_r(z_1,\ldots,z_p)=0\equiv\bigvee_{h\leqslant g}\bigwedge_{i\leqslant p} z_i=\beta_{hi}$$

and by the distributive property of alternative with respect to conjunction

$$\begin{aligned}\bigwedge_{r\leqslant s} f_r(z_1,\ldots,z_p)=0&\equiv\bigwedge_{i_1\leqslant p}\bigwedge_{i_2\leqslant p}\cdots\bigwedge_{i_g\leqslant p}\bigvee_{h\leqslant g} z_{i_h}=\beta_{hi_h}\\&\equiv\bigwedge_{i_1\leqslant p}\bigwedge_{i_2\leqslant p}\cdots\bigwedge_{i_g\leqslant p}\prod_{h=1}^{g}(z_{i_h}-\beta_{hi_h})=0.\end{aligned} \tag{A4}$$

By the Hilbert theorem on zeros it follows that for every integral vector $\boldsymbol{i}=[i_1,\ldots,i_g]\in\{1,2,\ldots,p\}^g=I$ and a suitable exponent e_i we have

$$\prod_{h=1}^{g}(z_{i_h}-\beta_{hi_h})^{e_i}=\sum_{r=1}^{s} f_r(z_1,\ldots,z_p)F_{r\boldsymbol{i}}(z_1,\ldots,z_p), \tag{A5}$$

where $F_{r\boldsymbol{i}}\in K_1[z_1,\ldots,z_p]$. If $\mathfrak{m}$ is prime to the denominators of $F_{r\boldsymbol{i}}$ and to the numerators as well as the denominators of α_{ij}, the system of congruences (A2) with $m=\mathfrak{m}^e$, $e=\max_{\boldsymbol{i}\in I} e_{\boldsymbol{i}}$, and the identity (A5) imply

$$\prod_{\substack{h=1\\ \beta_{hi_h}\neq 0}}^{g}\Big(\prod_{j=1}^{q}\alpha_{i_hj}^{x_j}-\beta_{hi_h}\Big)\equiv 0\bmod\mathfrak{m}\quad(\boldsymbol{i}\in I). \tag{A6}$$

Therefore, the system (A6) is soluble for all moduli prime to $D=M$ times a certain finite product. Applying Theorem 6 we infer that the system of equations

$$\prod_{h=1}^{g}\Big(\prod_{j=1}^{q}\alpha_{i_hj}^{x_j}-\beta_{hi_h}\Big)=0\quad(\boldsymbol{i}\in I)$$

is soluble in integers. By the equivalence (A4) this system is equivalent to (A3) and the proof is complete. □

References

[1] G. Darbi, *Sulla reducibilità delle equazioni algebriche*. Ann. Mat. Pura Appl. 4 (1925), 185–208.

[2] H. Hasse, *Zum Existenzsatz von Grunwald in der Klassenkörpertheorie*. J. Reine Angew. Math. 188 (1950), 40–64.

[3] D. Hilbert, *Die Theorie der algebraischen Zahlkörper*. In: Ges. Abhandlungen I, Chelsea, New York 1965.

[4] M. Kneser, *Lineare Abhängigkeit von Wurzeln*. Acta Arith. 26 (1975), 307–308.

[5] W. H. Mills, *Characters with preassigned values*. Canad. J. Math. 15 (1963), 169–171.

[6] A. Schinzel, *On power residues and exponential congruences*, Acta Arith. 27 (1975), 397–420; this collection: H4, 915–938.

[7] Th. Skolem, *Anwendung exponentieller Kongruenzen zum Beweis der Unlösbarkeit gewisser diophantischer Gleichungen*. Vid. Akad. Avh. Oslo I 1937, no. 12.

[8] —, *On the existence of a multiplicative basis for an arbitrary algebraic field*. Norske Vid. Selsk. Forh. (Trondheim) 20 (1947), no. 2, 4–7.

[9] N. Tschebotaröw [Chebotarev], *Über einen Satz von Hilbert* (Russian). Vestnik Ukr. Akad. Nauk, 1923, 3–7; Sobranie Sochineniĭ I, Moscow–Leningrad 1949–50, 14–17.

[10] —, *Grundzüge der Galoisschen Theorie*. Übersetzt und bearbeitet von H. Schwerdtfeger, Noordhoff, Groningen–Djakarta 1950.

[11] S. Znám, *On properties of systems of arithmetic sequences*. Acta Arith. 26 (1975), 279–283.

Originally published in
Comptes Rendus Mathématiques de l'Académie des Sciences. La Société Royale du Canada
Mathematical Reports of the Academy of Sciences. The Royal Society of Canada
1 (1979), 115–118

An extension of Wilson's theorem

with G. Baron (Wien)

The aim of this note is to prove the following extension of Wilson's theorem conjectured by W. Snyder in his Ph.D. thesis *A concept of Bernoulli numbers in algebraic function fields*, Univ. of Maryland 1977. Snyder has found interesting applications of his conjecture to differentials in rings of characteristic p.

Theorem. *For any prime p and any residues $x_i \bmod p$ we have*

$$(1)\qquad \sum_{\sigma\in S_{p-1}} x_{\sigma(1)}\big(x_{\sigma(1)}+x_{\sigma(2)}\big)\cdots\big(x_{\sigma(1)}+\ldots+x_{\sigma(p-1)}\big) \equiv \big(x_1+\ldots+x_{p-1}\big)^{p-1} \bmod p,$$

where the summation is taken over all permutations σ of $\{1, 2, \ldots, p-1\}$.

Let for positive integers $a_1, \ldots, a_r$ $C(a_1, \ldots, a_r)$ denote the coefficient of $X = \prod_{i=1}^{r} x_i^{a_i}$ in the sum $\sum_{\sigma\in S_n} P_\sigma$, where

$$P_\sigma = x_{\sigma(1)}\big(x_{\sigma(1)}+x_{\sigma(2)}\big)\cdots\big(x_{\sigma(1)}+\ldots+x_{\sigma(n)}\big) \quad (\sigma\in S_n).$$

Lemma 1. *Let $a_j > 1$ for $j \leqslant s$, $a_j = 1$ for $s < j \leqslant r$, $\sum_{i=1}^{r} a_i = n$. Then*

$$C(a_1, \ldots, a_r) = (n-r)\sum_{i=1}^{s} C(a_1, \ldots, a_{i-1}, a_i - 1, a_{i+1}, \ldots, a_r) + (n-r+1)(r-s)C(a_1, \ldots, a_{r-1}).$$

Proof. We have

$$\sum_{\sigma\in S_n} P_\sigma = \sum_{j=1}^{n} \sum_{\sigma\in S_n, \sigma(n)=j} P_\sigma = \sum_{j=1}^{n} \Sigma_j.$$

Presented by P. Ribenboim, F.R.S.C.

The coefficient of X in P_σ is the same as in $P_{\tau\sigma}$ where $\tau \in S_n$ is any permutation stable on $\{1, 2, \ldots, s\}$ and fixing the set $\{s+1, \ldots, r\}$. Hence the coefficient of X in Σ_j is 0 if $j \leqslant s$, is equal to the coefficient C_1 of X in Σ_r if $s < j \leqslant r$ and equal to the coefficient C_2 of X in $\Sigma_n = (x_1 + \ldots + x_n) \sum_{\sigma \in S_{n-1}} P_\sigma$ if $j > r$. If $r > s$, C_1 is equal to $C(a_1, \ldots, a_{r-1})$. On the other hand

$$C_2 = \sum_{i=1}^{s} C(a_1, \ldots, a_{i-1}, a_i - 1, a_{i+1}, \ldots, a_r) + \sum_{i=s+1}^{r} C(a_1, \ldots, a_{r-1}).$$

Hence

$$C(a_1, \ldots, a_r) = \sum_{j=s+1}^{r} C_1 + \sum_{j=r+1}^{n} C_2$$

$$= (n-r) \sum_{i=1}^{s} C(a_1, \ldots, a_{i-1}, a_i - 1, a_{i+1}, \ldots, a_r) + (n-r+1)(r-s) C(a_1, \ldots, a_{r-1}). \quad \square$$

In order to evaluate $C(a_1, \ldots, a_r)$ we introduce the following notation valid for all systems of $r \geqslant b \geqslant a \geqslant 0$ positive real numbers a_i: $R = \{1, 2, \ldots, r\}$,

$$S_1(a, b, r, q) = \sum_{i=a+1}^{b} a_i \sum\nolimits_i^* \sum_{k=1}^{q} \frac{(|T_k| + 1)!}{A(T_k) + a_i} \prod_{j=1,\, j \neq k}^{q} \frac{|T_j|!}{A(T_j) + 1},$$

$$S_2(a, b, r, q) = \sum_{i=a+1}^{b} \sum\nolimits_i^* \prod_{j=1}^{q} \frac{|T_j|!}{A(T_j) + 1},$$

where $1 \leqslant q < r$ and the inner summation $\sum_i^*$ in both sums is taken over all partitions (the order of summands neglected) of $R - \{i\}$ into q non-empty sets T_j of cardinality $|T_j|$ and $A(T_j) = \sum_{l \in T_j} a_l$. Moreover we set

$$S_1(a, b, r, r) = 0, \quad S_2(a, b, r, 0) = 0 \quad (r \geqslant 2),$$
$$S_2(0, 0, 1, 0) = 0, \quad S_2(0, 1, 1, 0) = 1.$$

Lemma 2. *For any positive $q \leqslant r$ the following identity holds*

$$S_1(0, r, r, q) + S_2(0, r, r, q-1) = (A(R) + q) \sum\nolimits^{**} \prod_{j=1}^{q} \frac{|R_j|!}{A(R_j) + 1},$$

where $\sum^{**}$ is taken over all partitions of R into q non-empty sets R_j.

Proof. For $q = r = 1$ the identity holds trivially. For $q = 1$, $r \geqslant 2$ we have

$$S_1(0, r, r, q) + S_2(0, r, r, q-1) = \sum_{i=1}^{r} a_i \frac{r!}{A(R)} = r! = (A(R) + 1) \frac{r!}{A(R) + 1}.$$

For $q \geqslant 2$ we group together all terms in $S_1(0, r, r, q)$ in which $T_k \cup \{i\} = T$. For any i, k we get $|T| \geqslant 2$. On the other hand for any $T \subset R$ with $|T| \geqslant 2$ we have

$$\sum_{i=1}^{r} a_i \sum_i^* \sum_{k=1,\, T_k \cup \{i\} = T}^{q} \frac{(|T_k|+1)!}{A(T_k)+a_i} \prod_{j=1,\, j\neq k}^{q} \frac{|T_j|!}{A(T_j)+1}$$

$$= \sum_{i \in T} a_i \sum_T^* \frac{|T|!}{A(T)} \prod_{j=1}^{q-1} \frac{|T_j|!}{A(T_j)+1} = \sum_T^* |T| \prod_{j=1}^{q-1} \frac{|T_j|!}{A(T_j)+1},$$

where $\sum_T^*$ is taken over all partitions of $R - T$ into $q-1$ non-empty sets T_j.

Hence

$$S_1(0, r, r, q) = \sum_{T \subset R,\, |T| \geqslant 2} \sum_T^* |T|! \prod_{j=1}^{q-1} \frac{|T_j|!}{A(T_j)+1}.$$

Now setting in $S_2(0, r, r, q-1)$, $\{i\} = T$ we get

$$S_2(0, r, r, q-1) = \sum_{T \subset R,\, |T|=1} \sum_T^* |T|! \prod_{j=1}^{q-1} \frac{|T_j|!}{A(T_j)+1},$$

thus

$$S_1(0, r, r, q) + S_2(0, r, r, q-1) = \sum^{**} \prod_{j=1}^{q} \frac{|R_j|!}{A(R_j)+1} \sum_{j=1}^{q} (A(R_j)+1)$$

$$= (A(R)+q) \sum^{**} \prod_{j=1}^{q} \frac{|R_j|!}{A(R_j)+1}. \quad \square$$

Lemma 3. *For any positive integers r, $a_1, \ldots, a_r$ with $a_1 + \ldots + a_r = n$ we have*

$$C(a_1, \ldots, a_r) = \frac{(n-r)!}{a_1! \cdots a_r!} \sum_{q=1}^{r} (-1)^{r-q} (n+q) \sum^{**} \prod_{j=1}^{q} \frac{|R_j|!}{A(R_j)+1}, \tag{2}$$

the inner sum being taken over all partitions of R into q non-empty subsets R_j.

Proof by induction on n. For $n = 1$ the lemma holds trivially. Assume that it is true for all sequences a_i' satisfying $\sum_{i=1}^{r} a_i' = n - 1$ and consider a sequence a_i with $\sum_{i=1}^{r} a_i = n \geqslant 2$. In view of symmetry we may assume that $a_j > 1$ for $j \leqslant s$, $a_j = 1$ for $j > s$. Let us denote the right hand side of (2) by $D(a_1, \ldots, a_r)$. By Lemma 1 and the inductive assumption

we have

$$C(a_1,\dots,a_r)=\frac{(n-r)!}{a_1!\cdots a_r!}\sum_{q=1}^{r}(-1)^{r-q}(n+q-1)!\,\big(S_1(0,s,r,q)+S_2(0,s,r,q-1)\big)$$
$$+\frac{(n-r+1)!}{a_1!\cdots a_r!}\sum_{q=1}^{r-1}(-1)^{r-q-1}(n+q-1)!\,S_2(s,r,r,q).$$

On the other hand, by Lemma 2

$$D(a_1,\dots,a_r)=\frac{(n-r)!}{a_1!\cdots a_r!}\sum_{q=1}^{r}(-1)^{r-q}(n+q-1)!\,\big(S_1(0,r,r,q)+S_2(0,r,r,q-1)\big)$$

hence

$$\frac{a_1!\cdots a_r!}{(n-r)!}\big(D(a_1,\dots,a_r)-C(a_1,\dots,a_r)\big)=(n+r-1)!\,S_1(s,r,r,r)$$
$$+\sum_{q=1}^{r-1}(-1)^{r-q}(n-q+1)!\,\big(S_1(s,r,r,q)-(r+q-1)S_2(s,r,r,q)\big)$$
$$+(-1)^{r-1}n!\,S_2(s,r,r,0).$$

However $S_1(s,r,r,r)=0$,

$$S_1(s,r,r,q)=\sum_{i=s+1}^{r}\sum_{i}^{*}\sum_{k=1}^{q}\frac{(|T_k|+1)!}{A(T_k)+1}\prod_{j=1,\,j\neq k}^{q}\frac{|T_j|!}{A(T_j)+1}$$
$$=\sum_{i=s+1}^{r}\sum_{i}^{*}\sum_{k=1}^{q}\big(|T_k|+1\big)\prod_{j=1}^{q}\frac{|T_j|!}{A(T_j)+1}=(r+q-1)S_2(s,r,r,q)$$

and since $r\geqslant 2$ or $s\geqslant 1$, $S_2(s,r,r,0)=0$. This gives

$$D(a_1,\dots,a_r)=C(a_1,\dots,a_r).\qquad\square$$

Proof of the theorem. Since both sides of the congruence (1) are symmetric it is enough to show that $a_1+\ldots+a_r=n=p-1$ implies

$$C(a_1,\dots,a_r)\equiv\frac{(p-1)!}{a_1!\cdots a_r!}\bmod p.$$

Now in formula (2) terms corresponding to $q>1$ are divisible by p since $(n+q)!\equiv 0 \bmod p$ and $A(R_j)+1<A(R)+1=p$. Hence

$$C(a_1,\dots,a_r)\equiv\frac{(n-r)!}{a_1!\cdots a_r!}\,(-1)^{r-1}\,\frac{(n+1)!\,r!}{n+1}$$
$$\equiv\frac{(p-1)!}{a_1!\cdots a_r!}\,(-1)^{r-1}(p-r-1)!\,r!\equiv\frac{(p-1)!}{a_1!\cdots a_r!}\,(p-2)!\bmod p$$

and (1) follows from Wilson's theorem.

Originally published in
Demonstratio Mathematica XVIII (1985), 377–394

Systems of exponential congruences

Dedicated to the memory
of Professor Roman Sikorski

Some years ago I proved the following theorem ([1], Theorem 2). Let K be an algebraic number field, $\alpha_1, \dots, \alpha_k, \beta$ non-zero elements of K. If for almost all prime ideals $\mathfrak{p}$ of K the congruence

$$\prod_{j=1}^{k} \alpha_j^{x_j} \equiv \beta \pmod{\mathfrak{p}}$$

is soluble in integers x_j then the equation

$$\prod_{j=1}^{k} \alpha_j^{x_j} = \beta$$

is soluble in integers. I have shown by an example that this theorem does not extend to systems of congruences of the form

$$\prod_{j=1}^{k} \alpha_{ij}^{x_j} \equiv \beta_i \pmod{\mathfrak{p}} \quad (i = 1, 2, \dots, h) \tag{1}$$

even for $h = 2$, $k = 3$.

Recently L. Somer [4] has considered systems of the form (1) for $k = 1$. The study of his work has suggested to me that the connection between the local and the global solubility of (1) may hold if for some $i \leqslant h$ the numbers α_{ij} are multiplicatively independent. The aim of this paper is to prove this assertion in the form of the following theorem.

Theorem 1. *Let K be an algebraic number field, α_{ij}, β_i $(i = 1, 2, \dots, h;\ j = 1, 2, \dots, k)$ non-zero elements of K and assume that for some $i \leqslant h$*

$$\prod_{j=1}^{k} \alpha_{ij}^{x_j} = 1,\ x_j \in \mathbb{Z} \quad \textit{implies} \quad x_j = 0 \textit{ for all } j \leqslant k.$$

If for almost all prime ideals $\mathfrak{p}$ of K in the sense of the Dirichlet density the system (1) *is*

soluble in integers x_j then the system of equations

$$\prod_{j=1}^{k} \alpha_{ij}^{x_j} = \beta_i \quad (i = 1, 2, \ldots, h) \tag{2}$$

is soluble in integers.

The following corollary is almost immediate.

Corollary. *If the system of congruences*

$$\alpha_i^x \equiv \beta_i \pmod{\mathfrak{p}} \quad (i = 1, 2, \ldots, h)$$

is soluble in integers x for almost all prime ideals $\mathfrak{p}$ of K then the system of equations

$$\alpha_i^x = \beta_i \quad (i = 1, 2, \ldots, h)$$

is soluble in integers.

Somer [4] has proved the above corollary under the assumption that either none of the α_i's is a root of unity or all the α_i's are roots of unity.

The next theorem shows that Theorem 1 cannot be extended further.

Theorem 2. *For every $k \geqslant 2$ there exist non-zero rational integers α_{ij}, β_i $(i = 1, 2; j = 1, 2, \ldots, k)$ such that $\alpha_{12}, \ldots, \alpha_{1k}$ are multiplicatively independent, the system* (1) *with $h = 2$ is soluble for all rational primes $\mathfrak{p}$, but the system* (2) *is insoluble in integers.*

In the sequel ζ_q denotes a primitive q-th root of unity.

For a rational matrix M den M denotes the least common denominator of the elements of M and M^T the transpose of M.

The proofs are based on eight lemmata.

Lemma 1. *For every rational square matrix A there exists a non-singular matrix U whose elements are integers in the splitting field of the characteristic polynomial of A such that*

$$U^{-1}AU = \begin{bmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_n \end{bmatrix} \tag{3}$$

with A_ν a square matrix of degree ϱ_ν:

$$A_\nu = \begin{bmatrix} \lambda_\nu & 1 & & \\ & \lambda_\nu & 1 & \\ & & \ddots & \ddots \\ & & & \lambda_\nu & 1 \\ & & & & \lambda_\nu \end{bmatrix} \quad (\nu = 1, 2, \ldots, n) \tag{4}$$

where the empty places (not the dots) are zeros.

Proof (see [5], §88). The elements of U can be made algebraic integers, since the left hand side of (3) is invariant with respect to the multiplication of U by a number. □

Lemma 2. *Let $L_0, L_j, M_j \in \mathbb{Z}[t_1, \dots, t_r]$ $(j = 1, 2, \dots, k)$ be homogeneous linear forms and M_j $(j = 1, 2, \dots, k)$ linearly independent. If the system of congruences*

$$\begin{aligned} &\sum_{j=1}^{k} x_j L_j(t_1, \dots, t_r) \equiv L_0(t_1, \dots, t_r) \pmod m \\ &\sum_{j=1}^{k} x_j M_j(t_1, \dots, t_r) \equiv 0 \pmod m \end{aligned} \tag{5}$$

is soluble in x_j for all moduli m and all integer vectors $[t_1, \dots, t_r]$, then $L_0 = 0$.

Proof. Let $L_j = \sum_{s=1}^{r} l_{js} t_s$ $(0 \leqslant j \leqslant k)$, $M_j = \sum_{s=1}^{r} m_{js} t_s$ $(1 \leqslant j \leqslant k)$. Taking if necessary $l_{js} = m_{js} = 0$ for $s > k$ we can assume that $r > k$. Since M_j's are linearly independent we can assume also that the matrix

$$M = [m_{js}]_{j,s \leqslant k}$$

is non-singular. Put

$$M^* = [m_{js}]_{\substack{j \leqslant k \\ k < s \leqslant r}},$$

$$L = [l_{js}]_{1 \leqslant j,s \leqslant k}, \quad L^* = [l_{js}]_{\substack{1 \leqslant j \leqslant k \\ k < s \leqslant r}},$$

$$\boldsymbol{l}_0 = [l_{01}, \dots, l_{0k}], \quad \boldsymbol{l}_0^* = [l_{0,k+1}, \dots, l_{0r}].$$

Let K_0 be the splitting field of the characteristic polynomial of LM^{-1}. In virtue of Lemma 1 there exists a matrix U whose elements are integers of K_0 such that

$$U^{-1} L M^{-1} U = \begin{bmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_n \end{bmatrix} \tag{6}$$

where A_ν of order ϱ_ν is given by (4) $(\nu = 1, 2, \dots, n)$.

We proceed to show that $\boldsymbol{l}_0 = \boldsymbol{0}$ and $\boldsymbol{l}_0^* = \boldsymbol{0}$. Let us write

$$\boldsymbol{l}_0 M^{-1} U = [l_1, \dots, l_k]. \tag{7}$$

Suppose that $\boldsymbol{l}_0 \neq 0$ hence $\boldsymbol{l}_0 M^{-1} U \neq 0$ and let the least $\kappa \leqslant k$ for which $l_\kappa \neq 0$ satisfy

$$\sigma_\nu = \sum_{\mu < \nu} \varrho_\mu < \kappa \leqslant \sum_{\mu \leqslant \nu} \varrho_\mu. \tag{8}$$

Let p be a prime which factorizes in K_0 into distinct prime ideals of degree one which divide neither den M^{-1} nor the numerator of l_κ nor the denominator of λ_ν.

Take the modulus $m = p^{\varrho_\nu}$ and let $\boldsymbol{t} := [t_1, \ldots, t_k]^T \in \mathbb{Z}^k$ satisfy the congruence

$$U^{-1}M\boldsymbol{t} \equiv \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ p \\ \vdots \\ p^{\varrho_\nu - 1} \\ 0 \\ \vdots \\ 0 \end{bmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix} \left.\begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix}\right\} \sigma_\nu \pmod{\mathfrak{p}^{\varrho_\nu}}, \tag{9}$$

where $\mathfrak{p}$ is a prime ideal factor of p in K_0. Since $\mathfrak{p}$ is unramified of degree one and does not divide den M^{-1} the congruence is soluble for rational integers. Take further

$$\boldsymbol{t}^* := [t_{k+1}, \ldots, t_r]^T = \boldsymbol{0}. \tag{10}$$

Setting $\boldsymbol{y} = [y_1, \ldots, y_k] = [x_1, \ldots, x_k]U$ we can rewrite the system (5) in the form

$$\boldsymbol{y}(U^{-1}LM^{-1}U)(U^{-1}M\boldsymbol{t}) \equiv \boldsymbol{l}_0 M^{-1}U(U^{-1}M\boldsymbol{t}) \pmod{p^{\varrho_\nu}}$$
$$\boldsymbol{y}(U^{-1}M\boldsymbol{t}) \equiv 0 \pmod{p^{\varrho_\nu}},$$

hence by (6)–(10)

$$\sum_{j=\sigma_\nu+1}^{\sigma_{\nu+1}} y_j\left(\lambda_\nu p^{j-\sigma_\nu-1} + p^{j-\sigma_\nu}\right) + y_{\sigma_{\nu+1}}\lambda_\nu p^{\varrho_\nu - 1} \equiv \sum_{j=\sigma_\nu+1}^{\sigma_{\nu+1}} l_j p^{j-\sigma_\nu-1} \pmod{\mathfrak{p}^{\varrho_\nu}}, \tag{11_1}$$

$$\sum_{j=\sigma_\nu+1}^{\sigma_{\nu+1}} y_j p^{j-\sigma_\nu-1} \equiv 0 \pmod{\mathfrak{p}^{\varrho_\nu}}. \tag{11_2}$$

The left hand side of (11_1) is congruent mod $\mathfrak{p}^{\varrho_\nu}$ to the left hand side of (11_2) multiplied by $(\lambda_\nu + p)$. Since $\lambda_\nu^{-1} \not\equiv 0 \pmod{\mathfrak{p}}$ it follows that

$$\sum_{j=\sigma_\nu+1}^{\sigma_{\nu+1}} l_j p^{j-\sigma_\nu-1} \equiv 0 \pmod{\mathfrak{p}^{\varrho_\nu}},$$

hence $l_\kappa \equiv 0 \pmod{\mathfrak{p}}$ contrary to the choice of $\mathfrak{p}$.

Therefore $\boldsymbol{l}_0 = \boldsymbol{0}$ and it remains to prove that $\boldsymbol{l}_0^* = \boldsymbol{0}$. Assume without loss of generality that

$$l_{0r} \neq 0.$$

Choose a rational integer $\lambda \neq \lambda_\nu$ $(\nu = 1, 2, \ldots, n)$ and take

$$m = 2|l_{0r}| \operatorname{den}(L - \lambda M)^{-1} > 0, \tag{12}$$
$$\boldsymbol{t}^* = [0, \ldots, 0, \operatorname{den}(L - \lambda M)^{-1}]^T.$$

With this choice of $\boldsymbol{t}^*$ we can find a $\boldsymbol{t} \in \mathbb{Z}^k$ such that

$$(L - \lambda M)\boldsymbol{t} = \lambda M^* \boldsymbol{t}^* - L^* \boldsymbol{t}^*$$

and then the system (5) gives for $\boldsymbol{x} = [x_1, \ldots, x_k]$

$$\boldsymbol{x}\lambda(M\boldsymbol{t} + M^*\boldsymbol{t}^*) \equiv l_{0r} \operatorname{den}(L - \lambda M)^{-1} \pmod m,$$
$$\boldsymbol{x}(M\boldsymbol{t} + M^*\boldsymbol{t}^*) \equiv 0 \pmod m,$$

hence $l_{0r} \operatorname{den}(L - \lambda M)^{-1} \equiv 0 \pmod m$.

The obtained contradiction with (12) completes the proof. □

Lemma 3. *For every rational square matrix A there exists a non-singular matrix U such that* (3) *holds with A_ν a square matrix of order ϱ_ν (in general not the same as in Lemma* 2*),*

$$A_\nu = \begin{bmatrix} -\alpha_{\nu 1} & 1 & & \\ -\alpha_{\nu 2} & & 1 & \\ \vdots & & & \ddots \\ -\alpha_{\nu,\varrho_\nu - 1} & & & 1 \\ -\alpha_{\nu\varrho_\nu} & & & \end{bmatrix} \tag{13}$$

where $\alpha_{\nu j} \in \mathbb{Q}$ and $x^{\varrho_\nu} + \sum_{j=1}^{\varrho_\nu} \alpha_{\nu j} x^{\varrho_\nu - j}$ is a power of a polynomial irreducible over $\mathbb{Q}$.

Proof (see [5], §88). The form of the matrix A has been changed by applying central symmetry (matrices symmetric to each other with respect to the common centre are similar). U can be made integral via multiplication by a suitable integer. □

Lemma 4. *Let $L_0, L_j, M_j \in \mathbb{Z}[t_1, \ldots, t_r]$ $(j = 1, 2, \ldots, k)$ be homogeneous linear forms, M_j's linearly independent. Let $a_0, a_j, b_j \in \mathbb{Z}$ $(j = 1, 2, \ldots, k)$ and w be a fixed positive integer.*

If for all moduli $m \equiv 0 \pmod w$ and for all integer vectors $[t_1, \ldots, t_r]$ the system of congruences

$$\sum_{j=1}^{k} x_j \left(L_j(t_1, \ldots, t_r) + a_j \frac{m}{w} \right) \equiv L_0(t_1, \ldots, t_r) + a_0 \frac{m}{w} \pmod m,$$
$$\sum_{j=1}^{k} x_j \left(M_j(t_1, \ldots, t_r) + b_j \frac{m}{w} \right) \equiv 0 \pmod m \tag{14}$$

is soluble in integers x_j then $L_0 = 0$ and $a_0 \equiv 0 \pmod w$.

Proof. When m runs through all positive integers divisible by w, m/w runs through all positive integers, hence applying Lemma 2 we infer that $L_0 = 0$. In order to show $a_0 \equiv 0 \pmod{w}$ we adopt the meaning of L, L^*, M, M^* from the proof of Lemma 2.

In virtue of Lemma 3 there exists a non-singular integral matrix U such that

$$U^{-1}LM^{-1}U = \begin{bmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_n \end{bmatrix}, \tag{15}$$

where A_ν of order ϱ_ν is given by (13). We can assume without loss of generality that $\alpha_{\nu\varrho_\nu} = 0$, $\varrho_1 \geqslant \varrho_\nu$ for $\nu \leqslant n_0$ and $\alpha_{\nu\varrho_\nu} \neq 0$ for $\nu > n_0$ (n_0 may be 0). It follows from the condition on $x^{\varrho_\nu} + \sum_{j=1}^{\varrho_\nu} \alpha_{\nu j} x^{\varrho_\nu - j}$ that

$$A_\nu = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix} \quad (1 \leqslant \nu \leqslant n_0), \tag{16}$$

where the empty places are zeros as before. Now put

$$U^{-1}\begin{bmatrix} a_1 \\ \vdots \\ a_k \end{bmatrix} = \operatorname{con}(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n), \quad U^{-1}\begin{bmatrix} b_1 \\ \vdots \\ b_k \end{bmatrix} = \operatorname{con}(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n), \tag{17}$$

where con denotes concatenation and for $\nu = 1, 2, \ldots, n$

$$\boldsymbol{a}_\nu = \begin{bmatrix} a_{\nu 1} \\ \vdots \\ a_{\nu\varrho_\nu} \end{bmatrix}, \quad \boldsymbol{b}_\nu = \begin{bmatrix} b_{\nu 1} \\ \vdots \\ b_{\nu\varrho_\nu} \end{bmatrix}. \tag{18}$$

Take

$$m_0 = w \operatorname{den} M^{-1} \operatorname{den} U^{-1} \operatorname*{l.c.m.}_{n_0 < \nu \leqslant n} \operatorname{den} A_\nu^{-1} \tag{19}$$

and put

$$m = m_0^{\varrho_1 + 1}, \tag{20}$$

$$\boldsymbol{t} = \begin{bmatrix} t_1 \\ \vdots \\ t_k \end{bmatrix} = M^{-1}U \begin{bmatrix} \boldsymbol{u}_1 \\ \vdots \\ \boldsymbol{u}_n \end{bmatrix}, \quad \boldsymbol{t}^* = \begin{bmatrix} t_{k+1} \\ \vdots \\ t_r \end{bmatrix} = \boldsymbol{0}, \tag{21}$$

where

$$\boldsymbol{u}_\nu = A^{-1}\boldsymbol{a}_\nu \frac{m_0^{\varrho_1+1}}{w} \quad (n_0 < \nu \leqslant n) \tag{22}$$

c and, for $\nu \leqslant n_0$, $\boldsymbol{u}_\nu$ is a vector with ϱ_ν components and the j-th component

$$u_{\nu j} = \frac{1}{w} \sum_{i=j}^{\varrho_\nu} m_0^{\varrho_1 - i + j} (a_{\nu i} - m_0 b_{\nu i}) \quad (1 \leqslant j \leqslant \varrho_\nu).$$

Since by (19) $\boldsymbol{u}_\nu \equiv \boldsymbol{0} \pmod{\text{den } M^{-1}}$ $(1 \leqslant \nu \leqslant n)$ the vector $\boldsymbol{t}$ defined by (21) is integral. Moreover by (16), (18) and the above we have

c (23) $$A_\nu \boldsymbol{u}_\nu + \boldsymbol{a}_\nu \frac{m_0^{\varrho_1+1}}{w} = m_0 \left(\boldsymbol{u}_\nu + \boldsymbol{b}_\nu \frac{m_0^{\varrho_1+1}}{w} \right) \quad (1 \leqslant \nu \leqslant n_0).$$

Setting

$$[x_1, \ldots, x_k]U = [\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n],$$

where $\boldsymbol{x}_\nu$ is a vector with ϱ_ν components, and using (15), (17), (20) and (21) we can rewrite the system (14) in the form

$$\sum_{\nu=1}^{n} \boldsymbol{x}_\nu \left(A_\nu \boldsymbol{u}_\nu + \boldsymbol{a}_\nu \frac{m_0^{\varrho_1+1}}{w} \right) \equiv a_0 \frac{m_0^{\varrho_1+1}}{w} \pmod{m_0^{\varrho_1+1}},$$

$$\sum_{\nu=1}^{n} \boldsymbol{x}_\nu \left(\boldsymbol{u}_\nu + \boldsymbol{b}_\nu \frac{m_0^{\varrho_1+1}}{w} \right) \equiv 0 \pmod{m_0^{\varrho_1+1}}.$$

In virtue of (22) this gives

(24_1) $$\sum_{\nu=1}^{n_0} \boldsymbol{x}_\nu \left(A_\nu \boldsymbol{u}_\nu + \boldsymbol{a}_\nu \frac{m_0^{\varrho_1+1}}{w} \right) \equiv a_0 \frac{m_0^{\varrho_1+1}}{w} \pmod{m_0^{\varrho_1+1}},$$

(24_2) $$\sum_{\nu=1}^{n_0} \boldsymbol{x}_\nu \left(\boldsymbol{u}_\nu + \boldsymbol{b}_\nu \frac{m_0^{\varrho_1+1}}{w} \right) \equiv \sum_{\nu=n_0+1}^{n} \boldsymbol{x}_\nu \left(A_\nu^{-1} \boldsymbol{a}_\nu - \boldsymbol{b}_\nu \right) \frac{m_0^{\varrho_1+1}}{w} \pmod{m_0^{\varrho_1+1}}.$$

In virtue of (23) the left hand side of (24_1) equals the left hand side of (24_2) multiplied by m_0. Hence

$$a_0 \frac{m_0^{\varrho_1+1}}{w} = m_0^{\varrho_1+1} \sum_{\nu=n_0+1}^{n} \boldsymbol{x}_\nu \left(A_\nu^{-1} \boldsymbol{a}_\nu - \boldsymbol{b}_\nu \right) \frac{m_0}{w} \pmod{m_0^{\varrho_1+1}}.$$

Since by (19) the vectors $\left(A_\nu^{-1} \boldsymbol{a}_\nu - \boldsymbol{b}_\nu \right) \frac{m_0}{w}$ are integral we get

$$a_0 \frac{m_0^{\varrho_1+1}}{w} \equiv 0 \pmod{m_0^{\varrho_1+1}}, \quad a_0 \equiv 0 \pmod{w},$$

which completes the proof. □

Lemma 5. *For every integral matrix A with all the k rows linearly independent there exist unimodular integral matrices B and C such that*

$$B^{-1}AC = \begin{bmatrix} e_1 & & & \\ & e_2 & & \\ & & \ddots & \\ & & & e_k \end{bmatrix}, \tag{25}$$

where the elements outside the principal diagonal are zeros, $e_k \neq 0$ and $e_i \mid e_{i+1}$ $(1 \leqslant i < k)$.

Proof. Without the condition $e_k \neq 0$ the lemma is proved in [5], §85. The condition $e_k \neq 0$ follows from the linear independence of the rows of A. □

Lemma 6. *Let $L_{ij} \in \mathbb{Z}[t_1, \ldots, t_r]$ $(1 \leqslant i \leqslant h,\ 0 \leqslant j \leqslant k)$ be homogeneous linear forms and suppose L_{1j} $(1 \leqslant j \leqslant k)$ linearly independent. Let $l_{ij} \in \mathbb{Z}$ $(1 \leqslant i \leqslant h,\ 0 \leqslant j \leqslant k)$. If the system of congruences*

$$\sum_{j=1}^{k} x_j \Big(L_{ij}(t_1, \ldots, t_r) + l_{ij} \frac{m}{w} \Big) \equiv L_{i0}(t_1, \ldots, t_r) + l_{i0} \frac{m}{w} \pmod{m} \quad (1 \leqslant i \leqslant h) \tag{26}$$

is soluble for all moduli $m \equiv 0 \pmod{w}$ and for all integer vectors $[t_1, \ldots, t_r]$ then there exist integers ξ_j $(1 \leqslant j \leqslant k)$ such that

$$\sum_{j=1}^{k} \xi_j L_{ij} = L_{i0} \quad (1 \leqslant i \leqslant h) \tag{27}$$

and

$$\sum_{j=1}^{k} \xi_j l_{ij} \equiv l_{i0} \pmod{w}. \tag{28}$$

Proof. Let

$$L_{1j} = \sum_{s=1}^{r} a_{js} t_s \quad (0 \leqslant j \leqslant k), \qquad A = [a_{js}]_{\substack{1 \leqslant j \leqslant k \\ 1 \leqslant s \leqslant r}}. \tag{29}$$

In virtue of Lemma 5 there exist unimodular integral matrices B, C such that (25) holds. Let

$$B^{-1} \begin{bmatrix} l_{11} \\ \vdots \\ l_{1k} \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_k \end{bmatrix}, \quad C^{-1} \begin{bmatrix} t_1 \\ \vdots \\ t_r \end{bmatrix} = \begin{bmatrix} t'_1 \\ \vdots \\ t'_r \end{bmatrix}, \tag{30}$$

$$[a_{01}, \ldots, a_{0r}]C = [c_1, \ldots, c_r].$$

Setting $[y_1, \dots, y_k] = [x_1, \dots, x_k]B$ we get from (25), (26) and (30)

$$\sum_{j=1}^{k} y_j \Big(e_j t'_j + b_j \frac{m}{w} \Big) \equiv \sum_{s=1}^{r} c_s t'_s + l_{10} \frac{m}{w} \pmod m. \tag{31}$$

Assume that c_s are not all zero for $s > k$ and that σ is the least index $> k$ such that $c_\sigma \neq 0$ we take $m = 2we_k|c_\sigma|$,

$$t'_s = \begin{cases} -\dfrac{b_s}{e_s}\dfrac{m}{w} & \text{for } s \leqslant k, \\ 1 & \text{for } s = \sigma, \\ 0 & \text{for } s > k,\ s \neq \sigma \end{cases}$$

and get from (31)

$$c_\sigma \equiv 0 \pmod{2|c_\sigma|},$$

a contradiction. Therefore $c_s = 0$ for all $s > k$ and taking $m = 2we_k$, $t'_j = -\dfrac{b_j}{e_j}\dfrac{m}{w}$ for $j \leqslant k$ we get from (31)

$$l_{10} \frac{m}{w} - \sum_{j=1}^{k} \frac{b_j c_j}{e_j} \frac{m}{w} \equiv 0 \pmod m,$$

hence

$$l_{10} \equiv \sum_{j=1}^{k} \frac{b_j c_j}{e_j} \pmod{w^+}. \tag{32}$$

Finally taking $m = we_k$ and for a fixed $j \leqslant k$

$$t'_s = \begin{cases} -\dfrac{m}{w}\dfrac{b_s}{e_s} + \dfrac{e_k}{e_j} & \text{if } s = j, \\ -\dfrac{m}{w}\dfrac{b_s}{e_s} & \text{if } s \neq j,\ s \leqslant k \\ 0 & \text{if } s > k, \end{cases}$$

we get from (31) and (32)

$$y_j e_k \equiv c_j e_k / e_j \pmod{e_k}, \quad c_j/e_j \in \mathbb{Z}.$$

Integers ξ_j defined by

$$[\xi_1, \dots, \xi_k] = [c_1/e_1, \dots, c_k/e_k]B^{-1}$$

satisfy (27) and (28) for $i = 1$ in virtue of (25), (29), (30) and (32). Take now $i \geqslant 1$ and consider the system of two congruences:

$$\sum_{j=1}^{k} x_j \Big(L_{ij}(t_1, \dots, t_r) + l_{ij} \frac{m}{w} \Big) \equiv L_{i0}(t_1, \dots, t_r) + l_{i0} \frac{m}{w} - \sum_{j=1}^{k} \xi_j \Big(L_{ij}(t_1, \dots, t_r) + l_{ij} \frac{m}{w} \Big) \pmod m$$

and

$$\sum_{j=1}^{k} x_j \Big(L_{1j}(t_1, \ldots, t_r) + l_{1j} \frac{m}{w} \Big) \equiv 0 \pmod{m}.$$

If $[x_1^0, \ldots, x_m^0]$ is a solution of the system (26), the above system has the solution $[x_1^0 - \xi_1, \ldots, x_m^0 - \xi_m]$, hence it is soluble for all moduli m and all integer vectors $[t_1, \ldots, t_r]$. Since L_{1j} are linearly independent we have in virtue of Lemma 4

$$L_{i0} - \sum_{j=1}^{k} \xi_j L_{ij} = 0 \quad \text{and} \quad l_{i0} - \sum_{j=1}^{k} \xi_j l_{ij} \equiv 0 \pmod{w},$$

thus (27) and (28) hold for all $i \leqslant h$. □

Lemma 7. *In any algebraic number field K there exists a multiplicative basis, i.e., such a sequence $\pi_1, \pi_2, \ldots$ that any non-zero element of K is represented uniquely as $\zeta \prod_{s=1}^{r} \pi_s^{x_s}$, where x_s are rational integers and ζ is a root of unity.*

Proof. See [3]. □

Lemma 8. *Let K be an algebraic number field, w the number of roots of unity contained in K, $w \equiv 0 \pmod 4$, n a positive integer,*

$$\sigma = \big(w, n, \underset{q \mid n,\ q \text{ prime}}{\text{l.c.m.}} [K(\zeta_q) : K]\big).$$

If

$$n \equiv 0 \Big(\text{mod } (w, n) \underset{q \mid n,\ q \text{ prime}}{\text{l.c.m.}} [K(\zeta_q) : K]\Big) \tag{33}$$

and $\alpha_1, \ldots, \alpha_r \in K$ have the property that

$$\zeta_w^{x_0} \prod_{s=1}^{r} \alpha_s^{x_s} = \gamma^{n/\sigma},\ \gamma \in K \quad \textit{implies} \quad x_1 \equiv x_2 \equiv \ldots \equiv x_r \equiv 0 \pmod{n/\sigma} \tag{34}$$

then for any integers $c_1, \ldots, c_r \equiv 0 \pmod \sigma$ and any c_0 there exists a set of prime ideals $\mathfrak{q}$ of $K(\zeta_n)$ of a positive Dirichlet density such that

$$\Big(\frac{\zeta_w}{\mathfrak{q}}\Big)_n = \zeta_{(w,n)}^{c_0}, \quad \Big(\frac{\alpha_s}{\mathfrak{q}}\Big)_n = \zeta_n^{c_s} \quad (1 \leqslant s \leqslant r). \tag{35}$$

Proof. This is a special case ($\zeta_4 \in K$) of Theorem 4 of [2]. In this theorem only the existence of infinitely many prime ideals $\mathfrak{q}$ with property (35) is asserted, but the existence of a set of a positive Dirichlet density is immediately clear from the proof based on the Chebotarev density theorem. □

Proof of Theorem 1. Without loss of generality we may assume that $\zeta_4 \in K$ and that α_{1j} $(j = 1, 2, \ldots, k)$ are multiplicatively independent. Let us set

$$\alpha_{ij} = \zeta_w^{a_{ij0}} \prod_{s=1}^{r} \pi_s^{a_{ijs}}, \quad \beta_i = \zeta_w^{b_{i0}} \prod_{s=1}^{r} \pi_s^{b_{is}}, \tag{36}$$

where w is the number of roots of unity contained in K and π_s are elements of the multiplicative basis described in Lemma 7. Take an arbitrary modulus $m \equiv 0 \pmod{w}$ and set in Lemma 8 $n = mm_1$, where $m_1 = \underset{p \leqslant P,\ p \text{ prime}}{\text{l.c.m.}} (p-1)$ and P is the greatest prime factor of m. Since every prime factor q of n satisfies $q \leqslant P$ the number n satisfies (33). The condition (34) is clearly satisfied by $\alpha_s = \pi_s$ $(1 \leqslant s \leqslant r)$. Hence for any integers $c_1, \ldots, c_r \equiv 0 \pmod{w}$ there exists a set S of prime ideals $\mathfrak{q}$ of $K(\zeta_n)$ of positive Dirichlet density such that

$$\left(\frac{\zeta_w}{\mathfrak{q}}\right)_n = \zeta_w, \quad \left(\frac{\pi_s}{\mathfrak{q}}\right)_n = \zeta_n^{c_s} \quad (1 \leqslant s \leqslant r). \tag{37}$$

The ideals $\mathfrak{p}$ of K divisible by at least one $\mathfrak{q} \in S$ form a set of positive Dirichlet density, hence by the assumption there exist integers x_j satisfying

$$\prod_{j=1}^{k} \alpha_{ij}^{x_j} \equiv \beta_i \pmod{\mathfrak{q}} \quad (i = 1, 2, \ldots, h)$$

for at least one $\mathfrak{q} \in S$. It follows from (36) and (37) that

$$\sum_{j=1}^{k} x_j \left(\sum_{s=1}^{r} a_{ijs} c_s + a_{ij0} \frac{n}{w} \right) \equiv \sum_{s=1}^{r} b_{is} c_s + b_{i0} \frac{n}{w} \pmod{n} \quad (1 \leqslant i \leqslant h).$$

Now take $c_s = wm_1 t_s$ $(1 \leqslant s \leqslant r)$,

$$\begin{cases} L_{ij} = w \sum_{s=1}^{r} a_{ijs} t_s & (1 \leqslant i \leqslant h,\ 1 \leqslant j \leqslant k), \\ L_{i0} = w \sum_{s=1}^{r} b_{is} t_s & (1 \leqslant i \leqslant h). \end{cases} \tag{38}$$

It follows that for all moduli $m \equiv 0 \pmod{w}$ and all integer vectors $[t_1, \ldots, t_r]$ the system of congruences

$$\sum_{j=1}^{k} x_j L_{ij}(t_1, \ldots, t_r) + a_{ij0} \frac{m}{w} \equiv L_{i0}(t_1, \ldots, t_r) + b_{i0} \frac{m}{w} \pmod{m}$$

is soluble in integers x_j. Since the numbers α_{1j} are multiplicatively independent the linear forms L_{1j} are linearly independent $(1 \leqslant j \leqslant k)$. Hence by Lemma 6 there exist integers $\xi_1, \ldots, \xi_k$ such that

$$\sum_{j=1}^{k} \xi_j L_{ij} = L_{i0} \quad \text{and} \quad \sum_{j=1}^{k} \xi_j a_{ij0} \equiv b_{i0} \pmod{w} \quad (1 \leqslant i \leqslant h).$$

It follows from (36) and (38) that $\xi_1, \ldots, \xi_k$ satisfy the system (2). □

Proof of Corollary. In view of Theorem 1 it remains to consider the case when for each $i \leqslant h$ the number α_i is a root of unity. But then either there exists a positive integer $x \leqslant w$ such that

$$\alpha_i^x = \beta_i \quad (1 \leqslant i \leqslant h)$$

or the system of congruences

$$\alpha_i^x \equiv \beta_i \pmod{\mathfrak{p}} \quad (1 \leqslant i \leqslant h)$$

is soluble only for prime ideals $\mathfrak{p}$ dividing

$$\prod_{x=1}^{w} \text{g.c.d.}_{1 \leqslant i \leqslant h} (\alpha_i^x - \beta_i). \qquad \square$$

Proof of Theorem 2. Since here $K = \mathbb{Q}$ we write p instead of $\mathfrak{p}$ and denote by p_j the j-th prime. We take

$$\alpha_{11} = -1, \quad \alpha_{1j} = p_{j-1} \ (2 \leqslant j \leqslant k), \quad \beta_1 = -1,$$

$$\alpha_{21} = 2, \quad \alpha_{2j} = 1 \ (2 \leqslant j \leqslant k), \quad \beta_2 = 1.$$

For $p = 2$ (1) has the solution $x_j = 0$ $(1 \leqslant j \leqslant k)$. For $p > 2$ we consider the index of 2, $\operatorname{ind} 2$ with respect to a fixed primitive root of p. If $\dfrac{p-1}{(\operatorname{ind} 2,\ p-1)}$ is odd, (1) has a solution determined by

$$x_1 \equiv \begin{cases} 1 \pmod 2 \\ 0 \left(\mod \dfrac{p-1}{(\operatorname{ind} 2,\ p-1)}\right), \end{cases} \qquad x_j = 0 \quad (2 \leqslant j \leqslant k).$$

If $\dfrac{p-1}{(\operatorname{ind} 2,\ p-1)}$ is even, (1) has a solution determined by

$$x_1 = 0, \quad x_2 \operatorname{ind} 2 \equiv \frac{p-1}{2} \pmod{p-1}, \quad x_j = 0 \ (3 \leqslant j \leqslant k).$$

On the other hand, (2) is clearly insoluble. $\square$

References

[1] A. Schinzel, *On power residues and exponential congruences*. Acta Arith. 27 (1975), 397–420; this collection: H4, 915–938.

[2] —, *Abelian binomials, power residues and exponential congruences*. Acta Arith. 32 (1977), 245–274; *Addendum*, ibid. 36 (1980), 101–104; this collection: H5, 939–970.

[3] Th. Skolem, *On the existence of a multiplicative basis for an arbitrary algebraic field*. Norske Vid. Selsk. Forh. (Trondheim) 20 (1947), no. 2, 4–7.

[4] L. Somer, *Linear recurrences having almost all primes as maximal divisors*. In: Fibonacci Numbers and their Applications (Patras, 1984), Math. Appl. 28, Reidel, Dordrecht 1986, 257–272.

[5] B. L. van der Waerden, *Algebra* II Teil. Springer, Berlin 1967.

Originally published in
Mathematical Proceedings of the Cambridge Philosophical Society
112 (1992), 225–232

On a problem in elementary number theory

with J. Wójcik (*Warsaw*)

Let $\operatorname{ord}_q(a)$ be the exponent with which a prime q occurs in the factorization of a rational number $a \neq 0$ and, if $\operatorname{ord}_q(a) = 0$, let $M_q(a)$ be the multiplicative group generated by a modulo q. In the course of a group-theoretical investigation J. S. Wilson found he needed some results about integers a, b such that $M_q(a) = M_q(b)$, indeed also for algebraic integers, and he proved some of what he needed. J. W. S. Cassels observed that Wilson's argument naturally proved the existence of infinitely many primes q with $M_q(a) = M_q(b)$ for rational integers a, b with $ab > 0$, $|a| > 1$, $|b| > 1$. J. G. Thompson found a proof for the case of integers a, b with $ab < 0$, $|a| > 1$, $|b| > 1$. He also posed the problem for rational $a,\ b$ (all this is unpublished). The aim of this paper is to prove that the answer to Thompson's question is affirmative. We also include the case $ab > 0$ settled by Thompson himself. We use the same technique devised by Wilson which has been elaborated by Cassels and Thompson. We thank Professor Cassels for the simplification of our original exposition and the referee for his suggestions.

Theorem. *For all* $a,\ b \in \mathbb{Q} \setminus \{0, 1, -1\}$ *there exist infinitely many primes* q *such that* $M_q(a) = M_q(b)$.

Without loss of generality $a \neq b$. The strategy is first to find one prime q with

$$\operatorname{ord}_q a = \operatorname{ord}_q b = \operatorname{ord}_q(a - b) \quad \text{and} \quad M_q(a) = M_q(b).$$

This requires a fairly elaborate subdivision into cases. At the end, a uniform argument deduces the existence of infinitely many such q.

It is convenient to enunciate one key idea in the following trivial

Proposition. *Let* q *be a prime. Suppose that* $\operatorname{ord}_q a = \operatorname{ord}_q b = 0$ *and that*

$$a^n \equiv b \bmod q$$

where n *is prime to* $q - 1$. *Then* $M_q(a) = M_q(b)$.

In the argument, we shall most often take n to be prime. Given $a,\ b$ we consider primes l in an appropriate arithmetic progression. A study of the factorization of $a^l - b$ then shows that it must be divisible by some prime $q \not\equiv 1 \bmod l$.

Notation. For all primes p put

$$\alpha_p = \operatorname{ord}_p a, \quad \beta_p = \operatorname{ord}_p b, \quad \gamma_p = \operatorname{ord}_p(a-b)$$

and further put

$$P = \prod_{\alpha_p=\beta_p=0} p^{\gamma_p}, \qquad P_1 = \prod_{p \mid P}(p-1).$$

Lemma 1. *If either $ab > 0$, $|a| \neq 1$, $|b| \neq 1$ or for some prime p_0 we have $\alpha_{p_0}\beta_{p_0} > 0$ and $\alpha_{p_0}, \beta_{p_0}, \gamma_{p_0}$ not all equal, then there exists a prime q such that $\alpha_q = \beta_q = \gamma_q = 0$ and $M_q(a) = M_q(b)$.*

Proof. Replacing if necessary a by a^{-1} and b by b^{-1}, we may assume without loss of generality

$$1 < |a| < |b| \quad \text{if } ab > 0, \tag{1}$$

$$0 < \alpha_{p_0} \leqslant \beta_{p_0} \quad \text{if } ab < 0. \tag{2}$$

Let l be a sufficiently large prime such that

$$l \equiv 1 \bmod p^{\gamma_p}(p-1) \quad \text{for all} \quad p \mid P.$$

Then

$$a^l \equiv a \bmod p^{\gamma_p+1},$$

so that

$$\operatorname{ord}_p(a^l - b) = \gamma_p \quad \text{for all} \quad p \mid P.$$

On the other hand for all primes p with $\alpha_p\beta_p > 0$ we have since l is large

$$\operatorname{ord}_p(a^l - b) = \begin{cases} l\alpha_p & \text{if } \alpha_p < 0, \\ \beta_p & \text{if } \alpha_p > 0 \end{cases} \tag{3}$$

and for all primes p with $\alpha_p\beta_p \leqslant 0$ the same is true in an obvious way. Finally if $\alpha_p = 0$, $\beta_p \neq 0$ we have

$$\operatorname{ord}_p(a^l - b) = \min\{0, \beta_p\}. \tag{4}$$

Hence

$$a^l - b = \operatorname{sgn} a \cdot P \prod_{\alpha_p<0} p^{l\alpha_p} \prod_{\substack{\alpha_p=0 \\ \beta_p\neq 0}} p^{\min\{0,\beta_p\}} \prod_{\alpha_p>0} p^{\beta_p} s,$$

where s is an integer prime to the numerators and the denominators of $a, b, a-b$ and positive by (1). We have

$$a^l - b \equiv a - b \bmod l, \qquad \prod_{\alpha_p<0} p^{l\alpha_p} \equiv \prod_{\alpha_p<0} p^{\alpha_p} \bmod l \tag{5}$$

and if $s \equiv 1 \bmod l$

$$\operatorname{sgn} a \cdot P \prod_{\alpha_p<0} p^{\alpha_p} \prod_{\substack{\alpha_p=0\\ \beta_p\neq 0}} p^{\min\{0,\beta_p\}} \prod_{\alpha_p>0} p^{\beta_p} \equiv a-b \bmod l.$$

For l large enough it follows that

$$\operatorname{sgn} a \cdot P \prod_{\alpha_p<0} p^{\alpha_p} \prod_{\substack{\alpha_p=0\\ \beta_p\neq 0}} p^{\min\{0,\beta_p\}} \prod_{\alpha_p>0} p^{\beta_p} = a-b,$$

and hence

$$\operatorname{sgn} a = \operatorname{sgn}(a-b),\ \alpha_p > 0 \quad \text{implies} \quad \gamma_p = \beta_p,\ \alpha_p \geqslant \beta_p. \tag{6}$$

By (1) and (6), $ab < 0$, so by (2), $\alpha_{p_0} = \beta_{p_0} = \gamma_{p_0}$ contrary to the assumption. Hence $s \not\equiv 1 \bmod l$ and s has a prime factor $q \not\equiv 1 \bmod l, \alpha_q = \beta_q = \gamma_q = 0$. By the Proposition with $n = l$ we have $M_q(a) = M_q(b)$. □

Lemma 2. *Let $ab < 0$. If for a prime $p_0 \mid P$ there exists an integer $r > 0$ prime to the exponent $\lambda(a)$ or $\lambda(b)$ to which a or b, respectively belongs* $\bmod p_0^{\gamma_{p_0}+1}$ *and such that*

$$\operatorname{ord}_{p_0}(a^r - b) \neq \gamma_{p_0} \quad \text{or} \quad \operatorname{ord}_{p_0}(b^r - a) \neq \gamma_{p_0},$$

respectively, then there exists a prime q such that $\alpha_q = \beta_q = \gamma_q = 0$ and $M_q(a) = M_q(b)$.

Proof. Assume without loss of generality that $(r, \lambda(a)) = 1$ and

$$\operatorname{ord}_{p_0}(a^r - b) \neq \gamma_{p_0}.$$

We choose a positive integer r_0 prime to PP_1 in the arithmetic progression $\lambda(a)x + r$. Let

$$\operatorname{ord}_p(a^{r_0} - b) = e_p \quad \text{for all} \quad p \mid P.$$

Let l be a sufficiently large prime in the arithmetic progression $\prod_{p\mid P} p^{e_p} P_1 x + r_0$. We have

$$a^l \equiv a^{r_0} \bmod p^{e_p+1} \quad \text{for all} \quad p \mid P,$$

and hence

$$\operatorname{ord}_p(a^l - b) = e_p \quad \text{for all} \quad p \mid P.$$

Since l is large we again have (3) and (4). Hence

$$a^l - b = \operatorname{sgn} a \prod_{p\mid P} p^{e_p} \prod_{\alpha_p<0} p^{l\alpha_p} \prod_{\substack{\alpha_p=0\\ \beta_p\neq 0}} p^{\min\{0,\beta_p\}} \prod_{\alpha_p>0} p^{\beta_p} s,$$

where s is an integer prime to the numerators and the denominators of a, b, $a-b$ and is positive since $ab < 0$. We again have (5) and if $s \equiv 1 \bmod l$ we would have

$$\operatorname{sgn} a \prod_{p\mid P} p^{e_p} \prod_{\alpha_p<0} p^{\alpha_p} \prod_{\substack{\alpha_p=0\\ \beta_p\neq 0}} p^{\min\{0,\beta_p\}} \prod_{\alpha_p>0} p^{\beta_p} \equiv a-b \bmod l.$$

For l large enough both sides of the congruence are equal, so

$$\gamma_{p_0} = e_{p_0} = \operatorname{ord}_{p_0}(a^{r_0} - b).$$

However $r_0 \equiv r \bmod \lambda(a)$, $a^{r_0} \equiv a^r \bmod p_0^{\gamma_{p_0}+1}$ and so

$$\gamma_{p_0} = \operatorname{ord}_{p_0}(a^r - b),$$

contrary to the assumption. Hence $s \not\equiv 1 \bmod l$ and s has a prime factor $q \not\equiv 1 \bmod l$, $\alpha_q = \beta_q = \gamma_q = 0$. By the Proposition with $n = l$ we have $M_q(a) = M_q(b)$. □

Lemma 3. *If for a prime $p_0 \mid P$ we have*

$$\gamma_{p_0} > \min\bigl\{\operatorname{ord}_{p_0}(a^2 - 1), \operatorname{ord}_{p_0}(b^2 - 1)\bigr\},$$

then p_0 satisfies the assumptions of Lemma 2.

Proof. Without loss of generality we may assume that

$$\gamma_{p_0} > \operatorname{ord}_{p_0}(a^2 - 1).$$

Let λ_0 be the exponent to which a belongs $\bmod p_0^{\gamma_{p_0}}$. Clearly $\lambda_0 > 2$, hence there exists an $r_0 \not\equiv 1 \bmod \lambda_0$ such that $(r_0, \lambda_0) = 1$. The arithmetic progression $\lambda_0 x + r_0$ contains a positive integer r prime to $\lambda(a)$ and we have

$$\begin{aligned}
\operatorname{ord}_{p_0}(a^r - a^{r_0}) &= \operatorname{ord}_{p_0}(a^{r-r_0} - 1) \geqslant \gamma_{p_0},\\
\operatorname{ord}_{p_0}(a^{r_0} - a) &= \operatorname{ord}_{p_0}(a^{r_0-1} - 1) < \gamma_{p_0},\\
\operatorname{ord}_{p_0}(a^r - b) &= \operatorname{ord}_{p_0}(a^r - a^{r_0} + a^{r_0} - a + a - b) < \gamma_{p_0}.
\end{aligned}$$

□

Lemma 4. *If for a prime $p_0 \mid P$ we have*

$$\gamma_{p_0} = \operatorname{ord}_{p_0}(a^2 - 1) = \operatorname{ord}_{p_0}(b^2 - 1) \tag{7}$$

then p_0 satisfies the assumptions of Lemma 2.

Proof. The condition (7) implies

$$a = \varepsilon + p_0^{\mu} a_1, \quad b = \varepsilon + p_0^{\mu} b_1, \quad \text{where} \quad \varepsilon = \pm 1, \ \ a_1, \, b_1 \in \mathbb{Q}, \tag{8}$$

$$\operatorname{ord}_{p_0} a_1 = \operatorname{ord}_{p_0} b_1 = 0, \tag{9}$$

$$\mu = \begin{cases} \gamma_{p_0} - 1 & \text{if } p_0 = 2, \\ \gamma_{p_0} & \text{if } p_0 > 2. \end{cases} \tag{10}$$

We choose a positive integer r such that

$$\begin{cases} a_1 r \equiv b_1 \bmod 4 & \text{if } p_0 = 2, \\ a_1 r \equiv b_1 \bmod p_0 & \text{if } p_0 > 2 \end{cases} \tag{11}$$

and

$$\bigl(r, \, p_0(p_0 - 1)\bigr) = 1. \tag{12}$$

This is possible in view of (9). Now (8), (10) and (11) imply

$$\operatorname{ord}_{p_0}(a^r - b) \geqslant \gamma_{p_0} + 1,$$

while (12) implies $\big(r, \lambda(a)\big) = 1$. □

Lemma 5. *For all $a, b \in \mathbb{Q}\setminus\{0, 1, -1\}$, there exists a prime q such that $\alpha_q = \beta_q = \gamma_q = 0$ and $M_q(a) = M_q(b)$.*

Proof. In view of Lemmas 1–4 it suffices to consider the case where $ab < 0$ and for all primes p

$$\text{either} \quad \alpha_p\beta_p \leqslant 0 \quad \text{or} \quad \alpha_p = \beta_p = \gamma_p, \tag{13}$$

for all $p \mid P$,

$$\gamma_p \leqslant \min\{\operatorname{ord}_p(a^2 - 1),\ \operatorname{ord}_p(b^2 - 1)\} \tag{14}$$

and

$$\gamma_p < \max\{\operatorname{ord}_p(a^2 - 1),\ \operatorname{ord}_p(b^2 - 1)\}. \tag{15}$$

The last two conditions can be reformulated. If $p = 2$,

$$\gamma_2 < \operatorname{ord}_2(a^2 - b^2) = \operatorname{ord}_2\big((a^2 - 1) - (b^2 - 1)\big)$$

and so (15) implies

$$\gamma_2 < \min\big\{\operatorname{ord}_2(a^2 - 1),\ \operatorname{ord}_2(b^2 - 1)\big\}, \tag{16}$$

which is stronger than (14). If $p > 2$

$$\gamma_p = \operatorname{ord}_p(a^2 - b^2) \geqslant \min\big\{\operatorname{ord}_p(a^2 - 1)\big\},\ \operatorname{ord}_p(b^2 - 1)\}$$

hence (14) and (15) are equivalent to (16) and

$$\begin{aligned}\min\big\{\operatorname{ord}_p(a^2 - 1), \operatorname{ord}_p(b^2 - 1)\big\} &= \gamma_p \\ &< \max\big\{\operatorname{ord}_p(a^2 - 1), \operatorname{ord}_p(b^2 - 1)\big\} \quad (p \neq 2).\end{aligned} \tag{17}$$

Note that (16) and (17) are invariant under the replacement of $\langle a, b\rangle$ by $\langle a^{-1}, b^{-1}\rangle$.

Assume first that for a prime $l \nmid P$

$$\alpha_l = \beta_l = \gamma_l \neq 0.$$

Replacing if necessary $\langle a, b\rangle$ by $\langle a^{-1}, b^{-1}\rangle$ we may suppose that

$$\alpha_l = \beta_l = \gamma_l > 0.$$

Hence $l > 2$. For every p with $|\alpha_p| + |\beta_p| > 0,\ \alpha_p\beta_p \leqslant 0$ we have

$$\operatorname{ord}_p(a^l - b) = \begin{cases} l\alpha_p & \text{if } \alpha_p < 0, \\ \min\{0, \beta_p\} & \text{if } \alpha_p = 0, \\ \beta_p = \gamma_p & \text{if } \alpha_p > 0. \end{cases}$$

The same is true by virtue of (13) if $\alpha_p\beta_p > 0$.

For $p \mid P$ if $p = 2$ or $p > 2$, $\operatorname{ord}_p(a^2-1) > \gamma_p$ we have

$$\operatorname{ord}_p(a^l - a) > \gamma_p, \quad \operatorname{ord}_p(a^l - b) = \operatorname{ord}_p(a^l - a + a - b) = \gamma_p;$$

if $p > 2$, $\operatorname{ord}_p(a^2-1) = \gamma_p < \operatorname{ord}_p(b^2-1)$ we have

$$\operatorname{ord}_p(a^{2l} - 1) = \gamma_p,$$
$$\operatorname{ord}_p(a^l - b) = \operatorname{ord}_p(a^{2l} - b^2) = \operatorname{ord}_p(a^{2l} - 1 - (b^2 - 1)) = \gamma_p.$$

Therefore

$$a^l - b = \prod_{\alpha_p < 0} p^{(l-1)\alpha_p}(a-b)s,$$

where s is a positive integer prime to the numerators and the denominators of a, b, $a-b$. Here $p^{l-1} \equiv 1 \bmod l$. If also $s \equiv 1 \bmod l$ we would have

$$a - b \equiv (a-b)s \prod_{\alpha_p < 0} p^{(l-1)\alpha_p} = a^l - b \equiv -b \bmod l^{\alpha_l + 1}, \quad a \equiv 0 \bmod l^{\alpha_l+1},$$

a contradiction.

Hence $s \not\equiv 1 \bmod l$ and s has a prime factor $q \not\equiv 1 \bmod l$, $\alpha_q = \beta_q = \gamma_q = 0$. By Proposition with $n = l$ we have $M_q(a) = M_q(b)$.

Therefore we may assume that

$$\alpha_p \beta_p \leqslant 0 \quad \text{for all primes } p. \tag{18}$$

Let

$$a = \frac{A_1}{A_2}, \quad b = \frac{B_1}{B_2},$$

where

$$A_i, B_i \in \mathbb{Z}, \quad A_1 B_1 < 0, \quad A_2 > 0, \quad B_2 > 0,$$
$$(A_1, A_2) = (B_1, B_2) = 1.$$

By (18), $(A_i, B_i) = 1$ $(i = 1, 2)$ and we have

$$P = |A_1 B_2 - A_2 B_1| \geqslant 2.$$

If P is odd, it has an odd prime factor l. If P is even we have by (16)

$$a \equiv b \equiv \varepsilon \bmod 2^{\gamma_2}, \quad \varepsilon = \pm 1,$$

hence

$$A_1 = \varepsilon A_2 + 2^{\gamma_2} A_3, \quad B_1 = \varepsilon B_2 + 2^{\gamma_2} B_3, \quad A_3, B_3 \in \mathbb{Z} \setminus \{0\} \tag{19}$$

and

$$P = 2^{\gamma_2} |A_3 B_2 - A_2 B_3| = 2^{\gamma_2} |A_3 B_1 - A_1 B_3|.$$

Since $A_1 B_1 < 0 < A_2 B_2$ it follows that $P > 2^{\gamma_2}$, so P has an odd prime factor l. By (17) and since $|a| \neq 1$, $|b| \neq 1$ we may assume without loss of generality that

$$a = \varepsilon + l^{\mu} a_1, \quad b = \varepsilon + l^{\nu} b_1,$$

where

$$\varepsilon = \pm 1, \quad a_1, b_1 \in \mathbb{Q}, \quad \operatorname{ord}_l a_1 = \operatorname{ord}_l b_1 = 0, \quad \mu = \gamma_l < \nu.$$

Clearly

$$a - b \equiv l^{\gamma_l} a_1 \bmod l^{\gamma_l + 1}. \tag{20}$$

Consider now the number $a^{l^{n-\mu}} - b$ (where $n \geqslant \mu$).

For every prime p with $|\alpha_p| + |\beta_p| > 0$ we have by (18)

$$\operatorname{ord}_p(a^{l^{n-\mu}} - b) = \begin{cases} l^{n-\mu}\alpha_p & \text{if } \alpha_p < 0, \\ \min\{0, \beta_p\} & \text{if } \alpha_p = 0, \\ \beta_p & \text{if } \alpha_p > 0. \end{cases}$$

For every $p \mid P$ with $p \neq l$, if $p = 2$ or $p > 2$, $\operatorname{ord}_p(a^2 - 1) > \gamma_p$, we have

$$\operatorname{ord}_p(a^{l^{n-\mu}} - a) > \gamma_p, \quad \operatorname{ord}_p(a^{l^{n-\mu}} - b) = \operatorname{ord}_p(a^{l^{n-\mu}} - a + a - b) = \gamma_p;$$

if $p > 2$, $\operatorname{ord}_p(a^2 - 1) = \gamma_p < \operatorname{ord}_p(b^2 - 1)$ we have

$$\operatorname{ord}_p(a^{2l^{n-\mu}} - 1) = \gamma_p,$$

$$\operatorname{ord}_p(a^{l^{n-\mu}} - b) = \operatorname{ord}_p(a^{2l^{n-\mu}} - b^2) = \operatorname{ord}_p\big(a^{2l^{n-\mu}} - 1 - (b^2 - 1)\big) = \gamma_p.$$

Finally we obtain by induction on $n \geqslant \mu$

$$a^{l^{n-\mu}} \equiv \varepsilon + l^n a_1 \bmod l^{n+1},$$

hence

$$a^{l^{\nu-\mu}} - b \equiv l^{\nu}(a_1 - b_1) \bmod l^{\nu+1}, \tag{21}$$

$$a^{l^{\nu-\mu+1}} - b \equiv -l^{\nu} b_1 \bmod l^{\nu+1}. \tag{22}$$

If $a_1 \not\equiv b_1 \bmod l$ we obtain

$$a^{l^{\nu-\mu}} - b = \prod_{\alpha_p < 0} p^{(l^{\nu-\mu}-1)\alpha_p} l^{\nu-\mu}(a - b)s,$$

where s is a positive integer prime to the numerators and the denominators of a, b, $a - b$. If $s \equiv 1 \bmod l$ we obtain from (20) and (21)

$$a_1 l^{\nu} \equiv (a - b) l^{\nu-\mu} s = (a^{l^{\nu-\mu}} - b) \prod_{\alpha_p < 0} p^{-(l^{\nu-\mu}-1)\alpha_p}$$

$$\equiv l^{\nu}(a_1 - b_1) \bmod l^{\nu+1}, \qquad b_1 \equiv 0 \bmod l,$$

a contradiction. Hence $s \not\equiv 1 \bmod l$ and s has a prime factor $q \not\equiv 1 \bmod l, \alpha_q = \beta_q = \gamma_q = 0$. By the Proposition with $n = l^{\nu-\mu}$ we have $M_q(a) = M_q(b)$.

If $a_1 \equiv b_1 \bmod l$ we obtain

$$a^{l^{\nu-\mu+1}} - b = \prod_{\alpha_p < 0} p^{(l^{\nu-\mu+1}-1)\alpha_p} l^{\nu-\mu}(a - b)s,$$

with s as above. If $s \equiv 1 \bmod l$ we obtain from (20) and (22)

$$a_1 l^{\nu} \equiv (a-b) l^{\nu-\mu} s = (a^{l^{\nu-\mu+1}} - b) \prod_{\alpha_p < 0} p^{-(l^{\nu-\mu+1}-1)\alpha_p} \equiv -l^{\nu} b_1 \bmod l^{\nu+1},$$

and hence $a_1 \equiv -b_1 \bmod l$, $2a_1 \equiv 0 \bmod l$, a contradiction. Thus $s \not\equiv 1 \bmod l$ and by the Proposition with $n = l^{\nu-\mu+1}$, s has a prime factor q with the desired property. □

Proof of the Theorem. Replacing a by a^{-1}, or b by b^{-1}, if necessary we may assume that

$$|a| > \max\{1, |b|\}. \tag{23}$$

We shall construct inductively an infinite sequence of distinct primes $q_1, q_2, \ldots$ such that

$$M_{q_k}(a) = M_{q_k}(b), \quad \alpha_{q_k} = \beta_{q_k} = \gamma_{q_k} = 0 \quad (k = 1, 2, \ldots)$$

and three infinite sequences of positive integers a_k, b_k and c_k such that $(a_k, b_k) = 1$ and for every integer $t \geqslant 0$

$$a^{a_k t + b_k} - b = \operatorname{sgn} a \prod_{\alpha_p < 0} p^{(a_k t + b_k)\alpha_p} \prod_{\substack{\alpha_p = 0 \\ \beta_p \neq 0}} p^{\min\{0, \beta_p\}} \prod_{\alpha_p > 0} p^{\beta_p} \prod_{p \mid P} p^{e_p} \prod_{i=1}^{k} q_i^{c_i} s, \tag{24}$$

where s is a positive integer prime to $q_1 q_2 \cdots q_k$ and to the numerators and the denominators of a, b, $a-b$. Here e_p are non-negative integers independent of k and t. For $k = 1$ we take $q_1 = q$, where q is a prime, the existence of which is asserted in Lemma 5. By that Lemma, $M_q(a) = M_q(b)$, hence $b \equiv a^r \bmod q$, $(r, \lambda) = 1$, where λ is the exponent to which a belongs mod q. We choose a positive integer b_1 such that

$$b_1 > \max_{\alpha_p \neq 0} \frac{\beta_p}{\alpha_p}, \quad b_1 \equiv r \bmod \lambda, \quad (b_1, 2qPP_1) = 1 \tag{25}$$

and put

$$\begin{aligned} &\operatorname{ord}_p(a^{b_1} - b) = e_p \quad (p \mid P), \\ &\operatorname{ord}_q(a^{b_1} - b) = c_1 \\ &a_1 = 2\lambda q^{c_1} \prod_{p \mid P} p^{e_p}(p-1). \end{aligned}$$

Clearly $(a_1, b_1) = 1$ and by virtue of (25) we have for $t \geqslant 0$

$$\operatorname{ord}_p(a^{a_1 t + b_1} - b) = \begin{cases} (a_1 t + b_1)\alpha_p & \text{if } \alpha_p < 0, \\ \min\{0, \beta_p\} & \text{if } \alpha_p = 0,\ \beta_p \neq 0, \\ \beta_p & \text{if } \alpha_p > 0; \end{cases}$$

$$a^{a_1 t + b_1} - b \equiv a^{b_1} - b \bmod \prod_{p \mid P} p^{e_p + 1} \cdot q^{c_1 + 1},$$

hence

$$\begin{aligned} &\operatorname{ord}_p(a^{a_1 t + b_1} - b) = e_p \quad \text{for all} \quad p \mid P, \\ &\operatorname{ord}_q(a^{a_1 t + b_1} - b) = c_1. \end{aligned}$$

Finally, since $a_1 t + b_1$ is odd we have by (23)

$$\operatorname{sgn}(a^{a_1 t + b_1} - b) = \operatorname{sgn} a.$$

Hence (24) holds for $k = 1$.

Assume now that we have constructed $q_1, a_1, b_1, c_1, \ldots, q_{k-1}, a_{k-1}, b_{k-1}, c_{k-1}$. Let l be a sufficiently large prime in the arithmetic progression $a_{k-1} t + b_{k-1}$ $(t \geqslant 0)$.

By the inductive assumption

$$a^l - b = \operatorname{sgn} a \prod_{\alpha_p < 0} p^{l\alpha_p} \prod_{\substack{\alpha_p = 0 \\ \beta_p \neq 0}} p^{\min\{0, \beta_p\}} \prod_{\alpha_p > 0} p^{\beta_p} \prod_{p \mid P} p^{e_p} \prod_{i=1}^{k-1} q_i^{c_i} s,$$

where s is a positive integer, prime to $q_1 q_2 \cdots q_{k-1}$ and to the numerators and the denominators of $a, b, a - b$. Since

$$a^l - b \equiv a - b \bmod l, \quad \prod_{\alpha_p < 0} p^{l\alpha_p} \equiv \prod_{\alpha_p < 0} p^{\alpha_p} \bmod l$$

we have $s \not\equiv 1 \bmod l$. Hence s has a prime factor q_k different from $q_1, q_2, \ldots, q_{k-1}$ and such that $q_k \not\equiv 1 \bmod l$. By Proposition with $n = l$ we have

$$M_{q_k}(a) = M_{q_k}(b) \quad \text{and} \quad \alpha_{q_k} = \beta_{q_k} = \gamma_{q_k} = 0.$$

We take

$$b_k \geqslant b_{k-1}, \quad b_k \equiv l \bmod a_{k-1}(q_k - 1), \quad (b_k, q_k) = 1,$$
$$c_k = \operatorname{ord}_{q_k}(a^{b_k} - b), \quad a_k = a_{k-1}(q_k - 1) q_k^{c_k}$$

and easily verify that $(a_k, b_k) = 1$ and (24) holds. □

Remark. We do not know whether for all $a, b, c \in \mathbb{Q}$, $abc \neq 0$, $|a| \neq 1$, $|b| \neq 1$, $|c| \neq 1$ there exist infinitely many primes q with $M_q(a) = M_q(b) = M_q(c)$.

Originally published in Russian in
Diofantovy Priblizheniya, Matematicheskie Zapiski 2
Moskva 1996, 121–126

On exponential congruences

In memory of N. I. Feldman

This paper is concerned with two problems on exponential congruences considered recently, the first one by C. Corralez Rodrigáñez and R. Schoof, the second by S. P. Tung.

Corralez Rodrigáñez and Schoof [1] have proved the following: Let K be an algebraic number field and let $\alpha, \beta \in K^*$. If, for almost all prime ideals $\mathfrak{p}$ of K and for all positive integers n, $\alpha^n \equiv 1 \bmod \mathfrak{p}$ implies $\beta^n \equiv 1 \bmod \mathfrak{p}$, then $\beta = \alpha^e$, $e \in \mathbb{Z}$ (almost all here and in the sequel means all except for a set of Dirichlet's density 0). This will be generalized as follows.

Theorem 1. *Let K be an algebraic number field and $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_k \in K^*$. If for almost all prime ideals $\mathfrak{p}$ of K and all integers $n_1, \dots, n_k$*

$$\prod_{i=1}^{k} \alpha_i^{n_i} \equiv 1 \bmod \mathfrak{p} \quad \textit{implies} \quad \prod_{i=1}^{k} \beta_i^{n_i} \equiv 1 \bmod \mathfrak{p}, \tag{1}$$

then $\alpha_i = \beta_i^e$ $(1 \leqslant i \leqslant k)$, $e \in \mathbb{Z}$.

If $\varphi \in \mathbb{Q}(t) \setminus \mathbb{Q}[t]$ then there exists an arithmetic progression P such that for $n \in P$, $\varphi(n) \notin \mathbb{Z}$ (see [3], lemma to Theorem 36, p. 195). S. P. Tung has asked in the correspondence with the author, whether a similar theorem holds for expressions

$$\frac{f(t)2^{F(t)} + g(t)}{h(t)}$$

and his question has been subsequently extended by J.-L. Nicolas to expressions

$$\frac{f(t)a^{F(t)} + g(t)b^{G(t)}}{h(t)}.$$

The answer is given by the following

Theorem 2. *Let $f, g, h, F, G \in \mathbb{Z}[t]$, $(f, g, h) = 1$, $h \notin \mathbb{Z}$, $a, b \in \mathbb{N}$, $a^{F(n)}b^{-G(n)}$ be not constant for $n \in \mathbb{Z}$. Then there exists an arithmetic progression P such that for $n \in P$*

$$\frac{f(n)a^{F(n)} - g(n)b^{G(n)}}{h(n)} \notin \mathbb{Z}. \tag{2}$$

Theorem 1 is an immediate consequence of the following two lemmas.

Lemma 1. *Let* $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{Z}^k$, $n \in \mathbb{N}$. *If for all* $\boldsymbol{x} \in \mathbb{Z}^k$, $\boldsymbol{ax} \equiv 0 \bmod n$ *implies* $\boldsymbol{bx} \equiv 0 \bmod n$, *then* $\boldsymbol{b} \equiv \boldsymbol{a}e \bmod n$, $e \in \mathbb{Z}$.

Proof. This is a special case of Lemma 2 in [2]. □

Lemma 2. *Let* $[K : \mathbb{Q}] < \infty$, $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_k \in K^*$. *If the system of congruences*

$$\alpha_i^x \equiv \beta_i \bmod \mathfrak{p} \quad (1 \leqslant i \leqslant k)$$

is solvable for almost all prime ideals $\mathfrak{p}$ *of* K *then the corresponding system of equations is solvable in rational integers.*

Proof. This is Corollary 1 in [4]. □

Proof of Theorem 1. Let g be a primitive root of a prime ideal $\mathfrak{p}$ and $\operatorname{ind}_g \alpha$ the index of α with respect to g determined $\bmod \varphi(\mathfrak{p})$, where φ is Euler's function. If $\operatorname{ord}_{\mathfrak{p}} \alpha_i = \operatorname{ord}_{\mathfrak{p}} \beta_i = 0$ $(1 \leqslant i \leqslant k)$ the implication (1) gives

$$\sum_{i=1}^{k} n_i \operatorname{ind}_g \alpha_i \equiv 0 \bmod \varphi(\mathfrak{p}) \quad \text{implies} \quad \sum_{i=1}^{k} n_i \operatorname{ind}_g \alpha_i \equiv 0 \bmod \varphi(\mathfrak{p}),$$

hence by Lemma 1

$$\operatorname{ind}_g \beta_i \equiv e_{\mathfrak{p}} \operatorname{ind}_g \alpha_i \bmod \varphi(\mathfrak{p}), \quad \text{where } e_{\mathfrak{p}} \in \mathbb{Z}.$$

Thus

$$\beta_i \equiv \alpha_i^{e_{\mathfrak{p}}} \bmod \mathfrak{p} \quad \text{and} \quad \beta_i = \alpha_i^e \quad (1 \leqslant i \leqslant k) \text{ for an } e \in \mathbb{Z},$$

by Lemma 2. □

In order to prove Theorem 2 we need three more lemmas.

Lemma 3. *Let* q *be a prime,* $[K : \mathbb{Q}] < \infty$, $A, B \in K^*$. *If for almost all prime ideals* $\mathfrak{p}$ *of* K *the solvability in* K *of the congruence* $x^q \equiv A \bmod \mathfrak{p}$ *implies the solvability in* K *of the congruence* $x^q \equiv B \bmod \mathfrak{p}$ *then*

$$B = A^r \Gamma^q, \quad \text{where } r \in \mathbb{Z},\ \Gamma \in K^*. \tag{3}$$

Proof. This is a special case of Theorem 1 in [2]. □

Lemma 4. *If* $h, F, G \in \mathbb{Z}[t]$, h *irreducible over* $\mathbb{Q}$; $a, b, c \in \mathbb{N}$, $a^{F(n)} \neq b^{G(n)}$ *for some* $n \in \mathbb{Z}$ *then there exists an arithmetic progression* P *such that for* $n \in P$

$$C\,\frac{a^{F(n)} - b^{G(n)}}{h(n)} \notin \mathbb{Z}. \tag{4}$$

Proof. Consider first the case where a, b are multiplicatively dependent. Then there exists a $c \in \mathbb{N}$ and $\alpha, \beta \in \mathbb{N} \cup \{0\}$ such that c is not a perfect power in $\mathbb{Q}$ and

$$a = c^{\alpha}, \quad b = c^{\beta}. \tag{5}$$

Let

$$h(\vartheta) = 0, \quad K = \mathbb{Q}(\vartheta), \quad d = [K : \mathbb{Q}]. \tag{6}$$

Since $a^{F(n)} \neq b^{G(n)}$ for some $n \in \mathbb{Z}$ we have $\alpha F - \beta G \neq 0$. Hence there exists an integer n_1 and a prime $q_1 > d$ such that

$$\alpha F(n_1) - \beta G(n_1) \not\equiv 0 \bmod q_1. \tag{7}$$

Take in Lemma 3 $q = q_1$, $A = 1$, $B = c$. We cannot have (3) since Γ satisfying (3) would be of degree q_1 and thus by (6) $d > q_1$, contrary to the choice of q_1. Therefore, by Lemma 3 there exists a prime ideal $\mathfrak{p}_1$ of degree 1 in K dividing neither cCq_1 nor the denominator of ϑ and such that the congruence $x^{q_1} \equiv c \bmod \mathfrak{p}_1$ is unsolvable in K. We have $\vartheta \equiv m_1 \bmod \mathfrak{p}_1$, $m_1 \in \mathbb{Z}$. Consider the arithmetic progression

$$P_1 = \{n \in \mathbb{Z} : n \equiv n_1 \bmod q_1,\ n \equiv m_1 \bmod p_1\},$$

where p_1 is the prime divisible by $\mathfrak{p}_1$. If $n \in P_1$ and (4) does not hold we have

$$h(n) \equiv h(\vartheta) \equiv 0 \bmod \mathfrak{p}_1,$$

hence by (5)

$$c^{\alpha F(n) - \beta G(n)} \equiv 1 \bmod \mathfrak{p}_1$$

and by (7)

$$\alpha F(n) - \beta G(n) \not\equiv 0 \bmod q_1.$$

It follows that for some integers ξ, η

$$1 = q_1\xi - (\alpha F(n) - \beta G(n))\eta$$

and $c \equiv (c^{\xi})^{q_1} \bmod \mathfrak{p}_1$ contrary to the choice of $\mathfrak{p}_1$.

Consider now the case where a, b are multiplicatively independent. Let

$$a = \prod_{i=1}^{k} p_i^{\alpha_i}, \quad b = \prod_{i=1}^{k} p_i^{\beta_i},$$

where p_i are distinct primes and α_i, $\beta_i \in \mathbb{N} \cup \{0\}$ $(1 \leqslant i \leqslant k)$. The vectors $[\alpha_1, \ldots, \alpha_k]$, $[\beta_1, \ldots, \beta_k]$ are linearly independent, hence renumbering if necessary the primes p_i we may assume that

$$D = \alpha_1\beta_2 - \alpha_2\beta_1 \neq 0.$$

Since $a^{F(n)} \neq b^{G(n)}$ for some $n \in \mathbb{Z}$ we may assume without loss of generality that $G \neq 0$. Hence there exists an integer n_2 and a prime $q_2 > d$ such that

$$G(n_2) \not\equiv 0 \bmod q_2, \quad q_2 \nmid D. \tag{8}$$

Take in Lemma 3 $q = q_2$, $A = a$, $B = b$. We cannot have (3) with $\Gamma \in \mathbb{Q}$ since it would imply $q_2 \mid D$, hence Γ satisfying (3) would be of degree q_2 and thus by (6) $d \geqslant q_2$, contrary to the choice of q_2. Therefore, by Lemma 3 there exists a prime ideal $\mathfrak{p}_2$ of degree 1 in K dividing neither $Cabq_2$ nor the denominator of ϑ and such that $x^{q_2} \equiv a \bmod \mathfrak{p}$ is solvable

in K, but $x^{q_2} \equiv b \bmod \mathfrak{p}$ is not. We have $\vartheta \equiv m_2 \bmod \mathfrak{p}_2, m_2 \in \mathbb{Z}$. Consider the arithmetic progression

$$P_2 = \{n \in \mathbb{Z} : n \equiv n_2 \bmod q_2,\ n \equiv m_2 \bmod p_2\},$$

where p_2 is the prime divisible by $\mathfrak{p}_2$. If $n \in P_2$ and (4) does not hold we have

$$h(n) \equiv h(\vartheta) \equiv 0 \bmod \mathfrak{p}_2,$$

hence

$$a^{F(n)} \equiv b^{G(n)} \bmod \mathfrak{p}_2,$$

and by (8) $G(n) \not\equiv 0 \bmod q_2$. It follows that for some integers ξ, η

$$1 = q_2\xi - G(n)\eta.$$

Since $a \equiv a_2^{q_2} \bmod \mathfrak{p}_2, a_2 \in K$ we infer that

$$b = b^{q_2\xi - G(n)\eta} \equiv \left(b^{\xi} a_2^{-F(n)\eta}\right)^{q_2} \bmod \mathfrak{p}_2,$$

contrary to the choice of $\mathfrak{p}_2$. □

Lemma 5. *Let* $[K : \mathbb{Q}] < \infty$; $\alpha_1, \alpha_2, \beta \in K^*$. *If the congruence* $\alpha_1^{x_1}\alpha_2^{x_2} \equiv \beta \bmod \mathfrak{p}$ *is solvable for almost all prime ideals* $\mathfrak{p}$ *of* K *then the corresponding equation is solvable in rational integers.*

Proof. This is a special case of Theorem 2 of [2]. □

Proof of Theorem 2. It suffices to consider the case where h is irreducible over $\mathbb{Q}$ and primitive. The case $h \mid fg$ is trivial, hence assume that $h \nmid fg$. Let us again define ϑ, K and d by (6). We shall consider two cases.

Case 1.

$$\frac{g(\vartheta)}{f(\vartheta)} = a^k b^{-l},\ k, l \in \mathbb{Z};$$

Case 2.

$$\frac{g(\vartheta)}{f(\vartheta)} \neq a^k b^{-l},\ k, l \in \mathbb{Z}.$$

1. In this case we have $h(t) \mid f(t)a^k - g(t)b^l$ and since h is primitive, also for all $n \in \mathbb{Z}$

$$h(n) \mid a^{-\min\{0,k\}} b^{-\min\{0,l\}} (f(n)a^k - g(n)b^l).$$

If (2) does not hold it follows that

$$h(n) \mid \big(f(n), h(n)\big) a^{-\min\{0,k\}} b^{-\min\{0,l\}} \big(a^{F(n)}b^l - a^k b^{G(n)}\big).$$

Now $(f(n), h(n)) \mid R$, where R is the resultant of f and h and since $h \nmid f$, $R \neq 0$. The assertion follows on taking in Lemma 4

$$C = a^{k-\min\{0,k\}} b^{l-\min\{0,l\}} |R|$$

and on replacing there F by $F-k$, G by $G-l$.

2. In this case by Lemma 5 there exists a prime ideal $\mathfrak{p}_0$ of degree 1 in K not dividing the denominator of ϑ such that for all $x, y \in \mathbb{Z}$: $f(\vartheta)a^x - g(\vartheta)b^y \not\equiv 0 \bmod \mathfrak{p}_0$. We have $\vartheta \equiv m_0 \bmod \mathfrak{p}_0$, $m_0 \in \mathbb{Z}$. Let $P_0 = \{n \in \mathbb{Z} : n \equiv m_0 \bmod p_0\}$, where p_0 is the prime divisible by $\mathfrak{p}_0$. If $n \in P_0$ and (2) does not hold we have $h(n) \equiv h(\vartheta) \equiv 0 \bmod \mathfrak{p}_0$, hence $f(\vartheta)a^{F(n)} - g(\vartheta)b^{G(n)} \equiv f(n)a^{F(n)} - g(n)b^{G(n)} \equiv 0 \bmod \mathfrak{p}_0$ contrary to the choice of $\mathfrak{p}_0$. □

Remark. By a slightly more complicated argument one can prove the following extension of Theorem 2.

Let $[K : \mathbb{Q}] < \infty$, $f, g, h \in K[t]$; $(f, g, h) = 1$, $h \notin K$; $F, G \in \mathbb{Q}[t]$ be integer valued, $\alpha, \beta \in K^*$, $\alpha^{F(n)}\beta^{-G(n)}$ be not constant for $n \in \mathbb{Z}$. Then there exists an arithmetic progression P such that for $n \in P$

$$\frac{f(n)\alpha^{F(n)} - g(n)\beta^{G(n)}}{h(n)} \quad \text{is not an integer of } K.$$

References

[1] C. Corralez Rodrigáñez, R. Schoof, *The support problem and its elliptic analogue*. J. Number Theory 64 (1997), 276–290.

[2] A. Schinzel, *On power residues and exponential congruences*. Acta Arith. 27 (1975), 397–420; this collection: H4, 915–938.

[3] —, *Selected Topics on Polynomials*. University of Michigan Press, Ann Arbor 1982.

[4] —, *Systems of exponential congruences*. Demonstratio Math. 18 (1985), 377–394; this collection: H7, 975–986.

Originally published in
Journal für die reine und angewandte Mathematik 494 (1998),
73–84

Une caractérisation arithmétique de suites récurrentes linéaires

avec Daniel Barsky (Villetaneuse) et Jean-Paul Bézivin (Caen)

A Monsieur le Professeur Martin Kneser
pour le soixante-dixième anniversaire de sa naissance

Résumé. On étudie la relation entre deux suites récurrentes u_n et v_n de nombres algébriques, quand tout diviseur premier de u_n divise v_n pour chaque n.

I. Introduction

Soit $u = (u_n)_{n\in\mathbb{N}}$ une suite récurrente linéaire d'éléments de $\mathbb{Z}$, c'est-à-dire une suite vérifiant une relation de la forme :

$$u_{n+s} + a_{s-1}u_{n+s-1} + \ldots + a_0 u_n = 0$$

avec les a_i dans $\mathbb{Z}$ fixés.

On considère l'ensemble $A(u) = \{p \text{ premier} : \exists n \in \mathbb{N},\ u_n \neq 0 \text{ et } p \mid u_n\}$, que nous appelerons *l'ensemble des diviseurs premiers* de la suite $u = (u_n)_{n\in\mathbb{N}}$.

On sait qu'en général l'ensemble $A(u)$ est infini, [10].

On peut demander quelle est la proportion des nombres premiers qui sont des diviseurs d'une suite récurrente donnée. Le premier pas dans cette direction a été accompli par H. Hasse, [6], qui montre par exemple que la densité au sens de Dirichlet de l'ensemble des diviseurs premiers de la suite $u_n = 2^n + 1$ est $7/24$. D'autres résultats de ce type, utilisant la méthode de démonstration de Hasse, ont été obtenus par J. Lagarias, [7], et C. Ballot, [1].

On peut demander aussi dans quelle mesure cet ensemble caractérise la suite récurrente linéaire. On voit aisément que si la suite possède un zéro entier, i.e. s'il existe $m \in \mathbb{N}$ tel que $u_m = 0$, alors l'ensemble $A(u)$ est l'ensemble des nombres premiers, à un nombre fini d'exception près. Il nous faut donc préciser un peu les conditons à imposer.

Nous allons nous intéresser à un résultat démontré par C. Corrales et R. Schoof, [4], et généralisé par A. Schinzel, [12], dont un cas particulier est le suivant :

Soient a et b deux éléments de $\mathbb{Z}$, tels que $|a| > 1$ et $|b| > 1$. Alors si

$$\{p \text{ premiers} : p \mid a^n - 1\} = \{p \text{ premiers} : p \mid b^n - 1\}$$

pour tout $n \in \mathbb{N}$, on a $a = b$.

Soit $\mathbb{K}$ un corps de nombres. Nous généralisons ce résultat à des suites récurrentes linéaires liées à des polynômes de $\mathbb{K}[x_1, \ldots, x_s]$ dont l'ensemble Ω des solutions dans les racines de l'unité est non vide et fini. Typiquement soit $P(x, y) = x + y + 1$ et soit j une racine primitive cubique de l'unité alors $\Omega = \{(j, j^2), (j^2, j)\}$ et si l'on a pour tout n :

$$\{\mathfrak{p}, \text{ idéaux premiers de } \mathbb{K} : \mathfrak{p} \mid a^n + b^n + 1\} = \{\mathfrak{p}, \text{ idéaux premiers de } \mathbb{K} : \mathfrak{p} \mid \alpha^n + \beta^n + 1\}$$

où $a, b, \alpha, \beta \in \mathbb{K}^*$ alors, avec quelques conditions techniques sur a, b, α, β (voir plus loin) et quitte à permuter, $a = \alpha$, $b = \beta$.

II. Résultats

Soit T un polynôme à s variables, à coefficients dans $\mathbb{K}$. On note Γ_∞ le groupe des racines de l'unité et Γ_m le groupe des racines m-ièmes de l'unité (éventuellement plongé dans un corps suffisamment grand). On note :

$$\Omega = \Omega(T) = \{\gamma = (\gamma_1, \ldots, \gamma_s) : \gamma_i \in \Gamma_\infty,\ 1 \leqslant i \leqslant s, \text{ tels que } T(\gamma_1, \ldots, \gamma_s) = 0\},$$
$$\Omega_m(T) = \Gamma_m^s \cap \Omega(T).$$

Soient $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s$ des éléments non nuls de $\mathbb{K}$. Nous allons démontrer aux paragraphes III et IV les résultats suivants :

Théorème 1. *Soient*

$$T'(x_1, \ldots, x_r) \in \mathbb{K}[x_1, \ldots, x_r] \quad \text{et} \quad T(x_1, \ldots, x_s) \in \mathbb{K}[x_1, \ldots, x_s]$$

deux polynômes tels que $\Omega(T')$ soit non vide et que $\Omega(T)$ soit fini. Soient

$$\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_r) \in (\mathbb{K}^*)^r \quad \text{et} \quad \boldsymbol{\beta} = (\beta_1, \ldots, \beta_s) \in (\mathbb{K}^*)^s.$$

On suppose que les α_i sont multiplicativement indépendants, c'est-à-dire que l'égalité $\prod_{i=1}^{r} \alpha_i^{x_i} = 1$ avec $x_1, \ldots, x_r \in \mathbb{Z}$ implique $x_1 = \ldots = x_r = 0$.

Enfin on suppose que pour tout entier $n > 0$ et que pour presque tout idéal premier $\mathfrak{p}$ de $\mathbb{K}$ (i.e. tous sauf un nombre fini) on a :

$$\mathfrak{p} \mid T'(\alpha_1^n, \ldots, \alpha_r^n) \implies \mathfrak{p} \mid T(\beta_1^n, \ldots, \beta_s^n).$$

Alors $\Omega(T)$ est non vide et il existe un entier naturel $d > 0$ tel que, pour tout $j \in \{1, \ldots, s\}$, il existe des $e_{i,j} \in \mathbb{Z}$ tels que :

$$\beta_j^d = \alpha_1^{e_{j,1}} \cdots \alpha_r^{e_{j,r}}.$$

Théorème 2. *On suppose que dans les hypothèses du théorème 1, on a $r = s = 1$, de sorte que $\boldsymbol{\alpha} = (\alpha_1)$ et n'est pas une racine de l'unité, et que $\boldsymbol{\beta} = (\beta_1)$. On pose $\alpha_1 = \alpha$ et*

$\beta_1 = \beta$. On suppose en outre que $T'(x)$ est séparable et $T'(0) \neq 0$. Soit w le nombre de racines de l'unité contenues dans le corps $\mathbb{K}$, et ζ_w une racine primitive w-ième de 1.

L'implication

$$\mathfrak{p} \mid T'(\alpha^n) \implies \mathfrak{p} \mid T(\beta^n)$$

est vraie pour presque tout idéal premier $\mathfrak{p}$ de $\mathbb{K}$ et pour tout entier $n > 0$, si et seulement s'il existe des entiers $a_0, a_1 > 0$, b_0, b_1 et $\gamma \in \mathbb{K}$ tels que $(a_1, b_1) = 1$ et $\alpha = \zeta_w^{a_0}\gamma^{a_1}$, $\beta = \zeta_w^{b_0}\gamma^{b_1}$ et si, pour tout $\mu \in \{0, \ldots, w-1\}$

$$T'(\zeta^{a_0\mu}x^{a_1}) \mid T(\zeta^{b_0\mu}x^{b_1})x^{-\min\{0,b_1\}\deg(T)}.$$

Théorème 3. *Soit Φ_n le polynôme cyclotomique d'ordre n, et k, l deux entiers positifs, avec l sans facteur carré. Soient $\alpha, \beta \in \mathbb{K}^*$, avec α non racine de l'unité. L'implication*

$$\mathfrak{p} \mid \Phi_k(\alpha^n) \implies \mathfrak{p} \mid \Phi_l(\beta^n)$$

est vraie pour tout entier $n > 0$ et presque tout idéal premier de $\mathbb{K}$, si et seulement si l divise k et $\beta = \alpha^{k\lambda/l}$, où $(\lambda, l) = 1$.

Corollaire 1. *On suppose que dans les hypothèses du théorème* 1*, on a $r = s$, et que de plus les α_i et les β_i sont des entiers de $\mathbb{K}$, et qu'aucun d'eux n'est une unité de $\mathbb{K}$ ni égal, à une racine de l'unité près, à une puissance parfaite dans $\mathbb{K}$. On suppose de plus que les α_i sont deux à deux premiers entre eux, ainsi que les β_i. Alors l'implication*

$$\mathfrak{p} \mid T'(\alpha_1^n, \ldots, \alpha_s^n) \implies \mathfrak{p} \mid T(\beta_1^n, \ldots, \beta_s^n)$$

est vraie pour tout entier $n > 0$ et presque tout idéal premier $\mathfrak{p}$ seulement s'il existe une permutation j_i de $\{1, \ldots, s\}$, et des entiers b_i tels que :

$$\beta_i = \zeta_w^{b_i}\alpha_{j_i}.$$

Corollaire 2. *On suppose que les éléments $\alpha_1, \alpha_2, \beta_1, \beta_2$ satisfont aux hypothèses du corollaire* 1*, avec $s = r = 2$; on suppose de plus que $w = 2$. Si*

$$\mathfrak{p} \mid \alpha_1^n + \alpha_2^n + 1 \implies \mathfrak{p} \mid \beta_1^n + \beta_2^n + 1$$

pour tout entier $n > 0$ et presque tout idéal premier $\mathfrak{p}$ de $\mathbb{K}$, alors on a $\{\alpha_1, \alpha_2\} = \{\beta_1, \beta_2\}$.

III. Lemmes préliminaires

Lemme 1. *Dans le corps de nombres $\mathbb{K}$, il existe une base multiplicative, c'est-à-dire une suite π_i $(i = 1, \ldots)$ d'éléments non nuls de $\mathbb{K}$ telle que tout élément $\alpha \in \mathbb{K}^*$ possède une unique représentation sous la forme* :

$$\alpha = \zeta_w^{a_0} \prod_{i=1}^{h} \pi_i^{a_i}$$

où $a_0 \in \{0, \ldots, w-1\}$, et $a_i \in \mathbb{Z}$, $1 \leqslant i \leqslant h$.

Preuve. Voir Skolem [15]. □

Lemme 2. *Avec les mêmes notations que dans le lemme précédent, pour tout entier positif m et tout vecteur $(t_0, \ldots, t_h)$ de $\mathbb{Z}^{h+1}$, il existe une infinité d'idéaux premiers $\mathfrak{p}$ de $\mathbb{K}(\zeta_{wm})$ tels que $\left(\frac{\zeta_w}{\mathfrak{p}}\right)_{wm} = \zeta_w^{t_0}$ et $\left(\frac{\pi_i}{\mathfrak{p}}\right)_{wm} = \zeta_{wm}^{wt_i}$, $1 \leqslant i \leqslant h$, où l'on a noté $\left(\frac{\alpha}{\mathfrak{p}}\right)_{wm}$ le symbole de Legendre pour les puissances wm-ièmes.*

Preuve. C'est un cas particulier du théorème 4 de Schinzel, [13]. □

Lemme 3. *Soient k, l deux entiers positifs, et $\boldsymbol{a} \in \mathbb{Z}^r$, $A \in M_{r,h}(\mathbb{Z})$. On suppose que A est de rang r, et que la matrice $B \in M_{s,h}(\mathbb{Z})$ possède la propriété que pour tout $\boldsymbol{t} \in \mathbb{Z}^h$ et tout entier positif m divisible par k on ait*:

$$A\boldsymbol{t} = \frac{m}{k}\,\boldsymbol{a} \implies lB\boldsymbol{t} \equiv \boldsymbol{0} \pmod{m}. \tag{1}$$

Alors il existe une matrice $C \in M_{s,r}(\mathbb{Q})$ telle que $B = CA$.

Preuve. On peut supposer sans nuire à la généralité, que la matrice A_1 constituée des r premières colonnes de A est inversible. Soit B_1 la matrice constituée des r premières colonnes des B. Supposons que $B \neq (B_1 A_1^{-1})A$. Alors $r < h$ et on peut supposer que si $\boldsymbol{a}_{r+1}$ et $\boldsymbol{b}_{r+1}$ sont les $r+1$-ième colonnes de A et B respectivement, on a:

$$\begin{pmatrix} c_1 \\ \vdots \\ c_h \end{pmatrix} = \boldsymbol{b}_{r+1} - (B_1 A_1^{-1})\boldsymbol{a}_{r+1} \neq \boldsymbol{0}.$$

Soit

$$c = \max_{1 \leqslant i \leqslant h} \{|c_i|\} \tag{2}$$

et posons

$$m = 2ckl\,(\det(A_1))^2\,. \tag{3}$$

Comme $c\det(A_1) \in \mathbb{Z}$, m est un entier positif divisible par $k\det(A_1)$.

On définit maintenant un vecteur entier $(t_1, \ldots, t_r)$ par

$$\begin{pmatrix} t_1 \\ \vdots \\ t_r \end{pmatrix} = \frac{m}{k}\,A_1^{-1}\boldsymbol{a} - \det(A_1)A_1^{-1}\boldsymbol{a}_{r+1} \tag{4}$$

et posons

$$\boldsymbol{t} = \begin{pmatrix} t_1 \\ \vdots \\ t_r \\ \det(A_1) \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{5}$$

Les formules précédentes impliquent que $A\boldsymbol{t} = \dfrac{m}{k}\,\boldsymbol{a}$, et par suite on a

$$l B\boldsymbol{t} \equiv \boldsymbol{0} \pmod{m}. \tag{6}$$

On a de plus, en tenant compte de (4) et de (5) :

$$l B\boldsymbol{t} = l B_1 \begin{pmatrix} t_1 \\ \vdots \\ t_r \end{pmatrix} + l \det(A_1)\boldsymbol{b}_{r+1}$$

$$= \frac{lm}{k}\, B_1 A_1^{-1}\boldsymbol{a} - l \det(A_1) B_1 A_1^{-1}\boldsymbol{a}_{r+1} + l \det(A_1)\boldsymbol{b}_{r+1}.$$

Avec la relation (6), ceci donne :

$$l \det(A_1)\big(\boldsymbol{b}_{r+1} - (B_1 A_1^{-1})\boldsymbol{a}_{r+1}\big) \equiv \boldsymbol{0} \left(\mathrm{mod}\ \frac{m}{k \det(A_1)}\right).$$

En vertu de (3), on obtient alors

$$\boldsymbol{b}_{r+1} - (B_1 A_1^{-1})\boldsymbol{a}_{r+1} \equiv \boldsymbol{0} \pmod{2c}$$

ce qui est une contradiction avec la relation (2). On a donc bien $B = (B_1 A_1^{-1})A$. □

Lemme 4. *Si A, B, C, l sont des entiers tels que $l \mid C$, l sans facteur carré, et pour tout $t \in \mathbb{Z}$ on a $(At + B, C) = \dfrac{C}{l}$, alors $C \mid A$.*

Preuve. En prenant $t = 0$ et $t = 1$ on trouve que $A = \dfrac{C}{l}\,a$, $B = \dfrac{C}{l}\,b$, avec $a, b \in \mathbb{Z}$.

c En outre, pour tout $t \in \mathbb{Z}$, on a $(at + b, l) = 1$. Comme l est sans facteur carré, si $l \nmid a$, il existe un nombre premier p divisant l et ne divisant pas a. En résolvant la congruence $at + b \equiv 0 \pmod{p}$, on trouve $(at + b, l) \equiv 0 \pmod{p}$, ce qui est impossible. □

Lemme 5. *Soient ℓ et m entiers positifs. On a*

$$\Phi_\ell(x^m) = \prod_{d \mid m} \Phi_{\ell d}(x), \quad \textit{si } (\ell, m) = 1,$$

$$\Phi_\ell(x^m) = \Phi_{\ell m}(x), \quad \textit{si tout facteur premier de } m \textit{ divise } \ell.$$

Preuve. Pour m premier le lemme est bien connu. La cas général en résulte par récurrence sur le nombre de facteurs premiers de m. □

IV. Démonstrations des résultats

Preuve du théorème 1. On pose :

$$\alpha_i = \zeta_w^{a_{i,0}} \prod_{j=1}^{h} \pi_j^{a_{i,j}}, \quad 1 \leqslant i \leqslant r, \tag{7}$$

$$\beta_i = \zeta_w^{b_{i,0}} \prod_{j=1}^{h} \pi_j^{b_{i,j}}, \quad 1 \leqslant i \leqslant s, \tag{8}$$

$$A = (a_{i,j}), \quad B = (b_{i,j}).$$

Comme les α_i sont multiplicativement indépendants, le rang de la matrice A est r.

Par hypothèse, il existe deux entiers k, l tels que

$$\Omega_k(T') \neq \emptyset, \quad \Omega(T) \subset \Omega_l(T). \tag{9}$$

Soit ζ_k une racine primitive k-ième de 1, et $(\zeta_k^{a_1}, \ldots, \zeta_k^{a_r}) \in \Omega_k(T')$; on pose $\boldsymbol{a} = \begin{pmatrix} a_1 \\ \vdots \\ a_r \end{pmatrix}$.

Nous allons démontrer que, pour tout vecteur $\boldsymbol{t} \in \mathbb{Z}^h$, et tout entier positif m divisible par k, l'égalité

$$A\boldsymbol{t} = \frac{m}{k}\,\boldsymbol{a} \tag{10}$$

implique que

$$lB\boldsymbol{t} \equiv \boldsymbol{0} \pmod{m}. \tag{11}$$

En vertu du lemme 2, il existe une infinité d'idéaux premiers $\mathfrak{p}$ de $\mathbb{K}(\zeta_{wm})$ tels que

$$\left(\frac{\zeta_w}{\mathfrak{p}}\right)_{wm} = 1, \quad \left(\frac{\pi_j}{\mathfrak{p}}\right)_{wm} = \zeta_{wm}^{wt_j}, \quad 1 \leqslant j \leqslant h, \tag{12}$$

où l'on a choisi la racine primitive ζ_{wm} telle que $\zeta_{wm}^{wm/k} = \zeta_k$. Donc en vertu de (7) et de (10),

$$\left(\frac{\alpha_i}{\mathfrak{p}}\right)_{wm} = \zeta_k^{a_k}$$

et comme

$$T'\left(\left(\frac{\alpha_1}{\mathfrak{p}}\right)_{wm}, \ldots, \left(\frac{\alpha_r}{\mathfrak{p}}\right)_{wm}\right) = 0$$

il en résulte que

$$T'\big(\alpha_1^{(N(\mathfrak{p})-1)/(wm)}, \ldots, \alpha_r^{(N(\mathfrak{p})-1)/(wm)}\big) \equiv 0 \pmod{\mathfrak{P}}$$

où N est la norme de $\mathbb{K}(\zeta_{wm})$ sur $\mathbb{K}$, et $\mathfrak{P}$ désigne l'idéal premier de $\mathbb{K}$ divisible par $\mathfrak{p}$.

Si la norme de $\mathfrak{p}$ est assez grande, on a par hypothèse que

$$T\big(\beta_1^{(N(\mathfrak{p})-1)/(wm)}, \ldots, \beta_s^{(N(\mathfrak{p})-1)/(wm)}\big) \equiv 0 \pmod{\mathfrak{P}}$$

donc

$$T\left(\left(\frac{\beta_1}{\mathfrak{p}}\right)_{wm}, \ldots, \left(\frac{\beta_s}{\mathfrak{p}}\right)_{wm}\right) \equiv 0 \pmod{\mathfrak{p}}$$

ce qui implique

$$N\left(T\left(\left(\frac{\beta_1}{\mathfrak{p}}\right)_{wm}, \ldots, \left(\frac{\beta_s}{\mathfrak{p}}\right)_{wm}\right)\right) \equiv 0 \pmod{N(\mathfrak{p})}.$$

Le côté gauche de cette congruence est borné par une constante ne dépendant que de T et de m. Si $N(\mathfrak{p})$ est suffisamment grande, cette congruence implique donc que

$$T\left(\left(\frac{\beta_1}{\mathfrak{p}}\right)_{wm}, \ldots, \left(\frac{\beta_s}{\mathfrak{p}}\right)_{wm}\right) = 0$$

et par suite $\Omega(T) \neq \emptyset$. Par l'inclusion (9) $\Omega(T) \subset \Omega_l(T)$, il en résulte que $\left(\frac{\beta_i}{\mathfrak{p}}\right)_{wm}^{l} = 1$ pour tout $i = 1, \ldots, s$.

Il suffit alors d'utiliser (8) et (12), qui donne la relation (11). Le lemme 3 implique alors l'existence d'une matrice $C \in M_{s,r}(\mathbb{Q})$ telle que

$$B = CA.$$

On pose $C = \left(\frac{e_{i,j}}{d}\right)$, $1 \leqslant i \leqslant s$, $1 \leqslant j \leqslant r$, où d est un entier positif divisible par w et où les $e_{i,j}$ sont dans $\mathbb{Z}$, et on obtient

$$\beta_i^d = \prod \alpha_j^{e_{i,j}}. \qquad \square$$

Preuve du théorème 2. Nous montrons tout d'abord que la condition est nécessaire. Supposons donc que pour tout entier n et presque tout idéal premier $\mathfrak{p}$ de $\mathbb{K}$ on ait

$$\mathfrak{p} \mid T'(\alpha^n) \implies \mathfrak{p} \mid T(\beta^n).$$

En vertu du théorème 1, il existe $d \in \mathbb{N}^*$, et $e \in \mathbb{Z}$ tels que $\beta^d = \alpha^e$.

Posons $\dfrac{e}{d} = \dfrac{b_1}{a_1}$, avec $a_1, b_1 \in \mathbb{Z}$, $a_1 > 0$ et $(a_1, b_1) = 1$.

Comme $\left(\dfrac{\beta^{a_1}}{\alpha^{b_1}}\right)^{(d,e)} = 1$, on a $\beta^{a_1} = \zeta_w^{c_1}\alpha^{b_1}$.

En prenant des entiers u, v tels que $ua_1 - vb_1 = 1$, et en posant $a_0 = c_1 u$, $b_0 = c_1 v$, et $\gamma = \alpha^u \beta^{-v}$, il vient

$$\alpha = \zeta_w^{a_0}\gamma^{a_1}, \quad \beta = \zeta_w^{b_0}\gamma^{b_1}.$$

Comme α n'est pas une racine de l'unité, il en est de même de γ.

Supposons maintenant que pour une valeur de $\mu \in \{0, \ldots, w-1\}$, on ait

$$T'(\zeta_w^{a_0\mu} x^{a_1}) \not\mid T(\zeta_w^{b_0\mu} x^{b_1}) x^{-\min\{0,b_1\}\deg(T)}. \tag{13}$$

Comme T' est séparable, et $T'(0) \neq 0$, le polynôme $T'(\zeta_w^{a_0\mu} x^{a_1})$ est aussi séparable, et si on pose

$$D(x) = \left(T'(\zeta_w^{a_0\mu} x^{a_1}),\, T(\zeta_w^{b_0\mu} x^{b_1}) x^{-\min\{0,b_1\}\deg(T)}\right)$$

on a

$$1 = \left(\frac{T'(\zeta_w^{a_0\mu} x^{a_1})}{D(x)}\,,\, T(\zeta_w^{b_0\mu} x^{b_1}) x^{-\min\{0,b_1\}\deg(T)}\right).$$

Il existe donc des polynômes U, $V \in \mathbb{K}[x]$ tels que

$$\frac{T'(\zeta_w^{a_0\mu} x^{a_1})}{D(x)}\, U(x) + T(\zeta_w^{b_0\mu} x^{b_1}) x^{-\min\{0,b_1\}\deg(T)} V(x) = 1. \tag{14}$$

Puisque $T'(0) \neq 0$, on a que $\dfrac{T(\zeta_w^{a_0\mu} x^{a_1})}{D(x)}$ n'est pas de la forme cx^m, avec $c \in \mathbb{K}$ et $m \in \mathbb{N}$.

Par un résultat d'Evertse ([5]), il en résulte que la suite récurrente $\dfrac{T'(\zeta_w^{a_0\mu} \gamma^{a_1(w\nu+\mu)})}{D(\gamma^{w\nu+\mu})}$ ($\nu = 1, 2, \dots$) a une infinité de diviseurs $\mathfrak{p}$ de $\mathbb{K}$.

En choisissant un diviseur $\mathfrak{p}$ tel que γ soit une unité $\mathfrak{p}$-adique et les coefficients de U, V, D des entiers $\mathfrak{p}$-adiques, il en résulte du fait que

$$\mathfrak{p} \mid T'(\alpha^{w\nu+\mu}) \implies \mathfrak{p} \mid T(\beta^{w\nu+\mu})$$

une contradiction avec la relation (14).

On a donc bien

$$T'(\zeta_w^{a_0\mu} x^{a_1}) \mid T(\zeta_w^{b_0\mu} x^{b_1}) x^{-\min\{0,b_1\}\deg(T)} \quad \forall \mu \in \{0, \dots, w-1\}.$$

Montrons maintenant que la condition est suffisante.

On suppose donc que

$$\alpha = \zeta_w^{a_0} \gamma^{a_1}, \quad \beta = \zeta_w^{b_0} \gamma^{b_1}$$

et

$$T'(\zeta_w^{a_0\mu} x^{a_1}) \mid T(\zeta_w^{b_0\mu} x^{b_1}) x^{-\min\{0,b_1\}\deg(T)} \quad \forall \mu \in \{0, \dots, w-1\}.$$

Soit $\mathfrak{p}$ un idéal premier tel que γ soit une unité $\mathfrak{p}$-adique, et que les coefficients des polynômes

$$\frac{T(\zeta_w^{b_0\mu} x^{b_1}) x^{-\min\{0,b_1\}\deg(T)}}{T'(\zeta_w^{a_0\mu} x^{a_1})}$$

soient des entiers $\mathfrak{p}$-adiques.

Alors :

$$\mathfrak{p} \mid T'(\zeta_w^{a_0\mu} \gamma^{(w\nu+\mu)a_1}) \implies \mathfrak{p} \mid T(\zeta_w^{b_0\mu} \gamma^{(w\nu+\mu)b_1}).$$

Donc, pour tout $n \equiv \mu \pmod{w}$, on a :

$$\mathfrak{p} \mid T'(\alpha^n) \implies \mathfrak{p} \mid T(\beta^n)$$

et comme cette propriété est vraie pour tout $\mu \in \{0, \ldots, w-1\}$, ceci achève la démonstration. □

Preuve du théorème 3. Montrons d'abord que la condition est nécessaire. On applique le théorème 2 avec $T' = \Phi_k$, $T = \Phi_l$, et on obtient

$$\alpha = \zeta_w^{a_0}\gamma^{a_1}, \quad \beta = \zeta_w^{b_0}\gamma^{b_1}, \quad (a_1, b_1) = 1,\ a_1 > 0 \tag{15}$$

et

$$\Phi_k(\zeta_w^{a_0\mu}x^{a_1}) \mid \Phi_l(\zeta_w^{b_0\mu}x^{b_1}) \quad \forall \mu \in \{0, \ldots, w-1\}.$$

Comme les zéros de Φ_k sont les ζ_k^{κ}, κ premier à k, et les zéros de Φ_l les ζ_l^{λ}, λ premier à l, on obtient que pour $\mu \in \mathbb{Z}$, tout κ premier à k et tout $t \in \mathbb{Z}$ on a :

$$\zeta_w^{b_0\mu}\zeta_{wa_1}^{-a_0\mu}\zeta_{ka_1}^{\kappa+tk} = \zeta_{kwa_1}^{b_0\mu ka_1 - b_1a_0\mu k + b_1w(\kappa+tk)} = \zeta_l^{\lambda}$$

avec λ premier à l.

Donc l divise kwa_1, et

$$\big(k(b_0a_1 - b_1a_0)\mu + w\kappa b_1 + wkb_1t, kwa_1\big) = \frac{kwa_1}{l}. \tag{16}$$

En appliquant le lemme 4 deux fois, on obtient

$$kwa_1 \mid wkb_1, \quad kwa_1 \mid k(b_0a_1 - b_1a_0) \tag{17}$$

comme $(a_1, b_1) = 1$, la première relation donne $a_1 = 1$, et la seconde $w \mid (b_0 - a_0b_1)$; donc en vertu de (15), il vient $\beta = \alpha^{b_1}$.

Il résulte de (16) et de (17) que

$$(w\kappa b_1, kw) = \frac{kw}{l}$$

et comme $(k, \kappa) = 1$, on trouve $b_1 = \dfrac{k}{l}\lambda$, $(\lambda, l) = 1$, donc $l \mid k$ et $\beta = \alpha^{k\lambda/l}$.

Montrons maintenant que la condition est suffisante.

Si l divise k et si $\beta = \alpha^{k\lambda/l}$, désignons par τ le plus grand diviseur de k premier à l et soit $n \in \mathbb{N}$. Alors d'après le lemme 5

$$\Phi_l(\beta^n) = \Phi_l(\alpha^{k\lambda n/l}) = \prod_{d \mid \lambda\tau} \Phi_{ld}(\alpha^{kn/(l\tau)}) = \prod_{d \mid \lambda\tau} \Phi_{kd/\tau}(\alpha^n).$$

c

Il en résulte que

$$\Phi_l(\beta^n)\Phi_k(\alpha^n)^{-1} = \prod_{d \mid \lambda\tau,\, d \neq \tau} \Phi_{kd/\tau}(\alpha^n)$$

et donc, pour tout idéal premier $\mathfrak{p}$ de $\mathbb{K}$ tel que α soit une unité $\mathfrak{p}$-adique on a :

$$\mathfrak{p} \mid \Phi_k(\alpha^n) \implies \mathfrak{p} \mid \Phi_l(\beta^n). \qquad \square$$

Preuve du corollaire 1. La condition que les α_i sont premiers deux à deux et ne sont pas des unités de $\mathbb{K}$ implique qu'ils sont multiplicativement indépendants. En appliquant le

théorème 1, il vient que

$$\beta_i^d = \prod_{j=1}^{r} \alpha_j^{e_{i,j}}$$

avec d entier > 0. Comme les β_i sont des entiers et les α_i ne sont pas des unités algébriques, il vient que les $e_{i,j}$ sont des entiers $\geqslant 0$. Comme les β_i sont premiers entre eux deux à deux, il vient que pour chaque j, au plus un des $e_{i,j}$ est non nul. Mais comme β_i n'est pas une unité de $\mathbb{K}$, il en résulte que pour chaque i au moins un des $e_{i,j}$ est non nul. Il existe donc une permutation j_i de $\{1, \ldots, r\}$ telle que

$$\beta_i^d = \alpha_{j_i}^{e_{i,j_i}}.$$

Comme ni α_i, ni β_i n'est, aux racines de l'unité près, une puissance parfaite dans $\mathbb{K}$, il vient finalement que $\beta_i = \zeta_w^{b_i} \alpha_j$, avec $b_i \in \mathbb{Z}$. □

Preuve du corollaire 2. On applique le corollaire 1 avec $T = T' = x_1 + x_2 + 1$. Il en résulte, que quitte à renuméroter, on peut écrire $\beta_i = \varepsilon_i \alpha_i$, où $\varepsilon_i \in \{\pm 1\}$, pour $i = 1, 2$.

• Si $\varepsilon_1 \varepsilon_2 = -1$, on obtient une contradiction pour n impair en utilisant un idéal premier de norme assez grande divisant $\alpha_1^n + \alpha_2^n + 1$ et donc $2\alpha_1^n$ ou $2\alpha_2^n$.

• Si $\varepsilon_1 = \varepsilon_2 = -1$, on obtient de même que $\mathfrak{p}$ divise la somme

$$(\alpha_1^n + \alpha_2^n + 1) + (\beta_1^n + \beta_2^n + 1) = 2.$$

D'où le résultat. □

V. Exemples de polynômes

Proposition 1. *Soit* $F(\boldsymbol{x}) = \sum_{\boldsymbol{h}} a_{h_1,\ldots,h_t} x_1^{h_1} \cdots x_t^{h_t}$ *et* $G(\boldsymbol{y}) = \sum_{\boldsymbol{l}} b_{l_1,\ldots,l_s} y_1^{l_1} \cdots y_s^{l_s}$ *des polynômes à coefficients dans* $\mathbb{Z}$ *tels que* $\Omega(F)$ *et* $\Omega(G)$ *soient finis et non vides.*

Soit $\|F\| = \sum_{\boldsymbol{h}} |a_{h_1,\ldots,h_t}|$. *Posons* $H(\boldsymbol{x}, \boldsymbol{y}) = \mu F(\boldsymbol{x}) + \lambda G(\boldsymbol{y})$ *avec* $\lambda, \mu \in \mathbb{Z}$ *et* $|\lambda| > |\mu| \cdot \|F\|$. *Alors* $\Omega(H) = \Omega(F) \times \Omega(G)$ *et est donc fini et non vide.*

Preuve. Soit $\boldsymbol{z} = (\boldsymbol{x}, \boldsymbol{y}) \in \Omega(H)$, et $\mathbb{K}$ un corps de nombres de degré N, contenant tous les x_i, y_j et leur conjugués. Soit $T = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$, alors :

$$\mu^N \prod_{\sigma \in T} F(\boldsymbol{x}^\sigma) = (-\lambda)^N \prod_{\sigma \in T} G(\boldsymbol{y}^\sigma) \implies \left|(-\lambda)^N \prod_{\sigma \in T} G(\boldsymbol{y}^\sigma)\right| \leqslant \|F\|^N |\mu|^N.$$

Si $G(\boldsymbol{y}) \neq 0$, il vient $|\lambda| \leqslant |\mu| \cdot \|F\|$, contradiction. Donc $G(\boldsymbol{y}) = 0$ et par conséquent $F(\boldsymbol{x}) = 0$. □

Cette proposition permet de construire des exemples à volonté :

(a) $1 + x_1 + \lambda(1 + y_1)$ avec $|\lambda| \geqslant 3$.

(b) $1 + x_1 + x_2 + \lambda(1 + y_1 + y_2)$ avec $|\lambda| \geqslant 4$.

(c) On peut aussi mélanger les variables $1 + x_1 + x_2 + \lambda(1 + x_1 + y_2)$ avec $|\lambda| \geqslant 4$ (il faut vérifier que Ω est non vide).

(d) Le polynôme $x + y + z - 3xyz$, où $\Omega = \{(1, 1, 1), (-1, -1, -1)\}$, permet aussi de construire des exemples de suites récurrentes linéaires caractérisées par l'ensemble de leurs diviseurs premiers.

(e) Enfin, on trouvera dans [11] une étude de ce type de polynômes ; par exemple, le polynôme

$$T(x, y) = x^2y - 2xy^2 + 2x - y \quad \text{où} \quad \Omega = \{(-i, ji), (i, -ji), (-i, j^2i), (i, -j^2i)\}$$

(cf. [11], page 132), est donc un polynôme possédant les propriétés utilisées dans les lignes qui précèdent.

Bibliographie

[1] Ch. Ballot, *Density of primes divisors of linear recurrence*. Mem. Amer. Math. Soc. 115 (1995), no. 551.

[2] Z. I. Borevitch, I. R. Chafarevitch, *Théorie des nombres*. Gauthier–Villars, Paris 1967.

[3] J. W. S. Cassels, A. Fröhlich (ed.), *Algebraic Number Theory*. Academic Press, London 1967.

[4] C. Corralez Rodrigáñez, R. Schoof, *The support problem and its elliptic analogue*. J. Number Theory 64 (1997), 276–290.

[5] J.-H. Evertse, *On sums of S-units and linear recurrences*. Compositio Math. 53 (1984), 225–244.

[6] H. Hasse, *Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl* $a \neq 0$ *von gerader bzw. ungerader Ordnung* mod p *ist*. Math. Ann. 166 (1966), 19–23.

[7] J. C. Lagarias, *The set of primes dividing the Lucas numbers has density* 2/3. Pacific J. Math. 118 (1985), 449–461; *Errata*, ibid. 162 (1994), 393–396.

[8] S. Lang, *Algebraic Number Theory*. Addison Wesley, Reading 1970.

[9] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 2nd edition. Springer and PWN, Berlin and Warsaw, 1990.

[10] G. Pólya, *Arithmetische Eigenschaften Reihenentwicklungen rationaler Funktionen*. J. Reine Angew. Math. 151 (1921), 1–31.

[11] W. M. Ruppert, *Solving algebraic equations in roots of unity*. J. Reine Angew. Math. 435 (1993), 119–156.

[12] A. Schinzel, *On exponential congruences*. In: Diofantovy Priblizheniya, Matematicheskie Zapiski 2, Moskva 1996, 121–126 (Russian); this collection: H9, 996–1000.

[13] —, *Abelian binomials, power residues and exponential congruences*. Acta Arith. 32 (1977), 245–274; *Addendum*, ibid. 36 (1980), 101–104; this collection: H5, 939–970.

[14] I. Schur, *Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen*. Sitzungsber. Berlin. Math. Ges. II (1912), 40–50.

[15] T. Skolem, *On the existence of a multiplicative basis for an arbitrary algebraic field*. Norske Vid. Selsk. Forh. (Trondheim) 20 (1947), no. 2, 4–7.

Originally published in
Acta Arithmetica 108 (2003), 77–94

On power residues

with M. Skałba (*Warszawa*)

Let n be a positive integer, K a number field, $\alpha_i \in K$ $(1 \leqslant i \leqslant k)$, $\beta \in K$. A simple necessary and sufficient condition was given in [7] in order that, for almost all prime ideals $\mathfrak{p}$ of K, solubility of the k congruences $x^{n_i} \equiv \alpha_i \pmod{\mathfrak{p}}$ should imply solubility of the congruence $x^n \equiv \beta \pmod{\mathfrak{p}}$, where $n_i \mid n$. The aim of this paper is to extend that result to the case where the congruence $x^n \equiv \beta \pmod{\mathfrak{p}}$ is replaced by the alternative of l congruences $x^n \equiv \beta_j \pmod{\mathfrak{p}}$. The general result is quite complicated, but it simplifies if n or K satisfy some restrictions. Here are precise statements, in which ζ_n denotes a primitive nth root of unity, $|A|$ is the cardinality of a set A, $K^n = \{x^n : x \in K\}$ and $\mathcal{F}$ is the family of all subsets of $\{1, \dots, l\}$.

Theorem 1. *Let n and n_i be positive integers, $n_i \mid n$ $(1 \leqslant i \leqslant k)$, K be a number field and $\alpha_i, \beta_j \in K^*$ $(1 \leqslant i \leqslant k, 1 \leqslant j \leqslant l)$. Consider the implication*

(i) *solubility in K of the k congruences $x^{n_i} \equiv \alpha_i \pmod{\mathfrak{p}}$ implies solubility in K of at least one of the l congruences $x^n \equiv \beta_j \pmod{\mathfrak{p}}$.*

Then (i) *holds for almost all prime ideals $\mathfrak{p}$ of K if and only if*

(ii) *for every unitary divisor $m > 1$ of n and, if $n \equiv 0 \pmod 4$, for every $m = 2m^*$, where m^* is a unitary divisor of the odd part of n, there exists an involution σ_m of $\mathcal{F}$ such that for all $A \subset \{1, \dots, l\}$*

$$|\sigma_m(A)| \equiv |A| + 1 \pmod 2, \tag{1}$$

$$\prod_{j \in \sigma_m(A)} \beta_j = \prod_{j \in A} \beta_j \prod_{i=1}^{k} \alpha_i^{a_i m/(m,n_i)} \Gamma^m, \tag{2}$$

where $a_i \in \mathbb{Z}$, $\Gamma \in K(\zeta_m)^*$.

Corollary 1. *Let $w_n(K)$ be the number of n-th roots of unity contained in K and assume that*

$$(w_n(K), \operatorname{lcm}[K(\zeta_q) : K]) = 1, \tag{3}$$

where the least common multiple is over all prime divisors q of n and additionally $q = 4$ if $4 \mid n$. The implication (i) *holds for almost all prime ideals $\mathfrak{p}$ of K if and only if there exists*

an involution σ of $\mathcal{F}$ such that for all $A \subset \{1, \dots, l\}$

$$|\sigma(A)| \equiv |A| + 1 \pmod 2 \tag{4}$$

and

$$\prod_{j \in \sigma(A)} \beta_j = \prod_{j \in A} \beta_j \prod_{i=1}^{k} \alpha_i^{a_i n/n_i} \gamma^n, \tag{5}$$

where $a_i \in \mathbb{Z}$, $\gamma \in K^*$.

The condition (3) holds for every K if $n = 2$ or $n = l^e$, where l is an odd prime, and for $K = \mathbb{Q}$ if n is odd.

Corollary 2. *For $n = n_i = 2$ $(1 \leqslant i \leqslant k)$,* (i) *holds for almost all prime ideals $\mathfrak{p}$ of K if and only if*

(iii) *there exists a subset A_0 of $\{1, \dots, l\}$ such that*

$$|A_0| \equiv 1 \pmod 2 \tag{6}$$

and

$$\prod_{j \in A_0} \beta_j = \prod_{i=1}^{k} \alpha_i^{a_i} \gamma_0^2, \tag{7}$$

where $a_i \in \mathbb{Z}$, $\gamma_0 \in K^*$.

Corollary 2 contains as a special case ($K = \mathbb{Q}$, $k = 0$) a theorem of Fried [3], rediscovered by Filaseta and Richman [2].

The case $n = 2^e$ $(e \geqslant 2)$ is covered by the following corollary, in which τ denotes the greatest integer such that $\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} \in K$. This corollary is of interest only if $\zeta_4 \notin K$, otherwise (3) holds.

Corollary 3. *For $n = 2^e$ $(e \geqslant 2)$ and $n_i > 1$ $(1 \leqslant i \leqslant k)$,* (i) *holds for almost all prime ideals $\mathfrak{p}$ of K if and only if simultaneously* (iii) *holds and*

(iv) *there exists an involution σ of $\mathcal{F}$ such that for all $A \subset \{1, \dots, l\}$ we have* (4) *and*

$$\prod_{j \in \sigma(A)} \beta_j = \varepsilon \prod_{j \in A} \beta_j \cdot \prod_{i=1}^{k} \alpha_i^{a_i n/n_i} \gamma^n, \tag{8}$$

where $a_i \in \mathbb{Z}$, $\gamma \in K^*$ and

$$\varepsilon \in \begin{cases} \{1, -1\} & \text{if } e < \tau, \\ \{1, (-1)^{n/2^\tau} (\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{n/2}\} & \text{if } e \geqslant \tau. \end{cases} \tag{9}$$

The case $K = \mathbb{Q}$, n odd is covered by Corollary 1. The case $K = \mathbb{Q}$, n even is covered by the following

Theorem 2. *Let $n = 2^\nu n^*$, $\nu > 0$, n^* odd, $n_i \mid n$ $(1 \leqslant i \leqslant k)$, $K = \mathbb{Q}$.*
The implication (i) *holds for almost all prime ideals $\mathfrak{p}$ of K if and only if*

(v) *for every $m = 2^\nu m^*$ and, if $\nu = 2$, for every $m = 2m^*$, where m^* is a unitary divisor of n^*, there exists an involution σ_m of $\mathcal{F}$ such that for all $A \subset \{1, \dots, l\}$ we have* (1) *and*

$$\prod_{j \in \sigma_m(A)} \beta_j = \varepsilon \prod_{j \in A} \beta_j \prod_{i=1}^{k} \alpha_i^{a_i m/(m,n_i)} \delta^{m/2} \gamma^m,$$

where $a_i \in \mathbb{Z}$, $\gamma \in \mathbb{Q}^*$, δ is a fundamental discriminant dividing m and

$$\varepsilon \in \begin{cases} \{1, -2^{m/2}\} & \text{if } m \equiv 4 \pmod 8, \\ \{1\} & \text{otherwise.} \end{cases}$$

Corollary 4. *Let $n = 2^\nu n^*$, $\nu \geqslant 0$, n^* odd, $\beta_1, \beta_2 \in \mathbb{Q}^*$. The alternative of congruences*

$$x^n \equiv \beta_j \pmod p \quad (1 \leqslant j \leqslant 2)$$

is soluble for almost all primes p, if and only if either

$$\beta_i \in \mathbb{Q}^n \tag{10}$$

for some $i \leqslant 2$, or there is a $j \leqslant 2$, a prime $q \mid n^*$ with $q^e \parallel n^*$ and some $\gamma_1, \gamma_2 \in \mathbb{Q}$ such that one of the following holds:

- $\nu = 1$ *and*

$$\beta_j = \big((-1)^{(q-1)/2} q\big)^{n/2} \gamma_1^n, \quad \beta_{3-j} = \gamma_2^{n/q^e}, \tag{11}$$

- $\nu = 2$ *and either*

$$\beta_j = -2^{n/2} \gamma_1^n, \quad \beta_{3-j} = \gamma_2^{n/2} \tag{12}$$

or

$$\beta_j = q^{n/2} \gamma_1^n, \quad \beta_{3-j} \in \{\gamma_2^{n/q^e}, -2^{n/2q^e} \gamma_2^{n/q^e}\}, \tag{13}$$

- $\nu \geqslant 3$ *and either*

$$\beta_j = 2^{n/2} \gamma_1^n \tag{14}$$

or

$$\beta_j \in \{q^{n/2} \gamma_1^n, 2^{n/2} q^{n/2} \gamma_1^n\}, \quad \beta_{3-j} \in \{\gamma_2^{n/q^e}, 2^{n/2q^e} \gamma_2^{n/q^e}\}. \tag{15}$$

The proofs are based on eight lemmas and use the *n-th power residue symbol*, which is defined as follows. If a number field K contains ζ_n, then for every prime ideal $\mathfrak{p}$ of K prime to n and every $\mathfrak{p}$-adic unit α of K, $(\alpha|\mathfrak{p})_n$ is a unique number ζ_n^j that satisfies the congruence

$$\alpha^{(N\mathfrak{p}-1)/n} \equiv \zeta_n^j \pmod{\mathfrak{p}},$$

where $N\mathfrak{p}$ is the absolute norm of $\mathfrak{p}$. Moreover, $\operatorname{ind} \alpha$ is the index of α with respect to a fixed primitive root modulo the relevant prime ideal.

We give two proofs of Corollary 2, one short using Theorem 1 and the other longer, but using neither Theorem 1 nor the lemmas below, except the classical Lemma 3.

At the end of the paper we give a deduction of the more difficult necessity part of Theorem 1 of [7] from Theorem 1 above.

We thank Professor J. Browkin for some helpful suggestions.

Lemma 1. *Let G be a finite abelian group, $\widehat{G}$ its group of characters and $g_j \in G$ $(1 \leqslant j \leqslant l)$. If*

$$\prod_{j=1}^{l} (\chi(g_j) - 1) = 0 \tag{16}$$

for every $\chi \in \widehat{G}$ then there exists an involution σ of $\mathcal{F}$ such that for all $A \subset \{1, \ldots, l\}$ we have (4) *and*

$$\prod_{j \in \sigma(A)} g_j = \prod_{j \in A} g_j.$$

Proof. For $g \in G$ let

$$c(g) = \sum_{\substack{A \subset \{1,\ldots,l\} \\ \prod_{j \in A} g_j = g}} (-1)^{|A|}.$$

The equality (16) can be written in the form

$$\sum_{g \in G} c(g)\chi(g) = 0$$

or, if h is any fixed element of G,

$$\sum_{g \in G} c(g)\chi(gh^{-1}) = 0.$$

Summing over all characters χ gives $|G|c(h) = 0$, hence $c(h) = 0$, and h being arbitrary, $c(g) = 0$ for all $g \in G$. It follows that for all $g \in G$ the number of subsets A of $\{1, \ldots, l\}$ with $\prod_{j \in A} g_j = g$ and $|A|$ odd equals the corresponding number with $|A|$ even, hence there is an involution σ_g of the family of subsets A of $\{1, \ldots, l\}$ with $\prod_{j \in A} g_j = g$ such that

$$|\sigma_g(A)| \equiv |A| + 1 \pmod 2.$$

The involution σ is obtained by putting together all involutions σ_g, i.e., $\sigma(A) = \sigma_g(A)$ for $g = \prod_{j \in A} g_j$. □

Lemma 2. *Let n be a positive integer, K and L be number fields, $K(\zeta_n) \subset L$, $\beta_j \in K^*$ $(1 \leqslant j \leqslant l)$. Let H be the multiplicative group generated by $\beta_1, \ldots, \beta_l$, and H_1 the*

intersection of H with L^n. For every $\chi \in \widehat{H/H_1}$ there exists a set $\mathcal{P}$, with positive Dirichlet density, of prime ideals $\mathfrak{P}$ of L such that

$$\chi([x]) = (x|\mathfrak{P})_n. \tag{17}$$

where $[x]$ is the coset of H_1 in H containing x.

Proof. By a theorem of Skolem [9] the field L has a multiplicative basis $\zeta_w, \pi_1, \pi_2, \ldots$, where ζ_w is a root of unity and $\pi_1, \pi_2, \ldots$ are generators of infinite order. Let π_s be the last generator that occurs in the representation of $\beta_1, \ldots, \beta_l$. We have

$$H/H_1 < J/J^n,$$

where J is the group generated by $\zeta_w, \pi_1, \ldots, \pi_s$. Indeed, $H < J$ and the relations $h_1 \in H$, $h_2 \in H$ and $h_1 h_2^{-1} \in J^n$ together imply $h_1 h_2^{-1} \in H_1$. Hence for every $\chi \in \widehat{H/H_1}$ there exists $\chi_1 \in \widehat{J/J^n}$ such that

$$\chi(y) = \chi_1(y) \quad \text{for} \quad y \in H/H_1. \tag{18}$$

Clearly $\chi_1(y)^n = 1$ for all $y \in J/J^n$. On the other hand, by Theorem 4 of [8] with $\sigma = 1$, for any integers $c_0, \ldots, c_s$ there exist infinitely many prime ideals $\mathfrak{P}$ of L such that

$$(\zeta_w|\mathfrak{P})_n = \zeta_n^{c_0}, \quad (\pi_r|\mathfrak{P})_n = \zeta_n^{c_r} \ (1 \leqslant r \leqslant s).$$

Since the proof is via the Chebotarev density theorem (see [8], p. 263), the infinite set of prime ideals in question has a positive Dirichlet density. Hence for every $\chi_1 \in \widehat{J/J^n}$ there exists a set $\mathcal{P}$ of positive Dirichlet density such that for $\mathfrak{P} \in \mathcal{P}$,

$$\chi_1(\overline{x}) = (x|\mathfrak{P})_n \quad \text{for} \quad x \in J, \tag{19}$$

where $\overline{x}$ is the coset of J^n in J containing x. Since by (18),

$$\chi([x]) = \chi_1(\overline{x}) \quad \text{for} \quad x \in H,$$

(17) follows from (19). □

Lemma 3. *Let $n \in \mathbb{N}$, K be a number field, $\zeta_n \in K$, and $\alpha_1, \ldots, \alpha_k, \beta$ elements of K^*. If*

$$\sqrt[n]{\beta} \in K\left(\sqrt[n]{\alpha_1}, \ldots, \sqrt[n]{\alpha_k}\right),$$

then

$$\beta = \prod_{i=1}^{k} \alpha_i^{a_i} \gamma^n,$$

where $a_i \in \mathbb{Z}$, $\gamma \in K^*$.

Proof. See [5], p. 222, formula (2). □

Lemma 4. *The condition* (i) *for almost all prime ideals* $\mathfrak{p}$ *of* K *implies the existence of an involution* σ *of* $\mathcal{F}$ *such that, for all* $A \subset \{1, \dots, l\}$, (4) *holds and*

$$\prod_{j\in\sigma(A)} \beta_j = \prod_{j\in A} \beta_j \cdot \prod_{i=1}^{k} \alpha_i^{a_i n/n_i} \Gamma^n \quad \text{for some} \quad a_i \in \mathbb{Z},\ \Gamma \in K(\zeta_n)^*. \tag{20}$$

Proof. Let χ be a character of the group H/H_1 described in Lemma 2 with $L = K(\zeta_n, \xi_1, \dots, \xi_k)$, where $\xi_i^{n_i} = \alpha_i$ $(1 \leqslant i \leqslant k)$. By Lemma 2 there exists a set $\mathcal{P}$, with positive Dirichlet density, of prime ideals $\mathfrak{P}$ of L such that

$$(x|\mathfrak{P})_n = \chi([x]) \text{ for } x \in H, \tag{21}$$

where $[x]$ is the coset of H_1 in H containing x. Since prime ideals of degree greater than 1 have Dirichlet density 0 and relative norms of prime ideals from $\mathcal{P}$ have positive Dirichlet density, there is $\mathfrak{P} \in \mathcal{P}$ such that $\mathfrak{p} = N_{L/K}\mathfrak{P}$ has the property that solubility in K of the k congruences $x^{n_i} \equiv \alpha_i \pmod{\mathfrak{p}}$ implies solubility of at least one of the l congruences $x^n \equiv \beta_j \pmod{\mathfrak{p}}$. Moreover, the congruence $x^{n_i} \equiv \alpha_i \pmod{\mathfrak{P}}$ has the solution $x = \xi_i$ in L, hence, $\mathfrak{P}$ being of relative degree 1, the congruence $x^{n_i} \equiv \alpha_i \pmod{\mathfrak{p}}$ has a solution in K and, by (i),

$$\prod_{j=1}^{l} \big((\beta_j|\mathfrak{P})_n - 1\big) = 0.$$

By (21) we have

$$\prod_{j=1}^{l} \big(\chi([\beta_j]) - 1\big) = 0$$

and, χ being arbitrary, it follows by Lemma 1 that there exists an involution σ of $\mathcal{F}$ such that (4) holds and

$$\prod_{j\in\sigma(A)} [\beta_j] = \prod_{j\in A} [\beta_j].$$

The last formula means that

$$\prod_{j\in\sigma(A)} \beta_j \prod_{j\in A} \beta_j^{-1} = \Gamma_1^n \quad \text{for some } \Gamma_1 \in L. \tag{22}$$

Since $\Gamma_1^n \in K(\zeta_n)$, by Lemma 3 we have

$$\Gamma_1^n = \prod_{i=1}^{k} \alpha_i^{a_i n/n_i} \Gamma^n \quad \text{for some } a_i \in \mathbb{Z},\ \Gamma \in K(\zeta_n),$$

which together with (22) gives (20). □

Lemma 5. *If there exists an involution σ of $\mathcal{F}$ such that, for all $A \subset \{1,\dots,l\}$,* (4) *holds and*

$$\prod_{j\in\sigma(A)} \beta_j = \prod_{j\in A} \beta_j \cdot \prod_{i=1}^{k} \alpha_i^{a_i m/(m,n_i)} \Gamma^m \tag{23}$$

for some $a_i \in \mathbb{Z}$ and $\Gamma \in K(\zeta_m)$, then the implication (i) *holds for all prime ideals $\mathfrak{p}$ of K such that all α_i, β_j are $\mathfrak{p}$-adic units and $(N\mathfrak{p}-1, n) = m$.*

Proof. Let $\mathfrak{p}$ satisfy the assumptions of the lemma and assume that the k congruences $x^{n_i} \equiv \alpha_i \pmod{\mathfrak{p}}$, hence also $x^{(m,n_i)} \equiv \alpha_i \pmod{\mathfrak{p}}$, are soluble in K. Let g be a primitive root mod $\mathfrak{p}$ and Φ_m the m-th cyclotomic polynomial. We have

$$\Phi_m(x) \equiv \prod_{(k,m)=1} (x - g^{(N\mathfrak{p}-1)k/m}) \pmod{\mathfrak{p}},$$

hence, by Dedekind's theorem, $\mathfrak{p}$ has a prime ideal factor $\mathfrak{P}$ in $K(\zeta_m)$ of relative degree 1. Solubility in K of the congruences in question implies

$$\big(\alpha_i^{a_i m/(m,n_i)} | \mathfrak{P}\big)_m = 1 \quad (1 \leqslant i \leqslant k)$$

and, since $(\Gamma^m|\mathfrak{P})_m = 1$, by (23) we have

$$\Big(\prod_{j\in\sigma(A)} \beta_j \Big| \mathfrak{P}\Big)_m = \Big(\prod_{j\in A} \beta_j \Big| \mathfrak{P}\Big)_m,$$

hence

$$\begin{aligned} 2\prod_{j=1}^{l} \big(1 - (\beta_j|\mathfrak{P})_m\big) &= \sum_{A\subset\{1,\dots,l\}} \Big((-1)^{|A|}\Big(\prod_{j\in A} \beta_j \Big| \mathfrak{P}\Big)_m + (-1)^{|\sigma(A)|}\Big(\prod_{j\in\sigma(A)} \beta_j \Big| \mathfrak{P}\Big)_m\Big) \\ &= \sum_{A\subset\{1,\dots,l\}} \big((-1)^{|A|} + (-1)^{|\sigma(A)|}\big)\Big(\prod_{j\in A} \beta_j \Big| \mathfrak{P}\Big)_m = 0. \end{aligned}$$

Thus $(\beta_j|\mathfrak{P})_m = 1$ for at least one $j \leqslant l$. Since $\mathfrak{P}$ is of relative degree 1, this means that the congruence

$$x^m \equiv \beta_j \pmod{\mathfrak{p}}$$

is soluble in K. Choosing an integer t such that $(N\mathfrak{p}-1)t \equiv m \pmod{n}$ we have for every $\mathfrak{p}$-adic unit x of K,

$$x^{(N\mathfrak{p}-1)t} \equiv 1 \pmod{\mathfrak{p}},$$

hence the congruence $x^n \equiv \beta_j \pmod{\mathfrak{p}}$ is soluble in K. □

Lemma 6. *Let $m, n_i \in \mathbb{N}\ (1 \leqslant i \leqslant k)$ and $n_i = n_i' n_i''$, where $(n_i'', m) = 1$. Let $\alpha_i, \beta_j \in K^*$ $(1 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant l)$. If there exists a prime ideal $\mathfrak{p}_0$ of K such that $m, n_i, \alpha_i, \beta_j$ are $\mathfrak{p}_0$-adic units, the congruences*

$$x^{n_i'} \equiv \alpha_i \pmod{\mathfrak{p}_0} \quad (1 \leqslant i \leqslant k) \tag{24}$$

are soluble in K and the congruences

$$x^m \equiv \beta_j \pmod{\mathfrak{p}_0} \quad (1 \leqslant j \leqslant l) \tag{25}$$

are insoluble in K, then there exists a set $\mathcal{P}$, with positive Dirichlet density, of prime ideals of K such that for $\mathfrak{p} \in \mathcal{P}$ the congruences

$$x^{n_i} \equiv \alpha_i \pmod{\mathfrak{p}} \quad (1 \leqslant i \leqslant k) \tag{26}$$

are soluble in K and the congruences

$$x^m \equiv \beta_j \pmod{\mathfrak{p}} \quad (1 \leqslant j \leqslant l) \tag{27}$$

are insoluble in K.

Proof. Assume first that all n_i are prime powers, $n_i = l_i^{\nu_i}$, where l_i are primes and let

$$\begin{aligned} I_0 &= \{1 \leqslant i \leqslant k : l_i \mid m\}, \\ I_1 &= \{1 \leqslant i \leqslant k : l_i \mid N\mathfrak{p}_0 - 1\} \setminus I_0, \\ I_2 &= \{1 \leqslant i \leqslant k\} \setminus I_0 \setminus I_1. \end{aligned}$$

Let further $(N\mathfrak{p}_0 - 1, m) = m'$. We set

$$L = K\big(\zeta_{n_i},\ \sqrt[n_i]{\alpha_i}\ (1 \leqslant i \leqslant k), \zeta_{m'},\ \sqrt[m']{\beta_j}\ (1 \leqslant j \leqslant l)\big),$$

take $\mathfrak{P}_0$ to be a prime ideal factor of $\mathfrak{p}_0$ in L, and let S be the element of the Galois group of L/K such that

$$\vartheta^S \equiv \vartheta^{N\mathfrak{p}_0} \pmod{\mathfrak{P}_0}$$

for all $\mathfrak{P}_0$-adic units ϑ of L.

By the assumption about congruences (24) the congruence

$$x^{n_i} \equiv \alpha_i \pmod{\mathfrak{p}_0}$$

has a solution $x_i \in K$ for $i \in I_0$, hence there exists a zero A_i of $x^{n_i} - \alpha_i$ such that $A_i \equiv x_i \pmod{\mathfrak{P}_0}$ and then

$$A_i^S = A_i. \tag{28}$$

For $i \in I_1 \cup I_2$ and $1 \leqslant j \leqslant l$, we choose A_i and B_j to be arbitrary zeros of $x^{n_i} - \alpha_i$ and $x^{m'} - \beta_j$, respectively.

By the assumption about congruences (25) also the congruences

$$x^{m'} \equiv \beta_j \pmod{\mathfrak{p}_0} \quad (1 \leqslant j \leqslant l) \tag{29}$$

are insoluble in K. We have

$$\begin{gathered}\zeta_{m'}^{S} = \zeta_{m'}^{N\mathfrak{p}_0} = \zeta_{m'}, \quad \zeta_{n_i}^{S} = \zeta_{n_i}^{N\mathfrak{p}_0} \quad (1 \leqslant i \leqslant k), \\ A_i^S = \zeta_{n_i}^{a_i} A_i \quad (i \in I_1 \cup I_2), \quad B_j^S = \zeta_{m'}^{b_j} B_j \quad (1 \leqslant j \leqslant l),\end{gathered} \tag{30}$$

where $a_i, b_j \in \mathbb{Z}$. Since the congruences (25) are insoluble in K we have

$$b_j \not\equiv 0 \pmod{m'} \quad (1 \leqslant j \leqslant l). \tag{31}$$

Put now

$$n_0 = \operatorname{lcm}\{n_i : i \in I_1\}.$$

We have

$$1 + N\mathfrak{p}_0 + \ldots + N\mathfrak{p}_0^{n_0-1} = (N\mathfrak{p}_0^{n_0} - 1)/(N\mathfrak{p}_0 - 1) \equiv 0 \pmod{n_i} \quad (i \in I_1),$$
$$1 + N\mathfrak{p}_0 + \ldots + N\mathfrak{p}_0^{n_0-1} \equiv n_0 \pmod{m'}.$$

It follows from (28) that

$$A_i^{S^{n_0}} = A_i \quad (i \in I_0) \tag{32}$$

and from (30) and (31) that

$$A_i^{S^{n_0}} = \zeta_{n_i}^{a_i(1+N\mathfrak{p}_0+\ldots+N\mathfrak{p}_0^{n_0-1})} A_i = A_i \quad (i \in I_1 \cup I_2), \tag{33}$$

$$B_j^{S^{n_0}} = \zeta_{m'}^{b_j(1+N\mathfrak{p}_0+\ldots+N\mathfrak{p}_0^{n_0-1})} B_j = \zeta_{m'}^{b_j n_0} B_j \neq B_j \quad (1 \leqslant j \leqslant l), \tag{34}$$

$$\zeta_{m'}^{S^{n_0}} = \zeta_{m'}. \tag{35}$$

If now $\mathfrak{P}$ is a prime ideal of L such that the Frobenius symbol

$$\left[\frac{L/K}{\mathfrak{P}}\right] = S^{n_0}$$

and $\mathfrak{p}$ is the prime ideal of K divisible by $\mathfrak{P}$ we infer from (32)–(35) that the congruences (26) are soluble in K and the congruences

$$x^{m'} \equiv \beta_j \pmod{\mathfrak{p}} \quad (1 \leqslant j \leqslant l),$$

hence also the congruences (27), are insoluble in K. However, by Chebotarev's density theorem the set of relevant prime ideals $\mathfrak{p}$ has a positive Dirichlet density.

Consider now the general case. Let

$$n_i = \prod_{j=1}^{h_i} q_{ij} \tag{36}$$

where for each i, q_{ij} $(1 \leqslant j \leqslant h_i)$ are powers of distinct primes. Since the congruences (24) are soluble in K, for each $i \leqslant k$ and each j such that $(q_{ij}, m) \neq 1$ the congruence

$$x^{q_{ij}} \equiv \alpha_i \pmod{\mathfrak{p}_0}$$

is soluble in K. Now, by the already proved case of the lemma, there exists a set $\mathcal{P}$, with positive Dirichlet density, of prime ideals of K such that for each $\mathfrak{p} \in \mathcal{P}$ the congruences

$$x^{q_{ij}} \equiv \alpha_i \pmod{\mathfrak{p}} \quad (1 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant h_i)$$

are soluble, but the congruences (27) insoluble. Thus for all i, j we have

$$\operatorname{ind} \alpha_i \equiv 0 \pmod{(N\mathfrak{p} - 1, q_{ij})}.$$

It now follows from (36) that for all i,

$$\operatorname{ind} \alpha_i \equiv 0 \pmod{(N\mathfrak{p} - 1, n_i)},$$

hence the congruences (26) are soluble. □

Lemma 7. *Suppose that* (i) *holds for almost all prime ideals* $\mathfrak{p}$ *of* K.

(vi) *If* m *is a unitary divisor of* n, *then for almost all prime ideals* $\mathfrak{p}$ *of* K, *solubility in* K *of the* k *congruences*

$$x^{(m,n_i)} \equiv \alpha_i \pmod{\mathfrak{p}} \tag{37}$$

implies solubility in K *of at least one congruence*

$$x^m \equiv \beta_j \pmod{\mathfrak{p}} \quad (1 \leqslant j \leqslant l). \tag{38}$$

(vii) *If* $n \equiv 0 \pmod 4$ *and* $m = 2m^*$, *where* m^* *is a unitary divisor of the odd part of* n, *then for almost all prime ideals* $\mathfrak{p}$ *of* K, *solubility in* K *of the* k *congruences*

$$x^{(m,n_i)} \equiv \alpha_i \pmod{\mathfrak{p}}$$

implies solubility in K *of at least one congruence*

$$x^m \equiv -1 \pmod{\mathfrak{p}}, \quad x^m \equiv \beta_j \pmod{\mathfrak{p}} \quad (1 \leqslant j \leqslant l).$$

Proof. In order to prove statement (vi) assume to the contrary that there exists a prime ideal $\mathfrak{p}_0$ of K such that m, n_i, α_i and β_j are $\mathfrak{p}_0$-adic units, the congruences (37) are soluble and the congruences (38) are insoluble. We apply Lemma 6 with

$$n_i' = (m, n_i), \quad n_i'' = \frac{n_i}{(m, n_i)}.$$

The assumptions of the lemma are satisfied, since with our choice of m

$$(m, n_i'') = \frac{(m^2, n_i)}{(m, n_i)} = 1$$

and the assertion of the lemma contradicts the assumptions of Lemma 7.

A similar argument shows that if statement (vii) were false, there would exist a set $\mathcal{P}$, with positive Dirichlet density, of prime ideals of K such that for $\mathfrak{p} \in \mathcal{P}$ the congruences

$$x^{n_i^*} \equiv \alpha_i \pmod{\mathfrak{p}} \quad (1 \leqslant i \leqslant k) \tag{39}$$

would be soluble and the congruences

$$x^m \equiv -1 \pmod{\mathfrak{p}}, \quad x^m \equiv \beta_j \pmod{\mathfrak{p}} \quad (1 \leqslant j \leqslant l) \tag{40}$$

insoluble, where n_i^* is the greatest divisor of n_i not divisible by 4. However, insolubility of $x^m \equiv -1 \pmod{\mathfrak{p}}$ implies

$$\frac{N\mathfrak{p}-1}{2} = \operatorname{ind}(-1) \not\equiv 0 \pmod{(N\mathfrak{p}-1, m)},$$

hence for $m \equiv 2 \pmod 4$, $N\mathfrak{p} \equiv 3 \pmod 4$ and then solubility of (39) implies solubility of (26), while (40) is insoluble, contrary to the assumption of the lemma. □

Proof of Theorem 1. *Necessity.* The existence of an involution σ_m satisfying (1) and (2) for m being a unitary divisor of n follows at once from Lemma 4 and (vi). In order to prove the same for m of the form $2m^*$, where m^* is a unitary divisor of the odd part of n, denote by $\overline{m}$ the least unitary divisor of n divisible by m. Let G_m, resp. $G_{\overline{m}}$, be the multiplicative subgroup of K^* generated by $\alpha_i^{m/(m,n_i)}$ $(1 \leqslant i \leqslant k)$ and $K(\zeta_m)^{*m}$, resp. by $\alpha_i^{\overline{m}/(\overline{m},n_i)}$ $(1 \leqslant i \leqslant k)$ and $K(\zeta_{\overline{m}})^{*\overline{m}}$.

If $G_{\overline{m}} \subset G_m$, then it suffices to take $\sigma_m = \sigma_{\overline{m}}$.

If $G_{\overline{m}} \not\subset G_m$, let $\delta \in G_{\overline{m}} \setminus G_m$. We have

$$\delta = \prod_{i=1}^{k} \alpha_i^{a_i \overline{m}/(\overline{m},n_i)} \Gamma^{\overline{m}}, \tag{41}$$

where $a_i \in \mathbb{Z}$, $\Gamma \in K(\zeta_{\overline{m}})^*$. By Theorem 3 of [8] we have $\Gamma^{\overline{m}} = \Gamma_0^{\overline{m}}$ for some $\Gamma_0 \in K(\zeta_{4m^*})$. Taking norms of both sides of (41) with respect to $K(\zeta_m)$ and denoting the norm of Γ_0 by Γ_1 we obtain

$$\delta^2 = \prod_{i=1}^{k} \alpha_i^{2a_i \overline{m}/(\overline{m},n_i)} \Gamma_1^{\overline{m}},$$

hence

$$\delta = \pm \prod_{i=1}^{k} \alpha_i^{a_i \overline{m}/(\overline{m},n_i)} \Gamma_1^{\overline{m}/2},$$

and, since

$$\frac{m}{(m,n_i)} \,\Big|\, \frac{\overline{m}}{(\overline{m},n_i)}, \quad m \,\Big|\, \frac{\overline{m}}{2}, \quad \Gamma_1 \in K(\zeta_m), \quad \delta \notin G_m,$$

the plus sign is excluded and we have

$$-1 \notin G_m \quad \text{and} \quad \delta \equiv -1 \pmod{{}^{\times} G_m}.$$

Since $\delta \equiv 1 \pmod{{}^{\times} G_{\overline{m}}}$ it follows that

$$\left[G_{\overline{m}} : G_m \cap G_{\overline{m}}\right] = 2, \quad G_{\overline{m}} = (G_m \cap G_{\overline{m}}) \cup \delta(G_m \cap G_{\overline{m}}).$$

From the existence of $\sigma_{\overline{m}}$ satisfying (1) and (2) it follows that for each $B \in K^*$,

$$\sum_{A \in V(B)} (-1)^{|A|} + \sum_{A \in V(\delta B)} (-1)^{|A|} = 0, \tag{42}$$

where

$$V(B) = \Big\{ A \in \mathcal{F} : \prod_{j\in A} \beta_j \equiv B \pmod{{}^{\times} G_m \cap G_{\overline{m}}} \Big\}.$$

Let $S = \big\{ \prod_{j\in A} \beta_j : A \in \mathcal{F} \big\}$ and let $\{B_1, \dots, B_r\}$ be a subset of S maximal with respect to the property that

$$B_i \equiv B \pmod{{}^{\times} G_m}, \quad B_j \not\equiv B_i \pmod{{}^{\times} G_m \cap G_{\overline{m}}} \quad \text{for} \quad j \neq i.$$

Set

$$U(B) = \Big\{ A \in \mathcal{F} : \prod_{j\in A} \beta_j \equiv B \pmod{{}^{\times} G_m} \Big\}.$$

Replacing B by B_i in (42) and summing with respect to i we obtain

$$\sum_{A\in U(B)} (-1)^{|A|} + \sum_{A\in U(-B)} (-1)^{|A|} = 0.$$

However, from (vii) and Lemma 4 it follows that

$$\sum_{A\in U(B)} (-1)^{|A|} + \sum_{A\in U(-B)} (-1)^{|A|+1} = 0.$$

Adding the last two inequalities we obtain

$$2 \sum_{A\in U(B)} (-1)^{|A|} = 0,$$

hence there exists an involution ϱ_B of the family of all subsets A of $\{1, \dots, l\}$ with $\prod_{j\in A} \beta_j = B$, such that

$$|\varrho_B(A)| \equiv |A| + 1 \pmod 2.$$

The involution σ_m is obtained by combining all involutions ϱ_B.

Sufficiency. Consider a prime ideal $\mathfrak{p}$ of K such that α_i, β_j are all $\mathfrak{p}$-adic units and let

$$(N\mathfrak{p} - 1, n) = m_1. \tag{43}$$

If $m_1 = 1$ the implication (i) is obvious.

If $m_1 > 1$, $m_1 \not\equiv 0 \pmod 2$ or $m_1 \equiv 0 \pmod 4$, let m be the least unitary divisor of n divisible by m_1. By condition (ii) we have (1) and (2) where $\Gamma \in K(\zeta_m)$. However, $\Gamma^m \in K$, hence also

$$\Gamma^m \in K(\zeta_q : q \mid m,\ q \text{ prime or } q = 4) =: K_0.$$

It follows now from Theorem 3 of [8] that $\Gamma^m = \Gamma_0^m$, where $\Gamma_0 \in K_0$. However, by the definition of m, we have $K_0 \subset K(\zeta_{m_1})$ and also

$$\frac{m_1}{(m_1, n_i)} \;\Big|\; \frac{m}{(m, n_i)}.$$

The implication (i) follows now from Lemma 5.

If $m_1 \equiv 2 \pmod 4$, we take $m = 2m^*$, where m^* is the least unitary divisor of n divisible by $m_1/2$, and argue as before. □

Proof of Corollary 1. Under the assumption (3) the conditions $\Gamma^n \in K$, $\Gamma \in K(\zeta_n)$ imply, by Theorem 3 of [8], that $\Gamma^n = \gamma^n$, $\gamma \in K$, hence for $\sigma = \sigma_n$, (1) implies (4) and (2) implies (5). □

First proof of Corollary 2. The necessity of condition (iii) follows from Corollary 1 on taking $A_0 = \sigma(\emptyset)$. Conversely, if (iii) holds, then we define the involution σ in Corollary 1 by $\sigma(A) = A \div A_0$ ($\div$ denotes the symmetric difference) and notice that

$$\prod_{j\in\sigma(A)} \beta_j = \prod_{j\in A} \beta_j \prod_{i=1}^{k} \alpha_i^{a_i} \Big(\gamma_0 \prod_{j\in A\cap A_0} \beta_j\Big)^2,$$

hence (4) and (5) are satisfied and, by Corollary 1, (i) holds for almost all prime ideals $\mathfrak{p}$ of K. □

Second (*direct*) *proof of Corollary* 2. In order to prove the necessity of the condition, choose a maximal subset $\{i_1, \dots, i_s\}$ of $\{1, \dots, l\}$ such that

$$\prod_{r=1}^{s} \beta_{i_r}^{e_r} \in L^2, \text{ where } L = K(\sqrt{\alpha_1}, \dots, \sqrt{\alpha_k}),$$

implies $e_r \equiv 0 \pmod 2$ $(1 \leqslant r \leqslant s)$.

By the theorem of Chebotarev [1] there exists a set $\mathcal{P}$, with positive Dirichlet density, of prime ideals $\mathfrak{P}$ of L of degree 1 such that

$$(\beta_{i_r}|\mathfrak{P})_2 = -1 \quad (1 \leqslant r \leqslant s). \tag{44}$$

Let $\mathfrak{p}$ be the prime ideal of K divisible by $\mathfrak{P}$. Since $\mathfrak{P}$ is of degree 1 and the k congruences $x^2 \equiv \alpha_i \pmod{\mathfrak{P}}$ are soluble in L, they are soluble in K and, by the implication,

$$(\beta_j|\mathfrak{p})_2 = 1 \quad \text{for at least one } j \leqslant k. \tag{45}$$

On the other hand, for each $j \leqslant l$, by the maximality of $\{i_1, \dots, i_s\}$ we have

$$\beta_j = \prod_{r=1}^{s} \beta_{i_r}^{e_{jr}} \gamma_j^2, \quad e_{jr} \in \{0, 1\},\ \gamma_j \in L. \tag{46}$$

If for each j we have

$$\sum_{r=1}^{s} e_{jr} \equiv 1 \pmod 2,$$

then the formulae (44) and (46) imply $(\beta_j|\mathfrak{P})_2 = -1$, contrary to (45). If for a certain j_0 we have

$$\sum_{r=1}^{s} e_{j_0 r} \equiv 0 \pmod 2,$$

then taking $A_0 = \{i_r : e_{j_0 r} = 1\} \div \{j_0\}$ we get (6) and

$$\prod_{j \in A_0} \beta_j = \begin{cases} \beta_{j_0}^2 \gamma_{j_0}^{-2} & \text{if } j_0 \in A_0, \\ \gamma_{j_0}^{-2} & \text{if } j_0 \notin A_0. \end{cases} \tag{47}$$

However, since $\gamma_{j_0}^{-2} \in K$, it follows by Lemma 3 that

$$\gamma_{j_0}^{-2} = \prod_{i=1}^{k} \alpha_i^{a_i} \gamma^2, \quad \text{for some } a_i \in \mathbb{Z},\ \gamma \in K,$$

which together with (47) implies (7).

In order to prove the sufficiency of the condition, let $\mathfrak{p}$ be a prime ideal of K such that α_i and β_j are $\mathfrak{p}$-adic units and the k congruences $x^2 \equiv \alpha_i \pmod{\mathfrak{p}}$ are soluble in K. Then (7) gives

$$\prod_{j \in A_0} (\beta_j | \mathfrak{p})_2 = 1 \neq (-1)^{|A_0|},$$

hence $(\beta_j | \mathfrak{p})_2 = 1$ for at least one $j \in A_0$. □

Proof of Corollary 3. *Necessity.* For $n = 2^e$, by a theorem of Hasse [4] (see also Lemma 6 in [8]), $\Gamma^n \in K$ with $\Gamma \in K(\zeta_n)$ implies $\Gamma^n = \varepsilon \gamma^n$, where ε is given by (9) and $\gamma \in K$, hence (iv) follows from (ii) for $\sigma = \sigma_n$. Also (iii) follows from (ii), on taking $m = 2$ and $A_0 = \sigma_2(\emptyset)$.

Sufficiency. There is only one unitary divisor $m > 1$ of $n = 2^e$, namely $m = n$, and for this m, (ii) follows from (iv) by the theorem of Hasse quoted above, used in the opposite direction. For $m = 2$, (ii) follows from (iii) on taking $\sigma_2(A) = A \div A_0$. □

Lemma 8. *Let m be even and $\alpha \in \mathbb{Q}^*$. Then $\alpha \in \mathbb{Q}(\zeta_m)^m$ if and only if*

$$\alpha = \varepsilon \delta^{m/2} \gamma^m,$$

where $\gamma \in \mathbb{Q}^*$, δ is a fundamental discriminant dividing m and

$$\varepsilon \in \begin{cases} \{1, -2^{m/2}\} & \text{if } m \equiv 4 \pmod 8, \\ \{1\} & \text{otherwise.} \end{cases}$$

Proof. This is a reformulation of a lemma of Mills [6]. □

Proof of Theorem 2. The necessity of the conditions follows at once from Theorem 1 and Lemma 8. In order to prove the sufficiency we consider the cases $\nu \leqslant 2$ and $\nu \geqslant 3$ separately. If $\nu \leqslant 2$, then (ii) follows from (v) and Lemma 8 for every even unitary divisor m of n. For an odd unitary divisor m of n it suffices to take $\sigma_m = \sigma_{2m}$.

For $\nu \geqslant 3$ and $m \not\equiv 2 \pmod 4$, (ii) follows as before, while for $m \equiv 2 \pmod 4$ it suffices to take $\sigma_m = \sigma_n$. Indeed, for $\nu \geqslant 3$ we have $\varepsilon = 1$ and for every number of the form $\varepsilon \delta^{n/2} \gamma^n$ with $\delta, \gamma \in \mathbb{Q}$ belongs to $\mathbb{Q}^m$. □

Proof of Corollary 4. *Necessity.* In the case $\nu = 0$ the assertion follows at once from Corollary 1. We shall consider in detail only the case $\nu = 1$; the proof in other cases is similar and will be only indicated briefly.

Applying Theorem 2 for $\nu = 1$ and $m = n$ we infer that for $\{j\} = \sigma_n(\emptyset)$,

$$\beta_j = \delta_n^{n/2}\gamma_n^n \quad \text{for some } \gamma_n \in \mathbb{Q}, \tag{48}$$

where δ_n is a fundamental discriminant dividing n. If $\delta_n = 1$ we have $\beta_j \in \mathbb{Q}^n$, hence (10) with $i = j$.

If $\delta_n = (-1)^{(q-1)/2}q$, where q is an odd prime, we have β_j as in (11). Now we apply Theorem 2 for $m_0 = 2$ and $m_1 = n/q^e$. If $\sigma_{m_i}(\emptyset) = \{j\}$ then

$$\beta_j = \delta_{m_i}^{m_i/2}\gamma_i^{m_i} \quad \text{for some } \gamma_i \in \mathbb{Q} \quad (i = 0, 1), \tag{49}$$

where δ_{m_i} is a fundamental discriminant dividing m_i. Now the equations (48) and (49) are incompatible, since denoting by $k(x)$ the square-free kernel of an integer x, we have

$$k(\delta_{m_i}^{m_i/2}\gamma_i^{m_i}) = \delta_{m_i} \neq \delta_n = k(\delta_n^{n/2}\gamma_n^n).$$

Therefore, $\sigma_{m_i}(\emptyset) = \{3 - j\}$ $(i = 0, 1)$ and we obtain

$$\beta_{3-j} = \delta_{m_i}^{m_i/2}\gamma_i^{m_i} \quad (i = 0, 1).$$

We have $\delta_{m_0} = 1$, hence $\beta_{3-j} \in \mathbb{Q}^{[2,n/2q^e]} = \mathbb{Q}^{n/q^e}$, which proves (11).

Suppose now that δ_n has at least two distinct prime factors q_1 and q_2 and $q_i^{e_i} \parallel n$. Applying Theorem 2 for $m_0 = 2$, $m_i = n/q_i^{e_i}$ $(i = 1, 2)$ we obtain, as before, $\sigma_{m_i}(\emptyset) = \{3 - j\}$ $(i = 0, 1, 2)$. Then

$$\beta_{3-j} \in \mathbb{Q}^2 \cap \bigcap_{i=1}^{2} \mathbb{Q}^{n/2q_i^{e_i}},$$

hence $\beta_{3-j} \in \mathbb{Q}^n$, which gives (10) with $i = 3 - j$.

For $\nu = 2$, let $\sigma_n(\emptyset) = \{j\}$.

If $\varepsilon = 1$ and $\delta_n = 1$ or -4 we obtain (10) with $i = j$.

If $\varepsilon = -2^{n/2}$ and $\delta_n = 1$ or -4 we consider $m_0 = 2$, $m_1 = n/2$ and obtain (12).

If $\varepsilon = -2^{n/2}$ and $\delta_n \neq 1, -4$ we consider $m_0 = 4$, $m_1 = n/2$ and obtain (10) with $i = 3 - j$.

If $\varepsilon = 1$ and δ_n has one odd prime factor q we consider $m_0 = 4$, $m_1 = n/q^e$ and obtain (13).

If $\varepsilon = 1$ and δ_n has at least two odd prime factors q_1, q_2 we consider $m_0 = 4$, $m_i = n/q_i^{e_i}$ $(i = 1, 2)$ and obtain (12) with j and $3 - j$ interchanged.

For $\nu \geqslant 3$ let $\sigma_n(\emptyset) = \{j\}$ and

$$\beta_j = \delta_n^{n/2}\gamma_n^n.$$

If $\delta_n = 1$ or -4 we obtain the case (10) with $i = j$.

If $\delta_n = \pm 8$ we obtain the case (14). If δ_n has one odd prime factor q we consider $m_0 = 2^\nu$, $m_1 = n/q^e$ and obtain (15). If δ_n has at least two odd prime factors q_1 and q_2 we consider $m_0 = 2^\nu$, $m_i = n/q_i^{e_i}$ $(i = 1, 2)$ and obtain (10) with $i = 3 - j$ or (14) with $3 - j$ in place of j.

Sufficiency. If (10) holds then for each relevant divisor m of n we take $\sigma_m = c_i d_i$, where c_i, d_i are the cycles $(\emptyset \to \{i\})$ and $(\{3-i\} \to \{1,2\})$, respectively.

If (11) holds, we take

$$\sigma_m = \begin{cases} c_j d_j & \text{if } q \mid m, \\ c_{3-j} d_{3-j} & \text{if } q \nmid m. \end{cases}$$

If (12) holds, we take

$$\sigma_m = \begin{cases} c_j d_j & \text{if } 4 \mid m, \\ c_{3-j} d_{3-j} & \text{if } 4 \nmid m. \end{cases}$$

If (13) holds, we take

$$\sigma_m = \begin{cases} c_j d_j & \text{if } q \mid m, \text{ or } 4 \nmid m, \\ c_{3-j} d_{3-j} & \text{if } q \nmid m \text{ and } 4 \mid m. \end{cases}$$

If (14) holds, we take

$$\sigma_m = c_j d_j.$$

If (15) holds, we take

$$\sigma_m = \begin{cases} c_j d_j & \text{if } q \mid m, \\ c_{3-j} d_{3-j} & \text{if } q \nmid m. \end{cases}$$

□

Deduction of Theorem 1 *of* [7] (*necessity part*) *from Theorem* 1 (*above*). Let $n = \prod_{j=0}^{l} p_j^{e_j}$, where $p_0 = 2$, p_j are distinct odd primes and $e_j > 0$ for $j > 0$. Applying Theorem 1 above with $m = p_j^{e_j}$ we infer that

$$\beta = \prod_{i=1}^{k} \alpha_i^{a_{ij} p_j^{e_j} / (n_i, p_j^{e_j})} \Gamma_j^{p_j^{e_j}} \tag{50}$$

for some $a_{ij} \in \mathbb{Z}$ and $\Gamma_j \in K(\zeta_{p_j^{e_j}})$ (for $m = 1$ the conclusion is trivial). By the theorem of Hasse [4] (see [8], Lemma 6)

$$\Gamma_j^{p_j^{e_j}} = \varepsilon \gamma_j^{p_j^{e_j}} \quad \text{for some } \gamma_j \in K,\ \varepsilon_j = 1 \text{ for } j > 0 \tag{51}$$

and

$$\begin{aligned} \varepsilon_0 &\in \{1\} && \text{if } e_0 \leqslant 1, \\ \varepsilon_0 &\in \{1, -1\} && \text{if } 1 < e_0 < \tau, \\ \varepsilon_0 &\in \left\{1, (-1)^{2^{\varepsilon_0 - \tau}} (\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{2^{\varepsilon_0 - 1}}\right\} && \text{if } e_0 \geqslant \tau. \end{aligned} \tag{52}$$

We take integers $u_0, \dots, u_l$ satisfying the linear equation

$$\sum_{j=0}^{l} \frac{n}{p_j^{e_j}} u_j = 1$$

and set

$$\gamma = \prod_{j=0}^{l} \gamma_j^{u_j}.$$

By (50) and (51) we have

$$\gamma^n = \prod_{j=0}^{n} \left(\gamma_j^{p_j^{e_j}}\right)^{nu_j/p_j^{e_j}} = \beta \varepsilon_0^{-nu_0/2^{\varepsilon_0}} \prod_{j=0}^{l} \prod_{i=1}^{k} \alpha_i^{-a_{ij} nu_j/(n_i, p_j^{e_j})},$$

hence

$$\beta \prod_{i=1}^{k} \alpha_i^{m_i n/n_i} = \varepsilon^{nu_0/2^{\varepsilon_0}} \gamma^n \tag{53}$$

for some $m_i \in \mathbb{Z}$, $\gamma \in K^*$.

If $e_0 \leqslant 1$, or $e_0 > \tau$, or $\varepsilon_0 = 1$, or u_0 is even, we obtain, by (51), condition (i) or (iv) of Theorem 1 of [7]. If $1 < e_0 \leqslant \tau$, $\varepsilon \neq 1$ and u_0 is odd we apply Theorem 1 above with $m = 2$. We obtain

$$\beta = \prod_{2|n_i} \alpha_i^{a_i} \gamma^2,$$

which combined with (53) gives, by (52),

$$\prod_{2|n_i} \alpha_i^{l_i} = -\delta^2$$

and

$$\beta \prod_{i=1}^{k} \alpha_i^{m_i n/n_i} = \begin{cases} -\gamma^n & \text{if } 1 < e_0 < \tau, \\ -\left(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2\right)^{n/2} \gamma_1^n & \text{if } e_0 = \tau, \end{cases}$$

for some $\delta, \gamma_1 \in K^*$. These are just conditions (ii) and (iii) of Theorem 1 of [7]. The proof that conditions (i)–(iv) are sufficient is easy. □

References

[1] N. G. Chebotarev, *Über einen Satz von Hilbert*. Vestnik Ukr. Akad. Nauk, 1923, 3–7; Sobranie Sochineniĭ I, Izd. Akad. Nauk SSSR, Moscow–Leningrad 1949–50, 14–17.

[2] M. Filaseta, D. R. Richman, *Sets which contain a quadratic residue modulo p for almost all p*. Math. J. Okayama Univ. 31 (1989), 1–8.

[3] M. Fried, *Arithmetical properties of value sets of polynomials*. Acta Arith. 15 (1969), 91–115.

[4] H. Hasse, *Zum Existenzsatz von Grunwald in der Klassenkörpertheorie*. J. Reine Angew. Math. 188 (1950), 40–64.

[5] —, *Vorlesungen über Klassenkörpertheorie*. Physica-Verlag, Würzburg 1967.

[6] W. H. Mills, *Characters with preassigned values*. Canad. J. Math. 15 (1963), 169–171.

[7] A. Schinzel, *On power residues and exponential congruences*. Acta Arith. 27 (1975), 397–420; this collection: H4, 915–938.

[8] —, *Abelian binomials, power residues and exponential congruences*. Acta Arith. 32 (1977), 245–274; *Addendum*, ibid. 36 (1980), 101–104; this collection: H5, 939–970.

[9] Th. Skolem, *On the existence of a multiplicative basis for an arbitrary algebraic field*. Norske Vid. Selsk. Forh. (Trondheim) 20 (1947), no. 2, 4–7.

Part I

Primitive divisors

Commentary on I: Primitive divisors

by C. L. Stewart

Let a and b be coprime integers with $|a| > |b| > 0$ and let n be a positive integer. A prime p is said to be a primitive divisor of $a^n - b^n$ if p divides $a^n - b^n$ but does not divide $a^m - b^m$ for any positive integer m which is smaller than n. The study of primitive divisors had its origins in the work of Bang [1], Zsigmondy [18] and Birkhoff and Vandiver [3] from 1886, 1892 and 1904 respectively. It follows from their analysis that the primitive divisors of $a^n - b^n$ are the prime factors of the n-th cyclotomic polynomial evaluated at a and b, $\Phi_n(a, b)$, with at most one exception. The exception, if it exists, is a prime factor of n. Gauss [7] and Dirichlet [6] factorized the polynomial $\Phi_n(x, 1)$ over a suitable quadratic number field. Aurifeuille and Le Lasseur (see [1]) deduced from it explicit non-trivial factorizations of the number $\Phi_n(x, y)$ for certain integers n, x and y. Factorizations of the type they considered are now known as Aurifeuillian factorizations. In a paper **I1** written during a stay at Trinity College in Cambridge in 1961, Schinzel gave some new Aurifeuillian factorizations. In addition, he used Aurifeuillian factorizations to give conditions under which $a^n - b^n$ has at least two primitive divisors. Stevenhagen [15] and Brent [4] have shown how to efficiently compute the factorizations given by Schinzel in **I1**. In [8], Granville and Pleasants show that Schinzel determined all possible such Aurifeuillian factorizations.

One may extend the notion of a primitive divisor to sequences of Lucas numbers and sequences of Lehmer numbers. In 1913 Carmichael [5] proved that if u_n is the n-th term, for $n > 12$, of a Lucas sequence whose associated characteristic polynomial has real roots and coprime coefficients then u_n possesses a primitive divisor. Rotkiewicz [13], in 1962, generalized Schinzel's argument of **I1** to give conditions under which u_n has at least two primitive divisors.

In 1930 Lehmer [10] introduced sequences which are more general than Lucas sequences but retain their striking divisibility properties and these sequences are now referred to as Lehmer sequences. Twenty-five years later Ward [17] established the analogue of Carmichael's result for Lehmer sequences. In a sequence of three papers **I2**, **I3** and **I4** Schinzel used the Aurifeuillian factorizations from **I1** to establish conditions under which Lucas or Lehmer numbers have at least k primitive prime factors with k equal to 2, 3, 4, 6 or 8.

Let A and B be non-zero integers in an algebraic number field K and let n be a positive integer. A prime ideal of the ring of algebraic integers of K is said to be a primitive divisor

of $A^n - B^n$ if it divides the ideal generated by $A^n - B^n$ but does not divide the ideal generated by $A^m - B^m$ for any positive integer m with $m < n$. In **I5** Schinzel proves that if A and B are non-zero coprime algebraic integers whose quotient is not a root of unity then $A^n - B^n$ has a primitive divisor provided that n exceeds $N(d)$, a number which is effectively computable in terms of d where d is the degree of A/B over $\mathbb{Q}$. In 1968 Postnikova and Schinzel [12] proved a weaker version of this result where $N(d)$ was replaced by $N(A, B)$, a number which is effectively computable in terms of A and B. The case $d = 2$ is of considerable interest since it gives information on non-degenerate Lucas and Lehmer sequences whose associated characteristic polynomial has coprime coefficients. In particular, if u_n is the n-th term of such a sequence and n exceeds $N(2)$ then u_n has a primitive divisor. Schinzel [14] had earlier established that u_n has a primitive divisor if n exceeds a number which is effectively computable in terms of the coefficients of the associated characteristic polynomial of the sequence. Stewart [16] proved that one may take $N(d) = \max\{2(2^d - 1), e^{452}d^{67}\}$ and that there are only finitely many such Lehmer sequences whose n-th term, $n > 6$, $n \neq 8$, 10 or 12, does not possess a primitive divisor; for Lucas sequences the appropriate requirement is $n > 4$, $n \neq 6$. Further these sequences may be determined by solving certain Thue equations. Bilu, Hanrot and Voutier [2] used a theorem of Laurent, Mignotte and Nesterenko [9] concerning lower bounds for linear forms in the logarithms of two algebraic numbers, as elaborated by Mignotte [2], to help explicitly determine all such exceptional Lucas and Lehmer sequences. In particular, they proved that if n exceeds 30 and u_n is a Lucas or Lehmer number, from a sequence as above, then u_n has a primitive prime factor.

Let A, B and d be as above and let k be a positive integer, ζ_k be a primitive k-th root of unity and K be an algebraic number field containing A, B and ζ_k. In **I6** Schinzel proves that for each positive real number ε there exists a positive number c which depends on d and ε such that if n exceed $c(1 + \log k)^{1+\varepsilon}$ then there is a prime ideal of the ring of algebraic integers of K that divides $A^n - \zeta_k B^n$ but does not divide $A^m - \zeta_k^j B^m$ for $m < n$ and any integer j. The case when $k = 1$ is the main result of **I5**.

References

[1] A. S. Bang, *Taltheoretiske Undersøgelser*. Tidsskrift for Mat. 4 (1886), 70–80, 130–137.

[2] Yu. Bilu, G. Hanrot, P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, with an appendix by M. Mignotte. J. Reine Angew. Math. 539 (2001), 75–122.

[3] G. D. Birkhoff, H. S. Vandiver, *On the integral divisors of* $a^n - b^n$. Ann. of Math. (2) 5 (1904), 173–180.

[4] R. P. Brent, *On computing factors of cyclotomic polynomials*. Math. Comp. 61 (1993), 131–149.

[5] R. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$ Ann. of Math. (2) 15 (1913), 30–70.

[6] P. G. Lejeune Dirichlet, *Vorlesungen über Zahlentheorie*, 4th ed. Friedr. Vieweg & Sohn, Braunschweig 1894.

[7] C. F. Gauss, *Disquisitiones Arithmeticae*. G. Fleischer, Leipzig 1801.

[8] A. Granville, P. Pleasants, *Aurifeuillian factorization*. Math. Comp. 75 (2006), 497–508.

[9] M. Laurent, M. Mignotte, Yu. Nesterenko, *Formes linéaires en deux logarithmes et déterminants d'interpolation*. J. Number Theory 55 (1995), 285–321.

[10] D. H. Lehmer, *An extended theory of Lucas' functions*. Ann. of Math. (2) 31 (1930), 419–448.

[11] E. Lucas, *Théorèmes d'arithmétique*. Atti. R. Acad. Sci. Torino 13 (1877–78), 271–284.

[12] L. P. Postnikova, A. Schinzel, *Primitive divisors of the expression $a^n - b^n$ in algebraic number fields*. Mat. Sb. (N.S.) 75 (117) (1968), 171–177 (Russian); English transl.: Math. USSR-Sb. 4 (1968), 153–159.

[13] A. Rotkiewicz, *On Lucas numbers with two intrinsic divisors*. Bull. Acad. Polon. Sci. Sér. Sci. Math. Astr. Phys. 10 (1962), 229–232.

[14] A. Schinzel, *The intrinsic divisors of Lehmer numbers in the case of negative discriminant*. Ark. Mat. 4 (1962), 413–416.

[15] P. Stevenhagen, *On Aurifeuillian factorizations*. Nederl. Akad. Wetensch. Indag. Math. 49 (1987), 451–468.

[16] C. L. Stewart, *Primitive divisors of Lucas and Lehmer numbers*. In: Transcendence Theory: Advances and Applications, Academic Press, London 1977, 79–92.

[17] M. Ward, *The intrinsic divisors of Lehmer numbers*. Ann. of Math. (2) 62 (1955), 230–236.

[18] K. Zsigmondy, *Zur Theorie der Potenzreste*. Monatsh. Math. 3 (1892), 265–284.

Originally published in
Proceedings of the Cambridge Philosophical Society
58 (1962), 555–562

On primitive prime factors of $a^n - b^n$

1.

Let a, b be relatively prime integers with $|a| > |b| > 0$. For any integer $n > 0$, let $\phi_n(a, b)$ denote the n-th cyclotomic polynomial, defined by

$$\phi_n(a, b) = \prod_{\substack{r=1 \\ (r,n)=1}}^{n} (a - \zeta_n^r b),$$

where ζ_n is a primitive n-th root of unity.

A prime is called a *primitive prime factor of* $a^n - b^n$ if it divides this number but does not divide $a^\nu - b^\nu$ for $0 < \nu < n$. Zsigmondy [14] proved, and Birkhoff and Vandiver [4] and Kanold [8] rediscovered, the following theorem (see [6], p. 195): the primitive prime factors of $a^n - b^n$ coincide with the prime factors of $\phi_n(a, b)$, except for a possible prime q_1 which may divide $\phi_n(a, b)$ (to the first power only) and also divide n, and may be a primitive prime factor of $a^\sigma - b^\sigma$, where $\sigma = n/q_1^\kappa$ and $(q_1, \sigma) = 1$. If there is such a prime q_1, then $q_1 = q(n)$, the greatest prime factor of n, since $\sigma \mid (q_1 - 1)$, whence $\sigma < q_1$.

There is at least one primitive prime factor of $a^n - b^n$ except in the following cases:

$$n = 1, \quad a - b = 1; \qquad n = 2, \quad a + b = \pm 2^\mu \quad (\mu \geqslant 1);$$
$$n = 3, \quad a = \pm 2, \quad b = \mp 1; \qquad n = 6, \quad a = \pm 2, \quad b = \pm 1.$$

If $\phi_n(a, b)$ is a prime, it is of course for $n > 6$ the only primitive prime factor of $a^n - b^n$. It is not obvious even that for every pair a, b there exists some n such that $a^n - b^n$ has two primitive prime factors. In the present paper we give conditions which will ensure that $a^n - b^n$ has at least two primitive prime factors, and in particular we prove that there are infinitely many n for which this happens. The last assertion is an immediate consequence of our main result, which follows. We use $k(n)$ to denote the square-free kernel of n, that is, n divided by its greatest square factor.

Theorem 2. *Let*

$$\eta = \begin{cases} 1 & \text{if } k(ab) \equiv 1 \pmod 4, \\ 2 & \text{if } k(ab) \equiv 2 \text{ or } 3 \pmod 4. \end{cases}$$

Communicated by H. Davenport

If $n/\eta k(ab)$ is an odd integer, then $a^n - b^n$ has at least two primitive prime factors except in the following cases:

$n = 1$; $a = \pm(2^\alpha + 1)^2,\ b = \pm(2^\alpha - 1)^2$ *or* $4a = \pm(p^\alpha + 1)^2,\ 4b = \pm(p^\alpha - 1)^2$;

$n = 2$; *same but with* $\mp$ *for* b *instead of* $\pm$;

$n = 3$; $|a| = \pm 3,\ b = \mp 1$ *or* $a = \pm 4,\ b = \pm 1$ *or* $a = \pm 4,\ b = \mp 3$;

$n = 4$; $|a| = 2,\ |b| = 1$;

$n = 6$; $a = \pm 3,\ b = \pm 1$ *or* $a = \pm 4,\ b = \mp 1$ *or* $a = \pm 4,\ b = \pm 3$;

$n = 12$; $|a| = 2,\ |b| = 1$ *or* $|a| = 3,\ |b| = 2$;

$n = 20$; $|a| = 2,\ |b| = 1$.

This theorem represents a continuation of the line of arithmetical investigations pursued by Aurifeuille and Le Lasseur [1], Lucas [11], Bickmore [3], Cunningham [5], Kraĭtchik ([9], [10], pp. 87–91), Rotkiewicz [13].

2.

The proof of Theorem 2 is based on the following properties of the cyclotomic polynomials. We write $\phi_n(x)$ for $\phi_n(x, 1)$, and similarly for other polynomials later.

Theorem 1. *Let $n > 1$ be square-free and let m be a divisor of n such that n/m is odd. Then there exist polynomials $P_{n,m}(x)$, $Q_{n,m}(x)$ with integral coefficients such that* ([1])

$$\phi_n(x) = P_{n,m}^2(x) - (-1|m)mx\,Q_{n,m}^2(x) \qquad (m \text{ odd}), \tag{1}$$

$$\phi_{2n}(x) = P_{n,m}^2(-x) + (-1|m)mx\,Q_{n,m}^2(-x) \qquad (m \text{ odd}), \tag{2}$$

$$\phi_{2n}(x) = P_{n,m}^2(x) - mx\,Q_{n,m}^2(x) \qquad (m \text{ even}). \tag{3}$$

Further, these polynomials can be found from the following formulae (where $\sqrt{c} \geqslant 0$ if $c \geqslant 0$ and $\sqrt{c} = i\sqrt{|c|}$ if $c < 0$):

$$P_{n,m}(x^2) - \big\{(-1|m)m\big\}^{1/2} x\,Q_{n,m}(x^2) = \prod_s (x - \zeta_n^s) \prod_t (x + \zeta_n^t) = \psi_{n,m}(x) \qquad (m \text{ odd}), \tag{4}$$

$$P_{n,m}(-x^2) - i\big\{(-1|m)m\big\}^{1/2} x\,Q_{n,m}(-x^2) = \prod_s (x + i\zeta_n^s) \prod_t (x - i\zeta_n^t) = \psi_{2n,m}(x) \qquad (m \text{ odd}), \tag{5}$$

where the products are over ([2])

$$0 < s < n, \quad 0 < t < n, \quad (st, n) = 1, \quad (s|m) = 1, \quad (t|m) = -1; \tag{6}$$

([1]) $(-1|m)$ is Jacobi's symbol of quadratic character.

([2]) If $m = 1$, the product over t is empty, and in (4) we get $\psi_{n,1}(x) = \phi_n(x)$.

and

$$P_{n,m}(x^2) - m^{1/2} x\, Q_{n,m}(x^2) = \prod_s (x - \zeta_{4n}^s) = \psi_{2n,m}(x) \quad (m \text{ even}), \tag{7}$$

where the product is over

$$0 < s < 4n, \quad (s, 4n) = 1, \quad (m|s) = 1. \tag{8}$$

The first part of this theorem when $n = m$ was proved by Lucas [12], and was enunciated for all odd n, m by Cunningham ([5], p. 53), who also stated that the polynomials P, Q can be found by 'conformal division'. A proof for the case $n = 3m$, m even (in our notation) was given recently by Beeger [2]. The second part of Theorem 1 seems to be new, as does the following lemma, on which the proof is based.

Lemma 1. *Let $n > 1$ be square-free and let $m > 1$ be an odd divisor of n. For $\varepsilon = \pm 1$, let*

$$A_{n,m}^{(\varepsilon)} = \tfrac{1}{2}\{Y_{n,m}(x) - \varepsilon\{(-1|m)m\}^{1/2} Z_{n,m}(x)\} = \prod_s (x - \zeta_n^s), \tag{9}$$

the product being over

$$0 < s < n, \quad (s, n) = 1, \quad (s|m) = \varepsilon. \tag{10}$$

Then $Y_{n,m}$, $Z_{n,m}$ have rational integral coefficients, and

$$\phi_n(x) = A_{n,m}^{(1)}(x) A_{n,m}^{(-1)}(x) = \tfrac{1}{4}\{Y_{n,m}^2 - (-1|m)m Z_{n,m}^2\}. \tag{11}$$

Proof. It follows from Dirichlet's generalization ([7], supplement VII) of a well-known theorem of Gauss that the desired polynomials exist when $m = n$. The coefficients of $A_{m,m}^{(1)}(x)$ and $A_{m,m}^{(-1)}(x)$ are integers of the field generated by $\{(-1|m)m\}^{1/2}$, and corresponding coefficients are algebraically conjugate.

Put $n = mk$. In the product (9), but without the condition $(s, n) = 1$ in (10), put $s = s' + um$, where

$$0 < s' < m, \quad 0 \leqslant u < k.$$

We find that

$$\prod_s (x - \zeta_n^s) = \prod_{s'} \prod_u (x - \zeta_n^{s'} \zeta_k^u) = A_{m,m}^{(\varepsilon)}(x^k).$$

Hence

$$A_{n,m}^{(\varepsilon)}(x) = (A_{m,m}^{(\varepsilon)}(x^k), \phi_n(x)).$$

It follows that the coefficients of $A_{n,m}^{(\varepsilon)}(x)$ are also integers of the field generated by $\{(-1|m)m\}^{1/2}$ and that corresponding coefficients are algebraically conjugate. Since the integers of the field are expressible as

$$\tfrac{1}{2}(y - \{(-1|m)m\}^{1/2} z),$$

where y, z are rational integers, the polynomials $Y_{n,m}$, $Z_{n,m}$ in (9) have rational integral coefficients.

(11) follows immediately from (9), on dividing the values of r in

$$\phi_n(x) = \prod_r (x - \zeta_n^r)$$

into two classes according as $(r|m) = 1$ or -1. □

Proof of Theorem 1. Suppose first that n is odd and $m = 1$. We have

$$\phi_n(x^2) = \prod_{(t,n)=1} (x^2 - \zeta_n^{2t}) = \prod_{(t,n)=1} (x - \zeta_n^t)(x + \zeta_n^t) = \phi_n(x)\phi_n(-x). \tag{12}$$

Define polynomials $P_{n,1}$, $Q_{n,1}$ by

$$\phi_n(x) = P_{n,1}(x^2) - xQ_{n,1}(x^2).$$

Then (4) holds for $m = 1$, since $\psi_{n,1}(x) = \phi_n(x)$ as noted earlier. The identity (12) implies that

$$\phi_n(x^2) = P_{n,1}^2(x^2) - x^2 Q_{n,1}(x^2),$$

and this gives (1) for $m = 1$ on replacing x^2 by x.

Suppose, secondly, that n is odd and $m > 1$. By (12) and Lemma 1,

$$\phi_n(x^2) = A_{n,m}^{(1)}(x)A_{n,m}^{(-1)}(x)A_{n,m}^{(1)}(-x)A_{n,m}^{(-1)}(-x). \tag{13}$$

Put

$$\psi_{n,m}(x) = A_{n,m}^{(1)}(x)A_{n,m}^{(-1)}(-x) = \prod_s (x - \zeta_n^s) \prod_t (x + \zeta_n^t), \tag{14}$$

with s, t as in (6). Express the polynomials $Y_{n,m}$, $Z_{n,m}$ of Lemma 1 in the form

$$Y(x) = T(x^2) + xU(x^2), \quad Z(x) = V(x^2) + xW(x^2).$$

Then we find that

$$\psi_{n,m}(x) = P_{n,m}(x^2) - \{(-1|m)m\}^{1/2} x Q_{n,m}(x^2), \tag{15}$$

where

$$P_{n,m}(x^2) = \tfrac{1}{4}\{T^2 - x^2U^2 - (-1|m)m(V^2 - x^2W^2)\},$$
$$Q_{n,m}(x^2) = \tfrac{1}{2}(TW - UV),$$

where $T = T(x^2)$, etc. Since $Y \equiv Z \pmod 2$ by (9), the polynomials $P_{n,m}$, $Q_{n,m}$ have integral coefficients. Now (15) gives (4), and (13), (14), (15) give (1) on replacing x^2 by x. Also (2) is a consequence of (1), in view of the identity

$$\phi_{2n}(x) = \phi_n(-x) \quad (n \text{ odd}), \tag{16}$$

and (5) is a consequence of (4).

We can now suppose that n, m are both even, say $n = 2n_1$, $m = 2m_1$, where n_1, m_1 are necessarily odd. We suppose first that $n_1 > 1$. By (12) and (16),

$$\phi_{2n}(x) = \phi_n(x^2) = \phi_{n_1}(-x^2) = \phi_{n_1}(ix)\phi_{n_1}(-ix).$$

Hence

$$\phi_{2n}(x^2) = \phi_{n_1}(\zeta_8^2 x^2)\phi_{n_1}(\zeta_8^{-2}x^2) = \phi_{n_1}(\zeta_8 x)\phi_{n_1}(-\zeta_8 x)\phi_{n_1}(\zeta_8^{-1}x)\phi_{n_1}(-\zeta_8^{-1}x). \tag{17}$$

It can be verified that the product on the right is the same as

$$\psi_{2n,m}(x)\psi_{2n,m}(-x),$$

where $\psi_{2n,m}(x) = \psi_{4n_1,2m_1}(x)$ is defined by the product in (7) with the conditions in (8). To do this, put $s \equiv 8u + n_1 v \pmod{8n_1}$, where $v = 1, 3, 5, 7$ and

$$0 < u < n_1, \quad (u, n_1) = 1.$$

The condition of quadratic character in (8) limits u to one of the two classes $\pmod{m_1}$ for each v. Considering cases according to the residues of m_1 and $n_1 \pmod 4$, we find that

$$\psi_{2n,m}(x) = \psi_{n_1,m_1}(\alpha\zeta_8 x)\psi_{n_1,m_1}(\beta\zeta_8^{-1}x),$$

where $\alpha = \pm 1$, $\beta = \pm 1$ and $\alpha = (-1|m_1)\beta$. Using the definition of ψ_{n_1,m_1} as a product in (4), we deduce from (17) that

$$\phi_{2n}(x^2) = \psi_{2n,m}(x)\psi_{2n,m}(-x). \tag{18}$$

Using the polynomial expression for ψ_{n_1,m_1} in (4) and putting

$$P_{n_1,m_1}(x) = K(x^2) + xL(x^2), \quad Q_{n_1,m_1}(x) = M(x^2) + xN(x^2),$$

we find that

$$\psi_{2n,m}(x) = P_{n,m}(x^2) - m^{1/2}xQ_{n,m}(x^2), \tag{19}$$

where

$$P_{n,m}(x) = K^2 + x^2L^2 + m_1x(M^2 + x^2N^2),$$
$$Q_{n,m}(x) = \pm(KM + x^2LN) \pm x(KN - ML),$$

in which K stands for $K(-x^2)$, etc., and the $\pm$ sign depends on the residue classes of n_1 and $m_1 \pmod 8$. We now have (7), and (3) follows from (18) and (19) on replacing x^2 by x. This completes the proof if $n_1 > 1$. If $n_1 = 1$, then $n = m = 2$, and

$$\phi_{2n}(x) = x^2 + 1,$$

and we can take $P_{2,2}(x) = x + 1$, $Q_{2,2}(x) = 1$. □

The preceding proof is analogous to Lucas's proof of the case $m = n$.

We note that in view of the identity

$$\phi_n(x) = \phi_{n^*}(x^{n/n^*}), \tag{20}$$

where n^* denotes the greatest square-free divisor of n, the assumption that n is square-free can be replaced, both in Lemma 1 and Theorem 1, by the weaker assumption that m is square-free.

3.

Proof of Theorem 2. Since the primitive prime factors of $a^n - b^n$ coincide with those of $|a|^n - |b|^n$ if $ab > 0$ or $n \equiv 0 \pmod 4$, and those of $|a|^{n/2} - |b|^{n/2}$ if $ab < 0$ and $n \equiv 2 \pmod 4$, and those of $|a|^{2n} - |b|^{2n}$ if $ab < 0$ and $n \equiv 1 \bmod 2$, it suffices to prove the theorem when $a > b > 0$.

Put $n = kl$, where l is the product of those prime factors of n which do not divide $\eta k(ab)$, and write $\nu = \eta k(ab)l$. Since every prime factor of n is a prime factor of ν, we have

$$\phi_n(a, b) = \phi_\nu(A, B), \quad \text{where} \quad A = a^{n/\nu}, \quad B = b^{n/\nu}. \tag{21}$$

The polynomials $\psi_{n,m}(x)$, $\psi_{2n,m}(x)$ were defined in Theorem 1 when $n > 1$ is square-free and n/m is an odd integer. We add the definition $\psi_{1,1}(x) = x - 1$. The hypotheses of Theorem 2 ensure that $\psi_{\nu,k(ab)}$ is defined. Using the corresponding homogeneous forms, we put

$$\phi_n^{(\varepsilon)}(a, b) = \psi_{\nu,k(ab)}(A^{1/2}, \varepsilon B^{1/2}) \quad \text{for} \quad \varepsilon = 1, -1. \tag{22}$$

Each of these is a rational integer; the quadratic irrationality on the left of (4), (5) or (7) disappears for the value of x in question, because of the definition of η. We have

$$\phi_n(a, b) = \phi_n^{(1)}(a, b)\phi_n^{(-1)}(a, b). \tag{23}$$

Since

$$\psi_{\nu,k(ab)}(x)\psi_{\nu,k(ab)}(-x) = \pm\phi_\nu(x^2),$$

the resultant R of the two polynomials on the left divides the discriminant of $\phi_\nu(x^2)$, and therefore also the discriminant of $x^{2\nu} - 1$, which is $(2\nu)^{2\nu}$. There exist polynomials $\chi^{(1)}(x)$, $\chi^{(-1)}(x)$ such that

$$\chi^{(1)}(x)\psi_{\nu,k(ab)}(x) + \chi^{(-1)}(x)\psi_{\nu,k(ab)}(-x) = R$$

identically in x. The coefficients of $\chi^{(1)}$, $\chi^{(-1)}$ are expressible integrally in terms of the coefficients of $\psi_{\nu,k(ab)}(x)$, and therefore involve only the quadratic irrational in (4), (5) or (7). On making the above relation homogeneous in x, y and putting $x = A^{1/2}$, $y = B^{1/2}$, we find that the irrationality disappears, and from the resulting relation between integers we deduce that any common prime factor of $\phi_n^{(1)}(a, b)$ and $\phi_n^{(-1)}(a, b)$ must divide $2\nu B$.

By (23) and Zsigmondy's theorem, quoted in §1, each prime factor of either $\phi_n^{(1)}(a, b)$ or $\phi_n^{(-1)}(a, b)$ is a primitive prime factor of $a^n - b^n$, except possibly for $q(n)$, if this occurs to the first power only. Since this prime does not divide $k(ab)$, it must equal $q(l)$.

If either $\phi^{(1)}$ or $\phi^{(-1)}$ is even, then 2 is a primitive prime factor of $a^n - b^n$, and this can happen only if $n = 1$. Apart from this case, no prime factor of $2k(ab)lB$ can be a primitive prime factor of $a^n - b^n$, and consequently $\phi^{(1)}$, $\phi^{(-1)}$ are relatively prime. In order to ensure the existence of two primitive prime factors of $a^n - b^n$, it is enough to have

$$|\phi_n^{(\varepsilon)}(a, b)| > \begin{cases} 1 & \text{if } q(l) < q(n), \\ q(l) & \text{if } q(l) = q(n), \end{cases} \tag{24}$$

for $\varepsilon = 1, -1$, since then $\phi^{(1)}, \phi^{(-1)}$ will have two distinct prime factors other than $q(l)$.

If $n = 1$ then $k(ab) = 1$ and $a^n - b^n$ has two prime factors except when

$$a = (2^\alpha + 1)^2,\ b = (2^\alpha - 1)^2 \quad \text{or} \quad 4a = (p^\alpha + 1)^2,\ 4b = (p^\alpha - 1)^2,$$

in accordance with the theorem.

If $n > 1$, suppose first that $l = 1$ or 3. It follows from (4), (5) or (7) and (22) that

$$|\phi_n^{(\varepsilon)}(a, b)| < (A^{1/2} + B^{1/2})^{\phi(\nu)} \leqslant (2A + 2B)^{\phi(\nu)/2}. \tag{25}$$

On the other hand, we have two lower bounds for $\phi_n(a, b)$. First,

$$\phi_n(a, b) = \phi_\nu(A, B) > (A - B)^{\phi(\nu)}.$$

Secondly,

$$\frac{\phi_\nu(A, B)}{\phi_\nu(1, 1)} = \prod_{\substack{r=1 \\ (r,\nu)=1}}^{\nu} \frac{A - \zeta_\nu^r B}{1 - \zeta_\nu^r},$$

and since

$$4\left|\frac{A - \zeta_\nu^r B}{1 - \zeta_\nu^r}\right|^2 = (A + B)^2 + (A - B)^2 \cot^2 \pi r/\nu$$

we obtain

$$\phi_\nu(A, B) > \left(\tfrac{1}{2}A + \tfrac{1}{2}B\right)^{\phi(\nu)}.$$

It follows from (23) and (25) that

$$|\phi_n^{(\varepsilon)}(a, b)| > \left\{\max\left(A^{1/2} - B^{1/2}, \left(\tfrac{1}{8}A + \tfrac{1}{8}B\right)^{1/2}\right)\right\}^{\phi(\nu)}.$$

This implies that (24) holds when $l = 1$ or 3 except possibly if $A^{1/2} - B^{1/2} < 1$ and $A + B < 8$, or if $n = l = 3$ and $A^{1/2} - B^{1/2} < 3^{1/2}$ and $A + B < 24$, or if $n > l = 3$ and $A^{1/2} - B^{1/2} < 3^{1/4}$ and $A + B < 192^{1/2}$. Direct examination of these cases leads to all the exceptions given in the theorem for $2 < n < 20$.

Suppose now that $l \geqslant 5$ and put $l = q(l)r$. Put $\nu' = \eta k(ab)r = \nu/q(l)$. It follows from (4), (5) or (7) and (22) that

$$\phi^{(\varepsilon)} = \phi_{\nu'}^{(\delta)}\left(A^{q(l)}, B^{q(l)}\right)/\phi_{\nu'}^{(\delta)}(A, B),$$

where $\delta = \pm 1$ depends on ε and on the residue classes of $k(ab)$ and of $q(l)$ (mod 4). Using the inequalities

$$(x^{1/2} - 1)^{\phi(\nu')} \leqslant \phi_{\nu'}^{(\delta)}(x) \leqslant (x^{1/2} + 1)^{\phi(\nu')} \quad (x > 1),$$

we get for $q(l) \geqslant 3$

$$\begin{aligned} |\phi^{(\varepsilon)}| &> \left(\frac{A^{q(l)/2} - B^{q(l)/2}}{A^{1/2} + B^{1/2}}\right)^{\phi(v')} \\ &\geqslant \left(\frac{A + B + (AB)^{1/2}}{A + B + 2(AB)^{1/2}}\,(A - B)A^{q(l)/2-3/2}\right)^{\phi(v')} \\ &> \left(2^{-1/2}(A - B)A^{q(l)/2-3/2}\right)^{\phi(v')}. \end{aligned}$$

Since l is odd and square-free, we have $q(l) \geqslant 5$, so $2^{-1/2}A^{q(l)/2-3/2} > q(l)$ except when either $l = 5$ or 15 and $A \leqslant 7$ or $l = 7, 21, 35$ or 105 and $A = 2$ or 3. Direct examination of these cases leads to the last exception stated in the theorem. This completes the proof. □

4.

It follows from the identity

$$\phi_n(c^h) = \prod_{d\,|\,h} \phi_{nd}(c) \quad \text{when} \quad (h, n) = 1$$

and from (16) and Theorem 2 that if $ab = \pm c^h$, where c, h are integers and $h \geqslant 3$ or $k(c)$ is odd and $h = 2$, then for infinitely many n, $a^n - b^n$ has three primitive prime factors. This suggests the following problems.

Problem 1. For every pair a, b, does there exist n such that $a^n - b^n$ has three primitive prime factors?

Problem 2. Does there exist a pair a, b with $ab \neq \pm c^h$ $(h \geqslant 2)$ such that $a^n - b^n$ has three primitive prime factors for infinitely many n ?

5.

In conclusion, we apply Theorem 2 to obtain lower bounds for $q(a^n - b^n)$, the greatest prime factor of $a^n - b^n$. We note first:

Lemma 2.
(i) *If $n > 2$, and we exclude the case $n = 3$, $a = \pm 2$, $b = \mp 1$, then $q(a^n - b^n) \geqslant n + 1$.*
(ii) *If $n > 2$, $n \not\equiv 0 \pmod 4$, and we exclude the cases $n = 3$, $|a| = 2$, $|b| = 1$ and $n = 6$, $|a| = 2$, $|b| = 1$, then $q(a^n - b^n) \geqslant 2n + 1$.*

Proof. Apart from the excluded cases, $a^n - b^n$ has at least one primitive prime factor q, by Zsigmondy's theorem. This is of the form $nk + 1$, and of the form $2nk + 1$ if n is odd. Thus it remains only to prove (ii) when $n \equiv 2 \pmod 4$. For this we observe that $a^{n/2} - b^{n/2}$

has a primitive prime factor q_1 of the form $nk+1$. Since $q \neq q_1$, one at least of q, q_1 is $\geqslant 2n+1$. □

Using Theorem 2 we shall prove

Lemma 3. *If $n > 2$ and $k(ab) \mid n$, and we exclude the cases $n = 4, 6, 12$, $|a| = 2$, $|b| = 1$, then $q(a^n - b^n) \geqslant 2n+1$.*

Proof. By Lemma 2 we can suppose $n \equiv 0 \pmod 4$. If $k(ab)$ is odd, $a^n - b^n$ has at least one primitive prime factor q by Zsigmondy's theorem. This is of the form $nk+1$, and so $q \equiv 1 \pmod{4k(ab)}$. Hence $k(ab)$ is a quadratic residue $\pmod q$, which implies that $a^{(q-1)/2} - b^{(q-1)/2}$ is divisible by q. Since q is a primitive prime factor of $a^n - b^n$, it is impossible that $q - 1 = n$, hence $q \geqslant 2n+1$.

The same argument applies if $k(ab)$ is even and $n/2k(ab)$ is even. If $k(ab)$ is even and $n/2k(ab)$ is odd, then apart from the exception of Theorem 2, which can be tested directly, $a^n - b^n$ has at least two primitive prime factors. One at least of these is $\geqslant 2n+1$. □

If $k(ab) = \pm 2$, we can combine Lemmas 2 and 3 to give

Theorem 3. *If $k(ab) = \pm 2$ and $n > 2$ and we exclude the cases $n = 4, 6, 12$, $|a| = 2$, $|b| = 1$, then $q(a^n - b^n) \geqslant 2n+1$.*

The same result holds if $k(ab) = \pm 1$ or more generally $ab = \pm c^h$ ($h \geqslant 2$). It suggests

Problem 3. Does there exist any pair a, b with $ab \neq \pm 2c^2, \pm c^h$ ($h \geqslant 2$) such that $q(a^n - b^n) > 2n$ for all sufficiently large n?

I conclude by expressing my thanks to Dr. B. J. Birch and Prof. H. Davenport for their kind assistance in the preparation of this paper, to Prof. T. Nagell and Mr. A. Rotkiewicz for their valuable suggestions, and to the Rockefeller Foundation whose fellowship I held when writing the paper.

References

[1] A. Aurifeuille, H. Le Lasseur, See: E. Lucas, *Théorèmes d'arithmétique*. Atti R. Acad. Sc. Torino 13 (1877–8), 271–284.

[2] N. G. W. H. Beeger, *On a new quadratic form for certain cyclotomic polynomial*. Nieuw Arch. Wiskunde (2) 23 (1951), 249–252.

[3] C. E. Bickmore, *On the numerical factors of $a^n - 1$*. Messenger of Math. (2) 25 (1895–6), 1–44; 26 (1896–7), 1–38.

[4] G. D. Birkhoff, H. S. Vandiver, *On the integral divisors of $a^n - b^n$*. Ann. of Math. (2) 5 (1904), 173–180.

[5] A. Cunningham, *Factorisation of $N = y^y \mp 1$ and $x^{xy} \mp y^{xy}$*. Messenger of Math. (2) 45 (1915), 49–75.

[6] L. E. Dickson, *History of the Theory of Numbers*, I. Washington 1919.

[7] P. G. L. Dirichlet, *Vorlesungen über Zahlentheorie*, 4th ed. Friedr. Vieweg & Sohn, Braunschweig 1894.

[8] H. J. Kanold, *Sätze über Kreisteilungspolynome und ihre Anwendungen auf einige zahlentheoretische Probleme*. J. Reine Angew. Math. 187 (1950), 169–182.

[9] M. Kraïtchik, *Décomposition de $a^n \pm b^n$ en facteurs dans le cas où nab est un carré parfait avec une table des décompositions numériques pour toutes les valeurs de a et b inférieures à* 100. Paris, 1922.

[10] —, *Recherches sur la Théorie des Nombres*, I. Paris, 1924.

[11] E. Lucas, *Sur la série récurrente de Fermat*. Bull. Bibl. Storia Sc. Mat. e Fis. 11 (1878), 783–789.

[12] —, *Sur les formules de Cauchy et de Lejeune Dirichlet*. Ass. Française pour l'Avanc. des Sci., Comptes Rendus 7 (1878), 164–173.

[13] A. Rotkiewicz, *The numbers of the form* $\dfrac{(4k+1)^{4k+1}-1}{4k}$, $\dfrac{(4k+3)^{4k+3}+1}{4k+4}$. Prace Mat. 5 (1961), 95–99 (Polish).

[14] K. Zsigmondy, *Zur Theorie der Potenzreste*. Monatsh. Math. 3 (1892), 265–284.

Originally published in
Acta Arithmetica VIII (1963), 213–223

On primitive prime factors of Lehmer numbers I

Lehmer numbers are called terms of the sequences

$$P_n(\alpha, \beta) = \begin{cases} (\alpha^n - \beta^n)/(\alpha - \beta), & n \text{ odd}, \\ (\alpha^n - \beta^n)/(\alpha^2 - \beta^2), & n \text{ even}, \end{cases}$$

where α and β are roots of the trinomial $z^2 - L^{1/2}z + M$, and L and M are rational integers (cf. [4]). Without any essential loss of generality (cf. [9]) we can assume that

$$L > 0, \quad M \neq 0, \quad K = L - 4M \neq 0. \tag{1}$$

Lehmer numbers constitute a generalization of the numbers $a^n - b^n$ (a, b—rational integers). A prime p is called a *primitive prime factor* of a number $a^n - b^n$ if

$$p \mid a^n - b^n \quad \text{but} \quad p \nmid a^k - b^k \quad \text{for} \quad k < n.$$

A proper (not merely automatical) generalization of this notion for Lehmer numbers is the notion of a prime factor p such that

$$p \mid P_n \quad \text{but} \quad p \nmid KLP_3 \cdots P_{n-1}$$

or, which is easily proved to be equivalent,

$$p \mid P_n \quad \text{but} \quad p \nmid nP_3 \cdots P_{n-1}.$$

D. H. Lehmer [4] calls such primes p primitive extrinsic prime factors of P_n. In a postscript to my paper [7] I stated erroneously that Lehmer calls them intrinsic divisors, the term which has been used in a different sense by M. Ward [9]. To simplify the terminology, I adopt in the present paper the following definition.

Definition. A prime p is called a *primitive prime factor* of the number P_n if $p \mid P_n$ but $p \nmid KLP_3 \cdots P_{n-1}$.

Assume that, besides the restrictions on L, M stated in (1),

$$(L, M) = 1, \quad \langle L, M \rangle \neq \langle 1, 1 \rangle, \langle 2, 1 \rangle, \langle 3, 1 \rangle \tag{2}$$

(i.e. β/α is not a root of unity).

Then it follows from the results of papers [2], [7], [9] that for $n \neq 1, 2, 3, 4, 6$, P_n has a primitive prime factor except

$$\text{for } K > 0 \quad \text{if } n = 5,\ \langle L, M\rangle = \langle 1, -1\rangle, \quad n = 10,\ \langle L, M\rangle = \langle 5, 1\rangle, \quad n = 12,\ \langle L, M\rangle = \langle 1, -1\rangle, \langle 5, 1\rangle$$

$$\text{for } K < 0 \quad \text{if } n \leqslant n_0(L, M)$$

where n_0 can be computed effectively.

I proved in [6] a theorem about numbers $a^n - b^n$ with two primitive prime factors. A. Rotkiewicz [5] generalized this theorem to so-called Lucas numbers (which correspond to Lehmer numbers for $L^{1/2}$ being a rational integer) under the assumptions $M > 0$, $K > 0$.

The main aim of the present paper is to generalize the above theorem to Lehmer numbers. To state the generalization in a possibly concise manner I introduce the following two sets $\mathfrak{M}$, $\mathfrak{N}$:

$$\mathfrak{M} = \big\{\langle L, M\rangle : (L, M) = 1;\ \langle L, M\rangle = \langle 12, -25\rangle, \langle 112, 25\rangle \text{ or } 1 \leqslant |M| \leqslant 15,\ 2M + 2|M| + 1 \leqslant L < \min(64 + 2M - 2|M|, 2M + 2|M| + 4|M|^{1/2} + 1)\big\},$$

$$\mathfrak{N} = \big\{\langle L, M\rangle : (L, M) = 1,\ \langle L, M\rangle = \langle 4, -1\rangle, \langle 8, 1\rangle \text{ or } 1 \leqslant |M| \leqslant 15,\ L = 2M + 2|M| + 1\big\}.$$

As can easily be verified, set $\mathfrak{M}$ consists of 184 and set $\mathfrak{N}$ of 32 pairs $\langle L, M\rangle$.

For an integer $n \neq 0$, let $k(n)$ denote the square-free kernel of n, that is, n divided by its greatest square factor. The following theorem holds.

Theorem 1. *For L, M satisfying* (1), (2), *put $\kappa = k\big(M \max(K, L)\big)$ and*

$$\eta = \begin{cases} 1 & \text{if } \kappa \equiv 1 \pmod 4, \\ 2 & \text{if } \kappa \equiv 2, 3 \pmod 4. \end{cases}$$

If $n \neq 1, 2, 3, 4, 6$ and $n/\eta\kappa$ is an odd integer, then P_n has at least two primitive prime factors except

1. *for $K > 0$, if $n = \eta|\kappa|$, $\langle L, M\rangle \in \mathfrak{M}_0 \subset \mathfrak{M}$ or $n = 3\eta|\kappa|$, $\langle L, M\rangle \in \mathfrak{N}_0 \subset \mathfrak{N}$ or $n = 5$, $\langle L, M\rangle = \langle 9, 1\rangle$ or $n = 10$, $\langle L, M\rangle = \langle 5, -1\rangle$ or $n = 20$, $\langle L, M\rangle = \langle 1, -2\rangle, \langle 9, 2\rangle$;*
2. *for $K < 0$, if $n \leqslant n_1(L, M)$.*

Finite sets $\mathfrak{M}_0$, $\mathfrak{N}_0$ and function $n_1(L, M)$ can be effectively computed.

Let us observe that the sequences P_n and $\overline{P}_n$ corresponding to $\langle L, M\rangle$ and $\langle \max(K, L), |M|\rangle$, respectively, are connected by the relation

$$P_n = \begin{cases} \overline{P}_n & \text{if } M > 0 \text{ or } n \text{ even}, \\ \overline{P}_{2n}/\overline{P}_n & \text{if } M < 0 \text{ and } n \text{ odd}. \end{cases}$$

Therefore the primitive prime factors of P_n coincide with those of $\overline{P}_n$ if $M > 0$ or $n \equiv 0 \pmod 4$, with those of $\overline{P}_{n/2}$ if $M < 0$ and $n \equiv 2 \pmod 4$ and with those of $\overline{P}_{2n}$ if $M < 0$ and $n \equiv 1 \pmod 2$. The remarks that

1. $\langle L, M\rangle \in \mathfrak{M}$ or $\mathfrak{N}$ if and only if $\langle \max(K, L), |M|\rangle \in \mathfrak{M}$ or $\mathfrak{N}$, respectively,
2. $\operatorname{sgn}\kappa = \operatorname{sgn} M$,
3. if κ is even, η's corresponding to κ and $-\kappa$ are equal; if κ is odd, the product of these η's is 2,

show that it suffices to prove the theorem for $M > 0$, $\kappa = k\big(M\max(K, L)\big) = k(LM)$.

Before proceeding further, we introduce some notation and recall some useful results from paper [6]. For any integer $n > 0$ let

$$Q_n(x, y) = \prod_{\substack{r=1\\(r,n)=1}}^{n} (x - \zeta_n^r y),$$

where ζ_n is a primitive n-th root of unity. Put $Q_n(x) = Q_n(x, 1)$ and similarly for other polynomials later. Denote by $q(n)$ the greatest prime factor of n. Further, for n satisfying the assumptions of Theorem 1, let l be the product of those prime factors of n which do not divide $\eta\kappa$, and write $\nu = \eta\kappa l$, $A = \alpha^{n/\nu}$, $B = \beta^{n/\nu}$. To obtain conformity of notation with paper [6] one should make in the latter the following permutation of letters: $\Phi \to Q$, $P \to R$, $Q \to S$.

Then by Theorem 1 of [6] and remark that $\nu > 2$,

$$Q_\nu(x^2) = \psi_{\nu,\kappa}(x)\psi_{\nu,\kappa}(-x), \tag{3}$$

where [1]

$$\psi_{\nu,\kappa}(x) = R_{\kappa l,\kappa}(x^2) - \kappa^{1/2} x S_{\kappa l,\kappa}(x^2) \quad (\kappa^{1/2} > 0), \tag{4}$$

$$= \begin{cases} \displaystyle\prod_{(r,\kappa l)=1} \big(x - (r|\kappa)\zeta_{\kappa l}^r\big) & \text{if} \quad \kappa \equiv 1 \pmod 4,\\ \displaystyle\prod_{(r,\kappa l)=1} \big(x + i(r|\kappa)\zeta_{\kappa l}^r\big) & \text{if} \quad \kappa \equiv 3 \pmod 4,\\ \displaystyle\prod_{\substack{(r,4\kappa l)=1\\(\kappa|r)=1}} (x - \zeta_{4\kappa l}^r) & \text{if} \quad \kappa \equiv 2 \pmod 4 \end{cases} \tag{5}$$

and $R = R_{\kappa l,\kappa}$, $S = S_{\kappa l,\kappa}$ are polynomials with rational integral coefficients.

Let us put, similarly as in [6], for $\varepsilon = \pm 1$,

$$Q_n^{(\varepsilon)}(\alpha, \beta) = \psi_{\nu,\kappa}(A^{1/2}, \varepsilon B^{1/2}), \tag{6}$$

where $\arg A^{1/2} = \frac{1}{2}\arg A$, $\arg B^{1/2} = \frac{1}{2}\arg B$. Then, if α, β are real, $\alpha > \beta > 0$, we have for $\varepsilon = \pm 1$

$$|Q_n^{(\varepsilon)}(\alpha, \beta)| > \big(\max\big(A^{1/2} - B^{1/2}, (\tfrac{1}{8}A + \tfrac{1}{8}B)^{1/2}\big)\big)^{\varphi(\nu)}, \tag{7}$$

$$|Q_n^{(\varepsilon)}(\alpha, \beta)| > \big(2^{-1/2}(A - B)A^{q(l)/2-3/2}\big)^{\varphi(\nu')} \quad (l \geqslant 3,\ \nu' = \nu/q(l)). \tag{8}$$

---

[1] $(r|\kappa)$ is Jacobi's symbol of quadratic character.

These inequalities were proved in [6] under the assumption that α, β are rational integers; however, the proof does not change if α, β are arbitrary real numbers, $\alpha > \beta > 0$.

Now we shall prove three lemmas.

Lemma 1. *If n satisfies the assumptions of Theorem 1, $M > 0$, $p \mid Q_n(\alpha, \beta)$ and p is not a primitive prime factor of $P_n(\alpha, \beta)$, then $p^2 \nmid Q_n(\alpha, \beta)$, and if $n \neq 2r^\alpha$ (r prime), then $p = q(n) = q(l)$. If $n = 2r^\alpha$ (r prime), $r \mid Q_n(\alpha, \beta)$ if and only if $r \mid L$.*

Proof. It follows from Theorems 3.3 and 3.4 of [4] that if the assumptions of the lemma are satisfied and $n \neq 12$, then $p^2 \nmid Q_n(\alpha, \beta)$ and $p = q(n)$. On the other hand, as can easily be verified,

$$Q_n(\alpha, \beta) = \sum_{i=0}^{\varphi(n)/2} a_i L^{\varphi(n)/2-i} M^i$$

where $a_0 = 1$ and $a_{\varphi(n)/2} = \pm 1$, unless $n = 2r^\alpha$ (r prime). For $n = 2r^\alpha$, $a_{\varphi(n)/2} = \pm r$, so that $r \mid Q_n(\alpha, \beta)$ if and only if $r \mid L$. For $n \neq 2r^\alpha$ we have, in view of $(L, M) = 1$, $(p, LM) = 1$ so $(p, \kappa) = 1$. Since all prime factors of n divide $\eta\kappa l$, the lemma is thus proved for all $n \neq 12$.

If $n = 12$, then $Q_n(\alpha, \beta) = L^2 - 4LM + M^2$; if p is an imprimitive prime factor of $P_n(\alpha, \beta)$, then $L \equiv kM \pmod p$ for some $k \leqslant 4$. Hence, if $p \mid Q_n(\alpha, \beta)$, then in view of $(L, M) = 1$, $p = 2$ or 3. On the other hand, it follows from $12 = \eta\kappa l$ that κ is even, LM is even and $p \neq 2$. Thus $p = 3 = l$ and $p^2 \nmid Q_n(\alpha, \beta)$, which completes the proof. □

Lemma 2. *If n satisfies the assumptions of Theorem 1, $\delta = k(L)^{-\{\varphi(n)/4\}}$ and $M > 0$, then the numbers $\delta Q_n^{(1)}(\alpha, \beta)$ and $\delta Q_n^{(-1)}(\alpha, \beta)$ are coprime rational integers* (2).

Proof. We show first that $\psi_{\nu,\kappa}(x)$ ($\nu > 1$) are reciprocal polynomials. For instance, let $\kappa \equiv 3 \pmod 4$. We have by (5)

$$\psi_{\nu,\kappa}(x^{-1}) = \prod_{(r,\kappa l)=1} \left(x^{-1} + i(r|\kappa)\zeta_{\kappa l}^r\right) = x^{-\varphi(\nu)} \prod_{(r,\kappa l)=1} \left(i(r|\kappa)\zeta_{\kappa l}^r\right) \prod_{(r,\kappa l)=1} \left(x - i(r|\kappa)\zeta_{\kappa l}^{-r}\right)$$
$$= x^{-\varphi(\nu)} i^{\varphi(\nu)} (-1)^{\varphi(\nu)/2} \prod_{(r,\kappa l)=1} \left(x + i(-r|\kappa)\zeta_{\kappa l}^{-r}\right) = x^{-\varphi(\nu)} \psi_{\nu,\kappa}(x).$$

Since in view of (4)

$$R_{\kappa l,\kappa}(x) = \frac{1}{2}\left(\psi_{\nu,\kappa}(x^{1/2}) + \psi_{\nu,\kappa}(-x^{-1/2})\right),$$
$$S_{\kappa l,\kappa}(x) = \frac{1}{2(\kappa x)^{1/2}}\left(\psi_{\nu,\kappa}(x^{1/2}) - \psi_{\nu,\kappa}(-x^{-1/2})\right),$$

it follows that the polynomials R, S are reciprocal. We now prove that these polynomials are of degrees $\frac{1}{2}\varphi(\nu)$ and $\frac{1}{2}\varphi(\nu) - 1$, respectively. In fact

$$Q_\nu(x) = R^2(x) - \kappa x S^2(x), \tag{9}$$

(2) $[x]$ and $\{x\}$ denote the integral and the fractional part of x, respectively.

whence degree $S <$ degree $R = \frac{1}{2}$ degree $Q_\nu = \frac{1}{2}\varphi(\nu)$. On the other hand, supposing that degree $S < \frac{1}{2}\varphi(\nu) - 1$,

$$R(x) = x^{\varphi(\nu)/2} + ax^{\varphi(\nu)/2-1} + bx^{\varphi(\nu)/2-2} + \dots$$

we should find by comparing both sides of (9) that

$$x^{\varphi(\nu)} - \mu(\nu)x^{\varphi(\nu)-1} + \dots = x^{\varphi(\nu)} + 2ax^{\varphi(\nu)-1} + \dots,$$

whence $\mu(\nu) = -2a = 0$ and, in view of the definition of ν, $\kappa \equiv 2 \pmod 4$. Since $Q_\nu(x) = Q_{\nu/2}(x^2)$, identity (9) gives again

$$x^{\varphi(\nu)} - \mu\big(\tfrac{1}{2}\nu\big)x^{\varphi(\nu)-2} + \dots = x^{\varphi(\nu)} + 2bx^{\varphi(\nu)-2} + \dots,$$

$\mu(\frac{1}{2}\nu) = -2b = 0$, which is impossible, because $\frac{1}{2}\nu$ is square-free.

It follows from the above that $(x+y)^{-\varphi(\nu)/2}R(x, y)$, $(x+y)^{1-\varphi(\nu)/2}S(x, y)$ are homogeneous symmetric functions of x, y of dimension 0; so they are rationally expressible in terms of $(x+y)^2$ and xy, and thus $(A+B)^{-\varphi(\nu)/2}R(A, B)$, $(A+B)^{-1-\varphi(\nu)/2}S(A, B)$ are rationally expressible by $(A+B)^2$ and AB. In their turn $(A+B)^2$, AB and $(A+B)/(\alpha+\beta)$ are rationally expressible by $(\alpha+\beta)^2$ and $\alpha\beta$. Therefore the numbers

$$\delta R(A, B) = \Big(\frac{L}{k(L)}\Big)^{\{\frac{1}{4}\varphi(\nu)\}}(\alpha+\beta)^{2[\frac{1}{4}\varphi(\nu)]}\Big(\frac{A+B}{\alpha+\beta}\Big)^{\frac{1}{2}\varphi(\nu)}(A+B)^{-\frac{1}{2}\varphi(\nu)}R(A, B),$$

$$\delta\,\frac{S(A, B)}{A+B} = \Big(\frac{L}{k(L)}\Big)^{\{\frac{1}{4}\varphi(\nu)\}}(\alpha+\beta)^{2[\frac{1}{4}\varphi(\nu)]}\Big(\frac{A+B}{\alpha+\beta}\Big)^{\frac{1}{2}\varphi(\nu)}(A+B)^{-1-\frac{1}{2}\varphi(\nu)}S(A, B),$$

are rationally expressible by $(\alpha+\beta)^2 = L$ and $\alpha\beta = M$ and as such are rational.

Since for $\varepsilon = \pm 1$

$$\delta Q_n^{(\varepsilon)}(\alpha, \beta) = \delta R(A, B) \pm \frac{A+B}{\alpha+\beta}\Big(\frac{AB}{\alpha\beta}\Big)^{1/2}\big(\kappa(\alpha+\beta)^2\alpha\beta\big)^{1/2}\delta\,\frac{S(A, B)}{A+B}$$

and the numbers

$$\frac{A+B}{\alpha+\beta}, \quad \Big(\frac{AB}{\alpha\beta}\Big)^{1/2} = \pm(\alpha\beta)^{(n-\nu)/2\nu}, \quad \big(\kappa(\alpha+\beta)^2\alpha\beta\big)^{1/2} = \kappa\Big(\frac{LM}{k(LM)}\Big)^{1/2}$$

are rational, the numbers $\delta Q_n^{(\varepsilon)}(\alpha, \beta)$ are also rational. If $\varphi(n) \equiv 0 \pmod 4$ or $k(L) = 1$ then $\delta = 1$, and it is immediately evident from (4) and (6) that these numbers are algebraic integers, consequently they are then rational integers.

Let $\varphi(n) \not\equiv 0 \pmod 4$ and $k(L) \neq 1$. Since $n \neq 1, 2, 4$, we have

$$n = r^\alpha \quad \text{or} \quad n = 2r^\alpha, \quad r \text{ prime} \equiv 3 \pmod 4.$$

Since $k(L) \mid \kappa \mid n$, $k(L)$ is odd, we get $k(L) = \kappa = r$, $n = 2r^\alpha$. We have to prove that the numbers $r^{-1/2}Q_n^{(\varepsilon)}(\alpha, \beta)$ are algebraic integers. First, since $\kappa = r^{1/2}$, it is clear from formula (4) that their difference is integral. Now in view of formulae (3) and (6)

$$Q_n(\alpha, \beta) = Q_n^{(1)}(\alpha, \beta)Q_n^{(-1)}(\alpha, \beta); \tag{10}$$

their product equals therefore $r^{-1}Q_n(\alpha, \beta)$ and is integral by Lemma 1. Thus the numbers $r^{-1/2}Q_n^{(\varepsilon)}(\alpha, \beta)$ are themselves integral. So we have proved that the numbers $\delta Q_n^{(\varepsilon)}(\alpha, \beta)$ ($\varepsilon = \pm 1$) are rational integers. It remains to prove that they are coprime.

By identity (3) the resultant R of polynomials $\psi_{v,\kappa}(x)$, $\psi_{v,\kappa}(-x)$ divides the discriminant of $Q_v(x^2)$ and therefore also the discriminant of $x^{2v}-1$, which is $(2v)^{2v}$. There exist polynomials $\chi^{(1)}(x)$, $\chi^{(-1)}(x)$ such that

$$\chi^{(1)}(x)\psi_{v,\kappa}(x)+\chi^{(-1)}(x)\psi_{v,\kappa}(-x)=R$$

identically in x. The coefficients of $\chi^{(1)}$, $\chi^{(-1)}$ are expressible integrally in terms of the coefficients of $\psi_{v,\kappa}(x)$ and therefore are algebraic integers. On making the above relation homogeneous in x, y and putting $x=A^{1/2}$, $y=B^{1/2}$, we deduce that any common prime factor of $\delta Q_n^{(1)}(\alpha,\beta)$ and $\delta Q_n^{(-1)}(\alpha,\beta)$ must divide $2vM$. By Lemma 1 and (10) each prime factor of $\delta Q_n^{(\varepsilon)}(\alpha,\beta)$ ($\varepsilon=\pm1$) is a primitive prime factor of P_n except possibly for $q(n)$, which then occurs to the first power only. Since no prime factor of $2vM$ can be a primitive prime factor of P_n, numbers $\delta Q_n^{(1)}(\alpha,\beta)$, $\delta Q_n^{(-1)}(\alpha,\beta)$ are relatively prime. The proof of the lemma is thus complete. □

Lemma 3. *If $\chi(r)$ is an arbitrary character* $\bmod m$, *$m>1$ and $|x|=1$, then*

$$\Pi=\prod_{\chi(r)=\text{const}\neq0}|x-\zeta_m^r|<\exp(2m^{1/2}\log^2 m).$$

Proof ([1]). We can assume without loss of generality that $\arg\zeta_m=2\pi/m$. Let e be the least positive exponent such that $\chi^{e+1}=\chi$. If $e=1$ much stronger estimation for Π is known (cf. [1]), if $e=\varphi(m)$ the lemma is satisfied trivially, and thus we can assume $\varphi(m)>e>1$. Let the product Π be taken over r such that $\chi(r)=\zeta_e^{j_0}$. Order these integers r according to the magnitude of $\left\{\frac{r}{m}-\frac{1}{2\pi}\arg x\right\}$ so that

$$\left\{\frac{r_1}{m}-\frac{1}{2\pi}\arg x\right\}<\ldots<\left\{\frac{r_k}{m}-\frac{1}{2\pi}\arg x\right\}\quad\left(k=\frac{\varphi(m)}{e}\right).$$

Denote by N_i and $N_{i,j}$ ($1\leqslant i\leqslant k$, $0\leqslant j<e$) the number of all non-negative integers $r<m$ such that $\left\{\frac{r}{m}-\frac{1}{2\pi}\arg x\right\}\leqslant\left\{\frac{r_i}{m}-\frac{1}{2\pi}\arg x\right\}$ and $\chi(r)=0$ or $\chi(r)=\zeta_e^j$, respectively. We have

c (11) $$\left|\big(m-\varphi(m)\big)\left\{\frac{r_i}{m}-\frac{1}{2\pi}\arg x\right\}-N_i\right|<2^{\nu(m)-1}\leqslant m^{1/2}\quad(1\leqslant i\leqslant k),$$

(12) $$\left|\sum_{j=0}^{e-1}N_{i,j}-m\left\{\frac{r_i}{m}-\frac{1}{2\pi}\arg x\right\}+N_i\right|<1\quad(1\leqslant i\leqslant k).$$

On the other hand, from a well-known theorem of Schur [8] (for imprimitivite
c character see [3] and the Addendum ([2])), which we apply successively to characters

([1]) The idea of this proof is due to P. Erdős. An earlier proof of the writer led to a weaker estimation for Π.

([2]) p. 1055

$\chi(r), \chi^2(r), \ldots, \chi^{e-1}(r)$, we get

$$\left|\zeta_e^{-hj_0}\sum_{j=0}^{e-1} N_{i,j}\zeta_e^{hj}\right| < m^{1/2}\log m \quad (1 \leqslant h < e,\ 1 \leqslant i \leqslant k). \tag{13}$$

Adding inequalities (11), (12), (13), we find

$$\left|eN_{i,j_0} - \varphi(m)\left\{\frac{r_i}{m} - \frac{1}{2\pi}\arg x\right\}\right| < em^{1/2}\log m \quad (1 \leqslant i \leqslant k).$$

Since $N_{i,j_0} = i$, putting for brevity $\pi\left\{\dfrac{r_i}{m} - \dfrac{1}{2\pi}\arg x\right\} - \pi\,\dfrac{i}{k} = \varrho_i$ we get for each $i \leqslant k$

$$|\varrho_i| \leqslant \pi k^{-1} m^{1/2}\log m.$$

Now, if $\arg\zeta_k = 2\pi/k$, we find

$$\begin{aligned}
&\prod_{i=1}^{k-1}|x-\zeta_m^{r_i}|\,|1-\zeta_k^i|^{-1} = \prod_{i=1}^{k-1}\left|\sin\Big(\frac{1}{2}\arg x - \pi\,\frac{r_i}{m}\Big)\right|\left|\sin\pi\,\frac{i}{k}\right|^{-1}\\
&= \prod_{i=1}^{k-1}\left|\sin\Big(\pi\,\frac{i}{k} + \varrho_i\Big)\right|\left|\sin\pi\,\frac{i}{k}\right|^{-1} = \prod_{i=1}^{k-1}\Big(|\cos\varrho_i| + |\sin\varrho_i|\,\left|\cot\pi\,\frac{i}{k}\right|\Big)\\
&\leqslant \prod_{i=1}^{[k/2]}\Big(1 + (\pi k^{-1}m^{1/2}\log m)\,\frac{k}{\pi i}\Big)^2 \leqslant \exp\Big(2m^{1/2}\log m\sum_{i=1}^{[k/2]}\frac{1}{i}\Big)\\
&< \exp\Big(2m^{1/2}\log m\Big(1 + \log\frac{k}{2}\Big)\Big).
\end{aligned}$$

Since, on the other hand, $\prod_{i=1}^{k-1}|1-\zeta_k^i| = k$ and $k = \varphi(m)/e < m/2$, we get

$$\begin{aligned}
\Pi &\leqslant 2\prod_{i=1}^{k-1}\big(|x-\zeta_m^{r_i}|\,|1-\zeta_k^i|^{-1}\big)\prod_{i=1}^{k-1}|1-\zeta_k^i|\\
&< m\exp\Big(2m^{1/2}\log m\Big(1+\log\frac{m}{4}\Big)\Big) \leqslant \exp(2m^{1/2}\log^2 m).
\end{aligned}$$

This proves the lemma. □

Proof of Theorem 1. As we already know, we can assume that $M > 0$. Then, in view of formula (8) and Lemmas 1 and 2, in order to prove Theorem 1 for a given index n, it is enough to establish that

$$|Q_n^{(\varepsilon)}(\alpha,\beta)| > \begin{cases} 1, & \text{if } q(l) < q(n) \text{ and } n \neq 2r^\alpha,\ r \text{ as below,}\\ r^{1/2}, & \text{if } n = 2r^\alpha,\ r = k(L) \text{ prime} \equiv 3 \pmod 4,\\ q(l), & \text{if } q(l) = q(n) \text{ and } n \neq 2r^\alpha,\ r \text{ as above.}\end{cases} \tag{14}$$

The proof of this inequality is different if α, β are real ($K > 0$) and if they are complex ($K < 0$); consequently the proof is divided into two parts.

1. $K > 0$. If $n > \nu = \eta\kappa l$, thus $n \geqslant 3\nu$, we apply (7) and find

$$|Q_n^{(\varepsilon)}(\alpha, \beta)| > (A^{1/2} - B^{1/2})^{\varphi(\nu)} \geqslant (\alpha^{3/2} - \beta^{3/2})^{\varphi(\nu)}$$
$$= \left(KL^{1/2} + M(L^{1/2} - 2M^{1/2})\right)^{\varphi(\eta\kappa)\varphi(l)/2} > (KL^{1/2})^{\varphi(\eta\kappa)\varphi(l)/2}.$$

Now, as can easily be verified, $(KL^{1/2})^{\varphi(\eta\kappa)/2} > 2$ for all L, M, so that

$$|Q_n^{(\varepsilon)}(\alpha, \beta)| > 2^{\varphi(l)} \geqslant 2^{q(l)-1} \geqslant q(l)$$

and inequality (14) holds. Thus we can assume that $n = \nu$, $A = \alpha$, $B = \beta$. We shall consider successively $l = 1$, $l = 3$ and $l \geqslant 5$.

If $l = 1$, we have to prove

$$|Q_n^{(\varepsilon)}(\alpha, \beta)| > 1 \quad \text{if} \quad n \neq 2r,\ r \text{ as below,} \tag{15}$$
$$|Q_n^{(\varepsilon)}(\alpha, \beta)| > r^{1/2} \quad \text{if} \quad n = 2r,\ r = k(L) \text{ prime} \equiv 3 \pmod 4.$$

Now, if $|Q_n^{(\varepsilon)}(\alpha, \beta)| \leqslant 1$, we have by inequality (7)

$$1 > \alpha^{1/2} - \beta^{1/2} = (L^{1/2} - 2M^{1/2})^{1/2}, \quad 1 > \tfrac{1}{8}\alpha + \tfrac{1}{8}\beta = \tfrac{1}{8}L^{1/2},$$

so that $L < 4M + 4M^{1/2} + 1$, $L < 64$. Since $4M < L$, we get $M \leqslant 15$ and $\langle L, M\rangle \in \mathfrak{M}$. It remains to consider the case $n = 2r$, r prime $\equiv 3 \pmod 4$, $r \geqslant 7$ (since $n \neq 6$), $k(L) = r$, $k(M) = 1$. By (7) we have

$$|Q_n^{(\varepsilon)}(\alpha, \beta)| > \left(\max(L^{1/2} - 2M^{1/2}, \tfrac{1}{8}L^{1/2})\right)^{\varphi(\nu)/2}.$$

Since $\varphi(\nu) = r - 1$, it suffices to establish the inequality

$$\max(L^{1/2} - 2M^{1/2}, \tfrac{1}{8}L^{1/2}) > r^{1/(r-1)}. \tag{16}$$

Since $r \geqslant 7$, $r^{1/(r-1)} \leqslant 7^{1/6} < 2^{1/2}$, inequality (16) holds certainly if $L > 128$. By an easy enumeration of cases we verify that it holds for each pair $\langle L, M\rangle$, with $k(L) = r$, $k(M) = 1$, unless $\langle L, M\rangle \in \mathfrak{M}$.

Suppose now that $l = 3$. If $q(n) > 3$ it is again sufficient to prove (15). By (8) we have

$$|Q_n^{(\varepsilon)}(\alpha, \beta)| > 2^{-1/2}(\alpha - \beta) \geqslant 1$$

unless $1 > 2^{-1/2}(\alpha - \beta) = 2^{-1/2}K^{1/2}$, i.e. $K = 1$. Since, as we already know, $|Q_n^{(\varepsilon)}(\alpha, \beta)| > 1$ unless $\langle L, M\rangle \in \mathfrak{M}$, we find that, if $q(n) > 3$, inequality (14) holds unless

$$\langle L, M\rangle \in \mathfrak{N}.$$

We have yet to consider the case $q(n) = l = 3$, i.e. $n = 12$, $k(LM) = 2$. We find directly

$$Q_{12}^{(\varepsilon)}(\alpha, \beta) = L - \varepsilon 2^{1/2} L^{1/2} M^{1/2} - M$$

and since $M < \frac{1}{4}L$,

$$|Q_n^{(\varepsilon)}(\alpha, \beta)| > (\tfrac{3}{4} - 2^{-1/2})L.$$

Thus $|Q_n^{(\varepsilon)}(\alpha, \beta)| > 3$ unless $L \leqslant 12(3 - 2^{3/2})^{-1} < 75$. By an enumeration of cases we find that $|Q_n^{(\varepsilon)}(\alpha, \beta)| > 3$ unless $\langle L, M\rangle \in \mathfrak{N}$.

It remains to consider $l \geqslant 5$. Here we notice first that for all $\langle L, M\rangle$ in question

$$2^{-1/2}K^{1/2}\alpha \geqslant 5 \qquad \text{or } \kappa \geqslant 2 \text{ or } \langle L, M\rangle = \langle 9, 1\rangle,$$
$$2^{-1/2}K^{1/2}\alpha \geqslant 5^{1/2} \quad \text{or } \kappa \geqslant 5 \text{ or } \langle L, M\rangle = \langle 9, 2\rangle,$$
$$2^{-1/2}K^{1/2}\alpha \geqslant 5^{1/4} \quad \text{or } \langle L, M\rangle = \langle 5, 1\rangle, \langle 9, 2\rangle.$$

It follows that, if $\langle L, M\rangle \neq \langle 5, 1\rangle, \langle 9, 1\rangle, \langle 9, 2\rangle$,

$$(2^{-1/2}K^{1/2}\alpha)^{\varphi(\eta\kappa)} > 5;$$

hence also for all $l \geqslant 5$

$$(2^{-1/2}K^{1/2}\alpha^{(q(l)-3)/2})^{\varphi(\eta\kappa)} > q(l), \tag{17}$$

and inequality (14) follows by (8).

If $\langle L, M\rangle = \langle 5, 1\rangle, \langle 9, 1\rangle, \langle 9, 2\rangle$, we find directly

$$(2^{-1/2}K^{1/2}\alpha^2)^{\varphi(\eta\kappa)} > 7;$$

hence (17) holds if $q(l) \geqslant 7$. It remains to consider the cases $\langle L, M\rangle = \langle 5, 1\rangle, \langle 9, 1\rangle, \langle 9, 2\rangle, l = 5$ or 15. Their direct examination leads to the exceptions stated in the theorem. The proof for $K > 0$ is complete.

2. $K < 0$. By the fundamental lemma of [7]

$$|Q_n(\alpha, \beta)| > |\alpha|^{\varphi(n) - 2^{\nu(n)}\log^2 n} \quad \text{for} \quad n > N(\alpha, \beta). \tag{18}$$

On the other hand, by (5) and (6), $Q_n^{(\varepsilon)}(\alpha, \beta)$ can easily be represented as the products of $B^{\varphi(\nu)/2}$ and 2 or 1 expressions of the form

$$\prod_{\chi(r)=\text{const}\neq 0} |x - \zeta_m^r|, \quad \text{where} \quad x = -A^{1/2}B^{-1/2},\ \pm iA^{1/2}B^{-1/2},$$

and $\chi(r)$ is a real character $\bmod m = \kappa$ or 4κ, respectively. Since $|A^{1/2}B^{-1/2}| = 1$, $m \leqslant 2n$, we get by Lemma 3

$$|Q_n^{(\varepsilon)}(\alpha, \beta)| < |\alpha|^{\varphi(n)/2}\exp\bigl(4(2n)^{1/2}(\log 2n)^2\bigr). \tag{19}$$

It follows from (10), (18) and (19) that for $n > N(\alpha, \beta)$

$$|Q_n^{(\varepsilon)}(\alpha, \beta)| > |\alpha|^{\varphi(n)/2 - 2^{\nu(n)}\log^3 n}\exp\bigl(-4(2n)^{1/2}(\log 2n)^2\bigr).$$

Since, however, if $K < 0$, $|\alpha| \geqslant 2^{1/2}$ and for $n > 10^{40}$

$$\frac{\log 2}{2}\bigl(\tfrac{1}{2}\varphi(n) - 2^{\nu(n)}\log^3 n\bigr) - 4(2n)^{1/2}(\log 2n)^2 > \log n,$$

we find for $n > \max\bigl(N(\alpha, \beta), 10^{40}\bigr)$

$$|Q_n^{(\varepsilon)}(\alpha, \beta)| > n,$$

which completes the proof. □

Let us remark that Theorem 1 implies the following

Corollary. *If $k(LM) = 1$, $K > 0$, n is odd > 3, then P_n has at least two primitive prime factors, except for $n = 5$, $\langle L, M\rangle = \langle 9, 1\rangle$.*

It follows that all terms from the fifth onwards of the above sequences P_n are composite.

Theorem 2. *If $k\big(M \max(K, L)\big) = \pm 1, \pm 2$, then $q(P_n) \geqslant n + 1$ for $n \geqslant n_0(L, M)$.*

The theorem follows at once from two lemmas.

Lemma 4. *If P_n is an arbitrary Lehmer sequence and n runs through all numbers $\not\equiv 0 \pmod 4$, then $q(P_n) \geqslant n + 1$ for $n \geqslant n_0(L, M)$.*

The proof is analogous to the proof of Lemma 2 of [6].

Lemma 5. *If P_n is an arbitrary Lehmer sequence and n runs through all numbers $\equiv 0 \pmod \kappa$, $\kappa = k\big(M \max(K, L)\big)$, then $q(P_n) \geqslant n + 1$ for $n \geqslant n_0(L, M)$.*

Proof. By Lemma 4 we can suppose $n \equiv 0 \pmod 4$. If κ is odd, then P_n has at least one primitive prime factor q for n large enough, by the theorem quoted in the introduction. q is of the form $nk + (KL|q)$ and so $q \equiv (KL|q) \pmod{4\kappa}$. Hence $(LM|q) = 1$, which in view of the formula

$$(\alpha/\beta)^{(q-(KL|q))/2} \equiv (LM|q) \pmod q \tag{20}$$

implies that $P_{(q-(KL|q))/2}$ is divisible by q. Since q is a primitive prime factor of P_n, we cannot have $q - (KL|q) = n$, whence $q \geqslant 2n - 1$.

The same argument applies if κ is even and $n/2\kappa$ is even. If the latter ratio is odd, then by Theorem 1 for n large enough P_n has at least two primitive prime factors. One at least of these is $\geqslant n + 1$, which completes the proof. □

Addendum*

Since the exact analogue of Schur's inequality for imprimitive characters is not explicitly proved in [3] nor apparently anywhere else we shall show

Theorem A1. *For every non-principal character $\chi \bmod m$ and all integers a, b*

$$\left|\sum_{n=a}^{b} \chi(n)\right| < m^{1/2} \log m.$$

Let $S(\chi) = \max\limits_{a,b}\left|\sum\limits_{n=a}^{b} \chi(n)\right|$. We shall need the following lemmas.

* Added in 2005

Lemma A1. *For a primitive character* $\chi_1 \bmod k > 1$

$$S(\chi_1) < \frac{2}{3} k^{1/2} \log k + \frac{1}{3} k^{1/2} \log 3.$$

Proof. Following Davenport ([1a], p. 136) we have

$$S(\chi_1) \leqslant 2k^{1/2} \int_{1/2k}^{1/2} (\sin \pi\beta)^{-1} \, d\beta.$$

Now $\sin \pi\beta > 2\beta$ and $\sin \pi\beta > 3\beta$ for $0 < \beta < \frac{1}{2}$ and $0 < \beta < \frac{1}{6}$, respectively, hence the right hand side is less than

$$\frac{2}{3} k^{1/2} \int_{1/2k}^{1/6} \frac{d\beta}{\beta} + k^{1/2} \int_{1/6}^{1/2} \frac{d\beta}{\beta}$$
$$= \frac{2}{3} k^{1/2} \log \frac{k}{3} + k^{1/2} \log 3 = \frac{2}{3} k^{1/2} \log k + \frac{1}{3} k^{1/2} \log 3. \qquad \square$$

Lemma A2. *For a primitive character* $\chi_1 \bmod k > 1$

$$S(\chi_1) < 1 + \frac{2}{\pi} k^{1/2} \Big(\frac{1}{2} \log k + \log \log k + 1 \Big) + \frac{2}{\pi} \, \frac{k \log k}{k^{1/2} \log k - 1} \, .$$

Proof. See [3], p. 83. $\square$

Lemma A3. *If* χ *is a character* $\bmod m$ *induced by a primitive character* $\chi_1 \bmod k$, *then*

$$S(\chi) \leqslant S(\chi_1) \sum_{d \mid m/k} |\mu(d) \chi_1(d)|.$$

Proof. See [3], p. 86. $\square$

Lemma A4. *If either* $m \neq 6k$ *or* $(k, 6) \neq 1$, *then in the notation of Lemma* A3

$$\sum_{d \mid m/k} |\mu(d) \chi_1(d)| < \frac{3}{2} \Big(\frac{m}{k} \Big)^{1/2}. \tag{A1}$$

Proof. Assume first that $m \neq 6k$ and let $\dfrac{m}{k} = 2^{\alpha} 3^{\beta} \prod_{i=1}^{l} p_i^{\gamma_i}$, where $\alpha \geqslant 0$, $\beta \geqslant 0$, $\gamma_i > 0$ and $p_i > 3$ are distinct primes. We have

$$\sum_{d \mid m/k} |\mu(d) \chi_1(d)| \leqslant \sum_{d \mid m/k} |\mu(d)| = 2^{l_0 + l}, \tag{A2}$$

where

$$l_0 = \begin{cases} 0 & \text{if } \alpha = \beta = 0, \\ 1 & \text{if } \alpha + \beta > 0, \ \alpha\beta = 0, \\ 2 & \text{if } \alpha\beta > 0. \end{cases}$$

Now

$$1 < \frac{3}{2}, \quad 2 < \frac{3}{2}\cdot 2^{1/2}, \quad 2^2 < \frac{3}{2}\cdot 12^{1/2}, \quad 2 < p_i^{1/2},$$

hence, unless $\alpha = \beta = 1$,

$$2^{l_0} < \frac{3}{2}(2^\alpha 3^\beta)^{1/2}, \quad 2^l < \left(\prod_{i=1}^{l} p_i^{\gamma_i}\right)^{1/2}$$

and (A1) follows from (A2). □

Assume now that $m = 6k$ and $(k, 6) \neq 1$. Then

$$\sum_{d\mid m/k} |\mu(d)\chi_1(d)| \leqslant 2 < \frac{3}{2}\cdot 6^{1/2}.$$

Proof of Theorem A1. Let χ_1 and χ have the meaning of Lemma A3. Since χ is non-principal, we have $m \geqslant k \geqslant 3$, hence if $m = k$ we obtain from Lemma A1

$$S(\chi) < \frac{2}{3}m^{1/2}\log m + \frac{1}{3}m^{1/2}\log 3 \leqslant m^{1/2}\log m.$$

If $m > k$, but either $m \neq 6k$ or $(k, 6) \neq 1$ we have by Lemmas A3, A1 and A4,

$$\begin{aligned} S(\chi) &\leqslant \Big(\frac{2}{3}k^{1/2}\log k + \frac{1}{3}k^{1/2}\log 3\Big)\cdot\frac{3}{2}\Big(\frac{m}{k}\Big)^{1/2} \\ &= m^{1/2}\log k + \frac{1}{2}m^{1/2}\log 3 \leqslant m^{1/2}\log m - m^{1/2}\log 2 + \frac{1}{2}m^{1/2}\log 3 \\ &< m^{1/2}\log m. \end{aligned}$$

It remains to consider the case $m = 6k$, $(k, 6) = 1$. Then, by Lemma A3,

$$S(\chi) \leqslant 4S(\chi_1). \tag{A3}$$

Clearly, $S(\chi_1) \leqslant \left[\frac{k}{2}\right] = \frac{k-1}{2}$, hence

$$S(\chi) \leqslant 2(k-1)$$

and, since $2(k-1) < (6k)^{1/2}\log 6k$ for $k \leqslant 49$, we may assume that $k \geqslant 53$. Then, by Lemma A2,

$$\begin{aligned} \frac{(6k)^{1/2}\log 6k - 4S(\chi_1)}{k^{1/2}\log k} &\geqslant \sqrt{6} - \frac{4}{\pi} - \frac{8\log\log k}{\pi\log k} - \frac{16/\pi - \sqrt{6}\log 6}{\log k} \\ &\quad - \frac{4}{k^{1/2}\log k} - \frac{8}{\pi(k^{1/2}\log^2 k - \log k)} =: f(k). \end{aligned}$$

For $k \geqslant 53$ the functions $\dfrac{\log\log k}{\log k}$, $\dfrac{1}{\log k}$, $\dfrac{1}{k^{1/2}\log k}$ and $\dfrac{1}{k^{1/2}\log^2 k - \log k}$ are all de-

creasing, thus

$$f(k) \geqslant f(53) > 0.21,$$
$$(6k)^{1/2} \log 6k - 4S(\chi_1) > 0,$$

and the theorem follows from (A3). □

References

[1] P. T. Bateman, *Note on the coefficients of the cyclotomic polynomial*. Bull. Amer. Math. Soc. 55 (1949), 1180–1181.

[1a] H. Davenport, *Multiplicative Number Theory*, third ed. Grad. Texts in Math. 74, Springer, New York 2000.

[2] L. K. Durst, *Exceptional real Lehmer sequences*. Pacific J. Math. 9 (1959), 437–441.

[3] E. Landau, *Abschätzungen von Charaktersummen, Einheiten und Klassenzahlen*. Nachr. Göttingen (1918), 79–97.

[4] D. H. Lehmer, *An extended theory of Lucas' functions*. Ann. of Math. (2) 31 (1930), 419–448.

[5] A. Rotkiewicz, *On Lucas numbers with two intrinsic divisors*. Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys. 10 (1962), 229–232.

[6] A. Schinzel, *On primitive prime factors of $a^n - b^n$*. Proc. Cambridge Philos. Soc. 58 (1962), 555–562; this collection: I1, 1036–1045.

[7] —, *The intrinsic divisors of Lehmer numbers in the case of negative discriminant*. Ark. Mat. 4 (1962), 413–416.

[8] I. Schur, *Einige Bemerkungen zu der vorstehenden Arbeit des Herrn G. Polya: Ueber die Verteilung der quadratischen Reste und Nichtreste*. Nachr. Göttingen (1918), 30–36.

[9] M. Ward, *The intrinsic divisors of Lehmer numbers*. Ann. of Math. (2) 62 (1955), 230–236.

Andrzej Schinzel
Selecta

Originally published in
Acta Arithmetica VIII (1963), 251–257

On primitive prime factors of Lehmer numbers II

The present paper is devoted to the investigation of Lehmer numbers with more than two primitive prime factors. We retain the notation of [3] with small changes that will be clear from the sequel.

In particular,

$$P_n(\alpha, \beta) = \begin{cases} (\alpha^n - \beta^n)/(\alpha - \beta), & n \text{ odd}, \\ (\alpha^n - \beta^n)/(\alpha^2 - \beta^2), & n \text{ even}, \end{cases}$$

where α and β are roots of the trinomial $z^2 - L^{1/2}z + M$, and L and M are rational integers, $K = L - 4M \neq 0$. Further, $\bar{z}$ denotes the complex conjugate of any given z and $k_e(n)$ denotes a positive integer n divided by the greatest e-th power dividing it. The main result of the paper runs as follows.

Theorem. *Let $(L, M) = 1$, $e = 3, 4$ or 6. If $L^{1/2}$ is rational, $K^{1/2}$ is an irrational integer of the field $\mathbb{Q}(\zeta_e)$, K is divisible by the cube of the discriminant of this field, $\kappa_e = k_e(M)$ is square-free,*

$$\eta_e = \begin{cases} 2 & \text{if } e = 6,\ M \equiv 3 \pmod 4, \\ 1 & \text{otherwise,} \end{cases}$$

and $n/\eta_e\kappa_e$ is an integer relatively prime to e, then for $n > n_e(L, M)$, P_n has at least e primitive prime factors, and $n_e(L, M)$ can be effectively computed.

Lemma 1. *Let e, m, n be positive integers, $m \mid n$, and let χ be a character* $\bmod m$ *such that $\chi^{e+1} = \chi$ and that for all $i \not\equiv 0 \pmod e$ characters χ^i have conductor m. Further, let*

$$\zeta_m = \exp(2\pi i/m), \quad \tau_i = 1 \text{ for } i \equiv 0 \pmod e,$$

$$\tau_i = \tau(\chi^i|\zeta_m) = \sum_{\substack{r=1 \\ (r,m)=1}}^{m} \chi^i(r)\zeta_m^r, \quad \text{otherwise,}$$

let χ_n be a character $\bmod n$ *induced by χ, and let $\chi(-1)^{1/e}$ be any fixed e-th root of $\chi(-1)$.*

Then, there exist polynomials $A_i(x, y)$ $(0 \leqslant i < e)$ *with coefficients from the field* $\mathbb{Q}(\zeta_e)$ *such that*

$$\psi(\chi_n; x, y) = \prod_{\substack{r=1 \\ (r,n)=1}}^{n} \left(x - \chi(-1)^{1/e}\chi(r)\zeta_n^r y\right)$$

$$= A_0(x^e, y^e) + \sum_{i=1}^{e-1} \chi(-1)^{i/e}\tau_i x^{e-i} y^i A_i(x^e, y^e),$$

$$\overline{A}_0(x, y) = A_0(y, x), \tag{1}$$

$$\overline{A}_i(x, y) = A_{e-i}(y, x)\chi^{i-1}(-1) \quad (0 < i < e). \tag{2}$$

Proof. In the course of this proof we shall denote by $a_1, a_2, \ldots, b_1, b_2, \ldots, c_1, c_2, \ldots, d_1, d_2, \ldots$, the numbers of the field $\mathbb{Q}(\zeta_e)$, by $p_i(\xi, \eta, \ldots)$ and $s_i(\xi, \eta, \ldots)$ the i-th fundamental symmetric function and the sum of the i-th powers of the indeterminates $\xi, \eta, \ldots$, respectively. The assumptions imply that $n \geqslant m \geqslant 5$. We have

$$\psi(\chi_n; x, y) = \sum_{j=0}^{\varphi(n)} (-1)^j \chi(-1)^{j/e} x^{\varphi(n)-j} y^j p_j\left(\chi_n(1)\zeta_n, \ldots, \chi_n(-1)\zeta_n^{-1}\right) \tag{3}$$

and by the Newton formulae

$$p_j = \sum_{\alpha_1+2\alpha_2+\ldots+k\alpha_k=j} a_{\alpha_1,\alpha_2,\ldots,\alpha_k} s_1^{\alpha_1} s_2^{\alpha_2} \cdots s_k^{\alpha_k}.$$

On the other hand,

$$s_i\left(\chi_n(1)\zeta_n, \ldots, \chi_n(-1)\zeta_n^{-1}\right) = \sum_{\substack{r=1 \\ (r,n)=1}}^{n} \chi_n^i(r)\zeta_n^{ri} = \tau(\chi_n^i|\zeta_n^i).$$

Now, it follows from well known results ([1], §20, Theorem IV) that under the conditions assumed with regard to character χ, $\tau(\chi_n^i|\zeta_n^i)$ can be different from zero only if

$$i \equiv 0 \pmod{e} \quad \text{or} \quad m \,\Big|\, \frac{n}{(n, i)}$$

and in this case

$$\tau(\chi_n^i|\zeta_n^i) = \tau_i \times \begin{cases} \pm\mu\left(\dfrac{n}{(n,i)}\right) \cdot \dfrac{\varphi(n)}{\varphi(n/(n,i))}, & \text{if } i \equiv 0 \pmod{e}, \\ \mu\left(\dfrac{n}{(n,i)m}\right)\chi^i\left(\dfrac{n}{(n,i)m}\right)\chi^{-i}\left(\dfrac{i}{(n,i)}\right)\dfrac{\varphi(n)}{\varphi(n/(n,i))}, & \\ \qquad \text{if } m \,\Big|\, \dfrac{n}{(n,i)},\ i \not\equiv 0 \pmod{e}. \end{cases}$$

This implies that

$$p_j\big(\chi_n(1)\zeta_n, \ldots, \chi_n(-1)\zeta_n^{-1}\big) = \sum_{\alpha_1+2\alpha_2+\ldots+k\alpha_k=j} b_{\alpha_1,\alpha_2,\ldots,\alpha_k}\tau_1^{\alpha_1}\tau_2^{\alpha_2}\cdots\tau_k^{\alpha_k}. \tag{4}$$

Now, it follows from other well known results ([1], §20, Theorem VIII) that for suitable $c_j \neq 0$, $\tau_j = c_j\tau_1^j$; thus if

$$\alpha_1 + 2\alpha_2 + \ldots + k\alpha_k = j \equiv i \pmod{e},$$

we have

$$\tau_1^{\alpha_1}\tau_2^{\alpha_2}\cdots\tau_k^{\alpha_k} = d_{\alpha_1,\alpha_2,\ldots,\alpha_k}\tau_i. \tag{5}$$

Formulae (3), (4), (5) give

$$\psi(\chi_n; x, y) = A_0(x^e, y^e) + \sum_{i=1}^{e-1} \chi(-1)^{i/e}\tau_i x^{e-i} y^i A_i(x^e, y^e), \tag{6}$$

where

$$A_0(x, y) = \sum_{\substack{0\leqslant j\leqslant\varphi(n)\\ \alpha_1+2\alpha_2+\ldots+k\alpha_k=j\equiv 0 \pmod e}} (-1)^j\chi(-1)^{j/e} b_{\alpha_1,\ldots,\alpha_k} d_{\alpha_1,\ldots,\alpha_k} x^{(\varphi(n)-j)/e} y^{j/e},$$

$$A_i(x, y) = \sum_{\substack{0<j\leqslant\varphi(n)\\ \alpha_1+2\alpha_2+\ldots+k\alpha_k=j\equiv i \pmod e}} (-1)^j\chi(-1)^{(j-i)/e} b_{\alpha_1,\ldots,\alpha_k} d_{\alpha_1,\ldots,\alpha_k} x^{(\varphi(n)-e+i-j)/e} y^{(j-i)/e}, \qquad (0 < i < e)$$

are polynomials with coefficients from the field $\mathbb{Q}(\zeta_e)$.

To prove formulae (1) and (2), notice that

$$\prod_{\substack{r=1\\(r,n)=1}}^{n} \overline{\chi}(r) = \overline{\chi}\Bigg(\prod_{\substack{r=1\\(r,n)=1}}^{n} r\Bigg) = \chi(-1)^{\varphi(n)/e}.$$

It follows that

$$\begin{aligned}
\overline{\psi}(\chi_n; x, y) &= \prod_{\substack{r=1\\(r,n)=1}}^{n} \big(x - \chi(-1)^{-1/e}\overline{\chi}(r)\overline{\zeta}_n^r y\big)\\
&= \prod_{\substack{r=1\\(r,n)=1}}^{n} \big(-\chi(-1)^{-1/e}\overline{\chi}(r)\overline{\zeta}_n^r\big) \prod_{\substack{r=1\\(r,n)=1}}^{n} \big(y - \chi(-1)^{1/e}\chi(r)\zeta_n^r x\big)\\
&= \chi(-1)^{-\varphi(n)/e} \prod_{\substack{r=1\\(r,n)=1}}^{n} \overline{\chi}(r)\psi(\chi_n; y, x) = \psi(\chi_n; y, x).
\end{aligned}$$

Applying formula (6) successively to $\psi(\chi_n; x, y)$ and $\psi(\chi_n; y, x)$ and taking into account

the well known equality

$$\overline{\tau}_i = \chi(-1)^i \tau_{e-i} \tag{7}$$

we find (1) and (2). □

Lemma 2. *If $e = 3$, 4 or 6 and ω is a product of normalized irrational primes of the field $\mathbb{Q}(\zeta_e)$ ([1]) such that $m = \omega\overline{\omega}$ is square-free and $(m, e) = 1$, then there exists a character χ satisfying the condition of Lemma 1 and such that*

$$\tau(\chi^i|\zeta_m) = \zeta_e^{\delta_i} \chi(-1)^{ie/(4,e^2)} \overline{\omega}^{(e-i)/e} \omega^{i/e} \quad (0 < i < e).$$

Here $\arg \omega^{1/e} = \frac{1}{e} \arg \omega$, $\arg \overline{\omega}^{1/e} = \frac{1}{e} \arg \overline{\omega}$ $(-\pi < \arg z \leqslant \pi)$, $\chi(-1)^{1/(4,e^2)}$ is any fixed $(4, e^2)$-th root of $\chi(-1)$ and

$$\overline{\zeta}_e^{\delta_i} = \zeta_e^{\delta_{e-i}} \chi(-1)^{[e^2+i(4,e^2)]/(4,e^2)}. \tag{8}$$

Proof. Let $\omega = \pi_1 \pi_2 \cdots \pi_k$ be the factorization of ω in the field $\mathbb{Q}(\zeta_e)$ into normalized irrational primes. Since $\omega\overline{\omega}$ is square-free, numbers $p_j = \pi_j \overline{\pi}_j$ $(j \leqslant k)$ are distinct rational primes, and since $(\omega\overline{\omega}, e) = 1$, $p_j \nmid e$. Now, for $e = 3$, 4, 6 there exist two characters χ mod p_j such that $\chi^{e+1} = \chi$ and all χ^i $(0 < i < e)$ are primitive. It follows from the formulae, given in [1], §20.4 that for one of these characters, which we denote by χ_j,

$$\tau(\chi_j|\zeta_{p_j})^e = \chi_j(-1)^{e^2/(4,e^2)} \overline{\pi}_j^{e-1} \pi_j, \tag{9}$$

whence by (7)

$$\tau(\chi_j^{e-1}|\zeta_{p_j})^e = \chi_j(-1)^{e^2/(4,e^2)} \overline{\pi}_j \pi_j^{e-1}. \tag{10}$$

Further, it follows from the connection between $\tau(\chi_j|\zeta_{p_j})$ and $\tau(\chi_j^i|\zeta_{p_j})$ (cf. [1], §20, Theorem IX) that

$$\tau(\chi_j^2|\zeta_{p_j})^e = \overline{\pi}_j^{e-2} \pi_j^2, \tag{11}$$

$$\tau(\chi_j^{e-2}|\zeta_{p_j})^e = \overline{\pi}_j^2 \pi_j^{e-2}. \tag{12}$$

Finally, formula (7) implies that for $e = 6$

$$\tau(\chi_j^3|\zeta_{p_j})^6 = \chi_j(-1) \overline{\pi}_j^3 \pi_j^3. \tag{13}$$

Formulae (9)–(13) can be written together as follows:

$$\tau(\chi_j^i|\zeta_{p_j})^e = \chi_j(-1)^{ie^2/(4,e^2)} \overline{\pi}_j^{e-i} \pi_j^i \quad (e = 3,\ 4,\ \text{or } 6). \tag{14}$$

Put

$$\zeta_m = \prod_{j=1}^{k} \zeta_{p_j}, \quad \chi = \prod_{j=1}^{k} \chi_j.$$

([1]) An irrational prime π of the field $\mathbb{Q}(\zeta_e)$ is normalized if $\pi = A + B\zeta_3$, $A \equiv -1 \pmod 3$, $B \equiv 0 \pmod 3$ for $e = 3$ or 6, and $\pi = A + B\zeta_4$, $A \equiv 1 \pmod 4$, $B \equiv 0 \pmod 2$ for $e = 4$.

It follows from the properties of characters χ_j that χ^i have conductor m for all $i \not\equiv 0 \pmod{e}$. Besides, we find from (14) and a well known theorem ([1], §20, Theorem VI) that

$$\tau(\chi^i|\zeta_m)^e = \chi(-1)^{ie^2/(4,e^2)}\overline{\omega}^{e-i}\omega^i.$$

It follows hence that

$$\tau(\chi^i|\zeta_m) = \zeta_e^{\delta_i}\chi(-1)^{ie/(4,e^2)}\overline{\omega}^{(e-i)/e}\omega^{i/e},$$

and by (7)

$$\overline{\zeta}_e^{\delta_i} = \chi(-1)^{[e^2+i(4,e^2)]/(4,e^2)}\zeta^{\delta_{e-i}},$$

which completes the proof. □

Proof of the Theorem. Since $k_e(\alpha\overline{\alpha}) = \kappa_e$, there exist two integers α_1 and ω of the field $\mathbb{Q}(\zeta_e)$ such that $\alpha = \alpha_1^e\omega$ and $\omega\overline{\omega} = \kappa_e$.

On the other hand, by the assumption about K we have

$$K \equiv 0 \pmod{27} \quad (e = 3 \text{ or } 6), \qquad K \equiv 0 \pmod{64} \quad (e = 4).$$

Therefore, since $K = L - 4M$, $(L, M) = 1$,

$$(M, e) = (\alpha\overline{\alpha}, e) = 1$$

and *a fortiori* $(\kappa_e, e) = 1$, $(\alpha_1, e) = 1$.

It follows from the latter equality that $\operatorname{Im}\alpha_1^e \equiv 0 \pmod{(1-\zeta_e^2)^2}$. Since also $\operatorname{Im}\alpha \equiv 0 \pmod{(1-\zeta_e^2)^2}$, we get $\operatorname{Im}\omega \equiv 0 \pmod{(1-\zeta_e^2)^2}$. Since $\omega\overline{\omega}$ is square-free, ω is not divisible by any rational prime and thus ω or $-\omega$ is a product of normalized irrational primes. But $P_n(-\alpha_1^e\omega, -\overline{\alpha}_1^e\overline{\omega}) = \pm P_n(\alpha, \beta)$, therefore we can assume that ω itself has the said property. Applying Lemma 2 to ω we find a character χ satisfying the conditions of Lemma 1 and such that formulae (1), (2) hold. Let χ_{n/η_e} be the induced character mod n/η_e (by the assumption $\kappa_e \mid n/\eta_e$), and let $\chi(-1)^{1/e}$ be any fixed e-th root of $\chi(-1)$.

Now, for $j = 0, 1, \ldots, e-1$, put

$$Q_n^{(j)}(\alpha, \beta) = \psi(\chi_{n/\eta_e}; \alpha^{1/e}, \zeta_e^j\beta^{1/e}),$$

where

$$\alpha^{1/e} = \alpha_1\omega^{1/e}, \quad \beta^{1/e} = \overline{\alpha^{1/e}}.$$

Since $\beta = \overline{\alpha}$, we find from Lemma 1 and Lemma 2

$$\begin{aligned} Q_n^{(j)}(\alpha, \beta) &= A_0(\alpha, \overline{\alpha}) \\ &+ \sum_{i=1}^{e-1} \zeta_e^{\delta_i+ij}\chi(-1)^{i/e}\chi(-1)^{ie/(4,e^2)}\overline{\omega}^{(e-i)/e}\omega^{i/e}(\alpha_1^e\omega)^{(e-i)/e}\left(\overline{\alpha}_1^e\overline{\omega}\right)^{i/e}A_i(\alpha, \overline{\alpha}) \\ &= A_0(\alpha, \overline{\alpha}) + \tfrac{1}{2}\omega\overline{\omega}\sum_{i=1}^{e-1}\Big(\zeta_e^{\delta_i+ij}\chi(-1)^{i/e}\chi(-1)^{ie/(4,e^2)}\alpha_1^{e-i}\overline{\alpha}_1^i A_i(\alpha, \overline{\alpha}) \\ &\qquad + \zeta_e^{\delta_{e-i}-ij}\chi(-1)^{(e-i)/e}\chi(-1)^{(e-i)e/(4,e^2)}\alpha_1^i\overline{\alpha}_1^{e-i}A_{e-i}(\alpha, \overline{\alpha})\Big). \end{aligned} \tag{15}$$

Now, by formula (1)

$$\overline{A_0(\alpha,\overline{\alpha})} = \overline{A}_0(\overline{\alpha},\alpha) = A_0(\alpha,\overline{\alpha}),$$

and by formulae (2) and (8)

$$\overline{\zeta_e^{\delta_i+ij}\chi(-1)^{i/e}\chi(-1)^{ie/(4,e^2)}\alpha_1^{e-i}\overline{\alpha}_1^{i}A_i(\alpha,\overline{\alpha})}$$

$$= \zeta_e^{\delta_{e-i}-ij}\chi(-1)^{(e^2+i(4,e^2))/(4,e^2)}\chi(-1)^{-i/e}\chi(-1)^{-ie/(4,e^2)}\overline{\alpha}_1^{e-i}\alpha_1^{i}\overline{A}_i(\overline{\alpha},\alpha)$$

$$= \zeta_e^{\delta_{e-i}-ij}\chi(-1)^{(e-i)/e}\chi(-1)^{(e-i)e/(4,e^2)}\alpha_1^{i}\overline{\alpha}_1^{e-i}A_{e-i}(\alpha,\overline{\alpha})$$

are real. Therefore, the numbers $Q_n^{(j)}(\alpha,\beta)$ are real. On the other hand, they are of course algebraic integers and by (15) they belong to the field $\mathbb{Q}\big(\zeta_e, \chi(-1)^{1/e}\big)$. Thus, if $\chi(-1)=1$, they must be rational integers. If $\chi(-1)=-1$, $e=4$ or 6 and $(m-1)/e$ is odd. Since $M\equiv m \pmod{2e}$, $(M-1)/e$ must be odd. This gives, for $e=4$, $M\equiv 5 \pmod 8$, which is incompatible with the condition that $L^{1/2}$ is rational, $K\equiv 0 \pmod{64}$. Thus $e=6$, and we conclude that in this case numbers $Q_n^{(j)}(\alpha,\beta)$ are real integers of the field $\mathbb{Q}(\zeta_{12})$. Taking the relative conjugates of the numbers $Q_n^{(j)}(\alpha,\beta)$ with respect to the field $\mathbb{Q}(\zeta_4)$, we find as in the case of complex conjugates that they are equal. This proves that $Q_n^{(j)}(\alpha,b)$ $(0\leqslant j<e)$ are rational integers in every case.

On the other hand, since $(n/\eta_e, e)=1$, we have

$$\prod_{i=0}^{e-1}\psi(\chi_{n/\eta_e};x,\zeta_e^i y) = \prod_{\substack{r=1\\(r,n/\eta_e)=1}}^{n/\eta_e}\big(x^e-\chi(-1)\zeta_{n/\eta_e}^{re}y^e\big) \tag{16}$$

$$= Q_{n/\eta_e}\big(x^e,\chi(-1)y^e\big).$$

It follows from the definition of η_e that $\eta_e=1$ unless $\chi(-1)=-1$, and in this case $\eta_e=2$. Therefore, we get from formula (16)

$$\prod_{j=0}^{e-1}Q_n^{(j)}(\alpha,\beta) = Q_{n/\eta_e}\big(\alpha,\chi(-1)\beta\big) = Q_n(\alpha,\beta). \tag{17}$$

Further, it follows from (16), as in the analogous situation in [3], that the common prime factors of any two numbers $Q_n^{(i)}$, $Q_n^{(j)}$ $(0\leqslant i<j<e)$ must divide the discriminant of $x^{en}-1$, equal to $(en)^{en}$. However, by Lemma 1 of [3], no prime factor of en can divide $Q_n(\alpha,\beta)$ with an exponent >1. Thus the numbers $Q_n^{(i)}(\alpha,\beta)$ $(0\leqslant i<e)$ are relatively prime in pairs, and in order to prove the theorem it suffices, again by Lemma 1 of [3], to establish the inequality

$$|Q_n^{(i)}(\alpha,\beta)|>n \quad (0\leqslant i<e). \tag{18}$$

To this end, notice that by Lemma 3 of [3]

$$\log|Q_n^{(i)}(\alpha,\beta)| < \frac{\varphi(n)}{e}\log|\alpha| + 2en^{1/2}\log^2 n. \tag{19}$$

On the other hand, by the fundamental lemma of [2], we have for $n > N(\alpha, \beta)$

$$\log |Q_n(\alpha, \beta)| > \big(\varphi(n) - 2^{\nu(n)} \log^3 n\big) \log |\alpha|. \tag{20}$$

It follows from (17), (19) and (20) that for $n > N(\alpha, \beta)$

$$\log |Q_n^{(i)}(\alpha, \beta)| > \Big(\frac{\varphi(n)}{e} - 2^{\nu(n)} \log^3 n\Big) \log |\alpha| - 2e(e-1)n^{1/2} \log^2 n.$$

Since $|\alpha| \geqslant 2^{1/2}$ and for $n > 10^{60}$

$$\Big(\frac{\varphi(n)}{e} - 2^{\nu(n)} \log^3 n\Big) \frac{\log 2}{2} - 2e(e-1)n^{1/2} \log^2 n > \log n \quad (e \leqslant 6)$$

inequality (18) certainly holds for

$$n > \max\big(10^{60}, N(\alpha, \beta)\big)$$

and the theorem is proved. □

References

[1] H. Hasse, *Vorlesungen über Zahlentheorie*. Springer, Berlin 1950.

[2] A. Schinzel, *The intrinsic divisors of Lehmer numbers in the case of negative discriminant*. Ark. Mat. 4 (1962), 413–416.

[3] —, *On primitive prime factors of Lehmer numbers* I. Acta Arith. 8 (1963), 213–223; this collection: I2, 1046–1058.

Originally published in
Acta Arithmetica XV (1968), 49–70

On primitive prime factors of Lehmer numbers III

1.

The main aim of this paper is to complete the results of [5], [7] and [8] concerning Lehmer numbers with a negative discriminant. About the case of a positive discriminant I have nothing new to say except that J. Brillhart and J. L. Selfridge have found explicitly the sets $\mathfrak{M}_0$ and $\mathfrak{N}_0$ occurring in Theorem 1 of [7]. The notation of [7] is retained. In particular $\zeta_n = \exp(2\pi i/n)$,

$$P_n(\alpha, \beta) = \begin{cases} (\alpha^n - \beta^n)/(\alpha - \beta), & n \text{ odd}, \\ (\alpha^n - \beta^n)/(\alpha^2 - \beta^2), & n \text{ even}, \end{cases}$$

where α and β are roots of the trinomial $z^2 - L^{1/2}z + M$ and L and M are rational integers. $k_e(n)$ is the e-th powers-free kernel of n, n^* is the product of all distinct prime factors of n, $\overline{z}$ is the complex conjugate of z. We assume

$$L > 0 > K = L - 4M, \tag{1}$$

$$(L, M) = 1, \quad \langle L, M\rangle \neq \langle 1, 1\rangle, \langle 2, 1\rangle, \langle 3, 1\rangle, \tag{2}$$

set

$$A = \max\big\{12, \log(M \min\{k(-K), k(L))\}\big\}, \quad B = \max\{12, \log M\}$$

and prove

Theorem 1. *If $n > 3 \cdot 10^{14} A^3$ then $P_n(\alpha, \beta)$ has at least one primitive prime factor.*

Theorem 2. *For L, M satisfying* (1), (2) *set*

$$\eta = \begin{cases} 1 & \text{if } k(LM) \equiv 1 \bmod 4, \\ 2 & \text{if } k(LM) \equiv 2 \text{ or } 3 \bmod 4, \end{cases}$$

$$\eta_1 = \begin{cases} 1 & \text{if } k(KM) \equiv 1 \bmod 4, \\ 2 & \text{if } k(KM) \equiv 2 \text{ or } 3 \bmod 4, \end{cases}$$

Corrigendum, Acta Arith. 16 (1969), 101

$$\eta_2 = \begin{cases} 1 & \text{if } k(KL) \equiv 1 \bmod 4, \\ 4 & \text{if } k(KL) \equiv 2 \text{ or } 3 \bmod 4. \end{cases}$$

If $n > 3 \cdot 10^{14} A^3$ *and* $n \equiv \eta k(LM) \bmod 2\eta k(LM)$ *or* $n \equiv \eta_1 k(KM) \bmod 2\eta_1 k(KM)$ *or* $n \equiv 0 \bmod \eta_2 k(KL)$, *then* $P_n(\alpha, \beta)$ *has two primitive prime factors*; *if all three congruences hold then* $P_n(\alpha, \beta)$ *has four primitive prime factors.*

Theorem 3. *Let* $e = 3, 4$ *or* 6 *and* ζ_e *belong to the field* $\mathbb{Q}\big(\sqrt{KL}\big)$. *Set*

$$\eta_3 = \begin{cases} 1 & \text{if } KL \equiv 0 \bmod 27, \\ 3 & \text{if } KL \not\equiv 0 \bmod 27; \end{cases} \qquad \eta_4 = \begin{cases} 1 & \text{if } \ K \equiv 0 \bmod 8, \\ 2 & \text{if } \ L \equiv 0 \bmod 8, \\ 4 & \text{if } KL \not\equiv 0 \bmod 8; \end{cases}$$

$$\eta_6 = \begin{cases} 1 & \text{if } K \equiv 0 \bmod 27, \ M \equiv 1 \bmod 4 \quad \text{or} \quad L \equiv 0 \bmod 27, \ M \equiv 3 \bmod 4, \\ 2 & \text{if } K \equiv 0 \bmod 27, \ M \equiv 3 \bmod 4 \quad \text{or} \quad L \equiv 0 \bmod 27, \ M \equiv 1 \bmod 4, \\ 3 & \text{if } K \equiv 6 \bmod 9, \quad M \equiv 1 \bmod 4 \quad \text{or} \quad L \equiv 3 \bmod 9, \quad M \equiv 3 \bmod 4, \\ 6 & \text{if } K \equiv 6 \bmod 9, \quad M \equiv 3 \bmod 4 \quad \text{or} \quad L \equiv 3 \bmod 9, \quad M \equiv 1 \bmod 4. \end{cases}$$

If $n/\eta_e k_e(M)^*$ *is an integer relatively prime to* e,

$$n > 3 \cdot 10^{14} \eta_e B^3 \quad \text{and} \quad n \frac{(2n, 8)}{(n^3, 8)} > 3 \cdot 10^{14} \eta_3 B^3 \quad \text{for} \quad e = 3, \ L \equiv 0 \bmod 3,$$

then $P_n(\alpha, \beta)$ *has* $e + (e, 2)\Big[\dfrac{\eta_e + 1}{4}\Big]$ *primitive prime factors.*

Proofs of these theorems given in §§2, 3, 4 respectively require some facts already established in [6], [7], [8] and also an improved version of Lemma 1 of [8] stated below as Lemma 3. An application to the estimation of the greatest prime factor of a linear recurrence of the second order is given in §5. The result obtained completes Theorem 8 of [9]. Unfortunately, the proof of a related result of [7] concerning the greatest prime factor of certain special Lehmer numbers contains a gap, which I am unable to fill in (in the present edition a weaker result has been proved).

2.

Lemma 1. *For* $n \neq 1, 2, 3, 4, 6$ *primitive prime factors of* $P_n(\alpha, \beta)$ *coincide with prime factors of* $Q_n(\alpha, \beta)/\big(n^*, Q_n(\alpha, \beta)\big)$ *and are of the form* $nt \pm 1$.

Proof. This follows from Theorems 3.2, 3.3 and 3.4 of [2]. □

Lemma 2. *For* $n > 3 \cdot 10^{14} A^3$, (1) *and* (2) *imply the inequality*

$$|Q_n(\alpha, \beta)| > n|\alpha|^{11\varphi(n)/13}. \tag{3}$$

Proof. We have

$$|Q_n(\alpha, \beta)| = |\alpha|^{\varphi(n)} \prod_{d|n} \left| \Big(\frac{\beta}{\alpha}\Big)^d - 1 \right|^{\mu(n/d)}. \tag{4}$$

In order to estimate $|(\beta/\alpha)^d - 1|$ we apply Theorem 2 of [9]. We set there

$$\langle \alpha', \alpha'' \rangle = \begin{cases} \langle \frac{1}{2}\sqrt{Lk(K)} + \frac{1}{2}\sqrt{Kk(K)}, \frac{1}{2}\sqrt{Lk(K)} - \frac{1}{2}\sqrt{Kk(K)} \rangle & \text{if } k(-K) \leqslant k(L), \\ \langle \frac{1}{2}\sqrt{Lk(L)} + \frac{1}{2}\sqrt{Kk(L)}, \frac{1}{2}\sqrt{Lk(L)} - \frac{1}{2}\sqrt{Kk(L)} \rangle & \text{if } k(-K) > k(L); \end{cases}$$

$$\beta' = \beta'' = 1,$$

$\alpha', \alpha'', \beta', \beta''$ are integers of the field $\mathbb{Q}\big(\sqrt{KL}\big)$, and we obtain

$$\log 2 \geqslant \log \left| \left(\frac{\beta}{\alpha}\right)^d - 1 \right| \geqslant -2^5 \cdot 10^5 a_1^3 (\log n + 2)^2, \tag{5}$$

where

$$a_1 = \max\big\{\pi, \log \max\{|eD|^{1/4}, |\alpha'\beta'|, |\alpha'\beta''|, |\alpha''\beta'|, |\alpha''\beta''|\}\big\}$$
$$= \max\big\{\pi, \tfrac{1}{2} \log \max\big\{|eD|^{1/2}, M \min\{k(-K), k(L)\}\big\}\big\}$$

and D is the discriminant of the field $\mathbb{Q}\big(\sqrt{KL}\big)$. Clearly

$$D \leqslant 4k(-K)k(L)$$

and an easy computation shows that

$$\tfrac{1}{4} \log 4ek(-K)k(L) \leqslant \max\big\{\pi, \tfrac{1}{2} \log\big(M \min\{k(-K), k(L)\}\big)\big\},$$

thus

$$a_1 = \max\big\{\pi, \tfrac{1}{2} \log\big(M \min\{k(-K), k(L)\}\big)\big\}.$$

Since by (1) $\log |\alpha| = \frac{1}{2} \log M$ we get from (4) and (5)

$$\log |Q_n(\alpha, \beta)| - \log n |\alpha|^{11\varphi(n)/13}$$
$$\geqslant \tfrac{2}{13} \varphi(n) \log |\alpha| - 3.2 \cdot 10^6 \cdot 2^{\nu(n)-1} a_1^3 (\log n + 2)^2 - 2^{\nu(n)-1} \log 2 - \log n$$
$$\geqslant \tfrac{1}{13} \varphi(n) \log M - 3.3 \cdot 10^6 \cdot 2^{\nu(n)-1} a_1^3 (\log n + 2)^2.$$

For $n > 3 \cdot 10^{14} A^3 > 5 \cdot 10^{17}$ we have in virtue of Theorem 15 of [4]

$$\varphi(n) > \frac{n}{e^\gamma \log\log n + 5/(2 \log\log n)} > \frac{n}{e^\gamma \log\log n + 0.675}. \tag{6}$$

On the other hand, for every n

$$2^{\nu(n)} < 39 \sqrt[6]{n}$$

(this can be proved elementarily). The functions

$$f_r(n) = \frac{n^{r/6}}{(e^\gamma \log\log n + 0.675)(\log n + 2)^2} \quad (r = 1 \text{ or } 5)$$

are increasing for $n > e^{13}$.

If $a_1 = \pi$ we find

$$\frac{\frac{1}{13} \varphi(n) \log M}{2^{\nu(n)-1} a_1^3 (\log n + 2)^2} > \frac{\log 2}{254\pi^3} f_5(n) \geqslant \frac{\log 2}{254\pi^3} f_5(5 \cdot 10^{17}) > 10^{6.56} > 3.3 \cdot 10^6.$$

If $a_1 = \frac{1}{2}\log(M\min\{k(-K), k(L)\}) \geqslant \pi$ we find $n > 24\cdot 10^{14}a_1^3$,

$$\log M = \left(\frac{1}{2} - \frac{\log(M^{-1}\min\{-K, L\})}{2\log(M\min\{-K, L\})}\right)\log(M\min\{-K, L\})$$
$$\geqslant \frac{2\pi - \log 2}{4\pi}\log(M\min\{-K, L\}) \geqslant \frac{2\pi - \log 2}{2\pi}a_1,$$

hence

$$\frac{\frac{1}{13}\varphi(n)\log M}{2^{\nu(n)-1}a_1^3(\log n + 2)^2} > \frac{2\pi - \log 2}{507\pi a_1^2} f_5(n) \geqslant \frac{2\pi - \log 2}{507\pi a_1^2} f_5(24\cdot 10^{14}a_1^3)$$
$$= \frac{2\pi - \log 2}{507\pi}(24\cdot 10^{14})^{2/3} f_1(24\cdot 10^{14}a_1^3)$$
$$\geqslant \frac{2\pi - \log 2}{507\pi}(24\cdot 10^{14})^{2/3} f_1(24\cdot 10^{14}\pi^3) > 10^{6.53} > 3.3\cdot 10^6.$$

This completes the proof. □

Proof of Theorem 1 follows at once from Lemmata 1 and 2. □

3.

Lemma 3. *Let e, n be positive integers, $n > 2$, $(e, 2n) = 1$ or 2. Let χ be a character* mod $n(e, n)$ *of order e with conductor f, where $\left(\frac{n(e,n)}{f}, e\right) = 1$. Set*

$$\psi_n(\chi; x, y) = \prod_{\substack{r=1\\(r,n)=1}}^{n}\left(x - \chi(r)\zeta_{n(e,n)}^r y\right).$$

Then

$$Q_n(x^e, y^e) = \prod_{\varepsilon^e=1}\psi_n(\chi; x, \varepsilon y), \tag{7}$$

$$\overline{\psi}_n(\chi; x, y) = \chi(-1)^{\varphi(n)/e}\psi_n(\chi; y, x), \tag{8}$$

$$\psi(\chi; x, y) = R_0(x^e, y^e) + \sum_{i=1}^{e-1}\tau(\chi^i)x^{e-i}y^i R_i(x^e, y^e), \tag{9}$$

where R_i are polynomials over $\mathbb{Q}(\zeta_e)$ and $\tau(\chi^i)$ are normalized primitive Gaussian sums belonging to characters χ^i.

Proof. Formula (7) follows at once, since

$$\prod_{\varepsilon^e=1}\psi_n(\chi; x, \varepsilon y) = \prod_{\substack{r=1\\(r,n)=1}}^{n}\prod_{\varepsilon^e=1}\left(x - \chi(r)\zeta_{n(e,n)}^r\varepsilon y\right) = \prod_{\substack{r=1\\(r,n)=1}}^{n}\left(x^e - \zeta_{n(e,n)}^{re}y^e\right).$$

To prove formula (8) we notice that the assumptions on e and f imply

$$n(e, n) = (e^3, n^2)n/(e^2, n), \quad \left((e^3, n^2), n/(e^2, n)\right) = 1,$$

c hence

$$\chi = \chi_{(e^3,n^2)}\chi_{n/(e^2,n)}, \tag{10}$$

where $\chi_{(e^3,n^2)}$ and $\chi_{n/(e^2,n)}$ are characters $\bmod (e^3, n^2)$ and $\bmod n/(e^2, n)$, respectively, the former primitive;

$$\prod_{\substack{r=1\\(r,n)=1}}^{n} r \equiv \begin{cases} 3 \bmod 8 & \text{if } n = 4,\ e = 2,\\ 1 \bmod (e^3, n^2) & \text{otherwise;}\end{cases}$$

$$\prod_{\substack{r=1\\(r,n)=1}}^{n} r \equiv \begin{cases} -1 \bmod n & \text{if } n \text{ has a primitive root,}\\ 1 \bmod n & \text{otherwise.}\end{cases}$$

Besides

$$\prod_{\substack{r=1\\(r,n)=1}}^{n} \zeta_{n(e,n)}^{-r} = (-1)^{\varphi(n)/(e,n)};$$

$$\frac{\varphi(n)}{e} \equiv \begin{cases} 1 \bmod 2 & \text{if } n = 4,\ e = 2,\\ \dfrac{p-1}{e} \bmod 2 & \text{if } n = p^\mu,\ p \text{ odd},\\ \dfrac{p-1}{2} \bmod 2 & \text{if } n = 2p^\mu,\ p \text{ odd}, e \text{ even},\\ 0 \bmod 2 & \text{otherwise.}\end{cases}$$

It follows hence

$$\prod_{\substack{r=1\\(r,n)=1}}^{n} \overline{\chi}(r)\zeta_{n(e,n)}^{-r}$$

$$= \begin{cases} -\chi(3) = \chi(-1)^{\varphi(n)/e} & \text{if } n = 4,\ e = 2,\\ \chi(-1) = (-1)^{(p-1)/e} = (-1)^{((p-1)/e)^2} & \\ \qquad = \chi(-1)^{\varphi(n)/e} & \text{if } n = p^\mu,\ p \text{ odd},\\ \chi_{n/2}(-1)(-1)^{(p-1)/2} = (-1)^{(p-1)/2}(-1)^{(p-1)/2} & \\ \qquad = 1 = \chi(-1)^{\varphi(n)/e} & \text{if } n = 2p^\mu,\ p \text{ odd},\ e \text{ even},\\ \chi(-1) = 1 = \chi(-1)^{\varphi(n)/e} & \text{if } n = 2p^\mu,\ p,\ e \text{ odd},\\ \chi(1) = 1 = \chi(-1)^{\varphi(n)/e} & \text{otherwise}\end{cases}$$

and we get

$$\begin{aligned}\overline{\psi}_n(\chi; x, y) &= \prod_{\substack{r=1\\(r,n)=1}}^{n} \left(x - \overline{\chi}(r)\zeta_{n(e,n)}^{-r} y\right)\\ &= (-1)^{\varphi(n)} \prod_{\substack{r=1\\(r,n)=1}}^{n} \overline{\chi}(r)\zeta_{n(e,n)}^{-r} \prod_{\substack{r=1\\(r,n)=1}}^{n} \left(y - \chi(r)\zeta_{n(e,n)}^{r} x\right)\\ &= (-1)^{\varphi(n)/e}\psi_n(\chi; y, x).\end{aligned}$$

In the proof of (9) we shall denote by $a_1, a_2, \dots, b_1, b_2, \dots, c_1, c_2, \dots, d_1, d_2, \dots$ numbers of the field $\mathbb{Q}(\zeta_e)$, by $p_i(\xi, \eta, \dots)$ and $s_i(\xi, \eta, \dots)$ the i-th fundamental symmetric function and the sum of i-th powers of the indeterminates $\xi, \eta, \dots$, respectively. We have

$$\psi_n(\chi; x, y) = \sum_{j=0}^{\varphi(n)} (-1)^j x^{\varphi(n)-j} y^j p_j\big(\chi(1)\zeta_{n(e,n)}, \dots, \chi(n-1)\zeta_{n(e,n)}^{n-1}\big) \tag{11}$$

and by Newton's formulae

$$p_j = \sum_{\alpha_1+2\alpha_2+\dots+k\alpha_k=j} a_{\alpha_1\alpha_2\dots\alpha_k} s_1^{\alpha_1} s_2^{\alpha_2} \cdots s_k^{\alpha_k}. \tag{12}$$

On the other hand, in the notation of [1], §20,

$$s_i\big(\chi(1)\zeta_{n(e,n)}, \dots, \chi(n-1)\zeta_{n(e,n)}^{n-1}\big) = \frac{1}{(n,e)}\,\tau\big(\chi^i|\zeta_{n(e,n)}^i\big). \tag{13}$$

This is obvious if $(n, e) = 1$; if $(n, e) = 2$ we have by (10)

$$\chi(r+n) = \chi_{(8,n^2)}(r+n)\chi_{n/(n,4)}(r+n) = -\chi_{(8,n^2)}(r)\chi_{n/(n,4)}(r) = -\chi(r); \tag{14}$$

$$2\sum_{\substack{r=1\\(r,n)=1}}^{n} \chi^i(r)\zeta_{2n}^{ri} = \sum_{\substack{r=1\\(r,n)=1}}^{n} \chi^i(r)\zeta_{2n}^{ri} + \sum_{\substack{r=1\\(r,n)=1}}^{n} \chi^i(r+n)\zeta_{2n}^{(r+n)i} = \tau(\chi^i|\zeta_{2n}^i).$$

Now, by the reduction theory for Gaussian sums, we have

$$\tau(\chi^i|\zeta_{n(e,n)}^i) = b_i\tau(\chi^i),$$

on the other hand, by the theory of Jacobi sums

$$\tau(\chi^i) = c_i\tau(\chi)^i \quad \text{with} \quad c_i \neq 0.$$

It follows by (13)

$$s_1^{\alpha_1} s_2^{\alpha_2} \cdots s_k^{\alpha_k} = d_{\alpha_1\alpha_2\dots\alpha_k}\tau\big(\chi^{\alpha_1+2\alpha_2+\dots+k\alpha_k}\big). \tag{15}$$

Formulae (11), (12) and (15) give (9) with

$$R_i(x, y) = \sum_{\substack{0\leqslant j\leqslant\varphi(n)\\ \alpha_1+2\alpha_2+\dots+k\alpha_k=j\equiv i \bmod e}} (-1)^j a_{\alpha_1\alpha_2\dots\alpha_k} d_{\alpha_1\alpha_2\dots\alpha_k} x^{\frac{\varphi(n)+i-j}{e} - \left[\frac{i+e-1}{e}\right]} y^{\frac{j-i}{e}}. \qquad \square$$

Corollary 1. *Let $n > 2$, χ be a quadratic character* $\bmod n(n, 2)$ *with conductor f, where $n(n, 2)/f$ is odd, and let ψ_n have the meaning of Lemma* 3. *Then*

$$Q_n(x^2, y^2) = \psi_n(\chi; x, y)\psi_n(\chi; x, -y), \tag{16}$$

$$\psi_n(\chi; x, y) = R(x^2, y^2) - \sqrt{\chi(-1)f}\, xyS(x^2, y^2), \tag{17}$$

where R and S are polynomials with rational coefficients and

$$R(x, y) = \chi(-1)^{\varphi(n)/2}R(y, x), \quad S(x, y) = \chi(-1)^{\varphi(n)/2+1}S(y, x). \tag{18}$$

Besides, for n even, $\varepsilon = \pm 1$,

$$\psi_n(\chi; x, \varepsilon y) = \prod_{\substack{r=1 \\ \chi(r)=\varepsilon}}^{2n} (x - \zeta_{2n}^r y). \tag{19}$$

Proof. Formulae (16), (17) and (18) follow from (7), (9) and (8), respectively, on taking into account that $\tau(\chi) = \sqrt{\chi(-1)f}$ is irrational. Besides for n even, $\varepsilon = \pm 1$,

$$\varepsilon\chi(r)\zeta_{2n}^r = \zeta_{2n}^{r+(1-\varepsilon\chi(r))n/2}$$

and in virtue of (14) the sequence

$$r + \frac{1 - \varepsilon\chi(r)}{2} n \quad (1 \leqslant r < n,\ (r, n) = 1)$$

is a permutation of the sequence r $(1 \leqslant r < 2n,\ \chi(r) = \varepsilon)$, which implies (19). □

Lemma 4. *Let* χ *be a quadratic character* mod n *with conductor* f *and*

$$\Phi_n^{(\varepsilon)}(\chi; x, y) = \omega_n^{\varepsilon}(\chi) \prod_{\substack{r=1 \\ \chi(r)=\varepsilon}}^{n} (x - \zeta_n^r y),$$

where $\varepsilon = \pm 1$ *and*

$$\omega_n(\chi) = \begin{cases} \displaystyle\prod_{\substack{r=1 \\ \chi(r)=1}}^{n} \zeta_n^r & \text{if } f = 3, \\ 1 & \text{otherwise.} \end{cases}$$

Then

$$Q_n(x, y) = \Phi_n^{(1)}(\chi; x, y)\Phi_n^{(-1)}(\chi; x, y), \tag{20}$$

$$\Phi_n^{(\varepsilon)}(\chi; x, y) = T(x, y) - \varepsilon\sqrt{\chi(-1)f}\, U(x, y), \tag{21}$$

where T, U *are polynomials with rational coefficients and*

$$\begin{aligned} &T(x, y) = x^{2^{\nu-2}}, && U(x, y) = y^{2^{\nu-2}} && \text{if } f = 4,\ n = 2^\nu, \\ &T(x, y) = -T(y, x), && U(x, y) = U(y, x) && \text{if } f = 8,\ n = 2^\nu,\ \chi(-1) = -1 \\ & && && \text{or } f = 4,\ n = 2^{\mu+2}q^\nu \\ & && && \text{or } f = q,\ n = q^\nu,\ q \text{ prime} \equiv 3 \bmod 4, \\ &T(x, y) = T(y, x), && U(x, y) = \chi(-1)U(y, x) && \text{otherwise.} \end{aligned} \tag{22}$$

Besides we have

$$\Phi_n^{(\varepsilon)}(\chi; x^2, y^2) = \begin{cases} \Phi_n^{(\varepsilon\chi(2))}(\chi; x, y)\, \Phi_n^{(\varepsilon\chi(2))}(\chi; x, -y) & (n \text{ odd}), \\ \omega_n(\chi)^{-\varepsilon}\Phi_{2n}^{(\varepsilon)}(\chi; x, y) & (n \text{ even}). \end{cases} \tag{23}$$

Proof. Let $n = 2^\mu m$, where m/f is odd. If f is odd, there exists an integer s such that $\chi(s) = 1$,

$$(s-1, m) = \sigma = \begin{cases} 3 & \text{if } f = 3, \\ 1 & \text{otherwise.} \end{cases}$$

Hence

$$(s-1) \sum_{\substack{r=1 \\ \chi(r)=\varepsilon}}^{m(n,2)} r = \sum_{\substack{r=1 \\ \chi(r)=\varepsilon}}^{m(n,2)} sr - \sum_{\substack{r=1 \\ \chi(r)=\varepsilon}}^{m(n,2)} r \equiv 0 \bmod m(n,2)$$

and

$$\sigma \sum_{\substack{r=1 \\ \chi(r)=\varepsilon}}^{n} r \equiv 0 \bmod n \qquad \text{if } n \text{ is odd,}$$

$$\sigma \sum_{\substack{r=1 \\ \chi(r)=\varepsilon}}^{2m} r \equiv \tfrac{1}{2}\varphi(m)m \bmod 2m \qquad \text{if } n \text{ is even.}$$

In the latter case

$$\sigma \sum_{\substack{r=1 \\ \chi(r)=\varepsilon}}^{n} r = \sigma \sum_{\substack{r=1 \\ \chi(r)=\varepsilon}}^{2m} \sum_{k=0}^{2^{\mu-1}-1} (r + 2km) = \sigma 2^{\mu-1} \sum_{\substack{r=1 \\ \chi(r)=\varepsilon}}^{2m} r + \sigma\varphi(m)m \sum_{k=0}^{2^{\mu-1}-1} k$$

$$\equiv 2^{\mu-2}\varphi(m)m + 2^{\mu-2}\varphi(m)m(2^{\mu-1}-1) \equiv 2^{2\mu-3}\varphi(m)m \equiv \frac{\varphi(n)n}{4} \bmod n.$$

It follows that for f odd

$$\prod_{\substack{r=1 \\ \chi(r)=\varepsilon}}^{n} \zeta_n^{r\sigma} = (-1)^{(n-1)\varphi(n)/2}. \tag{24}$$

In particular, $\omega_n(\chi)^6 = 1$ and $\omega_n(\chi)$ belongs to $\mathbb{Q}\big(\sqrt{\chi(-1)f}\big)$. Moreover, for n odd $\omega_n(\chi) = \omega_n(\chi)^{2\chi(2)}$, thus

$$\Phi_n^{(\varepsilon)}(\chi; x^2, y^2)$$

$$= \omega_n^{\varepsilon}(\chi) \prod_{\substack{r=1 \\ \chi(r)=\varepsilon\chi(2)}}^{n} (x^2 - \zeta_n^{2r} y^2) = \omega_n^{2\varepsilon\chi(2)} \prod_{\substack{r=1 \\ \chi(r)=\varepsilon\chi(2)}}^{n} (x - \zeta_n^r y) \prod_{\substack{r=1 \\ \chi(r)=\varepsilon\chi(2)}}^{n} (x + \zeta_n^r y)$$

$$= \Phi_n^{(\varepsilon\chi(2))}(\chi; x, y)\Phi_n^{(\varepsilon\chi(2))}(\chi; x, -y),$$

which proves (23) for n odd. For n even we have

$$\Phi_n^{(\varepsilon)}(\chi; x^2, y^2) = \omega_n(\chi)^{\varepsilon} \prod_{\substack{r=1 \\ \chi(r)=\varepsilon}}^{n} (x^2 - \zeta_n^r y^2) = \omega_n(\chi)^{\varepsilon} \prod_{\substack{r=1 \\ \chi(r)=\varepsilon}}^{n} (x - \zeta_{2n}^r y)(x - \zeta_{2n}^{r+n} y)$$
$$= \omega_n(\chi)^{\varepsilon} \prod_{\substack{r=1 \\ \chi(r)=\varepsilon}}^{2n} (x - \zeta_{2n}^r y) = \omega_n(\chi)^{-\varepsilon} \Phi_{2n}^{(\varepsilon)}(\chi; x, y).$$

Since (20) is obvious, it remains to prove (21) and (22). For f odd χ is induced by $(r|f)$, thus (21) follows from Lemma 1 of [6] and the remark after formula (20) there. Further, by (24),

$$\overline{\Phi}_n^{(\varepsilon)}(\chi; x, y) = \omega_n(\chi)^{-\varepsilon}(-1)^{\varphi(n)/2} \prod_{\substack{r=1 \\ \chi(r)=\varepsilon}}^{n} \zeta_n^{-r} \prod_{\substack{r=1 \\ \chi(r)=\varepsilon}}^{n} (y - \zeta_n^r x)$$
$$= (-1)^{\varphi(n)/2} \prod_{\substack{r=1 \\ \chi(r)=\varepsilon}}^{n} \zeta_n^{-r\sigma} \Phi_n^{(\varepsilon)}(\chi; y, x) = (-1)^{n\varphi(n)/2} \Phi_n^{(\varepsilon)}(\chi; y, x),$$

which implies (22) since $\frac{1}{2}n\varphi(n)$ is odd only for $n = q^{\nu}$, q prime $\equiv 3 \bmod 4$.

For f even $\chi(m/2 + r) = -\chi(r)$, hence by (23) and (19)

$$\Phi_n^{(\varepsilon)}(\chi; x, y) = \Phi_m^{(\varepsilon)}(\chi; x^{2^{\mu}}, y^{2^{\mu}}) = \begin{cases} x^{2^{\mu}} - \varepsilon\zeta_4 y^{2^{\mu}} & \text{if } m = 4, \\ \psi_{m/2}(\chi; x^{2^{\mu}}, \varepsilon y^{2^{\mu}}) & \text{if } m > 4 \end{cases}$$

and the lemma follows from Corollary 1 since for $m > 4$

$$\chi(-1)^{\varphi(m/2)/2} = \begin{cases} -1 & \text{if } f = 8,\ n = 2^{\nu},\ \chi(-1) = -1 \\ & \text{or } f = 4,\ n = 2^{\mu+2}q^{\nu},\ q \text{ prime} \equiv 3 \bmod 4, \\ 1 & \text{otherwise.} \end{cases} \qquad \square$$

Remark. Lemma 4 can also be deduced from the results of [3]. One has only to rectify the formulae for λ_{3N} and λ_{4N} given on p. 192 there.

Lemma 5. *If $n \equiv \eta k(LM) \bmod 2\eta k(LM)$, χ is the character $\bmod \eta n$ induced by $\big(k(LM)|r\big)$,*

$$Q_n^{(\varepsilon)}(\alpha, \beta) = \psi_n\big(\chi; \sqrt{\alpha}, \varepsilon\sqrt{\beta}\big) \quad (\varepsilon = \pm 1) \tag{25}$$

and $\delta = k(L)^{\{\varphi(n)/4\}}$, then $\delta^{-1} Q_n^{(1)}(\alpha, \beta)$ and $\delta^{-1} Q_n^{(-1)}(\alpha, \beta)$ are relatively prime rational integers dividing $Q_n(\alpha, \beta)$.

Proof. The assertion is proved as Lemma 1 in [7]. One has only to verify that $Q_n^{(\varepsilon)}(\alpha, \beta)$ defined by formula (6) there coincide with $Q_n^{(\varepsilon)}(\alpha, \beta)$ defined here. Alternatively one can proceed as below in the proof of Lemma 6. $\square$

Lemma 6. *If* $n \equiv \eta_1 k(KM) \bmod 2\eta_1 k(KM)$, χ_1 *is the character* $\bmod \eta_1 n$ *induced by* $\big(k(KM)|r\big)$,

$$Q_n'^{(\varepsilon)}(\alpha,\beta) = \psi_n\big(\chi_1; \sqrt{\alpha}, \varepsilon\sqrt{\beta}\big) \quad (\varepsilon = \pm 1) \tag{26}$$

and

$$\delta_1 = k(K)^{\{\varphi(n)/4\}},$$

then $\delta_1^{-1} Q_n'^{(1)}(\alpha,\beta)$ *and* $\delta_1^{-1} Q_n'^{(-1)}(\alpha,\beta)$ *are relatively prime rational integers dividing* $Q_n(\alpha,\beta)$.

Proof. Since $\chi_1(-1) = -1$, it follows from (17) and (18) that the functions $R(x,y)(x-y)^{\varphi(n)/2}$ and $S(x,y)(x-y)^{\varphi(n)/2-1}$ are symmetric of even degree thus are expressible rationally by $(x+y)^2$ and xy. Hence the numbers $R(\alpha,\beta)K^{\varphi(n)/4}$ and $S(\alpha,\beta)K^{\varphi(n)/4-1/2}$ are rational. Since

$$\sqrt{\chi_1(-1) f(\chi_1)\alpha\beta K} = \eta_1 k(KM)\sqrt{\frac{KM}{k(KM)}}$$

is rational, it follows from (17) and (26) that the numbers $K^{\varphi(n)/4}\psi_n\big(\chi_1; \sqrt{\alpha}, \varepsilon\sqrt{\beta}\big)$ and also $\delta_1 Q_n'^{(\varepsilon)}(\alpha,\beta)$ are rational.

They are also obviously algebraic integers, thus they are rational integers. $\delta_1^2 Q_n'^{(\varepsilon)}(\alpha,\beta)^2$ are perfect squares and since they are divisible by a square-free number δ_1^2 they are divisible by its square δ_1^4. Thus $\delta_1^{-1} Q_n'^{(\varepsilon)}(\alpha,\beta)$ are rational integers ($\varepsilon = \pm 1$). Finally, they are relatively prime. Indeed, the resultant of $\psi_n(\chi_1; x, y)$ and $\psi_n(\chi_1; x, -y)$ by (16) divides the discriminant of $Q_n(x^2, y^2)$ and *a fortiori* $(2n)^{2n}$. Since by (2) $(\alpha,\beta) = 1$, it follows from (26) that any common prime factor of $\delta_1^{-1} Q_n'^{(1)}(\alpha,\beta)$ and $\delta_1^{-1} Q_n'^{(-1)}(\alpha,\beta)$ divides $2n$. On the other hand, by Lemma 1 any prime factor of $2n$ divides $Q_n(\alpha,\beta)$ at most in the first power. Since by (16) and (26)

$$Q_n(\alpha,\beta) = Q_n'^{(1)}(\alpha,\beta) Q_n'^{(-1)}(\alpha,\beta),$$

we reach the desired conclusion. □

Lemma 7. *If* $n > 4$, $n \equiv 0 \bmod \eta_2 k(KL)$, χ_2 *is the character* $\bmod n$ *induced by* $\big(k(KL)|r\big)$, $\varepsilon = \pm 1$, *q denotes a prime* $\equiv 3 \bmod 4$,

$$Q_n''^{(\varepsilon)}(\alpha,\beta) = \begin{cases} \zeta_8^{\varepsilon}\Phi_n^{(\varepsilon)}(\chi_2;\alpha,\beta) & \text{if } n = 2^\nu,\ k(KL) = -1, \\ \Phi_n^{(-\varepsilon)}(\chi_2;\alpha,\beta) & \text{if } k(KL) \equiv 5 \bmod 8,\ n \text{ odd}, \\ \Phi_n^{(\varepsilon)}(\chi_2;\alpha,\beta) & \text{otherwise}; \end{cases} \tag{27}$$

$$\delta_2 = \begin{cases} \sqrt{2} & \text{if } n = 2^\nu, \quad k(KL) = -1, \\ \sqrt{-2} & \text{if } n = 2^\nu, \quad k(KL) = -2, \\ \sqrt{-1} & \text{if } n = 2^\mu q^\nu, \ k(KL) = -1, \\ \sqrt{k(K)} & \text{if } n = q^\nu, \quad k(KL) = -q, \\ \sqrt{k(L)} & \text{if } n = 2q^\nu, \quad k(KL) = -q, \\ 1 & \text{otherwise}, \end{cases}$$

then $\delta_2^{-1} Q_n''^{(1)}(\alpha, \beta)$ *and* $\delta_2^{-1} Q_n''^{(-1)}(\alpha, \beta)$ *are relatively prime rational integers dividing* $Q_n(\alpha, \beta)$.

Proof. It is enough to prove that $\delta_2 Q_n''^{(\varepsilon)}(\alpha, \beta)$ is rational for $\varepsilon = \pm 1$; the remainder can be proved like the corresponding part of Lemma 6.

If $n = 2^\nu$ ($\nu \geqslant 3$), $k(KL) = -1$ we have by (22)

$$\delta_2 Q_n''^{(\varepsilon)}(\alpha, \beta) = \sqrt{2}\,\zeta_8^{\varepsilon}(\alpha^{2^{\nu-2}} - \varepsilon\zeta_4\beta^{2^{\nu-2}})$$

$$= \alpha^{2^{\nu-2}} + \beta^{2^{\nu-2}} + \varepsilon\sqrt{-KL}\,\frac{\alpha^{2^{\nu-2}} - \beta^{2^{\nu-2}}}{\alpha^2 - \beta^2},$$

thus $\delta_2 Q_n''^{(\varepsilon)}(\alpha, \beta)$ can be expressed rationally in terms of $(\alpha + \beta)^2 = L$ and $\alpha\beta = M$ and is rational.

If $n = 2^\nu$, $k(KL) = -2$ or $n = 2^\mu q^\nu$, $k(KL) = -1$ it follows from (22) that $T(x, y)(x^2 - y^2)$ and $U(x, y)$ are symmetric functions of even degree, hence $T(\alpha, \beta)\sqrt{KL}$ and $U(\alpha, \beta)$ are rational. Since

$$\sqrt{\chi_2(-1) f(\chi_2) KL} = k(KL)\sqrt{\frac{\eta_2 KL}{k(KL)}} \tag{28}$$

and $\delta_2 = \sqrt{k(KL)}$, it follows from (21) and (27) that $\sqrt{KL}\,\Phi_n^{(\varepsilon)}(\chi_2; \alpha, \beta)$ and $\delta_2 Q_n''^{(\varepsilon)}(\alpha, \beta)$ are rational.

If $n = q^\nu$, $k(KL) = -q$, it follows from (22) that

$$T(x, y)(x - y) \quad \text{and} \quad U(x, y)(x + y)^{-1}$$

are symmetric functions of even degree, hence

$$\sqrt{k(K)}\,T(\alpha, \beta) \quad \text{and} \quad \sqrt{k(K)}\,U(\alpha, \beta)/\sqrt{KL}$$

are rational. In the remaining cases by (22)

$$T(x, y)(x + y)^{\varphi(n)/2} \quad \text{and} \quad U(x, y)(x + y)^{\varphi(n)/2}(x^2 - y^2)^{-1}$$

are symmetric functions of even degree, thus

$$k(L)^{\{\varphi(n)/4\}} T(\alpha, \beta) \quad \text{and} \quad k(L)^{\{\varphi(n)/4\}} U(\alpha, \beta)/\sqrt{KL}$$

are rational. The desired conclusion follows from (21), (27) and (28). □

Proof of Theorem 2. In order to prove the first part of the theorem it is enough to show in view of Lemmata 1, 5, 6 and 7 that for $n > 3 \cdot 10^{14} A^3$

$$\min\{|Q_n^{(\varepsilon)}(\alpha, \beta)|, |Q_n'^{(\varepsilon)}(\alpha, \beta)|, |Q_n''^{(\varepsilon)}(\alpha, \beta)|\} > n \quad (\varepsilon = \pm 1). \tag{29}$$

Now by (25)–(27), (19), Lemma 3 of [7] and Lemma in the Addendum (page 1085) we have

$$\max\{|Q_n^{(-\varepsilon)}(\alpha, \beta)|, |Q_n'^{(-\varepsilon)}(\alpha, \beta)|, |Q_n''^{(-\varepsilon)}(\alpha, \beta)|\} < |\alpha|^{\varphi(n)/2} \exp(4n^{1/2} \log^2 n). \tag{30}$$

Since $|\alpha| = \sqrt{M} \geqslant \sqrt{2}$ we get by (3) and (6) for $n > 3 \cdot 10^{14} A^3$

$$\begin{aligned}
&\log \min\{|Q_n^{(\varepsilon)}(\alpha,\beta)|, |Q_n'^{(\varepsilon)}(\alpha,\beta)|, |Q_n''^{(\varepsilon)}(\alpha,\beta)|\} - \log n \\
&= \log|Q_n(\alpha,\beta)| - \log \max\{|Q_n^{(-\varepsilon)}(\alpha,\beta)|, |Q_n'^{(-\varepsilon)}(\alpha,\beta)|, |Q_n''^{(-\varepsilon)}(\alpha,\beta)|\} - \log n \\
&> \tfrac{11}{13}\varphi(n)\log|\alpha| - \tfrac{1}{2}\varphi(n)\log|\alpha| - 4n^{1/2}\log^2 n \\
&> \frac{9\log 2}{52} n^{1/2}\log^2 n\Big(g(n) - \frac{208}{9\log 2}\Big),
\end{aligned}$$

where

$$g(n) = \frac{n^{1/2}}{(e^{\gamma}\log\log n + 0.675)\log^2 n}. \tag{30}$$

$g(n)$ is an increasing function for $n > e^5$ and

$$g(3\cdot 10^{14}A^3) > g(5\cdot 10^{17}) > 5\cdot 10^4 > \frac{208}{9\log 2}, \tag{31}$$

thus (29) follows.

To prove the second part of the theorem we show that if n satisfies all three congruences $n \equiv \eta k(LM) \bmod 2\eta k(LM)$, $n \equiv \eta_1 k(KM) \bmod 2\eta_1 k(KM)$ and $n \equiv 0 \bmod \eta_2 k(KL)$ then

$$Q_n^2(\alpha,\beta) = \prod_{\substack{\varepsilon=\pm 1\\ \theta=\pm 1}} Q_n^{(\varepsilon,\theta)}(\alpha,\beta), \tag{32}$$

where

$$Q_n^{(\varepsilon,\theta)}(\alpha,\beta) = \frac{\delta_0 Q_n^2(\alpha,\beta)}{Q_n^{(-\varepsilon)}(\alpha,\beta)\, Q_n'^{(-\theta)}(\alpha,\beta)\, Q_n''^{(-\varepsilon\theta)}(\alpha,\beta)}, \tag{33}$$

$$\delta_0 = \begin{cases} \sqrt{-1} & \text{if } n = 4q^{\nu},\ q \text{ prime} \equiv 3 \bmod 4,\ k(KL) = -1, \\ 1 & \text{otherwise;} \end{cases}$$

$Q_n^{(\varepsilon,\theta)}(\alpha,\beta)$ are rational integers relatively prime in pairs except for $n = q^{\nu}$ or $2q^{\nu}$, when two of them have the greatest common factor q.

It follows from Lemmata 5, 6 and 7 that for $\varepsilon = \pm 1$, $\theta = \pm 1$

$$(\delta\delta_1\delta_2)^{-1} Q_n^{(-\varepsilon)}(\alpha,\beta)\, Q_n'^{(-\theta)}(\alpha,\beta)\, Q_n''^{(-\varepsilon\theta)}(\alpha,\beta)$$

is rational. On the other hand

$$\delta\delta_1\delta_2 = \begin{cases} (-1)^n q & \text{if } n = q^{\nu} \text{ or } 2q^{\nu}, \\ \delta_0 & \text{otherwise.} \end{cases}$$

This implies that $Q_n^{(\varepsilon,\theta)}(\alpha,\beta)$ is rational. Moreover, since $\chi_2 = \chi\chi_1$, we have by

(25)–(27), (19) and (23) for n odd

$$\begin{aligned} Q_n^{(\varepsilon,\theta)}(\alpha,\beta) &= \frac{\delta_0 Q_n^{(\varepsilon)}(\alpha,\beta) Q_n^{\prime(\theta)}(\alpha,\beta)}{Q_n^{\prime\prime(-\varepsilon\theta)}(\alpha,\beta)} \\ &= \frac{\delta_0 \psi_n(\chi;\sqrt{\alpha},\varepsilon\sqrt{\beta})\psi_n(\chi_1;\sqrt{\alpha},\theta\sqrt{\beta})}{\Phi_n^{(-\varepsilon\theta)}(\chi\chi_1;\sqrt{\alpha},\sqrt{\beta})\Phi_n^{(-\varepsilon\theta)}(\chi\chi_1,\sqrt{\alpha},-\sqrt{\beta})} \\ &= \delta_0 \omega_n^{\varepsilon\theta}(\chi\chi_1) \prod_{\substack{r=1\\ \chi(r)=\varepsilon\\ \chi_1(r)=\theta}}^{n} \left(\sqrt{\alpha}-\zeta_n^r\sqrt{\beta}\right)^2 \prod_{\substack{r=1\\ \chi(r)=-\varepsilon\\ \chi_1(r)=-\theta}}^{n} \left(\sqrt{\alpha}+\zeta_n^r\sqrt{\beta}\right)^2, \end{aligned}$$

for n even

$$\begin{aligned} Q_n^{(\varepsilon,\theta)}(\alpha,\beta) &= \frac{\delta_0 Q_n^{(\varepsilon)}(\alpha,\beta) Q_n^{\prime(\theta)}(\alpha,\beta)}{Q_n^{\prime\prime(-\varepsilon\theta)}(\alpha,\beta)} \\ &= \frac{\delta_0 \Phi_{2n}^{(\varepsilon)}(\chi;\sqrt{\alpha},\sqrt{\beta})\Phi_{2n}^{(\theta)}(\chi_1;\sqrt{\alpha},\sqrt{\beta})}{\Phi_{2n}^{(-\varepsilon\theta)}(\chi\chi_1;\sqrt{\alpha},\sqrt{\beta})} = \delta_0 \prod_{\substack{r=1\\ \chi(r)=\varepsilon\\ \chi_1(r)=\theta}}^{2n} \left(\sqrt{\alpha}-\zeta_n^r\sqrt{\beta}\right). \end{aligned}$$

Therefore $Q_n^{(\varepsilon,\theta)}(\alpha,\beta)$ is an algebraic integer and hence a rational integer. Since

$$\begin{aligned} Q_n^{(\varepsilon,\theta)}(\alpha,\beta) Q_n^{(\varepsilon,-\theta)}(\alpha,\beta) &= Q_n^{(\varepsilon)}(\alpha,\beta)^2\delta_0^2, \\ Q_n^{(\varepsilon,\theta)}(\alpha,\beta) Q_n^{(-\varepsilon,\theta)}(\alpha,\beta) &= Q_n^{\prime(\theta)}(\alpha,\beta)^2\delta_0^2, \\ Q_n^{(\varepsilon,\theta)}(\alpha,\beta) Q_n^{(-\varepsilon,-\theta)}(\alpha,\beta) &= Q_n^{\prime\prime(\varepsilon\theta)}(\alpha,\beta)^2\delta_0^2, \end{aligned} \tag{34}$$

the greatest common factor of $Q_n^{(\varepsilon_1,\theta_1)}(\alpha,\beta)$ and $Q_n^{(\varepsilon_2,\theta_2))}(\alpha,\beta)$ for $\langle\varepsilon_1,\theta_1\rangle \neq \langle\varepsilon_2,\theta_2\rangle$ divides at least two of the numbers

$$\left(Q_n^{(1)}(\alpha,\beta)^2, Q_n^{(-1)}(\alpha,\beta)^2\right), \quad \left(Q_n^{\prime(1)}(\alpha,\beta)^2, Q_n^{\prime(-1)}(\alpha,\beta)^2\right), \quad \left(Q_n^{\prime\prime(1)}(\alpha,\beta)^2, Q_n^{\prime\prime(-1)}(\alpha,\beta)^2\right),$$

equal to $|\delta^2|$, $|\delta_1^2|$, $|\delta_2^2|$, respectively. However these numbers are $\{1,q,q\}$, $\{q,1,q\}$ or $\{1,1,1\}$ according to whether $n = q^\nu$, $2q^\nu$ or otherwise. It follows that $Q_n^{(\varepsilon,\theta)}(\alpha,\beta)$ are relatively prime in pairs except for $n = q^\nu$ or $2q^\nu$, when (35) shows that two of them have the greatest common factor q.

Now, by (3), (6), (30)–(32) and (34) we have for $n > 3\cdot 10^{14}A^3$

$$\begin{aligned} \log\left|Q_n^{(\varepsilon,\theta)}(\alpha,\beta)\right| - \log n^2 &> \frac{22}{13}\varphi(n)\log|\alpha| - \frac{3}{2}\varphi(n)\log|\alpha| - 12n^{1/2}\log^2 n \\ &\geqslant \frac{5}{52}\varphi(n)\log 2 - 12n^{1/2}\log^2 n \\ &> \frac{5\log 2}{52} n^{1/2}\log^2 n\left(g(n) - \frac{624}{5\log 2}\right) > 0. \end{aligned}$$

In virtue of (33) and Lemma 1 the theorem follows. □

Corollary 2. *If $e = 1, 2, 3, 4$ or 6, ζ_e belongs to the field $\mathbb{Q}(\sqrt{KL})$ and $n > 3 \cdot 10^{14} A^3$ then $\alpha^n - \zeta_e^i \beta^n$ has a rational prime factor of the form $\dfrac{e}{(i,e)} nt \pm 1$, relatively prime to $\alpha^e - \beta^e$.*

Proof. For $e = 1$ or 2 the corollary follows at once from the divisibility $Q_{ne}(\alpha, \beta) | \alpha^n - \zeta_e \beta^n$, Lemma 1 and Lemma 2.

For $e > 2$ since

$$\zeta_e^i = \zeta_{e/(i,e)}^{i/(i,e)},$$

it is enough to consider the case $i = \pm 1$. Then

$$Q_{ne}''^{(i)}(\alpha, \beta) \mid \alpha^n - \zeta_e^i \beta^n, \quad Q_{ne}''^{(i)}(\alpha, \beta) \mid Q_{ne}(\alpha, \beta)$$

and the corollary follows from Lemma 1 and (29). □

4.

In this and in the next section we call an integer $a + b\zeta_e$ of the field $\mathbb{Q}(\zeta_e)$ *normalized* if $e = 3$ or 6, $a \equiv -1 \bmod 3$, $b \equiv 0 \bmod 3$ or $e = 4$, $a \equiv 1 \bmod 4$, $b \equiv 0 \bmod 2$, *semi-normalized* if either $a + b\zeta_e$ or $-(a + b\zeta_e)$ is normalized. Two normalized integers of $\mathbb{Q}(\zeta_e)$ which divide each other are equal.

Lemma 8. *Let $e = 3, 4$ or 6 and ω be a semi-normalized integer of $\mathbb{Q}(\zeta_e)$ such that $(\omega, \overline{\omega}) = 1$. Then there exists a character χ of order e, even for $e = 6$, such that*

$$f(\chi) = \begin{cases} 4k_e(\omega\overline{\omega})^* & \text{if } e = 6,\ \omega\overline{\omega} \equiv 3 \bmod 4, \\ k_e(\omega\overline{\omega})^* & \text{otherwise,} \end{cases}$$

$$\tau(\chi^i) = c_i^e \overline{\omega}^{e-i} \omega^i, \quad \text{where} \quad c_i \in \mathbb{Q}(\zeta_e).$$

Proof. Let $\omega = \pm\omega_0^e \prod_{k=1}^{e-1} \omega_k^k$, where each ω_k is a product of distinct normalized irrational primes of $\mathbb{Q}(\zeta_e)$ and ω_k's are relatively prime in pairs. In virtue of Lemma 2 of [8] there exists for each ω_k a character χ_k of order e such that

$$f(\chi_k^i) = \omega_k \overline{\omega}_k, \quad \tau(\chi_k^i) = \chi_k(-1)^{ei/(2,e)} \overline{\omega}_k^{e-i} \omega_k^i \quad (0 < i < e).$$

Consider the character $\chi_0 = \prod_{k=1}^{e-1} \chi_k^k$. In virtue of well known theorems we have

$$f(\chi_0) = \prod_{k=1}^{e-1} \omega_k \overline{\omega}_k = k_e(\omega\overline{\omega})^*,$$

$$\tau(\chi_0^i) = \prod_{k=1}^{e-1} \tau(\chi_k^{ki})^e = \prod_{\substack{k=1 \\ ki \not\equiv 0 \bmod e}}^{e-1} \chi_k(-1)^{eki/(2,e)} \overline{\omega}_k^{e-e\{ki/e\}} \omega_k^{e\{ki/e\}}$$

$$= \chi_0(-1)^{ei/(2,e)} \prod_{k=1}^{e-1} \overline{\omega}_k^{ke-ki} \omega_k^{ki} \prod_{\substack{k=1 \\ ki \not\equiv 0 \bmod e}}^{e-1} \overline{\omega}_k^{-ke+e+e[ki/e]} \omega_k^{-e[ki/e]}$$

$$\times \prod_{\substack{k=1 \\ ki \equiv 0 \bmod e}}^{e-1} \overline{\omega}_k^{-ke+ki} \omega_k^{ki}$$

$$= \chi_0(-1)^{ei/(2,e)} c_i^e \overline{\omega}^{e-i} \omega^i,$$

where

$$c_i = \pm \omega_0^{-1} \prod_{k=1}^{e-1} \overline{\omega}_k^{-k-[-ki/e]} \omega_k^{-[ki/e]}.$$

For $e = 3$ or 4 we have $\chi_0(-1)^{e/(2,e)} = 1$. For $e = 6$

$$\chi_0(-1) = \prod_{k=1}^{5} \chi_k(-1)^k = (-1)^{(f(\chi_1\chi_3\chi_5)-1)/6},$$

thus $\chi_0(-1) = -1$ only if $f(\chi_1\chi_3\chi_5) = k(\omega\overline{\omega}) \equiv \omega\overline{\omega} \equiv 3 \bmod 4$.

Set now

$$\chi = \begin{cases} \chi_4\chi_0 & \text{if } e = 6,\ \omega\overline{\omega} \equiv 3 \bmod 4, \\ \chi_0 & \text{otherwise,} \end{cases}$$

where χ_4 is the primitive character $\bmod 4$. For $e = 6$, $\omega\overline{\omega} \equiv 3 \bmod 4$ we have

$$\chi(-1) = 1, \quad f(\chi) = 4k_e(\omega\overline{\omega})^*,$$

$$\tau(\chi^i)^e = \tau(\chi_4^i)^e \tau(\chi_0^i)^e = (-1)^i \chi_0(-1)^i c_i^e \overline{\omega}^{e-i} \omega^i = c_i^e \overline{\omega}^{e-i} \omega^i.$$

Thus the character χ satisfies the conditions of the lemma. □

Lemma 9. *Let e, ω and χ have the meaning of Lemma 8 and ε run through e-th roots of unity. If $m(m,e)/f(\chi)$ is an integer relatively prime to e, $\chi(-1)^{\varphi(m)/2e}$ is any square root of $\chi(-1)^{\varphi(m)/e}$,*

$$Q_m^{(\varepsilon)}(\omega, \overline{\omega}) = \chi(-1)^{\varphi(m)/2e} \psi_m(\chi; \omega^{1/e}, \varepsilon\overline{\omega}^{1/e}), \tag{35}$$

χ is considered as a character $\bmod m(m,e)$ and $m > 3 \cdot 10^{14} \max^3\{12, \log \omega\overline{\omega}\}$, then $Q_m^{(\varepsilon)}(\omega, \overline{\omega})$ are rational integers, relatively prime in pairs and $|Q_m^{(\varepsilon)}(\omega, \overline{\omega})| > m$.

Proof. We have $\chi(-1)^{\varphi(m)/2} = 1$ and by Lemma 8

$$\left(\tau(\chi^i)(\omega^{1/e})^{e-i}(\varepsilon\overline{\omega}^{1/e})^i\right)^e = c_i^e(\omega\overline{\omega})^e,$$

thus

$$\chi(-1)^{\varphi(m)/2e} \in \mathbb{Q}(\zeta_e) \quad \text{and} \quad \tau(\chi^i)(\omega^{1/e})^{e-i}(\varepsilon\overline{\omega}^{1/e})^i \in \mathbb{Q}(\zeta_e).$$

It follows hence that

$$\chi(-1)^{\varphi(m)/2e} R_0(\omega, \overline{\omega}) \in \mathbb{Q}(\zeta_e)$$

and

$$\chi(-1)^{\varphi(m)/2e} \tau(\chi^i)(\omega^{1/e})^{e-i}(\varepsilon\overline{\omega}^{1/e})^i R_i(\omega, \overline{\omega}) \in \mathbb{Q}(\zeta_e) \quad (0 < i < e),$$

thus by (9) and (36)

$$Q_m^{(\varepsilon)}(\omega, \overline{\omega}) \in \mathbb{Q}(\zeta_e).$$

On the other hand, $Q_m^{(\varepsilon)}(\omega, \overline{\omega})$ is real because by (8)

$$\begin{aligned}\overline{\chi(-1)^{\varphi(m)/2e}\psi_m(\chi; \omega^{1/e}, \varepsilon\overline{\omega}^{1/e})} &= \chi(-1)^{-\varphi(m)/2e}\psi_m(\chi; \overline{\omega}^{1/e}, \varepsilon^{-1}\omega^{1/e}) \\ &= \chi(-1)^{\varphi(m)/2e}\psi_m(\chi; \varepsilon^{-1}\omega^{1/e}, \overline{\omega}^{1/e}) \\ &= \chi(-1)^{\varphi(m)/2e}\psi_m(\chi; \omega^{1/e}, \varepsilon\overline{\omega}^{1/e}).\end{aligned}$$

Since $Q_m^{(\varepsilon)}(\omega, \overline{\omega})$ is obviously an algebraic integer it is a rational integer. To prove that $Q_m^{(\varepsilon)}(\omega, \overline{\omega})$ and $Q_m^{(\theta)}(\omega, \overline{\omega})$ are relatively prime for $\varepsilon \neq \theta$ we notice that by (7) the resultant of $\psi_m(\chi; x, \varepsilon y)$ and $\psi_m(\chi; x, \theta y)$ divides the discriminant of $Q_m(x^e, y^e)$ and *a fortiori* $(em)^{em}$. Since $(\omega, \overline{\omega}) = 1$ it follows by (36) that any common prime factor of $Q_m^{(\varepsilon)}(\omega, \overline{\omega})$ and $Q_m^{(\theta)}(\omega, \overline{\omega})$ divides em. On the other hand, by Lemma 1, any prime factor of $6m$ divides $Q_m(\omega, \overline{\omega})$ at most in first power. Since

$$Q_m(\omega, \overline{\omega}) = \prod_{\varepsilon} Q_m^{(\varepsilon)}(\omega, \overline{\omega}) \tag{36}$$

we reach the desired conclusion.

Now, if $(m, e) = 1$

$$\chi(-1)^{-\varphi(m)/2e} Q_m^{(\varepsilon)}(\omega, \overline{\omega}) = \overline{\omega}^{\varphi(m)/e} \prod_{\theta^e=1} \prod_{\substack{r=1 \\ \chi(r)=\theta}}^{m} \left(\frac{\omega^{1/e}}{\varepsilon\theta\overline{\omega}^{1/e}} - \zeta_m^r\right).$$

c

c Therefore, by Lemma 3 of [7]

$$|Q_m^{(\varepsilon)}(\omega, \overline{\omega})| \leqslant |\overline{\omega}|^{\varphi(m)/e} \exp(2em^{1/2}\log^2 m).$$

c If $(m, e) = 2$ the same conclusion follows from the lemma in the Addendum.

On the other hand, since $k\big((\omega + \overline{\omega})^2\big) = 1$ we have by Lemma 3 for $m > 3 \cdot 10^{14} \max^3\{12, \log \omega\overline{\omega}\} > 5 \cdot 10^{17}$

c $$|Q_m(\omega, \overline{\omega})| > m|\overline{\omega}|^{11\varphi(m)/13}.$$

It follows by (6), (31), (32) and (37) that for m in question

$$\begin{aligned}\log|Q_m^{(\varepsilon)}(\omega,\overline{\omega})| - \log m &> \frac{11}{13}\varphi(m)\log|\overline{\omega}| - \frac{e-1}{e}\varphi(m)\log|\overline{\omega}| - 2e(e-1)m^{1/2}\log^2 m\\ &\geqslant \frac{1}{78}\varphi(m)\log|\overline{\omega}| - 60m^{1/2}\log^2 m\\ &\geqslant \frac{\log 2}{156}m^{1/2}\log^2 m\left(g(m) - \frac{9360}{\log 2}\right) > 0.\end{aligned}$$

This completes the proof. □

Proof of Theorem 3. We set for $e = 3$ or 6

$$\langle\omega, m\rangle = \begin{cases}\langle\alpha, n\rangle & \text{if } K \equiv 0 \bmod 27,\\ \left\langle\zeta_4\alpha, n\,\dfrac{(2n,8)}{(n^3,8)}\right\rangle & \text{if } L \equiv 0 \bmod 27,\\ \left\langle\zeta_3^s\alpha, \dfrac{n}{3}\right\rangle & \text{if } K \equiv 6 \bmod 9,\\ \left\langle\zeta_{12}^s\alpha, \dfrac{n}{3}\cdot\dfrac{(2n,8)}{(n^3,8)}\right\rangle & \text{if } L \equiv 6 \bmod 9;\end{cases}$$

for $e = 4$

$$\langle\omega, m\rangle = \begin{cases}\langle\alpha, n\rangle & \text{if } K \equiv 0 \bmod 8,\\ \langle\zeta_4\alpha, n/2\rangle & \text{if } L \equiv 0 \bmod 8,\\ \langle\zeta_4\alpha^2, n/4\rangle & \text{if } KL \not\equiv 0 \bmod 8.\end{cases}$$

It can be verified that for a suitably chosen $s = \pm 1$, ω is a semi-normalized integer of $\mathbb{Q}(\zeta_e)$ and $m > 3\cdot 10^{14}B^3$. Moreover

$$\pm Q_n(\alpha,\beta) = \begin{cases}Q_m(\omega,\overline{\omega}) & \text{if } KL \equiv 0 \bmod e^3/(8,e^3),\\ Q_m(\omega,\overline{\omega})Q_m(\zeta_e^s\omega, \zeta_e^{-s}\overline{\omega}) & \text{otherwise.}\end{cases} \tag{37}$$

Since $\omega\overline{\omega} = M$ and $\left(n/\eta_e k_e(M)^*, e\right) = 1$, ω and m satisfy the assumptions of Lemma 9. Therefore by (37) $Q_m(\omega,\overline{\omega})$ has e pairwise relatively prime factors $> m$ and by Lemma 1 $Q_m(\omega,\overline{\omega})$ has e distinct prime factor $\equiv \pm 1 \bmod m$. These primes clearly do not divide n and again by Lemma 1 they are primitive prime factors of $P_n(\alpha,\beta)$. If $KL \equiv 0 \bmod e^3/(8,e^3)$ we have $e = e + (e,2)[(\eta_e+1)/4]$ and the theorem is proved. Otherwise the resultant of $Q_m(x,y)$ and $Q_m(\zeta_e^s x, \zeta_e^{-s}y)$ divides the discriminant of their product $Q_n(x,y)$ and *a fortiori* n^n. The same applies to the greatest common divisor of $Q_m(\omega,\overline{\omega})$ and $Q_m(\zeta_e^s\omega, \zeta_e^{-s}\overline{\omega})$. Therefore, the primitive prime factors mentioned beforehand do not divide $Q_m(\zeta_e^s\omega, \zeta_e^{-s}\overline{\omega})$. By Lemma 2 we have for $m > 3\cdot 10^{14}B^3$

$$\left|Q_m(\zeta_e^s\omega, \zeta_e^{-s}\overline{\omega})\right| > m,$$

thus for $e = 3$ we get from Lemma 1 and (38)

$$4 = e + (e,2)\left[\frac{\eta_e+1}{4}\right]$$

primitive prime factors of $P_n(\alpha, \beta)$.

Finally if $e = 4$ or 6 and $KL \not\equiv 0 \bmod e^3/8$, $P_m(\zeta_e^s \omega, \zeta_e^{-s}\overline{\omega})$ has by Theorem 2 two primitive prime factors. These factors by Lemma 1 divide $Q_m(\zeta_e^s \omega, \zeta_e^{-s}\overline{\omega})$, thus we get from (38)

$$e + 2 = e + (e, 2)\Big[\frac{\eta_e + 1}{4}\Big]$$

primitive prime factors of $P_n(\alpha, \beta)$. □

5.

Theorem 4. *Let u_n be a recurrence of the second order given by the formula $u_n = \Omega\omega^n + \Omega'\omega'^n$, where ω and ω' satisfy $z^2 - Pz + Q = 0$, P, Q, u_0, u_1 are rational integers,*

$$\Delta = P^2 - 4Q < 0, \quad P^2 \neq Q,\ 2Q,\ 3Q \tag{38}$$

and ω/ω', Ω/Ω' are multiplicatively dependent. If e is the number of roots of unity contained in $\mathbb{Q}(\sqrt{\Delta})$, u and v are the least in absolute value integers satisfying

$$(\omega/\omega')^{eu/2} = (-\Omega/\Omega')^{ev/2}, \quad v > 0, \tag{39}$$

$n > 0$ and $nv + u > 3 \cdot 10^{14} \max^3\{12, \log 2Q^2(P^2, Q)^{-1}\}$, then

$$q(u_n) \geqslant nv + u - 1$$

(*q denotes the greatest prime factor*).

Proof. Let r and s be integers such that

$$ru - sv = \sigma = (u, v).$$

It follows from (40) that $(\omega/\omega')^{u/\sigma}(-\Omega/\Omega')^{-v/\sigma}$ is a root of unity, hence by the definition of e

$$\Big(\frac{\omega}{\omega'}\Big)^{eu/\sigma}\Big(-\frac{\Omega}{\Omega'}\Big)^{-ev/\sigma} = 1$$

and by the choice of u and v, $\sigma \leqslant 2$.

It follows further from (40) that

$$\Big(\frac{\omega}{\omega'}\Big)^{\sigma e/2} = \Big(-\frac{\Omega}{\Omega'}\Big)^{-erv/2}\Big(\frac{\omega'}{\omega}\Big)^{esv/2}$$

whence

$$\frac{\omega^e}{\omega'^e} = \left(\Big(\frac{\Omega}{\Omega'}\Big)^r\Big(\frac{\omega'}{\omega}\Big)^s\right)^{ev/\sigma}. \tag{40}$$

The number $(\Omega/\Omega')^r(\omega'/\omega)^s$ is a quotient of two conjugates in $\mathbb{Q}(\sqrt{\Delta})$ and is different from ± 1 since by (39) ω/ω' is not a root of unity. Therefore, it can be represented in the form $\dfrac{(L^{1/2} + K^{1/2})/2}{(L^{1/2} - K^{1/2})/2}$, where L, K are rational integers, $L > 0$, $K < 0$, $\mathbb{Q}(\sqrt{KL}) = \mathbb{Q}(\sqrt{\Delta})$

and $(4L, L-K) = 4$. Set

$$L - K = 4M, \quad (L^{1/2} + K^{1/2})/2 = \alpha, \quad (L^{1/2} - K^{1/2})/2 = \beta.$$

α^e and β^e are relatively prime integers of $\mathbb{Q}(\sqrt{\Delta})$ semi-normalized if $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\zeta_e)$. Also $\omega^e(P^2, Q)^{-e/2}$ and $\omega'^e(P^2, Q)^{-e/2}$ are such integers and since by (41)

$$\frac{\omega^e(P^2, Q)^{-e/2}}{\omega'^e(P^2, Q)^{-e/2}} = \frac{\alpha^{ev/\sigma}}{\beta^{ev/\sigma}},$$

we get

$$\omega^e(P^2, Q)^{-e/2} = \pm\alpha^{ev/\sigma}, \quad \omega'^e(P^2, Q)^{-e/2} = \pm\beta^{ev/\sigma},$$

$$\omega = \zeta_{2e}^{-\mu}(P^2, Q)^{1/2}\alpha^{v/\sigma}, \quad \omega' = \zeta_{2e}^{\mu}(P^2, Q)^{1/2}\beta^{v/\sigma}. \tag{41}$$

Since $(\Omega^2\Delta, \Omega'^2\Delta) = \big((2u_1 - Pu_0)^2, u_1^2 - Pu_1u_0 + Qu_0^2\big) = \Delta_1$ is a rational integer and by (40)

$$\left(\frac{\Omega^2\Delta/\Delta_1}{\Omega'^2\Delta/\Delta_1}\right)^{ev/2} = \left(\frac{\alpha}{\beta}\right)^{euv/\sigma},$$

it follows as before that

$$\langle\Omega(\omega - \omega'), \Omega'(\omega' - \omega)\rangle = \begin{cases} \langle\zeta_{2e}^{-v}\Delta_1^{1/2}\alpha^{u/\sigma}, \zeta_{2e}^{v}\Delta_1^{1/2}\beta^{u/\sigma}\rangle & \text{if } u \geqslant 0, \\ \langle\zeta_{2e}^{-v}\Delta_1^{1/2}\beta^{|u|/\sigma}, \zeta_{2e}^{v}\Delta_1^{1/2}\alpha^{|u|/\sigma}\rangle & \text{if } u < 0. \end{cases} \tag{42}$$

Thus we obtain

$$u_n = \zeta_{2e}^{-(n-1)\mu-v}\Delta_1^{1/2}(P^2, Q)^{(n-1)/2}(\alpha\beta)^{(|u|-u)/2\sigma}\,\frac{\alpha^{(nv+u)/\sigma} - \zeta_e^{n\mu+v}\beta^{(nv+u)/\sigma}}{\alpha^{v/\sigma} - \zeta_e^{\mu}\beta^{v/\sigma}}.$$

Since ω/ω' is not a root of unity, by (41) α/β also is not such a root, hence $\langle L, M\rangle \neq \langle 1, 1\rangle$, $\langle 2, 1\rangle$, $\langle 3, 1\rangle$. Further, it follows from (42) that

$$M = \alpha\beta \leqslant \omega\omega'(P^2, Q)^{-1} = Q(P^2, Q)^{-1}.$$

Since $\min\{-K, L\} \leqslant 2M$, we get

$$A \leqslant \max\{12, \log 2Q^2(P^2, Q)^{-2}\}$$

and in virtue of Corollary 2 $\alpha^{(nv+u)/\sigma} - \zeta_e^{n\mu+v}\beta^{(nv+u)/\sigma}$ has a rational prime factor p of the form $\dfrac{e}{(n\mu + v, e)} \cdot \dfrac{nv + u}{\sigma}\, t \pm 1$ relatively prime to $\alpha^e - \beta^e$.

Since $\big((nv + u)/\sigma, v/\sigma\big) = 1$, the highest common factor of

$$\alpha^{(nv+u)/\sigma} - \zeta_e^{n\mu+v}\beta^{(nv+u)/\sigma} \quad \text{and} \quad \alpha^{v/\sigma} - \zeta_e^{\mu}\beta^{v/\sigma}$$

divides $\alpha^e - \beta^e$. Thus p is relatively prime to $\alpha^{v/\sigma} - \zeta_e^{\mu}\beta^{v/\sigma}$, we have $p \mid u_n$ and

$$q(u_n) \geqslant p \geqslant nv + u - 1$$

except possibly if

$$\sigma = 2, \quad n\mu + v \equiv 0 \bmod e. \tag{43}$$

In that case we have by the choice of u, v

$$\Big(\frac{\omega}{\omega'}\Big)^{eu/4} \neq \Big(-\frac{\Omega}{\Omega'}\Big)^{ev/4},$$

hence by (42), (43)

$$vv/2 \not\equiv \mu u/2 \bmod 2$$

and by (38) $(nv+u)/\sigma$ is odd. The prime p being of the form $(nv+u)t/2 \pm 1$ must be at least $nv+u-1$, which completes the proof. □

Addendum*

We shall prove the following lemma used in the proof of Theorem 2 instead of Lemma 3 of [7], if $(e, n) = 2$.

Lemma. *Let χ be a character* $\bmod 2n$ *of exponent $e \equiv n \equiv 0 \bmod 2$ and let $|x| = 1$. Then*

$$\Big|\prod_{r=1}^{n}(x - \chi(r)\zeta_{2n}^{r})\Big| \leqslant \exp(2en^{1/2}\log^2 n).$$

Proof. The left hand side does not exceed $2^{\varphi(n)}$, hence we may assume that

$$2^{\varphi(n)} > \exp(2en^{1/2}\log^2 n),$$

which gives

$$\frac{\varphi(n)}{e} > \frac{2n^{1/2}\log^2 n}{\log 2}, \tag{A1}$$

$$\frac{n^{1/2}}{\log^2 n^{1/2}} > \frac{16e}{\log 2} > 23e, \quad n^{1/2} > 23e(\log 23e)^2,$$

$$n > 529e^2(\log 23e)^4, \quad \log n > 12. \tag{A2}$$

For a non-negative integer $d < e$ let $r_{d1} < r_{d2} < \ldots < r_{dk_d}$ be all integers r such that $1 \leqslant r \leqslant n$ and $\chi(r) = \zeta_e^d$. Let N_i and N_{ij} be the number of $r \leqslant r_{di}$ such that $\chi(r) = 0$ and $\chi(r) = \zeta_e^i$, respectively. We have

$$N_i + \sum_{j=0}^{e-1} N_{ij} - r_{di} = 0, \tag{A3}$$

$$N_i = r_{di} - \sum_{\delta|2n}\mu(\delta)\Big[\frac{r_{di}}{\delta}\Big] = r_{di}\Big(1 - \sum_{\delta|2n}\frac{\mu(\delta)}{\delta}\Big) + \sum_{\delta|2n}\mu(\delta)\Big\{\frac{r_{di}}{\delta}\Big\},$$

* Added in 2005

hence

$$\left|\frac{r_{di}}{2n}\big(2n-\varphi(2n)\big)-N_i\right| \leqslant \max_{\varepsilon=\pm 1}\sum_{\substack{\delta\mid 2n\\ \mu(\delta)=\varepsilon}} 1 = 2^{\nu(2n)-1} < (2n)^{1/2}. \tag{A4}$$

On the other hand, by Theorem A1 from Addendum to paper I2 (p. 1055), which we apply successively to characters $\chi, \chi^2, \ldots, \chi^{e-1}$, we have

$$\left|\zeta_e^{-hd}\sum_{j=0}^{e-1} N_{ij}\zeta_e^{hj}\right| < (2n)^{1/2}\log 2n \quad (1\leqslant h<e,\ 1\leqslant i\leqslant k_d). \tag{A5}$$

Adding the inequalities (A4) and (A5) to the equality (A3) we obtain

$$\left|eN_{id}-\frac{\varphi(2n)}{2n}\,r_{di}\right| < e(2n)^{1/2}\log 2n.$$

Since $N_{id}=i$, it follows that

$$\left|\frac{r_{di}}{2n}-\frac{i}{\varphi(2n)/e}\right| < \frac{e(2n)^{1/2}\log 2n}{\varphi(2n)}\,. \tag{A6}$$

Defining N_0 and N_{0j} as the number of $r \leqslant n$ such that $\chi(r)=0$ and $\chi(r)=\zeta_e^j$, respectively, and arguing similarly we obtain

$$\left|\frac{n}{2n}-\frac{k_d}{\varphi(2n)/e}\right| < \frac{e(2n)^{1/2}\log 2n}{\varphi(2n)}\,,$$

hence

$$\frac{\varphi(n)}{e}+(2n)^{1/2}\log 2n > k_d > \frac{\varphi(n)}{e}-(2n)^{1/2}\log 2n. \tag{A7}$$

Now, put

$$l=\left\lceil \frac{\varphi(n)}{e}-(2n)^{1/2}\log 2n\right\rceil. \tag{A8}$$

It follows from (A1) and (A2) that

$$\frac{\varphi(n)}{e}-\frac{e}{2} > l > \frac{\varphi(n)}{2e}\,, \tag{A9}$$

hence we may choose an integer m prime to $e/2$ such that

$$\frac{\varphi(n)}{e} \geqslant m > \frac{\varphi(n)}{e}-\frac{e}{2} > l > m-(2n)^{1/2}\log 2n. \tag{A10}$$

It follows from (A1), (A2) and (A10) that

$$m > \pi(m-l). \tag{A11}$$

Let $x_0=\left[\frac{m}{\pi}\arg x+\frac{1}{2}\right]$. For $i\leqslant l$ we have

$$\frac{r_{di}}{2n}-\frac{1}{2\pi}\arg x=\frac{i-x_0}{2m}+\rho_{di},$$

where, by (A5), (A7)–(A9) and (A1)

$$|\rho_{di}| \leqslant \frac{e(2n)^{1/2}\log 2n}{\varphi(2n)} + \frac{i(\varphi(n)/e - m)}{2\varphi(n)m/e} + \frac{1}{4m} \tag{A12}$$
$$\leqslant \frac{e(2n)^{1/2}\log 2n}{2\varphi(n)} + \frac{e/2}{2\varphi(n)/e} + \frac{e}{2\varphi(n)} < \frac{e(2n)^{1/2}\log 3n}{2\varphi(n)}.$$

Now, we have

$$\prod_{r=1}^{n}|x - \chi(r)\zeta_{2n}^{r}| = \prod_{d=0}^{e-1}\prod_{i=1}^{k_d}|x - \zeta_e^d\zeta_{2n}^{r_{di}}| \leqslant 2\prod_{d=0}^{e-1}2^{k_d-l}\prod\nolimits_d\big(x - \zeta_e^d\zeta_{2n}^{r_{di}}\big),$$

where the product $\prod_d$ and later the sum $\sum_d$ are taken over all integers i such that $1 \leqslant i \leqslant l$ and

$$i \not\equiv \varepsilon m + x_0 \bmod 2m \quad \text{if} \quad d = \varepsilon\frac{e}{2} \quad (\varepsilon = 0 \text{ or } 1). \tag{A13}$$

Hence, by (A7) and (A8),

$$\prod_{r=1}^{n}|x - \chi(r)\zeta_{2n}^{r}| \leqslant 2^{2e(2n)^{1/2}\log 2n+1}\prod_{d=0}^{e-1}\prod\nolimits_d|x - \zeta_e^d\zeta_{2n}^{r_{di}}|. \tag{A14}$$

On the other hand,

$$\begin{aligned}
P &= \prod_{d=0}^{e-1}\prod\nolimits_d|x - \zeta_e^d\zeta_{2n}^{r_{di}}|\,|1 - \zeta_e^d\zeta_{2m}^{i-x_0}|^{-1}\\
&= \prod_{d=0}^{e-1}\prod\nolimits_d\Big|\sin\Big(\pi\frac{d}{e} + \pi\frac{r_{di}}{2n} - \frac{1}{2}\arg x\Big)\Big|\,\Big|\sin\Big(\frac{\pi d}{e} + \frac{\pi}{2m}(i - x_0)\Big)\Big|^{-1}\\
&= \prod_{d=0}^{e-1}\prod\nolimits_d\Big|\sin\Big(\pi\frac{d}{e} + \frac{\pi}{2m}(i - x_0) + \pi\rho_{di}\Big)\Big|\,\Big|\sin\Big(\frac{\pi d}{e} + \frac{\pi}{2m}(i - x_0)\Big)\Big|^{-1}\\
&\leqslant \prod_{d=0}^{e-1}\prod\nolimits_d\Big(|\cos\pi\rho_{di}| + |\sin\pi\rho_{di}|\,\Big|\cot\Big(\pi\frac{d}{e} + \frac{\pi}{2m}(i - x_0)\Big)\Big|\Big).
\end{aligned}$$

However, if $\big\|\frac{x}{\pi}\big\| \neq 0$ we have

$$|\cot x| \leqslant \frac{1}{\pi\big\|\frac{x}{\pi}\big\|}$$

and for i occurring in $\prod_d$ we have

$$\Big\|\frac{d}{e} + \frac{1}{2m}(i - x_0)\Big\| \neq 0,$$

hence by (A12)

$$P \leqslant \prod_{d=0}^{e-1}\prod\nolimits_d\Big(1 + \frac{|\rho_{di}|}{\big\|\frac{d}{e} + \frac{i-x_0}{2m}\big\|}\Big) \leqslant \exp\Big(\sum_{d=0}^{e-1}\sum\nolimits_d\frac{e(2n)^{1/2}\log 3n}{\big\|\frac{d}{e} + \frac{i-x_0}{2m}\big\|}\Big). \tag{A15}$$

Now, if

$$\frac{d_1}{e}+\frac{i_1-x_0}{2m}\equiv\frac{d_2}{e}+\frac{i_2-x_0}{2m}\bmod 1,\quad \text{where}\quad 0\leqslant d_\nu<e,\ 1\leqslant i_\nu\leqslant l,$$

then

$$\frac{e}{2}\,(i_1-x_0)\equiv\frac{e}{2}\,(i_2-x_0)\bmod m,$$

and, since $(m,\frac{e}{2})=1$, $i_1\equiv i_2 \bmod m$. In view of $1\leqslant i_\nu\leqslant l<m$, this gives $i_1=i_2$, hence $d_1\equiv d_2 \bmod e$; $d_1=d_2$.

Therefore,

$$\text{(A16)}\quad \sum_{d=0}^{e-1}\sum\nolimits_d \frac{e(2n)^{1/2}\log 3n/2\varphi(n)}{\left\|\frac{d}{e}+\frac{i-x_0}{2m}\right\|}\leqslant\sum_{j=1}^{em-1}\frac{e(2n)^{1/2}\log 3n/2\varphi(n)}{\|j/em\|}$$
$$=\frac{e(2n)^{1/2}\log 3n}{\varphi(n)}\left(1+\sum_{j=1}^{em/2-1}\frac{em}{j}\right)\leqslant\frac{e(2n)^{1/2}\log 3n}{\varphi(n)}\cdot\varphi(n)\log\varphi(n)$$
$$\leqslant e(2n)^{1/2}\big(\log^2 n+\log\tfrac{3}{2}\cdot\log n\big).$$

On the other hand,

$$\text{(A17)}\quad \prod_{d=0}^{e-1}\prod\nolimits_d|1-\zeta_e^d\zeta_{2m}^{i-x_0}|=\prod_{d=0}^{e-1}\Big(\prod\nolimits'_d|1-\zeta_e^d\zeta_{2m}^{i-x_0}|\cdot\prod\nolimits''_d|1-\zeta_e^d\zeta_{2m}^{i-x_0}|\Big)^{-1},$$

where the products $\prod'_d$ and $\prod''_d$ are taken over all integers i satisfying (A13) such that $1\leqslant i\leqslant m$ and $l<i\leqslant m$, respectively. Denoting by i_x the only positive integer $i\leqslant m$ such that $i\equiv x_0 \bmod m$ we have further

$$\text{(A18)}\quad \prod_{d=0}^{e-1}\prod\nolimits'_d|1-\zeta_e^d\zeta_{2m}^{i-x_0}|=\prod_{\substack{i=1\\ i\neq i_x}}^{m}\prod_{d=0}^{e-1}|1-\zeta_e^d\zeta_{2m}^{i-x_0}|\prod_{\substack{d=0\\ d\not\equiv\frac{i_x-x_0}{m}\cdot\frac{e}{2}\bmod e}}^{e-1}|1-\zeta_e^d\zeta_{2m}^{i_x-x_0}|$$
$$=\prod_{\substack{i=1\\ i\neq i_x}}^{m}|1-\zeta_m^{e(i-x_0)/2}|\cdot\prod_{f=1}^{e-1}|1-\zeta_e^f|=e\prod_{j=1}^{m-1}|1-\zeta_m^j|=em,$$

$$\text{(A19)}\quad \prod_{d=0}^{e-1}\prod\nolimits''_d|1-\zeta_e^d\zeta_{2m}^{i-x_0}|^{-1}=\prod_{\substack{i=l+1\\ i\neq i_x}}^{m}\prod_{d=0}^{e-1}|1-\zeta_e^d\zeta_{2m}^{i-x_0}|^{-1}$$
$$=\prod_{\substack{i=l+1\\ i\neq i_x}}^{m}|1-\zeta_m^{e(i-x_0)/2}|^{-1}.$$

When i runs through integers from $l+1$ to m except i_x, $\frac{e}{2}(i-x_0)$ gives distinct non-zero residues mod m. Hence, by (A11),

$$\prod_{\substack{i=l+1\\ i\neq i_x}}^{m} \left|1-\zeta_m^{e(i-x_0)/2}\right|^{-1} \leqslant \prod_{j=1}^{m-l} \min\left\{1, 2\sin\frac{\pi j}{m}\right\}^{-1} \leqslant \prod_{j=1}^{m-l}\frac{m}{\pi j}$$

$$\leqslant \exp\Big((m-l)\log\frac{m}{\pi(m-l)}+m-l\Big)$$

$$\leqslant \exp\Big((2n)^{1/2}\log 2n\cdot\log\frac{n^{1/2}}{2\pi\sqrt{2}\log 2n}+(2n)^{1/2}\log 2n\Big) < \exp\Big(\Big(\frac{n}{2}\Big)^{1/2}\log^2 n\Big).$$

It follows now from (A2) and (A14)–(A19) that

$$\left|\prod_{r=1}^{n}\big(x-\chi(r)\zeta_{2n}^{r}\big)\right|$$

$$\leqslant 2^{2e(2n)^{1/2}\log 2n+1}\exp\big(e(2n)^{1/2}\big(\log^2 n+\log\tfrac{3}{2}\log n\big)\big)\cdot em\cdot\exp\big(\big(\tfrac{n}{2}\big)^{1/2}\log^2 n\big)$$

$$\leqslant \exp\big(2\log 2\cdot e(2n)^{1/2}\log 2n+\log 2$$

$$+e(2n)^{1/2}\big(\log^2 n+\log\tfrac{3}{2}\cdot\log n\big)+\log\tfrac{n}{2}+\big(\tfrac{n}{2}\big)^{1/2}\log^2 n\big)$$

$$< \exp\big(2en^{1/2}\log^2 n\big). \ \square$$

References

[1] H. Hasse, *Vorlesungen über Zahlentheorie*. Springer, Berlin 1964.

[2] D. H. Lehmer, *An extended theory of Lucas' functions*. Ann. of Math. (2) 31 (1930), 419–448.

[3] T. Nagell, *Contributions à la théorie des corps et des polynômes cyclotomiques*. Ark. Mat. 5 (1964), 153–192.

[4] J. B. Rosser, L. Schoenfeld, *Approximate formulas for some functions of prime numbers*. Illinois J. Math. 6 (1962), 64–94.

[5] A. Schinzel, *The intrinsic divisors of Lehmer numbers in the case of negative discriminant*. Ark. Mat. 4 (1962), 413–416.

[6] —, *On primitive prime factors of $a^n - b^n$*. Proc. Cambridge Philos. Soc. 58 (1962), 555–562; this collection: I1, 1036–1045.

[7] —, *On primitive prime factors of Lehmer numbers* I. Acta Arith. 8 (1963), 213–223; this collection: I2, 1046–1058.

[8] —, *On primitive prime factors of Lehmer numbers* II. Acta Arith. 8 (1963), 251–257; this collection: I3, 1059–1065.

[9] —, *On two theorems of Gelfond and some of their applications*. Acta Arith. 13 (1967), 177–236; *Corrigendum* 16 (1969), 101; *Addendum* 56 (1996), 181.

Andrzej Schinzel
Selecta

Originally published in
Journal für die reine und angewandte Mathematik
268/269 (1974), 27–33

Primitive divisors of the expression $A^n - B^n$ in algebraic number fields

To Professor Helmut Hasse on his 75th birthday

Let A, B be non-zero integers of an algebraic number field K of degree l. A prime ideal $\mathfrak{P}$ of K is called a *primitive divisor* of $A^n - B^n$ if $\mathfrak{P} \mid A^n - B^n$ but $\mathfrak{P} \nmid A^m - B^m$ for $m < n$. It has been proved in [3] that if $(A, B) = 1$ and $\frac{A}{B}$ is not a root of unity then the primitive divisors exist for all $n > n_0(A, B)$ and the question has been raised whether the same is true for $n > n_0(K)$. A certain step in this direction was made by E. H. Grossman who proved in 1972 the following theorem (unpublished):

Let $E(A, B)$ be the set of positive integers n such that $A^n - B^n$ does not have a primitive divisor. Then

$$\mathrm{Card}\{n \in E(A, B) : n \leqslant x\} \leqslant \log_m x \quad \text{for} \quad x > x_0(m, l),$$

where $\log_m x$ denotes the m-fold iterated logarithm.

The aim of this paper is to give an affirmative answer to the question and in fact to prove the following stronger

Theorem 1. *If $(A, B) = 1$ and $\frac{A}{B}$ is not a root of unity then $A^n - B^n$ has a primitive divisor for all $n > n_0(d)$, where d is the degree of $\frac{A}{B}$ and $n_0(d)$ is effectively computable.*

The theorem is best possible up to the order of the function $n_0(d)$; an absolute constant cannot be expected since for $A = \sqrt[d]{2}$, $B = 1$, $A^d - B^d = 1$ has no primitive divisor.

The proof is based on four lemmata, the critical one being an easy consequence of the recent deep theorem of Baker [1], which we quote below with some changes in the notation:

Let $\alpha_1, \ldots, \alpha_k$ be non-zero algebraic numbers with degrees at most d and let the heights of $\alpha_1, \ldots, \alpha_{k-1}$ and α_k be at most H' and $H(\geqslant 2)$ respectively. For some effectively computable number $C > 0$ depending only on k, d and H' the inequalities

$$0 < |m_1 \log \alpha_1 + \ldots + m_k \log \alpha_k| < C^{-\log H \log M}$$

have no solution in rational integers $m_1, \ldots, m_k$ with absolute values at most $M(\geqslant 2)$ (the logarithms have their principal values).

Let $\mathbb{Q}\left(\frac{A}{B}\right) = K_0$, $\frac{A}{B} = \frac{\alpha}{\beta}$, where $\alpha, \beta \in K_0$; α, β are integers and $(\alpha, \beta) = \mathfrak{d}$.

Let S be a set of all isomorphic injections of K_0 in the complex field and set

$$w\left(\frac{\alpha}{\beta}\right) = \log \prod_{\sigma \in S} \max\{|\alpha^\sigma|, |\beta^\sigma|\} - \log N\mathfrak{d}$$

where N denotes the absolute norm in K_0. Clearly $w\left(\frac{\alpha}{\beta}\right)$ is independent of the choice of α, β in K_0.

Lemma 1. *If $|\alpha| = |\beta|$ but $\frac{\alpha}{\beta}$ is not a root of unity, then*

$$\log|\alpha^n - \beta^n| = n \log|\beta| + O\left(d + w\left(\frac{\alpha}{\beta}\right)\right) \log n,$$

where the constant in the symbol O depends only on d and is effectively computable.

Proof. We set in Baker's theorem $k = 2; \alpha_1 = -1, \alpha_2 = \frac{\alpha}{\beta}$, thus $\log \alpha_1 = \pi i, \log \alpha_2 = \vartheta i$, where $-\pi < \vartheta \leqslant \pi$. It follows that for a suitable constant C depending only upon d the inequality

$$0 < |\pi m + \vartheta n| < C^{-\log H \log M}$$

where H is the height of α, has no solution in rational integers m, n with absolute values at most M. However $\pi m + \vartheta n \neq 0$ since $\frac{\alpha}{\beta}$ is not a root of unity. On the other hand, if $|m| > n$ then

$$|\pi m + \vartheta n| \geqslant \pi.$$

Hence we can take $M = n$ and we obtain

$$\pi \left\| \frac{\vartheta}{\pi} n \right\| \geqslant C^{-\log H \log M}$$

where $\|x\|$ is the distance of x from the nearest integer. Since

$$2 \geqslant |e^{n\vartheta i} - 1| = 2 \sin \frac{n\vartheta}{2} \geqslant 2 \left\| \frac{n\vartheta}{\pi} \right\|$$

we get

$$\log|\alpha^n - \beta^n| = n \log|\beta| + \log|e^{n\vartheta i} - 1| = n \log|\beta| + O(\log H \log n). \tag{1}$$

The coefficients of the irreducible polynomial $N\mathfrak{d}^{-1} \prod_{\sigma \in S} (\beta^\sigma x - \alpha^\sigma)$ are rational integers and their absolute values do not exceed

$$N\mathfrak{d}^{-1} \prod_{\sigma \in S} (|\beta^\sigma| + |\alpha^\sigma|) \leqslant 2^d e^{w(\alpha/\beta)}.$$

It follows that

$$\log H = O\Big(d + w\Big(\frac{\alpha}{\beta}\Big)\Big),$$

which together with (1) implies the lemma. □

Lemma 2. *If* $|\alpha| \neq |\beta|$ *then*

$$\log|\alpha^n - \beta^n| = n \log \max\{|\alpha|, |\beta|\} + O\Big(d^2 + d w\Big(\frac{\alpha}{\beta}\Big)\Big),$$

where the constant in the symbol O *is absolute and effectively computable.*

Proof. Suppose without loss of generality that $|\alpha| < |\beta|$. We have for $n \geqslant 2$

$$2|\beta|^n \geqslant |\alpha^n - \beta^n| = |\beta|^n \left|\left|\frac{\alpha}{\beta}\right|^n - 1\right| \geqslant |\beta|^n \Big(1 - \left|\frac{\alpha}{\beta}\right|^2\Big) \tag{2}$$

and it remains to estimate $1 - \left|\dfrac{\alpha}{\beta}\right|^2$. Let T be the set of all isomorphic injections of $K_0\overline{K}_0$, where "bar" denotes the complex conjugation, and let $x^{\tau_0} = x$, $x^{\tau_1} = \overline{x}$. We have

$$\begin{aligned} 1 - \left|\frac{\alpha}{\beta}\right|^2 &= \big|N_{K_0\bar{K}_0/\mathbb{Q}}(\alpha\overline{\alpha} - \beta\overline{\beta})\big|\,|\beta|^{-2} \prod_{\substack{\tau \in T \\ \tau \neq \tau_0}} \big|(\alpha\overline{\alpha})^\tau - (\beta\overline{\beta})^\tau\big|^{-1} \\ &\geqslant N\mathfrak{d}^{2|T|/|S|} 2^{1-|T|} \prod_{\tau \in T} \max\big\{|\alpha^\tau \alpha^{\tau\tau_1}|, |\beta^\tau \beta^{\tau\tau_1}|\big\}^{-1} \\ &> N\mathfrak{d}^{2|T|/|S|} 2^{-|T|} \prod_{\tau \in T} \max\big\{|\alpha^\tau|, |\beta^\tau|\big\}^{-1} \prod_{\tau \in T} \max\{|\alpha^{\tau\tau_1}|, |\beta^{\tau\tau_1}|\}^{-1}. \end{aligned}$$

When τ runs over T, α^τ and $\alpha^{\tau\tau_1}$ run $|T|/|S| \leqslant d - 1$ times over α^σ ($\sigma \in S$). Hence

$$1 - \left|\frac{\alpha}{\beta}\right|^2 \geqslant 2^{-|T|} e^{-2w(\alpha/\beta)|T|/|S|} \geqslant 2^{-d(d-1)} e^{-2(d-1)w(\alpha/\beta)}$$

and by (2) the lemma follows. □

Lemma 3. *Let* ξ *be a number of the field* K_0 *and let* $\mathfrak{p}$ *be a prime ideal of* K_0 *which divides the rational prime* p *to the power* e ($e = \operatorname{ord}_\mathfrak{p} p > 0$). *If* $\operatorname{ord}_\mathfrak{p}(\xi - 1) > \Big[\dfrac{e}{p-1}\Big]$ *then*

$$\operatorname{ord}_\mathfrak{p}(\xi^n - 1) = \operatorname{ord}_\mathfrak{p}(\xi - 1) + \operatorname{ord}_\mathfrak{p} n.$$

Proof. See [3], Lemma 1. □

Lemma 4. *Let* $\Phi_n(x, y)$ *be the* n*-th cyclotomic polynomial in homogeneous form. If* $\mathfrak{P}$ *is a prime ideal of* K, $n > 2(2^d - 1)$, $\mathfrak{P} \mid \Phi_n(A, B)$, *and* $\mathfrak{P}$ *is not a primitive divisor of* $A^n - B^n$, *then*

$$\operatorname{ord}_\mathfrak{P} \Phi_n(A, B) \leqslant \operatorname{ord}_\mathfrak{P} n.$$

Proof. Let $\gamma = \dfrac{A}{B}$, $\mathfrak{p}$ be the prime ideal of K_0 divisible by $\mathfrak{P}$ to the power e_0 and let λ_i be the least exponent λ for which

$$\mathfrak{p}^i \mid \gamma^\lambda - 1.$$

It is obvious that $\mathfrak{p}^i \mid \gamma^\lambda - 1$ is equivalent to $\lambda_i \mid \lambda$. We have

$$\Phi_n(A, B) = B^{\varphi(n)}\Phi_n(\gamma, 1) = B^{\varphi(n)} \prod_{m \mid n} (\gamma^m - 1)^{\mu(n/m)}.$$

On the other hand, since $\mathfrak{P} \mid \Phi_n(A, B)$ and $(A, B) = 1$, $\mathfrak{P} \nmid B$. Hence

$$\operatorname{ord}_{\mathfrak{P}} \Phi_n(A, B) = e_0 \operatorname{ord}_{\mathfrak{p}} \Phi_n(\gamma, 1) = e_0 \sum_{m \mid n} \mu\Big(\frac{n}{m}\Big) \operatorname{ord}_{\mathfrak{p}}(\gamma^m - 1). \tag{3}$$

We use the notation of Lemma 3 and set $\left[\dfrac{e}{p-1}\right] = k$. If m is not a multiple of λ_1 then $\operatorname{ord}_{\mathfrak{p}}(\gamma^m - 1) = 0$. If m is a multiple of λ_i, but not a multiple of λ_{i+1} then

$$\operatorname{ord}_{\mathfrak{p}}(\gamma^m - 1) = i \quad (i \leqslant k).$$

Further, if m is a multiple of λ_{k+1} then by Lemma 3

$$\operatorname{ord}_{\mathfrak{p}}(\gamma^m - 1) = \operatorname{ord}_{\mathfrak{p}}(\gamma^{\lambda_{k+1}} - 1) + \operatorname{ord}_{\mathfrak{p}} \frac{m}{\lambda_{k+1}}.$$

Hence

$$\operatorname{ord}_{\mathfrak{p}} \Phi_n(\gamma, 1) = \sum_{i=1}^{m} \sum_{\substack{m \mid n \\ \lambda_i \mid m}} \mu\Big(\frac{n}{m}\Big) + \sum_{\substack{m \mid n \\ \lambda_{k+1} \mid m}} \mu\Big(\frac{n}{m}\Big)\big(\operatorname{ord}_{\mathfrak{p}}(\gamma^{\lambda_{k+1}} - 1) - k\big) + \sum_{\substack{m \mid n \\ \lambda_{k+1} \mid m}} \mu\Big(\frac{n}{m}\Big) \operatorname{ord}_{\mathfrak{p}} \frac{m}{\lambda_{k+1}}. \tag{4}$$

We note that $\lambda_{k+1} < n$. In fact, if $k = 0$ then the conditions that $\mathfrak{P} \mid A^n - B^n$ and $\mathfrak{P}$ is not a primitive divisor imply that there is a number $m < n$ such that $\mathfrak{P} \mid A^m - B^m$ and then $\mathfrak{p} \mid \gamma^m - 1$, i.e., $\lambda_1 < n$.

If $k > 0$ we have by Euler's theorem for the field K_0

$$\gamma^{\varphi(\mathfrak{p}^k)} \equiv 1 \bmod \mathfrak{p}^k, \quad \gamma^{\varphi(\mathfrak{p}^k)p} = \sum_{j=0}^{p} \binom{p}{j} \big(\gamma^{\varphi(\mathfrak{p}^k)} - 1\big)^j,$$

$$\operatorname{ord}_{\mathfrak{p}}\big(\gamma^{\varphi(\mathfrak{p}^k)p} - 1\big) \geqslant \min\{k + e, pk\} > k, \quad \text{thus} \quad \lambda_{k+1} \leqslant \varphi(\mathfrak{p}^k)p.$$

On the other hand, $k > 0$ implies $p \leqslant e + 1 \leqslant d + 1$ and since $N\mathfrak{p} \leqslant p^{d/e}$ we have

$$\lambda_{k+1} \leqslant p\varphi(\mathfrak{p}^k) \leqslant p\big(N(\mathfrak{p}^k) - 1\big) \leqslant p\big(p^{d/(p-1)} - 1\big) \leqslant 2(2^d - 1)$$

(the last inequality requires some elementary, but tedious calculations). It follows that $\lambda_1 \leqslant \lambda_2 \leqslant \ldots \leqslant \lambda_{k+1} < n$.

Hence $\sum\limits_{\substack{m\mid n\\ \lambda_i\mid m}} \mu\Big(\frac{n}{m}\Big) = 0$ $(i = 1, 2, \ldots, k+1)$ and by (4)

$$\begin{aligned}
\operatorname{ord}_{\mathfrak{p}} \Phi_n(\gamma, 1) &= \sum_{\substack{m\mid n\\ \lambda_{k+1}\mid m}} \mu\Big(\frac{n}{m}\Big) \operatorname{ord}_{\mathfrak{p}} \frac{m}{\lambda_{k+1}} \\
&= \sum_{\substack{m\mid n\\ \lambda_{k+1}\mid m\\ \operatorname{ord}_p(n/m)=0}} \mu\Big(\frac{n}{m}\Big) \operatorname{ord}_{\mathfrak{p}} \frac{m}{\lambda_{k+1}} + \sum_{\substack{m\mid n\\ \lambda_{k+1}\mid m\\ \operatorname{ord}_p(n/m)=1}} \mu\Big(\frac{n}{m}\Big) \operatorname{ord}_{\mathfrak{p}} \frac{m}{\lambda_{k+1}} \\
&= \sum_{\substack{m\mid n\\ \lambda_{k+1}\mid m\\ \operatorname{ord}_p(n/m)=1}} \left(\mu\Big(\frac{n}{mp}\Big) \operatorname{ord}_{\mathfrak{p}} \frac{mp}{\lambda_{k+1}} + \mu\Big(\frac{n}{m}\Big) \operatorname{ord}_{\mathfrak{p}} \frac{m}{\lambda_{k+1}}\right) \\
&= \sum_{\substack{m\mid n\\ \lambda_{k+1}\mid m\\ \operatorname{ord}_p(n/m)=1}} \mu\Big(\frac{n}{mp}\Big) \operatorname{ord}_{\mathfrak{p}} p = \begin{cases} e & \text{if } \dfrac{n}{\lambda_{k+1}} \text{ is a power of } p, \\ 0 & \text{otherwise.} \end{cases}
\end{aligned}$$

It follows by (3) that

$$\operatorname{ord}_{\mathfrak{P}} \Phi_n(A, B) \leqslant e_0 e \operatorname{ord}_p \frac{n}{\lambda_{k+1}} \leqslant \operatorname{ord}_{\mathfrak{P}} n. \qquad \square$$

Remark. Lemma 4 is an improvement of Lemma 2 of [3] where $2^l(2^l - 1)$ occurs instead of $2(2^d - 1)$. The possibility of replacing $2^l(2^l - 1)$ by $2l(2^l - 1)$ was first observed by E. Grossman (unpublished).

Proof of Theorem 1. In order to apply Lemma 4 we estimate $N_{K/\mathbb{Q}}\Phi_n(A, B)$. Clearly

$$\Phi_n(A, B) = B^{\varphi(n)}\Phi_n\Big(\frac{A}{B}, 1\Big) = B^{\varphi(n)}\Phi_n\Big(\frac{\alpha}{\beta}, 1\Big) = \Big(\frac{B}{\beta}\Big)^{\varphi(n)}\Phi_n(\alpha, \beta)$$

and since $\Big(\dfrac{B}{\beta}\Big) = \mathfrak{d}^{-1}$ we have

$$\big(\Phi_n(A, B)\big) = \mathfrak{d}^{-\varphi(n)}\big(\Phi_n(\alpha, \beta)\big),$$

$$\begin{aligned}\frac{d}{l}\log|N_{K/\mathbb{Q}}\Phi_n(A,B)| &= \log|N\Phi_n(\alpha,\beta)| - \varphi(n)\log N\mathfrak{d}\\ &= \sum_{\sigma\in S}\sum_{m|n}\mu\Big(\frac{n}{m}\Big)\log\big|(\alpha^\sigma)^m - (\beta^\sigma)^m\big| - \varphi(n)\log N\mathfrak{d}\\ &= \sum_{\sigma\in S}\sum_{m|n}\mu\Big(\frac{n}{m}\Big)\Big(m\log\max\{|\alpha^\sigma|,|\beta^\sigma|\} + O\Big(d + w\Big(\frac{\alpha}{\beta}\Big)\Big)\log m\Big)\\ &\qquad - \varphi(n)\log N\mathfrak{d}\\ &= \varphi(n)w\Big(\frac{\alpha}{\beta}\Big) + O\Big(d + w\Big(\frac{\alpha}{\beta}\Big)\Big)2^{\nu(n)}\log n,\end{aligned} \tag{5}$$

where the constant in O depends only on d and is effectively computable. Now, by the theorem of Blanksby and Montgomery [2] if $\dfrac{\alpha}{\beta}$ is an integer

$$w\Big(\frac{\alpha}{\beta}\Big) = \log\prod_{\sigma\in S}\max\Big\{\Big|\frac{\alpha^\sigma}{\beta^\sigma}\Big|, 1\Big\} \geqslant \log\Big(1 + \frac{1}{52d\log 6d}\Big) > \frac{1}{52d\log 6d + 1}.$$

If $\dfrac{\alpha}{\beta}$ is not an integer, then $(\beta) \neq \mathfrak{d}$ and

$$w\Big(\frac{\alpha}{\beta}\Big) \geqslant \log N\beta - \log N\mathfrak{d} \geqslant \log 2.$$

Thus in both cases

$$w\Big(\frac{\alpha}{\beta}\Big) > \frac{1}{52d\log 6d + 1}. \tag{6}$$

We have also (cf. [3])

$$\frac{\varphi(n)}{2^{\nu(n)}} \geqslant \sqrt{\frac{n}{30}}. \tag{7}$$

It follows from (5), (6) and (7) that for $n > n_0(d)$

$$|N_{K/\mathbb{Q}}\Phi_n(A,B)| > n^l$$

and this by Lemma 4 implies the theorem. We note for further use that for $n > n_1(d)$

$$|N_{K/\mathbb{Q}}\Phi_n(A,B)| > n^l e^{\frac{11}{13}\varphi(n)w(\frac{A}{B})(\frac{l}{d})}. \tag{8}$$

□

Corollary 1. *If $(A,B) = \mathfrak{D}$ and $\dfrac{A}{B}$ is not a root of unity then $A^n - B^n$ has a primitive divisor for all $n > \max\big(n_0(d), \varphi(\mathfrak{d})\big)$, where d is the degree of $\dfrac{A}{B}$ and $\mathfrak{d}$ is the maximal ideal of $\mathbb{Q}\Big(\dfrac{A}{B}\Big)$ divisible by $\mathfrak{D}$.*

Proof. The ideal $\mathfrak{D}$ is principal, equal say to (Δ) in a certain field K_1. Set $A_1 = A\Delta^{-1}$, $B_1 = B\Delta^{-1}$ and apply Theorem 1. It follows that $A_1^n - B_1^n$ has a primitive divisor in K_1 for all $n > n_0(d)$. On the other hand, ideals (A_1) and (B_1) are defined already in the field

$\mathbb{Q}\left(\frac{A}{B}\right)$ as the numerator and the denominator of $\left(\frac{A}{B}\right)$ in its reduced form. Set $\mathfrak{d} = \mathfrak{d}_1\mathfrak{d}_2$ where each prime factor of $\mathfrak{d}_1$ divides A_1B_1 and $(\mathfrak{d}_2, A_1B_1) = 1$. By Euler's theorem for the field K_0, $\mathfrak{d}_2 \Big| \left(\frac{A}{B}\right)^{\varphi(\mathfrak{d}_2)} - 1$ and *a fortiori* $\mathfrak{d}_2 \mid A_1^{\varphi(\mathfrak{d}_2)} - B_1^{\varphi(\mathfrak{d}_2)} \mid A_1^{\varphi(\mathfrak{d})} - B_1^{\varphi(\mathfrak{d})}$. It follows that for $n > \varphi(\mathfrak{d})$ a primitive divisor of $A_1^n - B_1^n$ is prime to $\mathfrak{d}_2$ and since it is obviously prime to $\mathfrak{d}_1$, it is a primitive divisor of $A^n - B^n$ in K_1. The corresponding prime ideal of K is a primitive divisor of $A^n - B^n$ in K. □

Corollary 2. *Let K, M be rational integers,*

$$L > 0 > K = L - 4M, \quad (L, M) = 1, \quad \langle L, M\rangle \neq \langle 1, 1\rangle,\ \langle 2, 1\rangle,\ \langle 3, 1\rangle, \tag{9}$$

let α, β be the roots of the trinomial $z^2 - L^{1/2}z + M$ and set

$$P_n(\alpha, \beta) = \begin{cases} \dfrac{(\alpha^n - \beta^n)}{(\alpha - \beta)} & \text{if } n \text{ is odd,} \\ \dfrac{(\alpha^n - \beta^n)}{(\alpha^2 - \beta^2)} & \text{if } n \text{ is even.} \end{cases}$$

There exists an effectively computable absolute constant c_0 such that $P_n(\alpha, \beta)$ for $n > c_0$ has a primitive prime factor (i.e. a prime factor not dividing $KLP_1 \cdots P_{n-1}$).

Proof. By (9), $(\alpha, \beta) = 1$ and $\frac{\alpha}{\beta}$ is not a root of unity. Since $\frac{\alpha}{\beta}$ is of degree 2 it is enough to take $c_1 = n_0(2)$ and to observe that a primitive divisor of $P_n(\alpha, \beta)$ in $\mathbb{Q}(\alpha, \beta)$ divides a rational prime which has the asserted property. □

Corollary 2 is an improvement of Theorem 1 of [6], where the corresponding property of $P_n(\alpha, \beta)$ was proved for $n > n_0(L, M)$ (given explicitly). Since for $n > 2$, $\Phi_n(\alpha, \beta) \in \mathbb{Q}$ and $w\left(\frac{\alpha}{\beta}\right) = 2\log|\alpha|$ the inequality (8) takes the form

$$|\Phi_n(\alpha, \beta)| > n|\alpha|^{11\varphi(n)/13} \quad \text{for} \quad n > c_1$$

which replaces Lemma 2 of [6]. This allows to improve Theorems 2 and 3 of that paper.

Let $k_e(n)$ be the e-th powers-free kernel of n, $k_2(n) = k(n)$, n^* be the product of all distinct prime factors of n. We have

Theorem 2. *For L, M satisfying* (9) *set*

$$\eta = \begin{cases} 1 & \text{if } k(LM) \equiv 1 \bmod 4, \\ 2 & \text{if } k(LM) \equiv 2 \text{ or } 3 \bmod 4, \end{cases}$$

$$\eta_1 = \begin{cases} 1 & \text{if } k(KM) \equiv 1 \bmod 4, \\ 2 & \text{if } k(KM) \equiv 2 \text{ or } 3 \bmod 4, \end{cases}$$

$$\eta_2 = \begin{cases} 1 & \text{if } k(KL) \equiv 1 \bmod 4, \\ 4 & \text{if } k(KL) \equiv 2 \text{ or } 3 \bmod 4. \end{cases}$$

There exists an effectively computable constant c_2 with the following property. If $n > c_2$ and

$$n \equiv \eta k(LM) \bmod 2\eta k(LM) \quad or \quad n \equiv \eta_1 k(KM) \bmod 2\eta_1 k(KM)$$
$$or \quad n \equiv 0 \bmod \eta_2 k(KL)$$

then $P_n(\alpha, \beta)$ has two primitive prime factors; if all three congruences hold then $P_n(\alpha, \beta)$ has four primitive prime factors.

Theorem 3. *Let $e = 3$, 4 or 6 and $\exp \dfrac{2\pi i}{e}$ belong to the field $\mathbb{Q}(\sqrt{KL})$. Set*

$$\eta_3 = \begin{cases} 1 & \text{if } KL \equiv 0 \bmod 27, \\ 3 & \text{if } KL \not\equiv 0 \bmod 27; \end{cases} \qquad \eta_4 = \begin{cases} 1 & \text{if } K \equiv 0 \bmod 8, \\ 2 & \text{if } L \equiv 0 \bmod 8, \\ 4 & \text{if } KL \not\equiv 0 \bmod 8; \end{cases} \qquad \eta_6 = \eta\eta_3.$$

There exists an effectively computable constant c_3 with the following property. If $\dfrac{n}{\eta_e k_e(M)^*}$ is an integer prime to e and $n > c_3$ then $P_n(\alpha, \beta)$ has $e + (e, 2)\left[\dfrac{\eta_e + 1}{4}\right]$ primitive prime factors.

An inspection of the proofs given in [6] shows that it is enough to take

$$c_2 = \max(c_1, 5 \cdot 10^{17}), \quad c_3 = \max(c_1, 3 \cdot 10^{18}).$$

I take this opportunity to mention papers of L. Rédei [4] and H. Sachs [5] dealing with the problem considered in [3] and not quoted in that paper. They have been brought to my attention by Dr. K. Szymiczek. Both papers contain results from which Lemma 4 above could easily be deduced, but the corresponding proofs are longer than the proof of that lemma.

References

[1] A. Baker, *A sharpening of the bounds for linear forms in logarithms*. Acta Arith. 21 (1972), 117–129.

[2] P. E. Blanksby, H. L. Montgomery, *Algebraic integers near the unit circle*. Acta Arith. 18 (1971), 355–369.

[3] L. P. Postnikova, A. Schinzel, *Primitive divisors of the expression $a^n - b^n$ in algebraic number fields*. Mat. Sb. (N.S.) 75 (1968), 171–177 (Russian); English transl.: Math. USSR-Sb. 4 (1968), 153–159.

[4] L. Rédei, *Über die algebraisch-zahlentheoretische Verallgemeinerung eines elementarzahlentheoretischen Satzes von Zsigmondy*. Acta Sci. Math. Szeged 19 (1958), 98–126.

[5] H. Sachs, *Untersuchungen über das Problem der eigentlichen Teiler*. Wiss. Z. Martin-Luther-Univ. Halle-Wittenberg. Math.-Nat. Reihe 6 (1956/57), 223–259.

[6] A. Schinzel, *On primitive prime factors of Lehmer numbers* III. Acta Arith. 15 (1968), 49–70; *Corrigendum*, ibid. 16 (1969), 101; this collection: I4, 1066–1089.

Andrzej Schinzel
Selecta

Originally published in
Mathematics of Computation 61 (1993), 441–444

An extension of the theorem on primitive divisors in algebraic number fields

In memory of D. H. Lehmer

Abstract. The theorem about primitive divisors in algebraic number fields is generalized in the following manner. Let A, B be algebraic integers, $(A, B) = 1$, $AB \neq 0$, A/B not a root of unity, and ζ_k a primitive root of unity of order k. For all sufficiently large n, the number $A^n - \zeta_k B^n$ has a prime ideal factor that does not divide $A^m - \zeta_k^j B^m$ for arbitrary $m < n$ and $j < k$.

The analogue of Zsigmondy's theorem in algebraic number fields [3] asserts the following.

If A, B are algebraic integers, $(A, B) = 1$, $AB \neq 0$, and A/B of degree d is not a root of unity, there exists a constant $n_0(d)$ such that for $n > n_0(d)$, $A^n - B^n$ has a prime ideal factor that does not divide $A^m - B^m$ for $m < n$.

This theorem will be extended as follows:

Theorem. *Let K be an algebraic number field, A, B integers of K, $(A, B) = 1$, $AB \neq 0$, A/B of degree d not a root of unity, and ζ_k a primitive k-th root of unity in K. For every $\varepsilon > 0$ there exists a constant $c(d, \varepsilon)$ such that if $n > c(d, \varepsilon)(1 + \log k)^{1+\varepsilon}$, there exists a prime ideal of K that divides $A^n - \zeta_k B^n$, but does not divide $A^m - \zeta_k^j B^m$ for $m < n$ and arbitrary j.*

The above theorem implies the finiteness of the number of solutions of generalized cyclotomic equations considered by Browkin ([1], p. 236).

The proof will follow closely the proof given in [3]. Let $\mathbb{Q}(A/B) = K_0$, $A/B = \alpha/\beta$, where $\alpha, \beta \in K_0, \alpha, \beta$ are integers, and $(\alpha, \beta) = \mathfrak{d}$. Let S and S_0 be the set of all isomorphic injections of $K_0(\zeta_k)$ and K_0, respectively, in the complex field, and set

$$w(\alpha/\beta) = \log \prod_{\sigma \in S_0} \max\{|\alpha^\sigma|, |\beta^\sigma|\} - \log N\mathfrak{d},$$

where N denotes the absolute norm in K_0. Here, $w(\alpha/\beta)$ is the logarithm of the Mahler measure of α/β and so it is independent of the choice of α, β in K_0.

Lemma 1. *If $|\alpha| = |\beta|$, but α/β is not a root of unity, then*

$$\log|\alpha^n - \zeta_k \beta^n| = n \log|\beta| + O(d + w(\alpha/\beta)) \log kn,$$

where the constant in the O-symbol depends only on d and is effectively computable.

Lemma 2. *If $|\alpha| \neq |\beta|$, then*

$$\log|\alpha^n - \zeta_k\beta^n| = n\log\max\{|\alpha|, |\beta|\} + O(d^2 + dw(\alpha/\beta)),$$

where the constant in the O-symbol is absolute and effectively computable.

The next lemma is just quoted from [3], where it occurs as Lemma 4.

Lemma 3. *Let $\phi_n(x, y)$ be the n-th cyclotomic polynomial in homogeneous form. If $\mathfrak{P}$ is a prime ideal of K, $n > 2(2^d - 1)$, $\mathfrak{P} \mid \phi_n(A, B)$, and $\mathfrak{P}$ is not a primitive divisor of $A^n - B^n$, then* $\operatorname{ord}_{\mathfrak{P}} \phi_n(A, B) \leqslant \operatorname{ord}_{\mathfrak{P}} n$.

Finally, we prove

Lemma 4. *Let*

$$\psi_n(x, y; \zeta_k) = \prod_{\substack{(j,n)=1 \\ j\equiv 1 \bmod k}} (x - \zeta_{kn}^j y).$$

We have

$$\psi_n(x, y; \zeta_k) = \prod_{\substack{m\mid n \\ (m,k)=1}} (x^{n/m} - \zeta_k^{\overline{m}} y^{n/m})^{\mu(m)}, \tag{1}$$

where $m\overline{m} \equiv 1 \bmod k$ and $\deg\psi_n = \varphi(n)\dfrac{(k, n)}{\varphi((k, n))}$.

Proof. The right hand side of (1) can be written as

$$\prod_{\substack{m\mid n \\ (m,k)=1}} \prod_{i=0}^{n/m-1} (x - \zeta_{n/m}^i \zeta_{kn/m}^{\overline{m}} y)^{\mu(m)}.$$

A factor $x - \zeta_{kn}^j y$ occurs in this product with the exponent

$$E = \sum_{\substack{m\mid n \\ (m,k)=1}} \mu(m) \sum_{\substack{i=0 \\ m(ki+\overline{m})\equiv j \bmod kn}}^{n/m-1} 1.$$

Now,

$$\sum_{\substack{i=0 \\ m(ki+\overline{m})\equiv j \bmod kn}}^{n/m-1} 1 = \begin{cases} \displaystyle\sum_{\substack{i=0 \\ ki+\overline{m}\equiv j/m \bmod kn/m}}^{n/m-1} 1 & \text{if } m \mid j, \\ 0 & \text{otherwise,} \end{cases}$$

and if $m \mid j$,

$$\sum_{\substack{i=0 \\ ki+\overline{m}\equiv j/m \bmod kn/m}}^{n/m-1} 1 = \begin{cases} 1 & \text{if } j \equiv 1 \bmod k, \\ 0 & \text{otherwise.} \end{cases}$$

Hence,

$$E = \begin{cases} \sum_{m\mid n,\, m\mid j} \mu(m) & \text{if } j \equiv 1 \bmod k, \\ 0 & \text{otherwise,} \end{cases}$$

and finally

$$E = \begin{cases} 1 & \text{if } (n, j) = 1,\ j \equiv 1 \bmod k, \\ 0 & \text{otherwise,} \end{cases}$$

which proves the first part of the lemma.

In order to prove the second part, we notice that there are exactly $\varphi(n)\dfrac{(k,n)}{\varphi((k,n))}$ positive integers $j \leqslant kn$ such that $(n, j) = 1$, $j \equiv 1 \bmod k$. □

Lemma 5. *For every $\varepsilon > 0$ there exists $c(d, \varepsilon)$ such that, if*

$$n > c(d, \varepsilon)(1 + \log k)^{1+\varepsilon},$$

then we have

$$\left|N_{K/\mathbb{Q}}\psi_n(A, B; \zeta_k)\right| > (nk)^{[K:\mathbb{Q}]}. \tag{2}$$

Proof. By Lemma 4,

$$\psi_n(A, B; \zeta_k) = \left(\frac{B}{\beta}\right)^{\varphi(n)(k,n)/\varphi((k,n))} \psi(\alpha, \beta; \zeta_k),$$

and since $(B/\beta) = \mathfrak{d}^{-1}$, we have

$$\left(\psi_n(A, B; \zeta_k)\right) = \mathfrak{d}^{-\varphi(n)(k,n)/\varphi((k,n))}\psi_n(\alpha, \beta; \zeta_k),$$

$$\begin{aligned}
&\frac{1}{[K : K_0(\zeta_k)]} \log |N_{K/\mathbb{Q}}\psi_n(A, B; \zeta_k)| \\
&\quad = \log |N_{K_0(\zeta_k)/\mathbb{Q}}\psi_n(\alpha, \beta; \zeta_k)| - [K_0(\zeta_k) : K_0]\varphi(n)\frac{(k,n)}{\varphi((k,n))} \log N\mathfrak{d} \\
&\quad = \sum_{\sigma\in S} \sum_{\substack{m\mid n \\ (m,k)=1}} \mu(m) \log\left|(\alpha^\sigma)^{n/m} - \zeta_k^{\overline{m}}(\beta^\sigma)^{n/m}\right| \\
&\qquad - [K_0(\zeta_k) : K_0]\varphi(n)\frac{(k,n)}{\varphi((k,n))} \log N\mathfrak{d} \\
&\quad = \sum_{\sigma\in S} \sum_{\substack{m\mid n \\ (m,k)=1}} \mu(m)\left(\frac{n}{m} \log \max\{|\alpha^\sigma|, |\beta^\sigma|\} + O\left(d + w\left(\frac{\alpha}{\beta}\right)\right) \log kn\right) \\
&\qquad - [K_0(\zeta_k) : K_0]\varphi(n)\frac{(k,n)}{\varphi((k,n))} \log N\mathfrak{d} \\
&\quad = [K_0(\zeta_k) : K_0]\left(\varphi(n)\frac{(k,n)}{\varphi((k,n))}\, w\left(\frac{\alpha}{\beta}\right) + O\left(d + w\left(\frac{\alpha}{\beta}\right)\right)2^{\nu(n)} \log kn\right),
\end{aligned}$$

where the constant in O depends only on d and is effectively computable. Now, by Dobrowolski's theorem [2], if α/β is an integer, then

$$w\Big(\frac{\alpha}{\beta}\Big) = \log \prod_{\sigma\in S_0} \max\Big\{\Big|\frac{\alpha^\sigma}{\beta^\sigma}\Big|, 1\Big\} \geqslant \log\Big(1 + c_1\Big(\frac{\log\log ed}{\log d}\Big)^3\Big) \geqslant c_2\Big(\frac{\log\log ed}{\log d}\Big)^3,$$

where c_1 and c_2 are absolute constants.

If α/β is not an integer, then $(\beta) \neq \mathfrak{d}$ and

$$w\Big(\frac{\alpha}{\beta}\Big) \geqslant \log N\beta - \log N\mathfrak{d} \geqslant \log 2.$$

Thus, in both cases,

$$w\Big(\frac{\alpha}{\beta}\Big) \geqslant c_2\Big(\frac{\log\log ed}{\log d}\Big)^3,$$

provided $c_2 \leqslant \log 2$.

Since for every $\varepsilon > 0$

$$\frac{\varphi(n)}{2^{\nu(n)}} > c_3(\varepsilon) n^{1-\varepsilon},$$

it follows that for $n > c(d,\varepsilon)(1+\log k)^{1+\varepsilon}$

$$\log\big|N_{K/\mathbb{Q}}\psi_n(A, B; \zeta_k)\big| > [K:\mathbb{Q}]\log nk,$$

which proves the lemma. □

c *Proof of the Theorem.* By Lemma 5, for $n > c(d,\varepsilon)(1+\log k)^{1+\varepsilon}$ we have (2), and thus $\psi_n(A, B; \zeta_k)$ has a prime ideal factor $\mathfrak{P}$ in K such that

$$\operatorname{ord}_{\mathfrak{P}} \psi_n(A, B; \zeta_k) > \operatorname{ord}_{\mathfrak{P}} kn.$$

But $\mathfrak{P} \mid \psi_n(A, B; \zeta_k) \mid \phi_{kn}(A, B)$, hence by Lemma 3 we have that $\mathfrak{P}$ is a primitive prime divisor of $A^{kn} - B^{kn}$ and thus does not divide $A^m - \zeta_k^j B^m$ for $m < n$ and arbitrary j. On the other hand,

$$\mathfrak{P} \mid \psi_n(A, B; \zeta_k) \mid A^n - \zeta_k B^n,$$

thus $\mathfrak{P}$ has the desired property. □

References

[1] J. Browkin, *K-theory, cyclotomic equations, and Clausen's function*. In: Structural Properties of Polylogarithms, Math. Surveys Monogr. 37, Amer. Math. Soc., Providence 1991, Chapter 11, 233–273.

[2] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*. Acta Arith. 34 (1979), 391–401.

[3] A. Schinzel, *Primitive divisors of the expression $A^n - B^n$ in algebraic number fields*. J. Reine Angew. Math. 268/269 (1974), 27–33; this collection: I5, 1090–1097.

Part J

Prime numbers

Commentary on J: Prime numbers

by Jerzy Kaczorowski

Papers **J1**, **J2**, **J3** and **J5** concern one of the most challenging open problems in the prime number theory. Hypothesis H is the common generalization of a conjecture of Dickson dated 1904 (the case of linear polynomials) and a conjecture of Buniakowski dated 1857 (the case of a single polynomial). Hypothesis H is sometimes formulated as a conjecture about prime values taken by polynomials in many variables (compare [43], Chapter 6). Lemma 4 in **J5** shows that polynomials in one variable already represent the general case.

The only instance where Hypothesis H is proved is still the classical Dirichlet theorem on primes in arithmetic progressions, which corresponds to the case of a single linear polynomial. Close approximations to it can be achieved by sieve methods. As early as 1937, G. Ricci [65] proved that if polynomials $f_1(x), \ldots, f_s(x)$ satisfy conditions of the Hypothesis H, there exists a positive integer k such that all numbers $f_1(m), \ldots, f_s(m)$ are P_k-almost primes (i.e. products of at most k primes) for infinitely many positive integers m. Value of k depends on degrees of the polynomials involved and can be made explicit. For instance H.-E. Richert [66] proved that an irreducible polynomial of degree $d \geqslant 1$ with integer coefficients, positive leading term and without fixed divisor attains infinitely many values which are P_{d+1}-almost primes (see also A. A. Bukhshtab [5]). The reader is referred to the classical treatise by H. Halberstam and H.-E. Richert [32] for a variety of similar results. For special polynomials dependence on d can be improved. For instance H. Iwaniec [44] proved that there are infinitely many positive integers m such that m^2+1 is a P_2-almost prime.

Adopting terminology from G. H. Hardy and J. E. Littlewood [33], conjecture formulated in **J3** is conjugated to Hypothesis H. There is no single instance where it is verified unconditionally except the "trivial" case $k = 0$, $\deg(g) = 1$, when it reduces to the Dirichlet prime number theorem. The closest approximations concern binary Goldbach problem. H. L. Montgomery and R. C. Vaughan [55] proved that the number of even integers not exceeding x which are not sums of two primes is $O(x^\theta)$ for certain $\theta < 1$ ($\theta = 0.914$ is admissible (see [50]), J. Pintz [62] announced $\theta = 2/3$). Generalized Riemann Hypothesis implies $\theta = 1/2 + \varepsilon$ for every $\varepsilon > 0$ as shown by G. Hardy and J. E. Littlewood [34]. The reader is referred to [62] for a very detailed survey on research done in connection with the Goldbach problem.

Another result which should be mentioned here as a close approximation to a special case of the Hypothesis H, is the famous theorem of J. R. Chen [6] saying that every

sufficiently large even integer is a sum of a prime and a product of at most two primes (i.e. a P_2-number).

Sierpiński's conjecture that for every $k > 1$ there exists a positive integer m for which the equation $\varphi(x) = m$ has exactly k solutions was proved for even k by K. Ford and S. Konyagin [19] and by K. Ford [18] in the full generality. (Theorem C_{14} from **J2** shows that Sierpiński's conjecture follows from Hypothesis H.)

A trivial consequence of Hypothesis H is that there are arbitrary long arithmetic progressions formed by primes. This was proved unconditionally by B. Green and T. Tao [30].

Hypothesis H implies that for every positive integer k, there exist infinitely many pairs of primes (p, p'), such that $p' = p + 2k$. In particular, denoting by p_n the n-th prime, we have

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log n} = 0.$$

This was proved recently by D. A. Goldston, J. Pintz and C. Y. Yıldırım [26]. The method of the proof seems to give more. It is observed in [27] that a suitably extended version of the Bombieri–Vinogradov prime number theorem would imply that the difference $p_{n+1} - p_n$ is bounded for infinitely many n's.

Artin's conjecture on primitive roots, another consequence of Hypothesis H, is still unproved at present (2005). Nevertheless, C. Hooley [41] proved that it follows from the Extended Riemann hypothesis (for the Dedekind zeta functions). For a weaker sufficient condition see [25]. Riemann Hypothesis for function fields is true, as proved by A. Weil [74], consequently the function field analog of the Artin conjecture is true as well. Using an idea of Gupta and Ram Murty [31], D. R. Heath-Brown [36] proved that for nonzero integers q, r and s which are multiplicatively independent and such that none of q, r, s, $-3qr$, $-3qs$, $-3rs$, qrs is a square, the Artin conjecture holds for at least one of them. See also [56]. For Artin's conjecture in algebraic number fields see W. Narkiewicz [58].

It is proved in **J1** that Hypothesis H implies that every positive rational number can be written in the form

$$\frac{p+1}{q+1}, \tag{1}$$

where p and q are primes (Theorem $C_{2.1}$). C. Badea [1] proved that for every positive rational r there exists a number $K = K(r)$ such that

$$r = \frac{a+1}{b+1},$$

for infinitely many a and b that are P_K-almost primes. Moreover, every sufficiently large integer n can be written in the form (1) with q prime and p a P_3-number, $p \leqslant n^{357/200}$. It is also known that the set of positive integers of the form (1) with p and q prime has a positive upper density, see P. D. T. A. Elliott [15], [14].

P. T. Bateman and R. A. Horn's heuristic arguments for the asymptotic formula in Hypothesis H are based on probabilistic arguments ([4]). Expected main term of the asymptotic formula agrees with what follows from the circle method disregarding estimates of the minor arcs, see the great classic by G. H. Hardy and J. E. Littlewood *Partitio Numerorum, III* [33]. Upper estimates of the proper size can be obtained by sieve methods,

see mentioned above book by H. Halberstam and H.-E. Richert. Sieve techniques provide lower estimates of the proper size for almost prime values of polynomials. Limitations to the equi-distribution of prime values of polynomials was discovered by J. Friedlander and A. Granville [21] by applying a method of H. Maier [52].

Suppose Hypothesis H is true for a polynomial f of degree $d > 1$. Then the sequence of the prime values of f is sparse in the sense that the number of $f(n) \leqslant x$, $f(n)$ prime, is $\ll x^\theta$ with $\theta < 1$ ($\theta = 1/d$ works). Primes of the form $x^4 + y^2$ provide an example of a sparse sequence of primes with $\theta = 3/4$, as proved by H. Iwaniec and J. Friedlander [22] and [23]. Similarly, primes of the form $x^3 + 2y^3$ provide an example of a sparse set of primes with $\theta = 2/3$, see D. R. Heath-Brown [37]. For an arbitrary binary cubic forms see D. R. Heath-Brown, B. Z. Moroz [38].

One can also judge how far existing methods are apart from what is needed for a proof of the Hypothesis H by considering Pyatetski-Shapiro prime number theorem. Let $\pi_c(x)$ denote the number of primes $p \leqslant x$ which are of the form $[n^c]$. Pyatetski-Shapiro [64] proved that

$$\pi_c(x) \sim \frac{x^{1/c}}{\log x}$$

as $x \to \infty$ for $1 \leqslant c < 12/11$. Observe that this provides a sparse sequence of primes with exponent $\theta = 1/c$, so one would expect that a method capable for treating the simplest non-linear case of the Hypothesis H, that means the case of the polynomial x^2+1, should give the range $1 \leqslant c \leqslant 2$ in Pyatetski-Shapiro's prime number theorem. Initial result from [64] was subject of a sequence of improvements by G. A. Kolesnik [46], [47], D. R. Heath-Brown [35] and H. Liu and J. Rivat [51], who was able to get $1 \leqslant c < 15/13$. See also [11], [10], [49] and [67].

About the G. H. Hardy and J. E. Littlewood conjecture implicitly formulated in [33] (compare $C_{12.2}$ in **J1**) that $\pi(x + y) \leqslant \pi(x) + \pi(y)$ for $x, y \geqslant 2$: P. Dusart [13] proved that it holds for $2 \leqslant x \leqslant y \leqslant \frac{7}{5} x \log x \log_2 x$. In general, Hardy–Littlewood's conjecture is not compatible with a special form of the Hypothesis H (k-tuples conjecture): inequality $\pi(x + y) \leqslant a\pi(x/a) + \pi(y)$ is not valid for $1 \leqslant a \leqslant 2$, see [39] and [7]. For other results see [72], [73], [28], [60], [61], [24] and [54].

The classical theorem of G. Rabinowitsch links prime values of the polynomial $x^2 + x + A$ and divisibility theory in the quadratic number field $\mathbb{Q}(\sqrt{1 - 4A})$. For prime values of quadratic polynomials see [29].

Let $q(n)$ denote the greatest prime divisor of an integer n. The problem of estimating $q(f(x))$ goes back to C. L. Siegel [69], who proved that $q(f(x)) \to \infty$ as $x \to \infty$ for every irreducible $f \in \mathbb{Z}[x]$ of degree $d > 1$. In Section 5 of **J4** the problem of estimating $q(f(x))$, where $f \in \mathbb{Z}[x]$ is a fixed quadratic or cubic polynomial is addressed. As a consequence of results on solvability of certain Diophantine equations, it is proved that if $\deg(f) = 2$ and f is not a square of a linear polynomial or $\deg(f) = 3$ and f is a binomial, then

$$\liminf_{x \to \infty} \frac{q(f(x))}{\log \log x} \geqslant c(f), \tag{2}$$

where $c(f) > 0$ is an effective constant which depends on f (see also [45]). The same holds for arbitrary irreducible polynomial $f \in \mathbb{Z}[x]$ of degree $d > 2$ as shown by S. V. Kotov [48].

Theorems 13, 14, 15 from Section 5 of **J4** concern Ω-estimates for $1/q(f(x))$. It is proved for instance (Theorem 15) that for any polynomial $f \in \mathbb{Z}[x]$ of degree > 1 one has

$$\liminf_{x\to\infty} \frac{\log q(f(x))}{\log |f(x)|} \leqslant c_1(f),$$

with an explicit constant $c_1(f)$. In cases when f is a binomial, the estimate can be improved (Theorems 13 and 14 in **J4**). For smooth values of polynomials with integer coefficients see N. M. Timofeev [71], A. Hildebrand [40], A. Balog, I. Ruzsa [2], C. Dartyge [8], G. Martin [53] and C. Dartyge, G. Martin, G. Tenenbaum [9]. Distribution of smooth shifted primes is considered in É. Fouvry, G. Tenenbaum [20], C. Pomerance, I. E. Shparlinski [63] and W. D. Bauka, A. Harcharras and I. E. Shparlinski [3].

There is a great difference between estimates for $q(f(x))$ holding for all sufficiently large x and Ω-estimates for this quantity, the latter are much sharper. For example, as a consequence of Richert's theorem [66] for every irreducible polynomial $f \in \mathbb{Z}[x]$ of degree $d \geqslant 1$ with positive leading term and no fixed prime divisors, we have $q(f(x)) = \Omega(x^{d/(d+1)})$. If $d = 2$ the exponent can be improved from $2/3$ to 1, as easily follows from Iwaniec theorem from [44]. Hypothesis H gives exponent d for every f satisfying our conditions.

Theorems of type (2) are probably very hard to improve. The famous abc-conjecture by J. Oesterlé and D. Masser (see [59]) predicts that for every $\varepsilon > 0$ there is a constant $c(\varepsilon) > 0$ such that for every non-zero relatively prime integers a, b, c satisfying $a + b = c$ one has

$$\max(|a|, |b|, |c|) \leqslant c(\varepsilon)\Big(\prod_{p|abc} p\Big)^{1+\varepsilon}.$$

Let $f(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_0$, $a_d > 0$, be a polynomial from $\mathbb{Z}[x]$ of degree $d \geqslant 2$ which is not of the form

$$a\Big(x - \frac{b}{da}\Big)^d$$

for certain $a, b \in \mathbb{Z}$, $a > 0$. We have

$$d^d a_d^{d-1} f(x) = (da_d x + a_{d-1})^d + h(x), \tag{3}$$

where $h \in \mathbb{Z}[x]$ is a non-zero polynomial of degree $\leqslant d - 2$. Taking sufficiently large integer x, writing

$$D(x) = \text{g.c.d.}\big(d^d a_d^{d-1} f(x), (da_d x + a_{d-1})^d, |h(x)|\big)$$

and applying *abc*-conjecture we obtain from (3)

$$\frac{x^d}{D(x)} \ll \max\Big(\frac{f(x)}{D(x)}, \frac{(da_d x + a_{d-1})^d}{D(x)}, \frac{|h(x)|}{D(x)}\Big)$$
$$\ll \exp\big((1+\varepsilon)\vartheta\big(q(f(x))\big)\big)\Big(\prod_{p\,\big|\,\frac{(da_d x+a_{d-1})h(x)}{D^2(x)}} p\Big)^{1+\varepsilon},$$

where

$$\vartheta(\xi) = \sum_{p\leqslant\xi} \log p$$

is the familiar theta function from the theory of prime numbers. By the Prime Number Theorem we have $\vartheta(\xi) \sim \xi$ as $\xi \to \infty$. Therefore the last expression is

$$\ll e^{(1+\varepsilon)q(f(x))}\left(\frac{x^{d-1}}{D^2(x)}\right)^{1+\varepsilon}$$

and consequently

$$\liminf_{x\to\infty} \frac{q(f(x))}{\log x} \geqslant 1.$$

Hence, even making so strong assumption as the *abc*-conjecture, one reduces just one log in (2).

Sharper estimates can be obtained for the greatest prime divisor of the product

$$\prod_{n\leqslant x} f(n).$$

Let us denote this quantity by $P(x, f)$. It was first considered in case of $f_0(x) = x^2 + 1$ by P. Chebyshev, who proved that $P(x, f_0)/x \to \infty$ as $x \to \infty$. This was improved and generalized by many authors, compare [57], [16], [42], [12], [17], [70]. The sharpest result for general polynomial was achieved by G. Tenenbaum [70]:

$$P(x, f) > x \exp\big((\log x)^\alpha\big)$$

for every $\alpha < 2 - \log 4 = 0.61370\ldots$. For $f(x) = f_0(x) = x^2 + 1$ the best result belongs to J. -M. Deshouillers and H. Iwaniec:

$$P(x, f_0) > x^{1.202}.$$

See also [68] and [42].

References

[1] C. Badea, *Note on a conjecture of P. D. T. A. Elliott*. Arch. Math. (Brno) 23 (1987), 89–94.

[2] A. Balog, I. Z. Ruzsa, *On an additive property of stable sets*. In: Sieve Methods, Exponential Sums, and their Applications in Number Theory (Cardiff, 1995), London Math. Soc. Lecture Note Ser. 237, Cambridge Univ. Press, Cambridge 1997, 55–63.

[3] W. D. Banks, A. Harcharras, I. E. Shparlinski, *Smooth values of shifted primes in arithmetic progressions*. Michigan Math. J. 52 (2004), 603–618.

[4] P. T. Bateman, R. A. Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers*. Math. Comp. 16 (1962), 363–367.

[5] A. A. Bukhshtab, *Combinatorial strengthening of the sieve of Eratosthenes method*. Uspekhi Mat. Nauk 22 (1967), no. 3 (135), 199–226 (Russian); English transl.: Russian Math. Surveys 22 (1967), 205–233.

[6] J. R. Chen, *On the representation of a larger even integer as the sum of a prime and the product of at most two primes*. Sci. Sinica 16 (1973), 157–176.

[7] D. A. Clark, N. C. Jarvis, *Dense admissible sequences*. Math. Comp. 70 (2001), 1713–1718.

[8] C. Dartyge, *Entiers de la forme* $n^2 + 1$ *sans grand facteur premier*. Acta Math. Hungar. 72 (1996), 1–34.

[9] C. Dartyge, G. Martin, G. Tenenbaum, *Polynomial values free of large prime factors*. Period. Math. Hungar. 43 (2001), 111–119.

[10] J.-M. Deshouillers, *Répartition de nombre premiers de la forme* $[n^c]$. In: Journées Arithmétiques (Grenoble 1973), Bull. Soc. Math. France Mém. 37, Paris, 1974, 49–52.

[11] —, *Nombres premiers de la forme* $[n^c]$. C. R. Acad. Sci. Paris Sér. A-B 282 (1976), A131–A133.

[12] J.-M. Deshouillers, H. Iwaniec, *On the greatest prime factor of* $n^2 + 1$. Ann. Inst. Fourier (Grenoble) 32:4 (1982), 1–11.

[13] P. Dusart, *Sur la conjecture* $\pi(x + y) \leqslant \pi(x) + \pi(y)$. Acta Arith. 102 (2002), 295–308.

[14] P. D. T. A. Elliott, *A conjecture of Kátai*. Acta Arith. 26 (1974/5), 11–20.

[15] —, *Arithmetic Functions and Integer Products*. Springer, New York 1985.

[16] P. Erdős, *On the greatest prime factor of* $\prod_{k=1}^{x} f(k)$. J. London Math. Soc. 27 (1952), 379–384.

[17] P. Erdős, A. Schinzel, *On the greatest prime factor of* $\prod_{k=1}^{x} f(k)$. Acta Arith. 55 (1990), 191–200.

[18] K. Ford, *The number of solutions of* $\phi(x) = m$. Ann. of Math. (2) 150 (1999), 283–311.

[19] K. Ford, S. Konyagin, *On two conjectures of Sierpiński concerning the arithmetic functions* σ *and* ϕ. In: Number Theory in Progress, Vol. 2 (Zakopane–Kościelisko, 1997), de Gruyter, Berlin 1999, 795–803.

[20] É. Fouvry, G. Tenenbaum, *Entiers sans grand facteur premier en progressions arithmetiques*. Proc. London Math. Soc. (3) 63 (1991), 449–494.

[21] J. Friedlander, A. Granville, *Limitations to the equi-distribution of primes* IV. Proc. Roy. Soc. London Ser. A 435 (1991), no. 1893, 197–204.

[22] J. Friedlander, H. Iwaniec, *The polynomial* $X^2 + Y^4$ *captures its primes*. Ann. of Math. (2) 148 (1998), 945–1040.

[23] —, —, *Asymptotic sieve for primes*. Ann. of Math. (2) 148 (1998), 1041–1065.

[24] R. Garunkštis, *On some inequalities concerning* $\pi(x)$. Experiment. Math. 11 (2002), 297–301.

[25] L. J. Goldstein, *On the generalized density hypothesis* I. In: Analytic Number Theory (Philadelphia, 1980), Lecture Notes in Math. 899, Springer, Berlin 1981, 107–128.

[26] D. A. Goldston, J. Pintz, C. Y. Yıldırım, *Small gaps between primes* II. Preprint 2005.

[27] D. A. Goldston, Y. Motohashi, J. Pintz, C. Y. Yıldırım, *Small gaps between primes exist*. Proc. Japan Acad. Ser. A Math. Sci. 82 (2006), 61–65.

[28] D. M. Gordon, G. Rodemich, *Dense admissible sets*. In: Algorithmic Number Theory (Portland, 1998), Lecture Notes in Comput. Sci. 1423, Springer, Berlin 1998, 216–225.

[29] A. Granville, R. A. Mollin, *Rabinowitsch revisited*. Acta Arith. 96 (2000), 139–153.

[30] B. Green, T. Tao, *The primes contain arbitrarily long arithmetic progressions*. Ann. of Math. (2), to appear.

[31] R. Gupta, M. Ram Murty, *A remark on Artin's conjecture*. Invent. Math. 78 (1984), 127–130.

[32] H. Halberstam, H.-E. Richert, *Sieve Methods*. Academic Press, London–New York 1974.

[33] G. H. Hardy, J. E. Littlewood, *Some problems of 'Partitio numerorum'* III. *On the expression of a number as a sum of primes*. Acta Math. 44 (1923), 1–70.

[34] —, —, *Some problems in 'Partitio numerorum'* V. *A further contribution to the study of Goldbach's problem*. Proc. London Math. Soc. (2) 22 (1924), 46–56.

[35] D. R. Heath-Brown, *The Pjateckiĭ–Šapiro prime number theorem*. J. Number Theory 16 (1983), 242–266.

[36] —, *Artin's conjecture for primitive roots*. Quart. J. Math. Oxford Ser. (2) 37 (1986), 27–38.

[37] —, *Primes represented by* $x^3 + 2y^3$. Acta Math. 186 (2001), 1–84.

[38] D. R. Heath-Brown, B. Z. Moroz, *Primes represented by binary cubic forms*. Proc. London Math. Soc. (3) 84 (2002), 257–288.

[39] D. Hensley, I. Richards, *Primes in intervals*. Acta Arith. 25 (1973/74), 375–391.

[40] A. Hildebrand, *On integer sets containing strings of consecutive integers*. Mathematika 36 (1989), 60–70.

[41] C. Hooley, *On Artin's conjecture*. J. Reine Angew. Math. 225 (1967), 209–220.

[42] —, *On the greatest prime factor of a quadratic polynomial*. Acta Math. 117 (1967), 281–299.

[43] M. N. Huxley, *The Distribution of Prime Numbers. Large Sieves and Zero-density Theorems*. Clarendon Press, Oxford 1972.

[44] H. Iwaniec, *Almost primes represented by quadratic polynomials*. Invent. Math. 47 (1978), 171–188.

[45] M. Keates, *On the greatest prime factor of a polynomial*. Proc. Edinburgh Math. Soc. (2) 16 (1969), 301–303.

[46] G. A. Kolesnik, *The distribution of primes in sequences of the form* $[n^c]$. Mat. Zametki 2 (1967), 117–128 (Russian).

[47] —, *Primes of the form* $[n^c]$. Pacific J. Math. 118 (1985), 437–447.

[48] S. V. Kotov, *The greatest prime factor of a polynomial*. Mat. Zametki 13 (1973), 515–522 (Russian); English transl.: Math. Notes 13 (1973), 313–317.

[49] D. Leitmann, D. Wolke, *Primzahlen der Gestalt* $[f(n)]$. Math. Z. 145 (1975), 81–92.

[50] H. Z. Li, *The exceptional set of Goldbach numbers* II. Acta Arith. 92 (2000), 71–88.

[51] H. Q. Liu, J. Rivat, *On the Pjateckiĭ-Šapiro prime number theorem*. Bull. London Math. Soc. 24 (1992), 143–147.

[52] H. Maier, *Primes in short intervals*. Michigan Math. J. 32 (1985), 221–225.

[53] G. Martin, *An asymptotic formula for the number of smooth values of a polynomial*. J. Number Theory 93 (2002), 108–182.

[54] G. Mincu, *A few inequalities involving* $\pi(x)$. An. Univ. Bucureşti Mat. 52 (2003), 55–64.

[55] H. L. Montgomery, R. C. Vaughan, *The exceptional set in Goldbach's problem*. Acta Arith. 27 (1975), 353–370.

[56] M. Ram Murty, *Artin's conjecture and elliptic analogues*. In: Sieve Methods, Exponential Sums, and their Applications in Number Theory (Cardiff, 1995), London Math. Soc. Lecture Note Ser. 237, Cambridge Univ. Press, Cambridge 1997, 325–344.

[57] T. Nagell, *Généralisation d'un théorème de Tchébycheff*. J. Math. Pure Appl. (8) 4 (1921), 343–356.

[58] W. Narkiewicz, *A note on Artin's conjecture in algebraic number fields*. J. Reine Angew. Math. 381 (1987), 110–115.

[59] J. Oesterlé, *Nouvelles approches du "théorème" de Fermat*. Séminaire Bourbaki, Vol. 1987/88. Astérisque 161–162 (1988), Exp. 694, 165–186.

[60] L. Panaitopol, *Inequalities concerning the function $\pi(x)$: applications*. Acta Arith. 94 (2000), 373–381.

[61] —, *Checking the Hardy–Littlewood conjecture in special cases.* Rev. Roumaine Math. Pures Appl. 46 (2001), 465–470.

[62] J. Pintz, *Recent results on the Goldbach conjecture*. Preprint 2005.

[63] C. Pomerance, I. E. Shparlinski, *Smooth orders and cryptographic applications*. In: Algorithmic Number Theory (Sydney, 2002), Lecture Notes in Comput. Sci. 2369, Springer, Berlin 2002, 338–348.

[64] I. I. Pyatetskii-Shapiro, *On the distribution of prime numbers of the form $[f(n)]$*. Mat. Sbornik (N.S.) 33 (75) (1953), 559–566 (Russian).

[65] G. Ricci, *Su la congettura di Goldbach e la costante di Schnirelmann*. Ann. Scuola Norm. Sup. Pisa (2) 6 (1937), 71–116.

[66] H.-E. Richert, *Selberg's sieve with weights*. Mathematika 16 (1969), 1–22.

[67] G. J. Rieger, *Über ein additives Problem mit Primzahlen*. Arch. Math. (Basel) 21 (1970), 54–58.

[68] T. N. Shorey, R. Tijdeman, *On the greatest prime factor of polynomials at integer points*. Compositio Math. 33 (1976), 187–195.

[69] C. L. Siegel, *The integer solutions of equation $y^2 = ax^n + bx^{n-1} + \ldots + k$*. J. London Math. Soc. 1 (1926), 66–68.

[70] G. Tenenbaum, *Sur une question d'Erdős et Schinzel* II. Inventiones Math. 99 (1990), 215–224.

[71] N. M. Timofeev, *Polynomials with small prime divisors*. Tashkent. Gos. Univ. Nauchn. Trudy 548 Voprosy Mat. (1977), 87–91 (Russian).

[72] V. Şt. Udrescu, *Some remarks concerning the conjecture $\pi(x + y) \leqslant \pi(x) + \pi(y)$*. Rev. Roumaine Math. Pures Appl. 20 (1975), 1201–1209 (insert).

[73] T. Vehka, I. Richards, *Explicit construction of an admissible set for the conjecture that sometimes $\pi(x + y) > \pi(x) + \pi(y)$*. Notices Amer. Math. Soc. 26 (1979), A-453.

[74] A. Weil, *On the Riemann hypothesis in functionfields*. Proc. Nat. Acad. Sci. U.S.A. 27 (1941), 345–347.

Originally published in
Acta Arithmetica IV (1958), 185–208

Sur certaines hypothèses concernant les nombres premiers

with W. Sierpiński (*Warszawa*)

La répartition des nombres premiers parmi les nombres naturels n'est pas encore suffisamment étudiée : c'est pourquoi depuis les temps les plus anciens on a énoncé diverses hypothèses concernant les nombres premiers. Plusieurs de ces hypothèses se sont montrées fausses ; quelques unes d'elles ne sont pas encore mises en défaut, et il y en a qui sont vérifiées pour tous les nombres ne dépassant pas un nombre très grand.

Une de plus anciennes hypothèses sur les nombres premiers, ayant au moins 25 siècles, était celle des Chinois : un nombre naturel $n > 1$ est premier si et seulement si le nombre $2^n - 2$ est divisible par n ([1]). La nécessité de cette condition a été démontrée il y a quelques centaines d'années. En 1681 Leibniz a essayé de démontrer qu'elle est suffisante, mais sa démonstration était basée sur un raisonnement faux, et en 1819 on a trouvé que l'hypothèse des Chinois était fausse, puisque le nombre $2^{341} - 2$ (qui a 103 chiffres) est divisible par 341, bien que le nombre $341 = 11 \cdot 31$ ne soit pas premier. Ensuite on a démontré (de nos temps) qu'il existe une infinité de nombres composés n pour lesquels le nombre $2^n - 2$ est divisible par n, impairs aussi bien que pairs. (Le plus petit de ces nombres pairs est le nombre $n = 161038 = 2 \cdot 73 \cdot 1103$ trouvé en 1950 par D. H. Lehmer).

P. Fermat supposait premiers tous les nombres $F_n = 2^{2^n} + 1$, où $n = 0, 1, 2, \ldots$. Cela est vrai pour $n = 0, 1, 2, 3$ et 4, mais, comme l'a trouvé L. Euler en 1772, le nombre F_5 (qui a 10 chiffres) est composé, car il est divisible par 641. Maintenant nous connaissons 29 nombres F_n composés, pour $n = 5, 6, 7, 8, 9, 10, 11, 12, 15, 16, 18, 23, 36, 38, 39, 55, 63, 73, 117, 125, 144, 150, 207, 226, 228, 268, 284, 316, 452$.

On peut donc énoncer l'hypothèse qu'il existe une infinité de nombres F_n composés. On a même énoncé l'hypothèse plus forte : les nombres F_n premiers sont en nombre fini. Ce sont peut-être seulement ceux que connaissait Fermat, à savoir les nombres F_n pour $n \leqslant 4$.

Le plus petit nombre F_n dont nous ne sachions pas s'il est premier ou non est F_{13}. Le plus grand nombre F_n composé connu est F_{452} dont le plus petit diviseur premier est le nombre $27 \cdot 2^{455} + 1$ (voir [14]).

Erratum Acta Arith. 5 (1959), 259.

([1]) Ancient Chinese mathematicians never made this conjecture, see [12a], p. 54, footnote d.

Le fait que le nombre F_{16} est composé met en défaut l'hypothèse que tous les nombres de la suite infinie

$$2+1,\ 2^2+1,\ 2^{2^2}+1,\ 2^{2^{2^2}}+1,\ 2^{2^{2^{2^2}}}+1,\ \ldots$$

sont premiers, puisque F_{16} est le cinquième terme de cette suite.

Quant aux nombres de Mersenne $M_n = 2^n - 1$ on a énoncé l'hypothèse que si le nombre M_n est premier, le nombre M_{M_n} est aussi premier. Or, d'après un calcul qui a été fait en 1953 par D. J. Wheeler, le nombre $M_{M_{13}} = 2^{8191} - 1$ (qui a 2466 chiffres) est composé, bien que le nombre M_{13} soit premier.

On a encore énoncé l'hypothèse que les nombres q_n ($n = 0, 1, 2, \ldots$), où $q_0 = 2$ et $q_{k+1} = 2^{q_k} - 1$ pour $k = 0, 1, 2, \ldots$, sont tous premiers. Cela est vrai pour $0 \leqslant n \leqslant 4$. Or, le nombre q_5 a plus de 10^{37} chiffres et nous ne savons pas s'il est premier ou non.

En 1742 Ch. Goldbach a énoncé l'hypothèse que tout nombre pair > 4 est la somme de deux nombres premiers impairs. On peut énoncer l'hypothèse G un peu plus forte : tout nombre pair > 6 est la somme de deux nombres premiers distincts. On peut démontrer que l'hypothèse G équivaut à l'hypothèse que tout nombre naturel > 17 est la somme de trois nombres premiers distincts. Or, de l'hypothèse de Goldbach A. Schinzel a déduit que tout nombre impair > 17 est la somme de trois nombres premiers distincts. En 1937 J. Vinogradoff a démontré que tout nombre impair suffisamment grand est la somme de trois nombres premiers impairs. Quant à l'hypothèse G, S. Gołaszewski et B. Leszczyński l'ont vérifiée pour tous les nombres pairs $\leqslant 50000$.

On a aussi énoncé l'hypothèse que le nombre des décompositions d'un nombre pair $2n$ en une somme de deux nombres premiers tend vers l'infini avec n (cf. [10], Conjecture A). Il est probable que les nombres pairs > 188 ont plus de 10 décompositions et que les nombres pairs > 4574 donnent plus de 100 décompositions.

Nous déduirons de l'hypothèse G quelques conséquences.

P_1. *Tout nombre impair est de la forme $n - \varphi(n)$ où n est un nombre naturel.*

Démonstration de l'implication $G \to P_1$. On a $1 = 2-\varphi(2), 3 = 9-\varphi(9), 5 = 25 - \varphi(25)$. Si m est un nombre impair > 5 on a $m+1 > 6$ et de G résulte l'existence des nombres premiers distincts p et q tels que $m+1 = p+q$ et on a $pq - \varphi(pq) = pq - (p-1)(q-1) = p + q - 1 = m$, donc $m = n - \varphi(n)$ pour $n = pq$. L'implication $G \to P_1$ se trouve ainsi démontrée. □

P_2. *Tout nombre impair $m > 7$ est de la forme $\sigma(n) - n$, où n est un nombre impair $> m$.*

Démonstration de l'implication $G \to P_2$. Si m est un nombre impair > 7, il résulte de G qu'il existe des nombres premiers distincts p et $q < p$ tels que $m - 1 = p + q$, et on a $\sigma(pq) - pq = (p+1)(q+1) - pq = p + q + 1 = m$. Comme m est impair > 7, les nombres p et q sont impairs, $q \geqslant 3$, donc $pq \geqslant 3p = 2p + p > p + q + 1 = m$ et en posant $n = pq$ on obtient un nombre impair $n > m$ tel que $m = \sigma(n) - n$. L'implication $G \to P_2$ est ainsi démontrée. □

P. Erdős a posé la question s'il existe une infinité de nombres naturels qui ne sont pas termes de la suite $\sigma(n) - n$. (Tels sont par exemple les nombres 2 et 5). Une question

analogue peut être posée pour la suite $n - \varphi(n)$. (Les quatre nombres naturels les plus petits qui ne sont pas termes de cette suite sont 10, 26, 34 et 50).

$P_{2.1}$. *Il existe des suites aussi longues que l'on veut*

$$n,\ f(n),\ ff(n),\ fff(n),\ \ldots, \quad où \quad f(n) = \sigma(n) - n, \tag{1}$$

dont le dernier terme est 1.

Démonstration de l'implication $P_2 \to P_{2.1}$. D'après P_2 pour tout nombre impair $m > 7$ il existe un nombre impair $n = g(m) > m$, tel que $f(n) = m$. Pour tout n impair > 7 la suite infinie de nombres naturels

$$n,\ g(n),\ gg(n),\ \ldots$$

est donc croissante. k étant un nombre naturel, posons $n = g^k(11)$. Nous obtenons ainsi la suite

$$n = g^k(11),\ f(n) = g^{k-1}(11),\ \ldots,\ f^k(n) = 11,\ f^{k+1}(n) = 1$$

(puisque $f(11) = \sigma(11) - 11 = 1$) qui a $k+2$ termes dont le dernier est $= 1$. L'implication $P_2 \to P_{2.1}$ se trouve ainsi démontrée. □

$P_{2.2}$. *Il existe un infinité de nombres naturels n tels que la suite infinie* (1) *est périodique.*

Démonstration de l'implication $P_2 \to P_{2.2}$. Soit $g(m)$ la fonction définie dans la démonstration de l'implication $P_2 \to P_{2.1}$ et posons pour k naturels $n = g^k(25)$. Nous obtiendrons la suite

$$n = g^k(25),\ f(n) = g^{k-1}(25),\ \ldots,\ f^k(n) = 25,\ f^{k+i}(n) = 6$$

pour $i = 1, 2, \ldots$ (puisque $f(25) = 6$ et $f(6) = 6$).

La suite infinie (1) a donc ici k nombres impairs suivis d'une infinité de nombres 6.

Il est à remarquer que L. E. Dickson a énoncé l'hypothèse que pour tout nombre naturel $n > 1$ la suite (1) ou bien se termine par le nombre 1 ou bien elle est périodique (Dickson [5]; cf. Catalan [3]).

On voit sans peine que l'on peut exprimer cette hypothèse en disant que la suite (1) est toujours bornée.

On ne sait pas s'il existe une infinité de nombres naturels n pour lesquels la suite (1) est périodique et la période est pure (comme par exemple pour $n = 220$, où la période est formée de deux termes ou pour $n = 12496$, où la période est formée de 5 termes).

En 1950 G. Giuga a énoncé l'hypothèse que pour qu'un nombre naturel $p > 1$ soit premier, il faut et il suffit que le nombre $1^{p-1} + 2^{p-1} + \ldots + (p-1)^{p-1} + 1$ soit divisible par p. (On démontre sans peine que cette condition est nécessaire). Il affirme que cette hypothèse est vraie pour tous les nombres $< 10^{1000}$.

Hypothèse de A. Schinzel. A. Schinzel a énoncé hypothèse H_0 suivante :

H_0. *s étant un nombre naturel et $f_1(x),\ f_2(x),\ \ldots,\ f_s(x)$ des polynômes irréductibles en x à coefficients entiers, où le coefficient de la plus haute puissance de x est positif, et satisfaisant à la condition*

C. *Il n'existe aucun entier* > 1 *qui divise le produit* $f_1(x)f_2(x)\cdots f_s(x)$ *quel que soit l'entier* x,

alors il existe au moins un nombre naturel x *pour lequel les nombres* $f_1(x)$, $f_2(x)$, ..., ..., $f_s(x)$ *sont tous premiers.*

On démontre sans peine que l'hypothèse H_0 équivaut à l'hypothèse H suivante :

H. *s étant un nombre naturel et* $f_1(x)$, $f_2(x)$, ..., $f_s(x)$ *des polynômes en* x *satisfaisant aux conditions de l'hypothèse* H_0, *il existe une infinité de hboxnombres naturels* x *pour lesquels les nombres* $f_1(x)$, $f_2(x)$, ..., $f_s(x)$ *sont premiers.*

En effet, supposons que l'hypothèse H_0 soit vraie et soient $f_1(x), f_2(x), \ldots, f_s(x)$ des polynômes satisfaisant aux conditions de l'hypothèse H_0. On démontre sans peine que, quel que soit le nombre naturel k, les polynômes $f_1(x+k)$, $f_2(x+k)$, ..., $f_s(x+k)$ satisfont aussi aux conditions de l'hypothèse H_0. D'après H_0 il existe donc un nombre naturel x tel que les nombres $f_1(x+k)$, $f_2(x+k)$, ..., $f_s(x+k)$ sont tous premiers et, comme on le prouve aisément, pour k suffisamment grand tous ces nombres premiers sont aussi grands que l'on veut. On a donc $H_0 \to H$ et comme, d'autre part, on a évidemment $H \to H_0$, l'equivalence $H_0 \equiv H$ se trouve démontrée.

Quant à l'hypothèse H il est à remarquer que du théorème 1 du travail de G. Ricci [13] on déduit sans peine que si les polynômes $f_1(x), f_2(x), \ldots, f_s(x)$ satisfont aux conditions de l'hypothèse H_0, il existe une constante C dépendant de $f_1, f_2, \ldots, f_s$ telle que pour une infinité de nombres naturels x chacun des nombres $f_1(x), f_2(x), \ldots, f_s(x)$ a au plus C diviseurs premiers.

Nous déduirons maintenant de l'hypothèse H plusieurs conséquences.

C_1. *Si* s *est un nombre naturel,* $a_1 < a_2 \ldots < a_s$ *des entiers et si les binômes* $f_i(x) = x + a_i$ $(i = 1, 2, \ldots, s)$ *satisfont à la condition* C, *il existe une infinité de nombres naturels* x *pour lesquels* $f_1(x)$, $f_2(x)$, ..., $f_s(x)$ *sont des nombres premiers consécutifs.*

Démonstration de l'implication $H \to C_1$. Nos binômes étant irréductibles et satisfaisant à la condition C, il résulte de H qu'il existe une infinité de nombres naturels x pour lesquels les nombres $f_i(x)$ $(i = 1, 2, \ldots, s)$ sont premiers. Soit $h \geqslant a_s - 2a_1 + 2$ un tel nombre naturel et posons

$$b = \frac{(h + a_s)!}{(h + a_1)!\,(h + a_2)\cdots(h + a_s)} \tag{2}$$

et

$$g_i(x) = bx + h + a_i \quad \text{pour} \quad i = 1, 2, \ldots, s.$$

On a $2(h + a_i) = h + h + 2a_i \geqslant h + h + 2a_1 \geqslant h + a_s + 2 > h + a_s$ et, le nombre $h + a_i = f_i(h)$ étant premier, les facteurs de $(h + a_s)!$ autres que $h + a_i$, étant $< 2(h + a_i)$, ne sont pas divisibles par $h + a_i$ et il en résulte que $(b, h + a_i) = 1$.

Supposons maintenant qu'il existe un nombre premier p tel que

$$p \mid g_1(x)g_2(x)\cdots g_s(x) \quad \text{pour} \quad x = 0, 1, 2, \ldots, p - 1.$$

On a donc $p \mid g_1(0)g_2(0)\cdots g_s(0) = (h+a_1)(h+a_2)\cdots(h+a_s)$ et tous ces facteurs étant premiers, il existe un nombre naturel $k \leqslant s$ tel que $p = h + a_k$ et d'après (2) et $h+a_s < 2(h+a_k) = 2p$ on en conclut que p ne divise pas b. Il existe donc pour tout nombre naturel $i \leqslant s$ un seul nombre x de la suite $0, 1, 2, \ldots, p-1$, tel que $p \mid bx+h+a_i = g_i(x)$ et il résulte tout de suite de $p \mid g_1(x)g_2(x)\cdots g_s(x)$ pour $x = 0, 1, 2, \ldots, p-1$ que $p \leqslant s$, donc $h + a_k \leqslant s$, et comme, d'autre part, $h + a_k \geqslant h + a_1 \geqslant a_s - a_1 + 2 \geqslant s + 1$ (puisque les entries $a_1, a_2, \ldots, a_s$ vont en croissant) on aboutit à une contradiction.

Les binômes irréductibles $g_i(x)$ $(i = 1, 2, \ldots, s)$ satisfont donc à la condition C et, d'aprés H, il existe une infinité de nombres naturels x tels que les nombres $g_i(x)$ $(i = 1, 2, \ldots, s)$ sont premiers. Si pour un tel x ces nombres premiers n'étaient pas consécutifs, il existerait un entier j tel que $a_1 \leqslant j \leqslant a_s$ et $j \neq a_1, a_2, \ldots, a_s$ tel que le nombre $q = bx + h + j > h + j$ serait premier. Or, comme $a_1 \leqslant j \leqslant a_s$ et $j \neq a_1, a_2, \ldots, a_s$, on a, d'aprés (2), $h + j \mid b$, donc $h + j \mid q > h + j$, ce qui est impossible, puisque $h + j > h + a_1$ qui est premier.

L'implication H $\rightarrow$ C_1 se trouve ainsi démontrée. □

$C_{1.1}$. *Tout nombre pair peut être représenté d'une infinité de manières comme la différence de deux nombres premiers consécutifs.*

Démonstration de l'implication $C_1 \rightarrow C_{1.1}$. Soit $f_1(x) = x$, $f_2(x) = x + 2n$ (où n est un nombre naturel donné). Comme

$$\big(f_1(1)\,f_2(1),\, f_1(2)\,f_2(2)\big) = \big(2n+1,\, 2(2+2n)\big) = 1,$$

il résulte de C_1 qu'il existe une infinité de nombres naturels x tels que x et $x + 2n$ sont deux nombres premiers consécutifs, oit $x = p_k$, $x + 2n = p_{k+1}$ (où p_i désigne le i-ème nombre premier), d'oú $2n = p_{k+1} - p_k$. Cela prouve que $C_1 \rightarrow C_{1.1}$ (cf. Hardy and Littlewood [10], Conjecture B). □

$C_{1.2}$. *m étant un nombre naturel donné, il existe $2m$ nombres premiers consécutifs formant m couples de nombres jumeaux.*

Démonstration de l'implication $C_1 \rightarrow C_{1.2}$. Soit

$$f_{2i-1}(x) = x + (2m)!\,(i-1),$$
$$f_{2i}(x) = x + (2m)!\,(i-1) + 2 \quad \text{pour} \quad i = 1, 2, \ldots, m$$

et

$$P(x) = f_1(x)\,f_2(x)\cdots f_{2m}(x).$$

Soit p un nombre premier tel que $p \mid P(x)$ pour $x = 0, 1, \ldots, p-1$. Comme $P(x)$ est un polynôme en x de degré $2m$ où le coefficient de x^{2m} est $= 1$, d'après le théorème de Lagrange la congruence $P(x) \equiv 0 \pmod p$ a au plus $2m$ racines. Or, comme $P(x) \equiv 0 \pmod p$ pour $x = 0, 1, \ldots, p-1$, on en conclut que $p \leqslant 2m$. Mais $P(1)$ est évidemment un nombre impair et comme $p \mid P(1)$, on trouve $p > 2$. D'autre part, d'après $p \leqslant 2m$ on a $p \mid (2m)!\,i$ pour i entier et comme $p \mid P(2)$, on trouve $p \mid 2^{3m}$, ce qui est impossible. Les binômes $f_j(x)$ $(j = 1, 2, \ldots, 2m)$ satisfont donc à la condition C et il résulte de C_1

qu'il existe une infinité de nombres naturels x tels que $f_j(x)$ $(j = 1, 2, \ldots, 2m)$ sont des nombres premiers consécutifs, $f_j(x) = p_{k+j-1}$ pour $j = 1, 2, \ldots, 2m$. On a donc $p_{k+2i-1} - p_{k+2i-2} = 2$ pour $i = 1, 2, \ldots, n$ et l'implication $C_1 \to C_{1.2}$ se trouve démontrée. □

On peut démontrer pareillement qu'il existe pour tout m naturel $4m + 1$ nombres premiers consécutifs dont les $2m$ premiers et de même les $2m$ derniers donnent m couples de nombres jumeaux.

V. Thébault a démontré [18] que si $n > 1$ termes d'une progression arithmétique de raison r sont des nombres premiers $> n$, alors r est divisible par tout nombre premier $\leqslant n$. Or, nous démontrerons que C_1 entraîne la conséquence suivante :

$C_{1.4}$. *Si r est un nombre naturel divisible par tout nombre premier $\leqslant n$, où n est un nombre naturel donnée > 1, il existe une infinité de systèmes de n nombres premiers consécutifs formant une progression arithmétique de raison r.*

Démonstration de l'implication $C_1 \to C_{1.4}$. Soit $f_i(x) = x + ir$ pour $i = 0, 1, 2, \ldots, \ldots, n - 1$. S'il existait un nombre premier p tel que $p \mid f_0(x) f_1(x) \cdots f_{n-1}(x)$ pour $x = 0, 1, 2, \ldots, p - 1$, il résulterait du théorème de Lagrange que $p \leqslant n$, donc $p \mid r$. D'autre part on a

$$p \mid f_0(1) f_1(1) \cdots f_{n-1}(1) = 1(1 + r)(1 + 2r) \cdots (1 + (n - 1)r)$$

et vu que $p \mid r$ on trouve $p \mid 1$, ce qui est impossible. La condition C est donc satisfaite et il résulte de C_1 qu'il existe une infinité de nombres naturels x tels que les nombres $f_i(x)$ $(i = 1, 2, \ldots, n)$ sont des nombres premiers consécutifs. Nous avons ainsi démontré que $C_1 \to C_{1.4}$. □

En particulier, pour $n = 3$, il résulte de $C_{1.4}$ qu'il existe pour tout nombre naturel h une infinité de nombres naturels k tels que $p_{k+1} - p_k = p_{k+2} - p_{k+1} = 6h$. Il en résulte qu'il existe une infinité de progressions arithmétiques formées de trois nombres premiers consécutifs. Or, d'après L. E. Dickson ([6], p. 425) Moritz Cantor a énoncé l'hypothèse ([2]) que trois nombres premiers consécutifs dont aucun n'est le nombre 3 ne peuvent pas former de progression arithmétique. En 1955 A. Schinzel a remarqué que cette hypothèse est en défaut puisque 47, 53 et 59 sont trois nombres premiers consécutifs formant une progression arithmétique de raison 6. Parmi les nombres < 1000 on trouve plusieurs telles progressions dont les premiers termes sont respectivement 151, 167, 367, 557, 587, 601, 647, 727, 941, 971. Les nombres 199, 211 et 223 et pareillement les nombres 1499, 1511 et 1523 forment des progressions arithmétiques de raison 12 composées de nombres premiers consécutifs et les nombres

$$251,\ 257,\ 263,\ 269 \quad \text{et} \quad 1741,\ 1747,\ 1753,\ 1759$$

forment des progressions arithmétiques de raison 6 composées chacune de quatre nombres premiers consécutifs. D'après $C_{1.4}$ (pour $n = 4$) il existe une infinité de telles progressions.

Nous déduirons maintenant de l'hypothèse H la conséquence suivante :

C_2. *a, b, c étant des nombres naturels tels que $(a,b) = (a,c) = (b,c) = 1$ et $2 \mid abc$, l'équation $ap - bq = c$ a une infinité de solutions en nombres premiers p et q.* (Cette hypothèse a été énoncée par Hardy et Littlewood [10], p. 45, Conjecture D).

Démonstration de l'implication $H \to C_2$. a, b, c étant des nombres naturels tels que $(a,b) = (a,c) = (b,c) = 1$ et $2 \mid abc$, il existe, on le sait, des nombres naturels r et s tels que $ar - bs = c$. Soit $f_1(x) = bx + r$, $f_2(x) = ax + s$, on a donc $f_1(x) f_2(x) = abx^2 + (ar + bs)x + rs$.

S'il existait un nombre premier p tel que $p \mid f_1(x) f_2(x)$ pour tout entier x, on aurait (pour $x = 0$) $p \mid rs$, donc (pour $x = \pm 1$) $p \mid ab \pm (ar + bs)$, d'où $p \mid 2ab$ et $p \mid 2(ar + bs)$. Si l'on avait $p = 2$, on aurait, d'après $p \mid rs$, $2 \mid r$ ou bien $2 \mid s$. Si $2 \mid r$, on ne peut avoir $2 \mid s$, puisqu'alors il viendrait $2 \mid ar \pm bs$, donc $2 \mid ab$ et $2 \mid c$, contrairement à $(ab, c) = 1$. Donc, si $2 \mid r$, s est impair et de $p \mid ab + (ar + bs)$ il résulte que $2 \mid (a+1)b$, donc ou bien a est impair ou bien b est pair. Si b était pair, alors, d'après $ar - bs = c$, c serait pair, contrairement à $(b, c) = 1$. Donc b est impair et a impair et aussi $c = ar - bs$ impair, contrairement à $2 \mid abc$. Donc r ne peut pas être pair ; s est donc pair et comme plus haut on démontre que cela implique une contradiction.

On a donc $p \neq 2$, par conséquent $p \mid ab$ et $p \mid ar + bs$ et, comme $p \mid rs$, d'après $p \mid ar^2 + brs$ on trouve $p \mid ar^2$, d'où $p \mid ar$ et, comme en vertu de $p \mid ars + bs^2$ on a $p \mid bs^2$, d'où $p \mid bs$, il vient $p \mid ar - bs = c$, ce qui est impossible, puisque $(ab, c) = 1$. Les binômes $f_1(x)$ et $f_2(x)$ satisfont donc à la condition C et il existe une infinité de nombres naturels x tels que $p = f_1(x)$ et $q = f_2(x)$ sont des nombres premiers, donc $bx + r = p$ et $ax + s = q$, ce qui donne $ap - bq = ar - bs = c$. L'implication $H \to C_2$ se trouve ainsi démontrée. □

Voici maintenant une conséquence de C_2 :

$C_{2.1}$. *Tout nombre rationnel positif peut être représenté d'une infinité de manières sous la forme $(p+1)/(q+1)$ ainsi que sous la forme $(p-1)/(q-1)$, où p et q sont des nombres premiers.*

Démonstration de l'implication $C_2 \to C_{2.1}$. Soit r un nombre rationnel > 1 ; on peut le représenter sous la forme $r = b/a$, où a et b sont des nombres naturels, $b > a$; $(a, b) = 1$ et il en résulte que $(a, b - a) = 1$ et on a évidemment $2 \mid ab(b - a)$. D'après C_2 il existe donc une infinité de systèmes de deux nombres premiers p et q tels que $ap - bq = b - a$, d'où $b/a = (p + 1)/(q + 1)$.

Si r était rationnel, $0 < r < 1$, on aurait $r = a/b$ où $b > a$ et on trouverait $a/b = (q+1)/(p+1)$. Pour la forme $(p-1)/(q-1)$ la démonstration serait analogue, en partant de l'équation $ap - bq = a - b$ pour $a > b$. Pour $r = 1$ la proposition $C_{2.1}$ est évidente.

En particulier, pour $r = 2$ il résulte de $C_{2.1}$ qu'il existe une infinité de nombres premiers p pour lesquels le nombre $2p + 1$, respectivement le nombre $2p - 1$ est premier. □

Si p et $2p + 1$ sont premiers, on a $\varphi(2p + 1) = 2p$, donc de $C_{2.1}$ résulte la proposition suivante :

$C_{2.1.1}$. *La suite $\frac{1}{2}\varphi(n)$ $(n = 1, 2, \dots)$ contient une infinité de nombres premiers.*

Soit k un nombre naturel pair. D'après $C_{2.1}$ il existe une infinité de nombres premiers $p > k$ tels que $2p-1$ est un nombre premier. k étant pair, on a $k = 2l$. Or, pour tout l naturel on a $\varphi(4l) = 2\varphi(2l)$, donc $\varphi(4lp) = 2\varphi(l)\varphi(p) = 2(p-1)\varphi(l)$ et $\varphi\big(2l(2p-1)\big) =$ c $\varphi(2l)\varphi(2p-1) = (2p-2)\varphi(2l)$ donc $\varphi(4lp-2l) = \varphi(4lp)$ et l'équation $\varphi(x+k) = \varphi(x)$ est remplie pour $x = 4lp - 2l$, $k = 2l$. On a ainsi la proposition suivante :

$C_{2.1.2}$. *L'équation $\varphi(x + k) = \varphi(x)$, où k est un nombre naturel pair, a une infinité de solutions.*

Pour k impairs l'étude de cette équation est beaucoup plus compliquée : voir A. Schinzel [16].

Il résulte tout de suite de $C_{2.1}$ qu'il existe pour tout nombre rationnel $r > 0$ une infinité de couples de nombres naturels x et y tels que $\sigma(x)/\sigma(y) = r$ (on peut prendre pour x et y des nombres premiers).

Une propriété analogue de la fonction φ peut aisément être démontrée sans faire appel à l'hypothèse H. En effet, si $r = l/m$, où l et m sont des nombres naturels et $(l, m) = 1$ et si k est un nombre naturel quelconque tel que $(k, lm) = 1$, on a

$$\varphi(l^2mk)/\varphi(lm^2k) = l/m = r.$$

Or, il résulte tout de suite $C_{2.1}$ que, pour tout nombre rationnel $r > 0$, l'équation $\varphi(x)/\varphi(y) = r$ a une infinité de solutions en nombres premiers x et y.

P. Erdős a démontré d'une façon élémentaire l'existence des suites infinies m_k et n_k $(k = 1, 2, \dots)$ de nombres naturels tels que $m_k/n_k \to +\infty$ et $\varphi(m_k) = \varphi(n_k)$ pour $k = 1, 2, \dots$. Sa méthode n'est pas applicable à la fonction σ. Or, $C_{2.1}$ entraîne le corollaire suivant :

$C_{2.1.3}$. *Quel que soit le nombre naturel k, il existe des nombres naturels m et n tels que $\sigma(m) = \sigma(n)$ et $m/n > k$.*

Démonstration de l'implication $C_{2.1} \to C_{2.1.3}$. Comme on sait, il existe pour tout nombre naturel k un nombre naturel l tel que $\sigma(l)/l > 2k$ (ce qui résulte par exemple de l'inégalité

$$\frac{\sigma(n!)}{n!} \geqslant \frac{1}{1} + \frac{1}{2} + \dots + \frac{1}{n} \quad \text{pour} \quad n = 1, 2, \dots$$

et de la divergence de la série harmonique). Or, d'après $C_{2.1}$ (pour $r = \sigma(l)$) il existe des nombres premiers $p > l$ et $q > l$ tels que

$$\frac{\sigma(p)}{\sigma(q)} = \frac{p+1}{q+1} = \sigma(l).$$

Posons $m = p$, $n = lq$. On aura donc $\sigma(n) = \sigma(lq) = \sigma(l)\sigma(q) = \sigma(p) = \sigma(m)$ donc $\sigma(m) = \sigma(n)$, et

$$\frac{m}{n} = \frac{p}{lq} = \frac{p}{\sigma(p)} \cdot \frac{\sigma(q)}{q} \cdot \frac{\sigma(l)}{l} > \frac{p}{p+1} \cdot 2k > k. \qquad \square$$

C_3. *Si a, b et c sont des entiers, $a > 0$, $(a, b, c) = 1$ et les nombres $a + b$ et c ne sont pas simultanément pairs, et $b^2 - 4ac$ n'est pas un carré, il existe une infinité de nombres premiers de la forme $ax^2 + bx + c$.* (Cf. Hardy et Littlewood [10], p. 48, Conjecture F).

Démonstration de l'implication H $\to$ C_3. Comme $b^2 - 4ac$ n'est pas un carré, le trinôme $ax^2 + bx + c$ est irréductible. Il remplit aussi la condition C, puisque

$$\big(f(0),\, f(1),\, f(2)\big) = (c, a+b+c, 4a+2b+c) = (c, a+b, 2a)$$
$$= (c, a+b, a) = (c, b, a) = 1.$$

c L'implication H $\to$ C_3 se trouve ainsi démontrée. □

$C_{3.1}$. *Si k est un entier et $-k$ n'est pas un carré, il existe une infinité de nombres premiers de la forme $x^2 + k$.* (Pour $k = 1$ cf. Hardy et Littlewood [10], p. 48, Conjecture E).

Pour déduire $C_{3.1}$ de C_3 il suffit de poser, dans C_3, $a = 1$, $b = 0$, $c = k$.

$C_{3.1.1}$. *Tout nombre naturel pair est d'une infinité de manières somme de deux nombres*
c *premiers conjugués du corps $\mathbb{Q}(\sqrt{-1})$.*

Démonstration de l'implication $C_{3.1} \to C_{3.1.1}$. Pour k naturel donné il existe, d'après $C_{3.1}$, une infinité de nombres premiers > 2 de la forme $p = x^2 + k^2$; ces nombres sont, on le voit sans peine, de la forme $4t + 1$, et on a $p = (k + xi)(k - xi)$ où $k + xi$ et $k - xi$ sont des nombres premiers conjugués du corps $\mathbb{Q}(\sqrt{-1})$, et $2k = (k + xi) + (k - xi)$.

Quant aux nombres impairs, on peut démontrer que tout nombre naturel impair < 29 est la somme de deux nombres premiers du corps $\mathbb{Q}(\sqrt{-1})$, mais il existe une infinité de nombres impairs qui ne sont pas de telles sommes, par exemple tous les nombres $170k + 29$ et tous les nombres $130k + 33$ où $k = 0, 1, 2, \ldots$.

Il est à remarquer que sans avoir recours à l'hypothèse H nous ne savons pas démontrer non seulement qu'il existe une infinité de nombres premiers de la forme $x^2 + 1$, où x est un nombre naturel, mais aussi qu'il existe une infinité de nombres premiers de la forme $x^2 + y^2 + 1$, où x et y sont des nombres naturels. Cependant on sait démontrer qu'il existe une infinité de nombres premiers de la forme $x^2 + y^2 + z^2 + 1$, où x, y, z sont des nombres naturels : tels sont, par exemple, tous les nombres premiers de la forme $8k + 7$.□

C_4. *L'équation $ax^2 + bx + c = dy$, où a, b, c, d sont des entiers, $a > 0$ et $d > 0$, a une infinité de solutions en nombres premiers x et y si et seulement si $\Delta = b^2 - 4ac$ n'est pas un carré (d'un nombre entier) et si elle a au moins une solution en nombres entiers x_0, y_0 tels que $(x_0 y_0, 6ad) = 1$.*

Démonstration de l'implication H $\to$ C_4. Nous prouverons sans avoir recours à l'hypothèse H que la condition est nécessaire.

Si l'équation $ax^2 + bx + c = dy$ a une infinité de solutions en nombres premiers, il existe des nombres premiers x_0 et y_0 plus grands que $6ad$ et tels que $ax_0^2 + bx_0 + c = dy_0$ et alors on a $(x_0 y_0, 6ad) = 1$.

Si Δ était un carré, soit $b^2 - 4ac = k^2$, où k est un entier $\geqslant 0$, on aurait, comme on le vérifie aisément $4ady_0 = (2ax_0 + b + k)(2ax_0 + b - k)$. Or, on déduit sans peine de cette égalité que pour x_0 premiers suffisamment grands le nombre y_0 ne peut pas être premier.

La condition de C_4 est donc nécessaire. Supposons maintenant que le nombre Δ ne soit pas un carré et que x_0 et y_0 soient des entiers tels que $ax_0^2 + bx_0 + c = dy_0$ et

$(x_0y_0, 6ad) = 1$. Posons

$$f_1(x) = dx + x_0, \quad f_2(x) = adx^2 + (2ax_0 + b)x + y_0.$$

Les polynômes f_1 et f_2 sont irréductibles, puisque

$$(2ax_0 + b)^2 - 4ady_0 = (2ax_0 + b)^2 - 4a(ax_0^2 + bx_0 + c) = b^2 - 4ac = \Delta$$

et, d'après l'hypothèse, Δ n'est pas un carré (d'un nombre rationnel).

S'il existait un nombre premier p tel que $p \mid f_1(x) f_2(x)$ pour x entiers, alors, en vertu du théorème de Lagrange, on aurait ou bien $p \leqslant 3$ ou bien $p \mid ad^2$, donc toujours $p \mid 6ad^2$ et $p \mid f_1(0) f_2(0) = x_0y_0$ et, comme $(x_0y_0, 6ad) = 1$, d'où $(x_0y_0, 6ad^2) = 1$, on aurait $p \mid 1$, ce qui est impossible. Les polynômes $f_1(x)$ et $f_2(x)$ satisfont donc aux conditions de l'hypothèse H, par conséquent pour une infinité de nombres naturels x les nombres $f_1(x) = p$ et $f_2(x) = q$ sont premiers et on vérifie sans peine que $ap^2 + bp + c = dq$. L'implication H $\rightarrow$ C_4 est ainsi démontrée. □

$C_{4.1}$. *Tout nombre rationnel $r > 1$ peut être représenté d'une infinité de manières sous la forme $(p^2 - 1)/(q - 1)$, où p et q sont des nombres premiers.*

Démonstration de l'implication $C_4 \rightarrow C_{4.1}$. Soit r un nombre rationnel > 1, donc $r = d/a$, où a et d sont des nombres naturels, $d > a$. Posons, dans C_4, $b = 0$, $c = d - a$. On aura donc $b^2 - 4ac = -4a(d - a) < 0$, ce qui n'est pas un carré. Or, les nombres $x_0 = y_0 = 1$ sont tels que $(x_0y_0, 6ad) = 1$ et $ax_0^2 + (d - a) = dy_0$. En vertu de C_4 il existe donc une infinité de nombres premiers p et q tels que $ap^2 + (d - a) = dq$, d'où $(p^2 - 1)/(q - 1) = d/a = r$, ce qui prouve que $C_4 \rightarrow C_{4.1}$. □

$C_{4.1.1}$. *Il existe une infinité de triangles orthogonaux de côtés naturels dont deux sont des nombres premiers.*

Démonstration de l'implication $C_{4.1} \rightarrow C_{4.1.1}$. Pour $r = 2$ il résulte de $C_{4.1}$ que l'équation $p^2 = 2q - 1$ a une infinité de solutions en nombres premiers. Or, cette équation équivaut évidemment à l'équation $p^2 + (q - 1)^2 = q^2$. On a donc $C_{4.1} \rightarrow C_{4.1.1}$. Voici quelques triangles satisfaisant aux conditions de $C_{4.1.1}$:

$$(3, 4, 5), \quad (5, 12, 13), \quad (11, 60, 61), \quad (19, 180, 181),$$

c $$(29{,}420{,}421), \quad (61{,}1860{,}1861).$$ □

Dans Scripta Mathematica 22 (1956), p. 158, Curiosum 435 (G. *An interesting observation*) on trouve l'observation qu'il existe un grand nombre de cas où pour p premier l'addition de l'unité au nombre triangulaire d'ordre p, respectivement la soustraction du nombre 2 donne un nombre premier, par exemple $t_3 + 1 = 7$, $t_7 + 1 = 29$, $t_5 - 2 = 13$. Nous déduirons de l'hypothèse H les conséquences $C_{4.2}$ et $C_{4.3}$ suivantes :

$C_{4.2}$. *Il existe une infinité de nombres premiers p tels que $\frac{1}{2}p(p + 1) + 1$ est un nombre premier.*

Démonstration de l'implication $C_4 \to C_{4.2}$. Posons, dans C_4, $a = b = 1$, $c = d = 2$. Le nombre $b^2 - 4ac = -7$ n'est pas un carré. L'équation $x^2 + x + 2 = 2y$ admet la solution $x_0 = -1$, $y_0 = 1$, qui remplit la condition $(x_0 y_0, 6ad) = 1$, et la proposition $C_{4.2}$ résulte immédiatement de C_4. □

$C_{4.3}$. *Il existe une infinité de nombres premiers p tels que le nombre $\frac{1}{2}p(p+1) - 2$ est premier.*

Démonstration de l'implication $C_4 \to C_{4.3}$. Posons, dans C_4, $a = b = 1$, $c = -4$, $d = 2$. Le nombre $b^2 - 4ac = 17$ n'est pas un carré. L'équation $x^2 + x - 4 = 2y$ admet la solution $x_0 = 1$, $y_0 = -1$, telle que $(x_0 y_0, 6ad) = 1$, donc C_4 entraîne immédiatement $C_{4.3}$. □

$C_{4.4}$. *La suite $\sigma(n)$ $(n = 1, 2, \dots)$ contient une infinité de nombres premiers.*

Démonstration de l'implication $C_4 \to C_{4.4}$. Posons, dans C_4, $a = b = c = d = 1$. Le nombre $b^2 - 4ac = -3$ n'est pas un carré. L'équation $x^2 + x + 1 = y$ admet la solution $x_0 = -1$, $y_0 = 1$, où $(x_0 y_0, 6ad) = 1$, et, comme pour p premiers on a $\sigma(p^2) = p^2 + p + 1$, C_4 entraîne la proposition $C_{4.4}$. □

C_5. *Tout nombre naturel peut être représenté d'une infinité de manières sous la forme $\sigma(x) - \sigma(y)$ (où x et y sont des nombres naturels).*

Démonstration de l'implication $H \to C_5$. Si n est pair, il existe, d'après $C_{1.1}$, une infinité de nombres premiers p et q tels que $p - q = n$, d'où $\sigma(p) - \sigma(q) = (p+1) - (q+1) = n$. Or, si n est impair, posons, dans C_4, $a = b = d = 1$, $c = n$. Le nombre $b^2 - 4ac = 1 - 4n < 0$ n'est pas un carré. Si $3 \mid n$, alors, n étant impair, on a $(n+2, 6) = 1$ et pour $x_0 = 1$, $y_0 = n+2$ on a $x_0^2 + x_0 + n = y_0$ et $(x_0 y_0, 6ad) = (n+2, 6) = 1$. Si l'on n'a pas $3 \mid n$, alors $(n, 6) = 1$ et pour $x_0 = -1$, $y_0 = n$ on trouve $x_0^2 + x_0 + n = y_0$ et $(x_0 y_0, 6ad) = (-n, 6) = 1$. D'après C_4 il existe donc une infinité de nombres premiers p et q tels que $p^2 + p + n = q$, d'où

$$\sigma(q) - \sigma(p^2) = q + 1 - (p^2 + p + 1) = q - p^2 - p = n.$$

On a donc $H \to C_5$. □

Il est à remarquer que pour la fonction φ la proposition analogue à C_5 est fausse, car on peut démontrer d'une façon élémentaire qu'aucun des nombres $2 \cdot 7^n - 1$ $(n = 1, 2, \dots)$ n'est de la forme $\varphi(x) - \varphi(y)$, mais, comme pour p et q premiers on a $\varphi(p) - \varphi(q) = p - q$, on déduit de $C_{1.1}$ que tout nombre pair est de la forme $\varphi(x) - \varphi(y)$.

C_6. *n étant un nombre impair > 1, k un entier donné quelconque qui n'est pas une puissance d'un entier à l'exposant $d > 1$ et $d \mid n$, il existe une infinité de nombres premiers de la forme $x^n + k$, où x est un nombre naturel* (pour $n = 3$ cf. Hardy et Littlewood [10], p. 50, Conjecture K). *Si, en outre k est pair, il existe une infinité de nombres premiers p tels que $p^n + k$ est un nombre premier.*

Démonstration de l'implication H $\to$ C_6. n étant un nombre impair et k n'étant pas une puissance d'un entier à l'exposant $d > 1$ et $d \mid n$, le polynôme $f_1(x) = x^n + k$ est irréductible. Or, on a $\big(f_1(0), f_1(1)\big) = (k, k+1) = 1$ et on déduit de H la première partie de C_6. Si k est pair, alors, en posant $f_2(x) = x$ on a $\big(f_1(-1)f_2(-1), f_1(1)f_2(1)\big) = (k-1, k+1) = 1$, la condition C est encore remplie et H entraîne la deuxième partie de C_6. □

Il est à remarquer que sans l'aide de l'hypothèse H nous ne savons démontrer même pas l'existence d'une infinité de nombres premiers de la forme $x^3 + y^3 + z^3$, où x, y et z sont des entiers. On sait cependant démontrer (sans l'aide de l'hypothèse H) l'existence d'une infinité de nombres premiers de la forme $x^3 + y^3 + z^3 + t^3$ où x, y, z, t sont des entiers : tels sont, par exemple, tous les nombres de la forme $9k \pm 1$.

C_7. *Il existe une infinité de nombres naturels n tels que chacun des nombres n, $n+1$, $n+2$ est le produit de deux nombres premiers distincts.*

Démonstration de l'implication H $\to$ C_7. Soit $f_1(x) = 10x + 1$, $f_2(x) = 15x + 2$, $f_3(x) = 6x + 1$. On a ici $a = f_1(0)f_2(0)f_3(0) = 2$ et $b = f_1(1)f_2(1)f_3(1) = 11 \cdot 17 \cdot 7$, donc $(a, b) = 1$ et il résulte de H qu'il existe une infinité de nombres naturels x tels que les nombres $p = 10x + 1$, $q = 15x + 2$, $r = 6x + 1$ sont premiers. Pour $n = 3p$ on trouve $n + 1 = 3p + 1 = 2(15x + 2) = 2q$, $n + 2 = 2q + 1 = 30x + 5 = 5(6x + 1) = 5r$ et $p \geqslant 11 > 3$, $q \geqslant 17 > 2$, $r \geqslant 7 > 5$, d'où il résulte que chacun des nombres n, $n + 1$, $n + 2$ est le produit de deux nombres premiers distincts. De C_7 résulte tout de suite l'existence d'une infinité de nombres naturels n tels que les nombres n, $n + 1$ et $n + 2$ ont le même nombre de diviseurs. □

Or, il n'existe pas quatre nombres naturels consécutifs dont chacun serait le produit de nombres premiers distincts, un de ces nombres étant toujours divisible par 4.

C_8. *Il existe pour tout nombre naturel s un nombre naturel m_s tel que chacune des équations $\varphi(x) = m_s$ et $\sigma(x) = m_s$ a plus de s solutions.* (Ce problème a été posé par P. Erdős).

Démonstration de l'implication H $\to$ C_8. Posons $f_i(x) = 2^i x + 1$ et $g_i(x) = 2^i x - 1$ $(i = 0, 1, \ldots, 2s + 1)$.

Comme $f_0(0) f_1(0) \cdots f_{2s+1}(0) g_0(0) g_1(0) \cdots g_{2s+1}(0) = 1$, les polynômes f_i et g_i $(i = 0, 1, \ldots, 2s + 1)$ satisfont à la condition C et d'après H, il existe un nombre naturel x tel que les nombres $f_i(x)$ et $g_i(x)$ pour $i = 0, 1, \ldots, 2s + 1$ sont premiers. Posons

$$a_i = f_i(x) f_{2s-i+1}(x), \quad b_i = g_i(x) g_{2s-i+1}(x), \quad (i = 0, 1, \ldots, 2s + 1)$$

$f_i(x)$ et $f_{2s-i+1}(x)$, respectivement $g_i(x)$ et $g_{2s-i+1}(x)$ (pour $i = 0, 1, \ldots, 2s + 1$) étant des nombres premiers distincts, on a

$$\big(f_i(x), f_{2s-i+1}(x)\big) = 1 \text{ et } \big(g_i(x), g_{2s-i+1}(x)\big) = 1 \quad \text{pour} \quad i = 0, 1, \ldots, 2s + 1,$$

donc, pour $i = 0, 1, \ldots, 2s + 1$:

$$\varphi(a_i) = \varphi\big(f_i(x)\big)\varphi\big(f_{2s-i+1}(x)\big) = 2^i x 2^{2s-i+1} x = 2^{2s+1} x^2,$$
$$\sigma(b_i) = \sigma\big(g_i(x)\big)\sigma\big(g_{2s-i+1}(x)\big) = 2^i x 2^{2s-i+1} x = 2^{2s+1} x^2.$$

Les nombres a_i $(i = 0, 1, \ldots, s)$ et de même les nombres b_i $(i = 0, 1, \ldots, s)$ étant distincts, l'implication $\mathrm{H} \to \mathrm{C}_8$ se trouve démontrée. □

Il est à remarquer qu'une proposition analogue pour la fonction φ a été démontrée sans avoir recours à l'hypothèse H par P. Erdős ([7], p. 213) et que, selon son avis, une modification de sa démonstration permettrait de démontrer une proposition analogue pour la fonction σ. Or, une démonstration tout à fait élémentaire pour la fonction φ a été donnée par A. Schinzel [15].

Sans avoir recours à l'hypothèse H nous ne savons par démontrer que l'équation $\varphi(x) = \sigma(y)$ a une infinité de solutions en nombres naturels x et y.

C_9. *Il existe une infinité de nombres premiers p pour lesquels le nombre $2^p - 1$ est composé.*

Démonstration de l'implication $\mathrm{H} \to \mathrm{C}_9$. Soit $f_1(x) = 4x - 1$, $f_2(x) = 8x - 1$. Il résulte de H qu'il existe une infinité de nombres naturels x pour lesquels les nombres $p = 4x - 1$ et $q = 8x - 1$ sont premiers. Mais alors on a $q - 1 = 2p$ et, comme on sait, $q \mid 2^p - 1$ et, si $x > 1$, on a $2^p - 1 > q$ et le nombre $2^p - 1$ est composé. Il résulte donc l'hypothèse H qu'il existe une infinité de nombres de Mersenne $M_p = 2^p - 1$ composés dont les indices p sont des nombres premiers. □

Un nombre naturel composé n est dit *absolument pseudo-premier* si pour tout entier a on a $n \mid a^n - a$.

C_{10}. *Il existe une infinité de nombres absolument pseudo-premiers.*

Démonstration de l'implication $\mathrm{H} \to \mathrm{C}_{10}$. Soit $f_1(x) = 6x + 1$, $f_2(x) = 12x + 1$, $f_3(x) = 18x + 1$. Comme $f_1(0) f_2(0) f_3(0) = 1$, il résulte de H qu'il existe une infinité de nombres naturels x tels que chacun des nombres $p = 6x + 1$, $q = 12x + 1$, $r = 18x + 1$ est premier et alors on le sait, le nombre pqr est absolument pseudo-premier (il est donc aussi un nombre de Carmichael) (voir [4], p. 271). □

C_{11} (Hypothèse de E. Artin). *Tout nombre entier $g \neq -1$ qui n'est pas un carré est racine primitive pour une infinité de nombres premiers.*

Démonstration de l'implication $\mathrm{H} \to \mathrm{C}_{11}$. Soit $g = a^2 b$, où a est un nombre naturel, b un entier qui n'est divisible par aucun carré > 1. Comme g n'est pas un carré, on a $b \neq 1$. Soit b_1 le plus grand diviseur impair de b.

Nous prouverons d'abord qu'il existe des binômes $f_1(x)$ et $f_2(x)$ satisfaisant à la condition C et tels que

1° *quel que soit le nombre naturel x, b est un non-résidu quadratique pour $f_1(x)$;*
2° *$f_1(x) - 1 = 2 f_2(x)$ si $b \neq 3$ et $f_1(x) - 1 = 4 f_2(x)$ si $b = 3$.*

Si $b < 0$, soit $f_1(x) = -4bx - 1$, $f_2(x) = -2bx - 1$. La condition 2° est évidemment remplie et, comme $f_1(0) f_2(0) = 1$, les binômes $f_1(x)$ et $f_2(x)$ satisfont à la condition C.

Si b est pair, on a $f_1(x) \equiv -1 \pmod 8$ et le symbole de Jacobi

$$\left(\frac{2}{f_1(x)}\right) = 1$$

et

$$\begin{aligned}\left(\frac{b}{f_1(x)}\right) = \left(\frac{-b_1}{f_1(x)}\right) = -\left(\frac{b_1}{f_1(x)}\right) &= -(-1)^{(b_1-1)/2}\left(\frac{f_1(x)}{b_1}\right)\\ &= -(-1)^{(b_1-1)/2}\left(\frac{-1}{b_1}\right) = -1,\end{aligned}$$

ce qui prouve que b est un non-résidu quadratique pour $f_1(x)$, c'est-à-dire que la condition 1° est remplie. Si b est impair, on a $b = -b_1$ et on parvient au même résultat.

Si $b > 0$ et b est pair, on a $b = 2b_1$. Soit $f_1(x) = 4bx + 2b - 1$, $f_2(x) = 2bx + b - 1$, $P(x) = f_1(x) f_2(x)$. On a $P(1) + P(-1) - 2P(0) = 16b^2$, $P(0) = (2b-1)(b-1)$ et, b étant pair, on a $\big(P(1) + P(-1) - 2P(0),\, P(0)\big) = 1$ et on en conclut que la condition C est remplie. La condition 2° est évidemment aussi remplie. Comme $b = 2b_1 = 2(2k+1)$, on trouve

$$f_1(x) \equiv 3 \pmod 8, \quad \text{d'où} \quad \left(\frac{2}{f_1(x)}\right) = -1$$

et

$$\begin{aligned}\left(\frac{b}{f_1(x)}\right) = \left(\frac{2}{f_1(x)}\right)\left(\frac{b_1}{f_1(x)}\right) = -\left(\frac{b_1}{f_1(x)}\right) &= -(-1)^{(b_1-1)/2}\left(\frac{f_1(x)}{b_1}\right)\\ &= -(-1)^{(b_1-1)/2}\left(\frac{-1}{b_1}\right) = -1,\end{aligned}$$

ce qui prouve que b est un non-résidu quadratique pour $f_1(x)$ et la condition 1° est remplie.

Soit maintenant b un nombre impair > 3, donc $b = q_1 q_2 \cdots q_k$, où q_i sont des nombres premiers ($i = 1, 2, \ldots, k$), $q_1 < q_2 < \ldots < q_k$ et $q_k > 3$. Le nombre premier q_k a donc au moins deux non-résidus quadratiques et l'un d'eux est $n_0 \not\equiv -1 \pmod{q_k}$. Le système des deux congruences $n \equiv -1 \pmod{4q_1 q_2 \cdots q_{k-1}}$ et $n \equiv -n_0 \pmod{q_k}$ a évidemment une solution $n = n_1$. Soit

$$f_1(x) = 4bx + n_1, \quad f_2(x) = 2bx + \tfrac{1}{2}(n_1 - 1), \quad P(x) = f_1(x) f_2(x).$$

On trouve sans peine

$$P(0) = \tfrac{1}{2} n_1(n_1 - 1), \quad P(1) + P(-1) - 2P(0) = 16b^2.$$

Or, comme $n_1 \equiv -1 \pmod{4q_1 q_2 \cdots q_{k-1}}$, d'où $\frac{1}{2}(n_1 - 1) \equiv -1 \pmod{2q_1 q_2 \cdots q_{k-1}}$, et $n_1 \not\equiv 0 \pmod{q_k}$ (puisque $n_1 \equiv -n_0 \pmod{q_k}$ et n_0 est un non-résidu quadratique pour q_k) et $\frac{1}{2}(n_1 - 1) \not\equiv 0 \pmod{q_k}$ (puisque $n_1 - 1 \equiv -n_0 - 1 \not\equiv 0 \pmod{q_k}$), on a $(4b, n_1) = 1$ et $\big(2b, \frac{1}{2}(n_1 - 1)\big) = 1$, d'où $\big(16b^2, \frac{1}{2} n_1(n_1 - 1)\big) = 1$, donc $\big(P(0), P(1) + P(-1) - 2P(0)\big) = 1$, d'où il résulte que les binômes $f_1(x)$ et $f_2(x)$ satisfont à la condition C. Or, la condition 2° est évidemment remplie. Or, on a $f_1(x) \equiv -1 \pmod{4q_1 q_2 \cdots q_{k-1}}$ et

$f_1(x) \equiv n_1 \pmod{q_k}$, d'où

$$\left(\frac{b}{f_1(x)}\right) = (-1)^{(b-1)/2}\left(\frac{f_1(x)}{b}\right) = \left(\frac{-f_1(x)}{b}\right) = \left(\frac{-n_1}{q_1 q_2 \cdots q_{k-1}}\right)\left(\frac{-n_1}{q_k}\right)$$
$$= \left(\frac{1}{q_1 q_2 \cdots q_{k-1}}\right)\left(\frac{n_0}{q_k}\right) = -1.$$

Le nombre b est donc un non-résidu quadratique pour $f(x)$ et la condition 1° est remplie.

Dans le cas $b = 3$ soit $f_1(x) = 12x + 5$, $f_2(x) = 3x + 1$. Ici on vérifie sans peine que les conditions C, 1° et 2° sont remplies.

Il résulte de l'hypothèse H qu'il existe une infinité de nombres naturels x tels que les nombres $f_1(x)$ et $f_2(x)$ sont tous les deux premiers. Soit x un de ces nombres, tel que $f_1(x) > g^4$. Si g appartenait modulo $f_1(x)$ à un exposant $< f_1(x) - 1$, on aurait, d'après 2°, $f_1(x) \mid g^{(f_1(x)-1)/2} - 1$ ou bien $f_1(x) \mid g^4 - 1$. Or, vu le théorème d'Euler relatif au symbole de Legendre, l'égalité $g = a^2 b$ et la condition 1°, on a

$$g^{(f_1(x)-1)/2} \equiv \left(\frac{g}{f_1(x)}\right) \equiv \left(\frac{b}{f_1(x)}\right) \equiv -1 \pmod{f_1(x)},$$

ce qui est incompatible avec $f_1(x) \mid g^{(f_1(x)-1)/2} - 1$ (puisque $f_1(x)$ est impair). On a donc $f_1(x) \mid g^4 - 1$, ce qui est impossible vu que $f_1(x) > g^4 > 1$. g est donc une racine primitive pour le module $f_1(x)$. L'hypothèse de Artin est donc une conséquence de l'hypothèse H.□

Nous étudierons maintenant la fonction

$$\varrho(x) = \overline{\lim_{y\to\infty}} [\pi(y + x) - \pi(y)].$$

(Cf. Hardy et Littlewood [10], p. 52–68).

On a $\varrho(1) = \varrho(2) = 1$, mais nous ne connaissons pas des valeurs $\varrho(x)$ pour aucun nombre naturel $x > 2$.

Il sera utile d'introduire la fonction auxiliaire

$$\overline{\varrho}(x) = \max_{0\leqslant y<x!} \big[\varphi(x!, y + x) - \varphi(x!, y)\big]$$

où $\varphi(m, n)$ désigne le nombre de nombres naturels ne dépassant pas n et premiers avec m.

De la définition de la fonction $\overline{\varrho}(x)$ résultent les lemmes suivantes :

Lemme 1.

$$\overline{\varrho}(x) = \max_{y,z=1,2,\ldots} \big\{\min\big[z, \varphi(z!, y + x) - \varphi(z!, y)\big]\big\}$$
$$\geqslant \max_{y=1,2,\ldots} \big\{\min\big[y, \pi(y + x) - \pi(y)\big]\big\} \geqslant \varrho(x).$$

Lemme 2. $\overline{\varrho}(x + 1) \geqslant \overline{\varrho}(x)$.

Lemme 3. $\overline{\varrho}(x) + \overline{\varrho}(y) \geqslant \overline{\varrho}(x + y)$.

Lemme 4. $\overline{\varrho}(x) \leqslant \varphi(x)$.

Nous démontrerons maintenant :

Théorème 1. $\overline{\varrho}(1) = \overline{\varrho}(2) = 1$, $\overline{\varrho}(3) = \overline{\varrho}(4) = \overline{\varrho}(5) = \overline{\varrho}(6) = 2$, $\overline{\varrho}(7) = \overline{\varrho}(8) = 3$, $\overline{\varrho}(9) = \ldots = \overline{\varrho}(12) = 4$, $\overline{\varrho}(13) = \ldots = \overline{\varrho}(16) = 5$, $\overline{\varrho}(17) = \ldots = \overline{\varrho}(20) = 6$, $\overline{\varrho}(21) = \ldots = \overline{\varrho}(26) = 7$, $\overline{\varrho}(27) = \ldots = \overline{\varrho}(30) = 8$, $\overline{\varrho}(31) = \overline{\varrho}(32) = 9$, $\overline{\varrho}(33) = \ldots = \overline{\varrho}(36) = 10$.

Démonstration. D'après de lemme 4 on trouve $\overline{\varrho}(2) \leqslant 1, \overline{\varrho}(6) \leqslant 2, \overline{\varrho}(12) \leqslant 4, \overline{\varrho}(30) \leqslant 8$. En vertu du lemme 3 on a $\overline{\varrho}(8) \leqslant \overline{\varrho}(6) + \overline{\varrho}(2) \leqslant 3$, $\overline{\varrho}(32) \leqslant \overline{\varrho}(30) + \overline{\varrho}(2) \leqslant 9$, $\overline{\varrho}(36) \leqslant \overline{\varrho}(30) + \overline{\varrho}(6) \leqslant 10$. Enfin il est facile de démontrer que parmi 16 nombres naturels consécutifs quelconques il y a au plus 5 nombres qui ne sont divisibles par aucun des nombres 2, 3 et 5, parmi 20 nombres naturels consécutifs quelconques il y a au plus 6 tels nombres et parmi 26 nombres naturels consécutifs quelconques il y a au plus 7 nombres qui ne sont divisibles par aucun des nombres 2, 3, 5 et 7. Donc $\overline{\varrho}(16) \leqslant 5$, $\overline{\varrho}(20) \leqslant 6$, $\overline{\varrho}(26) \leqslant 7$. D'autre part on a $\pi(1+1)-\pi(1) = 1, \pi(3+2)-\pi(2) = 2, \pi(7+4)-\pi(4) = 3$, $\pi(9+4)-\pi(4) = 4, \pi(13+6)-\pi(6) = 5, \pi(17+6)-\pi(6) = 6, \pi(21+10)-\pi(10) = 7$, $\pi(27+10)-\pi(10) = 8, \pi(31+10)-\pi(10) = 9, \pi(33+10)-\pi(10) = 10$. Donc, en vertu du lemme 1 on a $\overline{\varrho}(1) \geqslant 1$, $\overline{\varrho}(3) \geqslant 2$, $\overline{\varrho}(7) \geqslant 3$, $\overline{\varrho}(9) \geqslant 4$, $\overline{\varrho}(13) \geqslant 5$, $\overline{\varrho}(17) \geqslant 6$, $\overline{\varrho}(21) \geqslant 7$, $\overline{\varrho}(27) \geqslant 8$, $\overline{\varrho}(31) \geqslant 9$, $\overline{\varrho}(33) \geqslant 10$. La fonction $\overline{\varrho}(x)$ étant monotone (lemme 2), notre théorème résulte sans peine des inégalités obtenues. □

Appelons k-jumeaux (en allemand *k-linge*) k nombres premiers $k < q_1 < q_2 < \ldots$ $\ldots < q_k$ tels que $\overline{\varrho}(q_k - q_1) = k - 1$. Ainsi deux nombres premiers $q_1 > 2$ et q_2 seront 2-jumeaux si $\overline{\varrho}(q_2 - q_1) = 1$, c'est-à-dire $q_2 - q_1 = 2$. Les nombres premiers q_1, q_2, q_3 tel que $3 < q_1 < q_2 < q_3$ et $\overline{\varrho}(q_3 - q_1) = 2$ seront appelés 3-jumeaux etc.

Les données numériques concernant les nombres k-jumeaux ont été données
pour $k = 2$, $q_k \leqslant 10^6$ par G. H. Hardy et J. E. Littlewood ([10], p. 44),
pour $k = 3$, $q_k \leqslant 10^6$ par G. H. Hardy et J. E. Littlewood ([10], p. 63),
pour $k = 4$, $q_k \leqslant 10^6$ par G. H. Hardy et J. E. Littlewood ([10], p. 63),
pour $k = 4$, $10^6 < q_k \leqslant 2 \cdot 10^6$ par Ch. Sexton [17],
pour $k = 4$, $2 \cdot 10^6 < q_k \leqslant 3 \cdot 10^6$ par W. A. Golubew [8],
pour $k = 4$, $3 \cdot 10^6 < q_k \leqslant 5 \cdot 10^6$ par W. A. Golubew [9],
pour $k = 5$, $q_k \leqslant 2 \cdot 10^6$ par W. A. Golubew [8],
pour $k = 5$, $2 \cdot 10^6 < q_k \leqslant 5 \cdot 10^6$ par W. A. Golubew [9],
pour $k = 6$, $q_k \leqslant 14 \cdot 10^6$ par W. A. Golubew [9].

Le problème si pour tout k naturel il existe une infinité de nombres k-jumeaux équivaut, comme on le démontre sans peine, au problème si l'on a pour tout x, $\varrho(x) = \overline{\varrho}(x)$: l'hypothèse H résout donc ce problème positivement (voir plus loin C_{12}).

Théorème 2. $\overline{\varrho}(57) = \overline{\varrho}(58) = \overline{\varrho}(59) = \overline{\varrho}(60) = 15$.

Démonstration. L. Aubry a démontré (voir L. E. Dickson [6], p. 355) que parmi 30 nombres impairs consécutifs il y a au plus 15 nombres qui ne sont divisibles par aucun des nombres 3, 5 et 7. Il en résulte que $\overline{\varrho}(60) \leqslant 15$. D'autre part on a $\pi(57+16) - \pi(16) = 15$, donc $\overline{\varrho}(57) \geqslant 15$. Vu le lemme 2 on a donc $\overline{\varrho}(57) = \ldots = \overline{\varrho}(60) = 15$. □

Théorème 3. *On a* $\overline{\varrho}(95) = \ldots = \overline{\varrho}(100) = 23$.

Démonstration. A. Schinzel a démontré (dans un article qui paraître ailleurs ([2])) que parmi 100 nombres naturels consécutifs quelconques il y a au plus 23 nombres qui ne sont divisibles par aucun nombre premier $\leqslant 17$, d'où résulte tout de suite que $\overline{\varrho}(100) \leqslant 23$.
c D'autre part on a $\varphi(23!, 4083966+95) - \varphi(23!, 4083966) = 23$, donc d'après le lemme 1 : $\overline{\varrho}(95) \geqslant 23$.

La fonction $\overline{\varrho}(x)$ étant monotone on en obtient le théorème 3. □

En vertu du lemme 1, le théorème 3 donne $\varrho(100) \leqslant 23$, ce qui est incompatible avec l'inégalité $\varrho(97) \geqslant 24$ qui a été déduite à la p. 67 du travail cité de Hardy et Littlewood [10] de leur hypothèse X. Or, cette déduction était fausse, car ces auteurs affirment qu'aucun des nombres premiers $\geqslant 17$ et $\leqslant 113$ ne donne le reste 8 mod 17, ce qui n'est pas vrai, puisque $59 \equiv 8 \pmod{17}$.

Théorème 4. *On a* $\overline{\varrho}(x) \leqslant \pi(x)$ *pour* $1 < x \leqslant 132$.

Démonstration. Vu le théorème 1 nous avons $\overline{\varrho}(2) = 1 = \pi(2)$, $\overline{\varrho}(6) = 2 = \pi(3)$, $\overline{\varrho}(8) = 3 < \pi(7)$, $\overline{\varrho}(12) = 4 = \pi(9)$, $\overline{\varrho}(16) = 5 < \pi(13)$, $\overline{\varrho}(20) = 6 < \pi(17)$, $\overline{\varrho}(26) = 7 < \pi(21)$, $\overline{\varrho}(30) = 8 < \pi(27)$, $\overline{\varrho}(32) = 9 < \pi(31)$, $\overline{\varrho}(36) = 10 < \pi(33)$, et, les fonctions $\overline{\varrho}(x)$ et $\pi(x)$ étant monotones, cela prouve le théorème 4 pour $1 < x \leqslant 36$.

Or, en vertu du lemme 3 on a

$$\begin{aligned}
\overline{\varrho}(38) &\leqslant \overline{\varrho}(30) + \overline{\varrho}(8) &&= 8 + 3 = 11 < \pi(37),\\
\overline{\varrho}(42) &\leqslant \overline{\varrho}(30) + \overline{\varrho}(12) &&= 8 + 4 = 12 = \pi(39),\\
\overline{\varrho}(46) &\leqslant \overline{\varrho}(30) + \overline{\varrho}(16) &&= 8 + 5 = 13 < \pi(43),\\
\overline{\varrho}(50) &\leqslant \overline{\varrho}(30) + \overline{\varrho}(20) &&= 8 + 6 = 14 < \pi(47).
\end{aligned}$$

D'après le théorème 2 on a $\overline{\varrho}(60) = 15 = \pi(51)$. En vertu du lemme 3 on trouve

$$\begin{aligned}
\overline{\varrho}(62) &\leqslant \overline{\varrho}(60) + \overline{\varrho}(2) &&= 15 + 1 = 16 < \pi(61),\\
\overline{\varrho}(66) &\leqslant \overline{\varrho}(60) + \overline{\varrho}(6) &&= 15 + 2 = 17 < \pi(63),\\
\overline{\varrho}(68) &\leqslant \overline{\varrho}(60) + \overline{\varrho}(8) &&= 15 + 3 = 18 < \pi(67),\\
\overline{\varrho}(72) &\leqslant \overline{\varrho}(60) + \overline{\varrho}(12) &&= 15 + 4 = 19 = \pi(69),\\
\overline{\varrho}(76) &\leqslant \overline{\varrho}(60) + \overline{\varrho}(16) &&= 15 + 5 = 20 < \pi(73),\\
\overline{\varrho}(80) &\leqslant \overline{\varrho}(60) + \overline{\varrho}(20) &&= 15 + 6 = 21 = \pi(77),\\
\overline{\varrho}(86) &\leqslant \overline{\varrho}(60) + \overline{\varrho}(26) &&= 15 + 7 = 22 = \pi(81).
\end{aligned}$$

En vertu du théorème 3 on a $\overline{\varrho}(100) \leqslant 23 = \pi(87)$. En vertu du lemme 3 on trouve

$$\begin{aligned}
\overline{\varrho}(102) &\leqslant \overline{\varrho}(100) + \overline{\varrho}(2) &&= 23 + 1 = 24 < \pi(101),\\
\overline{\varrho}(106) &\leqslant \overline{\varrho}(100) + \overline{\varrho}(6) &&= 23 + 2 = 25 < \pi(103),\\
\overline{\varrho}(108) &\leqslant \overline{\varrho}(100) + \overline{\varrho}(8) &&= 23 + 3 = 26 < \pi(107),\\
\overline{\varrho}(112) &\leqslant \overline{\varrho}(100) + \overline{\varrho}(12) &&= 23 + 4 = 27 < \pi(109),\\
\overline{\varrho}(116) &\leqslant \overline{\varrho}(100) + \overline{\varrho}(16) &&= 23 + 5 = 28 < \pi(113),
\end{aligned}$$

([2]) Voir J2, p. 1139.

$$\overline{\varrho}(120) \leqslant \overline{\varrho}(100) + \overline{\varrho}(20) = 23 + 6 = 29 < \pi(117),$$
$$\overline{\varrho}(126) \leqslant \overline{\varrho}(100) + \overline{\varrho}(26) = 23 + 7 = 30 < \pi(121),$$
$$\overline{\varrho}(130) \leqslant \overline{\varrho}(100) + \overline{\varrho}(30) = 23 + 8 = 31 < \pi(127),$$
$$\overline{\varrho}(132) \leqslant \overline{\varrho}(100) + \overline{\varrho}(32) = 23 + 9 = 32 = \pi(131).$$

Les fonctions $\overline{\varrho}(x)$ et $\pi(x)$ étant monotones, nous en concluons que le théorème 4 est vrai pour $1 < x \leqslant 132$. □

Corollaire 1. *$\varrho(x) \leqslant \pi(x)$ pour $1 < x \leqslant 132$.*

La démonstration résulte du lemme 1 et du théorème 4.

Hardy et Littlewood ont énoncé ([10], p. 54) l'hypothèse que $\varrho(x) \leqslant \pi(x)$ quel que soit le nombre $x > 1$.

Corollaire 2. *Si $x > 1$, $y > 1$ et si l'un au moins des nombres x et y est $\leqslant 132$, on a*

$$\pi(x + y) \leqslant \pi(x) + \pi(y).$$

Démonstration. Sans nuire à la généralité nous pouvons supposer que $x < y, 1 < x \leqslant 132$. En vertu du théorème 4 on a donc $\overline{\varrho}(x) \leqslant \pi(x)$. Or, en vertu du lemme 1 on a, pour tout nombre y,

$$\min\big(y, \pi(x + y) - \pi(y)\big) \leqslant \pi(x).$$

Comme $y \geqslant x \geqslant \pi(x+y) - \pi(y)$, on a $\pi(x+y) - \pi(y) \leqslant \pi(x)$, c'est-à-dire $\pi(x+y) \leqslant \pi(x) + \pi(y)$. □

Il est à remarquer que E. Landau [12] a démontré que pour x suffisament grands on a $\pi(2x) < 2\pi(x)$.

Nous appliquerons maintenant l'hypothèse H à l'étude de la fonction $\varrho(x)$.

C_{12}. *$\varrho(x) = \overline{\varrho}(x)$ pour x naturels.*

Démonstration de $H \to C_{12}$. D'après le lemme 1 il suffit de prouver que $\varrho(x) \geqslant \overline{\varrho}(x)$. Dans ce but supposons que pour x naturel donné $s = \overline{\varrho}(x)$. D'après la définition de $\overline{\varrho}(x)$ il existe un entier y tel que $0 \leqslant y < x!$ et que $s = \varphi(x!, y + x) - \varphi(x!, y)$. Évidemment on a $s \leqslant x$ et il existe s entiers croissants $a_1, a_2, \ldots, a_s$, où $0 \leqslant a_1 < a_s \leqslant x$ tels que $(y + a_i, x!) = 1$ pour $i = 1, 2, \ldots, s$.

Soit $f_i(\xi) = \xi + a_i$ pour $i = 1, 2, \ldots, s$,

$$P(\xi) = \prod_{i=1}^{s} f_i(\xi).$$

Si p est un nombre premier tel que $p \mid P(\xi)$ pour ξ entiers, on a, d'après le théorème de Lagrange, $p \leqslant s \leqslant x$, donc $p \mid x!$ et, d'après $(y + a_i, x!) = 1$, $(y + a_i, p) = 1$ pour $i = 1, 2, \ldots, s$, et comme $P(y) = \prod_{i=1}^{s} (y + a_i)$, cela donne $\big(P(y), p\big) = 1$, contrairement à $p \mid P(y)$.

La condition C est donc remplie et d'après H il existe une infinité de nombres naturels ξ tels que le nombres $\xi + a_i$ $(i = 1, 2, \ldots, s)$ sont tous premiers. Comme $0 \leqslant a_1 < a_s \leqslant x$, il en résulte que $\pi(\xi + x) - \pi(\xi) \geqslant s = \overline{\varrho}(x)$ pour une infinité de nombres naturels ξ et, vu la définition de la fonction $\varrho(x)$ cela donne $\varrho(x) \geqslant \overline{\varrho}(x)$. L'implication $\mathrm{H} \to \mathrm{C}_{12}$ se trouve ainsi démontrée. □

$\mathrm{C}_{12.1}$. $\varrho(1) = \varrho(2) = 1$, $\varrho(3) = \ldots = \varrho(6) = 2$, $\varrho(7) = \varrho(8) = 3$, $\varrho(9) = \ldots = \varrho(12) = 4$, $\varrho(13) = \ldots = \varrho(16) = 5$, $\varrho(17) = \ldots = \varrho(20) = 6$, $\varrho(21) = \ldots = \varrho(26) = 7$, $\varrho(27) = \ldots = \varrho(30) = 8$, $\varrho(31) = \varrho(32) = 9$, $\varrho(33) = \ldots = \varrho(36) = 10$, $\varrho(57) = \ldots = \varrho(60) = 15$, $\varrho(95) = \ldots = \varrho(100) = 23$.

$\mathrm{C}_{12.1}$ est une conséquence immédiate de C_{12} et des théorèmes 1, 2 et 3.

$\mathrm{C}_{12.2}$. *L'hypothèse de Hardy et Littlewood suivant laquelle $\varrho(x) \leqslant \pi(x)$ pour x naturels > 1 équivaut à l'inégalité*

$$(*) \qquad \pi(x + y) \leqslant \pi(x) + \pi(y) \quad \textit{pour} \quad x > 1,\ y > 1.$$

Démonstration de $\mathrm{C}_{12} \to \mathrm{C}_{12.2}$. L'inégalité $(*)$ entraîne tout de suite l'inégalité $\varrho(x) \leqslant \pi(x)$ (sans avoir recours à l'hypothèse H).

Supposons maintenant que $\varrho(x) \leqslant \pi(x)$ pour x naturels > 1 et soient x et y deux nombres naturels > 1. Sans diminuer la généralité du raisonnement nous pouvons supposer que $1 < x \leqslant y$. Comme $\varrho(x) \leqslant \pi(x)$, on a, d'après C_{12}, $\overline{\varrho}(x) \leqslant \pi(x)$, donc d'après le lemme 1, pour tout y, $\min\big(y, \pi(x + y) - \pi(x)\big) \leqslant \pi(x)$. Or, $y \geqslant x \geqslant \pi(x + y) - y$, donc $\pi(x + y) - \pi(y) \leqslant \pi(x)$, c'est-à-dire $\pi(x + y) \leqslant \pi(x) + \pi(y)$. □

Il est intéressant qu'on ne puisse démontrer par le calcul ni la fausseté de l'hypothèse H ni celle de l'hypothèse de Hardy–Littlewood sur la fonction $\varrho(x)$. (Quant à cette dernière, si l'inégalité $\varrho(x) \geqslant 2$ avait lieu pour un x quelconque, on aurait $\varliminf\limits_{k \to \infty} (p_{k+1} - p_k) < \infty$). Il est cependant possible qu'on puisse trouver des nombres x et y plus grands que 1 pour lesquels $\pi(x + y) > \pi(x) + \pi(y)$, ce qui prouverait que l'hypothèse H et l'hypothèse de Hardy–Littlewood sur la fonction $\varrho(x)$ ne peuvent pas être simultanément vraies.

Hypothèse H_1 de W. Sierpiński. *Si pour un nombre naturel $n > 1$ les nombres $1, 2, 3, \ldots, n^2$ sont rangés successivement en n lignes, n nombres dans chaque ligne, alors chaque ligne contient au moins un nombre premier.*

La proposition que la deuxième ligne contient au moins un nombre premier équivaut évidemment au théorème de Tchebycheff que pour n naturels > 1 il existe entre n et $2n$ au moins un nombre premier.

La proposition que pour $n \geqslant 9$ chacune des 9 premières lignes contient au moins un nombre premier peut sans peine être déduite du théorème de R. Breusch [1] d'après lequel pour $x \geqslant 48$ il y a entre x et $\frac{9}{8}x$ au moins un nombre premier. Ensuite il est facile de déduire du théorème d'Hadamard–de la Vallée Poussin sur les nombres premiers que pour tout k et $n \geqslant n_0(k)$ chacune des k premières lignes contient au moins un nombre premier.

On a ici $\underline{\lim}_{k\to\infty} n_0(k) = +\infty$ et le problème se pose si le plus grand nombre n pour lequel il n'existe aucun nombre premier entre $(k-1)n$ et kn tend vers $+\infty$ avec k.

Par la méthode de Brun on pourrait démontrer (voir G. Ricci [13]), que chacune des lignes de notre carré contient un nombre dont le nombre des diviseurs premiers est limité par une constante universelle.

Consequence. *Entre deux carrés consécutifs il existe au moins deux nombres premiers distincts.*

En effet, pour démontrer cette implication, il suffit de remarquer que si n est un nombre naturel > 1 les nombres naturels consécutifs $(n-1)^2, (n-1)^2+1, \ldots, n^2$ forment les deux dernières lignes dans notre carré composé des nombres $1, 2, \ldots, n^2$. En observant que dans tout intervalle fermé dont les extrémités sont les cubes de nombres naturels consécutifs, il y a au moins deux carrés distincts, on en déduit tout de suite qu'entre deux cubes de nombres naturels consécutifs il y a au moins deux nombres premiers. Cette proposition n'est pas encore démontrée sans avoir recours à l'hypothèse H_1, mais on a démontré que pour n naturels suffisamment grands il existe entre n^3 et $(n+1)^3$ au moins un nombre premier. (On ne sait pourtant pas si cela est vrai pour tout n naturel).

Remarquons que l'hypothèse H_1 pour les nombre n premiers résulte tout de suite de l'hypothèse suivante énoncée en 1932 par R. Haussner : entre deux multiples consécutifs d'un nombre premier p_i qui sont tous les deux inférieurs à p_{i+1}^2 il existe au moins un nombre premier ([11], p. 192). Pour $n = 7$, par exemple, il résulte de l'hypothèse de R. Haussner que non seulement chacune des 7 lignes de notre carré des nombres $1, 2, \ldots, 49$, mais aussi les 10 lignes suivantes (dont la première contient sept nombres $50, 51, \ldots, 56$ et la dernière les nombres $113, 114, \ldots, 119$) contient chacune au moins un nombre premier. Il est intéressant de remarquer ici que la ligne suivante la 18-ème, formée des nombres $120, 121, \ldots, 126$, ne contient aucun nombre premier.

Hypothèse H_2 de A. Schinzel. *Si pour un nombre naturel $n > 1$ les nombres $1, 2, 3, \ldots, n^2$ sont rangés en n lignes, n nombres dans chaque ligne, alors, si $(k, n) = 1$, la k-ième collonne contient au moins un nombre premier.*

Nous ne savons pas quel sera le sort de nos hypothèses, cependant nous pensons que même si elles seront mises en défaut, cela ne sera pas sans profit pour la théorie des nombres.

Travaux cités

[1] R. Breusch, *Zur Verallgemeinerung des Bertrandschen Postulates, daß zwischen x und 2x stets Primzahlen liegen*. Math. Z. 34 (1932), 505–526.

[2] M. Cantor, *Ueber arithmetische Progressionen von Primzahlen*. Z. Math. Phys. 6 (1861), 340–343.

[3] E. Catalan, *Propositions et questions diverses*. Bull. Soc. Math. France 16 (1888), 128–129.

[4] J. Chernick, *On Fermat's simple theorem*. Bull. Amer. Math. Soc. 45 (1939), 269–274.

[5] L. E. Dickson, *Theorems and tables on the sum of the divisors of a number*. Quart. J. Math. 44 (1913), 264–288.

[6] L. E. Dickson, *History of the Theory of Numbers*. Chelsea, New York 1952.

[7] P. Erdős, *On the normal number of prime factors of* $p-1$ *and some related problems concerning Euler's* ϕ*-function*. Quart. J. Math. Oxford Ser. 6 (1935), 205–213.

[8] W. A. Golubew, *Abzählung von „Vierlingen" von* 2000000 *bis* 3000000 *und von „Fünflingen" von* 0 *bis* 2000000. Anz. Österreich. Akad. Wiss. Math.-Naturwiss. Kl., 1956, 153–157.

[9] —, *Abzählung von „Vierlingen" und „Fünflingen" bis zu* 5000000 *und von „Sechslingen" von* 0 *bis* 14000000. Anz. Österreich. Akad. Wiss. Math.-Naturwiss. Kl., 1957, 82–87.

[10] G. H. Hardy, J. E. Littlewood, *Some problems of 'Partitio numerorum'* III. *On the expression of a number as a sum of primes*. Acta Math. 44 (1923), 1–70.

[11] R. Haussner, *Über die Verteilung von Lücken- und Primzahlen*. J. Reine Angew. Math. 168 (1932), 192.

[12] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, T. 1. Teubner, Leipzig 1909.

[12a] J. Needham, *Science and Civilization in China*, vol. 3. *Mathematics and the Sciences of the Heavens and the Earth*. Cambridge Univ. Press, New York 1959.

[13] G. Ricci, *Su la congettura di Goldbach e la costante di Schnirelmann*. Ann. R. Scuola Norm. Sup. Pisa (2) 6 (1937), 71–116.

[14] R. M. Robinson, *Factors of Fermat numbers*. Math. Tables Aids Comput. 11 (1957), 21–22.

[15] A. Schinzel, *Sur un problème concernant la fonction* $\varphi(n)$. Czechoslovak Math. J. 6 (1956), 164–165; this collection: G3, 875–876.

[16] —, *Sur l'équation* $\varphi(x+k)=\varphi(x)$. Acta Arith. 4 (1958), 181–184.

[17] Ch. Sexton, *Abzählung von „Vierlingen" von* 1000000 *bis* 2000000. Anz. Österreich. Akad. Wiss. Math.-Naturwiss. Kl., 1955, 236–239.

[18] V. Thébault, *Sur les nombres premiers impairs*. C. R. Acad. Sci. Paris 218 (1944), 223–224.

Originally published in
Acta Arithmetica VII (1961), 1–8

Remarks on the paper "Sur certaines hypothèses concernant les nombres premiers"

In the paper [14] mentioned in the title some historical inaccuracies are committed which ought to be corrected, besides some new results strictly connected with the above paper arise, which seem to the writer worthy of mention. This is the aim of the present paper.

To begin with, as kindly pointed out by Professor P. T. Bateman, Hypothesis H coincides for the case of linear polynomials f_i with a conjecture of L. E. Dickson announced in [7]. Therefore, it is easy to see that C_1, C_2, C_7–C_{12} are consequences of Dickson's conjecture.

On the other hand, as Dickson quoted in [8], Vol. I, p. 333, V. Bouniakowsky conjectured ([1]) that if d is the greatest fixed divisor of a given irreducible polynomial $f(x)$ (with integral coefficients, the highest coefficient > 0) then the polynomial $f(x)/d$ represents infinitely many primes. This conjecture of Bouniakowsky implies Hypothesis H for the case $s = 1$ and therefore C_3 and the first part of C_6.

Now we shall deduce Bouniakowsky's conjecture from Hypothesis H. For further use we shall deduce the following stronger proposition.

C_{13}. *Let $F_1(x), F_2(x), \dots, F_s(x), G_1(x), G_2(x), \dots, G_t(x)$ be irreducible integer-valued polynomials of positive degree with the highest coefficient > 0. If there does not exist any integer > 1 dividing the product $F_1(x)F_2(x)\cdots F_s(x)$ for every x and if $G_j(x) \not\equiv F_i(x)$ for all $i \leqslant s$, $j \leqslant t$, then there exist infinitely many positive integers x such that the numbers $F_1(x), F_2(x), \dots, F_s(x)$ are primes and the numbers $G_1(x), G_2(x), \dots, G_t(x)$ are composite.*

Proof of the implication $H \to C_{13}$. Let $F_i = \Phi_i/d_i$, $G_j = \Gamma_j/e_j$, where Φ_i, Γ_i are polynomials with integral coefficients, d_i, e_j are positive integers. Let further $d = d_1 d_2 \cdots d_s$, $e = e_1 e_2 \cdots e_t$, $F = F_1 F_2 \cdots F_s$, $\Phi = \Phi_1 \Phi_2 \cdots \Phi_s$, $d = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$.

Since the polynomial F has no fixed divisor > 1, there exist integers x_i such that

$$F(x_i) \not\equiv 0 \pmod{p_i}.$$

We can assume that the polynomials F_i, G_j ($i \leqslant s$, $j \leqslant t$) are algebraically coprime, because otherwise either $G_j = F_i$ or $G_j(x)$ would be composite for all sufficiently large x. We have then $(F, G_j) = 1$ ($j \leqslant t$) and there exist polynomials $a_j(x)$, $b_j(x)$ with integral

coefficients and an integer $c_j \neq 0$ such that

$$a_j(x)F(x) - b_j(x)G_j(x) = c_j. \tag{1}$$

c Let $c = c_1c_2 \cdots c_t$. Since every non-constant polynomial possesses infinitely many prime divisors, there exist primes $q_j \nmid cde$ such that $q_j \mid G(y_j)$ for some integer y_j. Let $q = q_1q_2 \cdots q_t$.

In virtue of the Chinese Remainder Theorem, there exist integers z satisfying the following system of congruences

$$\begin{aligned} z &\equiv x_i \pmod{p_i^{\alpha_i+1}}, \quad i \leqslant s, \\ z &\equiv y_j \pmod{q_j}, \qquad j \leqslant t, \end{aligned} \tag{2}$$

c let z_0 be any of them. Let us consider polynomials

$$f_i(x) = F_i(dqx + z_0) = \frac{\Phi_i(dqx + z_0)}{d_i}.$$

Since $d_i \mid dq$ and $\Phi_i(z_0)/d_i = F_i(z_0)$ is an integer, polynomials f_i have integral coefficients and the highest coefficient > 0. Besides, they are irreducible. We shall show that $f(x) = f_1(x) \cdots f_s(x)$ has no fixed divisor > 1.

Suppose that prime p is such a divisor. We have by (2), since $p_i^{\alpha_i+1} \nmid d$,

$$f(0) = F(z_0) \equiv F(x_i) \not\equiv 0 \pmod{p_i}, \quad i \leqslant s,$$

and since $q_j \nmid e$,

$$G_j(z_0) \equiv G_j(y_j) \equiv 0 \pmod{q_j}.$$

It follows hence by (1), because $q_j \nmid c$, that

$$f(0) = F(z_0) \not\equiv 0 \pmod{q_j}.$$

Therefore, we must have $(p, dq) = 1$.

On the other hand, by the assumption about F, there exists an integer z_p such that

$$F(z_p) \not\equiv 0 \pmod{p}.$$

Let x_0 be a root of the congruence

$$dqx + z_0 \equiv z_p \pmod{p}.$$

Since $(d, p) = 1$, we have

$$f(x_0) = F(dqx_0 + z_0) = \frac{\Phi(dqx_0 + z_0)}{d} \equiv \frac{\Phi(z_p)}{d} = F(z_p) \not\equiv 0 \pmod{p}.$$

Our supposition about p is therefore false and the polynomials f_i satisfy the conditions of Hypothesis H. Thus, there exist infinitely many integers x such that numbers

c $f_i(x) = F_i(dqx + z_0)$ are primes. Meanwhile for every x

$$G_j(dqx + z_0) = \frac{\Gamma_j(dqx + z_0)}{e_j} \equiv \frac{\Gamma_j(z_0)}{e_j} = G_j(z_0) \equiv 0 \pmod{q_j}$$

then for sufficiently large x numbers $G_j(dqx + z_0)$ are composite. □

Now we shall deduce

C_{14}. *For every $k > 1$ there exist infinitely many numbers m_k such that the equation*

$$\varphi(y) = m_k$$

has exactly k solutions.

Proof of the implication $H \to C_{14}$. Consider first k even, $k = 2l$, and put in H

$$f_i(x) = 2x^{2i-1} + 1 \quad (i = 1, 2, \dots, 2l), \qquad f_{2l+1}(x) = x.$$

The polynomials $f_i(x)$ are irreducible, their highest coefficient is > 0 and since $f_1(-1) f_2(-1) \cdots f_{2l+1}(-1) = -1$, they satisfy the conditions of Hypothesis H. Therefore, there exist infinitely many integers x such that all $f_i(x)$ are primes. Consider for such $x > 5$ the equation

$$\varphi(y) = m_k = 4x^{4l}. \tag{3}$$

Since x is odd, $m_k \not\equiv 0 \pmod 8$, y may have only one of the following forms: p^α, $2p^\alpha$, $4p^\alpha$, $p^\alpha q^\beta$, $2p^\alpha q^\beta$, where p and q are primes > 2. If $\alpha > 1$ we should have $p(p-1) \mid 4x^{4l}$, whence as x is prime > 5, $p = x$ and $x - 1 \mid 4x^{4l}$, which is impossible. Therefore, there is $\alpha = 1$ and similarly, $\beta = 1$.

$y = p$ or $2p$ is impossible since then

$$p = \varphi(y) + 1 = 4x^{4l} + 1 \equiv 0 \pmod 5.$$

$y = 4p$ is also impossible, because then

$$p = \tfrac{1}{2}\varphi(y) + 1 = 2x^{4l} + 1 \equiv 0 \pmod 3.$$

In the case $y = pq$ or $2pq$, we get

$$(p - 1)(q - 1) = 4x^{4l},$$

whence

$$p = 2x^n + 1, \quad q = 2x^{4l-n} + 1.$$

Since for n even $2x^n + 1 \equiv 0 \pmod 3$, there remains the only possibility

$$y = (2x^{2i-1} + 1)(2x^{4l-2i+1} + 1) = f_i(x) f_{2l-i+1}(x) \tag{4}$$

or

$$y = 2 f_i(x) f_{2l-i+1}(x) \quad (i = 1, 2, \dots, l).$$

Since the numbers $f_i(x)$ are primes, the $2l$ values y given by formulae (4) satisfy (3), which completes the proof for even k.

Consider now odd k, $k = 2l + 3$ ($l = 0, 1, \dots$) and put in C_{13}

$$F_i(x) = 2x^{6i-3} + 1, \quad F_{l+i}(x) = 6x^{6i-1} + 1 \quad (i = 1, 2, \dots, l),$$

$$F_{2l+1}(x) = x, \quad F_{2l+2}(x) = 6x^{6l+2} + 1,$$

$$G_j(x) = 2x^{6j-5} + 1, \quad G_{l+j}(x) = 2x^{6j-1} \quad (j = 1, 2, \dots, l),$$

$$G_{2l+1}(x) = 2x^{6l+1} + 1, \quad G_{2l+2}(x) = 12x^{6l+2} + 1.$$

The polynomials F_i are irreducible and satisfy other conditions of C_{13}, because in view of

$$F(-1) = -5^l \cdot 7, \quad F(1) = 3^l \cdot 7^{l+1}, \quad F(2) \not\equiv 0 \pmod 7,$$

$F(x)$ has no fixed divisor > 1. Since $G_j \neq F_i$ $(i, j \leqslant 2l+2)$, there exist by C_{13} infinitely many integers x such that numbers $F_i(x)$ are primes and numbers $G_j(x)$ are composite $(i, j \leqslant 2l+2)$. Observe that the numbers $2x^n+1$ are composite for all positive $n \leqslant 6l+2$, $n \neq 6i-3$, because for n even $2x^n + 1 \equiv 0 \pmod 3$. Consider for x of the above kind the equation

$$\varphi(y) = m_k = 12x^{6l+2}. \tag{5}$$

c By much the same arguments as in case of (3), we infer that y may have only one of the following forms: $p, 2p, 4p, pq, 2pq$, where p, q are primes > 2 (the possibility $y = 9q$ or $18q$ fails, because we should have then $q = \frac{1}{6}\varphi(y) + 1 = 2x^{6l+2} + 1$).

It cannot be $y = p$ or $2p$, because then $p = \varphi(y) + 1 = 12x^{6l+2} + 1$, which is composite.

The case $y = 4p$ gives

$$p = \tfrac{1}{2}\varphi(y) + 1 = 6x^{6l+2} + 1 = F_{2l+2}(x). \tag{6}$$

In the case $y = pq$ or $2pq$, we get

$$(p-1)(q-1) = 12x^{6l+2},$$

whence $p - 1 = 2x^n$, $q - 1 = 6x^{6l+2-n}$ $(0 \leqslant n \leqslant 6l+2)$ or p, q change places.

The numbers $2x^n + 1$ being composite $(0 < n \leqslant 6l+2, n \neq 6i-3)$, the only two possibilities remain

1° $y = 3(6x^{6l+2} + 1) = 3F_{2l+2}(x)$ or $y = 6F_{2l+2}(x)$;

2° $y = (2x^{6i-3} + 1)(6x^{6(l-i)+5} + 1) = F_i(x)F_{2l-i+1}(x)$
or $y = 2F_i(x)F_{2l-i+1}(x)$ $(i = 1, 2, \ldots, l)$.

The numbers $F_i(x)$ being primes, the $2l+2$ values y given above satisfy (5), which together with (6) gives exactly $2l+3$ solutions of (5). □

C_{15}. *For every $k \geqslant 1$, there exist infinitely many numbers n_k such that the equation*

$$\sigma(y) = n_k$$

has exactly k solutions.

Proof of the implication $H \to C_{15}$. Put in H,

c $f_i(x) = 2(2x+1)^{2i} - 1$ $(i = 1, 2, \ldots, 2k)$, $f_{2k+1}(x) = x$, $f_{2k+2}(x) = 2x + 1$.

The polynomials $f_i(x)$ are irreducible, their highest coefficient is > 0 and since $f_1(-1)f_2(-1)\cdots f_{2k+2}(-1) = 1$, they satisfy the conditions of Hypothesis H. Therefore, there exist infinitely many integers x such that all $f_i(x)$ are primes and since c $(2^x - 1)/(2x+1)^{4k+2}$ tends to infinity, infinitely many of them satisfy the inequality $2^x - 1 > 4(2x+1)^{4k+2}$.

Consider for any such x the equation

$$\sigma(y) = n_k = 4(2x+1)^{4k+2}.$$

Suppose that $p^\alpha \mid y$, $p^{\alpha+1} \nmid y$, where p is prime, $\alpha > 1$. It follows from the above equation that $\dfrac{p^{\alpha+1}-1}{p-1} \Big| 4(2x+1)^{4k+2}$.

In virtue of the theorem of Zsigmondy (cf. [8], Vol. I, p. 195), $(p^{\alpha+1}-1)/(p-1)$ has at least one prime factor of the form $(\alpha+1)l+1$. Since $\alpha+1 > 2$ and the numbers x and $2x+1$ are primes, we clearly must have

$$(\alpha+1)l+1 = 2x+1, \quad \alpha+1 = x,$$

hence

$$2^x - 1 \leqslant \frac{p^x-1}{p-1} \leqslant 4(2x+1)^{4k+2},$$

which contradicts the assumption about x. The obtained contradiction proves that y is square-free, and since $n_k \not\equiv 0 \pmod 3$, $n_k \not\equiv 0 \pmod 8$, y may have only one of the forms p, pq where p and q are primes, $2 < p < q$.

$y = p$ is impossible since then

$$p = \sigma(y) - 1 = 4(2x+1)^{4k+2} - 1 \equiv 0 \pmod 3.$$

In the case $y = pq$ we get

$$(p+1)(q+1) = 4(2x+1)^{4k+2},$$

whence

$$p = 2(2x+1)^n - 1, \quad q = 2(2x+1)^{4k+2-n} - 1, \quad 0 < n < 2k+1.$$

Since $x \equiv -1 \pmod 3$, $2(2x+1)^n - 1 \equiv 0 \pmod 3$ for all odd n, there remains the only possibility

$$y = \big(2(2x+1)^{2i} - 1\big)\big(2(2x+1)^{4k+2-2i} - 1\big) = f_i(x) f_{2k+1-i}(x) \quad (i = 1, 2, \ldots, k).$$

Since the numbers $f_i(x)$ are primes, the k values of y given above satisfy the equation $\sigma(y) = n_k$, which completes the proof. □

P. Erdős proved without any conjecture that if there exists one m_k such that the equation $\varphi(y) = m_k$ has exactly k solutions, then there exist infinitely many such m_k ([9], Theorem 4), and the analogous theorem for the equation $\sigma(y) = n_k$ (l.c., p. 12). For $k = 1$ the well known conjecture of Carmichael states that such a number m_k does not exist and for $k > 1$ W. Sierpiński conjectured that m_k and n_k exist (cf. [9], p. 12). We have just deduced this conjecture from Hypothesis H; by more complicated arguments we could also deduce that for every pair $\langle k, l\rangle$, where $k \neq 1$, $l \geqslant 0$, there exist infinitely many numbers m such that the equation $\varphi(y) = m$ has exactly k solutions and the equation $\sigma(y) = m$ has exactly l solutions.

On page 191 ([1]) paper [14] contains two historical mistakes. The theorem about the difference of arithmetical progression formed by primes, ascribed to V. Thébault, was proved earlier by M. Cantor ([2]). On the other hand, the disproving of the M. Cantor conjecture about progressions formed by consecutive primes, ascribed to the writer, was made much earlier by F. H. Loud (cf. [4]).

Part of the paper [14] concerning functions ϱ, $\overline{\varrho}$ was covered to some extent by the results of H. Smith's paper [16]. It is easy to notice that the function Δn considered by Smith is connected with function $\overline{\varrho}$ by the condition $\overline{\varrho}(\Delta n) = n - 1 < \overline{\varrho}(1 + \Delta n)$ and "k-tuples" considered by him just correspond "nombres k-jumeaux" of [14].

Theorem 1 of [14] follows from the table given for Δn by Smith, his results further imply the following equalities

$$
\begin{aligned}
&\overline{\varrho}(37) = \ldots = \overline{\varrho}(42) = 11, && \overline{\varrho}(43) = \ldots = \overline{\varrho}(48) = 12,\\
&\overline{\varrho}(49) = \overline{\varrho}(50) = 13, && \overline{\varrho}(51) = \ldots = \overline{\varrho}(56) = 14,\\
&\overline{\varrho}(57) = \ldots = \overline{\varrho}(60) = 15, && \overline{\varrho}(61) = \ldots = \overline{\varrho}(66) = 16,\\
&\overline{\varrho}(67) = \ldots = \overline{\varrho}(70) = 17, && \overline{\varrho}(71) = \ldots = \overline{\varrho}(76) = 18,\\
&\overline{\varrho}(77) = \ldots = \overline{\varrho}(80) = 19, && \overline{\varrho}(81) = \ldots = \overline{\varrho}(84) = 20,\\
&\overline{\varrho}(85) = \ldots = \overline{\varrho}(90) = 21, && \overline{\varrho}(91) = \ldots = \overline{\varrho}(94) = 22,\\
&\overline{\varrho}(95) = \ldots = \overline{\varrho}(100) = 23, && \overline{\varrho}(101) = \ldots = \overline{\varrho}(110) = 24,\\
&\overline{\varrho}(111) = \ldots = \overline{\varrho}(114) = 25, && \overline{\varrho}(115) = \overline{\varrho}(116) = 26,
\end{aligned}
\tag{7}
$$

thus, in particular Theorems 2 and 3 of [14].

It dispenses the writer of the duty of publishing mentioned in [14] the laborious proof that $\overline{\varrho}(100) \leqslant 23$.

From formulae (7) it immediately follows that $\overline{\varrho}(x) \leqslant \pi(x)$ for $36 < x \leqslant 116$. Paper [14] contained a proof that $\overline{\varrho}(x) \leqslant \pi(x)$ for $1 < x \leqslant 132$. Owing to Smith's results, one can prove the stronger

Theorem. *$\overline{\varrho}(x) \leqslant \pi(x)$ for $1 < x \leqslant 146$.*

Proof. It is sufficient to prove the above inequality for $132 < x \leqslant 146$. Profiting by Lemma 3 of [14] we get

$$
\begin{aligned}
\overline{\varrho}(140) &\leqslant \overline{\varrho}(114) + \overline{\varrho}(26) = 25 + 7 = 32 = \pi(133),\\
\overline{\varrho}(146) &\leqslant \overline{\varrho}(114) + \overline{\varrho}(32) = 25 + 9 = 34 = \pi(141),
\end{aligned}
$$

which in view of monotonicity of functions $\overline{\varrho}$ and π gives the desired result. □

Analogously, as in [14], we obtain

Corollary. *If $x > 1$, $y > 1$ and if at least one of the numbers x and y is $\leqslant 146$, then*

$$\pi(x + y) \leqslant \pi(x) + \pi(y). \tag{8}$$

([1]) Page 1118 in this collection.

As to inequality (8), it was verified by E. Łukasiak for $1 < x, y < 1223 = p_{201}$.

H. Smith gave also in [16], numerical data concerning k-tuples for $7 \leqslant k \leqslant 15$, $q_k \leqslant 137 \cdot 10^6$. One may remark that there was omitted the 15-tuple formed by primes $17, \ldots, 73$.

As to Hypothesis H_1 of [14], we shall give the following remarks.

L. Skula noticed (written communication) that if H_1 is true, then also the intervals $[n^2+1, n^2+n]$ and $[n^2+n+1, n^2+2n]$ contain primes.

On the other hand Hypothesis H_1 is a simple consequence of the conjectures that for all $x \geqslant 117$ there is a prime between x and $x + \sqrt{x}$ or that for all $x \geqslant 8$ there is a prime between x and $x + \log^2 x$ (cf. H. Cramér [6]). Since these conjectures hold for $x \leqslant 20.3 \cdot 10^6$, as can be verified owing to A. E. Western ([17]) and D. H. Lehmer ([11]) tables, Hypothesis H_1 holds for all $n \leqslant 4500 < 10^3\sqrt{20.3}$.

As to Hypothesis H_2, it was verified by A. Gorzelewski for $n \leqslant 100$.

Finally, it seems interesting to review 17 conjectures concerning primes, written out by R. D. Carmichael from Dickson's book [8]: 13 from Volume I ([3], p. 401) and 4 from Volume II ([5], p. 76). One of these conjectures ([3], 14) is already proved ([13], [15]), 3 are consequences of Hypothesis H ([3], 6, 8, 11), 2 are consequences of Hypothesis H_1 ([3], 12, 13), 4 are various modifications of Goldbach conjecture ([3], 9; [5], 1, 2, 3), 7 are false. Among these latter: 2 are mentioned in [14], Schaffler's and Cantor's conjectures ([3], 7, 10), 3 concerning Mersenne primes M_n ([3], 1, 2, 3) are wrong respectively for $n = 13, 263, 607$, one concerning primitive roots ([3], 15) was recently disproved by A. Mąkowski ([12]) and one ([5], 4) we shall disprove now.

It states that every prime $18n \pm 1$, or else its triple, is expressible in the form $x^3 - 3xy^2 \pm y^3$. If it is true, then for all z, the form $x^3 - 3xy^2 \pm y^3$ represents at least $c\,\pi'(\frac{1}{3}z)$ numbers $\leqslant z$ ($\pi'(x)$ is the number of primes $18n \pm 1 \leqslant x$). But this is incompatible with Siegel's theorem (cf. [10], p. 139).

References

[1] V. Bouniakowsky, *Nouveaux théorèmes relatifs à la distinction des nombres premiers et à la décomposition des entiers en facteurs*. Mém. Acad. Sci. St. Pétersbourg (6), Sci. Math. Phys. 6 (1857), 305–329.

[2] M. Cantor, *Ueber arithmetische Progressionen von Primzahlen*. Z. Math. Phys. 6 (1861), 340–343.

[3] R. D. Carmichael, *Review of volume I "History of the Theory of Numbers"*. Amer. Math. Monthly 26 (1919), 396–403.

[4] —, *Note on prime numbers*. Amer. Math. Monthly 27 (1920), 71.

[5] R. D. Carmichael, *Review of volume II "History of the Theory of Numbers"*. Amer. Math. Monthly 28 (1921), 72–78.

[6] H. Cramér, *On the order of magnitude of the difference between consecutive prime numbers*. Acta Arith. 2 (1936), 23–46.

[7] L. E. Dickson, *A new extension of Dirichlet's theorem on prime numbers*. Messenger of Math. (2) 33 (1904), 155–161.

[8] —, *History of the Theory of Numbers*. Chelsea, New York 1952.

[9] P. Erdős, *Some remarks on Euler's φ-function*. Acta Arith. 4 (1958), 10–19.

[10] P. Erdős, K. Mahler, *On the number of integers which can be represented by a binary form*. J. London Math. Soc. 13 (1938), 134–139.

[11] D. H. Lehmer, *Tables concerning the distribution of primes up to* 37 *millions*. Mimeographed, 1957. Deposited in the UMT file.

[12] A. Mąkowski, *On a conjecture of Murphy*. An. Soc. Paran. Mat. (2) 3 (1960), 13.

[13] S. S. Pillai, *On some empirical theorem of Scherk*. J. Indian Math. Soc. 17 (1927–28), 164–171.

[14] A. Schinzel, W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*. Acta Arith. 4 (1958), 185–208; *Erratum*, ibid. 5 (1959), 259; this collection: J1, 1113–1133.

[15] W. Sierpiński, *Sur une propriété des nombres premiers*. Bull. Soc. Roy. Sci. Liège 21 (1952), 537–539.

[16] H. F. Smith, *On a generalization of the prime pair problem*. Math. Tables Aids Comput. 11 (1957), 249–254.

[17] A. E. Western, *Note on the magnitude of the difference between successive primes*. J. London Math. Soc. 9 (1934), 276–278.

Andrzej Schinzel
Selecta

Originally published in
Mathematics of Computation 17 (1963), 445–447

A remark on a paper of Bateman and Horn

Let $f_1, f_2, \ldots, f_k$ be distinct irreducible polynomials with integral coefficients and the highest coefficient positive, such that $f(x) = f_1(x) f_2(x) \cdots f_k(x)$ has no fixed divisor > 1. Denote by $P(N)$ the number of positive integers $x \leqslant N$ such that all numbers $f_1(x), f_2(x), \ldots, f_k(x)$ are primes.

P. T. Bateman and R. A. Horn [1] recently gave the heuristic asymptotic formula for $P(N)$:

$$P(N) \sim \frac{N}{\log^k N} (h_1 h_2 \cdots h_k)^{-1} \prod_p \Big(1 - \frac{\omega(p)}{p}\Big)\Big(1 - \frac{1}{p}\Big)^{-k}, \tag{1}$$

where h_i is the degree of f_i and $\omega(p)$ is the number of solutions of the congruence $f(x) \equiv 0 \pmod{p}$.

Formula (1) contains as particular cases six conjectures from a well known paper of Hardy and Littlewood [3] called by the latter Conjectures B, D, E, F, K, P, as well as their conditional theorem X1. This is evident except for Conjecture D, which concerns the number of solutions of the equation

$$ap - bp' = k \quad (a > 0,\ b > 0,\ (a, b) = 1) \tag{2}$$

in primes p, p' with $p \leqslant n$. In order to apply formula (1) here one should put $f_1(x) = u_0 + bx$, $f_2(x) = v_0 + ax$, $N = \dfrac{n - u_0}{b}$, where u_0, v_0 are fixed integers such that $au_0 - bv_0 = k$.

Conjectures denoted by Hardy and Littlewood by J, M, N are of distinctly different character; besides the first has been proved by S. Chowla [2] and Yu. V. Linnik [4]. Conjecture A (a strong form of Goldbach's Conjecture) is a particular case of C, Conjectures H and I are particular cases of G. It remains therefore to consider Conjectures C, G, L, which are, according to Hardy and Littlewood, conjugate to Conjectures D, F, K, respectively. We quote them below for the convenience of a reader, with slight changes in the notation (e.g. p, p' denote primes).

Conjecture C. *If a, b are fixed positive integers and $(a, b) = 1$ and $P(k)$ is the number of representations of k in the form*

$$k = ap + bp'$$

then

$$P(k) = o\left(\frac{k}{(\log k)^2}\right)$$

unless $(k, a) = 1$, $(k, b) = 1$, *and one and only one of* k, a, b *is even. But if these conditions are satisfied then*

$$P(k) \sim \frac{2C_2}{ab}\,\frac{k}{(\log k)^2}\prod\left(\frac{\mathfrak{p}-1}{\mathfrak{p}-2}\right),$$

where

$$C_2 = \prod_{p=3}^{\infty}\left(1 - \frac{1}{(p-1)^2}\right)$$

and the first product extends over all odd primes $\mathfrak{p}$ *which divide* k, a *or* b.

Conjecture G. *Suppose that* a *and* b *are integers, and* $a > 0$, *and let* $P(n)$ *be the number of representations of* n *in the form* $am^2 + bm + p$. *Then if* n, a, b *have a common factor, or if* n *and* $a + b$ *are both even, or if* $b^2 + 4an$ *is a square then*

$$P(n) = o\left(\frac{\sqrt{n}}{\log n}\right).$$

In all other cases

$$P(n) \sim \frac{\epsilon}{\sqrt{a}}\,\frac{\sqrt{n}}{\log n}\prod\left(\frac{\mathfrak{p}}{\mathfrak{p}-1}\right)\prod_{\substack{p\geqslant 3\\ p\nmid a}}\left(1 - \frac{1}{p-1}\left(\frac{b^2+4an}{p}\right)\right),$$

where $\mathfrak{p}$ *is a common odd prime divisor of* a *and* b, *and* ϵ *is* 1 *if* $a + b$ *is odd and* 2 *if* $a + b$ *is even.*

Conjecture L. *Every large number* n *is either a cube or the sum of a prime and a (positive) cube. The number* $P(n)$ *of representations is given asymptotically by*

$$P(n) \sim \frac{n^{1/3}}{\log n}\prod_{p}\left(1 - \frac{1}{p-1}\,(n)_p\right),$$

where $p \equiv 1 \pmod 3$, $p \nmid n$, *and* $(n)_p$ *is equal to* 1 *or to* $-\frac{1}{2}$ *according as* n *is or is not a cubic residue of* p.

A comparison of formula (1) with the above formulas of paper [3] suggests forcibly the following conjecture.

Let polynomials $f_1, f_2, \ldots, f_k$ $(k \geqslant 0)$, $f = f_1 f_2 \cdots f_k$ satisfy the same conditions as above. Let g be a polynomial with integral coefficients and the highest coefficient positive. Let n be a positive integer such that $n - g(x)$ is irreducible and $f(x)(n - g(x))$ has no fixed divisor > 1. Denote by $N(n) = N$ the number of positive integers x such that $n - g(x) > 0$ and by $P(n)$ the number of x's such that all numbers $f_1(x), f_2(x), \ldots, f_k(x)$ and $n - g(x)$

are primes. Then for large n we have

$$P(n) \sim \frac{N}{\log^{k+1} N} (h_0 h_1 \cdots h_k)^{-1} \prod_p \Big(1 - \frac{\omega(p)}{p}\Big)\Big(1 - \frac{1}{p}\Big)^{-k-1}, \tag{3}$$

where h_0 is the degree of g and $\omega(p)$ is the number of solutions of the congruence $f(x)(n - g(x)) \equiv 0 \pmod p$.

Conjectures C, G, L and therefore also A, H, I are particular cases of formula (3). To see this, as far as C is concerned, one should put

$$f_1(x) = bx + l, \quad g(x) = ax, \quad n = \frac{k - al}{b},$$

where l is an integer such that $al \equiv k \pmod b$, $-b < l \leqslant 0$. Conjecture A has been extensively verified ([3], p. 37). I have had no possibility to verify by computation the agreement of formula (3) with reality in other cases. For such comparisons one should replace $N(\log N)^{-k-1}$ by $\int_2^N (\log u)^{-k-1}\, du$, as is pointed out in [3].

I conclude with expressing my thanks to the referee for his valuable suggestions.

References

[1] P. T. Bateman, R. A. Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers*. Math. Comp. 16 (1962), 363–367.

[2] S. Chowla, *The representation of a number as a sum of four squares and a prime*. Acta Arith. 1 (1935), 115–122.

[3] G. H. Hardy, J. E. Littlewood, *Some problems of 'Partitio numerorum'* III. *On the expression of a number as a sum of primes*. Acta Math. 44 (1923), 1–70.

[4] Yu. V. Linnik, *An asymptotic formula in an additive problem of Hardy–Littlewood*. Izv. Akad. Nauk SSSR Ser. Mat. 24 (1960), 629–706 (Russian).

Originally published in
Acta Arithmetica XIII (1967), 228–236

On two theorems of Gelfond and some of their applications

5. The greatest prime factor of a quadratic or cubic polynomial

One of the consequences of Theorem 10 merits to be stated as a separate theorem ($q(n)$ denotes the greatest prime factor of n).

Theorem 11. *If $\nu = 2$ or 3, A and E are non-zero integers then*

$$\varlimsup_{x=\infty} \frac{q(Ax^\nu - E)}{\log\log x} \geqslant \begin{cases} \frac{4}{7} & \text{if } \nu = 2 \text{ and } AE \text{ is not a perfect square} \\ & \quad \text{or } \nu = 3 \text{ and } A^2E \text{ is a perfect cube,} \\ \frac{2}{7} & \text{if } \nu = 2 \text{ and } AE \text{ is a perfect square,} \\ \frac{3}{14} & \text{if } \nu = 3 \text{ and } A^2E \text{ is not a perfect cube.} \end{cases}$$

Proof. Since $Ax^\nu - E = A^{1-\nu}\big((Ax)^\nu - A^{\nu-1}E\big)$ we apply Theorem 10 case (iv) ([1]) with $\varepsilon P_1 = A^{\nu-1}E$ and obtain the assertion except in the case A^2E being a perfect cube. In this case we set $A^2E = F^3$ and since

$$q(y^3 - A^2E) \geqslant q(y^2 + Fy + F^2) = q\big((2y+F)^2 + 3F^2\big)$$

we apply Theorem 10 case (iv) with $\varepsilon P_1 = -3F^2$. □

Corollary 7. *If $f(x)$ is any quadratic polynomial without a double root, then*

$$\varlimsup_{x=\infty} \frac{q\big(f(x)\big)}{\log\log x} \geqslant \begin{cases} \frac{4}{7} & \text{if } f \text{ is irreducible,} \\ \frac{2}{7} & \text{if } f \text{ is reducible.} \end{cases}$$

Proof is obtained by reducing $f(x)$ to the canonical form. □

Theorem 11 can be improved if $\nu = 2$, $E \mid 4$ or $\nu = 3$, $E \mid 3$. The latter case was done by Nagell [18], cf. [19]. We prove

([1]) See Acta Arith. 13 (1967), p. 221.

Theorem 12. *If $A \neq 0$ is an integer and $E \mid 4$, then*

$$\varliminf_{x=\infty} \frac{q(Ax^2 - E)}{\log\log x} \geqslant \begin{cases} 4 & \text{if } AE \text{ is not a perfect square,} \\ 2 & \text{if } AE \text{ is a perfect square.} \end{cases}$$

Proof. It is sufficient to prove the theorem for $A > 0$ square-free and $(A, E) = 1$. Let $Ax^2 - E = d > AE^2$ and let d_0 be the square-free kernel of d. Clearly

$$d_o \leqslant \prod_{p \mid d} p. \tag{164}$$

The primes p dividing d have the property that AE is mod p a quadratic residue. If AE is not a perfect square the density of primes with that property is $1/2$, hence by the prime number theorem

$$\prod_{p \mid d} p \leqslant \exp\{\delta_1 q(d) + o(q(d))\} \tag{165}$$

where

$$\delta_1 = \begin{cases} 1 & \text{if } AE \text{ is a perfect square,} \\ \frac{1}{2} & \text{otherwise.} \end{cases}$$

On the other hand,

$$d = d_0 d_1^2, \quad (Ax)^2 - Ad_0 d_1^2 = AE.$$

Since $(Ax)^2 - AE > (AE)^2$, Ad_0 is not a perfect square. Moreover if $E = \pm 4$ we may assume $Ad_0 d_1$ odd.

Let U_1, V_1 be the least positive solution of the equation

$$U^2 - Ad_0 V^2 = AE \tag{166}$$

and consider the recurrence

$$u_n = \Omega\omega^n + \Omega'\omega'^n, \tag{167}$$

where

$$\omega = |AE|^{-1}\big(U_1 + V_1\sqrt{Ad_0}\big)^v, \quad \omega' = |AE|^{-1}\big(U_1 - V_1\sqrt{Ad_0}\big)^v,$$
$$\Omega = \big(U_1 + V_1\sqrt{Ad_0}\big)/2, \quad \Omega' = \big(-U_1 + V_1\sqrt{Ad_0}\big)/2$$

and $v = 1$ if $AE = 1$ or 4 or $E = -d_0$ or $-4d_0$, $v = 2$ otherwise. It follows from Theorems 11 and 13 of [19] that if $E \mid 2$, ω is the least greater than 1 totally positive unit of the ring generated by $\sqrt{Ad_0}$ and if $E = 4$, ω is the least such unit of the field R generated by $\sqrt{Ad_0}$. Hence ω does not exceed the sixth power of the fundamental unit of R. Applying (157) ([2]) with $D = Ad_0$ or $4Ad_0$ we get from (164) and (165)

$$\log\omega = O\big(\sqrt{d_0}\log d_0\big) \leqslant \exp\big\{\tfrac{1}{2}\delta_1 q(d) + o(q(d))\big\}.$$

([2]) See *ibid.*, p. 225.

It follows further from the quoted theorems of [19] that all the positive integers V satisfying (166) for a suitable integer U, are contained in $\{u_n\}$. Thus in particular

$$|d_1| = u_n.$$

Since $\omega/\omega' = (-\Omega/\Omega')^v$, it follows from Theorem 8 ([3]) that

$$q(d) \geqslant q(d_1) \geqslant nv \quad \text{or} \quad 24 \geqslant nv.$$

Now, by (167)

$$\log u_n = n \log \omega + O(1)$$

and we get

$$\log d = \log d_0 + 2 \log |d_1| \leqslant \delta_1 q(d) + o\big(q(d)\big) + q(d) \exp\big\{\tfrac{1}{2}\delta_1 q(d) + o\big(q(d)\big)\big\} = \exp\big\{\tfrac{1}{2}\delta_1 q(d) + o\big(q(d)\big)\big\}.$$

Solving this inequality with respect to $q(d)$ we obtain the theorem. □

The theorems which follow go in the direction opposite to that of Theorems 11 and 12.

Theorem 13. *If v, A, E are non-zero integers, $v \geqslant 2$, then*

$$\overline{\lim_{x=\infty}} \frac{\log q(Ax^v - E) \log\log\log x}{\log |Ax^v - E|} \leqslant \begin{cases} e^{-\gamma} \dfrac{2v}{\varphi(2v)} & \text{if } AE < -1, \\ 2e^{-\gamma} & \text{if } AE = -1, \\ e^{-\gamma} & \text{if } AE = 1, \\ e^{-\gamma} \dfrac{v}{\varphi(v)} & \text{if } AE > 1, \end{cases}$$

where γ is Euler's constant and φ is Euler's function.

Proof. We assume without loss of generality $A > 0$, set for positive integers n:

$$x_n = \begin{cases} A^{-1}(A^{v-1}E)^{2n} & \text{if } AE < -1, \\ 2^{2n-1} & \text{if } AE = -1, \\ 2^n & \text{if } AE = 1, \\ A^{-1}(A^{v-1}E)^n & \text{if } AE > 1 \end{cases}$$

and find

$$\log\log\log x_n = \log\log n + o(1).$$

On the other hand,

$$Ax_n^v - E = E \times \begin{cases} (A^{v-1}E)^{2vn-1} - 1 & \text{if } AE < -1, \\ (-2^v)^{2n-1} - 1 & \text{if } AE = -1, \\ 2^{vn} - 1 & \text{if } AE = 1, \\ (A^{v-1}E)^{vn-1} - 1 & \text{if } AE > 1. \end{cases}$$

([3]) See *ibid.*, p. 217.

Denoting by X_δ the δ-th cyclotomic polynomial and by $d(\delta)$ the number of divisors of δ we have for any positive integers $g > 1$ and m

$$g^m - 1 = \prod_{\delta \mid m} X_\delta(g)$$

and by [3], p. 178

$$q(g^m - 1) \leqslant \max_{\delta \mid m} |X_\delta(g)| \leqslant \max_{\delta \mid m} g^{\varphi(\delta)+d(\delta)} \leqslant g^{\varphi(m)+d(m)}.$$

It follows that

$$\varlimsup_{n=\infty} \frac{\log q(Ax_n^\nu - E) \log\log\log x_n}{\log |Ax_n^\nu - E|} \leqslant \varlimsup_{n=\infty} \frac{\big(\varphi(kn-1) + d(kn-1)\big) \log\log n}{kn},$$

where $k = 2\nu$ if $AE < -1$, $k = 2$ if $AE = -1$, $k = 1$ if $AE = 1$ and $k = \nu$ if $AE > 1$.

Now, a standard argument (cf. [14], §59) shows that

$$\varlimsup_{n=\infty} \frac{\varphi(kn-1) \log\log n}{kn} = e^{-\gamma} \frac{k}{\varphi(k)}.$$

Since

$$\varlimsup_{n=\infty} \frac{d(kn-1) \log\log n}{kn} = 0$$

the theorem follows. □

If $\nu = 2$, $E \mid 4$, Theorem 13 can be improved to the following

Theorem 14. *If A, E, r, s are integers, $Ar \neq 0$, $E \mid 4$, then*

$$\varlimsup_{x=\infty} \frac{\log q\big(A(rx+s)^2 - E\big) \log\log\log x}{\log |A(rx+s)^2 - E|} < \infty.$$

Proof. We assume without loss of generality that $A > 0$, $r > 0$, $s > |E|$ and set

$$\alpha = \frac{s\sqrt{A} + \sqrt{As^2 - E}}{\sqrt{|E|}}, \quad \beta = \frac{s\sqrt{A} - \sqrt{As^2 - E}}{\sqrt{|E|}}.$$

Then $\sqrt{A(As^2 - E)}$ generates a real quadratic field and α^2 is a unit of this field. Let l be the least positive exponent such that

$$\alpha^{2l} \equiv 1 \bmod r(\alpha + \beta).$$

We set for positive integers n

$$x_n = \frac{\sqrt{|E|}}{2r\sqrt{A}} \left(\alpha^{2ln+1} + \beta^{2ln+1}\right) - \frac{s}{r}.$$

We have $\dfrac{\sqrt{|E|}}{2r\sqrt{A}} (\alpha+\beta) = \dfrac{s}{r}$ and the quotient $\dfrac{\alpha^{2ln+1} + \beta^{2ln+1}}{\alpha + \beta}$ can be expressed rationally in terms of $(\alpha + \beta)^2 = 4As^2/E$ and $\alpha\beta = \pm 1$, thus x_n is rational. Moreover by the choice

of l

$$\frac{\alpha^{2ln+1}+\beta^{2ln+1}}{\alpha+\beta} \equiv 1 \bmod r,$$

thus x_n is an integer. Since $\alpha > |\beta|$, we have

$$\log\log\log x_n = \log\log n + o(1),$$
$$\log\big(A(rx_n+s)^2 - E\big) = 2ln\log\alpha + O(1).$$

On the other hand,

$$A(rx_n+s)^2 - E = \frac{|E|}{4}\big(\alpha^{2ln+1}-\beta^{2ln+1}\big)^2 = (As^2-E)\prod_{\substack{\delta\,|\,2ln+1\\ \delta>1}} X_\delta^2(\alpha,\beta),$$

where

$$X_\delta(\alpha,\beta) = \beta^{\varphi(\delta)}X_\delta\Big(\frac{\alpha}{\beta}\Big).$$

Since $X_\delta(\alpha,\beta)$ can be for $\delta > 2$ expressed rationally in terms of $(\alpha+\beta)^2$ and $\alpha\beta$, all factors on the right hand side are rational integers and we get

$$q\big(A(rx_n+s)^2-E\big) \leqslant \max\Big\{q(As^2-E), \max_{\substack{\delta\,|\,2ln+1\\ \delta>1}} |X_\delta(\alpha,\beta)|\Big\}$$
$$\leqslant \max\big\{q(As^2-E), \alpha^{\varphi(2ln+1)+d(2ln+1)}\big\}.$$

It follows like in the proof of Theorem 13:

$$\varlimsup_{n=\infty} \frac{\log q\big(A(rx_n+s)^2-E\big)\log\log\log x_n}{\log\big(A(rx_n+s)^2-E\big)}$$
$$\leqslant \varlimsup_{n=\infty} \frac{\big(\varphi(2ln+1)+d(2ln+1)\big)\log\log n}{2ln} = e^{-\gamma}\,\frac{2l}{\varphi(2l)} < \infty. \quad \square$$

Theorems 13 and 14 do not say anything about $q\big(f(x)\big)$ for a general quadratic polynomial $f(x)$. A much weaker but more general result is the following

Theorem 15. *If $f(x)$ is any polynomial of degree $\nu > 1$ with integer coefficients, then*

$$\varlimsup_{x=\infty} \frac{\log q\big(f(x)\big)}{\log|f(x)|} \leqslant \begin{cases} \frac{1}{2}P(4) & \text{for } \nu = 2,\\ \frac{1}{2}P(6) & \text{for } \nu = 3,\\ P(\nu) & \text{for } \nu > 3,\end{cases}$$

where

$$P(\nu) = \prod_{i=1}^{\infty}\Big(1-\frac{1}{u_i}\Big), \quad u_1 = \nu-1,\ u_{i+1} = u_i^2 - 2.$$

In the proof of this theorem we denote by S the set of all polynomials with integer coefficients and the leading coefficient positive.

Lemma 10. *If $F(x) \in S$ is a polynomial of degree d there exists a polynomial $H(x) \in S$ of degree $d-1$ such that $F\big(H(x)\big)$ has a factor $G(x) \in S$ of degree $d^2 - 2d$.*

Proof. Let $F(x) = a_0x^d + \ldots + a_d$. We set for any integer k

$$G_k(x) = x^d F\left(\frac{1}{x} - \frac{a_1}{(d-1)a_0} - k\right) = a_0\left(1 - \frac{a-1}{(d-1)a_0}\, x - x H_k(x)\right),$$

where $H_k(x)$ is a polynomial, $H_k(0) = dk$ and if $F\left(-\dfrac{a_1}{(d-1)a_0} - k\right) \neq 0$, $H_k(x)$ is of degree $d-1$ with the leading coefficient

$$-a_0^{-1} F\left(-\frac{a_1}{(d-1)a_0} - k\right).$$

Clearly

$$F\big(H_k(x) - k\big) \equiv F\left(-\frac{G_k(x)}{a_0x} + \frac{1}{x} - \frac{a_1}{(d-1)a_0} - k\right) \equiv F\left(\frac{1}{x} - \frac{a_1}{(d-1)a_0} - k\right) \equiv 0 \bmod G_k(x). \tag{168}$$

We choose k such that

$$(-1)^d F\left(-\frac{a_1}{(d-1)a_0} - k\right) > 0$$

and set

$$H(x) = H_k\big((-1)^{d-1}(d-1)^2 a_0^2 x\big) - k.$$

It is easy to verify that $H(x) \in S$. On the other hand, in view of (168), $F\big(H(x)\big)$ is divisible by $G_k\big((-1)^{d-1}(d-1)^2 a_0^2 x\big)$. The complementary factor of $F\big(H(x)\big)$ is of degree $d^2 - 2d$ and its suitable multiple belonging to S can be taken as $G(x)$. □

Lemma 11. *If $f(x)$ satisfies the assumptions of Theorem* 15*, then for any positive integer n there exists a polynomial $h_n(x) \in S$ of degree $u_1u_2 \cdots u_n$ such that $f\big(h_n(x)\big)$ has a factor $g_n(x) \in S$ of degree $u_{n+1} + 1$.*

Proof by induction with respect to n. For $n = 1$ the assertion follows from Lemma 10 on setting there $F = \pm f$. Assume that $f\big(h_n(x)\big)$ has a factor $g_n(x) \in S$ of degree $u_{n+1} + 1$. Applying Lemma 10 with $F = g_n(x)$ we find a polynomial $H(x) \in S$ of degree u_{n+1} such that $g_n\big(H(x)\big)$ has a factor $g_{n+1}(x) \in S$ of degree

$$(u_{n+1} + 1)^2 - 2(u_{n+1} + 1) = u_{n+1}^2 - 1 = u_{n+2} + 1.$$

Clearly $g_{n+1}(x)$ is also a factor of $F\big(h_n(H(x))\big)$ and we complete the proof by taking $h_{n+1}(x) = h_n\big(H(x)\big)$. □

Proof of Theorem 15. It follows easily by induction that

$$u_{n+1} + 1 = \nu \prod_{i=1}^{n} (u_i - 1) \quad (n = 1, 2, \dots).$$

Hence $\dfrac{u_{n+1}+1}{\nu u_1 u_2 \cdots u_n}$ tends to $P(\nu)$ decreasing monotonically. Since $P(\nu) \geqslant P(4) = 0.55\ldots > \frac{1}{2}$ for $\nu > 3$, we have

$$u_{n+1} + 1 > \nu u_1 \cdots u_n - u_{n+1} - 1.$$

By Gauss's Lemma we can assume that in Lemma 11 both polynomials $g_n(x)$ and $f\big(h_n(x)\big)/g_n(x)$ have integer coefficients. It follows that for $\nu > 3$

$$\begin{aligned}
\varlimsup_{x=\infty} \frac{\log q\big(f(x)\big)}{\log |f(x)|} &\leqslant \varlimsup_{x=\infty} \frac{\log q\big(f(h_n(x))\big)}{\log |f\big(h_n(x)\big)|} \\
&\leqslant \varlimsup_{x=\infty} \frac{\log \max\big\{|g_n(x)|, |f\big(h_n(x)\big)/g_n(x)|\big\}}{\log |f\big(h_n(x)\big)|} \\
&= \frac{\max\{u_{n+1}+1, \nu u_1 \cdots u_n - u_{n+1} - 1\}}{\nu u_1 u_2 \cdots u_n} = \frac{u_{n+1}+1}{\nu u_1 u_2 \cdots u_n}.
\end{aligned}$$

Since the last inequality holds for every n, we get

$$\varlimsup_{x=\infty} \frac{\log q\big(f(x)\big)}{\log |f(x)|} \leqslant P(\nu) \quad (\nu > 3).$$

It remains to consider $\nu = 2$ and $\nu = 3$. If $\nu = 2$ we have

$$f\big(x + f(x) + f\big(x + f(x)\big)\big) = f(x)\big(1 + f'(x) + \tfrac{1}{2} f''(x) f(x)\big) f_1(x),$$

where $f_1(x)$ is a quartic polynomial with integer coefficients. It follows by the already proved part of the theorem

$$\varlimsup_{x=\infty} \frac{\log q\big(f_1(x)\big)}{\log |f_1(x)|} \leqslant P(4)$$

and

$$\begin{aligned}
\varlimsup_{x=\infty} \frac{\log q\big(f(x)\big)}{\log |f(x)|} &\leqslant \varlimsup_{x=\infty} \frac{\log \max\big\{|f(x)|, \big|1 + f'(x) + \tfrac{1}{2} f''(x) f(x)\big|, q\big(f_1(x)\big)\big\}}{\log \big|f\big(x + f(x) + f\big(x + f(x)\big)\big)\big|} \\
&\leqslant \max\big\{\tfrac{1}{4}, \tfrac{1}{4}, \tfrac{1}{2} P(4)\big\} = \tfrac{1}{2} P(4).
\end{aligned}$$

If $\nu = 3$ there exists by Lemma 10 a polynomial $H(x) \in S$ such that

$$f\big(H(x)\big) = G_1(x) G_2(x),$$

where G_1, G_2 are cubic polynomials with integer coefficients. Applying again Lemma 10 with $F(x) = \pm G_1(x)$ we find a polynomial $H_1(x) \in S$ such that $G_1\big(H_1(x)\big) = G_3(x) G_4(x)$, where G_3, G_4 are cubic polynomials with integer coefficients. It follows by

the already proved part of the theorem

$$\overline{\lim_{x=\infty}} \frac{\log q\big(G_2(H_1(x))\big)}{\log |G_2\big(H_1(x)\big)|} \leqslant P(6)$$

and since $f\big(H\big(H_1(x)\big)\big) = G_2\big(H_1(x)\big)G_3(x)G_4(x)$

$$\overline{\lim_{x=\infty}} \frac{\log q\big(f(x)\big)}{\log |f(x)|} \leqslant \overline{\lim_{x=\infty}} \frac{\log \max\big\{q\big(G_2(H_1(x))\big), |G_3(x)|, |G_4(x)|\big\}}{\log\big|f\big(H(H_1(x))\big)\big|}$$

$$\leqslant \max\Big\{\tfrac{1}{2}P(6), \tfrac{1}{4}, \tfrac{1}{4}\Big\} = \tfrac{1}{2}P(6).$$

This completes the proof. □

The above proof of Theorem 15 suggests the following

Problem. *Does there exist for any polynomial $f(x) \in S$ and any $\varepsilon > 0$ a polynomial $h(x) \in S$ of degree d such that the degree of each irreducible factor of $f\big(h(x)\big)$ is less than εd ?*

I do not know the answer to this problem even for $f(x) = 4x^2 + 4x + 9$, $\varepsilon = \frac{1}{2}$.

Addendum*

In the formulation of Theorem 15 occurs the product $\prod_{i=1}^{\infty}\Big(1 - \frac{1}{u_i}\Big)$, $u_1 \geqslant 3$, $u_{i+1} = u_i^2 - 2$. I have overlooked that already in 1929 A. Ostrowski [A] gave the value of this product as $\dfrac{\sqrt{u_1^2 - 4}}{u_1 + 1}$ (l.c., formula (7.10)). Hence Theorem 15 takes the form:

Theorem 15′. *If $f(x)$ is any polynomial of degree $\nu > 1$ with integer coefficients then*

$$\overline{\lim_{x=\infty}} \frac{\log q\big(f(x)\big)}{\log x} \leqslant \begin{cases} \frac{1}{4}\sqrt{5} & \text{for } \nu = 2, \\ \frac{1}{4}\sqrt{21} & \text{for } \nu = 3, \\ \sqrt{(\nu-1)^2 - 4} & \text{for } \nu > 3. \end{cases}$$

References

[3] G. D. Birkhoff, H. S. Vandiver, *On the integral divisors of $a^n - b^n$*. Ann. of Math. (2), 5 (1904), 173–180.

[14] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*. Reprint, Chelsea, New York 1953.

* *Acta Arith.* 56 (1990), 181

[18] T. Nagell, *Über den größten Primteiler gewisser Polynome dritten Grades*. Math. Ann. 114 (1937), 284–292.

[19] —, *Contributions to the theory of a category of Diophantine equations of the second degree with two unknowns*. Nova Acta Soc. Sci. Upsal. (4) 16 (1955), no. 2.

[A] A. Ostrowski, *Ueber einige Verallgemeinerungen des Eulerschen Produktes*. Verh. Naturforsch. Ges. Basel 40 (1929), 153–214; Collected Mathematical Papers, vol. 3, Birkhäuser, Basel 1984, 352–413.

Originally published in
Acta Arithmetica XXXVIII (1980), 285–322

On the relation between two conjectures on polynomials

1.

The aim of this paper is to establish a relation between the conjecture H on simultaneous representation of primes by several irreducible polynomials (see [12] and [5]) and a conjecture on Diophantine equations with parameters that we shall denote by C. Both conjectures involve the notion of the fixed divisor of a polynomial, i.e. the greatest common divisor of all values the polynomial takes for integral values of the arguments. The conjectures run as follows.

H. *Let* $f_1(x), \dots, f_k(x)$ *be irreducible polynomials with integral coefficients and the leading coefficients positive such that* $\prod_{j=1}^{k} f_j(x)$ *has the fixed divisor* 1. *Then there exist infinitely many positive integers* x *such that all numbers* $f_j(x)$ *are primes.*

C. *Let* $F(x, y) \in \mathbb{Z}[x, y]$ *be a form such that*

(1) $F(x, y) = F_1(ax + by, cx + dy)$ *for any* $F_1 \in \mathbb{Z}[x, y]$ *and any* $a, b, c, d \in \mathbb{Z}$ *implies* $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = \pm 1.$

If $f(t_1, \dots, t_r) \in \mathbb{Z}[t_1, \dots, t_r]$ *has the fixed divisor equal to its content and the equation*

$$F(x, y) = f(t_1, \dots, t_r) \tag{2}$$

is soluble in integers x, y *for all integral vectors* $[t_1, \dots, t_r]$ *then there exist polynomials* $X, Y \in \mathbb{Z}[t_1, \dots, t_r]$ *such that identically*

$$F\big(X(t_1, \dots, t_r), Y(t_1, \dots, t_r)\big) = f(t_1, \dots, t_r). \tag{3}$$

A conjecture similar to C has been proposed by Chowla [3]. He has made no assumption (1) but required F and f to be irreducible and have the fixed divisor 1. The following example shows that this is not enough:

$$F(x, y) = x^2 + 3y^2, \quad f(t_1, t_2) = t_1^2 + t_1 t_2 + t_2^2.$$

In this example the set of values of $F(x, y)$ and of $f(t_1, t_2)$ is the same, but F and f are not equivalent by unimodular transformation, which answers in the negative a question of

Chowla (ibid., p. 73) repeated in [9]. The condition imposed in C on the fixed divisor of f is essential, as the following example shows

$$F(x, y) = 2x^2y^3, \quad f(t) = t^3(t+1)^4.$$

Here the solutions of the equations (2) are given by

$$x = 2(t+1)^2,\ y = \tfrac{1}{2}t \quad \text{if} \quad t \equiv 0 \bmod 2,$$
$$x = \tfrac{1}{4}(t+1)^2,\ y = 2t \quad \text{if} \quad t \equiv 1 \bmod 2,$$

but there are no integer-valued polynomials $X(t)$, $Y(t)$ satisfying (3). Another example with F primitive is given at the end of Section 2.

One special case of C corresponding to $F = x^2 + y^2$ has been proved in [3] and [4]. Chowla has also indicated how his conjecture for $F(x, y)$ quadratic should follow from the special case $k = 1$ of H. We shall extend these results in the following two theorems.

Theorem 1. C *holds if* $F(x, y) = x^k y^l$ $(k \geqslant 1, l \geqslant 1)$ *or if* F *is quadratic and equivalent* (*properly or improperly*) *to every form in its genus. For such and for no other quadratic* F C *extends to all polynomials* $f \in \mathbb{Z}[t_1, \ldots, t_r]$.

Theorem 2. H *implies* C *if* F *is a quadratic form or a reducible cubic form.*

We shall see (Corollary to Lemma 3) that C implies the following, less precise but more general assertion.

D. *Let* $F(x, y) \in \mathbb{Z}[x, y]$ *be any form and* $f \in \mathbb{Z}[t_1, \ldots, t_r]$ *any polynomial. If the equation* (2) *is soluble in integers* x, y *for all integral vectors* $[t_1, \ldots, t_r]$ *then there exist polynomials* $X, Y \in \mathbb{Q}[t_1, \ldots, t_r]$ *satisfying* (3).

D has been proved for $F = x^n$ and any r in [7] and [11] also for any irreducible quadratic F and $r = 1$ in [4], $r > 1$ in [14]; for reducible quadratic F it follows easily. We shall show

Theorem 3. H *implies* D *if* F *factorizes into two relatively prime factors in an imaginary quadratic field.*

In virtue of Theorem 3 H implies D for $F = x^n + y^n$. By a modification of the proof of that theorem in this special case we shall show yet

Theorem 4. H *implies* C *if* $F(x, y) = x^n + y^n$ $(n \geqslant 2)$. *For* $n = 2$ *and for no other* n *in question* C *extends to all polynomials* $f \in \mathbb{Z}[t_1, \ldots, t_r]$.

At the cost of considerable technical complications indicated briefly later one can extend Theorem 2 to all forms F splitting completely over a cyclic field except those with all zeros conjugate and real. The quantitative version of H formulated by Bateman and Horn [1] (see also [5]) implies C in the exceptional case at least for $r = 1$. Similarly Theorem 3 can be extended to all forms F that factorize into two distinct complex conjugate factors over an imaginary cyclic field.

2.

In the sequel we shall use the vector notation and write $\boldsymbol{t}$ instead of $[t_1, \ldots, t_r]$, $\boldsymbol{t}'$ instead of $[t_2, \ldots, t_r]$, $\|\boldsymbol{t}\|$ for $\max_{1 \leqslant i \leqslant r} |t_i|$. We shall denote the content of a polynomial f by $C(f)$, its total degree by $|f|$ and call a form F satisfying (1) primary. The letters $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ denote the set of positive integers, the ring of integers and the rational field, respectively. For a fixed field $\boldsymbol{K}$ N denotes the norm from $\boldsymbol{K}$ to $\mathbb{Q}$ or from $\boldsymbol{K}(\boldsymbol{t})$ to $\mathbb{Q}(\boldsymbol{t})$. The content of a polynomial over $\boldsymbol{K}$ is an ideal of $\boldsymbol{K}$ but if $\boldsymbol{K} = \mathbb{Q}$ it is often identified with the positive generator of this ideal. All considered forms are defined over $\mathbb{Z}$ unless stated to the contrary.

Lemma 1. *Let $P \in \mathbb{Z}[t]$, p be a prime dividing neither the leading coefficient nor the discriminant of P. If $t_0 \in \mathbb{Z}$, $P(t_0) \equiv 0 \bmod p$ then either $P(t_0) \not\equiv 0 \bmod p^2$ or $P(t_0 + p) \not\equiv 0 \bmod p^2$.*

Proof. Denoting the leading coefficient of P by a, the discriminant of P by D and its derivative by P' we have

$$P(t)U(t) + P'(t)V(t) = aD,$$

where $U, V \in \mathbb{Z}[t]$. Setting $t = t_0$ we infer from $P(t_0) \equiv 0 \bmod p$, $aD \not\equiv 0 \bmod p$ that $P'(t_0) \not\equiv 0 \bmod p$. Now from the expansion

$$P(t_0 + p) = P(t_0) + P'(t_0)p + \frac{P''(t_0)}{2} p^2 + \ldots$$

we get $P(t_0 + p) - P(t_0) \not\equiv 0 \bmod p^2$, whence the assertion. □

Lemma 2. *If a quadratic form F is primary then*

$$F = AG(x, y), \quad \textit{where} \quad A \in \mathbb{Z},\ G(x, y) \in \mathbb{Z}[x, y],$$

A is square-free, the discriminant Δ of G is either 1 or fundamental and $\left(\frac{\Delta}{p}\right) = -1$ for every prime factor p of A.

Proof. If G is reducible, $G = (ax + by)(a'x + b'y)$ we have

$$F(x, y) = (Aax + Aby)(a'x + b'y)$$

and by (1)

$$A \begin{vmatrix} a & b \\ a' & b' \end{vmatrix} = \pm 1, \quad A = \pm 1 \quad \text{and} \quad \Delta = \begin{vmatrix} a & b \\ a' & b' \end{vmatrix}^2 = 1.$$

If G is irreducible, let $G = ax^2 + bxy + cy^2$, and let ω_1, ω_2 be a basis of the ideal $\mathfrak{a} = \left(a, \frac{b + \sqrt{\Delta}}{2}\right)$. Then we have for suitable integers a_1, a_2, b_1, b_2

$$a = a_1\omega_1 + a_2\omega_2,$$

$$\frac{b + \sqrt{\Delta}}{2} = b_1\omega_1 + b_2\omega_2.$$

Let $\boldsymbol{K} = \mathbb{Q}(\sqrt{\Delta})$ and let us set

$$F_1(x, y) = Aa^{-1}N(x\omega_1 + y\omega_2).$$

Since $N\mathfrak{a} = |a|$ and $(\omega_1, \omega_2) \equiv 0 \bmod \mathfrak{a}$ we have

$$F_1(x, y) \in \mathbb{Z}[x, y].$$

On the other hand

$$ax + \frac{b + \sqrt{\Delta}}{2}\, y = (a_1x + b_1y)\omega_1 + (a_2x + b_2y)\omega_2,$$

hence

$$F(x, y) = F_1(a_1x + b_1y, a_2x + b_2y)$$

and by (1)

$$\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} = \pm 1.$$

It follows that $\left[a, \dfrac{b + \sqrt{\Delta}}{2}\right]$ is itself a basis for $\mathfrak{a}$ and by a well known result

$$|a| = \frac{1}{\sqrt{|d|}} \operatorname{abs} \begin{vmatrix} a & \dfrac{b + \sqrt{\Delta}}{2} \\ a & \dfrac{b - \sqrt{\Delta}}{2} \end{vmatrix},$$

c where d is the discriminant of $\boldsymbol{K}$. It follows that $\Delta = d$ is a fundamental discriminant. If A is not square-free or for some $p \mid A$ we have $\left(\dfrac{\Delta}{p}\right) = 0$ or 1 then for a suitable prime ideal $\mathfrak{p}$: $N\mathfrak{p} \mid A$.

Let $\mathfrak{p}\mathfrak{a}$ have an integral basis $[\Omega_1, \Omega_2]$ and let us set

$$F_1(x, y) = Aa^{-1}N\mathfrak{p}^{-2}N(x\Omega_1 + y\Omega_2).$$

Since $N(\Omega_1, \Omega_2) = |a|N\mathfrak{p}$ we have

$$F_1(x, y) \in \mathbb{Z}[x, y].$$

On the other hand

$$\omega_i N\mathfrak{p} = c_i\Omega_1 + d_i\Omega_2 \quad (i = 1, 2)$$

for suitable $c_i, d_i \in \mathbb{Z}$, hence

$$(\omega_1x + \omega_2y)N\mathfrak{p} = (c_1x + c_2y)\Omega_1 + (d_1x + d_2y)\Omega_2$$

and we get

$$F(x, y) = F_1(c_1x + c_2y, d_1x + d_2y).$$

Now by (1)

$$\begin{vmatrix} c_1 & c_2 \\ d_1 & d_2 \end{vmatrix} = \pm 1,$$

hence $[\omega_1 N\mathfrak{p}, \omega_2 N\mathfrak{p}]$ is a basis for $\mathfrak{a}\mathfrak{p}$ and $\mathfrak{a}N\mathfrak{p} = \mathfrak{a}\mathfrak{p}$, a contradiction. □

Remark. Similarly one can show that if a primary form $F(x, y)$ is irreducible and $F(\vartheta, 1) = 0$ then $[1, \vartheta]$ can be extended to a basis of the ideal $(1, \vartheta)$.

Proof of Theorem 1. Consider first $F(x, y) = x^k y^l$ and let

$$f(\boldsymbol{t}) = c \prod_{\nu=1}^{n} f_\nu(\boldsymbol{t})^{e_\nu} \tag{4}$$

be the canonical factorization of f into primitive irreducible polynomials with integral coefficients. In view of the condition on the fixed divisor of f for every prime factor p of c there exists a vector $\boldsymbol{t}_p \in \mathbb{Z}^r$ such that

$$\prod_{\nu=1}^{n} f_\nu(\boldsymbol{t}_p)^{e_\nu} \not\equiv 0 \bmod p.$$

It follows from (2) with $\boldsymbol{t} = \boldsymbol{t}_p$ that

$$\operatorname{ord}_p c = k\alpha + l\beta,$$

where $\alpha = \operatorname{ord}_p x$, $\beta = \operatorname{ord}_p y$, and we get

$$c = \pm \xi^k \eta^l, \quad \xi, \eta \in \mathbb{Z}. \tag{5}$$

On the other hand we can assume that $f(\boldsymbol{t})$ depends upon t_1. Let $a_0(\boldsymbol{t}')$, $D(\boldsymbol{t}')$ be the leading coefficient and the discriminant respectively of $\prod_{\nu=1}^{n} f_\nu(\boldsymbol{t})$ with respect to t_1. We have $a_0 D \neq 0$ and there exists a vector $\boldsymbol{t}'_0 \in \mathbb{Z}^{r-1}$ such that

$$a_0(\boldsymbol{t}'_0) D(\boldsymbol{t}'_0) \neq 0.$$

For every $\nu \leqslant n$ there exists a prime p and an integer t_0 such that

$$f_\nu(t_0, \boldsymbol{t}'_0) \equiv 0 \bmod p, \quad c a_0(\boldsymbol{t}'_0) D(\boldsymbol{t}'_0) \not\equiv 0 \bmod p. \tag{6}$$

Put

$$P(t) = \prod_{\nu=1}^{n} f_\nu(t, \boldsymbol{t}'_0). \tag{7}$$

Since $a_0(\boldsymbol{t}'_0) \neq 0$, the discriminant of $P(t)$ equals $D(\boldsymbol{t}'_0)$. Hence by (6) and Lemma 1 there exists a $t_1 \in \mathbb{Z}$ such that

$$P(t_1) \equiv 0 \bmod p, \quad P(t_1) \not\equiv 0 \bmod p^2.$$

We infer from (4), (5) and (6) that

$$(8)\quad f_\nu(t_1, \boldsymbol{t}_0') \equiv 0 \bmod p, \quad f_\nu(t_1, \boldsymbol{t}_0') \not\equiv 0 \bmod p^2, \quad f_\mu(t_1, \boldsymbol{t}_0') \not\equiv 0 \bmod p \ (\mu \neq \nu).$$

It follows from (2) with $\boldsymbol{t} = [t_1, \boldsymbol{t}_0']$, (6) and (8) that

$$(9)\qquad e_\nu = k\alpha_\nu + l\beta_\nu,$$

where $\alpha_\nu = \operatorname{ord}_p x$, $\beta_\nu = \operatorname{ord}_p y$. Take now

$$X_0(\boldsymbol{t}) = \xi \prod_{\nu=1}^{n} f_\nu(\boldsymbol{t})^{\alpha_\nu}, \quad Y_0(\boldsymbol{t}) = \eta \prod_{\nu=1}^{n} f_\nu(\boldsymbol{t})^{\beta_\nu}.$$

It follows from (5) and (9) that

$$X_0(\boldsymbol{t})^k Y_0(\boldsymbol{t})^l = \pm f(\boldsymbol{t}).$$

If the sign on the right hand side is positive we take $X = X_0$, $Y = Y_0$. If the sign is negative and either k or l is odd, we take $X = \pm X_0$, $Y = \pm Y_0$. If the sign is negative and k, l are both even we get a contradiction. Indeed, by (5) $c < 0$, by (9) $e_\nu \equiv 0 \bmod 2$, hence by (4) $f(\boldsymbol{t}) \leqslant 0$. Taking $\boldsymbol{t} \in \mathbb{Z}^r$ such that $f(\boldsymbol{t}) \neq 0$ we get from (2) $x^k y^l < 0$, which is impossible.

Consider now the case of F quadratic. By Lemma 2 F is of the form $AG(x, y)$, where A is square-free, $G(x, y)$ is a primitive form with discriminant Δ, $\left(\frac{\Delta}{p}\right) = -1$ for every prime factor p of A and either $\Delta = 1$ or Δ is fundamental. In the first case $F(x, y)$ is equivalent to xy and for the latter form one can take $X(\boldsymbol{t}) = f(\boldsymbol{t})$, $Y(\boldsymbol{t}) = 1$. In the second case, if $G(\vartheta, 1) = 0$, $\boldsymbol{K} = \mathbb{Q}(\vartheta)$ and $\mathfrak{a}$ is the ideal $(1, \vartheta)$, we have

$$G(x, y) = \frac{N(x - \vartheta y)}{N\mathfrak{a}}.$$

Changing, if necessary, the sign of A we can assume that

$$(10)\qquad F(x, y) = \frac{A}{N\mathfrak{a}} N(x - \vartheta y).$$

The solubility of the equation $N(\omega) = \dfrac{N\mathfrak{a}}{A} f(\boldsymbol{t})$ for all $\boldsymbol{t} \in \mathbb{Z}^r$ implies, by Theorem 1 of [14], the existence of a polynomial $\omega(\boldsymbol{t}) \in \boldsymbol{K}[\boldsymbol{t}]$ such that

$$(11)\qquad N\big(\omega(\boldsymbol{t})\big) = \frac{N\mathfrak{a}}{A} f(\boldsymbol{t}).$$

Let $\mathfrak{b} = C(\omega)$ and let

$$\mathfrak{b}\mathfrak{a}^{-1} = \prod_{i=1}^{j} \mathfrak{p}_i^{a_i} \prod_{i=1}^{j} \mathfrak{p}_i'^{b_i} \prod_{i=1}^{k} q_i^{c_i}$$

be the factorization of $\mathfrak{b}\mathfrak{a}^{-1}$ in prime ideals of $\boldsymbol{K}$. Here $\mathfrak{p}_i$ are distinct pairwise non-conjugate prime ideals of degree 1 in $\boldsymbol{K}$, $\mathfrak{p}_i'$ is conjugate to $\mathfrak{p}_i$ and q_i are prime ideals of degree 2 in $\boldsymbol{K}$. Since $AN(\mathfrak{b}\mathfrak{a}^{-1}) \in \mathbb{Z}$ and A has only prime ideal factors of degree 2 in $\boldsymbol{K}$,

we get

$$a_i + b_i \geqslant 0 \quad (1 \leqslant i \leqslant j),$$
$$2c_i + 1 \geqslant 0 \quad (1 \leqslant i \leqslant k),$$

hence

$$\max\{0, a_i\} + \min\{0, b_i\} \geqslant 0, \quad \max\{0, b_i\} + \min\{0, a_i\} \geqslant 0 \quad (1 \leqslant i \leqslant j), \tag{12}$$
$$c_i \geqslant 0 \quad (1 \leqslant i \leqslant k).$$

Let us consider the ideal

$$\mathfrak{c} = \prod_{i=1}^{j} \mathfrak{p}_i^{\min(0,b_i)-\min(0,a_i)} \mathfrak{p}_i'^{\min(0,a_i)-\min(0,b_i)}.$$

Since F is equivalent to every form in its genus the same is true about G, thus there is only one narrow class in the genus of $\mathfrak{a}$, or there are two such classes represented by $\mathfrak{a}$ and $\mathfrak{a}'$. In any case the principal genus consists only of the principal class and the class of $\mathfrak{a}^2$. Since $\mathfrak{p}_i' \sim \mathfrak{p}_i^{-1}$, $\mathfrak{c}$ belongs to the principal genus and we get $\mathfrak{c} \sim 1$ or $\mathfrak{c} \sim \mathfrak{a}^2$. In the former case let $\mathfrak{c} = (\gamma_1)$ with γ_1 totally positive and consider the polynomial

$$\omega_1(\boldsymbol{t}) = \gamma_1 \omega(\boldsymbol{t}).$$

We have

$$C(\omega_1) = (\gamma_1)C(\omega) = \mathfrak{c}\mathfrak{b} = \mathfrak{a} \prod_{i=1}^{j} \mathfrak{p}_i^{\max\{0,a_i\}+\min\{0,b_i\}} \prod_{i=1}^{j} \mathfrak{p}_i'^{\max\{0,b_i\}+\min\{0,a_i\}} \prod_{i=1}^{k} q_i^{c_i}$$

and by (12) $C(\omega_1) \equiv 0 \bmod \mathfrak{a}$.

It follows that all the coefficients of ω_1 are in $\mathfrak{a}$ and since, by Lemma 2, $[1, \vartheta]$ is a basis of $\mathfrak{a}$, we get

$$\omega_1(\boldsymbol{t}) = X_1(\boldsymbol{t}) - \vartheta Y_1(\boldsymbol{t}),$$

where $X_1, Y_1 \in \mathbb{Z}[\boldsymbol{t}]$. It follows now from (10) and (11) that

$$F\big(X_1(\boldsymbol{t}), Y_1(\boldsymbol{t})\big) = \frac{A}{N\mathfrak{a}} N\omega_1(\boldsymbol{t}) = \frac{A}{N\mathfrak{a}} N\gamma_1 N\omega(\boldsymbol{t}) = N\mathfrak{c} \cdot f(\boldsymbol{t}) = f(\boldsymbol{t}).$$

In the case $\mathfrak{c} \sim \mathfrak{a}^2$ let $\mathfrak{c}\mathfrak{a}^{-1}\mathfrak{a}' = (\gamma_2)$ with γ_2 totally positive and consider the polynomial

$$\omega_2(\boldsymbol{t}) = \gamma_2 \omega(\boldsymbol{t}).$$

We have

$$C(\omega_2) = (\gamma_2)C(\omega) = \mathfrak{c}\mathfrak{a}^{-1}\mathfrak{a}'\mathfrak{b}$$
$$= \mathfrak{a}' \prod_{i=1}^{j} \mathfrak{p}_i^{\max\{0,a_i\}+\min\{0,b_i\}} \prod_{i=1}^{j} \mathfrak{p}_i'^{\max\{0,b_i\}+\min\{0,a_i\}} \prod_{i=1}^{k} q_i^{c_i},$$

and by (12) $C(\omega_2) \equiv 0 \bmod \mathfrak{a}'$.

Since $[1, \vartheta']$ is a basis of $\mathfrak{a}'$, we infer that

$$\omega_2(\boldsymbol{t}) = X_2(\boldsymbol{t}) - \vartheta' Y_2(\boldsymbol{t}),$$

where $X_2, Y_2 \in \mathbb{Z}[\boldsymbol{t}]$. Since $N\gamma_2 = 1$, it follows as before that

$$F\big(X_2(\boldsymbol{t}), Y_2(\boldsymbol{t})\big) = f(\boldsymbol{t}).$$

It remains to prove that if there is a form inequivalent to F in the genus of F, then C does not extend to all polynomials $f \in \mathbb{Z}[\boldsymbol{t}]$. For this purpose let us observe that there exists then in $\boldsymbol{K}$ a class C of ideals such that C^2 is neither the principal class nor the class of $\mathfrak{a}^2$. Choose in C^{-1} a prime ideal $\mathfrak{p}$ of degree 1 with $N\mathfrak{p} = p$. There exists a prime ideal $\mathfrak{q}$ such that $\mathfrak{p}^2\mathfrak{a}\mathfrak{q}$ is principal, equal to, say (α). Consider the polynomials

$$\omega(t) = \alpha\,\frac{t^p - t}{p}, \quad f(t) = \frac{A}{N\mathfrak{a}}\,N\omega(t). \tag{13}$$

We have

$$C(f) = \frac{|A|}{N\mathfrak{a}}\,\frac{|N\alpha|}{p^2} = |A|N\mathfrak{q} \in \mathbb{Z},$$

hence $f(t) \in \mathbb{Z}[t]$. Also, since $\dfrac{t^p - t}{p} \in \mathbb{Z}$ for all $t \in \mathbb{Z}$ we have for all $t \in \mathbb{Z}$: $\omega(t) \in \mathfrak{a}$; $\omega(t) = x - \vartheta y$ and

$$f(t) = F(x, y)$$

for suitable $x, y \in \mathbb{Z}$. On the other hand, suppose that

$$f(t) = F\big(X(t), Y(t)\big), \quad X, Y \in \mathbb{Z}[t] \tag{14}$$

and let x, y be the leading coefficients of X, Y. Then comparing the leading coefficients on both sides of (14) we get by (13)

$$\frac{A}{N\mathfrak{a}}\,\frac{N\alpha}{p^2} = F(x, y) = \frac{A}{N\mathfrak{a}}\,N(x - \vartheta y), \quad N\mathfrak{q} = N\,\frac{(x - \vartheta y)}{\mathfrak{a}}.$$

Since $\mathfrak{q}$ is a prime ideal, $x - \vartheta y \in \mathfrak{a}$, it follows that

$$\frac{(x - \vartheta y)}{\mathfrak{a}} = \mathfrak{q} \quad \text{or} \quad \mathfrak{q}'.$$

Hence $\mathfrak{a}\mathfrak{q} \sim 1$ or $\mathfrak{a}\mathfrak{q}^{-1} \sim 1$. By the choice of $\mathfrak{q}$ this gives $\mathfrak{p}^2 \sim 1$ or $\mathfrak{p}^2\mathfrak{a}^2 \sim 1$ contrary to the choice of $\mathfrak{p}$. □

Remark. The above proof seems to suggest that if F satisfies (1) and for all $\boldsymbol{t} \in \mathbb{Z}^r$ the equation (2) is soluble in integers x, y, then there exist integer-valued polynomials $X(\boldsymbol{t})$, $Y(\boldsymbol{t})$ satisfying (3) identically. The following example shows that this is not the case.

Let $F(x, y) = x^2 + xy + 6y^2$, $\boldsymbol{K} = \mathbb{Q}(\sqrt{-23})$, $\omega = \dfrac{1 + \sqrt{-23}}{2}$,

$$f(t) = N\big((\tfrac{1}{2}\omega^4 - \omega)t^2 + \omega - 8\big).$$

The discriminant of F is -23 hence F is primary. Further, $f(t) \in \mathbb{Z}[t]$ since $(\frac{1}{2}\omega^4 - \omega, \omega - 8) = \dfrac{(2,\omega)}{(2,\omega')}$ with ω' conjugate to ω.

Moreover the equation $F(x, y) = f(t)$ is soluble in integers x, y for all $t \in \mathbb{Z}$. Indeed if $t \equiv 0 \bmod 2$ we can take

$$x + y\omega = \big(\tfrac{1}{2}\omega^4 - \omega\big)t^2 + \omega - 8$$

and if $t \equiv 1 \bmod 2$ we can take

$$x + y\omega = \frac{-3 - \sqrt{-23}}{-3 + \sqrt{-23}}\big[(\tfrac{1}{2}\omega^4 - \omega)t^2 + \omega - 8\big].$$

The number on the right hand side is an integer in $\boldsymbol{K}$ since for $t \equiv 1 \bmod 2$

$$(\tfrac{1}{2}\omega^4 - \omega)t^2 + \omega - 8 \equiv \tfrac{1}{2}\omega^4 - 8 \bmod 4(\omega^4 - 2\omega)$$

and we have in $\boldsymbol{K}$ the factorization into prime ideals

$$(2) = \mathfrak{p}\mathfrak{p}', \quad (\omega) = \mathfrak{p}\mathfrak{q}, \quad \big((-3 + \sqrt{-23})/2\big) = \mathfrak{p}^3.$$

On the other hand, the polynomial $(\frac{1}{2}\omega^4 - \omega)t^2 + \omega - 8$ is irreducible over $\boldsymbol{K}$ since $N\dfrac{8 - \omega}{\frac{1}{2}\omega^4 - \omega} = \dfrac{62}{381}$ is not a square in $\mathbb{Q}$. Therefore, if integer-valued polynomials $X(t)$, $Y(t)$ satisfied

$$F\big(X(t), Y(t)\big) = f(t)$$

identically, we should have either

$$X(t) + Y(t)\omega = \gamma(\tfrac{1}{2}\omega^4 - \omega)t^2 + \gamma(\omega - 8)$$

or

$$X(t) + Y(t)\omega' = \gamma(\tfrac{1}{2}\omega^4 - \omega)t^2 + \gamma(\omega - 8)$$

for some $\gamma \in \boldsymbol{K}$ with $N\gamma = 1$. Taking $t = 0$ and 1 we should get $\gamma(\frac{1}{2}\omega^4 - \omega, \omega - 8)$ integral, hence $(\gamma)\dfrac{\mathfrak{p}}{\mathfrak{p}'}$ integral and $(\gamma) = \dfrac{\mathfrak{p}'}{\mathfrak{p}}$. However the ideal on the right hand side is not principal.

3.

Lemma 3. *Every form $F(x, y)$ with at least two distinct zeros (in $\mathbf{P}^1(\mathbb{C})$) can be represented as $F_1(ax + by, cx + dy)$, where F_1 is primary, $a, b, c, d \in \mathbb{Z}$ and $\begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0$.*

Proof. Suppose that $F(x, y) = G(ax + by, cx + dy)$, $\begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0$. Let F^* be the product of all projectively distinct primitive irreducible factors of F and similarly G^* for G. It

follows that

$$F^* = \pm C^{-1} G^*(ax + by, cx + dy),$$

where $C = C\big(G^*(ax + by, cx + dy)\big) \mid C(F)$. Hence

$$\operatorname{disc} F^* = C^{2-2|F^*|} \operatorname{disc} G^* \cdot \begin{vmatrix} a & b \\ c & d \end{vmatrix}^{|F^*|(|F^*|-1)}$$

and since $\operatorname{disc} F^* \neq 0$, $|F^*| > 1$ the absolute value of $\begin{vmatrix} a & b \\ c & d \end{vmatrix}$ is bounded. Take now a representation of $F(x, y)$ as $G(ax + by, cx + dy)$, where $\operatorname{abs} \begin{vmatrix} a & b \\ c & d \end{vmatrix}$ is maximal. G must be primary, otherwise representing it as $G_1(a_1 x + b_1 y, c_1 x + d_1 y)$ we should obtain a representation of F as $G_1(\alpha x + \beta y, \gamma x + \delta y)$ with

$$\operatorname{abs} \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = \operatorname{abs} \begin{vmatrix} a & b \\ c & d \end{vmatrix} \cdot \operatorname{abs} \begin{vmatrix} a_1 & b_1 \\ c_1 & d_1 \end{vmatrix} > \operatorname{abs} \begin{vmatrix} a & b \\ c & d \end{vmatrix},$$

contrary to the choice of G, unless $\begin{vmatrix} a_1 & b_1 \\ c_1 & d_1 \end{vmatrix} = 0$. In the latter case, however, G and hence also F should have only one zero, contrary to the assumption. □

Corollary. C *implies* D.

Proof. Let $F(x, y) \in \mathbb{Z}[x, y]$ be any form, $f(t) \in \mathbb{Z}[t]$ any polynomial and suppose that for all $\boldsymbol{t} \in \mathbb{Z}^r$ there exist $x, y \in \mathbb{Z}$ satisfying $F(x, y) = f(\boldsymbol{t})$. If $F(x, y) = \text{const}$ or $f(\boldsymbol{t}) = \text{const}$, D is trivial. If $F(x, y)$ has only one zero, we take without loss of generality $F(x, y) = a(bx + cy)^n$, where $b \neq 0$. Applying Theorem 3 of [13] to the equation $au^n = f(\boldsymbol{t})$ we infer the existence of a polynomial $U(\boldsymbol{t}) \in \mathbb{Q}[\boldsymbol{t}]$ such that $aU(\boldsymbol{t})^n = f(\boldsymbol{t})$. It suffices to take $X(\boldsymbol{t}) = b^{-1} U(\boldsymbol{t})$, $Y(\boldsymbol{t}) = 0$.

If $F(x, y)$ has at least two distinct zeros then, by Lemma 3, $F(x, y) = F_1(ax + by, cx + dy)$, where F_1 is primary and $\begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0$. On the other hand there exists a vector $\boldsymbol{t}_0 \in \mathbb{Z}^r$ such that $f(\boldsymbol{t}_0) = e \neq 0$. Consider now the equation

$$F_1(x, y) = f(e\boldsymbol{t} + \boldsymbol{t}_0).$$

The polynomial on the right hand side has both the content and the fixed divisor equal to $|e|$, hence by C there exist polynomials $X_1, Y_1 \in \mathbb{Z}[\boldsymbol{t}]$ such that $F_1\big(X_1(\boldsymbol{t}), Y_1(\boldsymbol{t})\big) = f(e\boldsymbol{t} + \boldsymbol{t}_0)$. Determining $X(\boldsymbol{t})$, $Y(\boldsymbol{t})$ from the equations

$$aX(\boldsymbol{t}) + bY(\boldsymbol{t}) = X_1\Big(\frac{\boldsymbol{t} - \boldsymbol{t}_0}{e}\Big), \quad cX(\boldsymbol{t}) + dY(\boldsymbol{t}) = Y_1\Big(\frac{\boldsymbol{t} - \boldsymbol{t}_0}{e}\Big)$$

we get

$$X(t), Y(t) \in \mathbb{Q}[\boldsymbol{t}], \quad F\big(X(\boldsymbol{t}), Y(\boldsymbol{t})\big) = f(\boldsymbol{t}),$$

thus D holds. □

Lemma 4. H *implies the following.*

Let $f_\nu \in \mathbb{Z}[\boldsymbol{t}]$ $(1 \leqslant \nu \leqslant n)$ *be distinct irreducible polynomials such that their leading forms* $h_\nu(\boldsymbol{t})$ *all assume a positive value for a* $\boldsymbol{t} \in \mathbb{N}^r$ *and that* $\prod_{\nu=1}^{n} f_\nu(\boldsymbol{t})$ *has the fixed divisor* 1. *Then for any* B *there exists a* $\boldsymbol{t} \in \mathbb{N}^r$ *such that* $f_\nu(\boldsymbol{t})$ *are distinct primes* $> B$.

Proof. The condition that f_ν are irreducible and distinct implies that they are prime to each other. Indeed, otherwise two of them would differ by a constant factor $c \neq 1$. The numerator and the denominator of c would divide $\prod_{\nu=1}^{n} f_\nu(\boldsymbol{t})$ for all $\boldsymbol{t}$ hence $c = -1$. But this contradicts the condition on h_ν.

Let us choose an $\boldsymbol{a} \in \mathbb{N}^r$ such that

$$h_\nu(\boldsymbol{a}) > 0 \quad (1 \leqslant \nu \leqslant n) \tag{15}$$

and let

$$a = \big(|h_1| + |h_2| + \ldots + |h_r|\big)! \prod_{\nu=1}^{n} h_\nu(\boldsymbol{a}).$$

Since

$$f(\boldsymbol{t}) = \prod_{\nu=1}^{n} f_\nu(\boldsymbol{t})$$

has the fixed divisor 1 we infer from the Chinese Remainder Theorem the existence of a $\boldsymbol{\tau} \in \mathbb{Z}^r$ such that

$$\big(f(\boldsymbol{\tau}), a\big) = 1. \tag{16}$$

Consider the polynomials $f_\nu(\boldsymbol{a}x + a\boldsymbol{t} + \boldsymbol{\tau})$ $(1 \leqslant \nu \leqslant n)$.

They are irreducible as polynomials in $x, \boldsymbol{t}$ and prime to each other. Consequently the resultant $R_{\mu,\nu}(\boldsymbol{t})$ of $f_\mu(\boldsymbol{a}x + a\boldsymbol{t} + \boldsymbol{\tau})$ and $f_\nu(\boldsymbol{a}x + a\boldsymbol{t} + \boldsymbol{\tau})$ is non-zero for all $\mu < \nu \leqslant n$. By Hilbert's irreducibility theorem there exists a $\boldsymbol{t}_0 \in \mathbb{Z}^r$ such that $f_\nu(\boldsymbol{a}x + a\boldsymbol{t}_0 + \boldsymbol{\tau})$ $(1 \leqslant \nu \leqslant n)$ are all irreducible as polynomials in x and

$$\prod_{\mu<\nu}^{n} R_{\mu,\nu}(\boldsymbol{t}_0) \neq 0. \tag{17}$$

The leading coefficients of $f_\nu(\boldsymbol{a}x + a\boldsymbol{t}_0 + \boldsymbol{\tau})$ are positive by (15). Moreover

$$p(x) = \prod_{\nu=1}^{n} f_\nu(\boldsymbol{a}x + a\boldsymbol{t}_0 + \boldsymbol{\tau})$$

has the fixed divisor 1. Indeed, the $|p|$-th difference

$$\Delta^{|p|} p(0) = a,$$

on the other hand,

$$p(0) = f(a\boldsymbol{t}_0 + \boldsymbol{\tau}) \equiv f(\boldsymbol{\tau}) \bmod a$$

and we get $\big(p(0), \Delta^{|p|}(0)\big) = 1$ by (16).

By H there exist infinitely many $x \in \mathbb{N}$ such that $f_\nu(\boldsymbol{a}x + a\boldsymbol{t}_0 + \boldsymbol{\tau})$ are primes. For sufficiently large x we have $\boldsymbol{a}x + a\boldsymbol{t}_0 + \boldsymbol{\tau} \in \mathbb{N}^r$ and

$$f_\nu(\boldsymbol{a}x + a\boldsymbol{t}_0 + \boldsymbol{\tau}) > |B| + \sum_{\mu<\nu}^{n} |R_{\mu,\nu}(\boldsymbol{t}_0)|. \tag{18}$$

Thus the primes in question are $> B$. They are distinct since the common value of $f_\mu(\boldsymbol{a}x + a\boldsymbol{t}_0 + \boldsymbol{\tau})$ and $f_\nu(\boldsymbol{a}x + a\boldsymbol{t}_0 + \boldsymbol{\tau})$ would have to divide $R_{\mu,\nu}(\boldsymbol{t}_0)$ which is impossible by (17) and (18). □

Lemma 5. *Let $\boldsymbol{K}$ be the rational field or a quadratic field, Δ be the discriminant of $\boldsymbol{K}$ and let $\varphi_\nu \in \boldsymbol{K}[\boldsymbol{t}]$ $(1 \leqslant \nu \leqslant n)$ be polynomials irreducible over $\boldsymbol{K}$ and prime to each other. If*

$$\text{the fixed divisor of } \prod_{\nu=1}^{n} N\varphi_\nu(\boldsymbol{t}) \text{ equals } \prod_{\nu=1}^{n} NC(\varphi_\nu) \tag{19}$$

then for every $M \in \mathbb{N}$, there exists a $\mu \in \mathbb{N}$ prime to M with no prime ideal factor of degree 1 in $\boldsymbol{K}$ and $\boldsymbol{\tau} \in \mathbb{Z}^r$ with the following property. Let

$$\psi_\nu(\boldsymbol{t}) = \varphi_\nu(\mu\boldsymbol{t} + \boldsymbol{\tau}) \quad (1 \leqslant \nu \leqslant n).$$

For any $A \in \mathbb{N}$, $\boldsymbol{t}_1 \in \mathbb{Z}^r$ and $m \in \mathbb{N}$ prime to $\Delta \prod_{\nu=1}^{n} \dfrac{N\psi_\nu(\boldsymbol{t}_1)}{NC(\psi_\nu)}$ H implies the existence of a $\boldsymbol{t}_2 \in \mathbb{N}^r$ such that $\boldsymbol{t}_2 \equiv \boldsymbol{t}_1 \bmod m$, all the ideals $\dfrac{(\psi_\nu(\boldsymbol{t}_2))}{C(\psi_\nu)}$ are prime in $\boldsymbol{K}$, distinct and do not divide A.

Moreover, either $\mu = 1$, $\boldsymbol{\tau} = \boldsymbol{0}$ have the above property (this happens for $\boldsymbol{K} = \mathbb{Q}$) or there is a sequence of pairs $\langle \mu_i, \boldsymbol{\tau}_i \rangle$ with the above property such that $(\mu_i, \mu_h) = 1$ for $i \neq h$, and the number of distinct $\mu_i \leqslant x$ is greater than $cx^{1/n}/\log x$ for a certain $c > 0$ and all $x > x_0$.

Proof. We begin with a remark concerning the fixed divisor that we shall use twice. If $P \in \mathbb{Z}[\boldsymbol{t}]$ has the fixed divisor d then any fixed prime divisor p of $P(m\boldsymbol{t} + \boldsymbol{a})$ divides dm. Indeed, if $p \nmid d$ then there exists a $\boldsymbol{u} \in \mathbb{Z}^r$ such that $P(\boldsymbol{u}) \not\equiv 0 \bmod p$ and if $p \nmid m$ there exists a $\boldsymbol{v} \in \mathbb{Z}^r$ such that $m\boldsymbol{v} + \boldsymbol{a} \equiv \boldsymbol{u} \bmod p$, hence $P(m\boldsymbol{v} + \boldsymbol{a}) \not\equiv 0 \bmod p$.

Now we proceed to the proof of the lemma. Let

$$\begin{aligned} \varphi_\nu(\boldsymbol{t}) &= a_\nu f_\nu(\boldsymbol{t}) \quad (\nu \leqslant k), \\ N\varphi_\nu(\boldsymbol{t}) &= a_\nu f_\nu(\boldsymbol{t}) \quad (k < \nu \leqslant n), \end{aligned}$$

where $f_\nu \in \mathbb{Z}[\boldsymbol{t}]$ are irreducible over $\mathbb{Q}$ and

$$\begin{aligned} (a_\nu) &= C(\varphi_\nu) \quad (\nu \leqslant k), \\ |a_\nu| &= NC(\varphi_\nu) \quad (k < \nu \leqslant n). \end{aligned}$$

(If $\boldsymbol{K} = \mathbb{Q}$ we take $k = 0$.) Let h_ν be the leading form of f_ν. We can choose the signs

of a_ν so that for a suitable $\boldsymbol{t} \in \mathbb{N}^r$: $h_\nu(\boldsymbol{t}) > 0$ for all $\nu \leqslant n$. We have

$$\prod_{\nu=1}^{n} \frac{N\varphi_\nu(\boldsymbol{t})}{NC(\varphi_\nu)} = \pm \prod_{\nu=1}^{k} f_\nu^2(\boldsymbol{t}) \prod_{\nu=k+1}^{n} f_\nu(\boldsymbol{t}) \tag{20}$$

and (19) implies on an application of the Chinese Remainder Theorem that for a suitable $\boldsymbol{\tau}_0 \in \mathbb{Z}^r$

$$\Big(\Delta, \prod_{\nu=1}^{n} f_\nu(\boldsymbol{\tau}_0)\Big) = 1. \tag{21}$$

Let $f_\nu(\boldsymbol{\tau}_0) \equiv \varrho_\nu \bmod \Delta$, $\varrho_\nu > 0$ $(\nu \leqslant k)$. Without loss of generality we may assume that

$$\Big(\frac{\Delta}{\varrho_\nu}\Big) = 1 \quad (1 \leqslant \nu \leqslant j), \qquad \Big(\frac{\Delta}{\varrho_\nu}\Big) = -1 \quad (j < \nu \leqslant k). \tag{22}$$

Since φ_ν are prime to each other

$$(f_\lambda, f_\nu) = 1 \quad \text{unless} \quad \lambda = \nu \text{ or } \lambda > k,\ \nu > k \text{ and } \varphi_\lambda/\varphi_\nu' \in \boldsymbol{K}, \tag{23}$$

where φ_ν' is conjugate to φ_ν over $\mathbb{Q}(\boldsymbol{t})$.

In particular, $f_1, \ldots, f_j$ and $\prod_{\nu=j+1}^{n} f_\nu$ are prime to each other. Let $\boldsymbol{t} = [t, \boldsymbol{t}']$, $a_0(\boldsymbol{t}')$ be the leading coefficient of $\prod_{\nu=1}^{n} f_\nu(\boldsymbol{t})$, $D(\boldsymbol{t}')$ the discriminant of $\prod_{\nu=1}^{j} f_\nu(\boldsymbol{t})$ and $R(\boldsymbol{t}')$ the resultant of $\prod_{\nu=1}^{j} f_\nu(\boldsymbol{t})$, $\prod_{\nu=j+1}^{n} f_\nu(\boldsymbol{t})$ with respect to t. It follows that

$$a_0 DR \neq 0. \tag{24}$$

Since $f_\nu(\boldsymbol{t})$ are irreducible over $\boldsymbol{K}$ for $\nu \leqslant j$ we infer by Hilbert's irreducibility theorem that there exists a $\boldsymbol{\tau}' \in \mathbb{Z}^{r-1}$ such that $f_\nu(t, \boldsymbol{\tau}')$ are irreducible over $\boldsymbol{K}$ for $\nu \leqslant j$ and

$$a_0(\boldsymbol{\tau}')D(\boldsymbol{\tau}')R(\boldsymbol{\tau}') \neq 0. \tag{25}$$

Let $f_\nu(\vartheta_\nu, \boldsymbol{\tau}') = 0$ and $\boldsymbol{K}_\nu = \mathbb{Q}(\vartheta_\nu)$ $(\nu \leqslant j)$. We have $\boldsymbol{K} \not\subset \boldsymbol{K}_\nu$ and by Bauer's theorem there exist for each $\nu \leqslant j$ infinitely many primes with a prime ideal factor of degree 1 in $\boldsymbol{K}_\nu$, but not in $\boldsymbol{K}$. Choose for each $\nu \leqslant j$ a different prime p_ν with the above property and such that

$$p_\nu \nmid Ma_0(\boldsymbol{\tau}')D(\boldsymbol{\tau}')R(\boldsymbol{\tau}'). \tag{26}$$

Since p_ν does not split in $\boldsymbol{K}$ we have

$$\Big(\frac{\Delta}{p_\nu}\Big) = -1 \quad (\nu \leqslant j). \tag{27}$$

On the other hand, since p_ν has a prime ideal factor of degree 1 in $\boldsymbol{K}_\nu$, by Dedekind's theorem, there exists an integer u such that

$$f_\nu(u, \boldsymbol{\tau}') \equiv 0 \bmod p_\nu.$$

By (25) and (26) the discriminant of $\prod_{i=1}^{j} f_i(t, \boldsymbol{\tau}')$ equals $D(\boldsymbol{\tau}') \not\equiv 0 \bmod p_\nu$. Since $a_0(\boldsymbol{\tau}') \not\equiv 0 \bmod p_\nu$ and $\prod_{i=1}^{j} f_i(u, \boldsymbol{\tau}') \equiv 0 \bmod p_\nu$ we infer from Lemma 1 that either

$$\prod_{i=1}^{j} f_i(u, \boldsymbol{\tau}') \not\equiv 0 \bmod p_\nu^2$$

or

$$\prod_{i=1}^{j} f_i(u + p_\nu, \boldsymbol{\tau}') \not\equiv 0 \bmod p_\nu^2.$$

Therefore, there exists an integer τ_ν such that

$$f_\nu(\tau_\nu, \boldsymbol{\tau}') \equiv 0 \bmod p_\nu, \tag{28}$$

$$\prod_{i=1}^{j} f_i(\tau_\nu, \boldsymbol{\tau}') \not\equiv 0 \bmod p_\nu^2. \tag{29}$$

Moreover, since by (25) and (26) the resultant of $\prod_{i=1}^{j} f_i(t, \boldsymbol{\tau}')$ and $\prod_{i=j+1}^{n} f_i(t, \boldsymbol{\tau}')$ is equal to $R(\boldsymbol{\tau}') \not\equiv 0 \bmod p_\nu$, we have

$$\prod_{i=j+1}^{n} f_i(\tau_\nu, \boldsymbol{\tau}') \not\equiv 0 \bmod p_\nu. \tag{30}$$

Let us choose $\tau \equiv \tau_\nu \bmod p_\nu^2$ $(1 \leqslant \nu \leqslant j)$ and set

$$\mu = \prod_{\nu=1}^{j} p_\nu, \quad \boldsymbol{\tau} = [\tau, \boldsymbol{\tau}']. \tag{31}$$

By (28)–(30) we have

$$f_\nu(\boldsymbol{\tau}) \equiv 0 \bmod p_\nu, \tag{32}$$

$$\prod_{i=1}^{n} f_i(\boldsymbol{\tau}) \not\equiv 0 \bmod p_\nu^2. \tag{33}$$

We shall show that

$$\prod_{i=1}^{n} f_i(\mu \boldsymbol{t} + \boldsymbol{\tau}) = P(\mu \boldsymbol{t} + \boldsymbol{\tau})$$

has the fixed divisor d equal to $p_1 p_2 \cdots p_j$. Indeed by (19) and (20) the fixed divisor of $P(\boldsymbol{t})$ equals 1, hence d consists of prime factors of μ. However by (33)

$$d \not\equiv 0 \bmod p_\nu^2 \quad (\nu \leqslant j).$$

On the other hand by (31) and (32)

$$f_\nu(\mu \boldsymbol{t} + \boldsymbol{\tau}) \equiv f_\nu(\boldsymbol{\tau}) \equiv 0 \bmod p_\nu.$$

Thus $d = p_1 p_2 \cdots p_j$, the polynomials

$$\begin{aligned} g_\nu(\boldsymbol{t}) &= p_\nu^{-1} f_\nu(\mu \boldsymbol{t} + \boldsymbol{\tau}) \quad (\nu \leqslant j), \\ g_\nu(\boldsymbol{t}) &= f_\nu(\mu \boldsymbol{t} + \boldsymbol{\tau}) \quad (j < \nu \leqslant n) \end{aligned} \tag{34}$$

have integral coefficients, $\prod_{\nu=1}^{n} g_\nu(\boldsymbol{t})$ has the fixed divisor 1 and *a fortiori* the content 1. Moreover by (23)

$$g_\lambda \neq g_\nu \quad \text{unless} \quad \lambda = \nu \text{ or } \lambda > k,\ \nu > k \text{ and } \varphi_\lambda/\varphi_\nu' \in \boldsymbol{K}. \tag{35}$$

It follows that

$$\begin{aligned} \psi_\nu(\boldsymbol{t}) &= a_\nu p_\nu g_\nu(\boldsymbol{t}) \quad (\nu \leqslant j), \\ \psi_\nu(\boldsymbol{t}) &= a_\nu g_\nu(\boldsymbol{t}) \quad (j < \nu \leqslant k), \end{aligned} \tag{36}$$

$$N\psi_\nu(\boldsymbol{t}) = a_\nu g_\nu(\boldsymbol{t}) \quad (k < \nu \leqslant n), \tag{37}$$

where besides

$$C(\psi_\nu) = (a_\nu p_\nu) \quad (\nu \leqslant j), \qquad C(\psi_\nu) = (a_\nu) \quad (j < \nu \leqslant k), \tag{38}$$

$$NC(\psi_\nu) = |a_\nu| \quad (k < \nu \leqslant n). \tag{39}$$

It follows that

$$\prod_{\nu=1}^{n} \frac{N\psi_\nu(\boldsymbol{t})}{NC(\psi_\nu)} = \pm \prod_{\nu=1}^{k} g_\nu^2(\boldsymbol{t}) \prod_{\nu=k+1}^{n} g_\nu(\boldsymbol{t}).$$

If now for a $\boldsymbol{t}_1 \in \mathbb{Z}^r$ we have

$$\left(m, \Delta \prod_{\nu=1}^{n} \frac{N\psi_\nu(\boldsymbol{t}_1)}{NC(\psi_\nu)}\right) = 1$$

there exists a $\boldsymbol{t}_0 \in \mathbb{Z}^r$ satisfying

$$\boldsymbol{t}_0 \equiv \boldsymbol{t}_1 \bmod m, \quad \mu \boldsymbol{t}_0 + \boldsymbol{\tau} \equiv \boldsymbol{\tau}_0 \bmod \Delta. \tag{40}$$

Since

$$\left(m, \prod_{\nu=1}^{n} g_\nu(\boldsymbol{t}_0)\right) = \left(m, \prod_{\nu=1}^{n} g_\nu(\boldsymbol{t}_1)\right) = 1$$

and by (34) and (21)

$$\left(\Delta, \prod_{\nu=1}^{n} g_\nu(\boldsymbol{t}_0)\right) = \left(\Delta, \prod_{\nu=1}^{n} g_\nu(0)\right) = \left(\Delta, \prod_{\nu=1}^{n} f_\nu(\boldsymbol{\tau}_0)\right) = 1,$$

it follows that

$$\prod_{\nu=1}^{n} g_\nu(\Delta m \boldsymbol{t} + \boldsymbol{t}_0)$$

has the fixed divisor 1. The polynomials $g_\nu(\Delta m\boldsymbol{t}+\boldsymbol{t}_0)$ are irreducible and their leading forms all take a positive value for a suitable $\boldsymbol{t}\in\mathbb{N}^r$ in virtue of the corresponding property of $f_\nu(\boldsymbol{t})$. By Lemma 4 H implies the existence of an $\boldsymbol{x}\in\mathbb{N}^r$ such that $g_\nu(\Delta m\boldsymbol{x}+\boldsymbol{t}_0)$ are primes greater than $|A|$ and

$$g_\lambda(\Delta m\boldsymbol{x}+\boldsymbol{t}_0)\neq g_\nu(\Delta m\boldsymbol{x}+\boldsymbol{t}_0)\quad\text{unless}\quad g_\lambda=g_\nu. \tag{41}$$

Taking $\boldsymbol{t}_2=\Delta m\boldsymbol{x}+\boldsymbol{t}_0$ we get from (40)

$$\boldsymbol{t}_2\equiv\boldsymbol{t}_1 \bmod m,\quad \mu\boldsymbol{t}_2+\boldsymbol{\tau}\equiv\boldsymbol{\tau}_0 \bmod \Delta. \tag{42}$$

Thus by (34)

$$\begin{aligned} p_\nu g_\nu(\boldsymbol{t}_2)=f_\nu(\mu\boldsymbol{t}_2+\boldsymbol{\tau})\equiv f_\nu(\boldsymbol{\tau}_0)\equiv\varrho_\nu \bmod\Delta \quad (\nu\leqslant j),\\ g_\nu(\boldsymbol{t}_2)=f_\nu(\mu\boldsymbol{t}_2+\boldsymbol{\tau})\equiv f_\nu(\boldsymbol{\tau}_0)\equiv\varrho_\nu \bmod\Delta \quad (j<\nu\leqslant k)\end{aligned}$$

and we infer from (22) and (27) that

$$\left(\frac{\Delta}{g_\nu(\boldsymbol{t}_2)}\right)=-1\quad(\nu\leqslant k).$$

Hence, for $\nu\leqslant k$, $g_\nu(\boldsymbol{t}_2)$ are prime in $\boldsymbol{K}$ not dividing A and in virtue of (36) and (38) the same applies to the ideals $\mathfrak{a}_\nu=\dfrac{\big(\psi_\nu(\boldsymbol{t}_2)\big)}{C(\psi_\nu)}$. The remaining ideals $\mathfrak{a}_\nu$ $(k<\nu\leqslant n)$ are prime and do not divide A in virtue of (37) and (39).

Assuming

$$\lambda\neq\nu,\quad \mathfrak{a}_\lambda=\mathfrak{a}_\nu,$$

we get by (35) and (41) for a suitable $\gamma\in\boldsymbol{K}$

$$\lambda>k,\quad \nu>k,\quad \varphi_\lambda=\gamma\varphi'_\nu,\quad \psi_\lambda=\gamma\psi'_\nu,\quad C(\psi_\lambda)=(\gamma)C(\psi'_\nu),$$
$$\frac{\big(\psi_\nu(\boldsymbol{t}_2)\big)}{C(\psi_\nu)}=\frac{\big(\psi'_\nu(\boldsymbol{t}_2)\big)}{C(\psi'_\nu)},$$

thus the ideal $\mathfrak{a}_\nu$ is ambiguous.

By Dedekind's theorem $\mathfrak{a}_\nu\mid\Delta$, hence by (37) and (39)

$$g_\nu(\boldsymbol{t}_2)\mid\Delta.$$

However by (34) and (42)

$$g_\nu(\boldsymbol{t}_2)=f_\nu(\mu\boldsymbol{t}_2+\boldsymbol{\tau})\equiv f_\nu(\boldsymbol{\tau}_0) \bmod\Delta$$

and we get a contradiction with (21). The contradiction shows that the ideals $\mathfrak{a}_\nu$ are distinct and the proof of the first part of the lemma is complete.

To prove the second part we note that if $j=0$ then (31) gives $\mu=1$. The value of $\boldsymbol{\tau}$ is then irrelevant and can be taken $\boldsymbol{0}$. Therefore assume that $j>0$ and that we have already defined $\langle\mu_1,\boldsymbol{\tau}_1\rangle,\dots,\langle\mu_{i-1},\boldsymbol{\tau}_{i-1}\rangle$ $(i\geqslant 1)$, each μ_i with j prime factors. Then we replace in the above proof M by $M\mu_1\cdots\mu_{i-1}$ and define $\mu_i,\boldsymbol{\tau}_i$ by (31). It is clear that the sequence thus obtained satisfies $(\mu_i,\mu_h)=1$ for $i\neq h$. Denote by $P(\boldsymbol{K}_\nu)$ the set of primes with a prime ideal factor of degree 1 in $\boldsymbol{K}_\nu$. By Bauer's theorem $P(\boldsymbol{K}_\nu)\setminus P(\boldsymbol{K})$

has a positive density, say, δ_ν. Computing μ_i from (31) we take p_ν to be the least element of $P(\boldsymbol{K}_\nu) \setminus P(\boldsymbol{K})$ different from $\omega + j(i-1) + \nu - 1$ given primes, where ω is the number of prime factors of $Ma_0(\boldsymbol{\tau}')D(\boldsymbol{\tau}')R(\boldsymbol{\tau}')$. Hence for $i > i_0$ we have $p_\nu \leqslant 2\delta_\nu^{-1} ji \log ji$ and

$$\mu_i = \prod_{\nu=1}^{j} p_\nu \leqslant (c^{-1} ji \log ji)^j, \quad c = \tfrac{1}{2} \prod_{\nu=1}^{j} \delta_\nu^{1/j}.$$

Since the number of solutions of the inequality

$$(c^{-1} ji \log ji)^j \leqslant x$$

in positive integers i is for x large enough at least $\dfrac{cx^{1/j}}{\log x - 1}$, the number of distinct $\mu_i \leqslant x$ is at least

$$\frac{cx^{1/j}}{\log x - 1} - i_0 > \frac{cx^{1/n}}{\log x} \quad (x > x_0)$$

which completes the proof. □

Remark. The lemma extends to all cyclic fields.

Lemma 6. *Let $\boldsymbol{K}$ be any field, $\overline{\boldsymbol{K}}$ an algebraic closure of $\boldsymbol{K}$, $f \in \boldsymbol{K}[\boldsymbol{t}]$ a non-zero polynomial. If a form $F \in \boldsymbol{K}[x, y]$ has at least three distinct zeros in $\mathbf{P}^1(\overline{\boldsymbol{K}})$ then there exist no more than $|F|^3 3^{|f|}$ pairs $\langle X(\boldsymbol{t}), Y(\boldsymbol{t})\rangle$ such that $X, Y \in \boldsymbol{K}[\boldsymbol{t}]$, X, Y linearly independent over $\boldsymbol{K}$ and*

$$F\big(X(\boldsymbol{t}), Y(\boldsymbol{t})\big) = f(\boldsymbol{t}). \tag{43}$$

Proof. Without loss of generality we may assume that $\boldsymbol{K}$ is algebraically closed. By a linear transformation we can transform F to the form

$$F(x, y) = x^k y^l G(x, y), \quad k \geqslant 1,\ l \geqslant 1, \quad \big(G(x, y), xy\big) = 1.$$

Let us assign two solutions $\langle X_1, Y_1\rangle$ and $\langle X_2, Y_2\rangle$ of (43) to the same class if $X_2 = \xi X_1$, $Y_2 = \eta Y_1$ for some $\xi, \eta \in \boldsymbol{K} \setminus \{0\}$. The number of classes does not exceed the number of pairs of monic polynomials $x, y \in \boldsymbol{K}[\boldsymbol{t}]$ such that

$$xy \mid f(\boldsymbol{t}),$$

which is clearly bounded by $3^{|f|}$. The number of polynomials in one class can be estimated as follows.

If

$$F(\xi X_1, \eta Y_1) = F(X_1, Y_1)$$

then

$$F\Big(\xi \frac{X_1}{Y_1}, \eta\Big) = F\Big(\frac{X_1}{Y_1}, 1\Big)$$

and since X_1/Y_1 takes in $\boldsymbol{K}$ infinitely many values we have identically

$$F(\xi u, \eta) = F(u, 1).$$

Hence

$$\xi^k \eta^l G(\xi u, \eta) = G(u, 1)$$

and the comparison of the leading coefficients and of the constant terms on both sides gives

$$\xi^k \eta^l \xi^{|G|} = 1, \quad \xi^k \eta^l \eta^{|G|} = 1.$$

It follows that

$$\xi^{|G|} = \eta^{|G|}, \quad \xi^{|G|(k+l+|G|)} = 1, \quad \xi^{|G||F|} = 1.$$

Thus there are $|G|\,|F|$ possibilities for ξ and for each ξ at most $|G|$ possibilities for η, which gives at most $|F|\,|G|^2 \leqslant |F|^3$ possibilities for $\langle \xi, \eta \rangle$. The lemma follows. □

Lemma 7. *If $F(x, y) \in \mathbb{Z}[x, y]$ is a non-singular cubic form, then for every integer $a \neq 0$ the number of solutions of the equation $F(x, y) = az^3$ in integers x, y, z such that $(x, y, z) = 1$ and $1 \leqslant z \leqslant Z$ is $O\big((\log Z)^b\big)$, where b is a constant depending on F and a.*

Proof. It is enough to estimate the number of solutions with $|x| \leqslant |y|$. Assume that

$$F(x, y) = az^3, \quad 1 \leqslant z \leqslant Z \quad \text{and} \quad |x| \leqslant |y|. \tag{44}$$

If $F(1, 0) = 0$ we have $|F(x, y)| \geqslant |y|$ hence $h = \max\big(|x|, |y|, |z|\big) \ll Z^3$, where the constant in the symbol $\ll$ depends on a, later also on F. If $F(1, 0) \neq 0$ let

$$F(x, y) = a_0 \prod_{l=1}^{3} (x - \xi_l y), \tag{45}$$

where ξ_1 is the real zero of F nearest to x/y. Since $F(x, y) \neq 0$ we have by Thue's theorem

$$|x - \xi_1 y| \gg |y|^{-3/2}.$$

On the other hand $|x - \xi_2 y|\,|x - \xi_3 y| \gg y^2$. Hence by (44) and (45)

$$|a| z^3 = |F(x, y)| \gg y^{1/2} \quad \text{and} \quad h \ll Z^6.$$

Since $F(x, y) = az^3$ represents in projective coordinates a curve of genus 1, in virtue of a theorem of Néron (see [8], p. 82), the number of solutions of (44) is $O\big((\log Z^6)^{g/2+1}\big)$ where g is the rank of the curve. □

Remark. The lemma extends to all forms F with at least three distinct zeros. If the genus of the curve $F(x, y) = az^{|F|}$ is greater than 1 one needs a theorem of Mumford [10].

Lemma 8. *Let $\boldsymbol{K}$ be any field, U a finite subset of $\boldsymbol{K}$ and $P \in \boldsymbol{K}[\boldsymbol{t}]$, $P \neq 0$. The equation $P(\boldsymbol{t}) = 0$ has no more than $|P|\,|U|^{r-1}$ solutions $\boldsymbol{t} \in U^r$, where $|U|$ is the number of elements of U.*

Proof (by induction on r). For $r = 1$ the assertion is obvious. Assume that it holds for polynomials in $r - 1$ variables and let

$$P(\boldsymbol{t}) = \sum_{i=0}^{p} P_i(\boldsymbol{t}')t_1^{p-i}.$$

The solutions of $P(\boldsymbol{t}) = 0$ are of two kinds: satisfying $P_0(\boldsymbol{t}') = 0$ and $P_0(\boldsymbol{t}') \neq 0$. Since t_1 can take at most $|U|$ values, by the inductive assumption the number of solutions of the first kind does not exceed $|P_0|\,|U|^{r-1}$. Similarly since $\boldsymbol{t}'$ can take at most $|U|^{r-1}$ values the number of solutions of the second kind does not exceed $p|U|^{r-1}$. However $|P_0| + p \leqslant |P|$ and the proof is complete. □

Remark. A different proof can be obtained by an adaptation of the proof given by Schmidt for the special case $\boldsymbol{K} = U$ (see [17], p. 147, Lemma 3A).

Lemma 9. *If $f(\boldsymbol{t}), g(\boldsymbol{t}) \in \mathbb{Q}[\boldsymbol{t}]$, $g(\boldsymbol{t}) \mid f(\boldsymbol{t})^n$ and the fixed divisor of $f(\boldsymbol{t})$ equals $C(f)$ then the fixed divisor of $g(\boldsymbol{t})$ equals $C(g)$.*

Proof. Let the fixed divisor of g be $C(g)d$, $d \in \mathbb{N}$ and let $f(\boldsymbol{t})^n = g(\boldsymbol{t})h(\boldsymbol{t})$. Clearly for all $\boldsymbol{t} \in \mathbb{Z}^r$ $f(\boldsymbol{t})^n$ is divisible by $C(g)dC(h) = dC(f^n) = dC(f)^n$. On the other hand the fixed divisor of $f(\boldsymbol{t})^n$ is $C(f)^n$. Hence $d = 1$. □

Proof of Theorem 2. Consider first the case where F is a quadratic form. Then by Lemma 2

$$F(x, y) = A(ax^2 + bxy + cy^2), \quad \text{where} \quad A, a, b, c \in \mathbb{Z}$$

and either $\Delta = b^2 - 4ac = 1$ or Δ is a fundamental discriminant. Since the fixed divisor of $f(\boldsymbol{t})$ equals $C(f)$ we have $A \mid C(f)$ and we can assume without loss of generality that $A = 1$. Let $\boldsymbol{K} = \mathbb{Q}(\sqrt{\Delta})$,

$$f(\boldsymbol{t}) = l\prod_{\nu=1}^{n} \varphi_\nu(\boldsymbol{t})^{e_\nu} \tag{46}$$

be a factorization of $f(\boldsymbol{t})$ over $\boldsymbol{K}$ into irreducible factors such that φ_ν are distinct and have
c the coefficient of the first term in the inverse lexicographical order equal to 1. Since the fixed divisor of f equals $C(f)$ the condition (19) is satisfied in virtue of Lemma 9. Let $\mu, \boldsymbol{\tau}$ be parameters whose existence for $\{\varphi_\nu\}$ and $M = a$ is asserted in Lemma 5 and let

$$\psi_\nu = \varphi_\nu(\mu\boldsymbol{t} + \boldsymbol{\tau}) \quad (1 \leqslant \nu \leqslant n).$$

It follows that

$$f(\mu\boldsymbol{t} + \boldsymbol{\tau}) = l\prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t})^{e_\nu} \tag{47}$$

and

$$B = |l|\prod_{\nu=1}^{n} C(\psi_\nu)^{e_\nu} = C\big(f(\mu\boldsymbol{t} + \boldsymbol{\tau})\big) \in \mathbb{N}, \tag{48}$$

where an ideal in $\mathbb{Q}$ is identified with its positive generator. If $\Delta = 1$, F is equivalent to xy and Theorem 1 applies. Assume that $\Delta \neq 1$, thus $\boldsymbol{K}$ is a quadratic field. Taking $m = 1$ in Lemma 5 we infer that H implies the existence of a $\boldsymbol{t}_2 \in \mathbb{Z}^r$ such that $\dfrac{\big(\psi_\nu(\boldsymbol{t}_2)\big)}{C(\psi_\nu)}$ are distinct prime ideals of $\boldsymbol{K}$ not dividing B. By the assumption there exist $x_0, y_0 \in \mathbb{Z}$ such that

$$ax_0^2 + bx_0y_0 + cy_0^2 = f(\mu\boldsymbol{t}_2 + \boldsymbol{\tau}). \tag{49}$$

Hence, after a transformation

$$N\,\frac{\Big(ax_0 + \dfrac{b+\sqrt{\Delta}}{2}\,y_0\Big)}{\mathfrak{a}} = |f(\mu\boldsymbol{t}_2 + \boldsymbol{\tau})|, \quad \text{where} \quad \mathfrak{a} = \Big(a, \frac{b+\sqrt{\Delta}}{2}\Big).$$

It follows from (47) and (48) that for an integral ideal $\mathfrak{b}$ and some $\alpha_\nu \geqslant 0$

$$\Big(ax_0 + \frac{b+\sqrt{\Delta}}{2}\,y_0\Big)\mathfrak{a}^{-1} = \mathfrak{b}\prod_{\nu=1}^{n}\frac{\big(\psi_\nu(\boldsymbol{t}_2)\big)^{\alpha_\nu}}{C(\psi_\nu)^{\alpha_\nu}}, \quad \Big(\mathfrak{b}, \prod_{\nu=1}^{n}\frac{\big(\psi_\nu(\boldsymbol{t}_2)\big)}{C(\psi_\nu)}\Big) = 1. \tag{50}$$

On the other hand $\varphi_\nu^{e_\nu} \parallel f(\boldsymbol{t})$ implies $\varphi_\nu'^{e_\nu} \parallel f(\boldsymbol{t})$, where φ_ν' is conjugate to φ_ν with respect to $\mathbb{Q}(\boldsymbol{t})$. If $\varphi_\nu \notin \mathbb{Q}[\boldsymbol{t}]$ we have $\varphi_\nu' \neq \varphi_\nu$ and since φ_ν' has the coefficient of the leading term equal to 1, by (46)

$$\varphi_\nu' = \varphi_\lambda, \quad e_\nu = e_\lambda, \quad \psi_\nu' = \psi_\lambda \quad \text{for a } \lambda \neq \nu.$$

Thus without loss of generality we may assume that for a certain $k \equiv n \bmod 2$

$$\varphi_\nu' = \varphi_{\nu'}, \quad e_\nu = e_{\nu'}, \quad \psi_\nu' = \psi_{\nu'}, \quad \text{where} \quad \begin{aligned} \nu' &= \nu \quad (1 \leqslant \nu \leqslant k), \\ \nu' &= \nu - (-1)^{n-\nu} \quad (k < \nu \leqslant n). \end{aligned} \tag{51}$$

Hence by (48)

$$|ax_0^2 + bx_0y_0 + cy_0^2| = N\mathfrak{b}\prod_{\nu=1}^{n}\Big(\frac{\psi_\nu(\boldsymbol{t}_2)}{C(\psi_\nu)}\Big)^{\alpha_\nu+\alpha_{\nu'}}, \quad \Big(N\mathfrak{b}, \prod_{\nu=1}^{n}\frac{\big(\psi_\nu(\boldsymbol{t}_2)\big)}{C(\psi_\nu)}\Big) = 1$$

and a comparison with (49) gives

$$\alpha_\nu + \alpha_{\nu'} = e_\nu \quad (1 \leqslant \nu \leqslant n). \tag{52}$$

Let us define now $X(\boldsymbol{t})$, $Y(\boldsymbol{t})$ by the equation

$$\vartheta(\boldsymbol{t}) = aX(\boldsymbol{t}) + \frac{b+\sqrt{\Delta}}{2}\,Y(\boldsymbol{t}) = \Big(ax_0 + \frac{b+\sqrt{\Delta}}{2}\,y_0\Big)\prod_{\nu=1}^{n}\Big(\frac{\varphi_\nu(\boldsymbol{t})}{\psi_\nu(\boldsymbol{t}_2)}\Big)^{\alpha_\nu}. \tag{53}$$

The polynomials $X(\boldsymbol{t})$, $Y(\boldsymbol{t})$ have integral coefficients since by (50)

$$C\big(\vartheta(\nu\boldsymbol{t} + \boldsymbol{\tau})\big) = \Big(ax_0 + \frac{b+\sqrt{\Delta}}{2}\,y_0\Big)\prod_{\nu=1}^{n}\Big(\frac{C(\psi_\nu)}{\big(\psi_\nu(\boldsymbol{t}_2)\big)}\Big)^{\alpha_\nu} = \mathfrak{a}\mathfrak{b},$$

[c]

$$\mu^{|\vartheta|}C(\vartheta) \equiv 0 \bmod \mathfrak{a}$$

and $(\mu, a) = 1$ implies $C(\vartheta) \equiv 0 \bmod \mathfrak{a}$.

On the other hand, by (53), (49), (51), (52), (46) and (47)

$$\begin{aligned} F\big(X(\boldsymbol{t}), Y(\boldsymbol{t})\big) &= aX(\boldsymbol{t})^2 + bX(\boldsymbol{t})Y(\boldsymbol{t}) + cY(\boldsymbol{t})^2 \\ &= (ax_0^2 + bx_0y_0 + cy_0^2) \prod_{\nu=1}^{n} \Big(\frac{\varphi_\nu(\boldsymbol{t})\varphi_\nu'(\boldsymbol{t})}{\psi_\nu(\boldsymbol{t}_2)\psi_\nu'(\boldsymbol{t}_2)} \Big)^{\alpha_\nu} \\ &= f(\mu \boldsymbol{t}_2 + \boldsymbol{\tau}) \prod_{\nu=1}^{n} \Big(\frac{\varphi_\nu(\boldsymbol{t})}{\psi_\nu(\boldsymbol{t}_2)} \Big)^{\alpha_\nu + \alpha_{\nu'}} \\ &= f(\mu \boldsymbol{t}_2 + \boldsymbol{\tau}) \prod_{\nu=1}^{n} \Big(\frac{\varphi_\nu(\boldsymbol{t})}{\psi_\nu(\boldsymbol{t}_2)} \Big)^{e_\nu} = f(\boldsymbol{t}). \end{aligned}$$

Assume now that F is a reducible cubic form. If F is singular we have $F = (ax + by)^2 \cdot (cx + dy)$, hence by the condition (1)

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = \pm 1,$$

F is equivalent to $x^2 y$ and Theorem 1 applies.

If F is non-singular we have

$$F(x, y) = (a_0 x + b_0 y) F_1(x, y), \tag{54}$$

where F_1 is a non-singular primitive quadratic form. By Lemma 3 we have

$$F_1(x, y) = G(a_1 x + b_1 y, a_2 x + b_2 y), \tag{55}$$

where G is primary and primitive. Let us put $G(x, y) = ex^2 + gxy + hy^2$. By Lemma 2, the discriminant $\Delta = g^2 - 4eh$ equals 1 or is fundamental. The condition that F is primary implies that

$$d = \left(\begin{vmatrix} a_0 & a_1 \\ b_0 & b_1 \end{vmatrix}, \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}, \begin{vmatrix} a_2 & a_0 \\ b_2 & b_0 \end{vmatrix} \right) = 1. \tag{56}$$

Otherwise, by a classical result on integral matrices (see [2], p. 52) the linear forms $a_i x + b_i y$ $(0 \leqslant i \leqslant 2)$ would be expressible integrally in terms of two linear forms with determinant $d > 1$. Let $\boldsymbol{K} = \mathbb{Q}(\sqrt{\Delta})$ and let the factorization of $f(\boldsymbol{t})$ over $\boldsymbol{K}$ be given by (46). Since the fixed divisor of $f(\boldsymbol{t})$ equals $C(f)$ the condition (19) is satisfied in virtue of Lemma 9. By Lemma 6 the equation

$$F\big(X(\boldsymbol{t}), Y(\boldsymbol{t})\big) = f(\boldsymbol{t}) \tag{57}$$

has only finitely many solutions in polynomials $X(\boldsymbol{t}), Y(\boldsymbol{t}) \in \mathbb{Q}[\boldsymbol{t}]$ that are linearly independent. Let M be a positive integer such that $MX, MY \in \mathbb{Z}[\boldsymbol{t}]$ for all of them. We apply Lemma 5 to the sequence $\{\varphi_\nu\}$ with this M. Let $\mu, \boldsymbol{\tau}$ be any parameters with the property asserted in that lemma and let $\psi_\nu(\boldsymbol{t}) = \varphi_\nu(\mu \boldsymbol{t} + \boldsymbol{\tau})$. We have again the formulae (47) and (48).

We shall deduce from H the existence of polynomials $x(\boldsymbol{t}), y(\boldsymbol{t}) \in \mathbb{Z}[\boldsymbol{t}]$ such that $F\big(x(\boldsymbol{t}), y(\boldsymbol{t})\big) = f(\mu\boldsymbol{t} + \boldsymbol{\tau})$. This suffices to prove the theorem. Indeed the polynomials

$$X(\boldsymbol{t}) = x\Big(\frac{\boldsymbol{t} - \boldsymbol{\tau}}{\mu}\Big), \quad Y(\boldsymbol{t}) = y\Big(\frac{\boldsymbol{t} - \boldsymbol{\tau}}{\mu}\Big)$$

satisfy (57) and on one hand

$$\mu^{|x|}X, \mu^{|y|}Y \in \mathbb{Z}[\boldsymbol{t}],$$

on the other hand, if X, Y are linearly independent, we have by the choice of M

$$MX, MY \in \mathbb{Z}[\boldsymbol{t}].$$

Since $(\mu, M) = 1$ we get $X, Y \in \mathbb{Z}[\boldsymbol{t}]$.

If X, Y are linearly dependent, then $F\big(X(\boldsymbol{t}), Y(\boldsymbol{t})\big) = f(\boldsymbol{t}) = C_0(f) f_0(\boldsymbol{t})^3, C(f_0) = 1$ and

$$X(\boldsymbol{t}) = \xi\zeta^{-1} f_0(\boldsymbol{t}), \quad Y(\boldsymbol{t}) = \eta\zeta^{-1} f_0(\boldsymbol{t}), \quad \xi, \eta, \zeta \in \mathbb{Z}, \quad (\xi, \eta, \zeta) = 1;$$
$$F(\xi, \eta) = C(f)\zeta^3, \quad \zeta \mid \mu^{|f_0|}.$$

If the above holds for all pairs $\langle \mu_i, \boldsymbol{\tau}_i \rangle$ of the sequence mentioned in the last assertion of Lemma 5, then, using the obvious notation, we infer from $(\mu_i, \mu_h) = 1$ that either $|\zeta_i| \neq |\zeta_h|$ for $i \neq h$ or there exists an i with $|\zeta_i| = 1$. In the former case since $|\zeta_i| \leqslant \mu_i^{|f_0|}$ the number of distinct $|\zeta_i| \leqslant Z$ is $\Omega\Big(\dfrac{Z^{1/|f_0|n}}{\log Z}\Big)$, which contradicts Lemma 7. Therefore, the latter case holds and $X_i, Y_i \in \mathbb{Z}[\boldsymbol{t}]$.

In order to deduce the existence of $x(\boldsymbol{t}), y(\boldsymbol{t})$ we shall consider successively the cases $\Delta = 1$, $\Delta < 0$, $\Delta > 1$.

If $\Delta = 1$, by (47), (48) and Lemma 5, H implies the existence for every $\boldsymbol{t}_1 \in \mathbb{Z}^r$ and every m prime to $f(\mu\boldsymbol{t}_1 + \boldsymbol{\tau})$ of a $\boldsymbol{t}_2 \equiv \boldsymbol{t}_1 \bmod m$ such that $\dfrac{|\psi_\nu(\boldsymbol{t}_2)|}{C(\psi_\nu)}$ are distinct primes not dividing B $(1 \leqslant \nu \leqslant n)$.

On the other hand, since a unimodular transformation of G does not affect the condition (56), we can assume $G(x, y) = xy$.

By the assumption of C there exist integers x, y such that

$$F(x, y) = f(\mu\boldsymbol{t}_2 + \boldsymbol{\tau})$$

and it follows from (47), (48), (54) and (55) that for suitable integers c_i and nonnegative integers $\alpha_{i\nu}$ $(0 \leqslant i \leqslant 2, 1 \leqslant \nu \leqslant n)$

$$a_i x + b_i y = c_i \prod_{\nu=1}^{n} \Big(\frac{\psi_\nu(\boldsymbol{t}_2)}{C(\psi_\nu)}\Big)^{\alpha_{i\nu}}, \tag{58}$$

$$c_0 c_1 c_2 = B \operatorname{sgn} l, \quad \alpha_{0\nu} + \alpha_{1\nu} + \alpha_{2\nu} = e_\nu. \tag{59}$$

The set S of systems $\big[\{c_i\}, \{\alpha_{i\nu}\}\big]$ satisfying (59) is finite. It follows from (58) that

$$\prod_{s \in S} D_s(\boldsymbol{t}_2) = 0, \tag{60}$$

where for $s = \big[\{c_i\}, \{\alpha_{i\nu}\}\big]$:

$$D_s(\boldsymbol{t}) = \det[a_i, b_i, \Psi_{is}(\boldsymbol{t})]_{0\leqslant i\leqslant 2}, \quad \Psi_{is}(\boldsymbol{t}) = c_i \prod_{\nu=1}^{n} \Big(\frac{\psi_\nu(\boldsymbol{t})}{C(\psi_\nu)}\Big)^{\alpha_{i\nu}}.$$

Since $\Psi_{is}(\boldsymbol{t}_2) \equiv \Psi_{is}(\boldsymbol{t}_1) \bmod m$, $D_s(\boldsymbol{t}_2) \equiv D_s(\boldsymbol{t}_1) \bmod m$ and (60) gives

$$\prod_{s\in S} D_s(\boldsymbol{t}_1) \equiv 0 \bmod m.$$

The latter congruence holds for all m prime to $f(\mu\boldsymbol{t}_1 + \boldsymbol{\tau})$, hence

$$f(\mu\boldsymbol{t}_1 + \boldsymbol{\tau}) \prod_{s\in S} D_s(\boldsymbol{t}_1) = 0$$

and since $\boldsymbol{t}_1$ is an arbitrary integral vector

$$f(\mu\boldsymbol{t} + \boldsymbol{\tau}) \prod_{s\in S} D_s(\boldsymbol{t}) = 0$$

identically. However $f(\mu\boldsymbol{t} + \boldsymbol{\tau}) \neq 0$, thus there exists an $s \in S$ such that

$$D_s(\boldsymbol{t}) = 0.$$

By (56) the rank of the matrix $[a_i, b_i]_{0\leqslant i\leqslant 2}$ is two, thus the system of equations

$$a_i x + b_i y = \Psi_{is}(\boldsymbol{t}) \quad (0 \leqslant i \leqslant 2)$$

is soluble in polynomials $x, y \in \mathbb{Q}[\boldsymbol{t}]$.

Moreover, by Cramer's formulae

$$\begin{vmatrix} a_i & b_i \\ a_j & b_j \end{vmatrix} x, \begin{vmatrix} a_i & b_i \\ a_j & b_j \end{vmatrix} y \in \mathbb{Z}[\boldsymbol{t}] \quad (0 \leqslant i \leqslant j \leqslant 2)$$

and again by (56) $x, y \in \mathbb{Z}[\boldsymbol{t}]$. On the other hand, by (59), (48) and (47)

$$F(x, y) = \prod_{i=0}^{2}(a_i x + b_i y) = \prod_{i=0}^{2} c_i \prod_{\nu=1}^{n} \Big(\frac{\psi_\nu(\boldsymbol{t})}{C(\psi_\nu)}\Big)^{\alpha_{i\nu}} = B \operatorname{sgn} l \prod_{\nu=1}^{n} \Big(\frac{\psi_\nu(\boldsymbol{t})}{C(\psi_\nu)}\Big)^{e_\nu}$$
$$= l \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t})^{e_\nu} = f(\mu\boldsymbol{t} + \boldsymbol{\tau}).$$

Let us consider now the case $\Delta \neq 1$. Then, by Lemma 5 and (47), (48), H implies the existence for every $\boldsymbol{t}_1 \in \mathbb{Z}^r$ and every m prime to $\Delta f(\mu\boldsymbol{t}_1 + \boldsymbol{\tau})$ of a $\boldsymbol{t}_2 \equiv \boldsymbol{t}_1 \bmod m$ such that the ideals $\dfrac{\big(\psi_\nu(\boldsymbol{t}_2)\big)}{C(\psi_\nu)}$ $(\nu \leqslant n)$ are prime in $\boldsymbol{K}$, distinct and do not divide B. By the assumption of C there exist integers x, y such that

$$F(x, y) = f(\mu\boldsymbol{t}_2 + \boldsymbol{\tau})$$

and it follows from (47), (48), (51) and (55) that for suitable integral ideals $\mathfrak{a}, \mathfrak{b}$ and

nonnegative integers α_ν, β_ν $(1 \leqslant \nu \leqslant n)$

$$
\begin{aligned}
(a_0x + b_0y) &= \mathfrak{a} \prod_{\nu=1}^{n} \left(\frac{\big(\psi_\nu(\boldsymbol{t}_2)\big)}{C(\psi_\nu)} \right)^{\alpha_\nu}, \\
\left(e(a_1x + b_1y) + \frac{g + \sqrt{\Delta}}{2} (a_2x + b_2y) \right) \mathfrak{g}^{-1} &= \mathfrak{b} \prod_{\nu=1}^{n} \left(\frac{\psi_\nu(\boldsymbol{t}_2)}{C(\psi_\nu)} \right)^{\beta_\nu},
\end{aligned} \tag{61}
$$

where $\mathfrak{g} = \left(e, \dfrac{g + \sqrt{\Delta}}{2} \right)$,

$$
\mathfrak{a} N \mathfrak{b} = (B), \quad \alpha_\nu + \beta_\nu + \beta_{\nu'} = e_\nu \quad (1 \leqslant \nu \leqslant n), \tag{62}
$$

ν' is defined in (51). We get

$$
\begin{aligned}
a_0x + b_0y &= \alpha \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t}_2)^{\alpha_\nu}, \\
e(a_1x + b_1y) + \frac{g + \sqrt{\Delta}}{2} (a_2x + b_2y) &= \beta \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t}_2)^{\beta_\nu},
\end{aligned} \tag{63}
$$

where

$$
(\alpha) = \mathfrak{a} \prod_{\nu=1}^{n} C(\psi_\nu)^{-\alpha_\nu}, \quad (\beta) = \mathfrak{g}\mathfrak{b} \prod_{\nu=1}^{n} C(\psi_\nu)^{-\beta_\nu} \tag{64}
$$

and by (47) and (62)

$$
\alpha N \beta = le. \tag{65}
$$

Since $\mathfrak{a}$ is integral, $\Psi_0(\boldsymbol{t}; \alpha, \alpha_\nu) = \alpha \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t})^{\alpha_\nu}$ has integral coefficients. On the other hand, by (51) and (62) $\alpha_\nu = \alpha_{\nu'}$ $(k < \nu \leqslant n)$ and by (65) $\alpha \in \mathbb{Q}$, hence

$$
\Psi_0(\boldsymbol{t}; \alpha, \alpha_\nu) \in \mathbb{Z}[\boldsymbol{t}].
$$

Similarly, since $\mathfrak{b}$ is integral, $\beta \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t})^{\beta_\nu} \in \mathfrak{g}[\boldsymbol{t}]$ and we get

$$
\beta \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t})^{\beta_\nu} = e\Psi_1(t; \beta, \beta_\nu) + \frac{g + \sqrt{\Delta}}{2} \Psi_2(\boldsymbol{t}; \beta, \beta_\nu), \tag{66}
$$

where

$$
\Psi_i(\boldsymbol{t}; \beta, \beta_\nu) \in \mathbb{Z}[\boldsymbol{t}] \quad (i = 1, 2).
$$

The equations (63) take the form

$$
\begin{aligned}
a_0x + b_0y &= \Psi_0(\boldsymbol{t}_2; \alpha, \alpha_\nu), \\
a_ix + b_iy &= \Psi_i(\boldsymbol{t}_2; \beta, \beta_\nu) \quad (i = 1, 2).
\end{aligned} \tag{67}
$$

For a system $s = [\alpha, \beta, \{\alpha_\nu\}, \{\beta_\nu\}]$ we put

$$\Psi_{0s}(\boldsymbol{t}) = \Psi_0(\boldsymbol{t}; \alpha, \alpha_\nu), \quad \Psi_{is}(\boldsymbol{t}) = \Psi_i(\boldsymbol{t}; \beta, \beta_\nu) \quad (i = 1, 2)$$

and denote by S the set of all such systems satisfying (62) and (64). If $\Delta < 0$ the set S is finite. It follows from (67) that

$$\prod_{s \in S} D_s(\boldsymbol{t}_2) = 0, \tag{68}$$

where

$$D_s(\boldsymbol{t}) = \det\big[a_i, b_i, \Psi_{is}(\boldsymbol{t})\big]_{0 \leqslant i \leqslant 2}.$$

Since $\Psi_{is}(\boldsymbol{t}_2) \equiv \Psi_{is}(\boldsymbol{t}_1) \bmod m$ we infer from (68), as in the case $\Delta = 1$ from (60), that for a suitable $s \in S$ the system of equations

$$a_i x + b_i y = \Psi_{is}(\boldsymbol{t}) \quad (0 \leqslant i \leqslant 2)$$

is soluble in polynomials $x, y \in \mathbb{Z}[\boldsymbol{t}]$. By (54), (55), (66), (47), (65) and (51) we get

$$\begin{aligned} F(x, y) &= (a_0 x + b_0 y) N\Big(e(a_1 x + b_1 y) + \frac{g + \sqrt{\Delta}}{2}(a_2 x + b_2 y)\Big) e^{-1} \\ &= \Psi_{0s}(\boldsymbol{t}) N\Big(e\Psi_{1s}(\boldsymbol{t}) + \frac{g + \sqrt{\Delta}}{2}\Psi_{2s}(\boldsymbol{t})\Big) e^{-1} \\ &= \alpha \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t})^{\alpha_\nu} N\Big(\beta \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t})^{\beta_\nu}\Big) e^{-1} \\ &= \alpha N\beta e^{-1} \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t})^{\alpha_\nu + \beta_\nu + \beta_{\nu'}} = l \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t})^{e_\nu} = f(\mu \boldsymbol{t} + \boldsymbol{\tau}). \end{aligned}$$

If $\Delta > 0$ the set S is infinite. We can however divide it into finitely many classes assigning two systems $[\alpha, \beta, \{\alpha_\nu\}, \{\beta_\nu\}]$ and $[\alpha, \gamma, \{\alpha_\nu\}, \{\beta_\nu\}]$ to the same class if $\pm\gamma/\beta$ is a totally positive unit of $\boldsymbol{K}$. Then every class contains exactly one system satisfying

$$1 \leqslant \beta < \varepsilon, \tag{69}$$

where $\varepsilon > 1$ is the fundamental totally positive unit. Denoting the set of all systems satisfying (62), (64) and (68) by S_0 we infer from (67) the existence of a $\sigma \in \mathbb{Z}$ such that

$$\prod_{s \in S_0} D_{\sigma s}(\boldsymbol{t}_2) = 0,$$

where for $s = [\alpha, \beta, \{\alpha_\nu\}, \{\beta_\nu\}]$

$$D_{\sigma s}(\boldsymbol{t}) = \begin{vmatrix} a_0 & b_0 & \Psi_0(\boldsymbol{t}; \alpha, \alpha_\nu) \\ a_1 & b_1 & \Psi_1(\boldsymbol{t}; \varepsilon^\sigma \beta, \beta_\nu) \\ a_2 & b_2 & \Psi_2(\boldsymbol{t}; \varepsilon^\sigma \beta, \beta_\nu) \end{vmatrix}.$$

Since $D_{\sigma s}(\boldsymbol{t}_2) \equiv D_{\sigma s}(\boldsymbol{t}_1) \bmod m$ for all s we conclude that

$$\prod_{s \in S_0} D_{\sigma s}(\boldsymbol{t}_1) \equiv 0 \bmod m \tag{70}$$

where σ depends on m.

We have an identity

$$u\Big(e\Psi_{1s}(\boldsymbol{t}) + \frac{g+\sqrt{\Delta}}{2}\,\Psi_{2s}(\boldsymbol{t})\Big) = e\Phi_{1s}(\boldsymbol{t},u) + \frac{g+\sqrt{\Delta}}{2}\,\Phi_{2s}(\boldsymbol{t},u), \tag{71}$$

where

$$\Phi_{1s}(\boldsymbol{t},u) = \frac{1}{2}\Big[u\Big(1-\frac{g}{\sqrt{\Delta}}\Big) + u^{-1}\Big(1+\frac{g}{\sqrt{\Delta}}\Big)\Big]\Psi_{1s}(\boldsymbol{t}) + \frac{\Delta-g^2}{4e}\,\frac{u-u^{-1}}{\sqrt{\Delta}}\,\Psi_{2s}(\boldsymbol{t}),$$

$$\Phi_{2s}(\boldsymbol{t},u) = e\,\frac{u-u^{-1}}{\sqrt{\Delta}}\,\Psi_{1s}(\boldsymbol{t}) + \frac{1}{2}\Big[u\Big(1+\frac{g}{\sqrt{\Delta}}\Big) + u^{-1}\Big(1-\frac{g}{\sqrt{\Delta}}\Big)\Big]\Psi_{2s}(\boldsymbol{t}).$$

Since ε is conjugate to ε^{-1}

$$\Phi_{is}(\boldsymbol{t},\varepsilon^{\sigma}) \in \mathbb{Q}[\boldsymbol{t}] \quad (i=1,2)$$

and by (71)

$$\Psi_i(\boldsymbol{t};\varepsilon^{\sigma}\beta,\beta_{\nu}) = \Phi_{is}(\boldsymbol{t},\varepsilon^{\sigma}) \quad (i=1,2).$$

The congruence (70) takes the form

$$\prod_{s\in S_0} E_s(\boldsymbol{t}_1,\varepsilon^{\sigma}) \equiv 0 \bmod m, \tag{72}$$

where

$$E_s(\boldsymbol{t},u) = \begin{vmatrix} a_0 & b_0 & \Psi_{0s}(\boldsymbol{t}) \\ a_1 & b_1 & \Phi_{1s}(\boldsymbol{t},u) \\ a_2 & b_2 & \Phi_{2s}(\boldsymbol{t},u) \end{vmatrix}. \tag{73}$$

However $uE_s(\boldsymbol{t},u) \in \mathbb{Q}[\boldsymbol{t},u]$ and hence $u^{|S_0|}\prod_{s\in S_0} E_s(\boldsymbol{t}_1,u) \in \mathbb{Q}[u]$.

Since the congruence (72) is soluble for all m prime to $\Delta f(\mu\boldsymbol{t}_1+\boldsymbol{\tau})$, it follows from Theorem 6 of [15] that the equation

$$f(\mu\boldsymbol{t}_1+\boldsymbol{\tau})\prod_{s\in S_0} E_s(\boldsymbol{t}_1,\varepsilon^{\sigma}) = 0$$

is soluble in integers σ. Thus for every $\boldsymbol{t}_1 \in \mathbb{Z}^r$ either $f(\mu\boldsymbol{t}_1+\boldsymbol{\tau}) = 0$ or $f(\mu\boldsymbol{t}_1+\boldsymbol{\tau}) \neq 0$ and there exist a $\sigma \in \mathbb{Z}$ and an $s = \big[\alpha,\beta,\{\alpha_{\nu}\},\{\beta_{\nu}\}\big] \in S_0$ such that $E_s(\boldsymbol{t}_1,\varepsilon^{\sigma}) = 0$.

In the latter case it follows from (71) and (73) that

$$\begin{vmatrix} a_0 & b_0 & \Psi_{0s}(\boldsymbol{t}_1) \\ ea_1+\dfrac{g+\sqrt{\Delta}}{2}\,a_2 & eb_1+\dfrac{g+\sqrt{\Delta}}{2}\,b_2 & \varepsilon^{\sigma}\beta\displaystyle\prod_{\nu=1}^{n}\psi_{\nu}(\boldsymbol{t}_1)^{\beta_{\nu}} \\ ea_1+\dfrac{g-\sqrt{\Delta}}{2}\,a_2 & eb_1+\dfrac{g-\sqrt{\Delta}}{2}\,b_2 & \varepsilon^{-\sigma}\beta'\displaystyle\prod_{\nu=1}^{n}\psi_{\nu}(\boldsymbol{t}_1)^{\beta_{\nu'}} \end{vmatrix}$$

$$= -e\sqrt{\Delta}\,E_s(\boldsymbol{t}_1,\varepsilon^{\sigma}) = 0$$

and $\varepsilon^\sigma \beta \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t}_1)^{\beta_\nu}$ satisfies the quadratic equation

$$Lz^2 - K\Psi_{0s}(\boldsymbol{t}_1)z - L'N\beta \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t}_1)^{\beta_\nu+\beta_{\nu'}} = 0,$$

where β', L' are conjugate to β, L, respectively,

(74)
$$L = \begin{vmatrix} a_0 & b_0 \\ ea_1 + \dfrac{g-\sqrt{\Delta}}{2}\, a_2 & eb_1 + \dfrac{g-\sqrt{\Delta}}{2}\, b_2 \end{vmatrix},$$

$$K = \begin{vmatrix} ea_1 + \dfrac{g+\sqrt{\Delta}}{2}\, a_2 & eb_1 + \dfrac{g+\sqrt{\Delta}}{2}\, b_2 \\ ea_1 + \dfrac{g-\sqrt{\Delta}}{2}\, a_2 & eb_1 + \dfrac{g-\sqrt{\Delta}}{2}\, b_2 \end{vmatrix}$$

Since $e[a_0, b_0] \neq 0$ we have $L \neq 0$ by (56), and

(75)
$$\left\lceil \varepsilon^\sigma \beta \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t}_1)^{\beta_\nu} \right\rceil \ll \|\boldsymbol{t}_1\|^{|f|}$$

where $\lceil\ \rceil$ denotes the maximum modulus of the conjugates and the constant in the symbol $\ll$ depends on F, f, μ, $\boldsymbol{\tau}$, s.

On the other hand, by (47), (51), (62), (65) and (69)

$$\left\lceil \beta \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t}_1)^{\beta_\nu} \right\rceil \ll \|\boldsymbol{t}_1\|^{|f|/2}.$$

Since $f(\mu\boldsymbol{t}_1 + \boldsymbol{\tau}) \neq 0$ whence by (64)

$$\left| N\Big(\beta \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t}_1)^{\beta_\nu}\Big) \right| \gg N\mathfrak{g}\mathfrak{b} \gg 1$$

we get

$$\left\lceil \beta^{-1} \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t}_1)^{-\beta_\nu} \right\rceil < \|\boldsymbol{t}_1\|^{|f|/2}.$$

This together with (75) implies

$$\varepsilon^{|\sigma|} = \lceil \varepsilon^\sigma \rceil \ll \|\boldsymbol{t}_1\|^{3|f|/2}, \quad |\sigma| \leqslant \frac{3}{2}\,|f|\,\frac{\log \|\boldsymbol{t}_1\|}{\log \varepsilon} + \varrho,$$

where ϱ is a constant depending on F, f, μ, $\boldsymbol{\tau}$ but independent of s (S_0 is finite).

Let us choose now a positive integer T so large that

(76)
$$2T + 1 > |f|(|S_0| + 1)\Big(3|f|\,\frac{\log T}{\log \varepsilon} + 2\varrho + 1\Big).$$

If $\boldsymbol{t}_1$ runs through all integral vectors satisfying $\|\boldsymbol{t}_1\| \leqslant T$, σ runs through integers satisfying

$$|\sigma| \leqslant \frac{3}{2}\,|f|\,\frac{\log T}{\log \varepsilon} + \varrho.$$

The number of vectors in question is $(2T+1)^r$, the number of integers does not exceed $3|f|\,\dfrac{\log T}{\log \varepsilon} + 2\varrho + 1$, hence there is an integer σ_0 that corresponds to at least

$$(2T+1)^r\Big(3|f|\,\frac{\log T}{\log \varepsilon} + 2\varrho + 1\Big)^{-1}$$

different vectors $\boldsymbol{t}_1$ satisfying $\|\boldsymbol{t}_1\| \leqslant T$. By (76) we get more than $|f|(|S_0|+1) \times (2T+1)^{r-1}$ such vectors satisfying the equation

$$f(\mu\boldsymbol{t}_1 + \boldsymbol{\tau}) \prod_{s \in S_0} E_s(\boldsymbol{t}_1, \varepsilon^{\sigma_0}) = 0.$$

Since by (62), (71) and (73) the degree of $E_s(\boldsymbol{t}, \varepsilon^{\sigma_0})$ does not exceed $|f|$, the degree of the polynomial on the left hand side does not exceed $|f|(|S_0|+1)$ and Lemma 8 shows that

$$f(\mu\boldsymbol{t} + \boldsymbol{\tau}) \prod_{s \in S_0} E_s(\boldsymbol{t}, \varepsilon^{\sigma_0}) = 0$$

identically. Therefore, there exists an $s \in S_0$ such that $E_s(\boldsymbol{t}, \varepsilon^{\sigma_0}) = 0$ and by (56) the system of equations

$$\begin{aligned} a_0 x + b_0 y &= \Psi_{0s}(\boldsymbol{t}), \\ a_i x + b_i y &= \Phi_{is}(\boldsymbol{t}) \quad (i = 1, 2) \end{aligned}$$

is soluble in polynomials $x, y \in \mathbb{Z}[t]$. By (54), (55), (71), (66), (47), (62), (65) and (51) we get for these polynomials

$$\begin{aligned} F(x, y) &= (a_0 x + b_0 y) N\Big(e(a_1 x + b_1 y) + \frac{g + \sqrt{\Delta}}{2}\,(a_2 x + b_2 y)\Big) e^{-1} \\ &= \Psi_{0s}(\boldsymbol{t}) N\Big(\varepsilon^{-\sigma_0} e(a_1 x + b_1 y) + \varepsilon^{-\sigma_0}\,\frac{g + \sqrt{\Delta}}{2}\,(a_2 x + b_2 y)\Big) e^{-1} \\ &= \Psi_{0s}(\boldsymbol{t}) N\Big(e\Psi_{is}(\boldsymbol{t}) + \frac{g + \sqrt{\Delta}}{2}\,\Psi_{2s}(\boldsymbol{t})\Big) e^{-1} = f(\mu\boldsymbol{t} + \boldsymbol{\tau}) \end{aligned}$$

and the proof is complete. □

Remark. For the proof of a more general result mentioned in the introduction one needs more general versions of Lemmata 2, 5 and 7 and Theorem 7 of [16] instead of Theorem 6 of [15]. In the difficult case of an irreducible form F with all zeros real Theorem 7 of [16] does not suffice, but Skolem's conjecture on exponential congruences would do (see [18]). One could avoid this step in the proof provided it were known that the number of vectors $\boldsymbol{t}$ satisfying $\|\boldsymbol{t}\| \leqslant T$ and the conditions of Lemma 4 grows faster than $T^{r-1}(\log T)^{|F|}$. For $r = 1$ much more has been conjectured by Bateman and Horn [1].

4.

The next lemma is a refinement of Lemma 1 of [13].

Lemma 10. *Let $P \in \mathbb{Q}[\boldsymbol{t}, u]$ be a polynomial such that for no $\varphi \in \mathbb{Q}(\boldsymbol{t})$*

$$P\big(\boldsymbol{t}, \varphi(\boldsymbol{t})\big) = 0$$

identically. Then there exists a $\boldsymbol{t}_1 \in \mathbb{Z}^r$ such that for any $M \in \mathbb{N}$ there exists an $m \in \mathbb{N}$ prime to M such that for all $\boldsymbol{t} \in \mathbb{Z}^r$, $\boldsymbol{t} \equiv \boldsymbol{t}_1 \bmod m$ and all $u \in \mathbb{Q}$

$$P(\boldsymbol{t}, u) \neq 0.$$

Proof. Following the proof of Lemma 1 in [13] we take $m = q_1 \cdots q_k$, where in the notation of that paper the primes q_i are chosen not to divide M. □

Lemma 11. *Let $G, H \in \mathbb{Q}[x, y]$ be relatively prime forms, $p, g_i, h_i \in \mathbb{Q}[\boldsymbol{t}]$ $(i \leqslant I)$ arbitrary polynomials, $p \neq 0$.*

If for every $\boldsymbol{t}_1 \in \mathbb{Z}^r$ and for every integer m prime to $p(\boldsymbol{t})$ there are an $i \leqslant I$, a $\boldsymbol{t}_2 \in \mathbb{Z}^r$, $\boldsymbol{t}_2 \equiv \boldsymbol{t}_1 \bmod m$ and $x, y \in \mathbb{Q}$ satisfying

$$G(x, y) = g_i(\boldsymbol{t}_2), \quad H(x, y) = h_i(\boldsymbol{t}_2) \tag{77}$$

then there exist a $j \leqslant I$ and polynomials $X, Y \in \mathbb{Q}[\boldsymbol{t}]$ such that

$$G(X, Y) = g_j, \quad H(X, Y) = h_j.$$

Proof. If $G(x, y) - g_i(\boldsymbol{t})$, $H(x, y) - h_i(\boldsymbol{t})$ had a common factor $d(x, y, \boldsymbol{t}) \neq \text{const}$ then the leading forms of d with respect to x, y would divide $G(x, y)$ and $H(x, y)$. Thus for each $i \leqslant I$

$$\big(G(x, y) - g_i(\boldsymbol{t}), H(x, y) - h_i(\boldsymbol{t})\big) = 1.$$

Let $R_i(\boldsymbol{t}, x)$, $S_i(\boldsymbol{t}, y)$ be the resultants of $G(x, y) - g_i(\boldsymbol{t})$ and $H(x, y) - h_i(\boldsymbol{t})$ with respect to y and x respectively. It follows from the construction of resultants that the leading coefficients of R_i in x and of S_i in y are equal to the resultants of $G(1, z)$, $H(1, z)$ and of $G(z, 1)$, $H(z, 1)$ respectively. Hence these leading coefficients are independent of $\boldsymbol{t}$. Let

$$R_i(\boldsymbol{t}, x) = R_{i0}(\boldsymbol{t}, x) \prod_{\varrho=1}^{r_i} \big(x - R_{i\varrho}(\boldsymbol{t})\big), \tag{78}$$

$$S_i(\boldsymbol{t}, y) = S_{i0}(\boldsymbol{t}, y) \prod_{\sigma=1}^{s_i} \big(y - S_{i\sigma}(\boldsymbol{t})\big), \tag{79}$$

where R_{i0} and S_{i0} have no factor linear in x or y respectively. If for some triple (i, ϱ, σ) with $i \leqslant I$, $1 \leqslant \varrho \leqslant r_i$, $1 \leqslant \sigma \leqslant s_i$

$$G(R_{i\varrho}, S_{i\sigma}) = g_i \quad \text{and} \quad H(R_{i\varrho}, S_{i\sigma}) = h_i,$$

the lemma follows.

Therefore, suppose that for each triple (i, ϱ, σ) in question

$$G(R_{i\varrho}, S_{i\sigma}) \neq g_i \quad \text{or} \quad H(R_{i\varrho}, S_{i\sigma}) \neq h_i.$$

Then

c (80) $$T_{i\varrho\sigma} = \big(G(R_{i\varrho}, S_{i\sigma}) - g_i\big)^2 + \big(H(R_{i\varrho}, S_{i\sigma}) - h_i\big)^2 \neq 0$$

and we set in Lemma 10

(81) $$P(\boldsymbol{t}, u) = p(\boldsymbol{t}) \prod_{i=1}^{I} R_{i0}(\boldsymbol{t}, u) S_{i0}(\boldsymbol{t}, u) \prod_{\varrho=1}^{r_i} \prod_{\sigma=1}^{s_i} T_{i\varrho\sigma}(\boldsymbol{t}).$$

By that lemma with $M = 1$ there exist an $m \in \mathbb{N}$ and a $\boldsymbol{t}_1 \in \mathbb{Z}^r$ such that if $\boldsymbol{t} \equiv \boldsymbol{t}_1 \bmod m$ and $u \in \mathbb{Q}$ we have

(82) $$P(\boldsymbol{t}, u) \neq 0.$$

In particular, taking $\boldsymbol{t} = \boldsymbol{t}_1$ we get $p(\boldsymbol{t}_1) \neq 0$. Applying Lemma 10 again with $M = p(\boldsymbol{t}_1)$ we infer the existence of an integer m with the above property satisfying $\big(m, p(\boldsymbol{t}_1)\big) = 1$. However now by the assumption there exist an $i \leqslant I$, a $\boldsymbol{t}_2 \equiv \boldsymbol{t}_1 \bmod m$ and $x, y \in \mathbb{Q}$ such that (77) holds. By the fundamental property of resultants we have

$$R_i(\boldsymbol{t}, x) = 0 = S_i(\boldsymbol{t}, y)$$

and in view of (78), (79), (81) and (82) there exist ϱ, σ such that $1 \leqslant \varrho \leqslant r_i$, $1 \leqslant \sigma \leqslant s_i$,

$$x = R_{i\varrho}(\boldsymbol{t}_2), \quad y = S_{i\sigma}(\boldsymbol{t}_2).$$

It follows from (77) and (80) that

$$T_{i\varrho\sigma}(\boldsymbol{t}_2) = 0,$$

contrary to (81) and (82). □

Remark. Lemma 11 extends to any system of forms $G_1, \ldots, G_k \in \mathbb{Q}[x_1, \ldots, x_k]$ without a common non-trivial zero.

Proof of Theorem 3. If $f = 0$ the theorem is trivially true. If $f \neq 0$ let $f(\boldsymbol{t}_0) = e \neq 0$. We set $f_0(\boldsymbol{t}) = f(e\boldsymbol{t} + \boldsymbol{t}_0)$ and find as in the proof of Corollary to Lemma 3 that the fixed divisor of $f_0(\boldsymbol{t})$ equals $C(f_0)$. (If the fixed divisor of f equals $C(f)$ we can take directly $e = 1$, $\boldsymbol{t}_0 = \boldsymbol{0}$.) Let $\boldsymbol{K}$ be the least field over which F factorizes into two coprime factors
c G, H and let

(83) $$f_0(\boldsymbol{t}) = l \prod_{\nu=1}^{n} \varphi_\nu(\boldsymbol{t})^{e_\nu}$$

be a factorization of f over $\boldsymbol{K}$ into irreducible factors such that φ_ν are distinct and have the coefficient of the first term in the inverse lexicographical order equal to 1. Since the fixed divisor of $f_0(\boldsymbol{t})$ equals $C(f_0)$ the polynomials φ_ν satisfy (19) in virtue of Lemma 9. Let $\mu, \boldsymbol{\tau}$ be parameters whose existence for $\{\varphi_\nu\}$ and $\mu = 1$ is asserted in Lemma 5 and let

$$\psi_\nu = \varphi_\nu(\mu\boldsymbol{t} + \boldsymbol{\tau}) \quad (1 \leqslant \nu \leqslant n).$$

It follows that

$$f_0(\mu \boldsymbol{t} + \boldsymbol{\tau}) = l \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t})^{e_\nu} \tag{84}$$

and

$$B = |l| \prod_{\nu=1}^{n} C(\psi_\nu)^{e_\nu} = C\big(f_0(\mu \boldsymbol{t} + \boldsymbol{\tau})\big) \in \mathbb{N}, \tag{85}$$

where an ideal in $\mathbb{Q}$ is identified with its positive generator. Consider first the case where $\boldsymbol{K} = \mathbb{Q}$ and let

$$f_0(\mu \boldsymbol{t} + \boldsymbol{\tau}) = g_i(\boldsymbol{t}) h_i(\boldsymbol{t}) \quad (1 \leqslant i \leqslant I) \tag{86}$$

be all possible factorizations of the left hand side into two factors with integral coefficients. H implies that if $\big(m,\ f_0(\mu \boldsymbol{t}_1 + \boldsymbol{\tau})\big) = 1$ there exist an $i \leqslant I$, a $\boldsymbol{t}_2 \equiv \boldsymbol{t}_1 \bmod m$ and $x, y \in \mathbb{Z}$ such that

$$G(x, y) = g_i(\boldsymbol{t}_2), \quad H(x, y) = h_i(\boldsymbol{t}_2). \tag{87}$$

Indeed, by (84) and (85), the condition $\big(m,\ f_0(\mu \boldsymbol{t}_1 + \boldsymbol{\tau})\big) = 1$ implies

$$\left(m, \prod_{\nu=1}^{n} \frac{\psi_\nu(\boldsymbol{t}_1)}{C(\psi_\nu)}\right) = 1$$

and, by Lemma 5, H implies the existence of a $\boldsymbol{t}_2 \in \mathbb{Z}^r$, $\boldsymbol{t}_2 \equiv \boldsymbol{t}_1 \bmod m$ such that $\dfrac{|\psi_\nu(\boldsymbol{t}_2)|}{C(\psi_\nu)}$ $(\nu \leqslant n)$ are distinct primes not dividing B. By the assumption of D there exist $x, y \in \mathbb{Z}$ such that

$$G(x, y) H(x, y) = F(x, y) = f_0(\mu \boldsymbol{t}_2 + \boldsymbol{\tau})$$

and it follows from (84) and (85) that for some $a, b, \alpha_\nu, \beta_\nu \in \mathbb{Z}$, $\alpha_\nu \geqslant 0$, $\beta_\nu \geqslant 0$, we have

$$G(x, y) = a \prod_{\nu=1}^{n} \Big(\frac{\psi_\nu(\boldsymbol{t}_2)}{C(\psi_\nu)}\Big)^{\alpha_\nu}, \quad H(x, y) = b \prod_{\nu=1}^{n} \Big(\frac{\psi_\nu(\boldsymbol{t}_2)}{C(\psi_\nu)}\Big)^{\beta_\nu},$$
$$ab = B \operatorname{sgn} l, \quad \alpha_\nu + \beta_\nu = e_\nu \quad (1 \leqslant \nu \leqslant n).$$

Taking

$$g_i(\boldsymbol{t}) = a \prod_{\nu=1}^{n} \Big(\frac{\psi_\nu(\boldsymbol{t})}{C(\psi_\nu)}\Big)^{\alpha_\nu}, \quad h_i(\boldsymbol{t}) = b \prod_{\nu=1}^{n} \Big(\frac{\psi_\nu(\boldsymbol{t})}{C(\psi_\nu)}\Big)^{\beta_\nu}$$

we get (86) and (87). Now we apply Lemma 11 with $p(\boldsymbol{t}) = f_0(\mu \boldsymbol{t} + \boldsymbol{\tau})$ and we get the existence of $X_0, Y_0 \in \mathbb{Q}[\boldsymbol{t}]$ satisfying

$$G(X_0, Y_0) = g_j, \quad H(X_0, Y_0) = h_j$$

for some $j \leqslant I$. Setting

$$X(\boldsymbol{t}) = X_0\Big(\frac{\boldsymbol{t} - e\boldsymbol{\tau} - \boldsymbol{t}_0}{e\mu}\Big), \quad Y(\boldsymbol{t}) = Y_0\Big(\frac{\boldsymbol{t} - e\boldsymbol{\tau} - \boldsymbol{t}_0}{e\mu}\Big), \tag{88}$$

we get by (86)

$$F\big(X(\boldsymbol{t}), Y(\boldsymbol{t})\big) = g_j\Big(\frac{\boldsymbol{t} - e\boldsymbol{\tau} - \boldsymbol{t}_0}{e\mu}\Big) h_j\Big(\frac{\boldsymbol{t} - e\boldsymbol{\tau} - \boldsymbol{t}_0}{e\mu}\Big) = f_0\Big(\frac{\boldsymbol{t} - \boldsymbol{t}_0}{e}\Big) = f(\boldsymbol{t}).$$

Consider now the case where $\boldsymbol{K}$ is an imaginary quadratic field with discriminant Δ. Then

$$F(x, y) = \frac{v}{w} N\Phi(x, y), \tag{89}$$

where $v, w \in \mathbb{Z}$, $(v, w) = 1$, $\Phi \in \boldsymbol{K}[x, y]$ has integral coefficients and

$$\big(\Phi(x, y), \Phi'(x, y)\big) = 1, \tag{90}$$

where Φ' is conjugate to Φ over $\mathbb{Q}(x, y)$. Let

$$\frac{w}{v} f_0(\mu\boldsymbol{t} + \boldsymbol{\tau}) = \eta_i \eta_i'(\boldsymbol{t}) \quad (i \leqslant I) \tag{91}$$

be all the factorizations of the left hand side into two conjugate polynomials with integral coefficients in $\boldsymbol{K}$. Since $\boldsymbol{K}$ has finitely many units the number of such factorizations is finite. H implies that if $\big(m, \Delta f_0(\mu\boldsymbol{t}_1 + \boldsymbol{\tau})\big) = 1$ there exist an $i \leqslant I$, a $\boldsymbol{t}_2 \equiv \boldsymbol{t}_1 \bmod m$ and $x, y \in \mathbb{Z}$ such that

$$\Phi(x, y) = \eta_i(\boldsymbol{t}_2). \tag{92}$$

Indeed, by (84) and (85), we have

$$\Big(\frac{w}{v} f_0(\mu\boldsymbol{t} + \boldsymbol{\tau})\Big) = \Big(\frac{w}{v} B\Big) \prod_{\nu=1}^{n} \frac{\big(\psi_\nu(\boldsymbol{t})\big)^{e_\nu}}{C(\psi_\nu)^{e_\nu}}. \tag{93}$$

Since, by Lemma 5, $\prod_{\nu=1}^{n} \dfrac{N\psi_\nu(\boldsymbol{t})}{NC(\psi_\nu)}$ has the fixed divisor 1, $\prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t})^{e_\nu}$ has the fixed divisor $\prod_{\nu=1}^{n} C(\psi_\nu)^{e_\nu}$. On the other hand, for every $\boldsymbol{t} \in \mathbb{Z}^r$

$$\frac{w}{v} f_0(\mu\boldsymbol{t} + \boldsymbol{\tau}) = N\Phi(x, y) \in \mathbb{Z},$$

hence

$$\frac{w}{v} A \in \mathbb{Z}. \tag{94}$$

By (84) and (85) the condition $\big(m, \Delta f_0(\mu\boldsymbol{t}_1 + \boldsymbol{\tau})\big) = 1$ implies

$$\Big(m, \Delta \prod_{\nu=1}^{n} \frac{N\psi_\nu(\boldsymbol{t}_1)}{NC(\psi_\nu)}\Big) = 1$$

and, by Lemma 5, H implies the existence of a $\boldsymbol{t}_2 \equiv \boldsymbol{t}_1 \bmod m$ such that $\dfrac{\big(\psi_\nu(\boldsymbol{t}_2)\big)}{C(\psi_\nu)}$ $(\nu \leqslant n)$

are distinct prime ideals not dividing wB. By the assumption of D there exist $x_0, y_0 \in \mathbb{Z}$ such that

$$N\Phi(x_0, y_0) = \frac{w}{v} F(x_0, y_0) = \frac{w}{v} f(\mu \boldsymbol{t}_2 + \boldsymbol{\tau}) \tag{95}$$

and it follows from (93) and (94) that for an integral ideal $\mathfrak{b}$ and some integers $\alpha_\nu \geqslant 0$

$$\big(\Phi(x_0, y_0)\big) = \mathfrak{b} \prod_{\nu=1}^{n} \frac{\big(\psi_\nu(\boldsymbol{t}_2)\big)^{\alpha_\nu}}{C(\psi_\nu)^{\alpha_\nu}}, \quad \left(\mathfrak{b}, \prod_{\nu=1}^{n} \frac{\big(\psi_\nu(\boldsymbol{t}_2)\big)}{C(\psi_\nu)}\right) = 1.$$

On the other hand, in full analogy with (51), we can assume that for a certain $k \equiv n \bmod 2$

$$\psi'_\nu = \psi_{\nu'}, \quad e_\nu = e_{\nu'}, \quad \nu' = \nu \ (\nu \leqslant k), \quad \nu' = \nu - (-1)^{n-\nu} \ (\nu > k). \tag{96}$$

Hence

$$N\Phi(x_0, y_0) = N\mathfrak{b} \prod_{\nu=1}^{n} \left(\frac{\psi_\nu(\boldsymbol{t}_2)}{C(\psi_\nu)}\right)^{\alpha_\nu + \alpha_{\nu'}}, \quad \left(N\mathfrak{b}, \prod_{\nu=1}^{n} \frac{\big(\psi_\nu(\boldsymbol{t}_2)\big)}{C(\psi_\nu)}\right) = 1$$

and a comparison with (93) gives

$$\alpha_\nu + \alpha_{\nu'} = e_\nu \quad (1 \leqslant \nu \leqslant n). \tag{97}$$

Now let us put

$$\eta(\boldsymbol{t}) = \Phi(x_0, y_0) \prod_{\nu=1}^{n} \left(\frac{\psi_\nu(\boldsymbol{t})}{\psi_\nu(\boldsymbol{t}_2)}\right)^{\alpha_\nu}. \tag{98}$$

The polynomial $\eta(\boldsymbol{t})$ has integral coefficients in $\boldsymbol{K}$ since

$$C(\eta) = \big(\Phi(x_0, y_0)\big) \prod_{\nu=1}^{n} \frac{C(\psi_\nu)^{\alpha_\nu}}{\big(\psi_\nu(\boldsymbol{t}_2)\big)^{\alpha_\nu}} = \mathfrak{b}.$$

Moreover, by (95), (96), (97) and (84)

$$\begin{aligned}
\eta(\boldsymbol{t})\eta'(\boldsymbol{t}) &= N\Phi(x_0, y_0) \prod_{\nu=1}^{n} \left(\frac{\psi_\nu(\boldsymbol{t})\psi'_\nu(\boldsymbol{t})}{\psi_\nu(\boldsymbol{t}_2)\psi'_\nu(\boldsymbol{t}_2)}\right)^{\alpha_\nu} \\
&= \frac{w}{v} f_0(\mu \boldsymbol{t}_2 + \boldsymbol{\tau}) \prod_{\nu=1}^{n} \left(\frac{\psi_\nu(\boldsymbol{t})}{\psi_\nu(\boldsymbol{t}_2)}\right)^{\alpha_\nu + \alpha_{\nu'}} = \frac{w}{v} f_0(\mu \boldsymbol{t}_2 + \boldsymbol{\tau}) \prod_{\nu=1}^{n} \left(\frac{\psi_\nu(\boldsymbol{t})}{\psi_\nu(\boldsymbol{t}_2)}\right)^{e_\nu} \\
&= \frac{w}{v} f_0(\mu \boldsymbol{t} + \boldsymbol{\tau}).
\end{aligned}$$

Hence $\eta(\boldsymbol{t}) = \eta_i(\boldsymbol{t})$ for an $i \leqslant I$ and (92) follows immediately from (98). Now we apply Lemma 11 with $p(\boldsymbol{t}) = \Delta f_0(\mu \boldsymbol{t} + \boldsymbol{\tau})$,

$$G(x, y) = \Phi(x, y) + \Phi'(x, y), \quad H(x, y) = \big(\Phi(x, y) - \Phi'(x, y)\big)/\sqrt{\Delta}$$

and we get the existence of $X_0, Y_0 \in \mathbb{Q}[\boldsymbol{t}]$ satisfying

$$\Phi(X_0, Y_0) = \eta_j, \quad \Phi'(X_0, Y_0) = \eta'_j \tag{99}$$

for a $j \leqslant I$. Using again the transformation (88) we get by (89) and (90)

$$F\big(X(\boldsymbol{t}), Y(\boldsymbol{t})\big) = \frac{w}{v}\,\eta_j\Big(\frac{\boldsymbol{t} - e\boldsymbol{\tau} - \boldsymbol{t}_0}{e\mu}\Big)\eta_j'\Big(\frac{\boldsymbol{t} - e\boldsymbol{\tau} - \boldsymbol{t}_0}{e\mu}\Big) = \frac{w}{v}\,f_0\Big(\frac{\boldsymbol{t} - \boldsymbol{t}_0}{e}\Big) = f(\boldsymbol{t}). \quad \square$$

Lemma 12. *Let $k \in \mathbb{N}$ be odd, $a_i(\boldsymbol{t}) \in \mathbb{Z}[\boldsymbol{t}]$ $(0 \leqslant i \leqslant k)$, $a_0(\boldsymbol{t}) = 1$, $x(\boldsymbol{t}) \in \mathbb{Q}[\boldsymbol{t}]$. If*

$$\sum_{i=0}^{k-1} \binom{k}{i+1} a_i(\boldsymbol{t}) x(\boldsymbol{t})^{k-1-i} = 0 \tag{100}$$

then $x(\boldsymbol{t}) \in \mathbb{Z}[\boldsymbol{t}]$.

Proof. Suppose that $C(x) \notin \mathbb{Z}$. Then for some prime p

$$\operatorname{ord}_p C(x) = -c \leqslant -1.$$

The function $\operatorname{ord}_p C(P)$ is a valuation of the ring $\mathbb{Q}[\boldsymbol{t}]$ (see [6], p. 171). In virtue of the properties of valuations (100) implies

$$\operatorname{ord}_p\big(kC(x)^{k-1}\big) \geqslant \min_{0<i<k} \operatorname{ord}_p\left(\binom{k}{i+1} C(a_i) C(x)^{k-1-i}\right),$$

hence for a positive $i < k$

$$\operatorname{ord}_p k - (k-1)c \geqslant \operatorname{ord}_p \binom{k}{i+1} - (k-1-i)c$$

and

$$\operatorname{ord}_p k \geqslant \operatorname{ord}_p \binom{k}{i+1} + i. \tag{101}$$

However

$$\binom{k}{i+1} = \frac{k}{i+1}\binom{k-1}{i}$$

thus (101) implies

$$\operatorname{ord}_p(i+1) \geqslant i, \quad i+1 \geqslant p^i; \quad p = 2,$$

which is impossible since then the left hand side of (101) is 0. $\square$

Proof of Theorem 4. Let $n = 2^\alpha k$, k odd. In order to prove the first part of the theorem let us assume that the fixed divisor of f equals $C(f)$ and take in the proof of Theorem 3 $f_0 = f$. If $k > 1$ we take further $\boldsymbol{K} = \mathbb{Q}$, $\mu = 1$, $\boldsymbol{\tau} = \boldsymbol{0}$,

$$G(x, y) = x^{2^\alpha} + y^{2^\alpha}, \quad H(x, y) = \sum_{i+j=k-1} x^{2^\alpha i}\big(-y^{2^\alpha}\big)^j$$

and we get from (86) and (88) that for some polynomials $g, h \in \mathbb{Z}[\boldsymbol{t}]$ and $X, Y \in \mathbb{Q}[\boldsymbol{t}]$

$$\begin{gathered} g(\boldsymbol{t})h(\boldsymbol{t}) = f(\boldsymbol{t}), \\ G(X, Y) = g, \quad H(X, Y) = h. \end{gathered} \tag{102}$$

However

$$H(X,Y)=\sum_{i=0}^{k-1}\binom{k}{i+1}G(X,Y)^i(-X^{2^\alpha})^{k-1-i}$$

hence taking in Lemma 12

$$a_i(\boldsymbol{t})=g(\boldsymbol{t})^i\quad(0\leqslant i<k-1),\quad a_{k-1}(\boldsymbol{t})=-h(\boldsymbol{t}),\quad x(\boldsymbol{t})=-X(\boldsymbol{t})^{2^\alpha}$$

we get from (102) that

$$-X(\boldsymbol{t})^{2^\alpha}\in\mathbb{Z}[\boldsymbol{t}].$$

Thus $X(\boldsymbol{t})\in\mathbb{Z}[\boldsymbol{t}]$ and by symmetry $Y(\boldsymbol{t})\in\mathbb{Z}[\boldsymbol{t}]$. Moreover

$$X(\boldsymbol{t})^n+Y(\boldsymbol{t})^n=G(X,Y)H(X,Y)=f(\boldsymbol{t}).$$

If $k=1$ we take in the proof of Theorem 3 $\boldsymbol{K}=\mathbb{Q}(\zeta_4)$,

$$\Phi(x,y)=x^{2^{\alpha-1}}+\zeta_4 y^{2^{\alpha-1}},\quad v/w=1, \tag{103}$$

where ζ_q is a primitive q-th root of unity.

By Lemma 5 μ factorizes over $\boldsymbol{K}$ into prime ideals of degree 2. By (92) and (99) for some polynomials $\eta\in\mathbb{Z}[\zeta_4,\boldsymbol{t}]$ and $X_0,Y_0\in\mathbb{Q}[\boldsymbol{t}]$

$$\eta(\boldsymbol{t})\eta'(\boldsymbol{t})=f(\mu\boldsymbol{t}+\boldsymbol{\tau}),\quad \eta'\text{ conjugate to }\eta\text{ over }\mathbb{Q}(\boldsymbol{t}), \tag{104}$$

$$\Phi\big(X_0(\boldsymbol{t}),Y_0(\boldsymbol{t})\big)=\eta(\boldsymbol{t}). \tag{105}$$

Let us set

$$\vartheta(\boldsymbol{t})=\eta\Big(\frac{\boldsymbol{t}-\boldsymbol{\tau}}{\mu}\Big),\quad X(\boldsymbol{t})=X_0\Big(\frac{\boldsymbol{t}-\boldsymbol{\tau}}{\mu}\Big),\quad Y(\boldsymbol{t})=Y_0\Big(\frac{\boldsymbol{t}-\boldsymbol{\tau}}{\mu}\Big). \tag{106}$$

We have

$$\mu^{|\eta|}\vartheta(\boldsymbol{t})\in\mathbb{Z}[\zeta_4,\boldsymbol{t}]$$

hence, if $\mathfrak{p}$ is a prime ideal of $\boldsymbol{K}$ in the denominator of $C(\vartheta)$, $\mathfrak{p}\mid\mu$ and $\mathfrak{p}=\mathfrak{p}'$. However by (104)

$$\vartheta(\boldsymbol{t})\vartheta'(\boldsymbol{t})=f(\boldsymbol{t}),\quad NC(\vartheta)=C(f)\in\mathbb{Z}$$

hence $\operatorname{ord}_{\mathfrak{p}}C(\vartheta)=\frac{1}{2}\operatorname{ord}_{\mathfrak{p}}C(f)\geqslant 0$ and

$$\vartheta(\boldsymbol{t})\in\mathbb{Z}[\zeta_4,\boldsymbol{t}].$$

Now (103), (105) and (106) imply

$$X(\boldsymbol{t})^{2^{\alpha-1}},Y(\boldsymbol{t})^{2^{\alpha-1}}\in\mathbb{Z}[\boldsymbol{t}];\quad X(\boldsymbol{t}),Y(\boldsymbol{t})\in\mathbb{Z}[\boldsymbol{t}]$$

and we get by (104)

$$X(\boldsymbol{t})^{2^\alpha}+Y(\boldsymbol{t})^{2^\alpha}=f(\boldsymbol{t}).$$

The proof of the first part of the theorem is complete. In order to prove the second part it is enough to consider the case $n>2$ (for $n=2$ the assertion is contained in Theorem 1).

Let p be a prime satisfying

$$p \equiv 1 \bmod 2^{\alpha+1}, \quad p \not\equiv 1 \bmod 2n \quad \text{if} \quad n \neq 2^{\alpha} \tag{107}$$

and let us choose an integer c such that

$$c^n + 1 \equiv 0 \bmod p^n, \quad c = -1 \quad \text{if} \quad \alpha = 0.$$

Consider now the polynomial

$$f(t) = u(t)^n + v(t)^n, \tag{108}$$

where

$$u(t) = \frac{t(t-1)\cdots(t-p+1)}{p}, \quad v(t) = cu(t) + p^{n-1}.$$

It is easily seen that $f(t) \in \mathbb{Z}[t]$ and

$$|f| = \begin{cases} pn & \text{if } \alpha > 0, \\ p(n-1) & \text{if } \alpha = 0. \end{cases} \tag{109}$$

c

Moreover, since polynomials $u(t)$, $v(t)$ are integer-valued the equation $x^n + y^n = f(t)$ is soluble in $x, y \in \mathbb{Z}$ for all $t \in \mathbb{Z}$. On the other hand, suppose that

$$X(t)^n + Y(t)^n = f(t), \quad X, Y \in \mathbb{Z}[\boldsymbol{t}]. \tag{110}$$

Since

$$X(t)^n + Y(t)^n = \prod_{i=0}^{n-1} \left(X(t) - \zeta_{2n}^{2i+1} Y(t)\right)$$

we have

$$|f| \geqslant \begin{cases} n \max\{|X|, |Y|\} & \text{if } \alpha > 0, \\ (n-1) \max\{|X|, |Y|\} & \text{if } \alpha = 0. \end{cases}$$

Hence by (109)

$$\max\{|X|, |Y|\} \leqslant p. \tag{111}$$

Taking $i = 0, 1, \ldots, p-1$ we get $u(i) = 0$ hence

$$X(i)^n + Y(i)^n = p^{n(n-1)}. \tag{112}$$

If $n = 2^{\alpha}$, $\alpha > 1$ or $n = 3$ by special cases of Fermat's last theorem (111) implies

$$X(i)Y(i) = 0 \quad (0 \leqslant i < p). \tag{113}$$

If $n > 3$, by Zsigmondy's theorem either $X(i)Y(i) = 0$ or $X(i) = \pm Y(i)$ or $X(i)^n + Y(i)^n$ has the so-called primitive prime factor $\equiv 1 \bmod 2n$. The last two possibilities are incompatible with (107) and (112) hence (113) holds for all $n > 2$. By (112) if $X(i) = 0$, $Y(i) = p^{n-1}$ for $\alpha = 0$, $Y(i) = \pm p^{n-1}$ for $\alpha > 0$. In view of symmetry between X and Y we may assume that there is a set $S \subset \{0, 1, \ldots, p-1\}$ with the following

properties

$$|S| \geqslant \frac{p+1}{2(n,2)}, \quad X(i) = 0, \quad Y(i) = p^{n-1} \quad \text{for } i \in S.$$

(If n is even we can replace Y by $-Y$.) Let

$$P(t) = \prod_{i \in S} (t - i).$$

It follows that

$$|P| \geqslant \frac{p+1}{2(n,2)}, \quad X(t) \equiv 0 \bmod P(t), \quad Y(t) \equiv p^{n-1} \bmod P(t) \tag{114}$$

and we get from (108) and (110)

$$Y(t)^n \equiv v(t)^n \bmod P(t)^n.$$

Since $Y(t) \equiv v(t) \bmod P(t)$ and $(v, P) = 1$ we obtain

$$Y(t) \equiv v(t) \bmod P(t)^n.$$

However by (111)

$$\max\{|Y|, |v|\} \leqslant p < n|P|$$

hence

$$Y(t) = v(t) \notin \mathbb{Z}[t]. \qquad \square$$

References

[1] P. T. Bateman, R. A. Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers*. Math. Comp. 16 (1962), 363–367.

[2] A. Châtelet, *Leçons sur la théorie des nombres*. Paris 1913.

[3] S. Chowla, *Some problems of elementary number theory*. J. Reine Angew. Math. 222 (1966), 71–74.

[4] H. Davenport, D. J. Lewis, A. Schinzel, *Polynomials of certain special types*. Acta Arith. 9 (1964), 107–116; this collection: A6, 27–35.

[5] H. Halberstam, H.-E. Richert, *Sieve Methods*. Academic Press, London–New York 1974.

[6] H. Hasse, *Zahlentheorie*. Akademie-Verlag, Berlin 1963.

[7] T. Kojima, *Note on number-theoretical properties of algebraic functions*. Tôhoku Math. J. 8 (1915), 24–37.

[8] S. Lang, *Diophantine Geometry*. Interscience, New York–London 1962.

[9] W. J. LeVeque, *A brief survey of Diophantine equations*. In: Studies in Number Theory, Math. Assoc. Amer., Buffalo 1969, 4–24.

[10] D. Mumford, *A remark on Mordell's conjecture*. Amer. J. Math. 87 (1965), 1007–1016.

[11] P. Ribenboim, *Polynomials whose values are powers*. J. Reine Angew. Math. 268/269 (1974), 34–40.

[12] A. Schinzel, W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*. Acta Arith. 4 (1958), 185–208; *Erratum* ibid. 5 (1959), 259; this collection: J1, 1113–1133.

[13] A. Schinzel, *On Hilbert's Irreducibility Theorem*. Ann. Polon. Math. 16 (1965), 333–340; this collection: F1, 839–845.

[14] —, *On a theorem of Bauer and some of its applications* II. Acta Arith. 22 (1973), 221–231; this collection: C5, 210–220.

[15] —, *Abelian binomials, power residues and exponential congruences*. Acta Arith. 32 (1977), 245–274; this collection: H5, 939–970.

[16] —, *Addendum and corrigendum to* [15]. Ibid. 36 (1980), 101–104 (in this collection included into H5).

[17] W. M. Schmidt, *Equations over Finite Fields. An Elementary Approach*. Lecture Notes in Math. 536, Springer, Berlin 1976.

[18] Th. Skolem, *Anwendung exponentieller Kongruenzen zum Beweis der Unlösbarkeit gewisser diophantischer Gleichungen*. Vid. Akad. Avh. Oslo I 1937 nr. 12.

Part K

Analytic number theory

Commentary on K: Analytic number theory

by Jerzy Kaczorowski

1. Papers **K1** and **K4** concern the following closely related topics: values of Dirichlet L-functions at 1, class numbers of quadratic number fields, existence of the Siegel zero and character sums. Problems related to them occupy central position in number theory and attracted attention of many leading mathematicians.

Study of the ideal class group goes back to C. F. Gauss who used the language of binary quadratic forms (like in **K1**). Let d be a fundamental discriminant. Famous Dirichlet class number formula relates $h(d)$, the class number of $\mathbb{Q}(\sqrt{d})$, to $L(1, \chi_d)$, where

$$\chi_d(n) = \left(\frac{d}{n}\right)$$

is the Kronecker symbol. For instance if $d < -4$ we have

$$h(d) = \pi^{-1}\sqrt{d}L(1, \chi_d).$$

We refer to W. Narkiewicz [19] for the basic theory. The fact that the size of $L(1, \chi)$ is related to the exceptional zero was first observed by H. Hecke, who proved that if such a zero does not exist then $L(1, \chi_d) \gg (\log |d|)^{-1}$, see e.g. [17]. In particular for $d < 0$ we have then $h(d) \gg \sqrt{|d|}(\log |d|)^{-1}$. The main theorem of **K1** makes this relation very explicit, see also D. Goldfeld [10] and A. Granville, H. M. Stark [12]. E. Landau [17] introduced the idea of twisting L-functions by Dirichlet characters which proved to be very useful later on. Using it he proved that if $L(\beta, \chi) = L(\beta', \chi') = 0$ for certain real β and β' and two primitive real characters $\chi \pmod{|d|}$ and $\chi' \pmod{|d'|}$, then $\min(\beta, \beta') \leqslant 1 - c(\log(|dd'|))^{-1}$, c being a positive constant. Hence if real zeros exist they are very rare. This is a simple instance of a general repulsion principle saying roughly that if an L-function has a real zero close to 1 then for many other L-functions with comparable conductors such zeros cannot exist. This was mastered in papers by M. Deuring [7] and H. Heilbronn [16] and is known under the name the "Deuring–Heilbronn phenomenon". Yu. V. Linnik [18] exploited this in a clever way in his famous work on the least prime in an arithmetic progression. C. L. Siegel [24] proved that

$$L(1, \chi) \gg |d|^{-\varepsilon}$$

for every primitive character $\chi \pmod{|d|}$ and every positive ε. This implies that

$$h(d) \gg |d|^{1/2-\varepsilon}$$

as $d \to -\infty$. In particular, for every positive integer h_0 there are finitely many quadratic imaginary fields with the class number equal to h_0. Unfortunately Siegel's theorem is ineffective and consequently it cannot be used for determining fields with a given class number. In particular, it does not help in finding all fundamental discriminants $d < 0$ with $h(d) = 1$. This was done by K. Heegner [15] and H. M. Stark [25], who used arithmetic of elliptic curves, and independently by A. Baker [2], who used his theory of linear form in logarithms of algebraic numbers. See also [26]. Basing on ideas by J. Friedlander [9] and D. Goldfeld [11], B. Gross and D. Zagier [13] gave effective lower estimate for $h(d)$. Their method uses elliptic curves whose L-functions have central zero of the proper order. Choosing an elliptic curve of rank 3 and conductor 5077, J. Oesterlé [20] proved that for a negative fundamental discriminant

$$h(d) \geqslant \frac{1}{55} \prod_{p|d} \left(1 - \frac{2}{\sqrt{p}}\right) \log |d|.$$

Assuming the Modified Generalized Riemann Hypothesis (zeros are all on the critical line or on the real axis) lower estimates for $L(1, \chi_d)$ and $h(d)$ can be much improved, see P. Sarnak, A. Zaharescu [23]. For instance assuming MGRH for all L-functions of elliptic curves one has $L(1, \chi_d) \gg |d|^{-2/5-\varepsilon}$, where $\chi_d(37) = -1$, with an effective implied constant. Siegel's theorem can be also improved making other assumptions on the distribution of zeros of L-functions. B. Conrey and H. Iwaniec [6] proved that

$$h(d) \gg \sqrt{|d|}(\log |d|)^{-A}$$

for some constant $A > 0$ if the gap between consecutive zeros on the critical line is smaller than the average for sufficiently many pairs of zeros.

Connections between class numbers of quadratic number fields and character sums are well known. For instance if $d < -4$ is a fundamental discriminant, then

$$h(d) = -\frac{1}{|d|} \sum_{0<k<|d|} k\chi_d(k) = \frac{1}{2 - \chi_d(2)} \sum_{0<k<|d|/2} \chi_d(k),$$

see eg. [5]. In **K4** sums of type

$$\sum_{q_1|d|<n<q_2|d|} \chi_d(n) \tag{1}$$

are studied. It is known ([27]) that they can be expressed as linear combinations of generalized Bernoulli numbers. Of particular interest are cases when such a linear combination reduces just to a single term since then we have a clear expression of $h(Ed)$ for certain integer E in terms of a short sum of the form (1). As a result one obtains amazing relations, as for instance the following one

$$h(12d) = \sum_{(1/12)|d|<n<(1/10)|d|} \chi_d(n)$$

which holds for every fundamental discriminant $|d| \equiv 11$ or $59 \pmod{60}$.

2. The paper **K3** is devoted to the study of the difference

$$E(x) = \sum_{n \leqslant x} (r(n))^2 - 4x \log x - cx,$$

where c is a suitable constant and $r(n)$ stands for the number of representations of n as a sum of two squares of integers. Classical result by W. Sierpiński is that $E(x) \ll x^{3/4} \log x$ as $x \to \infty$, whereas S. Ramanujan stated without proof that $E(x) \ll x^{3/5+\varepsilon}$ for every positive ε. Up to now (2005) the best known upper estimate of $E(x)$ is still the one due to W. G. Nowak: $E(x) \ll x^{1/2}(\log x)^{8/3}(\log\log x)^{1/3}$. The main result from **K3**, saying that $E(x) = \Omega(x^{3/8})$, is the best known lower estimate of this function. The method of proof used in **K3** is an adaptation for the specific situation of the $r(n)$ function of a general method developed by R. Balasubramanian and K. Ramachandra [3] and R. Balasubramanian, K. Ramachandra and M. V. Subbarao [4] for treating omega estimates for summatory functions of coefficients of Dirichlet series satisfying appropriate analytic conditions.

3. The paper **K2** concerns a multiplicative property of the partition function $p(n)$. Classical result on $p(n)$ due to G. H. Hardy and S. Ramanujan [14] states that

$$p(n) = (4\sqrt{3}\,\lambda_n)^{-1} \exp(\pi\sqrt{2/3}\,\lambda_n) + O(\exp(\pi\sqrt{2/3}\,\lambda_n)\lambda_n^{-3}) \qquad (n \to \infty),$$

where $\lambda_n = \sqrt{n - (1/24)}$. The full asymptotic expansion was found by H. Rademacher [21]. For a variety of results concerning partition function see G. E. Andrews [1] and H. Rademacher [22].

P. Erdős and A. Ivić conjectured that $\omega(\prod_{m=1}^{N} p(m)) \to \infty$ as $N \to \infty$. This was proved by A. Schinzel, the proof appeared in [8]. Paper **K2** gives a quantitative solution of the Erdős–Ivić problem.

References

[1] G. E. Andrews, *The Theory of Partitions*. Cambridge Math. Lib., Cambridge Univ. Press, Cambridge 1998.

[2] A. Baker, *Linear forms in the logarithms of algebraic numbers* I. Mathematika 13 (1966), 204–216.

[3] R. Balasubramanian, K. Ramachandra, *Some problems of analytic number theory* III. Hardy-Ramanujan J. 4 (1981), 13–40.

[4] R. Balasubramanian, K. Ramachandra, M. V. Subbarao, *On the error function in the asymptotic formula for the counting function of k-full numbers*. Acta Arith. 50 (1988), 107–118.

[5] Z. I. Borevich, I. R. Shafarevich, *Number Theory*. Academic Press, New York 1966.

[6] B. Conrey, H. Iwaniec, *Spacing of zeros of Hecke L-functions and the class number problem*. Acta Arith. 103 (2002), 259–312.

[7] M. Deuring, *Imaginäre quadratische Zahlkörper mit der Klassenzahl* 1. Math. Z. 37 (1933), 405–415.

[8] P. Erdős, A. Ivić, *The distribution of values of a certain class of arithmetic functions at consecutive integers*. In: Number Theory, Colloq. Math. Soc. János Bolyai 51, North-Holland, Amsterdam 1990, 45–91.

[9] J. Friedlander, *On the class numbers of certain quadratic extensions*. Acta Arith. 28 (1976), 391–393.

[10] D. Goldfeld, *An asymptotic formula relating the Siegel zero and the class number of quadratic fields*. Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) 2 (1975), 611–615.

[11] —, *The class number of quadratic fields and the conjectures of Birch and Swinnerton–Dyer*. Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) 3 (1976), 624–663.

[12] A. Granville, H. M. Stark, *abc implies no "Siegel zeros" for L-functions of characters with negative discriminant*. Invent. Math. 139 (2000), 509–523.

[13] B. Gross, D. Zagier, *Heegner points and derivatives of L-series*. Invent. Math. 84 (1986), 225–320.

[14] G. H. Hardy, S. Ramanujan, *Asymptotic formulae in combinatory analysis*. Proc. London Math. Soc. (2) 17 (1918), 75–115.

[15] K. Heegner, *Diophantische Analysis und Modulfunktionen*. Math. Z. 56 (1952), 227–253.

[16] H. Heilbronn, *On the class-number in imaginary quadratic fields*. Quart. J. Math. Oxford 5 (1934), 150–160.

[17] E. Landau, *Über die Klassenzahl imaginär-quadratischer Zahlkörper*. Göttinger Nachr., 1918, 285–295.

[18] Yu. V. Linnik, *On the least prime in an arithmetic progression,* I. *The basic theorem*; II. *The Deuring-Heilbronn's phenomenon*. Mat. Sbornik (N.S.) 15 (57) (1944), 139–178 and 347–368.

[19] W. Narkiewicz, *Classical Problems in Number Theory*. PWN, Warsaw 1986.

[20] J. Oesterlé, *Nombres de classes des corps quadratiques imaginaires*. Séminaire Bourbaki, Vol. 1983/84. Astérisque 121–122 (1985), 309–323.

[21] H. Rademacher, *On the partition function* $p(n)$. Proc. London Math. Soc. (2) 43 (1937), 241–254.

[22] —, *Topics in Analytic Number Theory*. Ed. by E. Grosswald, J. Lehner and M. Newman, Die Grundlehren der mathematischen Wissenschaften 169, Springer, New York 1973.

[23] P. Sarnak, A. Zaharescu, *Some remarks on Landau-Siegel zeros*. Duke Math. J. 111 (2002), 495–507.

[24] C. L. Siegel, *Über die Classenzahl quadratischer Zahlkörper*. Acta Arith. 1 (1935), 83–86.

[25] H. M. Stark, *A complete determination of the complex quadratic fields of class-number one*. Michigan Math. J. 14 (1967), 1–27.

[26] —, *A historical note on complex quadratic fields with class number one*. Proc. Amer. Math. Soc. 21 (1969), 254–255.

[27] J. Szmidt, J. Urbanowicz, D. Zagier, *Congruences among generalized Bernoulli numbers*. Acta Arith. 71 (1995), 273–278.

Originally published in
Annali Scuola Normale Superiore – Pisa
Classe di Scienze, Serie IV 2 (1975), 571–583

On Siegel's zero

with D. M. Goldfeld (*Pisa*)

1.

Let d be fundamental discriminant, and let

$$\chi(n) = \left(\frac{d}{n}\right) \quad \text{(Kronecker's symbol)}.$$

It is well known (see [1]) that $L(s, \chi)$ has at most one zero β in the interval $(1 - c_1/\log|d|, 1)$ where c_1 is an absolute positive constant. The main aim of this paper is to prove

Theorem 1. *Let d, χ and β have the meaning defined above. Then the following asymptotic relation holds*

$$1 - \beta = \frac{6}{\pi^2}\,\frac{L(1,\chi)}{\sum' 1/a}\left(1 + O\Big(\frac{(\log\log|d|)^2}{\log|d|}\Big) + O\big((1-\beta)\log|d|\big)\right) \tag{1}$$

where $\sum'$ is taken over all quadratic forms (a, b, c) of discriminant d such that

$$-a < b \leqslant a < \tfrac{1}{4}\sqrt{|d|}, \tag{2}$$

and the constants in the O-symbols are effectively computable.

In order to apply the above theorem we need some information about the size of the sum $\sum' 1/a$. This is supplied by the following.

Theorem 2. *If (a, b, c) runs through a class C of properly equivalent primitive forms of discriminant d, supposed fundamental, then*

$$\sum_{\substack{\frac{1}{4}\sqrt{|d|}\geqslant|a|\geqslant b>-|a| \\ (a,b,c)\in C}} \frac{1}{|a|} \leqslant \begin{cases} \dfrac{1}{m_0} & \text{if } d < 0, \\[2ex] \dfrac{\log\varepsilon_0}{\log\big(\frac{1}{2}\sqrt{d}-1\big)} + \dfrac{4}{\sqrt{d}} & \text{if } d > 676, \end{cases}$$

where m_0 is the least positive integer represented by C and ε_0 is the least totally positive unit of the field $\mathbb{Q}\big(\sqrt{d}\big)$.

Theorems 1 and 2 together imply

Corollary. *For any $\eta > 0$ and $|d| > c(\eta)$ (d fundamental) we have*

$$1 - \beta \geqslant \begin{cases} \left(\frac{6}{\pi} - \eta\right)\frac{1}{\sqrt{|d|}} & \text{if } d < 0, \\ \left(\frac{6}{\pi^2} - \eta\right)\frac{\log d}{\sqrt{|d|}} & \text{if } d > 0, \end{cases}$$

where $c(\eta)$ is an effectively computable constant.

Remark. In the case $d < 0$, the constant $6/\pi$ could be improved by using the knowledge of all fields with class number $\leqslant 2$.

Similar inequalities with $6/\pi$ and $6/\pi^2$ replaced by unspecified positive constants have been claimed by Haneke [3], however, as pointed out by Pintz [8], Haneke's proof is defective and when corrected gives inequalities weaker by a factor $\log\log|d|$. Pintz himself has proved the first inequality of the corollary with the constant $6/\pi$ replaced by $12/\pi$ (see [8]).

For $d < 0$, the first named author [2] has obtained (1) with a better error term by an entirely different method. M. Huxley has also found a proof in the case $d < 0$ by a more elementary method different, however, from the method of the present paper.

The authors wish to thank Scuola Normale Superiore which gave them the opportunity for this joint work.

2.

The proofs of Theorems 1 and 2 are based on several lemmata.

Lemma 1. *Let $f(d) = (\log|d|/\log\log|d|)^2$. Then*

$$\sum_{N\mathfrak{a} \leqslant \frac{1}{4}\sqrt{|d|}f(d)} \frac{1}{N\mathfrak{a}} = \frac{\pi^2}{6}\sum{}' \frac{1}{a}\left(1 + O\left(\frac{(\log\log|d|)^2}{\log|d|}\right)\right),$$

where the left hand sum goes over all ideals $\mathfrak{a} \in \mathbb{Q}(\sqrt{d})$ with norm $\leqslant \frac{1}{4}\sqrt{|d|}f(d)$ and the constant in the O-symbol is effectively computable.

Proof. Every ideal $\mathfrak{a}$ of $\mathbb{Q}(\sqrt{d})$ can be represented in the form

$$\mathfrak{a} = u\left[a, \frac{b + \sqrt{d}}{2}\right]$$

where u, a are positive integers and $b^2 \equiv d \pmod{4a}$ (see [5], Theorem 59). If we impose the condition that

$$-a < b \leqslant a$$

then the representation becomes unique. Since $N\mathfrak{a} = u^2 a$, it follows that

$$\sum_{N\mathfrak{a} \leqslant \frac{1}{4}\sqrt{|d|} f(d)} \frac{1}{N\mathfrak{a}} = \sum{}' \frac{1}{a} \sum_{1 \leqslant u^2 \leqslant \sqrt{|d|} f(d)/4a} \frac{1}{u^2} + O\Bigg(\sum_{\frac{1}{4}\sqrt{|d|} < a < \frac{1}{4}\sqrt{|d|} f(d)} \frac{1}{a} \Bigg) \tag{3}$$

$$= \sum{}' \frac{1}{a} \Big(\frac{\pi^2}{6} + O\big((f(d))^{-1/2}\big) \Big) + O(S).$$

To estimate the sum S, we divide it into two sums S_1 and S_2. In the sum S_1, we gather all the terms $1/a$ such that a has at least one prime power factor

$$p^\alpha > l(d) = d^{1/21 \log\log |d|},$$
$$p^\alpha \mid a,$$

and in S_2 all the other terms.

Let $\nu(a)$ be the number of representations of a as $N\mathfrak{a}$ where $\mathfrak{a}$ has no rational integer divisor > 1. Then $\nu(a)$ is a multiplicative function satisfying

$$\nu(p^\alpha) = \begin{cases} 1 + \left(\dfrac{d}{p^\alpha}\right) & \text{if } p \nmid d \text{ or } \alpha = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Clearly

$$S_1 \leqslant \sum{}' \frac{1}{a} \sum{}'' \nu(p^\alpha) p^{-\alpha} \leqslant \sum{}' \frac{1}{a} \sum{}'' 2p^{-\alpha}$$

where $\sum''$ goes over all prime powers p^α with

$$\max\big(l(d), \sqrt{|d|}/4a\big) < p^\alpha \leqslant \sqrt{|d|} f(d)/4a.$$

Now, by a well known result of Mertens

$$\sum_{p^\alpha < x} p^{-\alpha} = \log\log x + c + O\big((\log x)^{-1}\big)$$

where c is a constant.

Hence

$$\sum_{x < p^\alpha < y} = \log\Big(\frac{\log y}{\log x}\Big) + O\big((\log x)^{-1}\big)$$
$$\leqslant \frac{\log y}{\log x} - 1 + O\big((\log x)^{-1}\big)$$
$$= \frac{\log y/x + O(1)}{\log x}.$$

This gives

$$\sum{}'' p^{-\alpha} \leqslant \frac{\log f(d) + O(1)}{\log l(d)} \ll \frac{(\log\log |d|)^2}{\log |d|}$$

c

and we get

$$S_1 = O\left(\frac{(\log\log|d|)^2}{\log|d|}\right)\sum{}' \frac{1}{a}. \tag{4}$$

To estimate S_2, we notice that each a occurring in it must have at least

$$k_0 = \left\lceil \frac{\log\left(\frac{1}{4}\sqrt{|d|}\right)}{\log l(d)} \right\rceil \geqslant 10\log\log|d|$$

distinct prime factors. Therefore

$$S_2 \leqslant \sum_{k\geqslant k_0} (1/k!)\left(\sum_{p^\alpha < l(d)} \nu(p^\alpha)p^{-\alpha}\right)^k < (1/k_0!)\sigma^{k_0}e^\sigma$$

where

$$\begin{aligned}\sigma &= \sum_{p^\alpha < l(d)} \nu(p^\alpha)p^{-\alpha} < 2\log\log l(d) + O(1)\\ &= 2\log\log|d| + O(1).\end{aligned}$$

Now, Stirling's formula gives $k_0! > k_0^{k_0}\exp(-k_0)$. Hence

$$\begin{aligned}\log S_2 &\leqslant -k_0\log k_0 + k_0\big((\log\sigma)+1\big) + \sigma\\ &\leqslant -k_0\big(\log 10 + \log\log\log|d| - \log 2 - \log\log\log|d| - 1\big) + \sigma\\ &< -3\log\log|d| + O(1)\end{aligned}$$

and

$$S_2 = O\big((\log|d|)^{-3}\big). \tag{5}$$

The lemma now follows from equations (3), (4) and (5). □

The next lemma gives the growth conditions for the Riemann zeta-function and Dirichlet L-functions on the imaginary axis.

Lemma 2. *For all real t*

$$|\zeta(it)| \ll \big(|t|^{1/2}+1\big)\log\big(|t|+2\big) \tag{6}$$

$$|L(it,\chi)| \ll \sqrt{|d|}\big(|t|^{1/2}+1\big)\log\big(|d|(|t|+2)\big). \tag{7}$$

Proof. If $|t| > t_0$, the estimate

$$|\zeta(it)| \ll |t|^{1/2}\log|t|$$

holds (see [10], p. 19). Since $\zeta(s)$ has no pole on the imaginary axis, we have

$$|\zeta(it)| \ll 1 \quad \text{for} \quad |t| \leqslant t_0$$

and the inequality (6) now follows.

To prove (7), we note that

$$|L(1-it,\chi)| \ll \log\bigl(|d|(|t|+2)\bigr)$$

(see [1], p. 17, Lemma 2 with $q=|d|$, $x=2|d|(|t|+2)$).

Now, by the fundamental equation for L-functions

$$|L(it,\chi)| = |L(1-it,\chi)|\,|d|^{1/2}\bigl|\Gamma(\tfrac{1}{2}it+A)\Gamma^{-1}(\tfrac{1}{2}-\tfrac{1}{2}it+A)\bigr|$$

where

$$A = \tfrac{1}{4}\bigl(1-\chi(-1)\bigr).$$

Using the formula

$$|\Gamma(s)| = \sqrt{2\pi}\,|t|^{\sigma-1/2}\exp(-\tfrac{1}{2}\pi t)\bigl(1+O(|t|^{-1})\bigr)$$

valid for $s=\sigma+it$, $0\leqslant\sigma\leqslant\frac{1}{2}$, $|t|>1$ (see [9], p. 395), equation (7) follows, upon noting that

$$\bigl|\Gamma(\tfrac{1}{2}t+A)\Gamma^{-1}(\tfrac{1}{2}-\tfrac{1}{2}t+A)\bigr| \ll 1 \quad \text{for} \quad |t|<1. \qquad \square$$

Proof of Theorem 1. By the standard argument ([4], p. 31)

$$\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\frac{y^s}{s(s+2)(s+3)}\,ds = \begin{cases}\dfrac{1}{6}-\dfrac{y^{-2}}{2}+\dfrac{y^{-3}}{3} & \text{if } y\geqslant 1,\\[2mm] 0 & \text{if } 0<y<1.\end{cases}$$

Since for $\mathrm{Re}(s)>1$

$$\zeta(s)L(s,\chi) = \sum(N\mathfrak{a})^{-s},$$

it follows that for any $x>0$

$$\begin{aligned} I &= \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\zeta(s+\beta)L(s+\beta,\chi)\,\frac{x^s}{s(s+2)(s+3)}\,ds\\ &= \sum_{N\mathfrak{a}\leqslant x}(N\mathfrak{a})^{-\beta}\left(\frac{1}{6}-\frac{(N\mathfrak{a})^2}{2x^2}+\frac{(N\mathfrak{a})^3}{3x^3}\right).\end{aligned}$$

c

Choose $x=\frac{1}{4}\sqrt{|d|}\,f(d)$ with $f(d)=\bigl(\log|d|/\log\log|d|\bigr)^2$.

If $N\mathfrak{a}\leqslant x$, we have

$$(N\mathfrak{a})^{-\beta} = (N\mathfrak{a})^{-1}\bigl(1+O((1-\beta)\log|d|)\bigr).$$

Hence

$$\begin{aligned} I = {}& \frac{1}{6}\sum_{N\mathfrak{a}\leqslant x}(N\mathfrak{a})^{-1}\bigl(1+O((1-\beta)\log|d|)\bigr)\\ &+ O\left(\sum_{N\mathfrak{a}\leqslant x/f(d)}(N\mathfrak{a})^{-1}f(d)^{-2}\right)+O\left(\sum_{x/f(d)\leqslant N\mathfrak{a}\leqslant x}(N\mathfrak{a})^{-1}\right),\end{aligned}$$

and by Lemma 1 (cf. formula (3))

$$I = \frac{1}{6}\sum{}' \frac{1}{a}\Big(1 + O\Big(\frac{(\log\log|d|)^2}{\log|d|}\Big) + O\big((1-\beta)\log|d|\big)\Big). \tag{8}$$

On the other hand, after shifting the line of integration to $\mathrm{Re}(s) = -\beta$

$$I = \frac{L(1,\chi)x^{1-\beta}}{(1-\beta)(3-\beta)(4-\beta)} + \frac{1}{2\pi i}\int_{-\beta-i\infty}^{-\beta+i\infty} \zeta(s+\beta)L(s+\beta,\chi)\,\frac{x^s}{s(s+2)(s+3)}\,ds. \tag{9}$$

By Lemma 2, the integral on the right does not exceed

$$O\big(x^{-\beta}\sqrt{|d|}\log|d|\big)$$

and since

$$x^{1-\beta} = 1 + O\big((1-\beta)\log|d|\big)$$
$$(3-\beta)(4-\beta) = 6 + O(1-\beta)$$

we get from (8) and (9)

$$1 - \beta = \frac{6}{\pi^2}\,\frac{L(1,\chi)}{\sum' 1/a}\Big(1 + O\Big(\frac{(\log\log|d|)^2}{\log|d|}\Big) + O\big((1-\beta)\log|d|\big)\Big). \qquad \square$$

3.

Proof of Theorem 2. For $d < 0$ it is enough to prove that every class contains at most one form satisfying

$$-|a| < b \leqslant |a| < \tfrac{1}{4}\sqrt{|d|}. \tag{10}$$

Now, since

$$|d| = 4ac - b^2$$

we infer from (10) that

$$a < \sqrt{|d|} < d/4a \leqslant c,$$

thus every form satisfying (10) is reduced, and it is well known that every class contains at most one such form.

For $d > 0$, let us choose in the class C a form[1] (α, β, γ) reduced in the sense of Gauss, i.e. such that

$$\beta + \sqrt{d} > 2|\alpha| > -\beta + \sqrt{d} > 0. \tag{11}$$

---

[1] β is not to be confused with Siegel's zero.

We can assume without loss of generality that $\alpha > 0$. Now, for any form $f \in C$, there exists a properly unimodular transformation

$$T = \begin{pmatrix} p & r \\ q & s \end{pmatrix}$$

taking (α, β, γ) into f. The first column of this transformation can be made to consist of positive rational integers by Theorem 79 of [5]. If f satisfies (10), we infer from

$$\alpha p^2 + \beta pq + \gamma q^2 = a \tag{12}$$

that

$$\left| p + \frac{\beta - \sqrt{d}}{2\alpha}\, q \right| = a \left| \alpha p + \frac{\beta + \sqrt{d}}{2}\, q \right|^{-1} \leqslant \frac{1}{4}\sqrt{d} \cdot 2\big(\sqrt{d}\, q\big)^{-1} = \frac{1}{2}\, q^{-1}$$

and by Lemma 16, p. 175 from [5], p/q is a convergent of the continued fraction expansion for

$$\omega = \frac{-\beta + \sqrt{d}}{2\alpha}\,.$$

From this point onwards, we shall use the notation of Perron's monograph [7]. Since by (11)

$$\omega^{-1} > 1 \quad \text{and} \quad 0 > (\omega')^{-1} > -1,$$

ω^{-1} is a reduced quadratic surd and it has a pure periodic expansion into a continued fraction. Hence

$$\omega = [0, \overline{b_1, b_2, \ldots, b_k}]$$

where the bar denotes the primitive period. The corresponding complete quotients form again a periodic sequence

$$\omega_\nu = \frac{P_\nu + \sqrt{d}}{Q_\nu}\,, \quad \omega_0 = \omega,$$

where for all $\nu \geqslant 1$, ω_ν is reduced,

$$\omega_\nu = \omega_{\nu+k}, \tag{13}$$

and k is the least number with the said property.

Lemma 3. *Let* $[0, \overline{b_1, b_2, \ldots, b_k}]$ *be the continued fraction for* ω *defined above. Then*

$$\sum_{(a,b,c)\in C}{}'' \frac{1}{|a|} \leqslant \frac{2}{\sqrt{d}} \sum_{\substack{\nu=2 \\ \sqrt{d}\geqslant b_\nu \geqslant 2}}^{[k,2]} \min\left(\frac{\sqrt{d}}{2}\,, b_\nu + 1 \right)$$

where the sum on the left is taken over all (a, b, c) *in the class* C *satisfying* (10).

Proof. If A_j/B_j is the j-th convergent of ω, we have by formula (18), §20 of [7]

$$(A_{\nu-1} Q_0 - B_{\nu-1} P_0)^2 - d(B_{\nu-1})^2 = (-1)^\nu Q_0 Q_\nu$$

which gives on simplification

$$\alpha A_{\nu-1}^2 + \beta A_{\nu-1}B_{\nu-1} + \gamma B_{\nu-1}^2 = (-1)^\nu Q_\nu/2. \tag{14}$$

Similarly, eliminating Q_ν from formulae (16) and (17) in §20 of [7], we get

$$2\alpha A_{\nu-1}A_{\nu-2} + \beta(A_{\nu-1}B_{\nu-2} + B_{\nu-1}A_{\nu-2}) + 2\alpha B_{\nu-1}B_{\nu-2} = (-1)^{\nu-1}P_\nu. \tag{15}$$

Let $p = A_{\nu-1}$, $q = B_{\nu-1}$ ($\nu \geqslant 1$). By (12)

$$a = (-1)^\nu Q_\nu/2.$$

Hence, by formula (1) of §6 of [7]

$$\begin{vmatrix} A_{\nu-1} & A_{\nu-2} \\ B_{\nu-1} & B_{\nu-2} \end{vmatrix} = (-1)^\nu$$

and since

$$\begin{vmatrix} A_{\nu-1} & r \\ B_{\nu-1} & s \end{vmatrix} = 1$$

it follows that

$$T = \begin{pmatrix} A_{\nu-1} & A_{\nu-2} \\ B_{\nu-1} & B_{\nu-2} \end{pmatrix} \begin{pmatrix} 1 & t \\ 0 & (-1)^\nu \end{pmatrix}, \quad t \in Z.$$

Thus we find using (14) and (15)

$$\begin{aligned} f = (\alpha, \beta, \gamma) &\begin{pmatrix} A_{\nu-1} & A_{\nu-2} \\ B_{\nu-1} & B_{\nu-2} \end{pmatrix} \begin{pmatrix} 1 & t \\ 0 & (-1)^\nu \end{pmatrix} \\ &= \left((-1)^\nu \frac{Q_\nu}{2}, (-1)^{\nu-1}P_\nu, (-1)^\nu \frac{Q_{\nu-1}}{2} \right) \begin{pmatrix} 1 & t \\ 0 & (-1)^\nu \end{pmatrix}. \end{aligned}$$

In order to make f satisfy (10) we must choose

$$t = (-1)^\nu \left[\frac{P_\nu}{Q_\nu} + \frac{1}{2} \right].$$

Thus f is uniquely determined by ω_ν and, in view of (13), we have

$$\sum_{(a,b,c)\in C}{}'' \frac{1}{|a|} \leqslant \sum_{\substack{\nu=1 \\ Q_\nu < \frac{1}{2}\sqrt{d}}}^{[k,2]} 2(Q_\nu)^{-1}. \tag{16}$$

Since ω_ν is reduced, we have further for ν in question

$$\sqrt{d} \geqslant \frac{2\sqrt{d}}{Q_\nu} > \frac{P_\nu + \sqrt{d}}{Q_\nu} > \frac{\sqrt{d}}{Q_\nu} \geqslant 2.$$

Hence for

$$b_\nu = [\omega_\nu],$$

we get the inequalities

$$\sqrt{d} > b_\nu \geqslant 2, \quad b_\nu + 1 > \sqrt{d}/Q_\nu,$$

and by (16), Lemma 3 follows. □

Now, let ε_0 be the least totally positive unit $\varepsilon_0 > 1$ of the ring $\mathbb{Z}[\sigma]$ where

$$\sigma = \begin{cases} \dfrac{1}{2}\sqrt{d} & \text{if } d \equiv 0 \pmod 4, \\ \dfrac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

By Theorem 7 of Chapter IV of [6]

$$\varepsilon_0 = \frac{u + v\sqrt{d}}{2},$$

where for $l = [k, 2]$,

$$v = (q_{l-1},\, p_{l-1} - q_{l-2},\, p_{l-2}), \quad u = p_{l-1} + q_{l-2}$$

and p_j, q_j are the numerator and denominator, respectively, of the j-th convergent for ω^{-1}. Moreover, since ω^{-1} satisfies the equation

$$-\gamma\omega^{-2} - \beta\omega^{-1} - \alpha = 0 \quad (-\gamma > 0),$$

we find from formula (1) of §2 of Chapter IV of [6] that

$$q_{l-2} - p_{l-1} = -\beta v, \quad -p_{l-2} = -\alpha v.$$

Hence

$$\varepsilon_0 = \frac{p_{l-1} + q_{l-2}}{2} + \frac{p_{l-2}\sqrt{d}}{2\alpha} = q_{l-2} + \frac{\beta + \sqrt{d}}{2\alpha}\, p_{l-2}.$$

Since $p_j = B_{j+1}, q_j = A_{j+1}$, we get

$$\varepsilon_0 = B_{l-1}\left(\frac{A_{l-1}}{B_{l-1}} + \frac{\beta + \sqrt{d}}{2\alpha}\right) \geqslant B_{l-1}\left(\omega + \frac{\beta + \sqrt{d}}{2\alpha}\right) = \frac{\sqrt{d}}{\alpha}\, B_{l-1}. \tag{17}$$

Now,

$$\omega_l = b_l + \omega_{l+1}^{-1} = b_l + \omega_1^{-1} = b_l + \omega, \quad \omega_l' = b_l + \omega'$$

and since ω_l is reduced $0 > b_l + \omega' > -1$

$$b_l = [-\omega'] = \left[\frac{\beta + \sqrt{d}}{2a\alpha}\right] < \frac{\sqrt{d}}{\alpha}.$$

Thus (17) gives

$$\varepsilon_0 > b_l B_{l-1} > \prod_{\nu=1}^{l} b_\nu,$$

and by (16)

$$\sum_{(a,b,c)\in C}'' \frac{1}{|a|} \leqslant \frac{2}{\sqrt{d}} \max \sum (x_i + 1) = \frac{2}{\sqrt{d}}\, M \tag{18}$$

where maximum is taken over all non-decreasing sequences of at most l real numbers satisfying

$$2 \leqslant x_i \leqslant \tfrac{1}{2}\sqrt{d} - 1 = D, \quad \prod x_i \leqslant \varepsilon_0.$$

Let $(x_1, x_2, \ldots, x_m)$ be a point in which the maximum is taken with the least number m. We assert that the sequence contains at most one term x with $2 < x < D$. Indeed, if we had $2 < x_i \leqslant x_{i+1} < D$, we could replace the numbers x_i, x_{i+1} by

$$\frac{x_i}{\min(x_i/2,\, D/x_{i+1})}, \quad x_{i+1} \min\Big(\frac{x_i}{2}, \frac{D}{x_{i+1}}\Big)$$

and the sum $\sum(x_i + 1)$ would increase. Also, if we had $x_1 = x_2 = x_3 = 2$, we could replace them by $x_1 = 8$, and the sum $\sum(x_i + 1)$ would remain the same while m would decrease.

Let

$$\frac{\varepsilon_0}{4} = D^e \theta, \quad \text{where} \quad e = \left[\frac{\log(\varepsilon_0/4)}{\log D}\right].$$

Using $d > 676$, we get

$$M = \begin{cases} \frac{1}{2} e\sqrt{d} + \max(4\theta + 1, 2\theta + 4) & \text{if } 4\theta < D, \\ \frac{1}{2} e\sqrt{d} + 2\theta + 4 & \text{if } 2\theta < D \leqslant 4\theta, \\ \frac{1}{2} e\sqrt{d} + \theta + 7 & \text{if } D \leqslant 2\theta. \end{cases}$$

Now,

$$e = \frac{\log \varepsilon_0}{\log D} - \frac{\log 4\theta}{\log D}.$$

Since for $1 \leqslant x \leqslant y$, $y(\log x / \log y) \geqslant x - 1$, and for $d > 676$, $D/\log D \geqslant 12/\log 12 > 4.8$, we obtain if $4\theta < D$,

$$\begin{aligned} M - \frac{1}{2}\sqrt{d}\,\frac{\log \varepsilon_0}{\log D} &= \max(4\theta + 1, 2\theta + 4) - D\,\frac{\log 4\theta}{\log D} - \frac{\log 4\theta}{\log D} \\ &< \max(4\theta + 1, 2\theta + 4) - \max(4\theta - 1, 6) \leqslant 2, \end{aligned}$$

if $2\theta < D \leqslant 4\theta$,

$$\begin{aligned} M - \frac{1}{2}\sqrt{d}\,\frac{\log \varepsilon_0}{\log D} &= 2\theta + 4 - D\,\frac{\log 2\theta}{\log D} - D\,\frac{\log 2}{\log D} - \frac{\log 4\theta}{\log D} \\ &< 2\theta + 4 - 2\theta + 1 - 3 - 1 = 1, \end{aligned}$$

if $D \leqslant 2\theta$,

$$M - \frac{1}{2}\sqrt{d}\,\frac{\log \varepsilon_0}{\log D} = \theta + 7 - D\,\frac{\log \theta}{\log D} - D\,\frac{\log 4}{\log D} - \frac{\log 4\theta}{\log D}$$
$$< \theta + 7 - \theta + 1 - 6 - 1 = 1.$$

This together with (18) gives the theorem. □

4.

Proof of Corollary. We can assume $1 - \beta < (\log |d|)^{-2}$. It follows then by Theorem 1 that, for every $\eta > 0$, there exists $c(\eta)$ such that if $d > c(\eta)$

$$1 - \beta \geqslant \frac{6}{\pi^2}\,\frac{L(1,\chi)}{\sum' 1/a}\Big(1 - \frac{\eta}{2}\Big). \tag{19}$$

Let h_0 be the number of classes of forms in question. For $d < -4$, we have

$$L(1,\chi) = \frac{\pi h_0}{\sqrt{|d|}}\,,$$

and by Theorem 2

$$\sum{}' \frac{1}{|a|} \leqslant h_0.$$

Hence by (19)

$$1 - \beta \geqslant \frac{6}{\pi^2}\,\frac{h_0 \pi}{h_0\sqrt{|d|}}\Big(1 - \frac{\eta}{2}\Big) > \Big(\frac{6}{\pi} - \eta\Big)\frac{1}{\sqrt{|d|}}\,.$$

For $d > 0$, we have

$$L(1,\chi) = \frac{h_0 \log \varepsilon_0}{\sqrt{d}}\,.$$

Now, for any class C of forms

$$\sum_{(a,b,c)\in C}{}'' \frac{1}{|a|} = \sum_{\substack{(a,b,c)\in C \\ \frac{1}{4}\sqrt{d} \geqslant a \geqslant b > -a}} \frac{1}{a} + \sum_{\substack{(-a,b,-c)\in C \\ \sqrt{d} \geqslant -a \geqslant b > a}} \frac{1}{|a|}\,.$$

If (a, b, c) runs through C, $(-a, b, -c)$ runs through another class which we denote by $-C$ (it may happen that $-C = C$). If $C_1 \neq C_2$, then $-C_1 \neq -C_2$. Hence

$$\sum_{C} \sum_{\substack{(a,b,c)\in C \\ \frac{1}{4}\sqrt{d} \geqslant |a| \geqslant |b| > -|a|}} \frac{1}{|a|} = 2\sum{}' \frac{1}{a}$$

and by Theorem 2

$$\sum{}' \frac{1}{a} \leqslant \frac{h_0}{2}\left(\frac{\log \varepsilon_0}{\log\left(\frac{1}{2}\sqrt{d}-1\right)}+\frac{4}{\sqrt{d}}\right) < \frac{h_0 \log \varepsilon_0}{\log d}\left(1+O\left(\frac{1}{\sqrt{d}}\right)\right),$$

where the constant in the O-symbol is effective. (Note that $\varepsilon_0 > \frac{1}{2}\sqrt{d}$.) This together with (19) gives the corollary. □

References

[1] H. Davenport, *Multiplicative Number Theory*. Markham, Chicago 1967.

[2] D. Goldfeld, *An asymptotic formula relating the Siegel zero and the class number of quadratic fields*. Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) 2 (1975), 611–615.

[3] W. Haneke, *Über die reellen Nullstellen der Dirichletschen L-Reihen*. Acta Arith. 22 (1973), 391–421.

[4] A. E. Ingham, *The Distribution of Prime Numbers*. Cambridge Univ. Press, Cambridge 1932.

[5] B. W. Jones, *The Arithmetic Theory of Quadratic Forms*. The Math. Assoc. of America, Buffalo 1950.

[6] S. Lang, *Introduction to Diophantine Approximations*. Addison–Wesley, Reading 1966.

[7] O. Perron, *Die Lehre von den Kettenbrüchen*, Band I. Teubner, Stuttgart 1954.

[8] J. Pintz, *Elementary methods in the theory of L-functions* II. *On the greatest real zero of a real L-function*. Acta Arith. 31 (1976), 273–289.

[9] K. Prachar, *Primzahlverteilung*. Springer, Berlin–Göttingen–Heidelberg 1957.

[10] E. Titchmarsh, *The Zeta Function of Riemann*. Cambridge 1930.

Originally published in
Proceedings of the Indian Academy of Sciences
Mathematical Sciences 97 (1987), 297–303

Multiplicative properties of the partition function

with E. Wirsing (Ulm)

Abstract. A lower bound for the multiplicatively independent values of $p(n)$ for $N \leqslant n < N + R$ is given. The proof depends on the Hardy–Ramanujan formula and is of an elementary nature.

1. Introduction

P. Erdős and A. Ivić [1] in their study of the number of non-isomorphic Abelian groups of a given order needed a lower estimate for the number $m(N)$ of multiplicatively independent values of the partition function $p(n)$ in $1 \leqslant n \leqslant N$. The first named author has proved (see [1], Lemma 2) that, denoting the number of prime divisors of n by $\omega(n)$, one has

$$\omega\Big(\prod_{n=1}^{N} p(n)\Big) \to \infty,$$

whence $m(N) \to \infty$, as $N \to \infty$.

In the present paper we give an explicit estimate for $m(N)$, at the same time eliminating from the proof the appeal to "linear forms in logarithms". What we actually treat is the number $m(N, N+R)$ of multiplicatively independent values of $p(n)$ in $N \leqslant n < N + R$, where R is relatively small compared to N.

2.

Theorem. *There is an N_0 such that*

$$m(N, N+R) \geqslant R\,\frac{\log N - \log R}{\frac{3}{2}\log N + R\log 2}$$

for $N \geqslant N_0$ and all $R \in \mathbb{N}$.

The same lower bound applies to

$$\omega\Big(\prod_{N \leqslant n < N+R} p(n)\Big),$$

which is, of course, $\geqslant m(N, N+R)$.

It will be seen that, given N, our bound decreases as a function of R for $R \geqslant \log^2 N$, more precisely if $R \log 2 > \frac{2}{3} \log N (\log N - 1 - \log R)$. Thus in the proof and in applications like Corollary 2 below there is no need to consider larger R.

Corollary 1.

$$m(N, N+R) \geqslant \left(\tfrac{2}{3} - o(1)\right) R \quad \textit{if} \quad R = o(\log N) \textit{ as } N \to \infty.$$

Corollary 2.

$$m(N, N+R) \geqslant \left(\frac{1}{\log 2} - o(1)\right) \log N \quad \textit{if} \quad \frac{R}{\log N} \to \infty \textit{ as } N \to \infty.$$

In particular we may state that

$$\omega\left(\prod_{n=1}^{N} p(n)\right) \geqslant m(N) \geqslant (1-\varepsilon) \frac{\log N}{\log 2} \quad \text{if} \quad N \geqslant N_0(\varepsilon).$$

Concerning the paper of Erdős and Ivić we have

Corollary 3. *Let $a(n)$ be the number of non-isomorphic Abelian groups of order n and $C(x)$ the number of distinct values of $a(n)$ for $n \leqslant x$. Then for every $\varepsilon > 0$ and $x \geqslant x_1(\varepsilon)$*

$$\log C(x) \geqslant \frac{(\log\log x)^2}{\log 16 + \varepsilon}.$$

Similarly for the number $D(x)$ of distinct values $a(n) \leqslant x$ with any n one has, if $x \geqslant x_2(\varepsilon)$,

$$\log D(x) \geqslant \frac{(\log\log x)^2}{\log 4 + \varepsilon}.$$

Proof of Corollary 3. Notation as in [1]. Our Corollary 2 allows to pick $p(k_i)$ multiplicatively independent, $k_1, \ldots, k_t \leqslant \sqrt{\log x}$, with $t(\log 4 + \varepsilon) \sim \log\log x$. The construction gives $C(x) \geqslant r^t$ where $2rt \log(rt) \leqslant \sqrt{\log x}$. Here $r = \left[(\log x)^{1/2-\varepsilon}\right]$ is admissible if $x \geqslant x_1$, which gives our proposition.

For the estimate of $D(x)$ take $k_1, \ldots, k_t \leqslant \log x$ with $t(\log 2 + \varepsilon) \sim \log\log x$. Now $D(x) \geqslant r^t$ upon the condition that $\sum_i r \log p(k_i) \leqslant \log x$, which because of $\log p(k) \ll \sqrt{k} \leqslant \sqrt{\log x}$ is again satisfied by $r \sim (\log x)^{1/2-\varepsilon}$. □

3.

The proof uses the Hardy–Ramanujan formula for $p(n)$ (see (1) below) to construct a large number of distinct linear combinations of the numbers $\log p(n)$ with bounded integral coefficients. If, on the other hand, the dimension of this $\mathbb{Z}$-module were too small it would contain too few elements with bounded height. This mechanism is rather unspecific. Thus the theorem as it stands applies to any function $q(n) = p(n) + O[\exp(c\sqrt{n})]$ where

$c < \pi\sqrt{2/3}$, and similar results can be proved whenever an arithmetic function $q(n)$ allows an expansion

$$\log q(n) = a_0 n^{\alpha_0} + a_1 n^{\alpha_1} + \ldots + b \log n + \text{remainder},$$

where $a_0 > 0, \alpha_0 > 0, \alpha_0 \notin \mathbb{N}, \alpha_0 > \alpha_1 > \ldots, \alpha_i - \alpha_{i+1} \gg 1$, and where the remainder term is small enough. The factor $2/3$ in Corollary 2 would become $(\alpha_0 + 1)^{-1}$.

Lemma 1. *Write Δ for the forward difference and put*

$$\Delta_r := |\Delta^r \log p(N)|.$$

Then, as $N \to \infty$, we have

$$\Delta_r = c_2 r! \left|\binom{1/2}{r}\right| N^{1/2-r}(1 + O(N^{-1/3}))$$

with some constant c_2, uniformly in $0 \leqslant r \leqslant N^{1/6}$.

Proof. The Hardy–Ramanujan formula (see [2]) gives

$$p(n) = c_1 f(n - \tfrac{1}{24}) + O[\exp(c_3\sqrt{n})], \tag{1}$$

where

$$f(x) := \left(\frac{1}{\sqrt{x}} \exp(c_2\sqrt{x})\right)', \quad c_2 > c_3 > 0.$$

The actual values

$$\left(c_1 = \frac{1}{\pi\sqrt{8}},\ c_2 = \pi\sqrt{2/3},\ c_3 = \frac{c_2}{2}\right)$$

are mostly irrelevant for our purpose. Keeping the abbreviation $x = n - 1/24$ we find

$$\begin{aligned} p(n) &= \frac{c_1}{2x}\left(c_2 - \frac{1}{\sqrt{x}}\right)\exp(c_2\sqrt{x}) + O[\exp(c_3\sqrt{x})] \\ &= \frac{c_1}{2x}\left(c_2 - \frac{1}{\sqrt{x}}\right)\exp(c_2\sqrt{x})\big(1 + O[\exp(-c_4\sqrt{x})]\big) \end{aligned}$$

with some $c_4 > 0$. Therefore

$$\log p(n) = g(x) + O[\exp(-c_4\sqrt{n})],$$

where

$$g(x) = c_2\sqrt{x} + \log\frac{c_1 c_2}{2} + \log\left(1 - \frac{1}{c_2\sqrt{x}}\right) - \log x$$

—apart from the $\log x$ term—is a power series that converges for all large x,

$$g(x) = \sum_{i=-1}^{\infty} a_i x^{-i/2} - \log x.$$

Actually

$$a_{-1} = c_2, \quad |a_i| \leqslant c_2^{-i} \quad \text{for} \quad i \geqslant 1.$$

The case $r = 0$ of the lemma is now obvious.

For $r \geqslant 1$ the generalized mean-value theorem gives

$$\Delta^r \log p(N) = g^{(r)}(\xi) + O\big(2^r \exp(-c_4\sqrt{N})\big),$$

where $N - \frac{1}{24} < \xi < N + r$. Hence for $r \geqslant 1$

$$\Delta^r \log p(N) = r! \sum_{\substack{i=-1 \\ i\neq 0}}^{\infty} a_i \binom{-i/2}{r} \xi^{-i/2-r} + (-1)^r (r-1)!\, \xi^{-r} + O\big(2^r \exp(-c_4\sqrt{N})\big).$$

If $i \geqslant 1$, $r \geqslant 1$, then

$$\binom{-(i+1)/2}{r}\binom{-i/2}{r}^{-1} = \prod_{j=0}^{r-1} \frac{\frac{i+1}{2}+j}{\frac{i}{2}+j} < \prod_{j=0}^{r-1} \frac{\frac{i}{2}+1+j}{\frac{i}{2}+j} = 1 + \frac{2r}{i} \leqslant 3r.$$

Similarly

$$r!\left|\binom{-1/2}{r}\right|(r-1)!^{-1} \leqslant r, \quad (r-1)!\left(r!\left|\binom{1/2}{r}\right|\right)^{-1} \leqslant 4r.$$

Therefore

$$\begin{aligned}\Delta_r &= c_2 r!\left|\binom{1/2}{r}\right|\xi^{1/2-r}\left(1 + \sum_{i=1}^{\infty} O\left(\left(\frac{4r}{c_2\sqrt{\xi}}\right)^i\right)\right) + O\big(2^r \exp(-c_4\sqrt{N})\big) \\ &= c_2 r!\left|\binom{1/2}{r}\right|\xi^{1/2-r}\left(1 + O\left(\frac{r}{\sqrt{N}}\right)\right) + O\big(2^r \exp(-c_4\sqrt{N})\big).\end{aligned}$$

We also have

$$\begin{aligned}\xi^{1/2-r} &= (N + O(r))^{1/2-r} = N^{1/2-r}\left(1 + O\left(\frac{r}{N}\right)\right)^{1/2-r} \\ &= N^{1/2-r}\left(1 + O\left(\frac{r^2}{N}\right)\right) \\ &= N^{1/2-r}\big(1 + O(N^{-2/3})\big)\end{aligned}$$

by our bound for r. Finally

$$2^r\left(r!\left|\binom{1/2}{r}\right|N^{1/2-r}\right)^{-1} \ll (2N)^r = \exp[o(\sqrt{N})],$$

whence altogether

$$\Delta_r = c_2 r!\left|\binom{1/2}{r}\right|N^{1/2-r}\big(1 + O(N^{-1/3}) + O[\exp(-c_4\sqrt{N}/2)]\big)$$

for all $r \leqslant N^{1/6}$, which is the lemma. □

Lemma 2. *Let $R \leqslant N^{1/6}$ and $1 \leqslant r \leqslant R$. Then*

$$\Delta_r/\Delta_{r-1} \leqslant R/N$$

provided that $N \geqslant N_0$. The N_0 does not depend on R.

Proof. Lemma 1 for $2 \leqslant r \leqslant N^{1/6}$ supplies

$$\frac{\Delta_r}{\Delta_{r-1}} = \frac{r-\frac{3}{2}}{N}\left(1+O(N^{-1/3})\right) = \frac{r}{N} - \frac{3}{2N} + O\Big(\frac{r}{N^{4/3}}\Big) < \frac{r}{N} \leqslant \frac{R}{N}$$

if $N \geqslant N_0$, and similarly for $r = 1$. □

Proof of the theorem. We assume, somewhat arbitrarily, $R \leqslant N^{1/6}$. This includes for large N the range $R \leqslant \log^2 N$ that by an earlier remark is relevant.

Consider now the numbers

$$\omega = \sum_{r=0}^{R-1} x_r \Delta_r, \quad \text{where} \quad x_r \in \mathbb{N}_0,\ x_r \leqslant \frac{N}{R} - 1.$$

They all are distinct because of

$$\sum_{r=s+1}^{R-1} x_r\Delta_r \leqslant \sum_{r=s+1}^{R-1}\Big(\frac{N}{R}-1\Big)\Delta_r \leqslant \sum_{r=s+1}^{R-1}(\Delta_{r-1}-\Delta_r) < \Delta_s.$$

The number A of the ω's is therefore

$$A = \Big[\frac{N}{R}\Big]^R > \Big(\frac{N}{R}-1\Big)^R = \Big(\frac{N}{R}\Big)^R\Big(1-\frac{R}{N}\Big)^R \geqslant \Big(\frac{N}{R}\Big)^R\Big(1+O\Big(\frac{1}{\sqrt{N}}\Big)\Big)$$

as $N \to \infty$.

On the other hand

$$\Delta_r = \varepsilon_r \sum_{s=0}^{r}(-1)^s\binom{r}{s}\log p(N+s), \quad \varepsilon_r = \pm 1,$$

implies that each ω is a linear combination over $\mathbb{Z}$ of the $\log p(n)$, $N \leqslant n < N+R$. If $q_1, \ldots, q_k$ denote the primes that make up the $p(N), \ldots, p(N+R-1)$,

$$p(n) = \prod_{j=1}^{k} q_j^{a_j(n)}, \quad a_j(n) \in \mathbb{N}_0,$$

say, then we obtain the representation

$$\omega = \sum_{j=1}^{k} y_j \log q_j$$

with

$$y_j := \sum_{0\leqslant s\leqslant r<R} \varepsilon_r(-1)^s\binom{r}{s}x_r a_j(N+s).$$

Trivially $a_j(n) \leqslant (\log p(n))/\log 2$. Therefore, if N is large,

$$a_j(n) \leqslant c_2 \frac{\sqrt{n}}{\log 2},$$

$$|y_j| \leqslant \frac{c_2}{\log 2}\sqrt{N+R} \sum_{r=0}^{R-1} 2^r x_r$$

$$\leqslant \frac{c_2}{\log 2}\sqrt{N+R} \cdot 2^R\Big(\frac{N}{R} - 1\Big) \leqslant \frac{c_2}{\log 2} N^{3/2} \frac{2^R}{R}$$

for $1 \leqslant j \leqslant k$.

If now $m(N, N+R) =: l$ then the ω's are elements of an l-dimensional $\mathbb{Z}$-module. A suitable choice of l of the coordinates y_j $(j = 1, \ldots, k)$ will then determine the $k - l$ others. Therefore the number A of the ω's cannot exceed

$$\left(\frac{2c_2}{\log 2} N^{3/2} \frac{2^R}{R} + 1\right)^l.$$

Consequently

$$\left(\frac{3c_2}{\log 2} N^{3/2} \frac{2^R}{R}\right)^l \geqslant \Big(\frac{N}{R}\Big)^R \left(1 + O\Big(\frac{1}{\sqrt{N}}\Big)\right). \tag{2}$$

Thus, if any $R_0 > 3c_2/\log 2$ and a suitable N_0 are chosen then for all $R \geqslant R_0$ and $N \geqslant N_0$

$$\big(2^R N^{3/2}\big)^l \geqslant \Big(\frac{N}{R}\Big)^R \frac{R_0 \log 2}{3c_2}\left(1 + O\Big(\frac{1}{\sqrt{N}}\Big)\right) \geqslant \Big(\frac{N}{R}\Big)^R,$$

as claimed. For each of the remaining $R < R_0$, formula (2) implies $3l \geqslant 2R - \varepsilon$, and therefore $3l \geqslant 2R$, if N is large enough, hence again $\big(2^R N^{3/2}\big)^l \geqslant (N/R)^R$.

References

[1] P. Erdős, A. Ivić, *The distribution of values of a certain class of arithmetic functions at consecutive integers*. In: Number Theory, vol. I (Budapest 1987), Colloq. Math. Soc. János Bolyai 51, North-Holland, Amsterdam 1990, 45–91.

[2] G. H. Hardy, S. Ramanujan, *Asymptotic formulae in combinatory analysis*. Proc. London Math. Soc. (2) 17 (1918), 75–115.

Andrzej Schinzel
Selecta

Originally published in
New Trends in Probability and Statistics vol. 2:
Analytic and Probabilistic Methods in Number Theory
VSP Utrecht & TEV Vilnius 1992, 165–171

On an analytic problem considered by Sierpiński and Ramanujan

Abstract. Let $r(n)$ be the number of representations of n as a sum of two squares. An Ω-estimate for the error term in the summation formula for $r(n)^2$ is obtained.

Let $r(n)$ be the number of representations of n as a sum of two squares.

W. Sierpiński in his doctorate thesis (see [6]), written in 1906, has proved the estimate

$$\sum_{n\leqslant x} r(n)^2 = 4x\log x + cx + O(x^{3/4}\log x),$$

where c is a certain constant. The same asymptotic formula with the better error term $O(x^{(3/5)+\varepsilon})$ was stated without proof in [4]. B. M. Wilson [8] indicated without giving the details that $O(x^{(3/5)+\varepsilon})$ can be replaced by $O(x^{(1/2)+\varepsilon})$ for every $\varepsilon > 0$. Recently, W. R. Recknagel [5] improved the error term to $O(x^{1/2}\log^4 x)$ and M. Kühleitner [2] has improved it further to $O(x^{1/2}(\log x)^{11/3}(\log\log x)^{1/3})$.

As far as I know, there is no Ω-result in the literature, and it is the aim of this paper to prove such a result.

Theorem. *We have*

$$\sum_{n\leqslant x} r(n)^2 = 4x\log x + cx + \Omega(x^{3/8}).$$

The proof is based on the approach of [1]. The possibility of using this approach has been indicated to me by Prof. A. Ivić. In comparison with [1], the present paper contains no new idea, but the work is motivated by historical reasons. I thank Dr. W. G. Nowak for pointing out some obscurities in an early draft of the paper, and the Department of Mathematics in Geneva for their help in preparing the manuscript.

Notation. $\zeta(s)$ is the Riemann zeta function, $\zeta_K(s)$ the Dedekind zeta function of the field $K = \mathbb{Q}(i)$, p denotes a general prime, A is a large constant, not necessarily the same at each occurrence, T is a sufficiently large real number,

$y = T^B$, where B is a sufficiently large constant;

$J = \{T^{2/3} \leqslant t \leqslant 2T$: for any complex number z with $\operatorname{Re} z \geqslant 1/3$ and $|\operatorname{Im} z - t| \leqslant (\log T)^{20}$ we have $\zeta(2z) \neq 0\}$;

$$J_1 = \{T^{2/3} - (\log T)^4 \leqslant t \leqslant 2T + (\log T)^4 : \text{for any complex number } z \text{ with } \operatorname{Re} z \geqslant 1/3 \text{ and } |\operatorname{Im} z - t| \leqslant (\log T)^{15} \text{ we have } \zeta(2z) \neq 0\}.$$

Lemma 1.

$$F(s) = \sum_{n=1}^{\infty} \frac{r(n)^2}{n^s} = \frac{16\zeta_K(s)^2}{(1+2^{-s})\zeta(2s)} \quad \textit{for} \quad \operatorname{Re} s > 1.$$

Proof. See [4]. □

Lemma 2. *If* $\operatorname{Re} s \geqslant 1/3$ *and* $|\operatorname{Im} s| \geqslant 1$, *then*

$$\zeta_K(s) = O\big((|t|+2)^A\big),$$

where $s = \sigma + it$.

Proof. See Lemma 7 in [7]. □

Lemma 3. *If* $\operatorname{Re} s \geqslant 1/3$ *and* $t \in J_1$, *then*

$$\frac{1}{\zeta(2s)} = O(|t|+2).$$

Proof. This is a consequence of Lemma 1 in [1]. □

Lemma 4. *If* $\operatorname{Re} s \geqslant 1/3$ *and* $t \in J_1$, *then*

$$F(s) = O\big((|t|+2)^A\big) \quad \textit{for a suitable} \quad A > 0.$$

Proof. This is a consequence of Lemmas 1–3. □

Lemma 5. *Let*

$$E(x) = \sum_{n \leqslant x} r(n)^2 - 4x\log x - cx.$$

If

$$\int_T^{\infty} \frac{E(u)^2}{u^{7/4}} e^{-u/y}\, du \leqslant \log^2 T,$$

$t = \operatorname{Im} s \in J$, *and* $\operatorname{Re} s = 3/8$, *then we have*

$$F(s) = \sum_{n \leqslant T_0} \frac{r(n)^2}{n^s} e^{-n/y} + s\int_0^1 \sum_{n > T_0} \frac{E(n+u)}{(n+u)^{s+1}} e^{-(n+u)/y}\, du + O\big((\log T)^{20}\big)$$

for a suitable T_0, $T \leqslant T_0 \leqslant 2T$.

Proof. We start with

$$\sum_{n=1}^{\infty} \frac{r(n)^2 e^{-n/y}}{n^s} = \frac{1}{2\pi i}\int_{\operatorname{Re} w = 2} F(s+w) y^w \Gamma(w)\, dw.$$

Now we break off the portion $|\operatorname{Im} w| \geqslant (\log T)^4$ of the integral, with a small error, and move the line of integration to $\operatorname{Re} w = -(1/24)$.

Now using the estimate of $F(s)$ given in Lemma 4 (and assuming that B is large enough), and using the fact that, since $t \in J$ and $t + \operatorname{Im} w \in J_1$, we see that the value of the integral on the horizontals $t+\operatorname{Im} w = c \in J_1$, as well as on the vertical $\operatorname{Re} w = -(1/24)$ is small. This proves that

$$\sum_{n=1}^{\infty} \frac{r(n)^2 e^{-n/y}}{n^s}$$

equals nearly the sum of the residues inside the contour. Thus we have

$$F(s) = \sum_{n=1}^{\infty} \frac{r(n)^2}{n^s}\, e^{-n/y} + O(T^{-10}) = \sum_{n \leqslant T_0} + \sum_{n > T_0} + O(T^{-10}).$$

Now

$$\begin{aligned}
\sum_{n>T_0} \frac{r(n)^2 e^{-n/y}}{n^s} &= \int_{T_0}^{\infty} \frac{1}{u^s}\, e^{-u/y}\, d\Big(\sum_{n \leqslant u} r(n)^2\Big) \\
&= \int_{T_0}^{\infty} \frac{1}{u^s}\, e^{-u/y}\, d\big(4u \log u + cu + E(u)\big) \\
&= \int_{T_0}^{\infty} \frac{1}{u^s}\, e^{-u/y} \big(4 \log u + 4 + c\big)\, du + \int_{T_0}^{\infty} \frac{1}{u^s}\, e^{-u/y}\, dE(u) \\
&= S_1 + S_2 \quad \text{(say)}.
\end{aligned}$$

The first integral does not exceed up to a constant factor

$$\int_{T_0}^{\infty} \frac{1}{u^s}\, e^{-u/y} u^{1/24}\, du,$$

and hence is small by Lemma 3 of [1]. Now S_2 is (after one integration by parts)

$$\left[\frac{E(u) e^{-u/y}}{u^s}\right]_{T_0}^{\infty} + s \int_{T_0}^{\infty} \frac{E(u) e^{-u/y}}{u^{s+1}}\, du + \frac{1}{y} \int_{T_0}^{\infty} \frac{E(u) e^{-u/y}}{u^s}\, du.$$

Hence, using Lemma 4 in [1], and choosing a suitable T_0 in the interval $T \leqslant T_0 \leqslant 2T$, we obtain

$$\begin{aligned}
S_2 &= s \int_{T_0}^{\infty} \frac{E(u)}{u^{s+1}}\, e^{-u/y}\, du + O(\log T) \\
&= s \sum_{n \geqslant T_0} \int_0^1 \frac{E(n+u)}{(n+u)^{s+1}}\, e^{-(n+u)/y}\, du + O(\log T).
\end{aligned}$$

This proves the lemma. □

Lemma 6. *We have*

$$\int_0^T \left|\sum_n b_n n^{it}\right|^2 dt = \sum_n \big(T + O(n)\big)\big(|b_n|^2\big)$$

for any sequence of complex numbers b_n provided the right hand side is convergent.

Proof. For the proof of this lemma we refer the reader to [3]. □

Lemma 7. *We have*

$$\int_{\substack{\operatorname{Re} s=3/8\\ \operatorname{Im} s=t\in J}} \left|\sum_{n\leqslant T_0} \frac{r(n)^2}{n^s}\, e^{-n/y}\right|^2 \frac{dt}{t^2} \ll 1.$$

Proof. It is sufficient to prove that

$$\int_{T^{2/3}}^{2T} \left|\sum_{n\leqslant T_0} \frac{r(n)^2}{n^{3/8}}\, e^{-n/y}\right|^2 \frac{dt}{t^2} \ll 1.$$

By Lemma 6, we have

$$\int_{2^m}^{2^{m+1}} \left|\sum_{n\leqslant T_0} \frac{r(n)^2}{n^{3/8}}\, e^{-n/y}\right|^2 dt = \sum_{n\leqslant T_0} \big(2^m + O(n)\big)\, \frac{r(n)^4}{n^{3/4}} \ll 2^m T_0^{1/4} \log^7 T_0 + T_0^{5/4} \log^7 T_0.$$

Hence

$$\int_{2^m}^{2^{m+1}} \left|\sum_{n\leqslant T_0} \frac{r(n)^2}{n^s}\, e^{-n/y}\right|^2 \frac{dt}{t^2} \leqslant \frac{T_0^{1/4} \log^7 T_0}{2^m} + \frac{T_0^{5/4} \log^7 T_0}{2^{2m}}.$$

Now, summing over m satisfying $(1/2)T_0^{2/3} < 2^m \leqslant 2T$, it follows that

$$\int_{T^{2/3}}^{2T} \left|\sum_{n\leqslant T_0} \frac{r(n)^2}{n^s}\, e^{-n/y}\right|^2 \frac{dt}{t^2} \ll 1.$$ □

Lemma 8. *If*

$$\int_T^\infty \frac{E(u)^2}{u^{7/4}}\, e^{-u/y}\, du \leqslant \log^2 T,$$

then we have

$$\int_{\substack{\operatorname{Re} s=3/8\\ \operatorname{Im} s=t\in J}} \left|\int_0^1 \sum_{n\geqslant T_0} \frac{E(n+u)e^{-(n+u)/y}}{(n+u)^{s+1}}\, du\right|^2 dt \ll \int_T^\infty \frac{|E(u)|}{u^{7/4}}\, e^{-2u/y}\, du,$$

for a suitable T_0, $T \leqslant T_0 \leqslant 2T$.

Proof. This follows from Lemma 6 in the same way as in [1] Lemma 8 follows from Lemma 6. □

Lemma 9. *If*

$$\int_T^\infty \frac{E(u)^2}{u^{7/4}}\, e^{-u/y}\, du \leqslant \log^2 T,$$

we have

$$\int_{\substack{\operatorname{Re} s=3/8\\ \operatorname{Im} s=t\in J}} \frac{|F(s)|^2}{|s|^2}\, dt \ll 1 + \int_T^\infty \frac{E(u)^2}{u^{7/4}}\, e^{-2u/y}\, du.$$

Proof. This follows from Lemmas 5, 7 and 8. □

Lemma 10. *Let*

$$f(s) = \sum_{n=1}^\infty \frac{b_n}{n^s}$$

be convergent in some half-plane and analytically continuable in $\sigma \geqslant 1/3$, $A \leqslant t \leqslant A + M$. *Then*

$$\int_A^{A+M} \left|f(3/8 + it)\right|^2 dt \gg M,$$

provided $M \geqslant \log A$, $b_1 = 1$, *and*

$$\max\left\{|f(s)| : A \leqslant t \leqslant A + M,\ \operatorname{Re} s \geqslant 3/8\right\} \leqslant e^A.$$

Proof. This is a consequence of Lemma 9 in [1] for $\alpha = 3/8$. □

Definition 1.

$$f(s) = \frac{\zeta_K(s + 1/4)^2}{(1 + 2^{-s})\zeta(2s)} = \sum_{n=1}^\infty \frac{b_n}{n^s}\,.$$

Lemma 11. *If an interval* $[A, A + M]$ *is contained in* J *and* $A \geqslant M \geqslant \log A$, *we have*

$$\int_A^{A+M} |f(3/8 + it)|^2\, dt \gg M.$$

Proof. It follows from the definition of $f(s)$ that $b_1 = 1$,

$$\sum_{n=1}^\infty \frac{b_n}{n^s} \quad \text{is convergent in} \quad \operatorname{Re} s > 3/4$$

and analytically continuable in the whole plane with poles at

$$s = \frac{3}{4}\,,\ \frac{(2k+1)\pi i}{\log 2}\,, \quad k \in \mathbb{Z},$$

and at the zeros of $\zeta(2s)$. If $\operatorname{Re} s \geqslant 3/8$ and $[A, A+M]$ is contained in J, then by Lemma 2 we have

$$\left|\zeta_K(s + 1/4)\right| \leqslant \left(|t| + 2\right)^{A/(2\log(2A+2))} \leqslant e^{A/2},$$

and by Lemma 3,

$$\left|\zeta(2s)^{-1}\right| \ll |t| + 2 \leqslant 2A + 2.$$

Hence $|f(s)| \leqslant e^A$ for A large enough. The lemma follows now from Lemma 10. □

Lemma 12. *If* $[A, A + M] \subset J$ *and* $A \geqslant M \geqslant \log A$, *we have*

$$\int_A^{A+M} \left|F(3/8 + it)\right|^2 dt \gg AM.$$

Proof. For $\operatorname{Re} s = 3/8$, we note that $|\zeta_K(1 - s)| = |\zeta_K(s + (1/4))|$. Using the functional equation

$$B^s \Gamma(s)\zeta_K(s) = B^{1-s}\Gamma(1 - s)\zeta_K(1 - s),$$

where B is a constant, we obtain for $\operatorname{Re} s = 3/8$,

$$\begin{aligned}|F(s)| = 16|f(s)|\,|\zeta_K(s)|^2|\zeta_K(1/4)|^{-2} &= 16|f(s)|\,|\zeta_K(s)|^2|\zeta_K(1 - s)|^{-2} \\ &= 16|f(s)|\,|B^{2-4s}\Gamma(1 - s)^2\Gamma(s)^{-2}| \gg \left|f(s)\right|\,|t|^{1/2}.\end{aligned}$$

Hence Lemma 12 follows from Lemma 11. □

Definition 2. For every x such that $T^{2/3} \leqslant x \leqslant 2T$,

$$J(x) = J \cap [x, 2x],$$

$N(x)$ is the number of zeros of $\zeta(2s)$ with $t \in \left[x - (\log T)^{20}, 2x + (\log T)^{20}\right]$ and $\operatorname{Re} s \geqslant 1/3$.

Lemma 13. *We have*

$$N(x) \ll x^{49/60}.$$

Proof. This follows from Lemma 13 in [1] for $\varepsilon = 1/6$. □

Definition 3. $J_2(x)$ is the portion of $J(x)$ obtained by deleting all connected components whose length is not greater than $\log 2x$.

Lemma 14. *We have*

$$\int_{J_2(x)} \left|F(3/8 + it)\right|^2 dt \gg x^2.$$

Proof. The total length of $[x, 2x] \setminus J_2(x)$ is $O\left(N(x)(\log T)^{20}\right) = O(x^{5/6})$. Hence the total length of $J_2(x)$ is $\gg x$. Now applying Lemma 12 to each connected component of $J_2(x)$ and adding we obtain Lemma 14. □

Lemma 15. *We have*

$$\int_{\substack{\operatorname{Re} s = 3/8 \\ \operatorname{Im} s = t \in J}} \frac{|F(s)|^2}{|s|^2}\, dt \gg \log T.$$

Proof. From Lemma 14 we have

$$\int_{J(x)} |F(3/8+it)|^2\,dt \gg x^2,$$

and Lemma 15 follows by integration by parts. □

Proof of the Theorem. By Lemma 9 and Lemma 15 we have

$$\int_T^\infty \frac{E(u)^2}{u^{7/4}}\,e^{-2u/y}\,du \gg \log T.$$

If for every $\varepsilon > 0$ we had $|E(u)| < \varepsilon u^{3/8}$ for $T \geqslant T_0(\varepsilon)$, it would follow that

$$\begin{aligned}\int_{T_0(\varepsilon)}^\infty \frac{E(u)^2}{u^{7/4}}\,e^{-2u/T_0(\varepsilon)^B}\,du &\leqslant \varepsilon^2\biggl(\int_{T_0(\varepsilon)}^{T_0(\varepsilon)^B}\frac{du}{u}+\int_1^\infty e^{-2v}\,\frac{dv}{v}\biggr)\\ &< \varepsilon^2\bigl(B\log T_0(\varepsilon)+1\bigr),\end{aligned}$$

in contrary to the above inequality. □

References

[1] R. Balasubramanian, K. Ramachandra, M. V. Subbarao, *On the error function in the asymptotic formula for the counting function of k-full numbers*. Acta Arith. 50 (1988), 107–118.

[2] M. Kühleitner, *On a question of A. Schinzel concerning the sum* $\sum_{n\leqslant x}(r(n))^2$. In: Österreichisch-Ungarisch-Slowakisches Kolloquium über Zahlentheorie (Maria Trost, 1992), Grazer Math. Ber. 318, Karl-Franzens-Univ. Graz, Graz 1993, 63–67.

[3] H. L. Montgomery, R. C. Vaughan, *Hilbert's inequality*. J. London Math. Soc. (2) 8 (1974), 73–82.

[4] S. Ramanujan, *Some formulae in the analytic theory of numbers*. Messenger of Math. (2) 45 (1916), 81–84; Collected papers, Cambridge 1927, 113–135.

[5] W. Recknagel, *Varianten des Gaußschen Kreisproblems*. Abh. Math. Sem. Univ. Hamburg 59 (1989), 183–189.

[6] W. Sierpiński, *Sur la sommation de la série* $\sum_{n>a}^{n\leqslant b} r(n)f(n)$*, où* $r(n)$ *signifie le nombre de décomposition du nombre n en une somme de deux carrés de nombres entiers*. Prace Mat. Fiz. 18 (1908), 1–59 (Polish); also in: Oeuvres choisies, T. I, Varsovie 1974, 109–154.

[7] W. Staś, *Über eine Anwendung der Methode von Turán auf die Theorie des Restgliedes im Primidealsatz*. Acta Arith. 5 (1959), 179–195.

[8] B. M. Wilson, *Proof of some formulae enunciated by Ramanujan*. Proc. London Math. Soc. (2) 21 (1922), 235–255.

Originally published in
Journal of Number Theory 78 (1999), 62–84

Class numbers and short sums of Kronecker symbols

with J. Urbanowicz (*Warszawa*) *and P. Van Wamelen* (*Baton Rouge*)

1. Introduction

We shall consider sums of the form

$$S(D, q_1, q_2) = \sum_{q_1|D|<n<q_2|D|} \left(\frac{D}{n}\right),$$

where D belongs to the set $\mathscr{F}$ of fundamental discriminants different from 1,

$$q_1, q_2 \in \mathbb{Q}; \quad 0 \leqslant q_1 < q_2 \leqslant 1. \tag{1.1}$$

Let r be the least common denominator of q_1 and q_2, and

$$\chi = \chi_D = \left(\frac{D}{\cdot}\right).$$

It follows from the result of Szmidt, Urbanowicz, and Zagier [5] that if $D \in \mathscr{F}$ and $(D, r) = 1$ we have

$$S(D, q_1, q_2) = \sum_{\psi} c_\psi B_{1,\chi\psi}, \tag{1.2}$$

where the sum is over all primitive characters ψ with conductor f_ψ such that

$$f_\psi \mid r \quad \text{and} \quad \psi(-1) = -\chi(-1), \tag{1.3}$$

$B_{1,\chi\psi}$ is the generalized first Bernoulli number attached to the character $\chi\psi$, and $c_\psi = c_\psi(D, q_1, q_2)$ are given explicitly. In particular, for all ψ satisfying (1.3)

$$c_\psi(D, 1-q_2, 1-q_1) = \chi(-1)c_\psi(D, q_1, q_2), \tag{1.4}$$

$$c_\psi(D, 0, 1-q_2) = -\chi(-1)c_\psi(D, 0, q_2), \tag{1.5}$$

$$c_\psi(D, q_1, 1-q_2) = c_\psi(D, q_1, q_2), \quad \text{if} \quad q_1 + q_2 \leqslant 1,\ D < 0, \tag{1.6}$$

$$c_\psi(D, q_1, q_2) = c_\psi(D_0, q_1, q_2) \tag{1.7}$$

Communicated by D. B. Zagier

provided

$$D, D_0 \in \mathscr{F}, \quad \operatorname{sgn} D = \operatorname{sgn} D_0, \quad \text{and} \quad D \equiv D_0 \Big(\operatorname{mod} r \, \frac{(r^3, 8)}{(r, 8)} \Big) \tag{1.8}$$

and

$$c_{\overline{\psi}}(D, q_1, q_2) = \overline{c}_{\psi}(D, q_1, q_2), \tag{1.9}$$

where the bar denotes the complex conjugation.

Denote by $C(D, q_1, q_2)$ the set of all primitive characters ψ satisfying (1.3) such that $c_\psi \neq 0$.

Definition. For $\varepsilon = 0$ or 1, let $\mathscr{P}_\varepsilon$ be the set of all pairs $\langle q_1, q_2 \rangle$ satisfying both (1.1) and

$$q_1 + q_2 \leqslant 1 \quad \text{and} \quad q_2 \leqslant \tfrac{1}{2} \text{ if } q_1 = 0 \text{ or } D < 0 \tag{1.10}$$

such that $\operatorname{card} C(D, q_1, q_2) = \varepsilon$ for at least one $D \in \mathscr{F}$ prime to r.

The aim of the present paper is to prove

Theorem. *The sets $\mathscr{P}_0$ and $\mathscr{P}_1$ are both finite. More precisely, $\mathscr{P}_0$ has* 55 *elements and $\mathscr{P}_1$ has* 116 *elements, as listed in Section* 5.

The sets $\mathscr{P}_\varepsilon$ are of interest for the following reason.

For each $\varepsilon = 0$, 1 and $\langle q_1, q_2 \rangle \in \mathscr{P}_\varepsilon$ the set of all $D \in \mathscr{F}$ prime to r satisfying $\operatorname{card} C(D, q_1, q_2) = \varepsilon$ is, by virtue of (1.7), the intersection of $\mathscr{F}$ with the union of some arithmetic progressions with the first term D_0 and the difference $r\big((r^3, 8)/(r, 8)\big) \operatorname{sgn} D_0$. Hence the condition $\operatorname{card} C(D, q_1, q_2) = \varepsilon$ if fulfilled by one $D \in \mathscr{F}$ prime to r is fulfilled by infinitely many such D. The condition (1.10) is justified by the formulae (1.4), (1.5), and (1.6); it permits us to retain in the theorem only essentially different cases.

Moreover, $\operatorname{card} C(D_0, q_1, q_2) = 0$, $(D_0, r) = 1$ and (1.8) imply, by virtue of (1.2), that

$$S(D, q_1, q_2) = 0. \tag{1.11}$$

Further,

$$\operatorname{card} C(D_0, q_1, q_2) = 1, \quad (D_0, r) = 1 \tag{1.12}$$

and (1.8) imply, by virtue of (1.3) and (1.9), that

$$C(D, q_1, q_2) = C(D_0, q_1, q_2) = \{\chi_E\},$$

where E is a fundamental discriminant satisfying

$$E \mid r, \quad \chi_E(-1) = -\chi_D(-1),$$

hence $(D, E) = 1$, $DE < 0$. It follows by (1.2) that for D satisfying (1.8) we have

$$S(D, q_1, q_2) = c_{\chi_E} B_{1, \chi_{DE}}.$$

We now recall (for example see [6]) that for every fundamental discriminant $D < -4$ we have

$$B_{1,\chi_D} = -h(D),$$

where $h(D)$ is the class number of the field $\mathbb{Q}(\sqrt{D})$ and infer that (1.8) and (1.12) imply

$$h(ED) = cS(D, q_1, q_2). \tag{1.13}$$

($c = -c_{\chi_E}^{-1}$). Now, relations of the form (1.11) and (1.13) have been studied by many authors, see e.g. Berndt [1], Mitchell and Johnson [4], and Hudson and Williams [3], mostly, but not exclusively in the case $q_2 - q_1 = 1/r$, $|D|$ a prime. All pairs $\langle q_1, q_2\rangle$ known to satisfy (1.1), (1.10), and (1.11) for some D prime to r happen to belong to $\mathscr{P}_0$ and $\mathscr{P}_0$ does not contain any new pair with $q_2 - q_1 = 1/r$. We do not know, however, whether the conditions (1.1), (1.10), and (1.11) for some D prime to r imply $\langle q_1, q_2\rangle \in \mathscr{P}_0$. Also, we cannot say anything about relation (1.11) with $(D_0, r) \neq 1$. On the other hand, as we shall show in Section 4, if $\langle q_1, q_2\rangle \in \mathscr{P}_0$, card $C(D_0, q_1, q_2) = 0$, and $(D_0, r) = 1$ then (1.8) implies (1.11) without the condition $D \in \mathscr{F}$, for all non-square discriminants D.

Further, all known pairs $\langle q_1, q_2\rangle$ satisfying (1.1), (1.10), and (1.13) for fixed E, c and some $D_0 \in \mathscr{F}$ prime to r happen to belong to $\mathscr{P}_1$, and again we do not know whether these conditions imply $\langle q_1, q_2\rangle \in \mathscr{P}_1$. In this case, however, there is a new relation with $q_2 - q_1 = 1/r$, namely

$$h(12D) = 4 \sum_{(1/12)|D|<n<(1/10)|D|} \left(\frac{D}{n}\right)$$

for all $D \in \mathscr{F}$, $|D| \equiv 11$ or $59 \pmod{60}$.

The paper is organized as follows: In Section 2 we prove three propositions on characters, in Section 3 we express $S(D, q_1, q_2)$ in the form (1.2) obtaining the formulae for c_ψ, and in Section 4 we apply the results of Sections 2 and 3 to prove the finiteness of the sets $\mathscr{P}_0$ and $\mathscr{P}_1$. Section 5 consists of two tables, which for every $\langle q_1, q_2\rangle \in \mathscr{P}_\varepsilon$ ($\varepsilon = 0, 1$) give arithmetic progression relevant to (1.11) or (1.13). In the former case r and in the latter case $e = E \operatorname{sgn} D$ and c are also given.

Professor A. Granville has communicated to us that he also proved the final theorem of the paper in a somewhat different way. The second author worked on the paper during his visits to the Carleton University, the Louisiana State University, and the University of Georgia. He warmly thanks Professors A. Granville and K. S. Williams for some helpful conversations and the staff of the universities for their hospitality. The third author was partially supported by Grant LESQF(1995–97)-RD-A-09 from the Louisiana Educational Quality Support Fund.

In the proofs of Propositions 1 and 2 of the next section we have used some hints from the referee which we gratefully acknowledge.

2. Dirichlet characters

In this section we prove three propositions giving the existence of Dirichlet characters with certain properties. For definitions and basic facts on Dirichlet characters we refer the

reader to Hasse [2]. Throughout the paper let ζ_m denote a fixed primitive m-th root of unity and φ denote the Euler totient function.

For a prime power P let g_P be a generator of the group of characters mod P, even if $P = 2^\alpha$, $\alpha \geqslant 3$. The following lemmas are implicit in [2] (Section 13, No. 6).

Lemma 1. *For every positive integer $m \not\equiv 2 \pmod 4$ there exists a primitive character of conductor m.*

Lemma 2. *If $P = p^\alpha$ (p an odd prime), then g_P^k has conductor P unless*

$$\frac{\varphi(p^\alpha)}{\varphi(p^{\alpha-1})} \mid k.$$

Proposition 1. *Let f be a positive integer with $f \not\equiv 2 \pmod 4$, and either $f \nmid 120$ or $40 \mid f$. Assume $\varepsilon = \pm 1$. Then there exists a non-real primitive character ψ of conductor f such that*

$$\psi(-1) = \varepsilon \quad \textit{and} \quad \psi(2)^2 \neq 1.$$

Lemma 3. *For every positive integer $f \not\equiv 2 \pmod 4$, $f \nmid 12$, and every $\varepsilon = \pm 1$ there exists a primitive character ξ of conductor f such that $\xi(-1) = \varepsilon$.*

Proof. By the assumption there exists a prime power P such that $P \mid f$, $(P, f/P) = 1$ and $P > 4$. By Lemma 1 there exists a primitive character ξ_0 of conductor f/P. We now take

$$\xi = \xi_0 g_P^{(3+\varepsilon\xi_0(-1))/2} \qquad \text{if } P \text{ is odd},$$
$$\xi = \xi_0 g_4^{(3+\varepsilon\xi_0(-1))/2} g_P \qquad \text{if } P \text{ is even}.$$

By Lemma 2, if $P > 4$ is odd, g_P^2 has conductor P, hence ξ has conductor f. Moreover $\xi(-1) = \varepsilon\xi_0(-1)^2 = \varepsilon$. □

Proof of Proposition 1. Assume first that $f \nmid 120$. Then there exists a prime power P such that

$$P \mid f, \quad P \nmid 120, \quad \left(P, \frac{f}{P}\right) = 1. \tag{2.1}$$

We distinguish two cases

(i) $f/P \mid 12$,
(ii) $f/P \nmid 12$.

In the case (i) there exists a primitive real character ξ of conductor f/P. We take

$$\psi = \begin{cases} \xi g_P^{(3+\varepsilon\xi(-1))/2} & \text{if } P \text{ is odd}, \\ \xi g_4^{(3+\varepsilon\xi(-1))/2} g_P & \text{if } P \text{ is even}, \end{cases}$$

and obtain $\psi(-1) = \varepsilon$. Also ψ is not real since g_P^2 (P odd) and g_P (P even) are not real. The same characters, by Lemma 2, have conductor P, hence ψ is primitive of conductor f. If we had $\psi(2)^2 = 1$ it would follow P odd, $g_P(2)^4 = 1$, hence $2^4 \equiv 1 \pmod P$, contrary to (2.1).

In the case (ii) by Lemma 3 there exists a primitive character ξ of conductor f/P such that $\xi(-1) = \varepsilon g_P(-1)$. We put

$$\psi_\pm = \xi g_P^{\pm 1}.$$

$\psi_\pm$ are primitive characters of conductor f, non-real since g_P is not real. Also $\psi_\pm(-1) = \varepsilon$. If we had $\psi_\pm(2)^2 = 1$ for both signs, it would follow that

$$1 = \psi_+(2)^2 \psi_-(2)^{-2} = g_P(2)^4,$$

hence $2^4 \equiv 1 \pmod P$, contrary to (2.1).

It remains to consider the case $40 \mid f \mid 120$. Here we take

$$\psi = \begin{cases} g_5 g_4^{(3-\varepsilon)/2} g_8, & \text{if } f = 40, \\ g_3 g_5 g_4^{(3+\varepsilon)/2} g_8, & \text{if } f = 120. \end{cases}$$ □

Proposition 2. *Let k, $f \in \mathbb{N}$, $(k, f) = 1$, $k \not\equiv \pm 1 \pmod f$, and f odd, $f \nmid 3 \cdot 5 \cdot 17$. For each $\varepsilon = \pm 1$ and $\eta = \pm 1$ there exists a non-real primitive character ψ of conductor d such that $d \mid f$ and*

$$\psi(-1) = \varepsilon, \quad \psi(k) \neq \eta, \quad \text{and} \quad \psi(p)^2 \neq 1 \text{ for all primes } p$$

such that

$$p \mid 2f \quad \text{and} \quad p \nmid d. \tag{2.2}$$

If the condition (2.2) *is restricted to $p \mid f$ and $p \nmid d$ then the condition $f \nmid 3 \cdot 5 \cdot 17$ can be relaxed to $f \nmid 3 \cdot 5$.*

Proof. Let

$$f = \prod_{i=1}^{h} p_i^{\alpha_i},$$

where the p_i are distinct primes. We put $p_i^{\alpha_i} = P_i$, and

$$\mathscr{P} = \{P_i : 1 \leqslant i \leqslant h\},$$
$$\mathscr{T} = \{P_i : 1 \leqslant i \leqslant h,\ k^2 \not\equiv 1 \pmod{P_i}\},$$

and we shall consider successively three cases:

(i) $\mathscr{T} \not\subset \{5, 17\}$.
(ii) $\varnothing \neq \mathscr{T} \subset \{5, 17\}$.
(iii) $\mathscr{T} = \varnothing$.

Case (i). Here there exists a $P \in \mathscr{P}$ such that

$$k^2 \not\equiv 1 \pmod P \quad \text{and} \quad 2^8 \not\equiv 1 \pmod P. \tag{2.3}$$

We put

$$\psi = \psi_1 \psi_2,$$

where

$$\psi_1(x) = \prod_{\substack{1 \leqslant i \leqslant h \\ p_i \nmid P}} \left(\frac{x}{p_i}\right),$$

and

$$\psi_2 = g_P, \quad \text{if } \psi_1(-1) = -\varepsilon, \tag{2.4}$$

$$\psi_2 = g_P^2, \quad \text{if } \psi_1(-1) = \varepsilon \quad \text{and either} \quad \psi_1(k) = \eta \text{ or } k^2 \not\equiv -1 \pmod{P}, \tag{2.5}$$

$$\psi_2 = g_P^4, \quad \text{if } \psi_1(-1) = \varepsilon \quad \text{and} \quad \psi_1(k) = -\eta \text{ and } \quad k^2 \equiv -1 \pmod{P}. \tag{2.6}$$

The characters ψ_1 and ψ_2 are primitive mod $\prod_{p_i \nmid P} p_i$ and P, respectively, and ψ_2 is not real since $\zeta_{\varphi(P)}^4 \notin \mathbb{R}$. Hence ψ is not real and is primitive $\bmod d = \prod_{p_i \nmid P} p_i P$. Thus the only prime satisfying (2.2) is 2 and the equality $\psi(2)^2 = 1$ would give

$$g_P(2)^8 = 1,$$

hence $2^8 \equiv 1 \pmod{P}$, contrary to (2.3). Moreover

$$\psi(-1) = \psi_1(-1)\psi_2(-1) = \varepsilon$$

and $\psi(k) = \eta$ would imply

$$\psi_2(k) = \eta\psi_1(k),$$

which gives in the case (2.4) $g_P(k) = \pm 1$; in the case (2.5) either $g_P(k)^2 = 1$ or $g_P(k)^2 = -1$ and $k^2 \not\equiv -1 \pmod{P}$ and in the case (2.6) $g_P(k)^4 = -1$ and $k^2 \equiv -1 \pmod{P}$, which in cases (2.4) and (2.5) contradicts $k^2 \not\equiv 1 \pmod{P}$. In case (2.6) we have $k^4 \equiv 1 \pmod{P}$ and so $g_P(k)^4 = 1$, a contradiction.

Before we proceed to the cases (ii) and (iii) we make the following observation. Since $f \nmid 2^8 - 1$, there exists the least $P \in \mathscr{P}$ such that

$$P \nmid 2^8 - 1. \tag{2.7}$$

Then if ψ_1 is a character $\bmod f/P$ and $c \mid 2$, at least one of the characters $\psi_\pm = \psi_1 g_P^{\pm c}$ satisfies $\psi(2)^2 \neq 1$; otherwise we should have

$$1 = \psi_+(2)^2\psi_-(2)^{-2} = g_P^{4c}(2),$$

hence $2^8 \equiv 1 \pmod{P}$, contrary to (2.7).

Therefore, whenever in the following the exponent of g_P divides 2 we obtain $\psi(2)^2 \neq 1$, replacing g_P by g_P^{-1}, if necessary.

Case (ii). Here we put

$$\psi = \begin{cases} g_5^2 g_{17} g_P^{(3-\varepsilon)/2} \prod_{q \in \mathscr{P}\setminus\{5,17,P\}} g_q^2, & \text{if } \mathscr{T} = \{5,17\} \text{ and } 3 \notin \mathscr{P}, \\ g_3 g_5^2 g_{17} g_P^{(3+\varepsilon)/2} \prod_{q \in \mathscr{P}\setminus\{3,5,17,P\}} g_q^2, & \text{if } \mathscr{T} = \{5,17\} \text{ and } 3 \in \mathscr{P}, \\ g_p g_P^{(3-\varepsilon)/2} \prod_{q \in \mathscr{P}\setminus\{p,P\}} g_q^2, & \text{if } \mathscr{T} \cap \{5,17\} = \{p\} \text{ and } 3 \notin \mathscr{P}, \\ g_3 g_p g_P^{(3+\varepsilon)/2} \prod_{q \in \mathscr{P}\setminus\{3,p,P\}} g_q^2, & \text{if } \mathscr{T} \cap \{5,17\} = \{p\} \text{ and } 3 \in \mathscr{P}. \end{cases}$$

By Lemma 2, ψ is a primitive character of conductor f. The only prime satisfying (2.2) is 2. Since $\big((3 \pm \varepsilon)/2\big) \mid 2$, a proper choice of g_P gives $\psi(2)^2 \neq 1$ and ψ is not real. Moreover,

$$\psi(-1) = -(-1)^{(3-\varepsilon)/2} = (-1)^{(3+\varepsilon)/2} = \varepsilon,$$

and $\psi(k) = \eta$ would imply

$$g_{17}(k)^2 = \psi(k)^2 = 1, \quad k^2 \equiv 1 \pmod{17}, \quad \text{if} \quad \mathscr{T} = \{5,17\},$$

or

$$g_p(k)^2 = \psi(k)^2 = 1, \quad k^2 \equiv 1 \pmod{p}, \quad \text{if} \quad \mathscr{T} \cap \{5,17\} = \{p\},$$

contrary to $17 \in \mathscr{T}$, or $p \in \mathscr{T}$, respectively.

Case (iii). Here we assume without loss of generality that $k \equiv 1 \pmod{P_i}$ for $i \leqslant j$, $k \equiv -1 \pmod{P_i}$ for $i > j$ and if $3 \in \{P_1, \dots, P_h\}$ then $3 = P_1$ or $3 = P_h$. Since $k \not\equiv \pm 1 \pmod{f}$ we have $1 \leqslant j < h$.

If either $3 \notin \{P_1, \dots, P_h\}$ or $3 = P_1$, $\eta = \varepsilon$ or $3 = P_h$, $\eta = 1$ we put

$$\psi = g_{P_1}^{(3-\varepsilon\eta)/2} g_{P_h}^{(3-\eta)/2} \prod_{i=2}^{h-1} g_{P_i}. \tag{2.8}$$

By Lemma 2, ψ is a primitive character of conductor f, thus the only prime satisfying (2.2) is 2. Since all the exponents on the right hand side of (2.8) divide 2, a proper choice of g_P gives $\psi(2)^2 \neq 1$ and that ψ is not real. Moreover,

$$\psi(-1) = (-1)^{(3-\varepsilon\eta)/2} \cdot (-1)^{(3-\eta)/2} = \varepsilon,$$
$$\psi(k) = (-1)^{(3-\eta)/2} = -\eta.$$

If $3 = P_1$, $\eta = -\varepsilon$ and $j > 1$ we put

$$\psi = g_3 g_{P_2} g_{P_h}^{(3-\eta)/2} \prod_{i=3}^{h-1} g_{P_i}^2. \tag{2.9}$$

By Lemma 2, ψ is a primitive character of conductor f, thus the only prime satisfying (2.2) is 2. Since all the exponents on the right hand side of (2.9) divide 2, a proper choice of g_P gives $\psi(2)^2 \neq 1$ and that ψ is not real. Similarly to the above we obtain $\psi(-1) = \varepsilon$ and $\psi(k) = -\eta$.

Likewise, if $P_h = 3$, $\eta = -1$ and $j < h-1$ we put

$$\psi = g_3 g_{P_1}^{(3+\varepsilon)/2} g_{P_{h-1}} \prod_{i=2}^{h-2} g_{P_i}^2. \tag{2.10}$$

By Lemma 2, ψ is a primitive character of conductor f, thus the only prime satisfying (2.2) is 2. Since all the exponents on the right hand side of (2.10) divide 2, a proper choice of g_P gives $\psi(2)^2 \neq 1$ and that ψ is not real. Moreover,

$$\psi(-1) = (-1)^{(3+\varepsilon)/2} = \varepsilon, \quad \psi(k) = 1.$$

If either

$$3 = P_1, \quad \eta = -\varepsilon, \quad \text{and} \quad j = 1 \tag{2.11}$$

or

$$3 = P_h, \quad \eta = -1, \quad \text{and} \quad j = h-1 \tag{2.12}$$

we put

$$\psi = \psi_1 \psi_2,$$

where

$$\psi_1(x) = \prod_{\substack{1 \leqslant i \leqslant h \\ p_i \nmid 3P}} \left(\frac{x}{p_i}\right),$$

$$\psi_2 = g_P^{(3+\varepsilon\psi_1(-1))/2}.$$

ψ_1, ψ_2 are primitive characters mod $\prod_{p_i \nmid 3P} p_i$ and P, respectively. Thus ψ is a primitive character mod $\prod_{p_i \nmid 3P} p_i P$, non-real since $\zeta_{\varphi(P)}^2 \notin \mathbb{R}$. We have

$$\psi(-1) = \psi_1(-1)\psi_2(-1) = \psi_1(-1)(-1)^{(3+\varepsilon\psi_1(-1))/2} = \varepsilon.$$

Moreover, (2.11) implies $k \equiv -1 \pmod{(f/3)}$, $\psi(k) = \psi_1(-1)\psi_2(-1) = \varepsilon \neq \eta$; (2.12) implies $k \equiv 1 \pmod{(f/3)}$, $\psi(k) = 1 \neq \eta$. The only primes satisfying (2.2) are 2 and 3 and the equalities $\psi(2)^2 = 1$, $\psi(3)^2 = 1$ would give $2^4 \equiv 1 \pmod P$ or $3^4 \equiv 1 \pmod P$, $P = 5$, contrary to (2.7).

This completes the proof of the proposition except for the last statement. That follows by inspection of the argument, where the prime 17 is avoided only because of the condition $\psi(2)^2 \neq 1$. □

Proposition 3. *Let $k, f \in \mathbb{N}$, $(k, f) = 1$, $k \not\equiv \pm 1 \pmod f$, and either $f \nmid 16 \cdot 3 \cdot 5$ or $16 \cdot 5 \mid f$. For each $\varepsilon = \pm 1$ there exists a non-real primitive character ψ of conductor d, where $d \mid f$ such that*

$$\psi(-1) = \varepsilon, \quad \psi(k) \neq 1, \quad \textit{and} \quad \psi(p)^2 \neq 1 \quad \textit{for all primes } p,$$

satisfying

$$p \mid f \quad \textit{and} \quad p \nmid d. \tag{2.13}$$

Proof. We shall distinguish four cases:

(i) $f \not\equiv 0 \pmod 4$,
(ii) $f \equiv 4 \pmod 8$,
(iii) $f = 2^\alpha f_1$, where $\alpha \geqslant 3$, f_1 odd, $f_1 \nmid 15$,
(iv) $f = 2^\alpha f_1$, where $f_1 \mid 15$ and either $\alpha \geqslant 5$ or $\alpha = 4$, $5 \mid f_1$.

For the sake of brevity in each case we only define a character ψ with the required properties, leaving to the reader the actual verification.

Case (i). If f is odd it suffices to take in Proposition 2 $\eta = 1$. If $f \equiv 2 \pmod 4$ it suffices in view of Proposition 2 to consider the case $17 \mid f \mid 510$. If $k \not\equiv \pm 1 \pmod{17}$ or $k \equiv -1 \pmod{17}$, $\varepsilon = -1$, we put

$$\psi = g_{17}^{(3+\varepsilon)/2}.$$

If $k \equiv -1 \pmod{17}$, $\varepsilon = 1$, there is a prime $p \mid f$ such that $k \not\equiv -1 \pmod p$. We put

$$\psi = g_p g_{17}.$$

If $k \equiv 1 \pmod{17}$, there is a prime $p \mid f$ such that $k \not\equiv 1 \pmod p$, $p = 3$ or 5. We put

$$\psi(x) = \begin{cases} g_3 g_{17}^{(3-\varepsilon)/2}, & \text{if } p = 3, \\ g_5^2 g_{17}^{(3+\varepsilon)/2}, & \text{if } p = 5,\ k \equiv \pm 2 \pmod 5, \\ g_5 g_{17}^{(7-\varepsilon)/2}, & \text{if } p = 5,\ k \equiv -1 \pmod 5, \text{ and either } f = 170 \text{ or } \varepsilon = 1, \\ g_3 g_5 g_{17}, & \text{otherwise.} \end{cases}$$

Case (ii). In Proposition 2 we replace f by $f/4$, ε by $-\varepsilon$, and η by $g_4(k)$. If $k \not\equiv \pm 1 \pmod{(f/4)}$ there exists by virtue of Proposition 2 a non-real primitive character ψ' of conductor d such that $d \mid f/4$ and

$$\psi'(-1) = -\varepsilon, \quad \psi'(k) \neq g_4(k) \tag{2.14}$$

and

$$\psi'(p)^2 \neq 1 \quad \text{for all primes} \quad p \mid (f/4),\ p \nmid d. \tag{2.15}$$

If $k \equiv -1 \pmod 4$, $k \equiv 1 \pmod{(f/4)}$, or if $k \equiv 1 \pmod 4$, $k \equiv -1 \pmod{(f/4)}$, $\varepsilon = 1$, the properties (2.14) and (2.15) belong to every primitive character $\psi' \bmod f/4$ with $\psi'(-1) = -\varepsilon$. In each case the character

$$\psi = g_4 \psi'$$

satisfies the condition of the proposition.

In the remaining case $k \equiv 1 \pmod 4$, $k \equiv -1 \pmod{(f/4)}$, $\varepsilon = -1$, there exists a prime power P such that

$$P \,\Big|\, \frac{f}{4}, \quad \Big(P, \frac{f}{4P}\Big), \quad P \neq 3, 5.$$

We put

$$\psi = \psi_1 \psi_2,$$

where

$$\psi_1(x) = \prod_{\substack{p\mid(f/4P)\\ p \text{ prime}}} \left(\frac{x}{p}\right), \quad \psi_2 = g_P^{(3-\psi_1(-1))/2}.$$

Case (iii). If $k \not\equiv \pm 1 \pmod{f_1}$ we argue as in the case $\alpha = 2$ above. If $k \equiv 1 \pmod{f_1}$ we have $k \not\equiv 1 \pmod{2^\alpha}$. We choose a character $\psi_2 \bmod 2^\alpha$ such that $\psi_2(k) \neq 1$ and then a non-real primitive character $\psi_1 \bmod f_1$ such that

$$\psi_1(-1) = \varepsilon\psi_2(-1).$$

Then $\psi = \psi_1\psi_2$ has the required properties.

If $k \equiv -1 \pmod{f_1}$ we have $k \not\equiv -1 \pmod{2^\alpha}$. We choose a non-trivial character $\psi_2 \bmod 2^\alpha$ such that $\psi_2(-k) \neq \varepsilon$ and then a non-real primitive character $\psi_1 \bmod f_1$ such that

$$\psi_1(-1) = \varepsilon\psi_2(-1).$$

The character $\psi = \psi_1\psi_2$ has the required properties.

Case (iv). If $k \not\equiv \pm 1 \pmod{2^{\alpha-1}}$ we put

$$\psi = g_4^{(3+\varepsilon)/2} g_{2^\alpha}.$$

The same formula is good if $k \equiv 1 + 2^{\alpha-1} \pmod{2^\alpha}$; or $k \equiv -1 + 2^{\alpha-1} \pmod{2^\alpha}$, $\varepsilon = 1$; or $k \equiv -1 \pmod{2^\alpha}$, $\varepsilon = -1$.

If $k \equiv -1 + 2^{\alpha-1} \pmod{2^\alpha}$, $\varepsilon = -1$, we put

$$\psi = \begin{cases} g_4 g_{2^\alpha}^2, & \text{if } \alpha \geqslant 5, \\ g_5 g_{2^\alpha}^2, & \text{if } \alpha = 4,\ k \not\equiv 1 \pmod 5, \\ g_5 g_{2^\alpha}, & \text{if } \alpha = 4,\ k \equiv 1 \pmod 5,\ f = 80, \\ g_3 g_5^2, & \text{if } \alpha = 4,\ k \equiv 1 \pmod 5,\ f = 240,\ k \equiv 1 \pmod 3), \\ g_3 g_4 g_5 g_{2^\alpha}, & \text{if } \alpha = 4,\ k \equiv 1 \pmod 5,\ f = 240,\ k \equiv -1 \pmod 3). \end{cases}$$

If $k \equiv \eta \pmod{2^\alpha}$, $\eta = \pm 1$, $\varepsilon = 1$, then f_1 has a prime factor p such that $k \not\equiv \eta \pmod p$. If $\alpha \geqslant 5$, or if $p = 3$, or if $p = 5 = f_1$ we put

$$\psi = g_4 g_p g_{2^\alpha}.$$

If $f = 240$, $k \equiv \eta \pmod{48}$, $k \not\equiv \eta \pmod 5$, $\varepsilon = 1$ we put

$$\psi = g_3 g_5 g_{2^\alpha}.$$

In the remaining case $k \equiv 1 \pmod{2^\alpha}$, $\varepsilon = -1$, f_1 has a prime factor p such that $k \not\equiv 1 \pmod p$. We put

$$\psi = \begin{cases} g_p g_{2^\alpha}, & \text{if } \alpha \geqslant 5, \text{ or if } p = 3, \text{ or if } p = 5 = f_1, \\ g_5 g_{2^\alpha}^2, & \text{otherwise.} \end{cases}$$

□

3. Character sums in terms of Bernoulli numbers

Let χ be a Dirichlet character mod M and let N be a multiple of M. For any integer $r > 1$ prime to N and natural m we have the formula from [5]:

$$mr^{m-1}\sum_{0<n<N/r}\chi(n)n^{m-1} = -B_{m,\chi}r^{m-1} + \frac{\bar\chi(r)}{\varphi(r)}\sum_{\psi}\bar\psi(-N)B_{m,\chi\psi}(N), \tag{3.1}$$

where the last sum is over all Dirichlet characters ψ mod r. Here for a Dirichlet character θ, $B_{m,\theta}$ denotes the generalized Bernoulli number attached to θ and

$$B_{m,\theta}(X) = \sum_{k=0}^{m}\binom{m}{k}B_{k,\theta}X^{m-k}.$$

Note that if the character θ mod T is induced from a character θ_1 mod some divisor of T, then we have

$$B_{m,\theta} = B_{m,\theta_1}\prod_{p\mid T}(1-\theta_1(p)p^{m-1}), \tag{3.2}$$

where the product is over all primes p dividing T. For more details see [5].

If $m = 1$ and χ is not trivial, formula (3.1) implies

$$\sum_{0<n<N/r}\chi(n) = -B_{1,\chi} + \frac{\bar\chi(r)}{\varphi(r)}\sum_{\psi}\bar\psi(-N)B_{1,\chi\psi}$$

because for non-trivial characters θ we have $B_{0,\theta} = 0$ and so $B_{1,\theta}(X) = B_{1,\theta}$.

Let χ be a non-trivial character of conductor M. Then the above identity and (3.2) give

$$\sum_{0<n<N/r}\chi(n) = -B_{1,\chi} + \frac{\bar\chi(r)}{\varphi(r)}\sum_{\psi}\bar\psi(-N)\prod_{q\mid r}(1-\chi\psi(q))B_{1,\chi\psi}, \tag{3.3}$$

where the last sum is over all primitive characters ψ with conductor f_ψ such that $f_\psi \mid r$ and where ψ has parity opposite to that of χ ($B_{1,\theta} = 0$ for even non-trivial θ).

Let $\chi = \left(\frac{D}{\cdot}\right)$, where $D \neq 1$ is a fundamental discriminant. We shall consider sums of the form

$$S(D, q_1, q_2) = \sum_{q_1|D|<n<q_2|D|}\left(\frac{D}{n}\right),$$

where

$$q_1, q_2 \in \mathbb{Q}; \quad 0 \leqslant q_1 < q_2 \leqslant 1,$$

$$q_i = \frac{k_i}{r_i},\ r_i \in \mathbb{N},\ k_i \in \mathbb{Z},\ (k_i, r_i) = 1,\ (r_i, D) = 1 \quad (i = 1, 2).$$

We put $r = \text{l.c.m.}(r_1, r_2)$ and $\rho = (r_1, r_2)$, so that

$$r = \frac{r_1}{\rho}\cdot\rho\cdot\frac{r_2}{\rho} \quad \text{and} \quad \left(\frac{r_1}{\rho}, \frac{r_2}{\rho}\right) = 1.$$

The formula (3.3) implies

Proposition 4. *For $r > 1$*

$$S(D, q_1, q_2) = \sum_{\psi} c_\psi B_{1,\chi\psi},$$

where the sum is over all primitive characters ψ with conductor f_ψ such that $f_\psi \mid r$ and $\psi(-1) = -\chi(-1)$ and where c_ψ are given by the formulae

1. *if $q_1 = 0$ ($r_1 = 1$, $k_2 = k$, $r_2 = r$),*

   (a) *and if ψ is trivial,*

$$c_\psi = -1 + \frac{\chi(r)}{\varphi(r)} \prod_{\substack{q \mid r \\ q \text{ prime}}} (1 - \chi(q));$$

   (b) *otherwise,*

$$c_\psi = \frac{\chi(r)\bar{\psi}(-k|D|)}{\varphi(r)} \prod_{\substack{q \mid r \\ q \text{ prime}}} (1 - \chi(q)\psi(q)); \tag{3.4}$$

2. *if $q_1 > 0$,*

   (a) *and if $f_\psi \mid \rho$,*

$$c_\psi = c'_\psi \cdot c''_\psi, \tag{3.5}$$

where

$$c'_\psi = \chi(\rho)\bar{\psi}(-|D|) \prod_{\substack{q \mid \rho \\ q \text{ prime}}} (1 - \chi(q)\psi(q))$$

and

$$c''_\psi = \frac{\chi(r_2/\rho)\bar{\psi}(k_2)}{\varphi(r_2)} \prod_{\substack{q \mid r_2,\, q \nmid \rho \\ q \text{ prime}}} (1 - \chi(q)\psi(q)) - \frac{\chi(r_1/\rho)\bar{\psi}(k_1)}{\varphi(r_1)} \prod_{\substack{q \mid r_1,\, q \nmid \rho \\ q \text{ prime}}} (1 - \chi(q)\psi(q));$$

   (b) *and if $f_\psi \mid r_2$ but $f_\psi \nmid \rho$,*

$$c_\psi = \frac{\chi(r_2)\bar{\psi}(-k_2|D|)}{\varphi(r_2)} \prod_{\substack{q \mid r_2 \\ q \text{ prime}}} (1 - \chi(q)\psi(q)); \tag{3.6}$$

   (c) *and if $f_\psi \mid r_1$ but $f_\psi \nmid \rho$,*

$$c_\psi = -\frac{\chi(r_1)\bar{\psi}(-k_1|D|)}{\varphi(r_1)} \prod_{\substack{q \mid r_1 \\ q \text{ prime}}} (1 - \chi(q)\psi(q)); \tag{3.7}$$

(d) *and if* $f_\psi \nmid r_1$, $f_\psi \nmid r_2$, *then* $c_\psi = 0$.

Corollary 1. *For all characters* ψ *satisfying* (1.3) *we have* (1.4), (1.5) *and* (1.6).

Proof. It follows by calculation from Proposition 4 that

$$c_\psi(D, 1-q_2, 1-q_1) = -\bar{\psi}(-1)c_\psi(D, q_1, q_2),$$
$$c_\psi(D, 0, 1-q_2) = \bar{\psi}(-1)c_\psi(D, 0, q_2),$$
$$c_\psi(D, q_1, 1-q_2) = c_\psi(D, q_1, q_2) \quad \text{if} \quad q_1 + q_2 \leqslant 1 \quad \text{and} \quad \psi(-1) = 1,$$

and then we use the condition $\psi(-1) = -\chi(-1)$. □

Corollary 2. *For all characters* ψ *satisfying* (1.3), (1.8) *implies* (1.7).

Proof. It follows from Proposition 4 that

$$c_\psi(D, q_1, q_2) = c_\psi(D_0, q_1, q_2),$$

provided $\chi_D(-1) = \chi_{D_0}(-1)$ and $\chi_D(q) = \chi_{D_0}(q)$ for all primes $q \mid r$. The first condition gives $\operatorname{sgn} D = \operatorname{sgn} D_0$, the second $D \equiv D_0 \pmod 8$ if $q = 2$ and $D \equiv D_0 \pmod q$ if $q > 2$. □

Corollary 3. *For all characters* ψ *satisfying* (1.3) *we have* (1.9).

Proof. This follows from Proposition 4 since χ is real. □

Corollary 4. *If* $c_\psi(D, q_1, q_2) = 0$ *for all characters* ψ *with* $f_\psi \mid r$ *and* $\psi(-1) = -\chi_D(-1)$, *then*

$$S(\chi, q_1, q_2) = \sum_{q_1 m < n < q_2 m} \chi(n) = 0$$

for every character $\chi \bmod m$ *induced from* χ_D *provided* $(m, r) = 1$.

Proof. It follows from (3.2) that the coefficient of $B_{1,\chi\psi}$ in the representation of $S(\chi, q_1, q_2)$ as the linear combination of generalized Bernoulli numbers derived from (3.3) is divisible by $c_\psi(D, q_1, q_2)$, hence 0. □

The last corollary justifies the remark made in the introduction about non-fundamental discriminants D. Indeed, if $D = D_1 s^2$, where $D_1 \in \mathscr{F}$, then $\left(\frac{D}{\cdot}\right)$ is induced from $\left(\frac{D_1}{\cdot}\right)$ and, assuming $(s, r) = 1$, the residue class of $D_1 s^2 \bmod r\big((r^3, 8)/(r, 8)\big)$ is admissible in the sense of (1.8).

4. Results

In this section we shall determine when $\operatorname{card} C(D, q_1, q_2) = 0$ or 1. Recall that $r = \text{l.c.m.}(r_1, r_2)$ and $\rho = (r_1, r_2)$.

Proposition 5. *Let* $C = C(D, q_1, q_2)$, *where* $D \in \mathscr{F}$, $(D, r) = 1$ *and* $\langle q_1, q_2\rangle$ *satisfy* (1.1). *Assume that* $r \nmid 8 \cdot 3 \cdot 5$ *and besides*

(a) $r \neq 14,\ 18$ *if* $\max\{r_1, r_2\} = 2\min\{r_1, r_2\} \equiv 2 \pmod 4$,
(b) $r \neq 16,\ 48$ *if* $r_1 = r_2 = r$, $q_1 + q_2 \neq 1$,
(c) $D > 0$ *if* $q_1 + q_2 = 1$.

Then C *contains a non-real character and*

$$\operatorname{card} C \geqslant 2.$$

Proof. It is enough to show that under the assumption of the theorem there exists both an even and an odd primitive non-real character ψ, such that $c_\psi \neq 0$. In view of (1.4) we may assume without loss of generality that $r_1 \leqslant r_2$. If $k_1 = 0$ a required ψ exists by virtue of Proposition 1 and formula (3.4). If $k_1 > 0$ we consider four cases:

(i) $r_1 \nmid r_2$,
(ii) $r_1 \mid r_2, r_1 \neq r_2$,
(iii) $r_1 = r_2, q_1 + q_2 \neq 1$,
(iv) $r_1 = r_2, q_1 + q_2 = 1$.

Case (i). In this case we have $r_1 < r_2$. If $r_2 \nmid 120$ and r_2 is odd or divisible by 4 then by virtue of Proposition 1 we can find both an even and an odd primitive non-real character ψ of conductor $f_\psi = r_2$. Moreover, $f_\psi \nmid \rho$ (recall $r_1 < r_2$) and it follows by (3.6) that for this ψ, $c_\psi \neq 0$. A similar argument shows that we get a non-zero c_ψ if $r_1 \nmid 120$ and r_1 is odd or divisible by 4. Then by virtue of Proposition 1 we can find a primitive non-real character of prescribed parity of conductor $f_\psi = r_1$ and by assumption (i) we have $f_\psi \nmid \rho$. Here we can use formula (3.7) and it remains to consider the cases when $r_2 \nmid 120$, $2 \parallel r_2$ or $r_1 \nmid 120$, $2 \parallel r_1$.

If $r_2 \nmid 120$ and $2 \parallel r_2$, by Proposition 1 we can find both an even and an odd primitive non-real character ψ of conductor $f_\psi = (r_2/2)$ such that $\psi(2) \neq \pm 1$. Moreover, the divisibility $(r_2/2) \mid \rho$ would imply $r_1 = r_2$ or $r_2 = 2r_1$, which is not the case. Thus $f_\psi \nmid \rho$ and by virtue of (3.6) $c_\psi \neq 0$.

If $r_1 \nmid 120$ and $2 \parallel r_1$, by Proposition 1 we can find a primitive non-real character of prescribed parity of conductor $f_\psi = (r_1/2)$ such that $\psi(2) \neq \pm 1$. If $f_\psi \nmid \rho$ we can use formula (3.7) and $c_\psi \neq 0$. If $(r_1/2) \mid \rho$ we have $(r_1/2) \mid r_2$ and in consequence $r_2 \nmid 120$. This case was considered above.

Case (ii). Here we may assume that $r_2 \nmid 120$ and by Proposition 1 we can find both an odd and an even primitive non-real character of conductor $f_\psi = (r_2/2)$ such that $\psi(2) \neq \pm 1$. If $f_\psi \nmid \rho$ we can use formula (3.6) and $c_\psi \neq 0$. The divisibility $(r_2/2) \mid \rho$ implies $(r_2/2) \mid r_1$ and by assumption we obtain $r_2 = 2r_1$.

Let $r_2 = 2r_1$ and $r_2 \nmid 120$. Then r_2 is even. If r_1 is divisible by 4, in virtue of Proposition 1 we can find a non-real primitive character of prescribed parity of conductor $f_\psi = r_2$. By assumption we have $f_\psi \nmid \rho$. Consequently we can use formula (3.6) and $c_\psi \neq 0$.

It remains to consider the case $2 \parallel r_2$ (r_1 odd). By virtue of Proposition 2 (for $k = 8$), since by (a) $r_1 \nmid 7$ and $r_1 \nmid 9$ we can find a primitive non-real character ψ of prescribed parity of conductor $d \mid r_1$ such that $\psi(8) \neq -\chi(2)$ and $\psi(q)^2 \neq 1$ for all primes q such

that $q \mid r_1$ and $q \nmid d$. By virtue of formula (3.5) it follows easily that $c'_\psi \neq 0$ for this ψ. We shall prove the same for c''_ψ by contradiction. The equality $c''_\psi = 0$ would imply

$$\chi(2)\bar{\psi}(k_2)\,(1 - \chi(2)\psi(2)) - \bar{\psi}(k_1) = 0,$$

and in consequence

$$\psi(k) + \psi(2) = \chi(2), \tag{4.1}$$

where $k_2 \equiv kk_1 \pmod d$. Therefore we obtain

$$|\psi(t) + 1| = 1,$$

where $k \equiv 2t \pmod d$ and hence

$$\operatorname{Re}\psi(t) = -\tfrac{1}{2}.$$

Therefore $\psi(t) = \zeta_3^{\pm 1}$ and $\psi(k) = \zeta_3^{\pm 1}\psi(2)$. Substituting it into formula (4.1) gives

$$\psi(2) = -\chi(2)\zeta_3^{\pm 1},$$

which implies

$$\psi(8) = -\chi(2),$$

a contradiction.

Case (iii). Here in view of (3.5) we have

$$c'_\psi = \chi(r)\bar{\psi}(-|D|)\prod_{q\mid r}\bigl(1 - \chi(q)\psi(q)\bigr)$$

and

$$\varphi(r)c''_\psi = \bar{\psi}(k_2) - \bar{\psi}(k_1).$$

Let k denote a natural number such that $1 \leqslant k \leqslant r-1$ and $k_2 \equiv kk_1 \pmod r$. Since $q_1 < q_2$, $q_1 + q_2 \neq 1$ we have $k_2 \not\equiv \pm k_1 \pmod r$, $k \not\equiv \pm 1 \pmod r$. By (b), $r \nmid 240$ or $80 \mid r$, hence by virtue of Proposition 3 we can find a non-real primitive character ψ of prescribed parity of conductor $d \mid r$ such that $\psi(k) \neq 1$ and $\psi(q)^2 \neq 1$ for all primes $q \mid r$ and $q \nmid d$. Hence we have $c'_\psi \neq 0$ and $c''_\psi \neq 0$, and in consequence $c_\psi \neq 0$.

Case (iv). Here by (c) we have $\chi(-1) = 1$, hence all characters ψ in question are odd and $\varphi(r)c''_\psi = 2\bar{\psi}(k_2) \neq 0$. Since $r \nmid 8\cdot 3\cdot 5$, by Proposition 1 there exists an odd primitive non-real character ψ of conductor $r\bigl((r,4)/(r^2,4)\bigr)$ with $\psi(2)^2 \neq 1$ if $2 \parallel r$. For this character we have $c'_\psi \neq 0$ and in consequence $c_\psi \neq 0$. □

Proof of the Theorem. Proposition 5 implies that there is only a small finite set of $\langle q_1, q_2\rangle$ satisfying (1.1) for which $\operatorname{card} C(D, q_1, q_2) < 2$ for at least one $D \in \mathscr{F}$ prime to r (with $D > 0$ if $q_1 + q_2 = 1$). It is now an easy matter to write a computer program to find given q_1, q_2, the congruence $|D|$ must satisfy to make at most one of the $c_\psi \neq 0$. The results of such a search are presented in the next section. It follows from them that if we only require

card $C \geqslant 2$, the conditions on r in Proposition 5 can be relaxed to $r \nmid 4 \cdot 3 \cdot 5$, $r \neq 8,\ 24$ and both (a), (c). □

Remark. Using Proposition 5 one can find all pairs $\langle q_1, q_2 \rangle$ such that $C(D, q_1, q_2)$ consists only of real characters for at least one D in $\mathscr{F}$ prime to r. For such pairs and for all D in $\mathscr{F}$ from a certain arithmetic progression,

$$S(D, q_1, q_2) = \sum_{i=1}^{k} a_i h(-e_i|D|),$$

where the coefficients a_i, e_i do not depend on D.

5. Tables

The following table lists values for r, q_1, q_2, s_0, and m such that $0 \leqslant q_1 < q_2$, $q_1 + q_2 \leqslant 1$ and $q_2 \leqslant \frac{1}{2}$ if $q_1 = 0$, r is the least common denominator of q_1, q_2 and

$$\sum_{q_1|D|<n<q_2|D|} \left(\frac{D}{n}\right) = 0,$$

for all fundamental discriminants $D \neq 1$ (in fact, for all non-square discriminants D) such that $|D| \equiv s_0 \pmod m$. For $q_2 > \frac{1}{2}$ we exclude $D > 0$. There are 55 such formulae.

r	q_1, q_2	s_0;m
2	$0, \frac{1}{2}$	1;4
4	$0, \frac{1}{4}$	3;8
4	$\frac{1}{4}, \frac{1}{2}$	7;8
6	$0, \frac{1}{6}$	5;8
6	$\frac{1}{6}, \frac{1}{3}$	11;12
6	$\frac{1}{6}, \frac{1}{2}$	5, 7;8*
6	$\frac{1}{6}, \frac{5}{6}$	5;8
6	$\frac{1}{3}, \frac{1}{2}$	23;24
10	$0, \frac{1}{10}$	3, 27;40
10	$0, \frac{3}{10}$	3, 27;40
10	$\frac{1}{10}, \frac{3}{10}$	3;8
18	$\frac{1}{9}, \frac{5}{18}$	11;24
18	$\frac{7}{18}, \frac{4}{9}$	11;24

r	q_1, q_2	s_0;m
12	$0, \frac{1}{12}$	5;24
12	$0, \frac{5}{12}$	5;24
12	$\frac{1}{12}, \frac{1}{6}$	5;24
12	$\frac{1}{12}, \frac{1}{4}$	13;24
12	$\frac{1}{12}, \frac{1}{3}$	17;24
12	$\frac{1}{12}, \frac{5}{12}$	5;8
12	$\frac{1}{12}, \frac{1}{2}$	5;24
12	$\frac{1}{12}, \frac{7}{12}$	5;12
12	$\frac{1}{12}, \frac{5}{6}$	5;24
12	$\frac{1}{12}, \frac{11}{12}$	5;24
12	$\frac{1}{6}, \frac{1}{4}$	7;8
30	$\frac{1}{30}, \frac{1}{5}$	73, 97;120
30	$\frac{1}{30}, \frac{11}{30}$	17, 33;40

r	q_1, q_2	s_0;m
12	$\frac{1}{6}, \frac{5}{12}$	5;24
12	$\frac{1}{6}, \frac{7}{12}$	5;24
12	$\frac{1}{4}, \frac{1}{3}$	23;24
12	$\frac{1}{4}, \frac{5}{12}$	13;24
12	$\frac{1}{3}, \frac{7}{12}$	17;24
12	$\frac{5}{12}, \frac{1}{2}$	5;24
12	$\frac{5}{12}, \frac{7}{12}$	5;24
14	$\frac{1}{14}, \frac{2}{7}$	3, 19, 27;56
14	$\frac{1}{7}, \frac{3}{14}$	3, 19, 27;56**
14	$\frac{5}{14}, \frac{3}{7}$	3, 19, 27;56**
18	$\frac{1}{18}, \frac{2}{9}$	11;24
30	$\frac{11}{30}, \frac{3}{5}$	17, 113;120
30	$\frac{2}{5}, \frac{17}{30}$	73, 97;120

* This case was listed in [4] only for $D = p \equiv 5 \pmod 8$.

** These cases were listed in [4] for $D = -p$ with a misprint, 9 instead of 19.

r	q_1, q_2	$s_0;m$
20	$\frac{1}{10}, \frac{1}{4}$	3, 27;40
20	$\frac{1}{4}, \frac{3}{10}$	3, 27;40
24	$\frac{1}{24}, \frac{5}{24}$	13;24
24	$\frac{1}{24}, \frac{11}{24}$	5;24
24	$\frac{5}{24}, \frac{7}{24}$	5;24
24	$\frac{7}{24}, \frac{11}{24}$	13;24

r	q_1, q_2	$s_0;m$
30	$\frac{1}{30}, \frac{3}{5}$	17, 113;120
30	$\frac{1}{10}, \frac{1}{6}$	11, 59;120
30	$\frac{1}{10}, \frac{1}{3}$	11, 59;120
30	$\frac{1}{6}, \frac{3}{10}$	11, 59;120
30	$\frac{1}{5}, \frac{7}{30}$	17, 113;120
30	$\frac{1}{5}, \frac{11}{30}$	73, 97;120

r	q_1, q_2	$s_0;m$
30	$\frac{1}{5}, \frac{17}{30}$	17, 113;120
30	$\frac{7}{30}, \frac{2}{5}$	73, 97;120
30	$\frac{7}{30}, \frac{17}{30}$	17, 33;40
30	$\frac{3}{10}, \frac{1}{3}$	11, 59;120

In the following table we list values for e, q_1, q_2, c, s_0, and m such that $0 \leqslant q_1 < q_2$, $q_1 + q_2 \leqslant 1$, $q_2 \leqslant \frac{1}{2}$ if $q_1 = 0$

$$c \sum_{q_1|D|<n<q_2|D|} \left(\frac{D}{n}\right) = h(-e|D|),$$

for all fundamental discriminants $D \neq 1$ relatively prime to r such that $|D| \equiv s_0 \pmod m$, $e|D| > 4$ and if m is odd, D has the prescribed sign. For $q_2 > \frac{1}{2}$ we exclude $D < 0$. We list 222 such formulae involving 116 different pairs $\langle q_1, q_2\rangle$. The section number sign "§" (resp., dagger "†") means that $D < 0$ (resp., $D > 0$).

e	q_1, q_2	c	$s_0;m$
1	$0, \frac{1}{2}$	$\frac{1}{3}$	3;8
1	$0, \frac{1}{2}$	1	7;8
1	$0, \frac{1}{3}$	$\frac{1}{2}$	1;3§
1	$0, \frac{1}{3}$	1	2;3§
1	$0, \frac{1}{4}$	1	7;8
1	$\frac{1}{4}, \frac{1}{2}$	$\frac{1}{3}$	3;8
1	$0, \frac{1}{6}$	-1	19;24
1	$0, \frac{1}{6}$	1	7, 11, 23;24
1	$\frac{1}{6}, \frac{1}{3}$	$\frac{1}{3}$	19;24
1	$\frac{1}{6}, \frac{1}{3}$	1	7;24
1	$\frac{1}{6}, \frac{1}{2}$	$\frac{1}{4}$	19;24
1	$\frac{1}{6}, \frac{1}{2}$	$\frac{1}{2}$	11;24
1	$\frac{1}{3}, \frac{1}{2}$	-1	7;24
1	$\frac{1}{3}, \frac{1}{2}$	$\frac{1}{2}$	11;24
1	$\frac{1}{3}, \frac{1}{2}$	1	19;24
1	$0, \frac{1}{10}$	1	11, 19;40
1	$0, \frac{3}{10}$	1	11, 19;40
1	$\frac{1}{10}, \frac{1}{2}$	$\frac{1}{3}$	3, 27;40

e	q_1, q_2	c	$s_0;m$
1	$\frac{1}{10}, \frac{1}{2}$	$\frac{1}{2}$	11, 19;40
1	$\frac{3}{10}, \frac{1}{2}$	$\frac{1}{3}$	3, 27;40
1	$\frac{3}{10}, \frac{1}{2}$	$\frac{1}{2}$	11, 19;40
1	$\frac{1}{6}, \frac{1}{4}$	-1	11;24
1	$\frac{1}{6}, \frac{1}{4}$	1	19;24
1	$\frac{1}{4}, \frac{1}{3}$	$\frac{1}{2}$	19;24
1	$\frac{1}{4}, \frac{1}{3}$	1	7, 11;24
1	$\frac{1}{14}, \frac{2}{7}$	1	11, 43, 51;56
1	$\frac{1}{7}, \frac{3}{14}$	-1	11, 43, 51;56
1	$\frac{5}{14}, \frac{3}{7}$	1	11, 43, 51;56
1	$\frac{1}{18}, \frac{2}{9}$	-1	19;24
1	$\frac{1}{9}, \frac{5}{18}$	1	19;24
1	$\frac{7}{18}, \frac{4}{9}$	-1	19;24
1	$\frac{1}{10}, \frac{1}{4}$	-1	11, 19;40
1	$\frac{1}{4}, \frac{3}{10}$	1	11, 19;40
1	$\frac{1}{10}, \frac{1}{6}$	-1	43, 67;120
1	$\frac{1}{10}, \frac{1}{6}$	$-\frac{1}{2}$	19, 91;120
1	$\frac{1}{10}, \frac{1}{6}$	1	83, 107;120

e	q_1, q_2	c	$s_0;m$
1	$\frac{1}{10}, \frac{1}{3}$	$\frac{1}{2}$	43, 67;120
1	$\frac{1}{10}, \frac{1}{3}$	1	19, 83;120
			91, 107;120
1	$\frac{1}{6}, \frac{3}{10}$	-1	83, 107;120
1	$\frac{1}{6}, \frac{3}{10}$	$\frac{1}{2}$	19, 91;120
1	$\frac{1}{6}, \frac{3}{10}$	1	43, 67;120
1	$\frac{3}{10}, \frac{1}{3}$	$\frac{1}{2}$	43, 67;120
1	$\frac{3}{10}, \frac{1}{3}$	1	19, 83;120
			91, 107;120
3	$0, \frac{1}{3}$	2	0;1†
3	$\frac{1}{3}, \frac{2}{3}$	-1	0;1†
3	$0, \frac{1}{6}$	1	1;8
3	$\frac{1}{6}, \frac{1}{3}$	-2	1;8
3	$\frac{1}{6}, \frac{1}{3}$	2	5;8
3	$\frac{1}{6}, \frac{1}{2}$	-1	1;8
3	$\frac{1}{6}, \frac{2}{3}$	-2	5;8
3	$\frac{1}{6}, \frac{2}{3}$	$-\frac{2}{3}$	1;8
3	$\frac{1}{6}, \frac{5}{6}$	$-\frac{1}{2}$	1;8

e	q_1, q_2	c	s_0;m
3	$\frac{1}{3}, \frac{1}{2}$	-2	1;4
3	$0, \frac{1}{12}$	2	17;24
3	$0, \frac{5}{12}$	-2	17;24
3	$\frac{1}{12}, \frac{1}{6}$	2	17;24
3	$\frac{1}{12}, \frac{1}{4}$	-2	1;24
3	$\frac{1}{12}, \frac{1}{3}$	2	5;24
3	$\frac{1}{12}, \frac{5}{12}$	-1	1;8
3	$\frac{1}{12}, \frac{1}{2}$	-2	17;24
3	$\frac{1}{12}, \frac{2}{3}$	-2	5;24
3	$\frac{1}{12}, \frac{2}{3}$	-1	17;24
3	$\frac{1}{12}, \frac{5}{6}$	$-\frac{2}{3}$	17;24
3	$\frac{1}{12}, \frac{11}{12}$	-1	17;24
3	$\frac{1}{6}, \frac{5}{12}$	$-\frac{2}{3}$	17;24
3	$\frac{1}{6}, \frac{7}{12}$	-2	17;24
3	$\frac{1}{4}, \frac{5}{12}$	-2	1;24
3	$\frac{1}{3}, \frac{5}{12}$	-2	5;24
3	$\frac{1}{3}, \frac{5}{12}$	-1	17;24
3	$\frac{1}{3}, \frac{7}{12}$	-2	5;24
3	$\frac{5}{12}, \frac{1}{2}$	2	17;24
3	$\frac{5}{12}, \frac{7}{12}$	1	17;24
3	$\frac{1}{18}, \frac{2}{9}$	-2	1;24
3	$\frac{1}{18}, \frac{2}{9}$	2	17;24
3	$\frac{1}{9}, \frac{5}{18}$	-2	1;24
3	$\frac{1}{9}, \frac{5}{18}$	2	17;24
3	$\frac{7}{18}, \frac{5}{9}$	-2	1;24
3	$\frac{7}{18}, \frac{5}{9}$	2	17;24
3	$\frac{1}{24}, \frac{5}{24}$	-2	1;24
3	$\frac{1}{24}, \frac{11}{24}$	-2	17;24
3	$\frac{5}{24}, \frac{7}{24}$	2	17;24
3	$\frac{7}{24}, \frac{11}{24}$	-2	1;24
3	$\frac{1}{30}, \frac{1}{5}$	-2	1, 49;120
3	$\frac{1}{30}, \frac{11}{30}$	-1	1, 41;120
			49, 89;120
3	$\frac{1}{30}, \frac{3}{5}$	-2	41, 89;120

e	q_1, q_2	c	s_0;m
3	$\frac{7}{30}, \frac{2}{5}$	-2	1, 49;120
3	$\frac{7}{30}, \frac{17}{30}$	-1	1, 41;120
			49, 89;120
3	$\frac{11}{30}, \frac{3}{5}$	2	41, 89;120
3	$\frac{2}{5}, \frac{17}{30}$	-2	1, 49;120
3	$\frac{1}{60}, \frac{11}{60}$	-2	1, 49;120
3	$\frac{7}{60}, \frac{17}{60}$	-2	1, 49;120
3	$\frac{13}{60}, \frac{23}{60}$	-2	1, 49;120
3	$\frac{19}{60}, \frac{29}{60}$	-2	1, 49;120
4	$0, \frac{1}{4}$	2	1;4
4	$\frac{1}{4}, \frac{1}{2}$	-2	1;4
4	$\frac{1}{4}, \frac{3}{4}$	-1	1;4
4	$\frac{1}{8}, \frac{3}{8}$	-2	1;8
4	$\frac{1}{8}, \frac{3}{8}$	2	5;8
4	$0, \frac{1}{12}$	2	13;24
4	$0, \frac{5}{12}$	2	13;24
4	$\frac{1}{12}, \frac{1}{6}$	-2	13;24
4	$\frac{1}{12}, \frac{1}{4}$	2	5;24
4	$\frac{1}{12}, \frac{1}{3}$	-2	1;24
4	$\frac{1}{12}, \frac{1}{2}$	-2	13;24
4	$\frac{1}{12}, \frac{7}{12}$	-1	1;12
4	$\frac{1}{12}, \frac{3}{4}$	-2	5;24
4	$\frac{1}{12}, \frac{3}{4}$	-1	13;24
4	$\frac{1}{12}, \frac{5}{6}$	-2	13;24
4	$\frac{1}{12}, \frac{11}{12}$	-1	13;24
4	$\frac{1}{6}, \frac{1}{4}$	2	5;8
4	$\frac{1}{6}, \frac{5}{12}$	2	13;24
4	$\frac{1}{6}, \frac{7}{12}$	-2	13;24
4	$\frac{1}{6}, \frac{3}{4}$	-2	5;8
4	$\frac{1}{4}, \frac{5}{12}$	-2	5;24
4	$\frac{1}{4}, \frac{7}{12}$	-2	5;24
4	$\frac{1}{4}, \frac{7}{12}$	-1	13;24
4	$\frac{1}{3}, \frac{7}{12}$	-2	1;24
4	$\frac{5}{12}, \frac{1}{2}$	-2	13;24

e	q_1, q_2	c	s_0;m
4	$\frac{1}{24}, \frac{11}{24}$	2	13;24
4	$\frac{5}{24}, \frac{7}{24}$	2	13;24
4	$\frac{5}{24}, \frac{11}{24}$	-2	1;24
4	$\frac{5}{24}, \frac{11}{24}$	2	13;24
4	$\frac{1}{60}, \frac{11}{60}$	2	73, 97;120
4	$\frac{7}{60}, \frac{17}{60}$	-2	73, 97;120
4	$\frac{13}{60}, \frac{23}{60}$	2	73, 97;120
4	$\frac{19}{60}, \frac{29}{60}$	-2	73, 97;120
5	$\frac{1}{5}, \frac{2}{5}$	2	0;1[§]
5	$\frac{1}{10}, \frac{1}{5}$	-4	11, 19;40
5	$\frac{1}{10}, \frac{1}{5}$	4	31, 39;40
5	$\frac{1}{10}, \frac{3}{10}$	1	7;8
5	$\frac{1}{10}, \frac{2}{5}$	$\frac{4}{3}$	31, 39;40
5	$\frac{1}{10}, \frac{2}{5}$	4	11, 19;40
5	$\frac{1}{10}, \frac{1}{2}$	2	7;8
5	$\frac{1}{5}, \frac{3}{10}$	$\frac{4}{3}$	31, 39;40
5	$\frac{1}{5}, \frac{3}{10}$	4	11, 19;40
5	$\frac{1}{5}, \frac{1}{2}$	4	31, 39;40
5	$\frac{3}{10}, \frac{2}{5}$	-4	31, 39;40
5	$\frac{3}{10}, \frac{2}{5}$	4	11, 19;40
5	$\frac{3}{10}, \frac{1}{2}$	-2	7;8
5	$\frac{2}{5}, \frac{1}{2}$	-4	31, 39;40
5	$\frac{1}{5}, \frac{1}{3}$	4	11, 14;15[§]
5	$\frac{1}{3}, \frac{2}{5}$	4	11, 14;15[§]
5	$\frac{1}{10}, \frac{1}{4}$	2	7;8
5	$\frac{1}{5}, \frac{1}{4}$	4	31, 39;40
5	$\frac{1}{4}, \frac{3}{10}$	2	7;8
5	$\frac{1}{4}, \frac{2}{5}$	4	31, 39;40
5	$\frac{1}{10}, \frac{1}{6}$	2	7;8
5	$\frac{1}{10}, \frac{1}{3}$	2	23;24
5	$\frac{1}{6}, \frac{1}{5}$	-4	11, 31, 59;120
			71, 79;120
			119;120
5	$\frac{1}{6}, \frac{3}{10}$	2	7;8

e	q_1, q_2	c	s_0;m
3	$\frac{1}{5}, \frac{7}{30}$	2	41, 89;120
3	$\frac{1}{5}, \frac{11}{30}$	−2	1, 49;120
3	$\frac{1}{5}, \frac{17}{30}$	−2	41, 89;120
5	$\frac{3}{10}, \frac{1}{3}$	−2	23;24
7	$\frac{1}{14}, \frac{2}{7}$	2	5;8
7	$\frac{1}{7}, \frac{11}{14}$	−2	5;8
7	$\frac{5}{14}, \frac{3}{7}$	−2	5;8
8	$\frac{1}{8}, \frac{1}{4}$	4	7;8
8	$\frac{1}{8}, \frac{3}{8}$	2	3;4
8	$\frac{1}{8}, \frac{1}{2}$	4	7;8
8	$\frac{1}{8}, \frac{5}{8}$	−2	1;4
8	$\frac{1}{4}, \frac{3}{8}$	4	7;8
8	$\frac{3}{8}, \frac{1}{2}$	−4	7;8
8	$\frac{1}{24}, \frac{5}{24}$	2	5;24
8	$\frac{1}{24}, \frac{7}{24}$	2	5;12
8	$\frac{1}{8}, \frac{1}{6}$	4	7;8
8	$\frac{1}{8}, \frac{1}{3}$	4	23;24
8	$\frac{1}{6}, \frac{3}{8}$	4	7;8
8	$\frac{5}{24}, \frac{11}{24}$	−2	5;12
8	$\frac{7}{24}, \frac{11}{24}$	−2	5;24
8	$\frac{1}{3}, \frac{3}{8}$	4	23;24
12	$\frac{1}{12}, \frac{1}{6}$	4	7, 11, 23;24
12	$\frac{1}{12}, \frac{1}{4}$	4	7;8
12	$\frac{1}{12}, \frac{1}{3}$	4	11, 19, 23;24
12	$\frac{1}{12}, \frac{5}{12}$	2	7, 11;24
			19, 23;24
12	$\frac{1}{12}, \frac{1}{2}$	4	7;8
12	$\frac{1}{6}, \frac{5}{12}$	4	7, 11, 23;24

e	q_1, q_2	c	s_0;m
4	$\frac{5}{12}, \frac{7}{12}$	−1	13;24
4	$\frac{1}{24}, \frac{7}{24}$	−2	1;24
4	$\frac{1}{24}, \frac{7}{24}$	2	13;24
12	$\frac{1}{4}, \frac{5}{12}$	4	7;8
12	$\frac{1}{3}, \frac{5}{12}$	4	11, 19, 23;24
12	$\frac{5}{12}, \frac{1}{2}$	−4	7;8
12	$\frac{1}{24}, \frac{5}{24}$	−4	19;24
12	$\frac{1}{24}, \frac{5}{24}$	4	7;24
12	$\frac{7}{24}, \frac{11}{24}$	−4	7;24
12	$\frac{7}{24}, \frac{11}{24}$	4	19;24
12	$\frac{1}{12}, \frac{1}{10}$	4	11, 59;120
12	$\frac{1}{12}, \frac{3}{10}$	4	11, 59;120
12	$\frac{1}{10}, \frac{5}{12}$	4	11, 59;120
12	$\frac{3}{10}, \frac{5}{12}$	4	11, 59;120
15	$\frac{1}{15}, \frac{11}{15}$	−4	$\pm 2;5^{\dagger}$
15	$\frac{2}{15}, \frac{7}{15}$	−4	$\pm 2;5^{\dagger}$
15	$\frac{1}{30}, \frac{1}{5}$	4	29, 53;120
			77, 101;120
15	$\frac{1}{30}, \frac{11}{30}$	2	13, 29, 37;120
			53, 61, 77;120
			101, 109;120
15	$\frac{1}{30}, \frac{2}{5}$	4	13;24
15	$\frac{1}{5}, \frac{11}{30}$	4	29, 53;120
			77, 101;120
15	$\frac{1}{5}, \frac{13}{30}$	4	13;24
15	$\frac{1}{5}, \frac{23}{30}$	−4	13;24
15	$\frac{7}{30}, \frac{2}{5}$	−4	29, 53;120
			77, 101;120

e	q_1, q_2	c	s_0;m
5	$\frac{1}{6}, \frac{2}{5}$	4	11, 31, 59;120
			71, 79;120
			119;120
15	$\frac{7}{30}, \frac{17}{30}$	−2	13, 29, 37;120
			53, 61, 77;120
			101, 109;120
15	$\frac{11}{30}, \frac{2}{5}$	−4	13;24
15	$\frac{2}{5}, \frac{17}{30}$	−4	29, 53;120
			77, 101;120
15	$\frac{1}{60}, \frac{11}{60}$	−4	61, 109;120
15	$\frac{7}{60}, \frac{17}{60}$	4	61, 109;120
15	$\frac{13}{60}, \frac{23}{60}$	4	61, 109;120
15	$\frac{19}{60}, \frac{29}{60}$	−4	61, 109;120
20	$\frac{1}{20}, \frac{11}{20}$	−4	1, 9;20
20	$\frac{3}{20}, \frac{13}{20}$	−4	1, 9;20
20	$\frac{1}{60}, \frac{11}{60}$	4	17, 113;120
20	$\frac{7}{60}, \frac{17}{60}$	4	17, 113;120
20	$\frac{13}{60}, \frac{23}{60}$	−4	17, 113;120
20	$\frac{19}{60}, \frac{29}{60}$	−4	17, 113;120
24	$\frac{1}{24}, \frac{11}{24}$	4	7;12
24	$\frac{1}{24}, \frac{13}{24}$	−4	1;12
24	$\frac{1}{24}, \frac{17}{24}$	−4	5;8
24	$\frac{1}{24}, \frac{19}{24}$	−4	5;12
24	$\frac{5}{24}, \frac{7}{24}$	4	7;12
24	$\frac{5}{24}, \frac{13}{24}$	−4	5;8
24	$\frac{5}{24}, \frac{17}{24}$	−4	1;12
24	$\frac{7}{24}, \frac{13}{24}$	−4	5;12

References

[1] B. C. Berndt, *Classical theorems on quadratic residues*. Enseignement Math. (2) 22 (1976), 261–304.

[2] H. Hasse, *Vorlesungen über Zahlentheorie*. Springer, Berlin 1964.

[3] R. H. Hudson, K. S. Williams, *Class number formulae of Dirichlet type*. Math. Comp. 39 (1982), 725–732.

[4] W. Johnson, K. J. Mitchell, *Symmetries for sums of the Legendre symbol*. Pacific J. Math. 69 (1977), 117–124.

[5] J. Szmidt, J. Urbanowicz, D. Zagier, *Congruences among generalized Bernoulli numbers*. Acta Arith. 71 (1995), 273–278.

[6] L. C. Washington, *Introduction to Cyclotomic Fields*. Grad. Texts in Math. 83. Second ed., Springer, New York 1997.

Part L

Geometry of numbers

Commentary on L: Geometry of numbers

by Wolfgang M. Schmidt

When $\boldsymbol{x}$ is a point in $\mathbb{Z}^k$, write $h(\boldsymbol{x})$ for its maximum norm, and when $S \subset \mathbb{R}^k$ is a rational subspace of dimension m, write $\widehat{H}(S) = h(\boldsymbol{X})$, where $\boldsymbol{X} \in \mathbb{Z}^{\binom{k}{m}}$ is a Grassmann vector of S with coprime coordinates. When $0 < m \le \ell \le k$ and $m < k$, and S is again of dimension m, then there are linearly independent integer points $\boldsymbol{p}_1, \dots, \boldsymbol{p}_\ell$ whose span contains S and which have

$$\prod_{i=1}^{\ell} h(\boldsymbol{p}_i) \le c\widehat{H}(S)^{(k-\ell)/(k-m)}$$

with a constant c depending on k, ℓ, m.

The series of papers [5], **L1**, [6], **L2** is concerned with the infimum $c_0(k, \ell, m)$ of the constants c where this holds. In **L1** the value $c_0(3, 2, 1) = 2/\sqrt{3}$ is established, whereas in **L2** an upper bound for $c_0(k, \ell, m)$ is given, with equality when $\ell = m \le 2$. These bounds are independent of k, but in [4] an estimate is given which depends on k and is better when $k = o(\ell^2)$. Very roughly speaking, the argument depends on two steps, first the existence of a rational space $T \supset S$ of dimension ℓ with small $\widehat{H}(T)$, and then of ℓ independent integer points $\boldsymbol{p}_1, \dots, \boldsymbol{p}_\ell$ in T with small product $\prod h(\boldsymbol{p}_i)$. Lemma 1 of **L2** is of independent interest and gives a purely geometric fact about parallelopipeds containing a given parallelohedron.

In the related work **L4** the analog of the above problem is taken up with the Euclidean norm $|\boldsymbol{x}|$ in place of $h(\boldsymbol{x})$ and with $H(S) = |\boldsymbol{X}|$ in place of $\widehat{H}(S) = h(\boldsymbol{X})$. Let $c(k, \ell, m)$ be the analog of $c_0(k, \ell, m)$. Given a lattice Λ and s with $0 < s < \operatorname{rank} \Lambda$, let $\gamma_s(\Lambda)$ be minimal such that there is a sublattice $\Gamma \subset \Lambda$ of rank s with $\det \Gamma \le \gamma_s(\Lambda)(\det \Lambda)^{s/r}$, and for $r > s$ let $\gamma_{r,s}$ (the generalized Hermite constant as defined by Rankin) be the supremum of $\gamma_s(\Lambda)^2$ over all lattices Λ of rank r (so that $\gamma_r = \gamma_{r1}$ is the ordinary Hermite constant). Then

$$\gamma_{k-m,k-\ell}^{1/2} \le c(k, \ell, m) \le \gamma_{k-m,k-\ell}^{1/2} \gamma_\ell^{1/2}.$$

Also, $c(k, 2, 1) \to \infty$ as $k \to \infty$. The proof of the further estimate $c(3, 2, 1) \ge 6/(722)^{1/4}$ depends on the explicit construction of a sequence of one-dimensional subspaces. It is also shown that the successive minima $\lambda_i(\Lambda)$ $(i = 1, \dots, r)$ with respect to a symmetric convex

body of a full lattice Λ in $\mathbb{R}^r$ are continuous in the natural topology of the space of such lattices, and the same could easily be shown for the functions $\gamma_s(\Lambda)$.

In **L3** it is established that if certain sets of coprime polynomials in $\mathbb{Z}[T, T_1, \dots, T_\ell]$ have no fixed prime divisor as $(t, t_1, \dots, t_\ell)$ ranges through $\mathbb{Z}^{\ell+1}$, then there are integers $t_1^*, \dots, t_\ell^*$ and an arithmetic progression $\mathcal{P}$ such that these sets of polynomials are coprime at $(t, t_1^*, \dots, t_\ell^*)$ for every $t \in \mathcal{P}$. This is later used to prove the interesting but not explicitly stated fact that when $\boldsymbol{b}_1, \dots, \boldsymbol{b}_\ell$ are independent points in $\mathbb{Z}^{\ell+1}$, then for every t in a certain arithmetic progression there are points $\boldsymbol{g}_1, \dots, \boldsymbol{g}_\ell$ with $|\boldsymbol{g}_i - t\boldsymbol{b}_i| \ll 1\,(i = 1, \dots, \ell)$ which are the basis of a primitive lattice in $\mathbb{Z}^{\ell+1}$. Of a theorem on the Geometry of Numbers whose proof is stated to be a generalization of arguments of Chaładus and Aliev, we will mention only some consequences. For $\ell \geq 2$ let $c(\ell, \infty)$ be the infimum of the constants c such that for every $\boldsymbol{x} \in \mathbb{Z}^{\ell+1} \setminus \{\boldsymbol{0}\}$ there is an $\boldsymbol{a} \in \mathbb{Z}^{\ell+1} \setminus \{\boldsymbol{0}\}$ with inner product $\boldsymbol{ax} = 0$ and $h(\boldsymbol{a}) \leq ch(\boldsymbol{x})^{1/\ell}$. Then $c(\ell, \infty) \geq 1$ and $c(2, \infty) = 4/3$, $c(3, \infty) = 27/19$. As for Siegel's Lemma, suppose $A \subset \mathbb{R}^n$ is a rational subspace of dimension $m < n$. Then there is an integer point $\boldsymbol{x} \in \mathbb{Z}^n \setminus \{\boldsymbol{0}\}$ which is orthogonal to A and has $|\boldsymbol{x}| \leq \gamma_{n-m}^{1/2} H(A)^{1/(n-m)}$, and here the constant $\gamma_{n-m}^{1/2}$ is best possible. This can also be derived from [7] or [8].

References

[1] I. Aliev, *On a decomposition of integer vectors*. Ph.D. Thesis. Institute of Mathematics, Polish Academy of Sciences, Warsaw 2001.

[2] —, *On a decomposition of integer vectors* II. Acta Arith. 102 (2002), 373–391.

[3] S. Chaładus, *On the densest lattice packing of centrally symmetric octahedra*. Math. Comp. 58 (1992), 341–345.

[4] S. Chaładus, Yu. Teterin, *Note on a decomposition of integer vectors* II. Acta Arith. 57 (1991), 159–164.

[5] A. Schinzel, *A decomposition of integer vectors* I. Bull. Polish Acad. Sci. Math. 35 (1987), 155–159.

[6] —, *A decomposition of integer vectors* III. Bull. Polish Acad. Sci. Math. 35 (1987), 693–703.

[7] J. L. Thunder, *An adelic Minkowski–Hlawka theorem and an application to Siegel's lemma*. J. Reine Angew. Math. 475 (1996), 167–185.

[8] T. Watanabe, *On an analog of Hermite's constant*. J. Lie Theory 10 (2000), 33–52.

Andrzej Schinzel
Selecta

Originally published in
PLISKA Studia mathematica bulgarica
11 (1991), 15–23

A decomposition of integer vectors II

with S. Chaładus (*Warszawa*)

In this paper we shall consider integer vectors $\boldsymbol{n} = [n_1, n_2, \ldots, n_k]$ and write for such vectors: $h(\boldsymbol{n}) = \max |n_i|, l(\boldsymbol{n}) = \sqrt{n_1^2 + n_2^2 + \ldots + n_k^2}$. One of us has recently proved [3] that for every non-zero vector $\boldsymbol{n} \in \mathbb{Z}^k$ $(k > 1)$ there is a decomposition: $\boldsymbol{n} = u\boldsymbol{p} + v\boldsymbol{q}$, $u, v \in \mathbb{Z}$, where $\boldsymbol{p}, \boldsymbol{q} \in \mathbb{Z}^k$ are linearly independent and

$$h(\boldsymbol{p})h(\boldsymbol{q}) \leqslant 2h(\boldsymbol{n})^{(k-2)/(k-1)}.$$

The exponent $(k-2)/(k-1)$ cannot be improved (see [2], Remark after Lemma 1). It is natural to ask for the best value of the coefficient. We shall answer this question for $k = 3$ by proving the following two theorems.

Theorem 1. *For every non-zero vector $\boldsymbol{n} \in \mathbb{Z}^3$ there exist linearly independent vectors $\boldsymbol{p}, \boldsymbol{q} \in \mathbb{Z}^3$, such that $\boldsymbol{n} = u\boldsymbol{p} + v\boldsymbol{q}$, $u, v \in \mathbb{Z}$ and*

$$h(\boldsymbol{p})h(\boldsymbol{q}) < \sqrt{\tfrac{4}{3}\, h(\boldsymbol{n})}.$$

Theorem 2. *For every $\varepsilon > 0$ there exists a non-zero vector $\boldsymbol{n} \in \mathbb{Z}^3$, such that for all non-zero vectors $\boldsymbol{p}, \boldsymbol{q} \in \mathbb{Z}^3$ and all $u, v \in \mathbb{Q}$, $\boldsymbol{n} = u\boldsymbol{p} + v\boldsymbol{q}$ implies*

$$h(\boldsymbol{p})h(\boldsymbol{q}) > \sqrt{\left(\tfrac{4}{3} - \varepsilon\right) h(\boldsymbol{n})}.$$

Originally, in the proof of Theorem 1 some computer calculations were used which were kindly performed by Dr. T. Regińska. We thank her for the help.

The proof of Theorem 1 will be based on geometry of numbers. The inner product of two vectors $\boldsymbol{n}, \boldsymbol{m}$ will be denoted by $\boldsymbol{nm}$, their exterior product by $\boldsymbol{n} \times \boldsymbol{m}$, the area of a plane domain $\boldsymbol{D}$ by $A(\boldsymbol{D})$.

Lemma 1. *Let a_i, b_i be real numbers $(i = 1, 2, 3)$ and M_1, M_2, M_3 the three minors of order two of the matrix $\begin{bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{bmatrix}$ not all equal to 0. The area of the domain $\boldsymbol{H}$: $|a_i x + b_i y| \leqslant 1$ $(i = 1, 2, 3)$ equals*

$$\frac{2|M_1M_2| + 2|M_1M_3| + 2|M_2M_3| - M_1^2 - M_2^2 - M_3^2}{|M_1M_2M_3|}$$

if each of the numbers $|M_1|, |M_2|, |M_3|$ *is less than the sum of the two others, and* $4/\max\{|M_1|, |M_2|, |M_3|\}$ *otherwise.*

Proof. We may assume without loss of generality that

$$|M_1| = \operatorname{abs}\begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} > 0, \quad |M_1| \geqslant |M_2| = \operatorname{abs}\begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix}, \quad |M_1| \geqslant |M_3| = \operatorname{abs}\begin{vmatrix} a_1 & a_3 \\ b_1 & b_3 \end{vmatrix}.$$

The affine transformation $a_1x + b_1y = X$, $a_2x + b_2y = Y$ transforms the domain $\boldsymbol{H}$ into the domain

$$\boldsymbol{H}' : |X| \leqslant 1,\ |Y| \leqslant 1;\ \left|\frac{M_2}{M_1}\,X - \frac{M_3}{M_1}\,Y\right| \leqslant 1.$$

If $|M_2| + |M_3| > |M_1|$, the domain $\boldsymbol{H}'$ is obtained from the square $|X| \leqslant 1$, $|Y| \leqslant 1$ by subtracting two rectangular triangles, symmetric to each other with respect to $(0, 0)$, with the vertices

$$\pm\Big(1, -\operatorname{sgn}\frac{M_2}{M_3}\,\frac{|M_1| - |M_2|}{|M_3|}\Big), \quad \pm\Big(1, -\operatorname{sgn}\frac{M_2}{M_3}\Big), \quad \pm\Big(\frac{|M_1| - |M_3|}{|M_2|}, -\operatorname{sgn}\frac{M_2}{M_3}\Big).$$

Hence,

$$A(\boldsymbol{H}') = 4 - \frac{(|M_2| + |M_3| - |M_1|)^2}{|M_2|\,|M_3|}.$$

If $|M_2|+|M_3| \leqslant |M_1|$, then $\boldsymbol{H}'$ coincides with the square $|X| \leqslant 1, |Y| \leqslant 1$ and $A(\boldsymbol{H}') = 4$. Since $A(\boldsymbol{H}) = A(\boldsymbol{H}')/|M_1|$, the lemma follows. □

Lemma 2. *If* $0 \leqslant a \leqslant b < 1$, *then the domain*

$$\boldsymbol{D} : |x| \leqslant 1,\ |y| \leqslant 1,\ |ax + by| \leqslant 1,\ x^2 + y^2 + (ax + by)^2 \leqslant \tfrac{3}{2}$$

contains an ellipse $\boldsymbol{E}$ *with*

$$A(\boldsymbol{E}) > \pi\sqrt{\tfrac{3}{4}}. \tag{1}$$

Proof. We take

$$\boldsymbol{E} : f(x, y) = x^2 + c\Big(\frac{ab}{b^2 + 1}\,x + y\Big)^2 \leqslant 1,$$

where

$$c = \max\Big\{\frac{2}{3}\,(b^2 + 1),\ \frac{(b^2 + 1)^2}{(b^2 + 1)^2 - a^2b^2}\Big\}. \tag{2}$$

In order to see that $|x| \leqslant 1$, $|y| \leqslant 1$ for $(x, y) \in \boldsymbol{E}$, we notice that by (2)

$$\min_y f(x, y) = x^2, \quad \min_x f(x, y) = \frac{c}{c\,\frac{a^2b^2}{(b^2+1)^2} + 1}\,y^2 \geqslant y^2. \tag{3}$$

Moreover, for $(x, y) \in \boldsymbol{E}$ we have by (2)

$$(4)\quad x^2 + y^2 + (ax + by)^2 \leqslant \frac{3}{2}\left(\frac{2}{3}\,\frac{a^2+b^2+1}{b^2+1}\,x^2 + \frac{2}{3}\,(b^2+1)\Big(\frac{ab}{b^2+1}\,x + y\Big)^2\right) \leqslant \frac{3}{2}\,f(x, y) \leqslant \frac{3}{2}\,.$$

If for $(x, y) \in \boldsymbol{E}$ we had $|ax + by| > 1$, it would follow

$$(5)\qquad x^2 + y^2 < \tfrac{1}{2}\,,$$

hence, by the Cauchy–Schwarz inequality

$$(6)\qquad (ax + by)^2 \leqslant (a^2 + b^2)(x^2 + y^2) < 2 \cdot \tfrac{1}{2} = 1,$$

a contradiction. Thus, for $(x, y) \in \boldsymbol{E}$ we have

$$(7)\qquad |ax + by| \leqslant 1.$$

Finally, $A(\boldsymbol{E}) = \pi/\sqrt{c}$ and since by (2) $c < 4/3$, (1) follows. □

Lemma 3. *Let* $\boldsymbol{n} \in \mathbb{Z}^3 \setminus \{[0, 0, 0]\}$. *The lattice of integer vectors* $\boldsymbol{m} \in \mathbb{Z}^3$ *satisfying* $\boldsymbol{nm} = 0$ *has a basis* $\boldsymbol{a} = [a_1, a_2, a_3]$, $\boldsymbol{b} = [b_1, b_2, b_3]$, *such that*

$$(8)\quad \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} = \frac{n_3}{(n_1, n_2, n_3)}\,, \quad \begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix} = \frac{n_1}{(n_1, n_2, n_3)}\,, \quad \begin{vmatrix} a_3 & a_1 \\ b_3 & b_1 \end{vmatrix} = \frac{n_2}{(n_1, n_2, n_3)}\,.$$

Proof. Since $\boldsymbol{na} = \boldsymbol{nb} = 0$ and $\boldsymbol{a}, \boldsymbol{b}$ are linearly independent, we have

$$\boldsymbol{n} = c(\boldsymbol{a} \times \boldsymbol{b})$$

for a certain $c \in \mathbb{Q}$. However, the numbers $\begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}$, $\begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix}$ and $\begin{vmatrix} a_3 & a_1 \\ b_3 & b_1 \end{vmatrix}$ are relatively prime (see e.g. [1], p. 53); hence the formulae (8) hold with $\pm$ sign on the right hand side. Changing if necessary the order of $\boldsymbol{a}, \boldsymbol{b}$, we get the lemma. □

Lemma 4. *For every vector* $\boldsymbol{n} \in \mathbb{Z}^3$ *different from* $[0, 0, 0]$ *and* $[\pm 1, \pm 1, \pm 1]$ *for any choice of signs, there exists a vector* $\boldsymbol{m} \in \mathbb{Z}^3$ *such that*

$$(9)\qquad \boldsymbol{mn} = 0,$$

$$(10)\qquad 0 < h(\boldsymbol{m}) < \sqrt{\tfrac{4}{3}\,h(\boldsymbol{n})}$$

and

$$(11)\qquad l(\boldsymbol{m}) < \sqrt{2h(\boldsymbol{n})}\,.$$

Proof. Without loss of generality we may assume that

$$(12)\qquad 0 \leqslant n_1 \leqslant n_2 \leqslant n_3 > 0.$$

If $n_2 = n_3$ we take

$$\boldsymbol{m} = \begin{cases} [1, 0, 0] & \text{if } n_1 = 0, \\ [0, 1, -1] & \text{if } n_1 \neq 0, \end{cases}$$

and we find (9)–(11) satisfied, unless $n_1 = n_2 = n_3 = 1$. Therefore, we may assume besides (12) that $n_2 > n_3$.

In virtue of Lemma 2 the domain

$$\boldsymbol{D}:\ |X| \leqslant 1,\ |Y| \leqslant 1,\ \left|\frac{n_1}{n_3}X + \frac{n_2}{n_3}Y\right| \leqslant 1,\ X^2 + Y^2 + \left(\frac{n_1}{n_3}X + \frac{n_2}{n_3}Y\right)^2 \leqslant \frac{3}{2}$$

contains an ellipse $\boldsymbol{E}$ with $A(\boldsymbol{E}) > \pi\sqrt{3/4}$.

Let $\boldsymbol{a}, \boldsymbol{b}$ be a basis the existence of which is asserted by Lemma 3. The substitution

$$X = \frac{a_1 x + b_1 y}{\sqrt{\frac{4}{3}n_3}}, \quad Y = \frac{a_2 x + b_2 y}{\sqrt{\frac{4}{3}n_3}}$$

transforms $\boldsymbol{D}$ into the domain

$$\boldsymbol{D}':\ |a_i x + b_i y| \leqslant \sqrt{\tfrac{4}{3}n_3} \quad (i = 1, 2, 3), \quad \sum_{i=1}^{3}(a_i x + b_i y)^2 \leqslant 2n_3.$$

Hence, $\boldsymbol{D}'$ contains an ellipse $\boldsymbol{E}'$ with

$$A(\boldsymbol{E}') = \frac{4}{3}n_3\left|\begin{matrix} a_1 & a_2 \\ b_1 & b_2 \end{matrix}\right|^{-1} A(\boldsymbol{E}) > \pi\sqrt{\frac{4}{3}}\,(n_1, n_2, n_3) \geqslant \pi\sqrt{\frac{4}{3}},$$

by (8). Since the packing constant for ellipses is $\pi/\sqrt{12}$, it follows that $\boldsymbol{E}'$ and, hence, $\boldsymbol{D}'$ contains in its interior a point $(x_0, y_0) \in \mathbb{Z}^2$ different from $(0, 0)$. Putting $\boldsymbol{m} = x_0\boldsymbol{a} + y_0\boldsymbol{b}$, we get the assertion of the lemma. □

Lemma 5. *If* $0 \leqslant a \leqslant 1$, $0 \leqslant b \leqslant 1$ *and* $a + b > 1$, *the area of the hexagon* $|x| \leqslant 1$, $|y| \leqslant 1$, $|ax + by| \leqslant 1$ *is greater than* $\left(24/(a^2 + b^2 + 1)\right)^{1/2}$.

Proof. In virtue of Lemma 1 the area in question equals

$$(2ab + 2a + 2b - a^2 - b^2 - 1)/ab,$$

thus, it remains to prove that for (a, b) in the domain

$$\boldsymbol{G}:\ 0 \leqslant a \leqslant 1,\ 0 \leqslant b \leqslant 1,\ a + b > 1$$

the following inequality holds

$$f(a, b) = (2ab + 2a + 2b - a^2 - b^2 - 1)^2(a^2 + b^2 + 1) - 24a^2b^2 > 0.$$

We have $\partial\boldsymbol{G} = \boldsymbol{L}_1 \cup \boldsymbol{L}_2 \cup \boldsymbol{L}_3$, where

$$\boldsymbol{L}_1 = \{(a, 1) : 0 \leqslant a \leqslant 1\}, \quad \boldsymbol{L}_2 = \{(1, b) : 0 \leqslant b \leqslant 1\},$$
$$\boldsymbol{L}_3 = \{(a, 1 - a) : 0 \leqslant a \leqslant 1\}.$$

We find $f(a, 1) = a^2(a - 1)^3(a - 5) + 3a^2$, but $a^2(a - 1)^3(a - 5) \geqslant 0$ for $a \leqslant 1$, hence $f(a, 1) \geqslant 3a^2 \geqslant 0$. In view of symmetry between a and b, $f(1, b) \geqslant 3b^2 \geqslant 0$.

Moreover, $f(a, 1 - a) = 8a^2(1 - a)^2(2a - 1)^2 \geqslant 0$. Hence, for $(a, b) \in \partial\boldsymbol{G}$ we have $f(a, b) \geqslant 0$ with the equality attained only if $(a, b) \notin \boldsymbol{G}$. It suffices to show that in the interior of $\boldsymbol{G}$ the function $f(a, b)$ has no local extremum.

c Indeed, putting $g(a,b) = 2ab + 2a + 2b - a^2 - b^2 - 1$, we find

$$\frac{\partial f}{\partial a} = 2ag^2 + 2(2b + 2 - 2a)(a^2 + b^2 + 1)g - 48ab^2,$$
$$\frac{\partial f}{\partial b} = 2bg^2 + 2(2a + 2 - 2b)(a^2 + b^2 + 1)g - 48a^2b,$$

hence

$$a\frac{\partial f}{\partial a} - b\frac{\partial f}{\partial b} = 2(a-b)\big((a+b)g + (a^2+b^2+1)(2-2a-2b)\big),$$
$$b\frac{\partial f}{\partial a} - a\frac{\partial f}{\partial b} = 4(b-a)\big((a+b+1)(a^2+b^2+1)g - 12ab(a+b)\big).$$

The equations $\partial f/\partial a = \partial f/\partial b = 0$ imply $a = b$ or

$$(a+b)g + (a^2+b^2+1)(2-2a-2b) = 0, \tag{13}$$
$$(a+b+1)(a^2+b^2+1)g - 12ab(a+b) = 0.$$

Eliminating g from the above equations we obtain

c $$2(a^2+b^2+1)^2\big((a+b)^2 - 1\big) - 12ab(a+b)^2 = 0. \tag{14}$$

The left hand sides of the equations (13) and (14) are symmetric functions of a, b. Expressing them in terms of $s = a + b$ and $p = ab$, then eliminating p, we get

$$s(s-1)(2s-1)(4s^2 - s + 1) = 0.$$

c For $s = a + b > 1$ this is clearly impossible, there remains the possibility $a = b$. However, in that case

$$\frac{\partial f}{\partial a} = 16a^3 - 24a^2 + 18a - 4 = 2(2a-1)^3 + 3(2a-1) + 1 > 1. \qquad \square$$

Lemma 6. *For every non-zero vector $\boldsymbol{n} = [n_1, n_2, n_3] \in \mathbb{Z}^3$ there exist linearly independent vectors $\boldsymbol{p}, \boldsymbol{q} \in \mathbb{Z}^3$ such that $\boldsymbol{pn} = \boldsymbol{qn} = 0$, and*

$$h(\boldsymbol{p})h(\boldsymbol{q}) < \sqrt{\frac{2}{3}}\, l(\boldsymbol{n}),$$

if each of the numbers $|n_1|$, $|n_2|$, $|n_3|$ is less than the sum of the two others;

$$h(\boldsymbol{p})h(\boldsymbol{q}) \leqslant h(\boldsymbol{n}), \quad \textit{otherwise}.$$

Proof. We may assume without loss of generality that $0 \leqslant n_1 \leqslant n_2 \leqslant n_3 > 0$.

In virtue of Lemmata 1 and 5 the area $A(\boldsymbol{K})$ of the domain

$$\boldsymbol{K} : |X| \leqslant 1,\ |Y| \leqslant 1,\ \left|\frac{n_1}{n_3}X - \frac{n_2}{n_3}Y\right| \leqslant 1$$

satisfies

$$\begin{cases} A(\boldsymbol{K}) > \sqrt{\dfrac{24}{n_1^2+n_2^2+n_3^2}}\, n_3, & \text{if } n_1 + n_2 > n_3, \\ A(\boldsymbol{K}) = 4, & \text{otherwise.} \end{cases} \tag{15}$$

Let a, b be a basis the existence of which is asserted in Lemma 3. The affine transformation $X = a_1x + b_1y$, $Y = a_2x + b_2y$ transforms the domain $\boldsymbol{K}$ into the domain

$$\boldsymbol{K}' : |a_ix + b_iy| \leqslant 1 \quad (i = 1, 2, 3)$$

satisfying

$$A(\boldsymbol{K}') = A(\boldsymbol{K})\,\frac{(n_1, n_2, n_3)}{n_3}\,. \tag{16}$$

In virtue of Minkowski's second theorem there exist two linearly independent integer vectors $[x_1, y_1]$ and $[x_2, y_2]$ such that

$$|a_ix_j + b_iy_j| \leqslant \lambda_j \quad (i = 1, 2, 3;\ j = 1, 2) \tag{17}$$

and

$$\lambda_1\lambda_2 A(\boldsymbol{K}') \leqslant 4. \tag{18}$$

Putting $\boldsymbol{p} = \boldsymbol{a}x_1 + \boldsymbol{b}y_1$, $\boldsymbol{q} = \boldsymbol{a}x_2 + \boldsymbol{b}y_2$, we infer that $\boldsymbol{p}, \boldsymbol{q}$ are linearly independent, satisfy $\boldsymbol{pn} = \boldsymbol{qn} = 0$ and in virtue of (15), (18)

$$h(\boldsymbol{p})h(\boldsymbol{q}) \leqslant \lambda_1\lambda_2 \begin{cases} < \sqrt{\frac{2}{3}}\, l(\boldsymbol{n}), & \text{if } n_1 + n_2 > n_3, \\ \leqslant n_3, & \text{otherwise.} \end{cases}$$ □

Proof of Theorem 1. If $\boldsymbol{n} = [\varepsilon_1, \varepsilon_2, \varepsilon_3]$, where $\varepsilon_i \in \{1, -1\}$, it suffices to take $\boldsymbol{p} = [\varepsilon_1, \varepsilon_2, 0], \boldsymbol{q} = [0, 0, \varepsilon_3]$. If $\boldsymbol{n} \neq [\varepsilon_1, \varepsilon_2, \varepsilon_3]$ for every choice of $\varepsilon_1, \varepsilon_2, \varepsilon_3$, then by Lemma 4 there exists a vector $\boldsymbol{m} \in \mathbb{Z}^3$ satisfying the conditions

$$\boldsymbol{mn} = 0, \tag{19}$$

$$0 < h(\boldsymbol{m}) < \sqrt{\tfrac{4}{3}\, h(\boldsymbol{n})}, \quad 0 < l(\boldsymbol{m}) < \sqrt{2h(\boldsymbol{n})}\,. \tag{20}$$

Now, by Lemma 6 applied with $\boldsymbol{n}$ replaced by $\boldsymbol{m}$ there exist vectors $\boldsymbol{p}, \boldsymbol{q} \in \mathbb{Z}^3$ such that

$$\boldsymbol{pm} = \boldsymbol{qm} = 0, \quad \dim(\boldsymbol{p}, \boldsymbol{q}) = 2 \tag{21}$$

and

$$h(\boldsymbol{p})h(\boldsymbol{q}) < \max\left\{\sqrt{\tfrac{2}{3}}\, l(\boldsymbol{m}), h(\boldsymbol{m})\right\}. \tag{22}$$

The equations (19) and (21) imply that $\boldsymbol{n} = u\boldsymbol{p} + v\boldsymbol{q}$; $u, v \in \mathbb{Q}$, while the inequalities (20) and (22) imply that $h(\boldsymbol{p})h(\boldsymbol{q}) < \big((4/3)h(\boldsymbol{n})\big)^{1/2}$.

It follows that the number $c_0(3)$ defined in [3] by the formula

$$c_0(k) = \sup_{\substack{\boldsymbol{n}\in\mathbb{Z}^k \\ \boldsymbol{n}\neq\boldsymbol{0}}} \inf_{\substack{\boldsymbol{p},\boldsymbol{q}\in\mathbb{Z}^k \\ \dim(\boldsymbol{p},\boldsymbol{q})=2 \\ \boldsymbol{n}=u\boldsymbol{p}+v\boldsymbol{q},\ u,v\in\mathbb{Q}}} h(\boldsymbol{p})h(\boldsymbol{q})h(\boldsymbol{n})^{-(k-2)/(k-1)}$$

satisfies $c_0(3) \leqslant \sqrt{4/3}$ and if $c_0(3) = \sqrt{4/3}$, the supremum occurring in the definition of $c_0(k)$ is not attained. By Theorem 2 of [3] there exist vectors $\boldsymbol{p}_0, \boldsymbol{q}_0 \in \mathbb{Z}^3$ linearly independent and such that $\boldsymbol{n} = u_0\boldsymbol{p}_0 + v_0\boldsymbol{q}_0$, $u_0, v_0 \in \mathbb{Z}$, and $h(\boldsymbol{p}_0)h(\boldsymbol{q}_0) < \big((4/3)h(\boldsymbol{n})\big)^{1/2}$. The proof of Theorem 1 is complete. □

The proof of Theorem 2 is again based on several lemmata. We shall set for $t = 1, 2, 3, \ldots$

$$\boldsymbol{n}_t = \big[(2t^2+2t)(6t^2+4t-1),\ (2t^2+2t)(6t^2+6t-1),\ (4t^2+4t)^2-(2t^2-1)(2t^2+2t-1)\big],$$

and for vectors $\boldsymbol{m}, \boldsymbol{p}, \ldots$ we shall denote the v-th coordinate by m_v, p_v, respectively.

Lemma 7. *If $\boldsymbol{n}_t\boldsymbol{m} = 0$, $\boldsymbol{m} \in \mathbb{Z}^3$, $0 < h(\boldsymbol{m}) \leqslant 8t^2 + 8t - 2$, then we have $\boldsymbol{m} = \pm\boldsymbol{m}_i$ for an $i \leqslant 6$, where*

$$\begin{aligned}
\boldsymbol{m}_1 &= [6t^2 + 6t - 1, -(6t^2 + 4t - 1), 0],\\
\boldsymbol{m}_2 &= [2t^2 + 2t - 1, -(4t^2 + 4t), 2t^2 + 2t],\\
\boldsymbol{m}_3 &= [4t^2 + 4t, -(2t^2 - 1), -(2t^2 + 2t)],\\
\boldsymbol{m}_4 &= [2t^2 + 2t + 1, 2t^2 + 4t + 1, -(4t^2 + 4t)],\\
\boldsymbol{m}_5 &= [2, 6t^2 + 8t + 1, -(6t^2 + 6t)]\ (t \neq 1),\\
\boldsymbol{m}_6 &= [6t^2 + 6t + 1, 4t + 2, -(6t^2 + 6t)].
\end{aligned}$$

Proof. The vectors $\boldsymbol{m}_i$ $(1 \leqslant i \leqslant 6)$ all satisfy the equation $\boldsymbol{n}_t\boldsymbol{m}_i = 0$. Since the vectors $\boldsymbol{m}_1$ and $\boldsymbol{m}_2$ are linearly independent, every vector $\boldsymbol{m} \in \mathbb{Z}^3$ satisfying $\boldsymbol{n}_t\boldsymbol{m} = 0$ is of the form $u\boldsymbol{m}_1 + v\boldsymbol{m}_2$, $u, v \in \mathbb{Q}$.

Let $u = a/c$, $v = b/c$, $a, b, c \in \mathbb{Z}$, $(a, b, c) = 1$, $c > 0$. It follows from

$$c \mid am_{1i} + bm_{2i}, \quad c \mid am_{1j} + bm_{2j}$$

that $c \mid (a, b)(m_{1i}m_{2j} - m_{2i}m_{1j})$, hence, $c \mid m_{1i}m_{2j} - m_{2i}m_{1j}$ $(1 \leqslant i < j \leqslant 3)$.

But $(m_{11}m_{23} - m_{21}m_{13}, m_{12}m_{23} - m_{22}m_{13}) = m_{23}(m_{11}, m_{12}) = m_{23}$ and $(m_{23}, m_{11}, m_{22} - m_{21}, m_{12}) = (m_{23}, m_{21}, m_{12}) = 1$, hence, $c = 1$ and we get $\boldsymbol{m} = a\boldsymbol{m}_1 + b\boldsymbol{m}_2$. Considering the third coordinate, we find $|b|(2t^2 + 2t) \leqslant 8t^2 + 8t - 2$, hence, $|b| \leqslant 3$.

Considering the first coordinate, we get

$$|a(6t^2 + 6t + 1) + b(2t^2 + 2t - 1)| \leqslant 8t^2 + 8t - 2;$$

$$|a|(6t^2 + 6t - 1) \leqslant 8t^2 + 8t - 2 + |b|(2t^2 + 2t - 1) \leqslant 14t^2 + 14t - 15,$$

hence, $|a| \leqslant 1$ or $a = \pm 2$, $b = 3$. For $a = 0$ we get

$$\boldsymbol{m} = b[2t^2 + 2t - 1, -(4t^2 + 4t), 2t^2 + 2t] = \pm\boldsymbol{m}_2.$$

For $|a| = 1$ the inequality for the second coordinate

$$|a(6t^2 + 4t - 1) + b(4t^2 + 4t)| \leqslant 8t^2 + 8t - 2$$

gives $b = 0$ or $ab < 0$. For $a = \pm 1$, $b = 0$ we get $\boldsymbol{m} = \pm\boldsymbol{m}_1$; for $a = \pm 1$, $b = \mp 1$ we get $\boldsymbol{m} = \pm\boldsymbol{m}_3$; for $a = \pm 1$, $b = \mp 2$ we get $\boldsymbol{m} = \pm\boldsymbol{m}_4$; for $a = \pm 1$, $b = \mp 3$ we get $\boldsymbol{m} = \pm\boldsymbol{m}_5$; for $a = \pm 2$, $b = \mp 3$ we get $\boldsymbol{m} = \pm\boldsymbol{m}_6$. □

Lemma 8. *If $\boldsymbol{p}, \boldsymbol{q} \in \mathbb{Z}^3$ are linearly independent and $\boldsymbol{p}\boldsymbol{m}_1 = \boldsymbol{q}\boldsymbol{m}_1 = 0$, then*

$$h(\boldsymbol{p})h(\boldsymbol{q}) > 4t^2 + 4t.$$

Proof. $\boldsymbol{pm}_1 = 0$ implies $p_1 \equiv 0 \bmod 6t^2 + 4t - 1$, $p_2 \equiv 0 \bmod 6t^2 + 6t - 1$. Hence, $p_1 = p_2 = 0$ or $|p_2| \geqslant 6t^2 + 6t - 1$. Similarly, $q_1 = q_2 = 0$ or $|q_2| \geqslant 6t^2 + 6t - 1$. Since $\boldsymbol{p}, \boldsymbol{q}$ are linearly independent, $h(\boldsymbol{p})h(\boldsymbol{q}) \geqslant 6t^2 + 6t - 1 > 4t^2 + 4t$. □

Lemma 9. *If $\boldsymbol{p}, \boldsymbol{q} \in \mathbb{Z}^3$ are linearly independent and $\boldsymbol{pm}_2 = \boldsymbol{qm}_2 = 0$, then*

$$h(\boldsymbol{p})h(\boldsymbol{q}) \geqslant 4t^2 + 4t.$$

Proof. The equation

$$\boldsymbol{pm}_2 = (2t^2 + 2t - 1)p_1 - (4t^2 + 4t)p_2 + (2t^2 + 2t)p_3 = 0$$

gives $p_1 \equiv 0 \bmod 2t^2 + 2t$, hence, $p_1 = 0$ or $|p_1| \geqslant 2t^2 + 2t$. The former possibility gives $|p_3| \geqslant 2$. Similarly, $q_1 = 0$, $|q_3| \geqslant 2$ or $|q_1| \geqslant 2t^2 + 2t$. Since $\boldsymbol{p}, \boldsymbol{q}$ are linearly independent, $p_1 = q_1 = 0$ is excluded, hence,

$$h(\boldsymbol{p})h(\boldsymbol{q}) \geqslant \min\{2(2t^2 + 2t), (2t^2 + 2t)^2\} \geqslant 4t^2 + 4t.$$ □

Lemma 10. *If $\boldsymbol{p}, \boldsymbol{q} \in \mathbb{Z}^3$ are linearly independent and $\boldsymbol{pm}_3 = \boldsymbol{qm}_3 = 0$, then*

$$h(\boldsymbol{p})h(\boldsymbol{q}) \geqslant 4t^2 + 4t.$$

Proof. The equation

$$\boldsymbol{pm}_3 = (4t^2 + 4t)p_1 - (2t^2 - 1)p_2 - (2t^2 + 2t)p_3 = 0$$

gives $p_2 \equiv 0 \bmod 2t^2 + 2t$, hence $p_2 = 0$ or $|p_2| \geqslant 2t^2 + 2t$. The further proof is similar to that of Lemma 9. □

Lemma 11. *If $\boldsymbol{p} \in \mathbb{Z}^3$, $\boldsymbol{pm}_4 = 0$, then either $\boldsymbol{p} = \boldsymbol{0}$ or $h(\boldsymbol{p}) \geqslant 2t + 1$.*

Proof. The equation

$$\boldsymbol{pm}_4 = (2t^2 + 2t + 1)p_1 + (2t^2 + 4t + 1)p_2 - (4t^2 + 4t)p_3 = 0$$

gives

$$(2t^2 + 2t)(p_1 + p_2 - 2p_3) + p_1 + (2t + 1)p_2 = 0. \tag{24}$$

If $p_1 + p_2 - 2p_3 = 0$, then $p_1 + (2t + 1)p_2 = 0$ and either $p_1 = 0$ or $|p_1| \geqslant 2t + 1$. If $p_1 + p_2 - 2p_3 \neq 0$, then since by (24) $p_1 \equiv p_2 \bmod 2$, we obtain

$$p_1 + p_2 - 2p_3 = 2s,\ s \in \mathbb{Z} \setminus \{0\}, \quad p_1 + (2t + 1)p_2 = -(4t^2 + 4t)s.$$

Hence, $p_3 + tp_2 = -(2t^2 + 2t + 1)s$ and

$$\max\{|p_2|, |p_3|\} \geqslant \frac{2t^2 + 2t + 1}{t + 1} > 2t,$$

thus $h(\boldsymbol{p}) \geqslant 2t + 1$. □

Lemma 12. *If $\boldsymbol{p}, \boldsymbol{q} \in \mathbb{Z}^3$ are linearly independent and $\boldsymbol{pm}_5 = \boldsymbol{qm}_5 = 0$, then*

$$h(\boldsymbol{p})h(\boldsymbol{q}) > 4t^2 + 4t \quad (t \neq 1).$$

Proof. The equation

$$\boldsymbol{pm}_5 = 2p_1 + (6t^2 + 8t + 1)p_2 - (6t^2 + 6t)p_3 = 0$$

gives

$$2p_1 + (2t + 1)p_2 + (6t^2 + 6t)(p_2 - p_3) = 0.$$

If $p_2 = p_3$, we get $p_1 \equiv 0 \bmod 2t + 1$, hence, $|p_1| \geqslant 2t + 1$. If $p_2 \neq p_3$, we get $(2t + 3)\max\{|p_1|, |p_2|\} \geqslant 6t^2 + 6t$, hence

$$\max\{|p_1|, |p_2|\} \geqslant \frac{6t^2 + 6t}{2t + 3} > 3t - 2$$

and $h(\boldsymbol{p}) \geqslant 3t - 1$. Similarly, $q_2 = q_3$ and $|q_1| \geqslant 2t + 1$ or $h(\boldsymbol{q}) \geqslant 3t - 1$. Since $\boldsymbol{p}, \boldsymbol{q}$ are linearly independent, $p_2 = p_3, q_2 = q_3$ is excluded and we get for $t \neq 1$

$$h(\boldsymbol{p})h(\boldsymbol{q}) \geqslant \min\big\{(2t + 1)(3t - 1), (3t - 1)^2\big\} \geqslant (2t + 1)(3t - 1). \qquad \square$$

Lemma 13. *If $\boldsymbol{p}, \boldsymbol{q} \in \mathbb{Z}^3$ are linearly independent and $\boldsymbol{pm}_6 = \boldsymbol{qm}_6 = 0$, then*

$$h(\boldsymbol{p})h(\boldsymbol{q}) \geqslant 4t^2 + 4t.$$

The equation

$$\boldsymbol{pm}_6 = (6t^2 + 6t + 1)p_1 + (4t + 2)p_2 - (6t^2 + 6t)p_3 = 0$$

gives

$$(6t^2 + 6t)(p_1 - p_3) + p_1 + (4t + 2)p_2 = 0.$$

If $p_1 - p_3 = 0$, we get $p_1 \equiv 0 \bmod 4t + 2$, hence, $|p_1| \geqslant 4t + 2$. If $|p_1 - p_3| \geqslant 2$, we get

$$(4t + 3)\max\{|p_1|, |p_2|\} \geqslant 2(6t^2 + 6t),$$

hence,

$$\max\{|p_1|, |p_2|\} \geqslant \frac{12t^2 + 12t}{4t + 3} > 3t$$

and $h(\boldsymbol{p}) \geqslant 3t + 1$. If $p_1 - p_3 = \pm 1$, we get $p_1 + (4t + 2)p_2 = \mp(6t^2 + 6t)$, hence

$$\text{either} \quad |p_1| \geqslant 4t + 2 \quad \text{or} \quad p_2 = \Big(\mp\frac{(6t^2 + 6t)}{4t + 2}\Big) \quad \text{or} \quad p_2 = \Big(\mp\frac{(6t^2 + 6t)}{4t + 2}\Big) + 1.$$

The last two formulae give the following possible values for $\mp[p_1, p_2]$:

$$\Big[3t, \frac{3t}{2}\Big], \quad \Big[t - 1, \frac{3t + 1}{2}\Big], \quad \Big[-t - 2, \frac{3t + 2}{2}\Big], \quad \Big[-3t - 3, \frac{3t + 3}{2}\Big].$$

Hence, either $h(\boldsymbol{p}) \geqslant 3t + 2\{t/2\}$ or $p_1 - p_3 = \pm 1$ and $p_2 = \big((3t + 2)/2\big)$. Similarly, either $h(\boldsymbol{q}) \geqslant 3t + 2\{t/2\}$ or $q_2 - q_3 = \pm 1$ and $q_2 = \big((3t + 2)/2\big)$. Since $\boldsymbol{p}, \boldsymbol{q}$ are linearly independent it follows that

$$h(\boldsymbol{p})h(\boldsymbol{q}) \geqslant \Big(3t + 2\Big\{\frac{t}{2}\Big\}\Big)\Big(\frac{3t + 2}{2}\Big) \geqslant 4t^2 + 4t. \qquad \square$$

Proof of Theorem 2. Since

$$\lim_{t\to\infty} \frac{4t^2+4t}{\sqrt{(4t^2+4t)^2-(2t^2-1)(2t^2+2t-1)}} = \sqrt{\frac{4}{3}},$$

for every $\varepsilon > 0$ there exist integers t such that

$$4t^2+4t > \sqrt{\left(\tfrac{4}{3}-\varepsilon\right)h(\boldsymbol{n}_t)} \tag{25}$$

and we fix such a value of t.

If $\boldsymbol{n}_t = u\boldsymbol{p} + v\boldsymbol{q}$, $u, v \in \mathbb{Q}$ and $\boldsymbol{p}, \boldsymbol{q} \in \mathbb{Z}^3$ are linearly dependent, then since $(n_{t1}, n_{t2}, n_{t3}) = 1$, we have either $\boldsymbol{p} = \boldsymbol{0}$ or $\boldsymbol{p} = s\boldsymbol{n}_t$, $s \in \mathbb{Z}\setminus\{0\}$, thus $h(\boldsymbol{p}) \geqslant h(\boldsymbol{n}_t)$, and similarly for $\boldsymbol{q}$. It follows that for $\boldsymbol{p} \neq \boldsymbol{0}$, $\boldsymbol{q} \neq \boldsymbol{0}$

$$h(\boldsymbol{p})h(\boldsymbol{q}) \geqslant h(\boldsymbol{n}_t)^2 > \sqrt{\left(\tfrac{4}{3}-\varepsilon\right)h(\boldsymbol{n}_t)}\,.$$

If $\boldsymbol{p}, \boldsymbol{q}$ are linearly independent, then $\boldsymbol{p}\times\boldsymbol{q} \neq \boldsymbol{0}$ and $(\boldsymbol{p}\times\boldsymbol{q})\boldsymbol{n}_t = 0$. On the other hand, either $h(\boldsymbol{p})h(\boldsymbol{q}) \geqslant 4t^2+4t$ or $h(\boldsymbol{p}\times\boldsymbol{q}) \leqslant 2h(\boldsymbol{p})h(\boldsymbol{q}) \leqslant 2(4t^2+4t-1) = 8t^2+8t-2$. In the latter case in virtue of Lemma 7 we have $\boldsymbol{p}\times\boldsymbol{q} = \boldsymbol{m}_i$, for an $i \leqslant 6$. Hence, $\boldsymbol{p}\boldsymbol{m}_i = \boldsymbol{q}\boldsymbol{m}_i = 0$ and from Lemmata 8–13 we obtain $h(\boldsymbol{p})h(\boldsymbol{q}) \geqslant 4t^2+4t$.

In view of (25) the theorem follows. □

Remark. There exist decompositions $\boldsymbol{n}_t = u\boldsymbol{p} + v\boldsymbol{q}$ with $h(\boldsymbol{p})h(\boldsymbol{q}) = 4t^2+4t$, namely

$$\boldsymbol{n}_t = (6t^2+4t-1)\big[2t^2+2t, 0, -(2t^2+2t-1)\big] + (2t^2+2t)(6t^2+6t-1)[0,1,2]$$

or

$$\boldsymbol{n}_t = (2t^2+2t)(6t^2+4t-1)[1,0,2] + (6t^2+6t-1)[0, 2t^2+2t, 1-2t^2].$$

References

[1] A. Châtelet, *Leçons sur la théorie des nombres*. Paris 1913.

[2] A. Schinzel, *Reducibility of lacunary polynomials* VII. Monatsh. Math. 102 (1986), 309–337; *Errata*, Acta Arith. 53 (1989), 95.

[3] —, *A decomposition of integer vectors* I. Bull. Polish Acad. Sci. Math. 35 (1987), 155–159.

Andrzej Schinzel
Selecta

Originally published in
Journal of the Australian Mathematical Society
Series A 51 (1991), 33–49

A decomposition of integer vectors IV

In memory of Kurt Mahler

Abstract. Given m linearly independent vectors $\boldsymbol{n}_1, \dots, \boldsymbol{n}_m \in \mathbb{Z}^k$ and an integer $l \in [m, k]$ one proves the existence of l linearly independent vectors $\boldsymbol{p}_1, \dots, \boldsymbol{p}_l \in \mathbb{Z}^k$ or $\boldsymbol{q}_1, \dots, \boldsymbol{q}_l \in \mathbb{Z}^k$ of small size (suitably measured) such that the $\boldsymbol{n}_i$'s are linear combinations of $\boldsymbol{p}_j$'s with rational coefficients or of $\boldsymbol{q}_j$'s with integer coefficients.

In order to generalize the results of [10] (Part III of this series) let us introduce the following notation. Given m linearly independent vectors $\boldsymbol{n}_1, \dots, \boldsymbol{n}_m \in \mathbb{Z}^k$ let $H(\boldsymbol{n}_1, \dots, \boldsymbol{n}_m)$ denote the maximum of the absolute values of all minors of order m of the matrix

$$\begin{pmatrix} \boldsymbol{n}_1 \\ \vdots \\ \boldsymbol{n}_m \end{pmatrix}$$

and $D(\boldsymbol{n}_1, \dots, \boldsymbol{n}_m)$ the greatest common divisor of these minors. Furthermore, let

$$h(\boldsymbol{n}) = H(\boldsymbol{n}) \quad \text{for } \boldsymbol{n} \neq \boldsymbol{0}, \quad h(\boldsymbol{0}) = 0.$$

Definition 1. For $k \geqslant l \geqslant m$, $k > m$, let

$$c_0(k, l, m) = \sup \inf \left(\frac{D(\boldsymbol{n}_1, \dots, \boldsymbol{n}_m)}{H(\boldsymbol{n}_1, \dots, \boldsymbol{n}_m)} \right)^{(k-l)/(k-m)} \prod_{i=1}^{l} h(\boldsymbol{p}_i),$$

$$c_1(k, l, m) = \sup \inf \left(\frac{D(\boldsymbol{n}_1, \dots, \boldsymbol{n}_m)}{H(\boldsymbol{n}_1, \dots, \boldsymbol{n}_m)} \right)^{(k-l)/(k-m)} \prod_{i=1}^{l} h(\boldsymbol{q}_i),$$

where the supremum is taken over all sets of linearly independent vectors $\boldsymbol{n}_1, \dots, \boldsymbol{n}_m \in \mathbb{Z}^k$ and the infimum is taken over all sets of linearly independent vectors $\boldsymbol{p}_1, \dots, \boldsymbol{p}_l \in \mathbb{Z}^k$ or $\boldsymbol{q}_1, \dots, \boldsymbol{q}_l \in \mathbb{Z}^k$ such that for all $i \leqslant m$,

$$\boldsymbol{n}_i = \sum_{j=1}^{l} u_{ij} \boldsymbol{p}_j, \quad u_{ij} \in \mathbb{Q}, \qquad \boldsymbol{n}_i = \sum_{j=1}^{l} u_{ij} \boldsymbol{q}_j, \quad u_{ij} \in \mathbb{Z}.$$

The Bombieri–Vaaler refinement [1] of the Siegel lemma easily leads (on the lines of the proof of (8) in [10]) to the conclusion that $c_0(k, l, m)$ is finite, first obtained by Yu. Teterin. The aim of this paper is to give bounds for $c_0(k, l, m)$ and $c_1(k, l, m)$ which

Communicated by J. H. Loxton

are independent of k. First however we shall introduce three further series of constants, this time of geometric character.

Definition 2. For a given positive integer m, let κ_m be the volume of the unit ball in $\mathbb{R}^m$,

$$g_0(m) = \sup \inf \frac{\operatorname{vol} \mathbb{P}}{\operatorname{vol} \mathbb{K}}, \quad g_1(m) = \sup \inf \frac{\operatorname{vol} \mathbb{P}}{\operatorname{vol} \mathscr{E}(\mathbb{K})} \cdot \frac{\kappa_m}{2^m},$$

where the suprema are taken over all m-dimensional convex bodies $\mathbb{K}$ situated in $\mathbb{R}^m$, symmetric with respect to the origin, the infima are taken over all parallelopipeds $\mathbb{P}$ containing $\mathbb{K}$ symmetric with respect to the origin and $\mathscr{E}(\mathbb{K})$ denotes the ellipsoid of the maximum volume contained in $\mathbb{K}$. (It is unique; see [7].) Clearly

$$\frac{2^m}{\kappa_m} \leqslant g_0(m) \leqslant \frac{2^m}{\kappa_m} g_1(m).$$

The best published result pertaining to $g_0(m)$, $g_1(m)$ seems to be the following inequality due to Dvoretzky and Rogers ([4], Theorem 5A):

$$g_1(m) \leqslant \left(\frac{m^m}{m!}\right)^{1/2}.$$

Professor A. Pełczyński who indicated to me the paper [4] has improved the above inequality by showing together with S. J. Szarek that (see [9], Proposition 2.1)

$$g_1(m)^2 \leqslant \binom{\frac{m(m+1)}{2}}{m} \left(\frac{2}{m+1}\right)^m$$

and, on the other hand, they have proved that (*ibid.*, Section 6)

$$g_1(m)^2 \geqslant \frac{2m}{m+1}.$$

For $m \leqslant 2$ the two bounds coincide and give

$$g_1(1) = 1, \quad g_1(2) = \sqrt{\tfrac{4}{3}}.$$

According to Theorem 5.1 of [9], for every $\varepsilon > 0$,

$$\log g_1(m) = \frac{m}{2} + o(m^{2/3+\varepsilon}).$$

I am indebted to Professor Pełczyński also for the paradigm (for $l = 2$) of the proof of Lemma 1 below, which he has since proved in another way (see [9], Corollary 3.1).

We shall prove

Theorem 1. *For all integers k, l, m satisfying $k \geqslant l \geqslant m$, $k > m > 0$,*

$$(1) \quad c_0(k,l,m) \leqslant \min\left\{(l-m+1)^{1/2} g_1(m) \gamma_l^{l/2}, \frac{l!}{m!} g_0(m), \binom{l}{m}^{l/2} l^{(l-m)/2} g_1(l) \gamma_l^{l/2}\right\},$$

where γ_l is the Hermite constant. For $l = m \leqslant 2$ we have here equality.

c **Theorem 2.** *For all integers k, l, m satisfying $k \geqslant l \geqslant m$, $k > m > 0$ we have*

$$\frac{c_1(k,l,m)}{c_0(k,l,m)} \leqslant f(l) = \sup_{\mathbb{A}} \inf_{\mathbb{U}} \left(\sum_{j=1}^{l} |\delta_{ij}| \right),$$

where $[\delta_{ij}] = \mathbb{U}\mathbb{A}^{-1}$, $\mathbb{A}$ and $\mathbb{U}$ run through all lower triangular non-singular integral matrices and all lower triangular integral matrices of order l, respectively. Moreover

$$f(l) \leqslant \frac{(l+\lambda+1)!}{4^{l-\lambda}(2\lambda+1)!} \quad \text{where} \quad \lambda = \left[\frac{1+\sqrt{16l+17}}{4} \right].$$

S. Chaładus and Yu. Teterin prove in the forthcoming paper [2] that the exponent $(k-l)/(k-m)$ in the definition of $c_0(k,l,m)$ is the correct one, that is, for any smaller exponent the corresponding supremum is infinite. Moreover they give an estimate for $c_0(k,l,m)$ that depends on k and is better than (1) for $k = o(l^2)$.

Let us note that for large l the minimum on the right hand side of (1) is equal to the first term for $m < c_1 l/\log l$, to the last term for $m > c_2 l$, where c_1, c_2 are suitable constants, $c_1 > 0$, $c_2 < 1$, provided in the latter case that γ_l, $\log\bigl(g_0(l)\kappa_l/2^l\bigr)$ are regularly growing functions and

$$\liminf_{l\to\infty} \frac{\log g_0(l) - \frac{l}{2}\log\gamma_l}{l} > \frac{1}{2}.$$

For $m = 1$, (1) constitutes an improvement over Theorem 1 of [8] already for $l > 50$. The problem of existence of a bound for $c_0(k,l,m)$ depending only on m remains open also for $m = 1$.

Lemma 1. *If $\mathbb{A}$ is a parallelohedron given by the inequalities*

$$|\boldsymbol{a}_i \boldsymbol{x}| \leqslant 1, \quad \boldsymbol{a}_i \in \mathbb{R}^l \quad (1 \leqslant i \leqslant k)$$

then for every parallelopiped $\mathbb{P}$ containing $\mathbb{A}$, symmetric with respect to $\mathbf{0}$ and for a suitable subset S of $\{1, 2, \ldots, k\}$ of cardinality l we have

$$\operatorname{vol}\mathbb{P} \geqslant \operatorname{vol}\mathbb{P}_0(S),$$

where $\mathbb{P}_0(S)$ is the parallelopiped

$$|\boldsymbol{a}_i \boldsymbol{x}| \leqslant 1 \quad (i \in S).$$

Proof. We shall proceed by induction on the number n of pairs of parallel $(l-1)$-dimensional faces of $\mathbb{P}$ that do not contain $(l-1)$-dimensional faces of $\mathbb{A}$ (in the sequel, briefly, faces). If $n = 0$ the assertion is true. Suppose it is true for the case of $n-1$ pairs of parallel faces and consider a parallelopiped $\mathbb{P}$ symmetric with respect to $\mathbf{0}$ with exactly n pairs of parallel faces not containing faces of $\mathbb{A}$. Let $\mathbb{P}$ be given by the inequalities

$$|\boldsymbol{b}_i \boldsymbol{x}| \leqslant 1, \quad \boldsymbol{b}_i \in \mathbb{R}^l \quad (1 \leqslant i \leqslant l)$$

and let $\boldsymbol{b}_1 \boldsymbol{x} = \pm 1$ be the pair of hyperplanes corresponding to one of the n pairs in question. Replacing $\mathbb{P}$ if necessary by a smaller parallelopiped we may assume that there is $\boldsymbol{x}_0 \in \mathbb{A}$

such that

$$\boldsymbol{b}_1\boldsymbol{x}_0 = 1. \tag{2}$$

Let $I = \{i \leqslant k : |\boldsymbol{a}_i\boldsymbol{x}_0| = 1\}$ and let

$$\boldsymbol{a}_i\boldsymbol{x}_0 = \varepsilon_i \quad (i \in I). \tag{3}$$

From the fact that the hyperplane $\boldsymbol{b}_1\boldsymbol{x} = 1$ is supporting $\mathbb{A}$ at $\boldsymbol{x}_0$ it follows that

$$\varepsilon_i\boldsymbol{a}_i\boldsymbol{t} \leqslant 0\ (i \in I) \quad \text{implies} \quad \boldsymbol{b}_1\boldsymbol{t} \leqslant 0 \text{ for } \boldsymbol{t} \in \mathbb{R}^l. \tag{4}$$

Indeed, suppose for some $\boldsymbol{t}_0 \in \mathbb{R}^l$ that $\varepsilon_i\boldsymbol{a}_i\boldsymbol{t}_0 \leqslant 0$ and $\boldsymbol{b}_1\boldsymbol{t}_0 > 0$. Then for

$$\boldsymbol{t}_1 = \frac{\boldsymbol{t}_0}{lh(\boldsymbol{t}_0)} \min\left\{\min_{i\notin I} \frac{1 - |\boldsymbol{a}_i\boldsymbol{x}_0|}{h(\boldsymbol{a}_i)}, \min_{i\in I} \frac{2}{h(\boldsymbol{a}_i)}\right\}$$

we have $\pm(\boldsymbol{x}_0 + \boldsymbol{t}_1) \in \mathbb{A}$, $\boldsymbol{b}_1(\boldsymbol{x}_0 + \boldsymbol{t}_1) > 1$, $\boldsymbol{b}_1(-\boldsymbol{x}_0 - \boldsymbol{t}_1) < -1 < 1$, and thus the hyperplane $\boldsymbol{b}_1\boldsymbol{x} = 1$ divides $\mathbb{A}$. This contradiction proves (4). Hence by a theorem of Farkas ([5], page 5. I owe this reference to Professor S. Rolewicz. There is a related earlier statement in [8], page 45) we have

$$\boldsymbol{b}_1 = \sum_{i\in I} \varepsilon_i\boldsymbol{a}_i\lambda_i,$$

where

$$\lambda_i \geqslant 0 \quad (i \in I) \tag{5}$$

and by (2) and (3)

$$\sum_{i\in I} \lambda_i = 1. \tag{6}$$

Therefore,

$$\begin{aligned}\big(\operatorname{vol}\mathbb{P}\big)^{-1} &= 2^{-l}\left|\det\left(\sum_{i\in I} \varepsilon_i\boldsymbol{a}_i\lambda_i, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_l\right)\right| \\ &= 2^{-l}\left|\sum_{i\in I} \lambda_i \det(\varepsilon_i\boldsymbol{a}_i, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_l)\right|.\end{aligned} \tag{7}$$

Regarding λ_i as variables restricted by the conditions (5) and (6), we easily see that the right hand side of (7) takes the maximum for $\lambda_i = 1$ if $i = i_0$, $\lambda_i = 0$ otherwise. Hence

$$\operatorname{vol}\mathbb{P} \geqslant \operatorname{vol}\mathbb{P}_1, \tag{8}$$

where $\mathbb{P}_1$ is the parallelopiped

$$|\boldsymbol{a}_{i_0}\boldsymbol{x}| \leqslant 1, \quad |\boldsymbol{b}_i\boldsymbol{x}| \leqslant 1 \quad (2 \leqslant i \leqslant l).$$

However $\mathbb{P}_1$ contains $\mathbb{A}$ and it has only $n - 1$ pairs of parallel faces that do not contain faces of $\mathbb{A}$. Thus by the inductive assumption there exists a set $S \subset \{1, 2, \ldots, k\}$ of cardinality l and with the property

$$\operatorname{vol}\mathbb{P}_1 \geqslant \operatorname{vol}\mathbb{P}_0(S).$$

In view of (8) this gives

$$\operatorname{vol}\mathbb{P} \geqslant \operatorname{vol}\mathbb{P}_0(S)$$

and concludes the inductive argument. □

Lemma 2. *For all linearly independent vectors* $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_l \in \mathbb{R}^k$ *the domain*

$$\mathbb{C} : h(\boldsymbol{c}_1 x_1 + \ldots + \boldsymbol{c}_l x_l) \leqslant 1$$

satisfies

$$\operatorname{vol}\mathbb{C} \geqslant \frac{2^l}{g_0(l)H(\boldsymbol{c}_1, \ldots, \boldsymbol{c}_l)}, \quad \operatorname{vol}\mathscr{E}(\mathbb{C}) \geqslant \frac{\kappa_l}{g_1(l)H(\boldsymbol{c}_1, \ldots, \boldsymbol{c}_l)}.$$

Proof. Put

$$\boldsymbol{a}_i = [c_{1i}, c_{2i}, \ldots, c_{li}] \quad (1 \leqslant i \leqslant k). \tag{9}$$

Then

$$\mathbb{C} = \{\boldsymbol{x} \in \mathbb{R}^l : |\boldsymbol{a}_i \boldsymbol{x}| \leqslant 1 \text{ for all } i \leqslant k\}$$

and clearly $\mathbb{C}$ is a convex body symmetric with respect to $\mathbf{0}$. By Definition 2

$$\operatorname{vol}\mathbb{C} \geqslant g_0(l)^{-1} \inf \operatorname{vol}\mathbb{P}, \quad \operatorname{vol}\mathscr{E}(\mathbb{C}) \geqslant g_1(l)^{-1}2^{-l}\kappa_l \inf \operatorname{vol}\mathbb{P},$$

where the infimum is taken over all parallelopipeds $\mathbb{P}$ symmetric with respect to $\mathbf{0}$ and containing $\mathbb{C}$. However by Lemma 1 the infimum can be replaced by the minimum taken over the finite set of all parallelopipeds

$$\mathbb{P}_0(S), \quad |\boldsymbol{a}_i \boldsymbol{x}| \leqslant 1 \quad (i \in S),$$

where S runs through all subsets of $\{1, \ldots, k\}$ of cardinality l. Since

$$\operatorname{vol}\mathbb{P}_0(S) = 2^l \left|\det\{\boldsymbol{a}_i : i \in S\}\right|^{-1}$$

we have by (9) that

$$\min \operatorname{vol}\mathbb{P}_0(S) = 2^l H(\boldsymbol{c}_1, \ldots, \boldsymbol{c}_l)^{-1}$$

and the lemma follows. □

Lemma 3. *If for all linearly independent vectors* $\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m \in \mathbb{Z}^k$ *such that* $D(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m) = 1$ *there exist linearly independent vectors* $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_l \in \mathbb{Z}^k$ *such that*

$$\boldsymbol{n}_i = \sum_{j=1}^{l} u_{ij} \boldsymbol{p}_j, \quad u_{ij} \in \mathbb{Q}$$

and

$$\prod_{j=1}^{l} h(\boldsymbol{p}_j) \leqslant cH(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)^{(k-l)/(k-m)}$$

then $c_0(k, l, m) \leqslant c$.

Proof. Consider m linearly independent vectors $\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m \in \mathbb{Z}^k$ and let $\mathscr{N}$ be the linear space spanned by them over $\mathbb{R}$. Further, let $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$ be a basis of the lattice $\mathscr{N} \cap \mathbb{Z}^k$ and $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_{k-m} \in \mathbb{Z}^k$ linearly independent vectors perpendicular to $\mathscr{N}$. Since $\mathscr{N} \cap \mathbb{Z}^k$ is the lattice of all solutions $\boldsymbol{x} \in \mathbb{Z}^k$ of the system $\boldsymbol{c}_i \boldsymbol{x} = 0$ $(1 \leqslant i \leqslant k-m)$, we have by the known theorem ([3], page 53) that

$$D(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m) = 1. \tag{10}$$

On the other hand clearly

$$\begin{pmatrix} \boldsymbol{n}_1 \\ \vdots \\ \boldsymbol{n}_m \end{pmatrix} = \mathbb{A} \begin{pmatrix} \boldsymbol{b}_1 \\ \vdots \\ \boldsymbol{b}_m \end{pmatrix}, \tag{11}$$

where $\mathbb{A}$ is an integral square matrix of order m. It follows from (11) that

$$D(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m) = |\det \mathbb{A}|\, D(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m),$$
$$H(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m) = |\det \mathbb{A}|\, H(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m)$$

and by (10)

$$H(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m) = \frac{H(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)}{D(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)}. \tag{12}$$

By the assumption of the lemma there exist linearly independent vectors $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_l \in \mathbb{Z}^k$ and a matrix $\mathbb{U} \in \mathscr{M}_{m,l}(\mathbb{Q})$ such that

$$\begin{pmatrix} \boldsymbol{b}_1 \\ \vdots \\ \boldsymbol{b}_m \end{pmatrix} = \mathbb{U} \begin{pmatrix} \boldsymbol{p}_1 \\ \vdots \\ \boldsymbol{p}_l \end{pmatrix}, \tag{13}$$

and

$$\prod_{j=1}^{l} h(\boldsymbol{p}_j) \leqslant c H(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m)^{(k-l)/(k-m)}. \tag{14}$$

It follows from (11) and (13) that

$$\begin{pmatrix} \boldsymbol{n}_1 \\ \vdots \\ \boldsymbol{n}_m \end{pmatrix} = \mathbb{A}\mathbb{U} \begin{pmatrix} \boldsymbol{p}_1 \\ \vdots \\ \boldsymbol{p}_l \end{pmatrix},$$

while from (12) and (14) that

$$\prod_{j=1}^{l} h(\boldsymbol{p}_j) \leqslant c \left(\frac{H(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)}{D(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)} \right)^{(k-l)/(k-m)}.$$

Thus, by Definition 1, $c_0(k, l, m) \leqslant c$. □

Lemma 4. *Let $\mathbb{K}$ be a convex domain symmetric with respect to $\mathbf{0}$ in the linear subspace $\mathscr{L} : x_1 = \ldots = x_m = 0$ of $\mathbb{R}^k$, not containing in its interior any point of the lattice*

$\mathscr{L} \cap \mathbb{Z}^k$ except $\mathbf{0}$ and let $\| \ \|_{\mathbb{K}}$ be the corresponding distance function. Let $\boldsymbol{n}_1, \dots, \boldsymbol{n}_m \in \mathbb{Z}^k$ and $\mathscr{N}$ be the linear space spanned by $\boldsymbol{n}_1, \dots, \boldsymbol{n}_m$ over $\mathbb{R}$. If $\Delta = \det(n_{ij})_{i,j \leqslant m} \neq 0$ and $D(\boldsymbol{n}_1, \dots, \boldsymbol{n}_m) = 1$ there exist vectors $\boldsymbol{n}_{m+1}, \dots, \boldsymbol{n}_k \in \mathbb{Z}^k$ such that $\boldsymbol{n}_1, \dots, \boldsymbol{n}_k$ are linearly independent and

$$\prod_{i=m+1}^{k} \left\| (\boldsymbol{n}_i + \mathscr{N}) \cap \mathscr{L} \right\|_{\mathbb{K}} \leqslant 2^{k-m} \big(\operatorname{vol} \mathbb{K}\big)^{-1} |\Delta|^{-1}.$$

Remark. Since $\Delta \neq 0$ we have $\mathscr{N} \cap \mathscr{L} = \{\mathbf{0}\}$, and hence $(\boldsymbol{n}_i + \mathscr{N}) \cap \mathscr{L}$ consists of one point and $\left\| (\boldsymbol{n}_i + \mathscr{N}) \cap \mathscr{L} \right\|_{\mathbb{K}}$ means the distance from this point to $\mathbf{0}$ measured through $\mathbb{K}$.

Proof. If $|\Delta| = 1$ the desired conclusion follows directly from Minkowski's second theorem. Indeed, by that theorem applied to the domain $\mathbb{K}$ there exist linearly independent vectors $\boldsymbol{n}_{m+1}, \dots, \boldsymbol{n}_k \in \mathscr{L} \cap \mathbb{K}$ such that

$$\prod_{i=m+1}^{k} \|\boldsymbol{n}_i\|_{\mathbb{K}} \leqslant 2^{k-m} \big(\operatorname{vol} \mathbb{K}\big)^{-1}.$$

Since $\mathscr{N} \cap \mathscr{L} = \{\mathbf{0}\}$ we have $(\boldsymbol{n}_i + \mathscr{N}) \cap \mathscr{L} = \{\boldsymbol{n}_i\}$ $(m < i \leqslant k)$ and $\boldsymbol{n}_1, \dots, \boldsymbol{n}_k$ are linearly independent. Therefore assume that $|\Delta| > 1$. Let $\Delta_i(\boldsymbol{x})$ be the determinant of the matrix obtained from $(n_{ij})_{i,j \leqslant m}$ by replacing the ith row by the first m coordinates of the vector $\boldsymbol{x}$.

Let us take a real number $r > 1$ and consider in $\mathbb{R}^k$ the domain

$$\mathbb{D}_r(\mathbb{K}) : \max_{1 \leqslant \mu \leqslant m} |\Delta_\mu(\boldsymbol{x})| + |\Delta|^r \left\| \boldsymbol{x}\Delta - \sum_{\mu=1}^{m} \boldsymbol{n}_\mu \Delta_\mu(\boldsymbol{x}) \right\|_{\mathbb{K}}^{(k-m)r} \leqslant |\Delta|^{(k-m)r}.$$

Then $\mathbb{D}_r(\mathbb{K})$ is convex and symmetric with respect to $\mathbf{0}$. In order to compute its volume we make the affine transformation

$$\frac{\Delta_\mu(\boldsymbol{x})}{\Delta^{(k-m)r}} = y_\mu \quad (\mu = 1, \dots, m), \qquad x_\mu = y_\mu \quad (\mu = m+1, \dots, k).$$

This transformation has Jacobian equal to $\Delta^{(k-m)rm-m+1}$ and it transforms $\mathbb{D}_r(\mathbb{K})$ into

$$\mathbb{D}'_r(\mathbb{K}) : \max_{1 \leqslant \mu \leqslant m} |y_\mu| + |\Delta|^r \left\| [\mathbf{0}, y_{m+1}, \dots, y_k] - \sum_{\mu=1}^{m} \boldsymbol{n}'_\mu y_\mu \Delta^{(k-m)r-1} \right\|_{\mathbb{K}}^{(k-m)r} \leqslant 1,$$

where $\boldsymbol{n}'_\mu$ is the projection of $\boldsymbol{n}_\mu$ on $\mathscr{L}$. Clearly

$$\begin{aligned}
&\operatorname{vol} \mathbb{D}_r(\mathbb{K}) = |\Delta|^{(k-m)rm-m+1} \operatorname{vol} \mathbb{D}'_r(\mathbb{K}) \\
&= |\Delta|^{(k-m)rm-m+1} \operatorname{vol} \mathbb{K} \int_{\max_{1 \leqslant \mu \leqslant m} |y_\mu| \leqslant 1} dy_1\, dy_2 \cdots dy_m \left(\frac{1 - \max |y_\mu|}{|\Delta|^r} \right)^{1/r} \\
&= 2^m |\Delta|^{((k-m)r-1)m} \operatorname{vol} \mathbb{K} \int_0^1 m t^{m-1} (1-t)^{1/r}\, dt.
\end{aligned}$$

Put $\int_0^1 mt^{m-1}(1-t)^{1/r}\,dt = I_{r,m}$.

Let $\lambda_i = \inf\{\lambda : \dim \lambda\mathbb{D}_r(\mathbb{K}) \cap \mathbb{Z}^k \geqslant i\}$ $(1 \leqslant i \leqslant k)$. By Minkowski's second theorem there exist linearly independent points $\boldsymbol{m}_1, \ldots, \boldsymbol{m}_k$ such that

$$\boldsymbol{m}_i \in \lambda_i \mathbb{D}_r(\mathbb{K}) \cap \mathbb{Z}^k \tag{15}$$

and

$$\prod_{i=1}^{k} \lambda_i \leqslant 2^k \operatorname{vol} \mathbb{D}_r(\mathbb{K})^{-1} = 2^{k-m} I_{r,m}^{-1} \big(\operatorname{vol} \mathbb{K}\big)^{-1} |\Delta|^{(1-(k-m)r)m}. \tag{16}$$

We shall show that

$$\lambda_i = |\Delta|^{1-(k-m)r} \quad (1 \leqslant i \leqslant m) \tag{17}$$

and

$$\boldsymbol{m}_i \in \mathscr{N} \quad (1 \leqslant i \leqslant m). \tag{18}$$

Indeed, for $i \leqslant m$, $\mu \leqslant m$ we have

$$\Delta_\mu(\boldsymbol{n}_i) = \Delta \quad \text{if } \mu = i, \quad 0 \text{ otherwise};$$

$$\Delta \boldsymbol{n}_i = \sum_{\mu=1}^{m} \boldsymbol{n}_\mu \Delta_\mu(\boldsymbol{n}_i),$$

and hence

$$\boldsymbol{n}_i \in |\Delta|^{1-(k-m)r} \mathbb{D}_r(\mathbb{K}) \quad (1 \leqslant i \leqslant m). \tag{19}$$

On the other hand, if $\boldsymbol{x} \in \lambda\mathbb{D}_r(\mathbb{K}) \cap \mathbb{Z}^k$ and $\boldsymbol{x} \notin \mathscr{N}$ we have $\Delta\boldsymbol{x} \neq \sum_{\mu=1}^{m} \boldsymbol{n}_\mu \Delta_\mu(\boldsymbol{x})$, and thus by the assumption about $\mathbb{K}$, $\big\|\Delta\boldsymbol{x} - \sum_{\mu=1}^{m} \boldsymbol{n}_\mu \Delta_\mu(\boldsymbol{x})\big\|_{\mathbb{K}} \geqslant 1$ and by the definition of $\mathbb{D}_r(\mathbb{K})$,

$$\lambda^{(k-m)r} |\Delta|^{(k-m)r} \geqslant |\Delta|^r; \quad \lambda \geqslant |\Delta|^{-1+1/(k-m)} > |\Delta|^{1-(k-m)r}. \tag{20}$$

If $\boldsymbol{x} \in \lambda\mathbb{D}_r(\mathbb{K}) \cap \mathbb{Z}^k$ and $\boldsymbol{x} \in \mathscr{N}$ we have $\Delta\boldsymbol{x} = \sum_{\mu=1}^{m} \boldsymbol{n}_\mu \Delta_\mu(\boldsymbol{x})$ and thus by the assumption that $D(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m) = 1$ we have $\Delta_\mu(\boldsymbol{x}) \equiv 0 \pmod{\Delta}$, and hence either $\boldsymbol{x} = \boldsymbol{0}$ or $\max_{1 \leqslant \mu \leqslant m} |\Delta_\mu(\boldsymbol{x})| \geqslant |\Delta|$, which by the definition of $\mathbb{D}_r(\mathbb{K})$ implies

$$\lambda \geqslant |\Delta|^{1-(k-m)r}. \tag{21}$$

The claims (17) and (18) follow from (19), (20) and (21).

From (16) and (17) we infer that

$$\prod_{i=m+1}^{k} \lambda_i \leqslant 2^{k-m} \big(\operatorname{vol} \mathbb{K}\big)^{-1} I_{r,m}^{-1}$$

and since by (15)

$$|\Delta|^r \left\| \Delta \boldsymbol{m}_i - \sum_{\mu=1}^{x} \boldsymbol{n}_\mu \Delta_\mu(\boldsymbol{m}_i) \right\|_{\mathbb{K}}^{(k-m)r} \leqslant |\Delta|^{(k-m)r} \lambda_i^{(k-m)r}$$

we obtain

$$\prod_{i=m+1}^{k} \left\| \boldsymbol{m}_i - \Delta^{-1} \sum_{\mu=1}^{m} \boldsymbol{n}_\mu \Delta_\mu(\boldsymbol{m}_i) \right\|_{\mathbb{K}} \leqslant 2^{k-m} \big(\operatorname{vol} \mathbb{K}\big)^{-1} |\Delta|^{-1} I_{r,m}^{-1}. \tag{22}$$

Moreover, by (18), $\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m, \boldsymbol{m}_{m+1}, \ldots, \boldsymbol{m}_k$ are linearly independent. For every $r > 1$ there corresponds a certain choice of vectors $\boldsymbol{m}_i \in \mathbb{Z}^k$, however the set of values which we can obtain on the left hand side of (22) is discrete. Therefore there exist vectors $\boldsymbol{n}_i$ $(m < i \leqslant k)$ such that $\boldsymbol{n}_i$ $(1 \leqslant i \leqslant k)$ are linearly independent and

$$\prod_{i=m+1}^{k} \left\| \boldsymbol{n}_i - \Delta^{-1} \sum_{\mu=1}^{m} \boldsymbol{n}_\mu \Delta_\mu(\boldsymbol{n}_i) \right\|_{\mathbb{K}} \leqslant 2^{k-m} \big(\operatorname{vol} \mathbb{K}\big)^{-1} |\Delta|^{-1} \lim_{r\to\infty} I_{r,m}^{-1}.$$

However

$$\left\{ \boldsymbol{n}_i - \Delta^{-1} \sum_{\mu=1}^{m} \boldsymbol{n}_\mu \Delta_\mu(\boldsymbol{n}_i) \right\} = (\boldsymbol{n}_i + \mathscr{N}) \cap \mathscr{L}$$

and

$$\lim_{r\to\infty} I_{r,m} = \int_0^1 m t^{m-1}\, dt = 1,$$

which proves the lemma. □

Lemma 5. *If $m < k$, $\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m \in \mathbb{Z}^k$, $D(\boldsymbol{n}_1, \boldsymbol{n}_2, \ldots, \boldsymbol{n}_m) = 1$ there exist vectors $\boldsymbol{n}_{m+1}, \ldots, \boldsymbol{n}_k \in \mathbb{Z}^k$ such that $\boldsymbol{n}_1, \ldots, \boldsymbol{n}_k$ are linearly independent and for each $l \in [m, k]$ the domain $\mathbb{D} : h\big(\sum_{i=1}^{l} x_i \boldsymbol{n}_i\big) \leqslant 1$, contained in $\mathbb{R}^d$, satisfies*

$$\operatorname{vol} \mathbb{D} \geqslant \frac{2^l m!}{g_0(m) l!}\, H(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)^{-(k-l)/(k-m)} \tag{23}$$

and

$$\operatorname{vol} \mathscr{E}(\mathbb{D}) \geqslant \max\left\{ \frac{\kappa_l}{g_1(m)(l-m+1)^{l/2}}, \frac{\kappa_l}{g_1(l)} \binom{l}{m}^{-1/2} l^{(m-l)/2} \right\} \times H(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)^{(k-l)/(k-m)}. \tag{24}$$

Proof. Without loss of generality we may assume that $H(\boldsymbol{n}_1, \boldsymbol{n}_2, \ldots, \boldsymbol{n}_m) = |\Delta|$, where $\Delta = \det(n_{ij})_{i,j\leqslant m}$. By Lemma 4 applied with $\mathbb{K} = \{\boldsymbol{x} \in \mathscr{L} : h(\boldsymbol{x}) \leqslant 1\}$ there exist

vectors $\boldsymbol{n}_{m+1}, \dots, \boldsymbol{n}_k \in \mathbb{Z}^k$ such that $\boldsymbol{n}_1, \dots, \boldsymbol{n}_k$ are linearly independent and

$$\prod_{i=m+1}^{k} h(\boldsymbol{n}_i') \leqslant |\Delta|^{-1}, \quad \text{where} \quad \{\boldsymbol{n}_i'\} = (\boldsymbol{n}_i + \mathscr{N}) \cap \mathscr{L} \quad (m < i \leqslant k). \tag{25}$$

Permuting the vectors $\boldsymbol{n}_i$ if necessary we may assume that the sequence $h(\boldsymbol{n}_i')$ is nondecreasing. Then (25) implies

$$\prod_{i=m+1}^{l} h(\boldsymbol{n}_i') \leqslant H(\boldsymbol{n}_1, \dots, \boldsymbol{n}_m)^{-(l-m)/(k-m)}. \tag{26}$$

In order to prove (23) let us write explicitly

$$\boldsymbol{n}_i' = \boldsymbol{n}_i - \sum_{\mu=1}^{m} a_{i\mu} \boldsymbol{n}_\mu \quad (m < i \leqslant l).$$

Then

$$\sum_{i=1}^{l} x_i \boldsymbol{n}_i = \sum_{\mu=1}^{m} \boldsymbol{n}_\mu \left(x_\mu + \sum_{i=m+1}^{l} a_{i\mu} x_i \right) + \sum_{i=m+1}^{l} x_i \boldsymbol{n}_i'$$

and

$$h\left(\sum_{i=1}^{l} x_i \boldsymbol{n}_i \right) \leqslant h\left(\sum_{\mu=1}^{m} \boldsymbol{n}_\mu \left(x_\mu + \sum_{i=m+1}^{l} a_{i\mu} x_i \right) \right) + \sum_{i=m+1}^{l} |x_i| h(\boldsymbol{n}_i'). \tag{27}$$

It follows by a change of variables that

$$\operatorname{vol} \mathbb{D} \geqslant \int_{\mathbb{D}_0} dx_{m+1} \cdots dx_l \operatorname{vol} \left\{ \boldsymbol{x} \in \mathbb{R}^m : h\left(\sum_{\mu=1}^{m} x_\mu \boldsymbol{n}_\mu \right) \leqslant 1 - \sum_{i=m+1}^{l} |x_i| h(\boldsymbol{n}_i') \right\},$$

where $\mathbb{D}_0$ is the domain $\sum_{i=m+1}^{l} |x_i| h(\boldsymbol{n}_i') \leqslant 1$. However by Lemma 2,

$$\operatorname{vol} \left\{ \boldsymbol{x} \in \mathbb{R}^m : h\left(\sum_{\mu=1}^{m} x_\mu \boldsymbol{n}_\mu \right) \leqslant c \right\} \geqslant \frac{2^m c^m}{g_0(m) H(\boldsymbol{n}_1, \dots, \boldsymbol{n}_m)},$$

and hence

$$\begin{aligned} \operatorname{vol} \mathbb{D} = \frac{2^m}{g_0(m) H(\boldsymbol{n}_1, \dots, \boldsymbol{n}_m)} \int_{\mathbb{D}_0} \left(1 - \sum_{i=m+1}^{l} |x_i| h(\boldsymbol{n}_i') \right)^m dx_{m+1} \cdots dx_l \\ = \frac{2^l m!}{g_0(m) l!\, H(\boldsymbol{n}_1, \dots, \boldsymbol{n}_m)} \prod_{i=m+1}^{l} h(\boldsymbol{n}_i')^{-1} \end{aligned}$$

and (23) follows from (26).

In order to prove the part of (24) corresponding to the first term of the maximum on the right hand side, let $\mathbb{D}_1$ be the domain $h\big(\sum_{i=1}^{m} x_i \boldsymbol{n}_i\big) \leqslant 1$. The ellipsoid $\mathscr{E}(\mathbb{D}_1)$ is given by the inequality $F_1(x_1, \dots, x_m) \leqslant 1$, where F_1 is a positive definite quadratic form.

Since $\mathscr{E}(\mathbb{D}_1) \subset \mathbb{D}_1$ we have for all $\boldsymbol{x} \in \mathbb{R}^m$,

$$\sqrt{F_1(x_1, \dots, x_m)} = \|\boldsymbol{x}\|_{\mathscr{E}(\mathbb{D}_1)} \geqslant \|\boldsymbol{x}\|_{\mathbb{D}_1} = h\left(\sum_{i=1}^{m} x_i \boldsymbol{n}_i\right). \tag{28}$$

By virtue of Lemma 2, we have

$$\operatorname{vol} \mathscr{E}(\mathbb{D}_1) \geqslant \kappa_m g_1(m)^{-1} H(\boldsymbol{n}_1, \dots, \boldsymbol{n}_m)^{-1}.$$

However

$$\operatorname{vol} \mathscr{E}(\mathbb{D}_1) = \frac{\kappa_m}{\sqrt{d(F_1)}},$$

and thus

$$\sqrt{d(F_1)} \leqslant g_1(m) H(\boldsymbol{n}_1, \dots, \boldsymbol{n}_m). \tag{29}$$

Consider now the quadratic form

$$F(x_1, \dots, x_l) = (l - m + 1) F_1\left(\dots, x_\mu + \sum_{i=m+1}^{l} a_{i\mu} x_i, \dots\right) + (l - m + 1) \sum_{i=m+1}^{l} x_i^2 h^2(\boldsymbol{n}_i').$$

For all $\boldsymbol{x} \in \mathbb{R}^l$ we have by the Cauchy inequality, by (28) and (27), that

$$\begin{aligned}\sqrt{F(x_1, \dots, x_l)} &\geqslant \sqrt{F_1\left(\dots, x_\mu + \sum_{i=m+1}^{l} a_{i\mu} x_i, \dots\right)} + \sum_{i=m+1}^{l} |x_i| h(\boldsymbol{n}_i') \\ &\geqslant h\left(\sum_{\mu=1}^{m} \boldsymbol{n}_\mu \left(x_\mu + \sum_{i=m+1}^{l} a_{i\mu} x_i\right)\right) + \sum_{i=m+1}^{l} |x_i| h(\boldsymbol{n}_i') \geqslant h\left(\sum_{i=1}^{l} x_i \boldsymbol{n}_i\right),\end{aligned}$$

and thus the ellipsoid

$$\mathbb{E}: \ F(x_1, \dots, x_l) \leqslant 1$$

is contained in $\mathbb{D}$ and by the definition of $\mathscr{E}(\mathbb{D})$,

$$\operatorname{vol} \mathscr{E}(\mathbb{D}) \geqslant \operatorname{vol} \mathbb{E} = \frac{\kappa_l}{\sqrt{d(F)}}. \tag{30}$$

Since F is obtained from the quadratic form

$$(l - m + 1)\left(F_1 + \sum_{i=m+1}^{l} x_i^2 h^2(\boldsymbol{n}_i')\right)$$

by a unimodular substitution, we have

$$\sqrt{d(F)} = (l-m+1)^{l/2}\sqrt{d(F_1)} \prod_{i=m+1}^{l} h(\boldsymbol{n}_i')$$

and by (26), (29) and (30),

$$\operatorname{vol} \mathscr{E}(\mathbb{D}) \geqslant \kappa_l (l-m+1)^{-l/2} H(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)^{(k-l)/(k-m)}.$$

In order to prove the remaining part of (24) note that

$$H(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_l) = H(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m, \boldsymbol{n}_{m+1}', \ldots, \boldsymbol{n}_l').$$

Let M be a minor of order l of the matrix

$$\begin{pmatrix} \boldsymbol{n}_1 \\ \vdots \\ \boldsymbol{n}_m \\ \boldsymbol{n}_{m+1}' \\ \vdots \\ \boldsymbol{n}_l' \end{pmatrix}$$

and S the set of indices of the columns of M. Developing M according to the first m rows we obtain from the Laplace theorem

$$|M| \leqslant H(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m) \sum |M_{j_1,\ldots,j_{l-m}}|, \tag{31}$$

where $M_{j_1,\ldots,j_{l-m}}$ is the minor of

$$\begin{pmatrix} \boldsymbol{n}_{m+1}' \\ \vdots \\ \boldsymbol{n}_l' \end{pmatrix}$$

consisting of the columns $j_1, \ldots, j_{l-m}$, while $\{j_1, \ldots, j_{l-m}\}$ runs through all subsets of S of cardinality $l-m$.

By the generalized Hadamard inequality ([1], formula (2.6))

$$\sum M_{j_1,\ldots,j_{l-m}}^2 \leqslant \prod_{i=m+1}^{l} \sum_{j\in S} n_{ij}'^2 \leqslant l^{l-m} \prod_{i=m+1}^{l} h(\boldsymbol{n}_i')^2,$$

and hence, by the Cauchy inequality,

$$\sum |M_{j_1,\ldots,j_{l-m}}| \leqslant \binom{l}{m}^{1/2} l^{(l-m)/2} \prod_{i=m+1}^{l} h(\boldsymbol{n}_i'). \tag{32}$$

The inequalities (26), (31) and (32) give

$$|M| \leqslant \binom{l}{m}^{1/2} l^{(l-m)/2} H(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)^{(k-l)/(k-m)},$$

and hence by the arbitrary choice of M

$$H(\boldsymbol{n}_1, \dots, \boldsymbol{n}_l) \leqslant \binom{l}{m}^{1/2} l^{(l-m)/2} H(\boldsymbol{n}_1, \dots, \boldsymbol{n}_m)^{(k-l)/(k-m)}.$$

Now Lemma 2 applied with $\mathbb{C} = \mathbb{D}$ implies

$$\operatorname{vol} \mathscr{E}(\mathbb{D}) \geqslant \frac{\kappa_l}{g_1(l)} \binom{l}{m}^{-1/2} l^{(m-l)/2} H(\boldsymbol{n}_1, \dots, \boldsymbol{n}_m)^{-(k-l)/(k-m)}. \qquad \square$$

Proof of Theorem 1. Let $\boldsymbol{n}_1, \dots, \boldsymbol{n}_m \in \mathbb{Z}^k$ be linearly independent and $D(\boldsymbol{n}_1, \dots, \boldsymbol{n}_m) = 1$. Let $\boldsymbol{n}_{m+1}, \dots, \boldsymbol{n}_l$ be vectors the existence of which is asserted in Lemma 5 and consider the domain $\mathbb{D}: h\big(\sum_{j=1}^{l} x_j \boldsymbol{n}_j\big) \leqslant 1$. Let

$$\mu_i = \min\{\mu : \dim \mu\mathbb{D} \cap \mathbb{Z}^l \geqslant i\} \quad (1 \leqslant i \leqslant l).$$

By Minkowski's second theorem there exist linearly independent vectors $\boldsymbol{y}_i = [y_{i1}, \dots, y_{il}]$ $(1 \leqslant i \leqslant l)$ such that

$$\boldsymbol{y}_i \in \mu_i \mathbb{D} \cap \mathbb{Z}^l \tag{33}$$

and

$$\prod_{i=1}^{l} \mu_i \leqslant 2^l \big(\operatorname{vol} \mathbb{D}\big)^{-1}. \tag{34}$$

By another theorem of Minkowski (see [8], §51 or [6], §18, Theorem 3),

$$\prod_{i=1}^{l} \mu_i \leqslant \Delta\big(\mathscr{E}(\mathbb{D})\big)^{-1}, \tag{35}$$

where $\Delta\big(\mathscr{E}(\mathbb{D})\big)$ is the critical determinant of $\mathscr{E}(\mathbb{D})$ and by the definition of the Hermite constant

$$\Delta\big(\mathscr{E}(\mathbb{D})\big)^{-1} = \gamma_l^{l/2} \frac{\kappa_l}{\operatorname{vol} \mathscr{E}(\mathbb{D})} \tag{36}$$

(see [6], formula (37.6)). Let us put

$$\boldsymbol{p}_i = \sum_{j=1}^{l} y_{ij} \boldsymbol{n}_j \quad (1 \leqslant i \leqslant l). \tag{37}$$

It follows from the definition of $\mathbb{D}$ and from (34)–(37) that $h(\boldsymbol{p}_i) = \mu_i$, hence by (34)–(37)

$$\prod_{i=1}^{l} h(\boldsymbol{p}_i) \leqslant \min\big\{2^l \big(\operatorname{vol} \mathbb{D}\big)^{-1}, \gamma_l^{l/2} \kappa_l \big(\operatorname{vol} \mathscr{E}(\mathbb{D})\big)^{-1}\big\}$$

and by Lemma 5

$$\prod_{i=1}^{l} h(\boldsymbol{p}_i) \leqslant \min\Big\{ \frac{l!}{m!}\, g_0(m),\, (l-m+1)^{l/2} g_1(m) \gamma_l^{l/2},\, \binom{l}{m}^{1/2} l^{(l-m)/2} g_1(l) \gamma_l^{l/2} \Big\} H(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)^{(k-l)/(k-m)}.$$

Moreover, since $\boldsymbol{y}_1, \ldots, \boldsymbol{y}_l$ are linearly independent the system (37) can be solved with respect to $\boldsymbol{n}_1, \ldots, \boldsymbol{n}_l$ and we obtain

$$\boldsymbol{n}_i = \sum_{j=1}^{l} u_{ij} \boldsymbol{p}_j, \quad u_{ij} \in \mathbb{Q} \quad (1 \leqslant i \leqslant l).$$

Since $\boldsymbol{n}_i$ $(1 \leqslant i \leqslant l)$ are linearly independent so are $\boldsymbol{p}_j$ $(1 \leqslant j \leqslant l)$ and we obtain from (37) and Lemma 3 that

$$c_0(k,l,m) \leqslant \min\Big\{ (l-m+1)^{l/2} g_1(m) \gamma_l^{l/2},\, \frac{l!}{m!}\, g_0(m),\, \binom{l}{m}^{1/2} l^{(l-m)/2} g_1(l) \gamma_l^{l/2} \Big\}, \tag{38}$$

which proves the first part of the theorem.

In order to prove the second part let us observe that if $l = m = 1$ the right hand side of (38) equals 1, while it immediately follows from the definition of $c_0(k,l,m)$ that $c_0(k,1,1) \geqslant 1$. If $l = m = 2$ the right hand side of (38) equals $\frac{4}{3}$, since

$$g_1(2) = \sqrt{\frac{4}{3}}, \quad \gamma_2 = \sqrt{\frac{4}{3}}, \quad g_0(2) \geqslant \frac{4}{3}.$$

On the other hand, consider the following vectors in $\mathbb{Z}^k$ $(k \geqslant 3)$

$$\boldsymbol{n}_1 = [2t, 4t+1, 2t, 0, \ldots, 0], \quad \boldsymbol{n}_2 = [4t-1, 2t, -2t, 0, \ldots, 0] \quad (t \in \mathbb{N}).$$

We have here

$$H(\boldsymbol{n}_1, \boldsymbol{n}_2) = 12t^2 + 2t, \quad D(\boldsymbol{n}_1, \boldsymbol{n}_2) = 1.$$

Hence, if

$$\boldsymbol{n}_i = \sum_{j=1}^{2} u_{ij} \boldsymbol{p}_j, \quad u_{ij} \in \mathbb{Q},\ \boldsymbol{p}_j \in \mathbb{Z}^k \quad (1 \leqslant i, j \leqslant 2)$$

we have

$$\boldsymbol{p}_j = \boldsymbol{n}_1 x_j + \boldsymbol{n}_2 y_j, \quad [x_j, y_j] \in \mathbb{Z}^2 \setminus \{\boldsymbol{0}\} \quad (1 \leqslant j \leqslant 2).$$

If $x_j = y_j$ we have $|p_{j2}| > 6t$, otherwise $|p_{j3}| \geqslant 2t$, and thus $h(\boldsymbol{p}_j) \geqslant 2t$ $(1 \leqslant j \leqslant 2)$. If for an $\varepsilon > 0$ we have

$$h(\boldsymbol{p}_1) h(\boldsymbol{p}_2) \leqslant \big(\tfrac{4}{3} - \varepsilon\big) H(\boldsymbol{n}_1, \boldsymbol{n}_2) = \big(\tfrac{4}{3} - \varepsilon\big)(12t^2 + 2t)$$

then for $t > t_0(\varepsilon)$

$$h(\boldsymbol{p}_1)h(\boldsymbol{p}_2) < (16 - 10\varepsilon)t^2 \tag{39}$$

and since $h(\boldsymbol{p}_j) \geqslant 2t$ we obtain $h(\boldsymbol{p}_j) < (8 - 5\varepsilon)t^2$ $(1 \leqslant j \leqslant 2)$. Hence for $t > t_1(\varepsilon)$, by consideration of the first three coordinates of $\boldsymbol{p}_j$

$$|2x_j + 4y_j| \leqslant 7, \quad |4x_j + 2y_i| \leqslant 7, \quad |2x_j - 2y_j| \leqslant 7;$$

$|x_j| \leqslant 1$, $|y_j| \leqslant 1$ and since $[x_j, y_j] \neq [0, 0]$, $h(\boldsymbol{p}_j) \geqslant 4t - 1$ $(1 \leqslant j \leqslant 2)$. It follows that

$$h(\boldsymbol{p}_1)h(\boldsymbol{p}_2) \geqslant 16t^2 - 8t + 1,$$

which for $t > \max\{t_0(\varepsilon), t_1(\varepsilon), \varepsilon^{-1}\}$ contradicts (39). This shows that $c_0(k, 2, 2) = \frac{4}{3}$ and completes the proof of the theorem. □

Proof of Theorem 2. The proof does not differ essentially from the proof of Theorem 2 in [10]. In formula (14) and in the fourth displayed formula on page 701 there, one has to replace $c_0(k, l)$ by $c_0(k, l, m)$ and $h(\boldsymbol{n})^{(k-l)/(k-m)}$ by $\Big(\dfrac{H(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)}{D(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)}\Big)^{(k-l)/(k-m)}$. □

Note added in proof. Yu. Teterin has remarked that Lemma 4 holds under a weaker assumption, namely that $\operatorname{vol} \mathbb{K} < \infty$ instead of $\mathbb{K}$ not containing in its interior any point of the lattice $\mathscr{L} \cap \mathbb{Z}^k$ except $\mathbf{0}$. To see this, it suffices to apply the original formulation to the body of $\lambda\mathbb{K}$ for suitable λ.

References

[1] E. Bombieri, J. D. Vaaler, *On Siegel's Lemma*. Invent. Math. 73 (1983), 11–32; *Addendum*, ibid. 75 (1984), 377.

[2] S. Chaładus, Yu. Teterin, *Note on a decomposition of integer vectors* II. Acta Arith. 57 (1991), 159–164.

[3] A. Châtelet, *Leçons sur la théorie des nombres*. Paris 1913.

[4] A. Dvoretzky, C. A. Rogers, *Absolute and unconditional convergence in normed linear spaces*. Proc. Nat. Acad. Sci. U.S.A. 36 (1950), 192–197.

[5] J. Farkas, *Über die Theorie der einfachen Ungleichungen*. J. Reine Angew. Math. 124 (1902), 1–27.

[6] P. M. Gruber, C. G. Lekkerkerker, *Geometry of Numbers*. North–Holland, Amsterdam 1987.

[7] F. John, *Extremum problems with inequalities as subsidiary conditions*. In: Studies and Essays Presented to R. Courant on his 60th Birthday, January 8, 1948, Interscience, New York 1948, 187–204.

[8] H. Minkowski, *Geometrie der Zahlen*. Leipzig 1896; reprint Chelsea, New York 1953.

[9] A. Pełczyński, S. J. Szarek, *On parallelepipeds of minimal volume containing a convex symmetric body in* $\mathbb{R}^n$. Math. Proc. Cambridge Philos. Soc. 109 (1991), 125–148.

[10] A. Schinzel, *A decomposition of integer vectors* III. Bull. Polish Acad. Sci. Math. 35 (1987), 693–703.

Andrzej Schinzel
Selecta

Originally published in
Monatshefte für Mathematik
137 (2002), 239–251

A property of polynomials with an application to Siegel's lemma

Dedicated to Professor Edmund Hlawka
at the occasion of his 85th birthday

Abstract. It is proved that natural necessary conditions imply the existence of infinitely many integer c points at which given multivariate polynomials with integer coefficients take relatively prime values. As a consequence the best constant in the simplest case of Siegel's lemma is expressed in terms of critical determinants of suitable star bodies.

The first aim of this paper is to prove the following:

Theorem 1. *Let* $F, F_{\mu\nu} \in \mathbb{Z}[T, T_1, \dots, T_l]$ $(1 \leqslant \mu \leqslant m,\ 1 \leqslant \nu \leqslant n)$, $F \neq 0$ *and for each* $\mu \leqslant m$, $F_{\mu\nu}$ $(1 \leqslant \nu \leqslant n)$ *be relatively prime. If the product*

$$\Pi = \prod_{\mu=1}^{m} \big(F_{\mu 1}(t, t_1, \dots, t_l), \dots, F_{\mu n}(t, t_1, \dots, t_l)\big)$$

has no fixed prime divisor for $[t, t_1, \dots, t_l]$ *running over* $\mathbb{Z}^{l+1}$, *then there exist integers* $t_1^*, \dots, t_l^*$ *and an arithmetic progression* $\mathscr{P}$ *such that for* $t \in \mathscr{P}$

$$F(t, t_1^*, \dots, t_l^*) \neq 0$$

and for each $\mu \leqslant m$ *the numbers* $F_{\mu\nu}(t, t_1^*, \dots, t_l^*)$ $(1 \leqslant \nu \leqslant n)$ *are relatively prime.*

This implies at once

Corollary 1. *Let* $F_{\mu\nu} \in \mathbb{Z}[T, T_1, \dots, T_l]$ $(1 \leqslant \mu \leqslant m,\ 1 \leqslant \nu \leqslant n)$ *and for each* $\mu \leqslant m$, $F_{\mu\nu}$ $(1 \leqslant \nu \leqslant n)$ *be relatively prime. If the numbers* $F_{\mu\nu}(t, t_1, \dots, t_l)$ $(1 \leqslant \nu \leqslant n)$ *are relatively prime simultaneously* $(1 \leqslant \mu \leqslant m)$ *for at least one integer point* $[t, t_1, \dots, t_l]$, *then they are relatively prime simultaneously for infinitely many integer points.*

The following consequence of Theorem 1 is less obvious:

Theorem 2. *Let* $f(\boldsymbol{x})$ *and* $g(\boldsymbol{x})$ *be the distance functions of two bounded star bodies in* $\mathbb{R}^{l+1}$, *both functions symmetric with respect to the coordinates of* $\boldsymbol{x}$ *and even with respect to each of them. Let for* $\boldsymbol{\alpha} \in \mathbb{R}^l$

$$S_{\boldsymbol{\alpha}} = \{\boldsymbol{x} \in \mathbb{R}^l : f\big(\boldsymbol{x}, \boldsymbol{\alpha}\boldsymbol{x}\big) < 1\},$$

where $\boldsymbol{\alpha x}$ is the inner product. Then

$$C(f,g) := \limsup_{\substack{\boldsymbol{a}\in(\mathbb{Z}\setminus\{0\})^{l+1}\\ h(\boldsymbol{a})\to\infty}} \inf_{\substack{\boldsymbol{x}\in\mathbb{Z}^{l+1}\setminus\{\boldsymbol{0}\}\\ \boldsymbol{ax}=0}} \frac{f(\boldsymbol{x})^l}{g(\boldsymbol{a})}$$

$$= \sup_{\boldsymbol{a}\in(\mathbb{Z}\setminus\{0\})^{l+1}} \inf_{\substack{\boldsymbol{x}\in\mathbb{Z}^{l+1}\setminus\{\boldsymbol{0}\}\\ \boldsymbol{ax}=0}} \frac{f(\boldsymbol{x})^l}{g(\boldsymbol{a})} = \sup_{\boldsymbol{\alpha}\in\mathbb{A}_l} \frac{\Delta(S_{\boldsymbol{\alpha}})^{-1}}{g(\boldsymbol{\alpha},1)},$$

where $\mathbb{A}_l = \{[\alpha_1,\dots,\alpha_l]\in\mathbb{Q}^l : 0<\alpha_1\leqslant\alpha_2\leqslant\dots\leqslant\alpha_l\leqslant 1\}$ and $\Delta(\cdot)$ is the critical determinant, $h(\boldsymbol{a})$ is defined below.

This in turn implies several corollaries, some of which are implicit in the literature and some are new. In order to formulate them we use the following notation.

For $\boldsymbol{x}=[x_1,\dots,x_n]\in\mathbb{R}^n$ and $0<p<\infty$,

$$h_{np}(\boldsymbol{x}) = h_p(\boldsymbol{x}) = \left(\sum_{k=1}^n |x_k|^p\right)^{1/p},$$

$$h_{n\infty}(\boldsymbol{x}) = h(\boldsymbol{x}) = \max_{1\leqslant k\leqslant n} |x_k|,$$

$$c(l,p) = \sup_{\boldsymbol{a}\in\mathbb{Z}^{l+1}\setminus\{\boldsymbol{0}\}} \inf_{\substack{\boldsymbol{x}\in\mathbb{Z}^{l+1}\setminus\{\boldsymbol{0}\}\\ \boldsymbol{ax}=0}} \frac{h_p(\boldsymbol{x})^l}{h_p(\boldsymbol{a})}.$$

Corollary 2. *$c(l,2)=\gamma_l^{l/2}$, where γ_l is the Hermite constant.*

The inequality $c(l,2)\leqslant\gamma_l^{l/2}$ is contained in Theorem 4D of [7]. The reverse inequality has been proved even in greater generality (see below), but not published, by Vaaler. The referee pointed out that it is a direct consequence of the results of [9] and [11] and Prof. Thunder has kindly supplied a proof.

Corollary 3. *For $l\geqslant 2$,*

$$c(l,\infty) = \sup_{\boldsymbol{\alpha}\in\mathbb{A}_{l-2}} \Delta(H_{\boldsymbol{\alpha}})^{-1} \geqslant 1,$$

where $H_{\boldsymbol{\alpha}}$ is a generalized hexagon in $\mathbb{R}^l$ given by the inequalities

$$|x_k|\leqslant 1\ (1\leqslant k\leqslant l), \quad \left|\sum_{i=1}^{l-2}\alpha_i x_i + x_{l-1} + x_l\right| \leqslant 1.$$

This corollary is new.

Corollary 4. *$c(2,\infty)=4/3$.*

This corollary is implicit in [5], namely the inequality $c(2,\infty)\leqslant 4/3$ is contained in Lemma 4 of [5], while the inequality $c(2,\infty)\geqslant 4/3$ is a consequence of Lemma 7 of [5].

Corollary 5. $c(3, \infty) = 27/19$.

The inequality $c(3, \infty) \geqslant 27/19$ has been proved by Chaładus [4], while the inequality $c(3, \infty) \leqslant 27/19$ has been recently proved by Aliev [1]. The proof of Theorem 2 is a generalization of arguments of Chaładus and Aliev.

Corollary 6. *For $l \geqslant 4$,*

$$1 \leqslant c(l, \infty) \leqslant \sqrt{l+1}.$$

The inequality $c(l, \infty) \leqslant \sqrt{l+1}$ is implicit in Theorem 1 of [2], the inequality $c(l, \infty) \geqslant 1$ seems to be new.

In order to formulate Theorem 3 we need more notation. Let for a matrix $A \in \mathbb{Z}^{m\times n}$ of rank m, $D(A)$ be the greatest common divisor of all minors of A of order m,

$$H(A) = \frac{\sqrt{\det AA^T}}{D(A)}.$$

Combining Corollary 2 with a result of Thunder [8] we shall show

Theorem 3. *For all positive integers m and n, where $m < n$, we have*

$$c_0(m,n) := \limsup_{\substack{A\in\mathbb{Z}^{m\times n}\\ \operatorname{rank} A=m\\ H(A)\to\infty}} \inf_{\substack{\boldsymbol{x}\in\mathbb{Z}^n\setminus\{\mathbf{0}\}\\ A\boldsymbol{x}=\mathbf{0}}} \frac{h_2(\boldsymbol{x})^{n-m}}{H(A)}$$

$$= \sup_{\substack{A\in\mathbb{Z}^{m\times n}\\ \operatorname{rank} A=m}} \inf_{\substack{\boldsymbol{x}\in\mathbb{Z}^n\setminus\{\mathbf{0}\}\\ A\boldsymbol{x}=\mathbf{0}}} \frac{h_2(\boldsymbol{x})^{n-m}}{H(A)} = \gamma_{n-m}^{(n-m)/2}.$$

A more general form of Theorem 3, concerning algebraic number fields has been proved, but not published, by Vaaler, via geometry of numbers over adeles. The referee pointed out it is a direct consequence of the results of [9] and [11].

Proof of Theorem 1. We shall proceed by induction on l. For $l = 0$, since $F_{\mu\nu}$ are relatively prime ($1 \leqslant \nu \leqslant n$) there exist polynomials $A_{\mu\nu} \in \mathbb{Z}[t]$ such that

$$\sum_{\nu=1}^{n} A_{\mu\nu} F_{\mu\nu} = R_\mu \in \mathbb{Z} \setminus \{0\}. \tag{1}$$

By the assumption about Π for each prime p dividing $\prod_{\mu=1}^{m} R_\mu$ there exist indices $\nu_{p1}, \ldots, \nu_{pm}$ and $\tau_p \in \mathbb{Z}$ such that for all $\mu \leqslant m$

$$F_{\mu\nu_{p\mu}}(\tau_p) \not\equiv 0 \bmod p. \tag{2}$$

Now taking $t \equiv \tau_p \bmod p$ for all primes p dividing $\prod_{\mu=1}^{m} R_\mu$ we obtain from (1) and (2) for all $\mu \leqslant m$

$$\operatorname*{g.c.d.}_{1\leqslant\nu\leqslant n} F_{\mu\nu}(t) = 1$$

and, if t is large enough, also $F(t) \neq 0$.

Now we assume that the theorem is true for polynomials in l variables and proceed to prove that it is true for polynomials in $l+1$ variables. There is no loss of generality in assuming that they are all different from 0. Let $F = F_{00}$,

$$F_{\mu\nu} = \sum_{\rho=0}^{r_{\mu\nu}} T^{r_{\mu\nu}-\rho} G_{\mu\nu\rho}(T_1, \dots, T_l), \text{ where } G_{\mu\nu 0} \neq 0 \tag{3}$$

and for each μ the polynomials $G_{\mu\nu\rho}$ $(1 \leqslant \nu \leqslant n,\ 0 \leqslant \rho \leqslant r_{\mu\nu})$ are relatively prime.

Let P be the product of all primes not exceeding $\sum_{\mu=1}^{m} \max_{1\leqslant\nu\leqslant n} r_{\mu\nu}$. For each prime p dividing P there exist indices $\nu_{p1}, \dots, \nu_{pm}$ and integers $\tau_p, \tau_{p1}, \dots, \tau_{pl}$ such that

$$F_{\mu\nu_{p\mu}}(\tau_p, \tau_{p1}, \dots, \tau_{pl}) \not\equiv 0 \bmod p \quad (1 \leqslant \mu \leqslant m). \tag{4}$$

By the Chinese remainder theorem there exist integers $u_1^*, \dots, u_l^*$ such that

$$u_j^* \equiv \tau_{pj} \bmod p \quad \text{for all } p \mid P \quad (1 \leqslant j \leqslant l). \tag{5}$$

Since $F_{\mu\nu}$ $(1 \leqslant \nu \leqslant n)$ are relatively prime there exist $A_{\mu\nu} \in \mathbb{Z}[T, T_1, \dots, T_l]$ such that

$$\sum_{\nu=1}^{n} A_{\mu\nu} F_{\mu\nu} = R_\mu \in \mathbb{Z}[T_1, \dots, T_l] \setminus \{0\} \quad (1 \leqslant \mu \leqslant m). \tag{6}$$

We have

$$G_{000}(PV_1 + u_1^*, \dots, PV_l + u_l^*) \prod_{\mu=1}^{m} R_\mu(PV_1 + u_1^*, \dots, PV_l + u_l^*) \neq 0$$

and for each μ the polynomials $G_{\mu\nu\rho}(PV_1+u_1^*, \dots, PV_l+u_l^*)$ $(1 \leqslant \nu \leqslant n, 0 \leqslant \rho \leqslant r_{\mu\nu})$ are relatively prime. Moreover

$$\prod_{\mu=1}^{m} \text{g.c.d.}_{\nu\leqslant n,\ \rho\leqslant r_{\mu\nu}} G_{\mu\nu\rho}(Pv_1 + u_1^*, \dots, Pv_l + u_l^*)$$

has no fixed prime divisor p when $[v_1, \dots, v_l]$ runs over $\mathbb{Z}^l$. Indeed, suppose that such p exists. In view of (3)–(5) we have $p \nmid P$. Hence for every vector $[t_1, \dots, t_l] \in \mathbb{Z}^l$ there exists a vector $[v_1, \dots, v_l] \in \mathbb{Z}^l$ such that $t_j \equiv Pv_j + u_j^* \bmod p$ $(1 \leqslant j \leqslant l)$ and we obtain

$$\prod_{\mu=1}^{m} \text{g.c.d.}_{\nu\leqslant n,\ \rho\leqslant r_{\mu\nu}} G_{\mu\nu\rho}(t_1, \dots, t_l) \equiv 0 \bmod p,$$

which by (3) gives

$$\prod_{\mu=1}^{m} \text{g.c.d.}_{\nu\leqslant n} F_{\mu\nu}(t, t_1, \dots, t_l) \equiv 0 \bmod p,$$

contrary to the assumption about Π.

Therefore, we may apply the inductive assumption to polynomials

$$G_{000}(PV_1 + u_1^*, \dots, PV_l + u_l^*) \prod_{\mu=1}^{m} R_\mu(PV_1 + u_1^*, \dots, PV_l + u_l^*)$$

and

$$G_{\mu\nu\rho}(PV_1 + u_1^*, \dots, PV_l + u_l^*) \quad (1 \leqslant \mu \leqslant m,\ 1 \leqslant \nu \leqslant n,\ 0 \leqslant \rho \leqslant r_{\mu\nu}).$$

We obtain existence of integers $v_1^*, \dots, v_l^*$ such that

$$G_{000}(Pv_1^* + u_1^*, \dots, Pv_l^* + u_l^*) \prod_{\mu=1}^{m} R_\mu(Pv_1^* + u_1^*, \dots, Pv_l^* + u_l^*) \neq 0 \tag{7}$$

and for each $\mu \leqslant m$

$$\underset{\nu \leqslant n,\ \rho \leqslant r_{\mu\nu}}{\text{g.c.d.}} \ G_{\mu\nu\rho}(Pv_1^* + u_1^*, \dots, Pv_l^* + u_l^*) = 1. \tag{8}$$

Let us put

$$t_j^* = Pv_j^* + u_j^* \quad (1 \leqslant j \leqslant l) \tag{9}$$

and consider polynomials in one variable $F(T, t_1^*, \dots, t_l^*)$ and $F_{\mu\nu}(T, t_1^*, \dots, t_l^*)$. We have $F(T, t_1^*, \dots, t_l^*) \neq 0$, since by (7) and (9) $G_{000}(t_1^*, \dots, t_l^*) \neq 0$ and for each $\mu \leqslant m$ the polynomials $F_{\mu\nu}(T, t_1^*, \dots, t_l^*)$ $(1 \leqslant \nu \leqslant n)$ are relatively prime in view of (6), since by (7) and (9) $R_\mu(t_1^*, \dots, t_l^*) \neq 0$. Suppose that a prime p is a fixed divisor of

$$\prod_{\mu=1}^{m} \underset{\nu \leqslant n}{\text{g.c.d.}} \ F_{\mu\nu}(t, t_1^*, \dots, t_l^*)$$

when t runs over $\mathbb{Z}$. By (4), (5) and (9) we have for each $\mu \leqslant m$

$$F_{\mu\nu_{p\mu}}(\tau, t_1^*, \dots, t_l^*) \not\equiv 0 \bmod p, \quad \text{if } p \mid P,$$

hence $p \nmid P$, $p > \sum_{\mu=1}^{m} \max_{1 \leqslant \nu \leqslant n} r_{\mu\nu}$.

In view of (8) for each $\mu \leqslant m$ there exist indices $\nu_\mu \leqslant n$ and $\rho_\mu \leqslant r_{\mu\nu}$ such that

$$G_{\mu\nu_\mu\rho_\mu}(t_1^*, \dots, t_l^*) \not\equiv 0 \bmod p.$$

By Lagrange's theorem and (3) the congruence

$$\prod_{\mu=1}^{m} F_{\mu\nu_\mu}(t, t_1^*, \dots, t_l^*) \equiv 0 \bmod p$$

has at most $\sum_{\mu=1}^{m} r_{\mu\nu_\mu} < p$ solutions, hence it is not satisfied identically.

The obtained contradiction shows that

$$\prod_{\mu=1}^{m} \underset{1 \leqslant \nu \leqslant n}{\text{g.c.d.}} \ F_{\mu\nu}(t, t_1^*, \dots, t_l^*)$$

has no fixed prime divisor when t runs over $\mathbb{Z}$ and, by the already proved case $l = 0$ of the theorem, there exists an arithmetic progression $\mathscr{P}$ such that for $t \in \mathscr{P}$ we have $F(t, t_1^*, \ldots, t_l^*) \neq 0$ and for each $\mu \leqslant m$ the numbers $F_{\mu\nu}(t, t_1^*, \ldots, t_l^*)$ $(1 \leqslant \nu \leqslant n)$ are relatively prime. □

For the proof of Theorem 2 we need

Lemma. *Let Λ be a sublattice of $\mathbb{Z}^n$ with a basis $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$, $A = \begin{pmatrix} \boldsymbol{a}_1 \\ \boldsymbol{a}_2 \\ \vdots \\ \boldsymbol{a}_m \end{pmatrix}$ and let $\Lambda^{\perp}$, $\Lambda^{\perp\perp}$ be the sublattice of $\mathbb{Z}^n$ consisting of all vectors orthogonal to Λ, or $\Lambda^{\perp}$, respectively. We have*

$$\Lambda = \Lambda^{\perp\perp}$$

if and only if $D(A) = 1$.

Proof. See [6], p. 336 and [3], p. 15. □

Proof of Theorem 2. We shall prove first that

$$\sup_{\boldsymbol{a} \in (\mathbb{Z}\setminus\{0\})^{l+1}} \inf_{\substack{\boldsymbol{x} \in \mathbb{Z}^{l+1} \setminus \{\boldsymbol{0}\} \\ \boldsymbol{a}\boldsymbol{x} = 0}} \frac{f(\boldsymbol{x})^l}{g(\boldsymbol{a})} \leqslant \sup_{\boldsymbol{\alpha} \in \mathbb{A}_l} \frac{\Delta(S_{\boldsymbol{\alpha}})^{-1}}{g(\boldsymbol{\alpha}, 1)} =: s. \tag{10}$$

Let $\boldsymbol{a} = [a_1, \ldots, a_{l+1}] \in (\mathbb{Z} \setminus \{0\})^{l+1}$. Since $f(\boldsymbol{x})$ and $g(\boldsymbol{x})$ are symmetric with respect to the coordinates of $\boldsymbol{x}$ and even with respect to each of them, we may assume that

$$0 < a_1 \leqslant a_2 \leqslant \ldots \leqslant a_{l+1}$$

and, since $g(\boldsymbol{a})$ is homogeneous of degree 1, we may assume that

$$(a_1, \ldots, a_{l+1}) = 1.$$

We have $[a_1/a_{l+1}, \ldots, a_l/a_{l+1}] \in \mathbb{A}_l$, hence

$$\Delta(S_{a_1/a_{l+1}, \ldots, a_l/a_{l+1}})^{-1} \leqslant sg\Big(\frac{a_1}{a_{l+1}}, \ldots, \frac{a_l}{a_{l+1}}, 1\Big).$$

Therefore, by the property of critical determinants, every full lattice Λ in $\mathbb{R}^l$ with determinant $d(\Lambda)$ has a non-zero point $(y_1, \ldots, y_l)$ such that

$$f\Big(y_1, \ldots, y_l, \sum_{k=1}^{l} \frac{a_k}{a_{l+1}} y_k\Big)^l \leqslant sg\Big(\frac{a_1}{a_{l+1}}, \ldots, \frac{a_l}{a_{l+1}}, 1\Big) d(\Lambda).$$

Consider now the lattice Λ_0 obtained as projection on the hyperplane $x_{l+1} = 0$ of the

lattice Λ_1 of integer vectors orthogonal to $\boldsymbol{a}$. Let $\boldsymbol{b}_1, \dots, \boldsymbol{b}_l$ be a basis of Λ_1

$$\boldsymbol{b}_k = (b_{k1}, \dots, b_{k,l+1}), \quad B = \begin{pmatrix} \boldsymbol{b}_1 \\ \vdots \\ \boldsymbol{b}_l \end{pmatrix},$$

and let B_k be the minor of B obtained by omitting the k-th column. Since $\Lambda_1 = \Lambda_1^{\perp\perp}$, by Lemma we have

$$\big(B_1, -B_2, \dots, (-1)^l B_{l+1}\big) = 1$$

and $\boldsymbol{b}_k\big(B_1, -B_2, \dots, (-1)^l B_{l+1}\big) = 0$ $(1 \leqslant k \leqslant l)$. Since $(a_1, \dots, a_{k+1}) = 1$ and $\boldsymbol{b}_k \boldsymbol{a} = 0$ there exists an $\varepsilon = \pm 1$ such that $\varepsilon a_k = (-1)^{k+1} B_k$ $(1 \leqslant k \leqslant l)$ and, in particular,

$$a_{l+1} = \big|\det(b_{ij})_{1 \leqslant i,j \leqslant l}\big| = d(\Lambda_0).$$

Hence there exist integers $u_1, \dots, u_l$ not all zero such that

$$f\Big(\sum_{j=1}^{l} b_{j1}u_j, \dots, \sum_{j=1}^{l} b_{jl}u_j, \sum_{k=1}^{l} \frac{a_k}{a_{l+1}} \sum_{j=1}^{l} b_{jk}u_j\Big)^l \leqslant sg\Big(\frac{a_1}{a_{l+1}}, \dots, \frac{a_l}{a_{l+1}}, 1\Big) a_{l+1} = sg(a_1, \dots, a_{l+1}). \tag{11}$$

However, by the definition of Λ_1,

$$\sum_{k=1}^{l+1} a_k b_{jk} = 0 \quad (1 \leqslant j \leqslant l),$$

hence

$$\sum_{k=1}^{l+1} \frac{a_k}{a_{l+1}} b_{jk} = -b_{j,l+1} \quad (1 \leqslant j \leqslant l)$$

and inequality (11) takes the form

$$f\Big(\sum_{j=1}^{l} \boldsymbol{b}_j u_j\Big)^l \leqslant sg(\boldsymbol{a}).$$

Taking $\boldsymbol{x} = \sum_{j=1}^{l} \boldsymbol{b}_j u_j$ we find $\boldsymbol{x} \in \Lambda_1$, hence $\boldsymbol{a}\boldsymbol{x} = 0$ and

$$\frac{f(\boldsymbol{x})^l}{g(\boldsymbol{a})} \leqslant s,$$

which proves (10).

Now we shall prove that

$$\limsup_{\boldsymbol{a}\in(\mathbb{Z}\setminus\{0\})^{l+1}} \inf_{\substack{\boldsymbol{x}\in\mathbb{Z}^{l+1}\setminus\{\boldsymbol{0}\}\\ \boldsymbol{a}\boldsymbol{x}=0}} \frac{f(\boldsymbol{x})^l}{g(\boldsymbol{a})} \geqslant \frac{\Delta(S_{\boldsymbol{\alpha}})^{-1}}{g(\boldsymbol{\alpha},1)} \tag{12}$$

for all $\boldsymbol{\alpha}\in\mathbb{A}_l$.

$S_{\boldsymbol{\alpha}}$ as an open bounded star body has a critical lattice Λ. Let $\boldsymbol{a}_1,\dots,\boldsymbol{a}_l$ be a basis of Λ. Take a positive $\delta<1$ and choose $\boldsymbol{b}_1,\dots,\boldsymbol{b}_l$ in $\mathbb{Q}^l$ such that

$$h(\boldsymbol{b}_j-\boldsymbol{a}_j)<\delta \quad (1\leqslant j\leqslant l), \tag{13}$$

$$\left|\det(\boldsymbol{b}_1^T,\dots,\boldsymbol{b}_l^T)-d(\Lambda)\right|<\delta d(\Lambda)=\delta\Delta(S_{\boldsymbol{\alpha}}). \tag{14}$$

Choose a positive integers d such that $d\boldsymbol{b}_j\in\mathbb{Z}^l$ and $d\alpha_k b_{jk}\in\mathbb{Z}$ for all $j,k\leqslant l$, where b_{jk} is the kth coordinate of $\boldsymbol{b}_j$. We shall apply Theorem 1 taking $m=1$, $F=1$ and taking for $F_{1\nu}$ $(1\leqslant\nu\leqslant l+1)$ all minors of order l of the matrix

$$M=M(T,T_1,\dots,T_l)$$
$$=\begin{pmatrix} db_{11}T+T_1 & db_{12}T & \dots & db_{1l}T & d\sum_{k=1}^{l}\alpha_k b_{1k}T\\ db_{21}T & db_{22}T+T_2 & \dots & db_{2l}T & d\sum_{k=1}^{l}\alpha_k b_{2k}T\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ db_{l1}T & db_{l2}T & \dots & db_{ll}T+T_l & d\sum_{k=1}^{l}\alpha_k b_{lk}T \end{pmatrix},$$

where $T,T_1,\dots,T_l$ are variables. Let $M_i=M_i(T,T_1,\dots,T_l)$ and m_i be the minor obtained by omitting the ith column in M, or in the matrix

$$\begin{pmatrix} b_{11} & b_{12} & \dots & b_{1l} & \sum_{k=1}^{l}\alpha_k b_{1k}\\ \vdots & \vdots & & \vdots & \vdots\\ b_{l1} & b_{l2} & \dots & b_{ll} & \sum_{k=1}^{l}\alpha_k b_{lk} \end{pmatrix}, \text{ respectively.}$$

We have, by (14),

$$|m_{l+1}|=\left|\det(b_{jk})\right|\neq 0, \tag{15}$$

$$|m_i|=\alpha_i|m_{l+1}| \quad (1\leqslant i\leqslant l) \tag{16}$$

and

$$M_i=d^l m_i T^l+\text{polynomial of degree less than } l \text{ in } T, \tag{17}$$

hence M_i is a non-zero polynomial independent of T_i $(1\leqslant i\leqslant l)$. A possible non-constant common factor of $M_1,\dots,M_{l+1}$ would have to belong to $\mathbb{Q}[T]$ and, since these minors are homogeneous in $T,T_1,\dots,T_l,T$ would be a common factor. However

$$M_{l+1}\equiv T_1T_2\dots T_l \bmod T,$$

hence $T \not\parallel M_{l+1}$ and $M_{l+1}(0, 1, \dots, 1) = 1$. By Theorem 1 there exist integers $t_1^*, \dots, t_l^*$ and an arithmetic progression $\mathscr{P}$ such that for $t \in \mathscr{P}$ we have

$$\big(M_1(t, t_1^*, \dots, t_l^*), \dots, M_{l+1}(t, t_1^*, \dots, t_l^*)\big) = 1. \tag{18}$$

Let

$$\boldsymbol{a}(t) = \Big[M_1(t, t_1^*, \dots, t_l^*), \dots, (-1)^l M_{l+1}(t, t_1^*, \dots, t_l^*)\Big].$$

We shall show that for every $\varepsilon > 0$, sufficiently small $\delta > 0$ and sufficiently large $t \in \mathscr{P}$ every integer vector $\boldsymbol{x} \neq \boldsymbol{0}$ such that $\boldsymbol{a}(t)\boldsymbol{x} = 0$ satisfies

$$f(\boldsymbol{x})^l > (1-\varepsilon)\frac{\Delta(S_{\boldsymbol{\alpha}})^{-1}}{g(\boldsymbol{\alpha}, 1)}\, g\big(\boldsymbol{a}(t)\big). \tag{19}$$

By (14)–(17) we have for $\delta < \varepsilon/2$ and sufficiently large t

$$g\big(\boldsymbol{a}(t)\big) = \big(1 + o(1)\big) d^l t^l\, |m_{l+1}|\, g(\boldsymbol{\alpha}, 1) \leqslant d^l t^l g(\boldsymbol{\alpha}, 1)\Big(1 + \frac{\varepsilon}{2}\Big)\Delta(S_{\boldsymbol{\alpha}}). \tag{20}$$

On the other hand, the rows of the matrix $M(t, t_1^*, \dots, t_l^*)$ are orthogonal to $\boldsymbol{a}(t)$ and by (18) and Lemma they form a basis for the lattice of all integer vectors with this property. Therefore, for every $\boldsymbol{x} = [x_1, \dots, x_{l+1}]$ in $\mathbb{Z}^{l+1} \setminus \{\boldsymbol{0}\}$ satisfying $\boldsymbol{a}(t)\boldsymbol{x} = 0$ we have

$$x_k = \sum_{j=1}^{l} u_j (d b_{jk} t + \delta_{jk} t_k^*) \quad (1 \leqslant k \leqslant l), \tag{21}$$

$$x_{l+1} = \sum_{j=1}^{l} u_j \Big(d \sum_{k=1}^{l} \alpha_k b_{jk} t\Big), \tag{22}$$

where δ_{jk} is the Kronecker delta and u_j are integers not all equal to 0. Assume that, contrary to (19),

$$f(\boldsymbol{x})^l \leqslant (1-\varepsilon)\,\frac{\Delta(S_{\boldsymbol{\alpha}})^{-1}}{g(\boldsymbol{\alpha}, 1)}\, g\big(\boldsymbol{a}(t)\big), \tag{23}$$

hence, in particular, $\varepsilon < 1$. By (20) this gives for $\delta < \varepsilon/2$ and sufficiently large t

$$f(\boldsymbol{x})^l \leqslant (1-\varepsilon)\Big(1 + \frac{\varepsilon}{2}\Big) d^l t^l < d^l t^l$$

and, since f is homogeneous of degree 1 and the set $\{\boldsymbol{x} \in \mathbb{R}^{l+1} : f(\boldsymbol{x}) < 1\}$ is bounded,

$$h(\boldsymbol{x}) \leqslant c_f d t, \quad \text{where } c_f \text{ depends only on } f.$$

Solving the system (21) by means of Cramer's formulae we obtain by virtue of (13)–(14) for $\delta < \varepsilon/2$ and sufficiently large t

$$|u_j| \leqslant c_{f, \boldsymbol{a}_k} \quad (1 \leqslant j \leqslant l),$$

where $c_{f, \boldsymbol{a}_k}$ depends only on f and on $\boldsymbol{a}_1, \dots, \boldsymbol{a}_m$.

From the continuity of f at the point

$$\Big[\sum_{j=1}^{l} u_j \boldsymbol{a}_j, \sum_{k=1}^{l} \alpha_k \sum_{j=1}^{l} u_j a_{jk}\Big]$$

we infer that for δ small enough

$$f\Big(\sum_{j=1}^{l} u_j \boldsymbol{b}_j, \sum_{k=1}^{l} \alpha_k \sum_{j=1}^{l} u_j b_{jk}\Big) \geqslant \Big(1 - \frac{\varepsilon}{2l}\Big) f\Big(\sum_{j=1}^{l} u_j \boldsymbol{a}_j, \sum_{k=1}^{l} \alpha_k \sum_{j=1}^{l} u_j a_{jk}\Big),$$

hence, by the choice of $\boldsymbol{a}_j$,

$$f\Big(\sum_{j=1}^{l} u_j \boldsymbol{b}_j, \sum_{k=1}^{l} \alpha_k \sum_{j=1}^{l} u_j b_{jk}\Big)^l > \Big(1 - \frac{\varepsilon}{2l}\Big)^l > 1 - \frac{\varepsilon}{2},$$

by (21) and (22)

$$f(\boldsymbol{x})^l > \Big(1 - \frac{\varepsilon}{2}\Big) d^l t^l + o(t^l),$$

by (20)

$$\frac{f(\boldsymbol{x})^l}{g\big(\boldsymbol{a}(t)\big)} > \big(1 + o(1)\big)\, \frac{2-\varepsilon}{2+\varepsilon}\, \frac{\Delta(S_{\boldsymbol{\alpha}})^{-1}}{g(\boldsymbol{\alpha}, 1)},$$

which for t large enough contradicts (23). The obtained contradiction proves (19) and (12). □

Proof of Corollary 2. For $f = h_{l+1,2} = h_2$ we have

$$S_{\boldsymbol{\alpha}} = \Big\{[x_1, \ldots, x_l] \in \mathbb{R}^l : \sum_{k=1}^{l} x_k^2 + \Big(\sum_{k=1}^{l} \alpha_k x_k\Big)^2 \leqslant 1\Big\}.$$

The matrix of the relevant quadratic form is AA^T, where

$$A = \begin{pmatrix} 1 & 0 & \ldots & 0 & \alpha_1 \\ 0 & 1 & \ldots & 0 & \alpha_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & \alpha_k \end{pmatrix},$$

hence

$$\Delta(S_{\boldsymbol{\alpha}}) = \frac{\gamma_l^{-l/2}}{\sqrt{\det AA^T}} = \frac{\gamma_l^{-l/2}}{\sqrt{\sum_{k=1}^{l} \alpha_k^2 + 1}} \quad \text{and} \quad \frac{\Delta(S_{\boldsymbol{\alpha}})^{-1}}{h_2(\boldsymbol{\alpha}, 1)} = \gamma_l^{l/2}.$$

It remains to consider $\boldsymbol{a} \in \mathbb{Z}^l$ with at least one coordinate 0, say $a_1 = 0$.

Then $\boldsymbol{a}\boldsymbol{x} = 0$ for $\boldsymbol{x} = [1, 0, \dots, 0]$ and

$$\frac{h_2(\boldsymbol{x})^l}{h_2(\boldsymbol{a})} \leqslant 1 < \gamma_l^{l/2}. \qquad \square$$

Proof of Corollary 3. For $f = h_{l+1,\infty} = h$, $\boldsymbol{\alpha} \in \mathbb{A}_l$ we have

$$S_{\boldsymbol{\alpha}} \supset H_{\alpha_1/\alpha_{l-1},\dots,\alpha_{l-2}/\alpha_{l-1}}.$$

Indeed, if $\boldsymbol{x} \in H_{\alpha_1/\alpha_{l-1},\dots,\alpha_{l-2}/\alpha_{l-1}}$ we have

$$|x_k| \leqslant 1 \quad (1 \leqslant k \leqslant l), \tag{24}$$

$$\left|\sum_{k=1}^{l-2} \frac{\alpha_k}{\alpha_{l-1}} x_k + x_{l-1} + x_l\right| \leqslant 1, \tag{25}$$

hence multiplying the last inequality (24) by $\alpha_l/\alpha_{l-1} - 1$ and adding to (25) we obtain

$$\left|\sum_{k=1}^{l} \frac{\alpha_k}{\alpha_{l-1}} x_k\right| \leqslant \frac{\alpha_l}{\alpha_{l-1}} \quad \text{and} \quad \left|\sum_{k=1}^{l} \alpha_k x_k\right| \leqslant \alpha_l \leqslant 1,$$

thus $\boldsymbol{x} \in S_{\boldsymbol{\alpha}}$. It follows that

$$\Delta(S_{\boldsymbol{\alpha}})^{-1} \leqslant \Delta\big(H_{\alpha_1/\alpha_{l-1},\dots,\alpha_{l-2}/\alpha_{l-1}}\big)^{-1}$$

and

$$\sup_{\boldsymbol{\alpha}\in\mathbb{A}_l} \frac{\Delta(S_{\boldsymbol{\alpha}})^{-1}}{h(\boldsymbol{\alpha}, 1)} = \sup_{\boldsymbol{\alpha}\in\mathbb{A}_l} \Delta(S_{\boldsymbol{\alpha}})^{-1} \leqslant \sup_{\boldsymbol{\alpha}\in\mathbb{A}_{l-2}} \Delta(H_{\boldsymbol{\alpha}})^{-1}.$$

Since for $\boldsymbol{\alpha} \in \mathbb{A}_{l-2}$, $H_{\boldsymbol{\alpha}} = S_{\boldsymbol{\alpha},1,1}$, the inequality in the opposite direction is obvious. Also $\Delta(H_{\boldsymbol{\alpha}}) \leqslant 1$, since the only integer point inside $H_{\boldsymbol{\alpha}}$ is $\boldsymbol{0}$.

It remains to consider $\boldsymbol{a} \in \mathbb{Z}^l$ with at least one coordinate 0, say $a_1 = 0$. Then $\boldsymbol{a}\boldsymbol{x} = 0$ for $\boldsymbol{x} = [1, 0, \dots, 0]$ and we have

$$\frac{h(\boldsymbol{x})^l}{h(\boldsymbol{a})} \leqslant 1 \leqslant \sup_{\boldsymbol{\alpha}\in\mathbb{A}_{l-2}} \Delta(H_{\boldsymbol{\alpha}})^{-1}. \qquad \square$$

Proof of Corollary 4. By Corollary 3 we have

$$c(2, \infty) = \Delta(H)^{-1},$$

where H is the hexagon $|x_1| \leqslant 1$, $|x_2| \leqslant 1$, $|x_1 + x_2| \leqslant 1$. Clearly

$$\Delta(H) = \frac{\operatorname{vol} H}{4} = \frac{3}{4}. \qquad \square$$

Proof of Corollary 5. By Corollary 3 we have

$$c(3, \infty) = \sup_{\alpha\in\mathbb{A}_1} \Delta(H)^{-1}.$$

Now, by the result of Whitworth [12]

$$\Delta(H_\alpha) = \begin{cases} \dfrac{3}{4} & \text{if } \alpha \leqslant \dfrac{1}{2} \\ -\dfrac{\alpha^2 + 3\alpha - 24 + \alpha^{-1}}{27} & \text{if } 1 \geqslant \alpha \geqslant \dfrac{1}{2}. \end{cases}$$

Hence $\Delta(H_\alpha)$ takes its minimum in the interval $[0, 1]$ at $\alpha = 1$ and $\Delta(H_1) = 19/27$. □

Remark 1. Using the equality $\Delta(H_\alpha) = \frac{3}{4}$ if $\alpha \leqslant \frac{1}{2}$ and following the first part of the proof of Theorem 2 we infer that if $\boldsymbol{a} = [a_1, a_2, a_3, a_4] \in \mathbb{Z}^4$, $0 \leqslant a_1 \leqslant a_2 \leqslant a_3 \leqslant a_4$ and $a_1 \leqslant \frac{1}{2}a_2$, then there exists $\boldsymbol{x} \in \mathbb{Z}^4$ such that $0 < h(\boldsymbol{x}) \leqslant \sqrt[3]{\frac{4}{3}h(\boldsymbol{a})}$. This improves a conditional result of Chaładus [4] obtained under an unproved assumption and the stronger condition $a_4 \leqslant -2a_1 + a_2 + a_3$.

Proof of Corollary 6. By Corollary 3 we have

$$c(l, \infty) = \sup_{\boldsymbol{\alpha} \in \mathbb{A}_{l-2}} \Delta(H_{\boldsymbol{\alpha}})^{-1} \geqslant 1.$$

Now, by Minkowski's theorem and Theorem 1 of Vaaler [10]

$$\Delta(H_{\boldsymbol{\alpha}}) \geqslant \frac{\operatorname{vol} H_{\boldsymbol{\alpha}}}{2^l} \geqslant \left(\sqrt{\sum_{k=1}^{l} \alpha_k^2 + 1} \right)^{-1} \geqslant \frac{1}{\sqrt{l+1}}. \qquad \square$$

Proof of Theorem 3. By Corollary 1 for every positive integer l and every $\varepsilon > 0$ there exist infinitely many $\boldsymbol{a}$ in $\mathbb{Z}^{l+1}$ such that every $\boldsymbol{y} \in \mathbb{Z}^{l+1} \setminus \{\boldsymbol{0}\}$ with $\boldsymbol{a}\boldsymbol{y} = 0$ satisfies

$$\frac{h_2(\boldsymbol{y})^l}{h_2(\boldsymbol{a})} > \gamma_l^{l/2} - \varepsilon. \tag{26}$$

Replacing if necessary $\boldsymbol{a}$ by $\boldsymbol{a}/D(\boldsymbol{a})$ we may assume that $D(\boldsymbol{a}) = 1$. Take now $l = n - m$, $A = (a_{ij})$ where $i \leqslant m$, $j \leqslant n$,

$$a_{ij} = \begin{cases} a_j, & \text{if } i = 1,\ j \leqslant l+1, \\ 1, & \text{if } i > 1,\ j = n - m + i, \\ 0, & \text{otherwise.} \end{cases}$$

We have

$$H(A) = \frac{h_2(\boldsymbol{a})}{D(\boldsymbol{a})} = h_2(\boldsymbol{a}). \tag{27}$$

On the other hand, $\boldsymbol{x} \in \mathbb{Z}^n$, $A\boldsymbol{x} = \boldsymbol{0}$ implies $\boldsymbol{x} = [\boldsymbol{y}, 0, \ldots, 0]^T$, where $\boldsymbol{y} \in \mathbb{Z}^{l+1}$, $\boldsymbol{a}\boldsymbol{y} = 0$, hence by (27) and (26)

$$\frac{h_2(\boldsymbol{x})^l}{H(A)} = \frac{h_2(\boldsymbol{y})^l}{h_2(\boldsymbol{a})} > \gamma_l^{l/2} - \varepsilon,$$

where $H(A)$ can be arbitrarily large. This proves that $c_0(m,n) \geqslant \gamma_{n-m}^{(n-m)/2}$.

In order to prove the remaining part of the theorem consider a matrix $A \in \mathbb{Z}^{m\times n}$ of rank m. Let Λ be a lattice spanned by the rows of A, and $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_l$ $(l = n-m)$ be a basis of $\Lambda^\perp$ and $B = \begin{pmatrix} \boldsymbol{b}_1 \\ \vdots \\ \boldsymbol{b}_l \end{pmatrix}$.

Since $\Lambda^{\perp\perp\perp} = \Lambda^\perp$ we have by Lemma $D(B) = 1$, hence $H(B) = \sqrt{\det BB^T}$.

On the other hand, by Theorem 1 of Thunder [8] we have

$$H(A) = H(B).$$

Consider the ellipsoid

$$E : \sum_{j=1}^{n}\Big(\sum_{k=1}^{l} b_{kj}u_k\Big)^2 \leqslant 1.$$

The matrix of the quadratic form on the left hand side is BB^T, hence

$$\Delta(t) = \frac{\gamma_l^{-l/2}}{\sqrt{\det BB^T}}.$$

By the property of critical determinants there exist integers u_k not all 0 such that

$$h_2^l\Big(\sum_{k=1}^{l}\boldsymbol{b}_k u_k\Big) \leqslant \gamma_l^{l/2}\sqrt{\det BB^T} = \gamma_l^{l/2}H(B) = \gamma_l^{l/2}H(A).$$

Taking $\boldsymbol{x}^T = \sum_{k=1}^{l}\boldsymbol{b}_k u_k$ we obtain $\boldsymbol{x} \in \mathbb{Z}^n \setminus \{\boldsymbol{0}\}$, $A\boldsymbol{x} = \boldsymbol{0}$ and

$$\frac{h_2(\boldsymbol{x})^l}{H(A)} \leqslant \gamma_l^{l/2},$$

which completes the proof. □

Remark 2. Since for ellipsoids the anomaly is 1 the last argument shows in fact the existence of linearly independent vectors $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_l$ in $\mathbb{Z}^n$ such that $A\boldsymbol{x}_k = \boldsymbol{0}$ $(1 \leqslant k \leqslant l)$ and

$$\prod_{k=1}^{l} h(\boldsymbol{x}_k) \leqslant \gamma_l^{l/2}H(A).$$

References

[1] I. Aliev, *On a decomposition of integer vectors*. Ph.D. Thesis. Institute of Mathematics, Polish Academy of Sciences, Warsaw 2001.

[2] E. Bombieri, J. D. Vaaler, *On Siegel's Lemma*. Invent. Math. 73 (1983), 11–32; *Addendum*, ibid. 75 (1984), 377.

[3] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*. Springer, Berlin 1959.

[4] S. Chaładus, *On the densest lattice packing of centrally symmetric octahedra*. Math. Comp. 58 (1992), 341–345.

[5] S. Chaładus, A. Schinzel, *A decomposition of integer vectors* II. Pliska Stud. Math. Bulgar. 11 (1991), 15–23; this collection: L1, 1249–1258.

[6] D. R. Heath-Brown, *Diophantine approximation with square-free numbers*. Math. Z. 187 (1984), 335–344.

[7] W. M. Schmidt, *Diophantine Approximations and Diophantine Equations*. Lecture Notes in Math. 1467, Springer, Berlin 1991.

[8] J. L. Thunder, *Asymptotic estimates for rational points of bounded height on flag varieties*. Compositio Math. 88 (1993), 155–186.

[9] —, *An adelic Minkowski–Hlawka theorem and an application to Siegel's lemma*. J. Reine Angew. Math. 475 (1996), 167–185.

[10] J. D. Vaaler, *A geometric inequality with applications to linear forms*. Pacific J. Math. 83 (1979), 543–553.

[11] T. Watanabe, *On an analog of Hermite's constant*. J. Lie Theory 10 (2000), 33–52.

[12] J. V. Whitworth, *On the densest packing of sections of a cube*. Ann. Math. Pura Appl. (4) 27 (1948), 29–37.

Originally published in
Monatshefte für Mathematik
144 (2005), 177–191

On vectors whose span contains a given linear subspace

with I. Aliev (Wien) and W. M. Schmidt (Boulder)*

Abstract. Estimates are given for the product of the lengths of integer vectors spanning a given linear subspace.

The aim of this paper is to estimate for $k > l > m > 0$

$$c(k,l,m) = \sup \inf H(S)^{(l-k)/(k-m)} \prod_{i=1}^{l} |\boldsymbol{p}_i|, \tag{1}$$

where the supremum is taken over all subspaces S of $\mathbb{Q}^k$ of dimension m and the infimum is taken over all sets of linearly independent vectors $\boldsymbol{p}_1, \dots, \boldsymbol{p}_l$ in $\mathbb{Z}^k$, whose span contains S. Here $H(S)$ is the determinant of the lattice $S \cap \mathbb{Z}^k$ and $|\boldsymbol{p}|$ is the Euclidean norm of $\boldsymbol{p}$.

Let $\gamma_{r,s}$ be the generalized Hermite constant, as defined by Rankin [7], i.e. the least number such that every lattice Λ of rank r in $\mathbb{R}^r$ has a sublattice Γ of rank s and determinant

$$\det \Gamma \leqslant \gamma_{r,s}^{1/2} (\det \Lambda)^{s/r} .$$

Here, $\gamma_{r,1} = \gamma_{r,r-1} = \gamma_r$ is the ordinary Hermite constant. We shall prove

Theorem 1.

$$\gamma_{k-m,k-l}^{1/2} \leqslant c(k,l,m) \leqslant \gamma_{k-m,k-l}^{1/2} \gamma_l^{l/2}.$$

Corollary 1.

$$\gamma_{k-1}^{1/2} \leqslant c(k,2,1) \leqslant \gamma_{k-1}^{1/2} \sqrt{\frac{4}{3}}.$$

Theorem 2.

$$c(3,2,1) \geqslant 6/(722)^{1/4} > \gamma_2.$$

Communicated by F. Grunewald

* The first author was supported by FWF Austrian Science Fund, project M672.

A related problem has been considered in [1], [4], [5] and [8]. Given m linearly independent vectors $\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m$ in $\mathbb{Z}^k$ let $H(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)$ denote the maximum of the absolute values of $m \times m$-minors of the matrix $(\boldsymbol{n}_1^t, \ldots, \boldsymbol{n}_m^t)$ and $D(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)$ the greatest common divisor of these minors. Furthermore, let $h(\boldsymbol{n}) = H(\boldsymbol{n})$ for $\boldsymbol{n} \neq \boldsymbol{0}$. In [1], [4], [5] and [8] the following quantity has been estimated

$$c_0(k, l, m) = \sup \inf \left(\frac{D(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)}{H(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)} \right)^{(k-l)/(k-m)} \prod_{i=1}^{l} h(\boldsymbol{p}_i), \tag{2}$$

where the supremum is taken over all sets of linearly independent vectors $\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m$ in $\mathbb{Z}^k$ and the infimum is taken over all sets of linearly independent vectors $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_l$ in $\mathbb{Z}^k$ such that for all $i \leqslant m$

$$\boldsymbol{n}_i = \sum_{j=1}^{l} u_{ij} \boldsymbol{p}_j, \quad u_{ij} \in \mathbb{Q}.$$

In particular, it has been proved in [8] that for fixed l, m

$$\limsup_{k \to \infty} c_0(k, l, m) < \infty, \tag{3}$$

in [1] that

$$c_0(k, 2, 1) \leqslant \frac{2}{k^{1/(k-1)}},$$

in [4] that $c_0(3, 2, 1) = 2/\sqrt{3}$, and in [5] that

$$c_0(k, l, m) \leqslant \gamma_{k-m,k-l}^{1/2} \binom{k}{m}^{(k-l)/2(k-m)}. \tag{4}$$

Taking for $\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m$ a basis of the lattice $S \cap \mathbb{Z}^k$ and using the inequalities

$$|\boldsymbol{p}| \leqslant k^{1/2} h(\boldsymbol{p}), \quad \frac{H(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)}{D(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)} \leqslant H(S)$$

one obtains from (1), (2) and (4)

$$c(k, l, m) \leqslant \gamma_{k-m,k-l}^{1/2} \binom{k}{m}^{(k-l)/2(k-m)} k^{l/2},$$

following the proof in [5] one can omit the factor $\binom{k}{m}^{(k-l)/2(k-m)}$. It follows from Corollary 1 that, in contrast to (3),

$$\lim_{k \to \infty} c(k, 2, 1) = \infty$$

and from Theorem 2 that, at least for $k = 3$ the lower bound given in Corollary 1 for $c(k, 2, 1)$ is not sharp. The proof of Theorem 2 is based on the following theorem of independent interest.

Theorem 3. *If Λ_t is a sequence of lattices in $\mathbb{R}^l$ convergent to a full lattice Λ and $\lambda_i(K, \Lambda)$ is the i-th minimum of Λ with respect to a centrally symmetric convex body K, then for each $i \leqslant l$*

$$\lim_{t\to\infty} \lambda_i(K, \Lambda_t) = \lambda_i(K, \Lambda).$$

(We say, following [3], Chapter V, §3, that a sequence of lattices Λ_t in $\mathbb{R}^l$ is convergent to a lattice Λ, if there exists a linear homogeneous transformation τ_t such that $\Lambda_t = \tau_t \Lambda$ and $\|\tau_t - \iota\|$ tends to 0 for t tending to infinity, where ι is the identity transformation and $\|\tau\| = l \max_{1\leqslant i,j\leqslant l} |\tau_{ij}|$.)

Corollary 2. *Let $f_t(x, y)$ be a sequence of positive definite quadratic forms over $\mathbb{R}$, m_t and $\overline{m}_t$ be the first and the second minimum of $f_t(u, v)$ for $(u, v) \in \mathbb{Z}^2$. If*

$$\lim_{t\to\infty} f_t = f,$$

where f is positive definite, then

$$\lim_{t\to\infty} m_t = m, \quad \lim_{t\to\infty} \overline{m}_t = \overline{m},$$

where m and $\overline{m}$ are the first and the second minimum of f, respectively.

For $i = 1$ Theorem 3 has been known, see [3], Chapter V, §3.3, Remark. The proof of Theorem 1 is based on the following

Proposition 1. *Let S be an m-dimensional subspace of $\mathbb{Q}^k$.*

(i) *When $0 < n < m < k$, there is a subspace $T \subset S$ of dimension n with*

$$H(T) \leqslant \gamma_{m,n}^{1/2} H(S)^{n/m}. \tag{5}$$

The constant $\gamma_{m,n}^{1/2}$ here is best possible.

(ii) *When $m < l < k$, there is a subspace $T \supset S$ of dimension l in $\mathbb{Q}^k$ with*

$$H(T) \leqslant \gamma_{k-m,k-l}^{1/2} H(S)^{(k-l)/(k-m)}. \tag{6}$$

The constant $\gamma_{k-m,k-l}^{1/2}$ here is best possible.

Proof. (i) A lattice $\Lambda \subset \mathbb{Z}^k$ is primitive if $\Lambda = S \cap \mathbb{Z}^k$, where S is the subspace of $\mathbb{Q}^k$ spanned by Λ. There is a (C) correspondence of subspaces of $\mathbb{Q}^k$ and primitive lattices. To a space S corresponds $\Lambda = S \cap \mathbb{Z}^k$, and to a primitive lattice Λ corresponds the space S spanned by it. When S, Λ correspond to each other, $\dim S = \operatorname{rank} \Lambda$, and $H(S) = \det \Lambda$. To a subspace T of S corresponds a primitive sublattice Γ of Λ. The existence of T as claimed in (i) now follows from the definition of $\gamma_{m,n}$.

Let $\mathbb{O}_m$ be the orthogonal group in $\mathbb{R}^m$, and $\widetilde{\mathbb{O}}_m$ the group of matrices $K = \lambda O$ with $\lambda \in \mathbb{R}^+$, $O \in \mathbb{O}_m$. Full lattices Λ, Λ' in $\mathbb{R}^m$ are similar, if $\Lambda' = K\Lambda$ with $K \in \widetilde{\mathbb{O}}_m$. Let $\gamma_{m,n}(\Lambda)$ be the minimum such that there is a sublattice Γ of Λ of rank n with

$$\det \Gamma = \gamma_{m,n}^{1/2}(\Lambda) \, (\det \Lambda)^{n/m} .$$

Similar lattices Λ, Λ' have $\gamma_{m,n}(\Lambda) = \gamma_{m,n}(\Lambda')$.

When $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ is a basis of Λ, the matrix $A = (\boldsymbol{a}_1^t, \ldots, \boldsymbol{a}_m^t) \in \mathbb{GL}_m(\mathbb{R})$ with columns $\boldsymbol{a}_1^t, \ldots, \boldsymbol{a}_m^t$ will also be called a basis. Now A can uniquely be written as $A = KZ$, with $K \in \mathbb{O}_m$ and $Z \in \mathscr{H}_m$, the generalized half-plane (see, e.g. [10], p. 38). The general basis of Λ is AM with $M \in \mathbb{GL}_m(\mathbb{Z})$ and $AM = K_M Z_M$, where again $K_M \in \mathbb{O}_m$, $Z_M \in \mathscr{H}_m$. The map $Z \mapsto Z_m$ determines an action of $\mathbb{GL}_m(\mathbb{Z})$ on $\mathscr{H}_m$. Let $\mathscr{F}_m$ be $\mathscr{H}_m$ modulo this action, i.e., where Z, Z_M with $M \in \mathbb{GL}_m(\mathbb{Z})$ are identified. Then to Λ corresponds a unique $\overline{Z} = \overline{Z}(\Lambda) \in \mathscr{F}_m$, and $\overline{Z}(\Lambda) = \overline{Z}(\Lambda')$ precisely when Λ, Λ' are similar. There is a certain measure μ on $\mathscr{F}_k$ with $\mu(\mathscr{F}_k) = 1$, and $\mu(D) > 0$ for every non-empty open subset D.

A lattice Λ of rank m in $\mathbb{R}^k$ is a full lattice in the space it spans, and $\overline{Z}(\Lambda) \in \mathscr{F}_m$ is again well defined. In [10] it was shown that when $D \subset \mathscr{F}_m$ is open and non-empty, then the number of primitive lattices Λ of rank m with $\overline{Z}(\Lambda) \in D$ and the determinant not exceeding T is asymptotically equal to $c_{k,m}\mu(D)T^k$, as $T \to \infty$, where $c_{k,m} > 0$. Therefore as Λ ranges through primitive lattices of rank m in $\mathbb{R}^k$, the elements $\overline{Z}(\Lambda)$ will be dense in $\mathscr{F}_m$. There is a lattice Λ_1 with $\gamma_{m,n}(\Lambda_1) = \gamma_{m,n}$. Set $\overline{Z}_1 = \overline{Z}(\Lambda_1)$. Given $\epsilon > 0$ we have

$$\gamma_{m,n}(\Lambda) > \gamma_{m,n} - \epsilon, \tag{7}$$

when Λ is near Λ_1, i.e., when Λ has a basis near some fixed basis of Λ_1. There is a neighborhood D of $\overline{Z}_1$ in $\mathscr{F}_m$ such that (7) holds when $\overline{Z}(\Lambda) \in D$. By the density property enunciated above, there is a primitive lattice Λ of rank m with (7). Since $\epsilon > 0$ was arbitrary, and by the correspondence (C) of rational subspaces and primitive lattices, we see that the constant $\gamma_{m,n}^{1/2}$ in (5) is best possible.

(ii) The orthogonal complement $S^\perp$ of S has dimension $k - m$. By (i) there is a space $T^\perp \subset S^\perp$ of dimension $k - l$ with

$$H(T^\perp) \leqslant \gamma_{k-m,k-l}^{1/2} H(S^\perp)^{(k-l)/(k-m)}.$$

The orthogonal complement T of $T^\perp$ has $T \supset S$, $\dim T = l$. Now (6) is a consequence of

$$H(S^\perp) = H(S), \quad H(T^\perp) = H(T). \tag{8}$$

(For a proof of the last formulae, see [2], pp. 27–28.) By (i), there is for any $\epsilon > 0$ a space $S^\perp$ of dimension $k - m$ such that

$$H(T^\perp) \geqslant (\gamma_{k-m,k-l}^{1/2} - \epsilon) H(S^\perp)^{(k-l)/(k-m)}, \tag{9}$$

for any space $T^\perp \subset S^\perp$ of dimension $k - m$. Let S be the orthogonal complement of $S^\perp$. When $T \supset S$, $\dim T = l$, then $T^\perp$ satisfies (9), hence by (8)

$$H(T) \geqslant (\gamma_{k-m,k-l}^{1/2} - \epsilon) H(S)^{(k-l)/(k-m)}.$$

This shows that the constant in (6) is best possible. □

Proposition 2. *Let S be an m-dimensional subspace of $\mathbb{Q}_k$. When $0 < n \leqslant m$, there are linearly independent integer vectors $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$ in S with*

$$|\boldsymbol{p}_1| \cdots |\boldsymbol{p}_n| \leqslant \gamma_m^{n/2} H(S)^{n/m}. \tag{10}$$

The constant $\gamma_m^{n/2}$ here is best possible.

Proof. By Minkowski's second theorem for balls (see [3], Chapter VIII, Theorem I) in $\Lambda = S \cap \mathbb{Z}^k$ there are independent vectors $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_m$ with

$$|\boldsymbol{p}_1| \cdots |\boldsymbol{p}_m| \leqslant \gamma_m^{m/2} \det \Lambda = \gamma_m^{m/2} H(S),$$

where $|\boldsymbol{p}_1| \leqslant \ldots \leqslant |\boldsymbol{p}_m|$, so that (10) holds. The constant $\gamma_m^{n/2}$ is best possible in (10) by the definition of γ_m. □

Proof of Theorem 1. Let T be a space as in the part (ii) of Proposition 1. By Proposition 2 there are integer vectors $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_l$ which span T and have

$$|\boldsymbol{p}_1| \cdots |\boldsymbol{p}_l| \leqslant \gamma_l^{l/2} H(T) \leqslant \gamma_l^{l/2} \gamma_{k-m,k-l}^{1/2} H(S)^{(k-l)/(k-m)}.$$

This implies

$$c(k, l, m) \leqslant \gamma_{k-m,k-l}^{1/2} \gamma_l^{l/2}.$$

On the other hand, let $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_l$ be independent and with span T containing S. Then

$$|\boldsymbol{p}_1| \cdots |\boldsymbol{p}_l| \geqslant H(T)$$

(cf. [2], formula (2.6)) and for $\epsilon > 0$ we shall necessarily have by Proposition 1(ii)

$$H(T) > (\gamma_{k-l,k-m}^{1/2} - \epsilon) H(S)^{(k-l)/(k-m)}.$$

This proves

$$c(k, l, m) \geqslant \gamma_{k-l,k-m}^{1/2}.$$ □

Proof of Corollary 1. From Theorem 1 we obtain

$$\gamma_{k-1,k-2}^{1/2} \leqslant c(k, 2, 1) \leqslant \gamma_{k-1,k-2}^{1/2} \gamma_2$$

and it suffices to use $\gamma_{k-1,k-2} = \gamma_{k-1}$, $\gamma_2 = \sqrt{4/3}$. □

Proof of Theorem 3. We will use properties of convergent sequences of lattices as given in [3]. When $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_l$ is a basis of a lattice Λ in $\mathbb{R}^l$, the matrix $A = (\boldsymbol{a}_1^t, \ldots, \boldsymbol{a}_l^t)$ will also be called a basis of Λ, as in the proof of Theorem 1. There is a finite set $\mathscr{V}$ of non-singular integer matrices such that when $M \subset \Lambda$ are lattices with $[\Lambda : M] \leqslant l!$ and B is a basis of Λ, then there is a $V \in \mathscr{V}$ such that $A = BV$ is a basis of M. Conversely, when A is a basis of M, then there is a $U \in \mathscr{V}$ and a basis B of U with $A = BU$ (see [3], Chapter I, §2.2, where the roles of Λ, M are reversed).

Let $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_l$ be independent elements of Λ with $F(\boldsymbol{a}_i) = \lambda_i$ $(i = 1, \ldots, l)$, where $\lambda_1, \ldots, \lambda_l$ are the successive minima of Λ and F is the distance function determined

by K. Here $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_l$ generate a sublattice $M \subset \Lambda$ with $[\Lambda : M] \leqslant l!$ (*ibid.*, p. 219). Say $A = (\boldsymbol{a}_1^t, \ldots, \boldsymbol{a}_l^t)$, $A = BV$ with B a basis of Λ. Now, if $\Lambda_t \to \Lambda$ for lattices $\Lambda_1, \Lambda_2, \ldots$ there are bases B_t of Λ_t with $B_t \to B$. Setting $A_t = B_t V$, say $A_t = (\boldsymbol{a}_{1t}^t, \ldots, \boldsymbol{a}_{lt}^t)$, the points $\boldsymbol{a}_{1t}, \ldots, \boldsymbol{a}_{lt}$ are independent in Λ_t and $\lim F(\boldsymbol{a}_{it}) = F(\boldsymbol{a}_i) = \lambda_i$ $(i = 1, \ldots, l)$. So, if $\lambda_{1t}, \ldots, \lambda_{lt}$ are the successive minima of Λ_t, we have $\limsup \lambda_{it} \leqslant \lambda_i$ $(i = 1, \ldots, l)$.

Set now $A_t^* = \big((\boldsymbol{a}_{1t}^*)^t, \ldots, (\boldsymbol{a}_{lt}^*)^t\big)$, where $(\boldsymbol{a}_{1t}^*)^t, \ldots, (\boldsymbol{a}_{lt}^*)^t$ are independent in Λ_t with $F(\boldsymbol{a}_{it}^*) = \lambda_{it}$ $(i = 1, \ldots, l)$, where $\lambda_{1t}, \ldots, \lambda_{lt}$ are the minima of Λ_t. We have $A_t^* = B_t^* V_t$, where B_t^* is a basis of Λ_t and $V_t \in \mathscr{V}$. Pick i_0, $1 \leqslant i_0 \leqslant l$, and set $\widetilde{\lambda}_{i_0} = \liminf \lambda_{i_0 t}$, as $t \to \infty$. Pick a subsequence, where $\lambda_{i_0 t} \to \widetilde{\lambda}_{i_0}$, and a subsequence of that one, where V_t is constant, so that $A_t^* = B_t^* V^*$, with $V^* \in \mathscr{V}$.

Since the sequence Λ_t is convergent, the minima λ_{it} are bounded, i.e. the $F(\boldsymbol{a}_{it}^*)$ are bounded, therefore the lengths a_{it}^* are bounded. So taking a further subsequence, A_t^* is convergent, say $A_t^* \to A^* = (\boldsymbol{a}_1^*, \ldots, \boldsymbol{a}_l^*)$. Thus $B_t^* \to B^*$, where B^* is a basis of Λ and $A^* = B^* V^*$. Thus $\boldsymbol{a}_1^*, \ldots, \boldsymbol{a}_l^*$ are in Λ and linearly independent. In particular, $F(\boldsymbol{a}_1^*) \leqslant \ldots \leqslant F(\boldsymbol{a}_{i_0}^*)$, so that λ_{i_0} the i_0-th minimum of Λ, has $\lambda_{i_0} \leqslant F(\boldsymbol{a}_{i_0}^*) = \widetilde{\lambda}_{i_0} = \liminf \lambda_{i_0 t}$. Since i_0 was arbitrary in $\{1, \ldots, l\}$, and by above inequality involving lim sup, we see that

$$\lim_{t \to \infty} \lambda_{it} = \lambda_i \quad (1 \leqslant i \leqslant l). \qquad \square$$

Proof of Corollary 2. If $f_t = a_t u^2 + b_t uv + c_t v^2$ it suffices to put in Theorem 3 $l = 2$, $K = \{(x, y) : x^2 + y^2 \leqslant 1\}$,

$$\Lambda_t = \big(\sqrt{a_t}, 0\big)\mathbb{Z} \oplus \left(\frac{b_t}{2\sqrt{a_t}}, \frac{\sqrt{4a_t c_t - b_t^2}}{2\sqrt{a_t}}\right)\mathbb{Z}. \qquad \square$$

The proof of Theorem 2 is based on Corollary 2 and on four lemmas.

Lemma 1. *Let* $\boldsymbol{n} = (15t^2 - t - 4, 3t^2 - 1, 3t^2 - t - 1) \times (69t^2 - 5, 21t^2 - 2, 0)$. *If* $t \in \mathbb{Z}$, $t \not\equiv -7 \bmod 17$, $t \not\equiv \pm 3 \bmod 11$,

$$\boldsymbol{m}\boldsymbol{n} = 0 \quad \textit{and} \quad |\boldsymbol{m}| \leqslant 18t^2, \quad \boldsymbol{m} \in \mathbb{Z}^3 \setminus \{\boldsymbol{0}\}, \tag{11}$$

then for large t

$$\boldsymbol{m} = \pm\boldsymbol{m}_1, \pm\boldsymbol{m}_2, \pm\boldsymbol{m}_3,$$

where

$$\begin{aligned}
\boldsymbol{m}_1 &= (15t^2 - t - 4, 3t^2 - 1, 3t^2 - t - 1),\\
\boldsymbol{m}_2 &= (9t^2 + 4t + 11, 9t^2 + 2, -12t^2 + 4t + 4),\\
\boldsymbol{m}_3 &= (-6t^2 + 5t + 15, 6t^2 + 3, -15t^2 + 5t + 5).
\end{aligned}$$

Proof. (11) implies that

$$\boldsymbol{m} = u(15t^2 - t - 4, 3t^2 - 1, 3t^2 - t - 1) + v(69t^2 - 5, 21t^2 - 2, 0),$$

where $u, v \in \mathbb{Q}$. Since $\boldsymbol{m} \in \mathbb{Z}^3$ we have

$$u(15t^2 - t - 4) + v(69^2 - 5) \in \mathbb{Z}, \tag{12}$$

$$u(3t^2 - 1) + v(21t^2 - 2) \in \mathbb{Z}, \tag{13}$$

$$u(3t^2 - t - 1) \in \mathbb{Z}. \tag{14}$$

The relations (12) and (13) give $uD \in \mathbb{Z}$, where

$$\begin{aligned} D &= (21t^2 - 2)(15t^2 - t - 4) - (3t^2 - 1)(69t^2 - 5) \\ &\equiv (7t + 5)(4t + 1) - t(23t + 18) \\ &\equiv 5t^2 + 9t + 5 \\ &\equiv -t^2 + 11t + 7 \bmod 3t^2 - t - 1, \end{aligned}$$

hence

$$3D \equiv 32t + 20 = 4(8t + 5) \bmod 3t^2 - t - 1.$$

However $\gcd(2, 3t^2 - t - 1) = 1$, $64(3t^2 - t - 1) - (8t + 5)(24t - 23) = 51$, for $t \not\equiv -7 \bmod 17$, $8t + 5 \not\equiv 0 \bmod 17$, for $t \not\equiv -1 \bmod 3$, $8t + 5 \not\equiv 0 \bmod 3$ and for $t \equiv 1 \bmod 3$, $D \equiv 1 \bmod 3$. Thus $\gcd(D, 3t^2 - t - 1) = 1$ and (12)–(14) imply $u \in \mathbb{Z}$. Hence

$$v(69t^2 - 5) \in \mathbb{Z}, \quad v(21t^2 - 2) \in \mathbb{Z}. \tag{15}$$

However

$$(69t^2 - 5)7 - (21t^2 - 2)23 = 11,$$

hence if $t \not\equiv \pm 3 \bmod 11$, we have $\gcd(69t^2 - 5, 21t^2 - 2) = 1$ and (15) implies $v \in \mathbb{Z}$. Now, if $|\boldsymbol{m}| \leqslant 18t^2$ we have

$$|\boldsymbol{m}|^2 = Au^2 + 2Buv + Cv^2 \leqslant 324t^4, \tag{16}$$

where for t tending to infinity

$$\begin{aligned} A &= (15t^2 - t - 4)^2 + (3t^2 - 1)^2 + (3t^2 - t - 1)^2 = 243t^4 + O(t^3), \\ B &= (15t^2 - t - 4)(69t^2 - 5) + (3t^2 - 1)(21t^2 - 2) = 1098t^4 + O(t^3), \\ C &= (69t^2 - 5)^2 + (21t^2 - 2)^2 = 5202t^4 + O(t^3), \end{aligned}$$

hence

$$AC - B^2 = 58482t^8 + O(t^7) = 81 \cdot 722t^8 + O(t^7).$$

The inequality (16) gives

$$\begin{aligned} u^2 &\leqslant \frac{324Ct^4}{AC - B^2} = \frac{4C}{722t^4 + O(t^3)} < 29 + O(t^{-1}), \\ v^2 &\leqslant \frac{324At^4}{AC - B^2} = \frac{4A}{722t^4 + O(t^3)} < 2 + O(t^{-1}), \end{aligned}$$

hence for large t

$$|u| \leqslant 5, \quad |v| \leqslant 1$$

and (16) implies

$$243u^2 + 2196uv + 5202v^2 \leqslant 324,$$
$$(27u + 112v)^2 + 722v^2 \leqslant 972.$$

We obtain either $u = \pm 1$, $v = 0$, or $v = \pm 1$, $u = -4v$, or $u = -5v$. The first case gives $\boldsymbol{m} = \pm \boldsymbol{m}_1$, the second case $\boldsymbol{m} = \pm \boldsymbol{m}_2$, the third case $\boldsymbol{m} = \pm \boldsymbol{m}_3$. □

Lemma 2. *If $\boldsymbol{p} \in \mathbb{Z}^3 \setminus \{\mathbf{0}\}$ and $\boldsymbol{p}\boldsymbol{m}_1 = 0$, then for t tending to infinity*

$$|\boldsymbol{p}| \geqslant \sqrt{18}t + o(t).$$

Proof. We easily verify that

$$\boldsymbol{p}_1\boldsymbol{m}_1 = \boldsymbol{q}_1\boldsymbol{m}_1 = 0,$$

where

$$\boldsymbol{p}_1 = (t, -4t - 1, 1 - t), \quad \boldsymbol{q}_1 = (1, -3t - 3, 3t - 1).$$

Since $\boldsymbol{p}_1, \boldsymbol{q}_1$ are linearly independent, $\boldsymbol{p}\boldsymbol{m}_1 = 0$, $\boldsymbol{p} \in \mathbb{Z}^3$ implies

$$\boldsymbol{p} = u\boldsymbol{p}_1 + v\boldsymbol{q}_1,$$

where $u, v \in \mathbb{Q}$. Now $\boldsymbol{p} \in \mathbb{Z}^3$ implies

$$\begin{gathered} ut + v \in \mathbb{Z}, \\ u(4t + 1) + v(3t + 3) \in \mathbb{Z}, \\ u(1 - t) + v(3t - 1) \in \mathbb{Z}, \end{gathered} \tag{17}$$

hence by taking determinants

$$u(3t^2 - t - 1) \in \mathbb{Z}, \quad u(3t^2 - 1) \in \mathbb{Z}, \quad u(15t^2 - t - 4) \in \mathbb{Z}. \tag{18}$$

However

$$15t^2 - t - 4 - 4(3t^2 - 1) - (3t^2 - t - 1) = 1,$$

hence $\gcd(3t^2 - t - 1, 3t^2 - 1, 15t^2 - t - 4) = 1$, (18) implies $u \in \mathbb{Z}$ and by (17) $v \in \mathbb{Z}$. Now

$$|\boldsymbol{p}|^2 = A_1(t)u^2 + 2B_1(t)uv + C_1(t)v^2,$$

where

$$A_1(t) = 18t^2 + O(t), \quad B_1(t) = 9t^2 + O(t), \quad C_1(t) = 18t^2 + O(t).$$

The sequence of quadratic forms

$$\frac{A_1(t)}{t^2}\, x^2 + 2\,\frac{B_1(t)}{t^2}\, xy + \frac{C_1(t)}{t^2}\, y^2$$

tends to $18x^2 + 18xy + 18y^2$ and this quadratic form has minimum 18. It follows by Corollary 2 that

$$|\boldsymbol{p}|^2 \geqslant 18t^2 + o(t^2),$$

which gives Lemma 2. □

Lemma 3. *If* $\boldsymbol{p}\boldsymbol{m}_2 = \boldsymbol{q}\boldsymbol{m}_2 = 0$, *where* $\boldsymbol{p}, \boldsymbol{q} \in \mathbb{Z}^3$, $\boldsymbol{p}, \boldsymbol{q}$ *linearly independent,* $t \equiv 2 \bmod 28$, *then for* t *tending to infinity*

$$|\boldsymbol{p}|\,|\boldsymbol{q}| \geqslant \sqrt{328}t^2 + o(t^2).$$

Proof. We easily verify that

$$\boldsymbol{p}_2\boldsymbol{m}_2 = \boldsymbol{q}_2\boldsymbol{m}_2 = 0,$$

where

$$\boldsymbol{p}_2 = (12t + 20, -28t - 56, -12t - 27),$$
$$\boldsymbol{q}_2 = (84t + 572, -84t - 1624, -761).$$

Now, take $t \equiv 2 \bmod 28$ and

$$\boldsymbol{r}_2 = \frac{29}{112}\,\boldsymbol{p}_2 + \frac{1}{112}\,\boldsymbol{q}_2 = \Big(\frac{27t + 72}{7}, -8t - 29, -\frac{87t + 386}{28}\Big) \in \mathbb{Z}^3.$$

If $\boldsymbol{p} \in \mathbb{Z}^3$ and $\boldsymbol{p}\boldsymbol{m}_2 = 0$, then $\boldsymbol{p} = u\boldsymbol{p}_2 + v\boldsymbol{r}_2$, where $u, v \in \mathbb{Q}$. We assert that $u, v \in \mathbb{Z}$. Indeed, $\boldsymbol{p} \in \mathbb{Z}^3$ implies

$$(12t + 20)u + \frac{27t + 72}{7}\,v \in \mathbb{Z},$$
$$(28t + 56)u + (8t + 29)v \in \mathbb{Z},$$
$$(12t + 27)u + \frac{87t + 386}{28}\,v \in \mathbb{Z},$$

hence on taking determinants $D_1u, D_2u, D_3u \in \mathbb{Z}$, where

$$D_1 = -12t^2 + 4t + 4, \quad D_2 = -9t^2 - 2, \quad D_3 = -9t^2 - 4t - 11.$$

However,

$$-3D_1 + 7D_2 - 3D_3 = 7$$

and for $t \in \mathbb{Z}$, $7 \nmid D_2$, hence $\gcd(D_1, D_2, D_3) = 1$ and $u \in \mathbb{Z}$. Similarly $v \in \mathbb{Z}$. By Corollary 2 the problem reduces to finding the first two minima of the quadratic form

$$\Big(12u + \frac{27}{7}\,v\Big)^2 + (28u + 8v)^2 + \Big(12u + \frac{87}{28}\,v\Big)^2.$$

By reduction we find that the first minimum m is obtained for $u = 2$, $v = -7$,

$$m = 3^2 + \Big(24 - \frac{87}{4}\Big)^2 = 9 + \frac{81}{16} = 14.0625$$

and the second minimum $\overline{m}$ is obtained for $u = 1$, $v = -3$,

$$\overline{m} = \left(\frac{3}{7}\right)^2 + 4^2 + \left(\frac{75}{28}\right)^2 = 23.358418.$$

Hence

$$m\overline{m} = 328.47775. \qquad \square$$

Lemma 4. *If $\boldsymbol{p}\boldsymbol{m}_3 = \boldsymbol{q}\boldsymbol{m}_3 = 0$, where $\boldsymbol{p}, \boldsymbol{q} \in \mathbb{Z}^3$, $\boldsymbol{p}, \boldsymbol{q}$ linearly independent and $t \equiv 15 \bmod 55$, then for t tending to infinity*

$$|\boldsymbol{p}|\,|\boldsymbol{q}| \geqslant \sqrt{328}t^2 + o(t^2).$$

Proof. One easily verifies that $\boldsymbol{p}_3\boldsymbol{m}_3 = \boldsymbol{q}_3\boldsymbol{m}_3 = 0$, where

$$\boldsymbol{p}_3 = (10t + 25, -15t - 65, -10t - 36),$$
$$\boldsymbol{q}_3 = (165t + 1425, 165t - 3760, -2019).$$

Now, take $t \equiv 15 \bmod 55$ and

$$\boldsymbol{r}_3 = \frac{171}{275}\,\boldsymbol{p}_3 + \frac{1}{275}\,\boldsymbol{q}_3 = \left(\frac{75t + 228}{11}, \frac{-96t - 595}{11}, \frac{-342t - 1635}{55}\right) \in \mathbb{Z}^3.$$

If $\boldsymbol{p}\boldsymbol{m}_3 = 0$ and $\boldsymbol{p} \in \mathbb{Z}^3$ we have

$$\boldsymbol{p} = u\,\boldsymbol{p}_3 + v\boldsymbol{r}_3,$$

where $u, v \in \mathbb{Q}$. We assert that $u, v \in \mathbb{Z}$. Indeed, $\boldsymbol{p} \in \mathbb{Z}^3$ implies

$$(10t + 25)u + \frac{75t + 228}{11}\,v \in \mathbb{Z},$$
$$(15t + 65)u + \frac{96t + 595}{11}\,v \in \mathbb{Z},$$
$$(10t + 36)u + \frac{342t + 1635}{55}\,v \in \mathbb{Z},$$

hence D_1u, D_2u, $D_3u \in \mathbb{Z}$, where

$$D_1 = -15t^2 + 5t + 5,$$
$$D_2 = -6t^2 - 3,$$
$$D_3 = 6t^2 - 5t - 15.$$

However

$$2D_1 - 3D_2 + 2D_3 = -11$$

and for $t \in \mathbb{Z}$, $11 \nmid D_1$, hence $\gcd(D_1, D_2, D_3) = 1$ and $u \in \mathbb{Z}$. Similarly $v \in \mathbb{Z}$. By Lemma 1 the problem reduces to finding the first two minima of the quadratic form

$$\left(10u + \frac{75}{11}\,v\right)^2 + \left(15u + \frac{96}{11}\,v\right)^2 + \left(10u + \frac{342}{55}\,v\right)^2 = A_3u^2 + 2B_3uv + C_3v^2,$$

where

$$A_3 = 425, \quad B_3 = 261.2727, \quad C_3 = 161.3186.$$

By reduction we find the first minimum

$$4A - 12B + 9C = 16.5948,$$

the second minimum

$$9A - 30B + 25C = 19.7834,$$

the product 328.30. □

Proof of Theorem 2. Take an $\epsilon > 0$ and a large integer t such that $t \not\equiv -7 \bmod 17$, $t \equiv 2 \bmod 28$, $t \equiv 15 \bmod 55$ and suppose that

$$\boldsymbol{n} = u\boldsymbol{p} + v\boldsymbol{q},$$
$$\boldsymbol{n} = (15t^2 - t - 4, 3t^2 - 1, 3t^2 - t - 1) \times (69t^2 - 5, 21t^2 - 2, 0),$$

where $\boldsymbol{p}, \boldsymbol{q} \in \mathbb{Z}^3$,

$$|\boldsymbol{p}|\,|\boldsymbol{q}| \leqslant \left(\frac{6}{(722)^{1/4}} - \epsilon\right)\sqrt{|\boldsymbol{n}|}\,.$$

Since

$$|\boldsymbol{n}| = 9\sqrt{722}t^4 + O(t^3),$$

it follows that

$$|\boldsymbol{p} \times \boldsymbol{q}| \leqslant |\boldsymbol{p}|\,|\boldsymbol{q}| \leqslant \left(18 - \frac{\epsilon}{2}\right)t^2, \tag{19}$$

where we may assume without loss of generality that $\boldsymbol{p}, \boldsymbol{q}$ are linearly independent. Therefore $\boldsymbol{p} \times \boldsymbol{q} \neq \boldsymbol{0}$ and since $(\boldsymbol{p} \times \boldsymbol{q})\boldsymbol{n} = 0$ we obtain, by Lemma 1, that $\boldsymbol{p} \times \boldsymbol{q} = \pm\boldsymbol{m}_1, \pm\boldsymbol{m}_2, \pm\boldsymbol{m}_3$. If $\boldsymbol{p} \times \boldsymbol{q} = \pm\boldsymbol{m}_i$, then $\boldsymbol{p}\boldsymbol{m}_i = \boldsymbol{q}\boldsymbol{m}_i = 0$ implies, by Lemma $i + 1$, that $|\boldsymbol{p}|\,|\boldsymbol{q}| \geqslant (18 + o(1))t^2$, contrary to (19). □

Appendix

We give a proof independent of [10] of the part of Proposition 1(i).

Proposition 3. *If $n < m < k$ and $\epsilon > 0$ there exists an m-dimensional subspace S of $\mathbb{Q}^k$ such that for every n-dimensional subspace T of S we have*

$$H(T) > (1 - \epsilon)\gamma_{m,n}^{1/2} H(S)^{n/m}. \tag{20}$$

Notation. For a positive integer n we put $[n] = \{1, \ldots, n\}$, for a vector $\boldsymbol{a}$, a_i is the i-th coordinate of $\boldsymbol{a}$ and for a matrix $A = (a_{ij})$, $A_{I,J} = \det(a_{ij})_{i \in I,\, j \in I}$, $|J|$ is the cardinality of a set J.

Lemma 5. *If $n < m < k$ for every three matrices $U \in \mathbb{R}^{n\times m}$ and $A, B \in \mathbb{R}^{m\times k}$ we have*

$$\left|\det UAA^tU^t - \det UBB^tU^t\right| \leqslant \binom{k}{n}\binom{m}{n} \max|A_{I,J} - B_{I,J}| \max|A_{I,J} + B_{I,J}| \det UU^t,$$

where the maxima are taken over all subsets I, J of $[m]$ and $[k]$, respectively, with $|I| = |J| = n$.

Proof. This follows at once from the identities

$$\det UAA^tU^t = \sum_{J\subset[k],\,|J|=n} \left(\sum_{I\subset[m],\,|I|=n} U_{[n],I}A_{I,J}\right)^2, \tag{21}$$

$$\det UU^t = \sum_{J\subset[m],\,|J|=n} U^2_{[n],J} \tag{22}$$

and from the Cauchy–Schwarz inequality. □

Lemma 6. *If $n \leqslant m$ for every non-singular matrix $A \in \mathbb{R}^{m\times m}$, there exists a positive number $c(A)$ such that for every matrix $U \in \mathbb{R}^{n\times m}$ we have*

$$\det UAA^tU^t \geqslant c(A) \det UU^t.$$

Proof. The right hand side of identity (21) is a quadratic form in $U_{[n],I}$ ($I \subset [m]$, $|I| = n$). We shall show that for $k = m$ it is positive definite. Otherwise there would exist x_I not all equal to 0 such that

$$\sum_{I\subset[m],\,|I|=n} x_I A_{I,J} = 0$$

for all $J \subset [m]$, $|J| = n$. It follows hence that $\det B = 0$ where

$$B = (A_{I,J})_{I,J\subset[m],\,|I|=|J|=n}.$$

However, by the statement 184 on p. 178 of [6], $\det B$ is a power of $\det A$, hence $\det B \neq 0$ and the obtained contradiction shows that the form in question is positive definite.

Now we use the following argument, kindly supplied by M. Skałba, that is simpler than our original one. Reducing a positive definite quadratic form $f \in \mathbb{R}[x_1, \ldots, x_l]$ to a diagonal form by an orthogonal transformation with matrix (c_{ij}) we obtain that

$$f(x_1, \ldots, x_l) = \sum_{j=1}^{l} \lambda_j \left(\sum_{i=1}^{l} c_{ji}x_i\right)^2.$$

Hence

$$f(x_1, \ldots, x_l) \geqslant \lambda_1 \sum_{j=1}^{l}\left(\sum_{i=1}^{l} c_{ji}x_i\right)^2 = \lambda_1 \sum_{i=1}^{l} x_i^2,$$

where λ_1 is the least characteristic root of f. Applying this to our quadratic form and using identity (22) we obtain the lemma. □

Proof of Proposition 3. It is enough to consider $k = m + 1$, $\epsilon < 1$. By the definition of $\gamma_{m,n}$ there exists a full lattice Λ in $\mathbb{R}^m$ such that for every n-dimensional sublattice Γ of Λ we have

$$\det \Gamma \geqslant \gamma_{m,n}(\det \Lambda)^{n/m}.$$

Let $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$ be a basis of Λ and let $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$ in $\mathbb{Q}^m$ be so close to $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$, respectively, that taking

$$A = \begin{pmatrix} \boldsymbol{a}_1 \\ \vdots \\ \boldsymbol{a}_m \end{pmatrix}, \quad B = \begin{pmatrix} \boldsymbol{b}_1 \\ \vdots \\ \boldsymbol{b}_m \end{pmatrix}$$

we have

$$|\det B| < \left(1 + \frac{\epsilon}{2}\right) |\det A| \tag{23}$$

and

$$\max |B_{I,J} - A_{I,J}| \leqslant \min\left\{a, \frac{c(A)\epsilon}{6\binom{m}{n}^2 a}\right\},$$

where $a = \max |A_{I,J}|$ and the maxima are taken over all subsets I, J of $[m]$ with $|I| = |J| = n$.

Let d be a positive integer such that $d\boldsymbol{b}_i \in \mathbb{Z}^m$ $(1 \leqslant i \leqslant m)$ and let us consider the matrix

$$C = C(t, t_1, \ldots, t_{2m}) = \begin{pmatrix} db_{11}t + t_1 & \ldots & db_{1m}t & t_{m+1} \\ \vdots & \ddots & \vdots & \vdots \\ db_{m1}t & \ldots & db_{mm}t + t_m & t_{2m} \end{pmatrix}.$$

We have

$$C_{[m],[m]} \equiv t_1 \cdots t_m \bmod t, \tag{24}$$

hence $C_{[m],[m]} \neq 0$ and also for all $j \leqslant m$

$$C_{[m],[m+1]-\{j\}}(t, t_1, \ldots, t_m, db_{1j}t, \ldots, db_{jj}t + t_j, \ldots, db_{mj}t) = (-1)^{m+j} C_{[m],[m]},$$

hence $C_{[m],[m+1]-\{j\}} \neq 0$. However $C_{[m],[m]}$ is independent of $t_{m+1}, \ldots, t_{2m}$ and $C_{[m],[m+1]-\{j\}}$ is independent of t_j $(1 \leqslant j \leqslant m)$, hence the greatest common divisor D of $C_{[m],[m+1]-\{j\}}$ $(1 \leqslant j \leqslant m+1)$, which is homogeneous in $t, t_1, \ldots, t_{2m}$ could depend only on t and by (24) $D = 1$. Also the $m + 1$ polynomials in question have no common fixed numerical divisor > 1, since by (24)

$$C_{[m],[m]}(0, 1, \ldots, 1) = 1.$$

Hence, by Theorem 1 of [9], there exist integers $t_1^*, \ldots, t_{2m}^*$ and an arithmetic progression

$\mathscr{P} \subset \mathbb{Z}$ such that for $t \in \mathscr{P}$

$$\gcd_{1 \leqslant j \leqslant m+1} C_{[m],[m+1]-\{j\}}(t, t_1^*, \ldots, t_{2m}^*) = 1. \tag{25}$$

Let $\boldsymbol{c}_j$ be the j-th row of $C(t, t_1^*, \ldots, t_{2m}^*)$ and consider the lattice Λ_1 and the linear subspace S of $\mathbb{Q}^m$ spanned by $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_m$. For $t \in \mathscr{P}$ tending to infinity we have by (25)

$$H(S) = \det \Lambda_1 = \sqrt{\sum_{j=1}^{m+1} C_{[m],[m+1]-\{j\}}(t, t_1^*, \ldots, t_{2m}^*)^2} \tag{26}$$

$$= d^m t^m \, |\det B| + O(t^{m-1}).$$

Assume now that $t \in \mathscr{P}$ and T is an n-dimensional subspace of S. Since Λ_1 is primitive, the lattice $T \cap \mathbb{Z}^{m+1}$ is generated by $\sum_{j=1}^{m} u_{ij} \boldsymbol{c}_j$ $(1 \leqslant i \leqslant n)$, where $u_{ij} \in \mathbb{Z}$ and we put $(u_{ij})_{i \leqslant n,\, j \leqslant m} = U$.

Assume, contrary to (20), that

$$H(T) \leqslant (1 - \epsilon) \gamma_{m,n}^{1/2} H(S)^{n/m}.$$

Hence, by (23) and (26) we have for t large enough

$$H(T) \leqslant \left(1 - \frac{\epsilon}{2}\right) \gamma_{m,n}^{1/2} \, |\det A|^{n/m} .$$

However

$$H(T) = \sqrt{\det U C C^t U^t},$$

where

$$C(t) = C(t, t_1^*, \ldots, t_{2m}^*),$$

thus

$$\det U \, \frac{C(t)}{dt} \, \frac{C(t)^t}{dt} \, U^t \leqslant \left(1 - \frac{\epsilon}{2}\right)^2 \gamma_{m,n} \, |\det A|^{2n/m} .$$

Applying Lemma 5 to the matrices U, $C(t)/dt$ and B' equal to B augmented by the $(m+1)$-th column consisting of zeros we obtain

$$\det U B B^t U^t = \det U B' (B')^t U^t \leqslant \left(1 - \frac{\epsilon}{2}\right)^2 \gamma_{m,n} \, |\det A|^{2n/m} + O(t^{-1}) \det U U^t .$$

We now apply Lemma 5 to the matrices U, A and B and obtain

$$\det U A A^t U^t \leqslant \left(1 - \frac{\epsilon}{2}\right)^2 \gamma_{m,n} \, |\det A|^{2n/m} + \left(\frac{\epsilon}{2} \, c(A) + O(t^{-1})\right) \det U U^t . \tag{27}$$

However, by Lemma 6 the left hand side is at least $c(A) \det U U^t$. Hence for t large enough

$$c(A) \det U U^t \leqslant \gamma_{m,n} \, |\det A|^{2n/m}$$

and combining this with (27) we obtain for t large enough

$$\det U A A^t U^t < \gamma_{m,n} \, |\det A|^{2n/m} .$$

It follows that the lattice Γ_1 generated by $\sum_{j=1}^{m} u_{ij}\boldsymbol{a}_j$ $(1 \leqslant j \leqslant n)$ satisfies

$$\det \Gamma_1 < \gamma_{m,n}^{1/2} (\det \Lambda)^{n/m},$$

contrary to the choice of Λ. The obtained contradiction proves (20). □

References

[1] I. Aliev, *On a decomposition of integer vectors* II. Acta Arith. 102 (2002), 373–391.

[2] E. Bombieri, J. D. Vaaler, *On Siegel's Lemma*. Invent. Math. 73 (1983), 11–32; *Addendum*, ibid. 75 (1984), 377.

[3] J. W. S. Cassels, *An Introduction to the Geometry of Numbers*. Springer, Berlin 1959.

[4] S. Chaładus, A. Schinzel, *A decomposition of integer vectors* II. Pliska Stud. Math. Bulgar. 11 (1991), 15–23; this collection: L1, 1249–1258.

[5] S. Chaładus, Yu. Teterin, *Note on a decomposition of integer vectors* II. Acta Arith. 57 (1991), 159–164.

[6] T. Muir, *A Treatise on the Theory of Determinants*. Dover, New York 1960.

[7] R. A. Rankin, *On positive definite quadratic forms*. J. London Math. Soc. 28 (1953), 309–314.

[8] A. Schinzel, *A decomposition of integer vectors* IV. J. Austral. Math. Soc. Ser. A 51 (1991), 33–49; this collection: L2, 1259–1273.

[9] —, *A property of polynomials with an application to Siegel's lemma*. Monatsh. Math. 137 (2002), 239–251; this collection: L3, 1274–1287.

[10] W. M. Schmidt, *The distribution of sublattices of* $\mathbb{Z}^m$. Monatsh. Math. 125 (1998), 37–81.

Part M

Other papers

Commentary on M: Other papers*

by Stanisław Kwapień

M1. Since the publication of the paper, it has become customary to call Gołąb–Schinzel (in the sequel it is abbreviated to G–S) equation the functional equation appearing in the title of the paper. A motivation for considering the equation was an observation made by J. Aczél and S. Gołąb connecting the equation with subgroups of the group $\mathcal{A}$ of affine transformations of $\mathbb{R}^1$ into itself. If we identify an affine transformation T of $\mathbb{R}^1$, given by the formula $T(x) = a + bx$, with the pair $(a, b) \in \mathbb{R}^1 \times (\mathbb{R}^1 \setminus \{0\})$ then the function f fulfils the G–S equation if and only if the part of the graph of f which is $\mathbb{R}^1 \times (\mathbb{R}^1 \setminus \{0\})$ is a subgroup of $\mathcal{A}$. Perhaps more important reason of the popularity of the G–S equation is that it is one of the simplest functional equations which combines conditions like in the Cauchy equation and of iterative type.

In their paper S. Gołąb and A. Schinzel do not pursue connections with the theory of groups and their subgroups. Instead, they give a treatment of the equation as elementary as possible. The main results of the article are:

I. The only differentiable solutions of the equation are the function $f \equiv 0$ and the functions $f_m(x) = 1 + mx$, where m is an arbitrary, fixed real number.

II. The only continuous solutions are the functions as in I and the functions $\max\{f_m, 0\}$, where f_m is as in I.

III. A complete and simple description of trivial solutions of the equation is given (a function f is called trivial iff its values are in the set $\{-1, 0, +1\}$). It is proved that a trivial function is a solution of the equation if and only if it is identically equal to 0, or identically equal to 1, or it is the difference of the indicator functions of an additive subgroup of $\mathbb{R}^1$ and its disjoint translation.

IV. A complete and simple description of nontrivial and non-microperiodic solutions of the equation is found (a function on $\mathbb{R}^1$ is said to be microperiodic if it has arbitrary small periods). It is proved that f is such a solution if and only if $f = f_m I_G(f_m)$, where f_m is as in I and I_G is the indicator function of a set G which is a multiplicative subgroup of $\mathbb{R}^1 \setminus 0$, containing -1.

---

* The paper **M2** is commented in the next article by E. Szemerédi.

The question of a description of measurable solutions of the G–S equation is left open in the paper.

The article started a steady flow of works concerning the equation and its generalizations. In a recent review paper by J. Brzdęk [7], the author lists 82 publications closely related to the G–S equation. For the list and a throughout review of all the subsequent developments to the G–S equation we refer the reader to that paper. Here we will point out only some of them.

A form of a general solution of the G–S equation was given independently by P. Javor [10] and S. Wołodźko [15]. Lemma 1 from **M1** is a basic tool for this goal. We will sketch their result. It is easier to describe the inverse $g = f^{-1}$, which in general is a multifunction, and we will do that. If f is not identically equal to 0, what will be assumed in the sequel, then g is defined on a multiplicative subgroup G of $\mathbb{R} \setminus \{0\}$ (eventually $G \cup \{0\}$ if f admits values equal to 0). The set $A = g(1)$ is an additive subgroup of $\mathbb{R}$ (it is the group of the periods of f). It follows by the G–S equation that A is closed under multiplication by numbers from G, i.e., $rA = A$ for $r \in G$. Moreover Lemma 1 implies that the values of g, restricted to G, are different cosets of A. Therefore the restriction of g to G can be treated as an usual 1–1 function from G into the quotient group $\mathbb{R}/A$. The G–S equation implies that $g(xy) = g(x) + xg(y)$ for $x, y \in G$ (since $rA = A$ for $r \in G$ the multiplication by elements of G is defined on the quotient group $\mathbb{R}/A$). If 0 is a value of f then $g(0) = \mathbb{R} \setminus g(G)$. Conversely, having such a multiplicative subgroup G, an additive subgroup A closed under the multiplication by numbers from G and a 1–1 function $g : G \to \mathbb{R}/A$ which fulfils the above equation then putting $g(0) = \mathbb{R} \setminus g(G)$ if the last set is nonempty we obtain a solution f of the G–S equation such that $g = f^{-1}$. For many groups G, A we see easily that the only functions g with the above properties are of the form $g(x) = xa - a$ for $x \in G$, where a is a fixed element of $\mathbb{R}/A$. For a discussion when it is so we refer the reader to the book of K. S. Brown [5], Ch. 4, Sect. 2, p. 89, or S. Balcerzyk [3], Ch. X, Sect. 4, p. 333. It is true if there exists $y \in G$ such that $1/(y-1)$ is in the ring generated in $\mathbb{R}$ by G. In particular this is satisfied if f is continuous or has the Darboux property.

The above description of solutions allows us to obtain not only the results I–IV, stated above, but also those from many other articles as well. In particular, by the very same method, we obtain a description of continuous functions fulfilling the G–S equation in the case when the function f is defined on a linear topological vector space instead on $\mathbb{R}^1$. The continuous solutions of the G–S equation on a topological vector space are the same as in II, except that mx has to be understood as $m(x)$, where m is a continuous linear functional on the topological vector space. An exposition of this result and those of P. Javor and S. Wołodźko can be found in Chapter XI of the monograph by J. Aczél and J. Dhombres [1].

If we restrict the domain of f to $\mathbb{R}_+$ or $\mathbb{R} \setminus \{0\}$ then we cannot repeat directly the above method to find solutions of such equations. Several papers treat this problem, concentrating on a description of continuous solutions of such equations. They are called the conditional G–S equation or the G–S equation with restricted domains in those papers. In most cases the continuous solutions are similar as in the original G–S equation. An elegant paper of J. Aczél, J. Schwaiger [2] is the most representative for this approach. Another direction of generalizations considered in the papers are the G–S equations of a more general form.

The equations of the form $f(f(y)^k x + f(x)^l y) = \lambda f(x) f(y)$, and more general, were investigated in many papers. Essentially new types of continuous solutions of these generalized G–S equations were found, see e.g. J. Brzdęk [6]. Of special interest is the paper by P. Kahlig, J. Matkowski [12]. In the paper the authors found continuous solutions on $\mathbb{R}^+$ of the equations $f(x + ys(x)^r) = s(x) f(y)$, where $s : \mathbb{R}_+ \to \mathbb{R}_+$ is a fixed monotone function and r is a fixed positive number. It is closely related to the G–S equation and the continuous solutions of the both equations are of the same type. What makes this paper interesting is that the authors present some applications to nonlinear processes of meteorology and fluid mechanics. The differential equations describing evaporation of cloud droplets, water discharging from reservoir, etc., exhibit some symmetries which are expressed by the G–S equation modified in the above way. We end this short review with mentioning recent results on the stability of the G–S equation. A typical result in this direction is that of J. Chudziak [8]. The result says that if for a continuous function f on $\mathbb{R}$ the expression $f[x + yf(x)] - f(x) f(y)$ is bounded on $\mathbb{R} \times \mathbb{R}$ then either f is a bounded function or it is an unbounded solution to the G–S equation ([1]).

M3. The paper treats in an elementary way a special case which can be put in a broad scheme considered in Potential Theory associated with a random walk, resp. with a Markov process. According to the general scheme for a given random walk, resp. Markov process, and a region A we can associate in a natural way a set ∂A—called the Martin boundary of A, and a kernel $H_A : A \times (A \cup \partial A) \to \mathbb{R}^+$, in such a way that nonnegative functions which are superharmonic in A for the potential theory, associated to random walks, resp. Markov process, are precisely those which can be represented as $\sum_{p \in C} H_A(x, p)\mu(p)$, resp. by $\int_C H_A(x, p) d\mu(p)$, where $C = A \cup \partial A$ and μ is a nonnegative function, resp. measure, on C. A subject of numerous papers in the probabilistic potential theory is a study of the behavior of the function $H_A(x, p)$, especially when x approaches ∂A. Harnack's inequalities are estimates, independent of p, from above and below of the ratio $H_A(x, p)/H_A(y, p)$. There are very few random walks (resp. Markov processes) and regions when the kernel H_A can be explicitly computed as it is in the classical potential theory with A being a ball. This makes the problem quite difficult. For this probabilistic point of view we refer the reader to Chapter 3 of the monograph of F. Spitzer [14]. The paper treats simple, symmetric random walk on the plane while A is a disc. Although an explicit formula for the kernel is not given (probably there is no simple one), quite precise bounds on the kernel are proved. The paper is an outgrowth of a problem posed at one of the mathematical olympiads in Poland. It is dedicated to Stefan Straszewicz, one of the founders of The Mathematical Olympiads in Poland and their chairman through the first twenty years of their existence. The author's deep and strong involvement in organizations of these mathematical competitions for youths is very well known and highly appreciated in Poland.

([1]) The author of this commentary would like to thank Janusz Brzdęk for providing his review paper on the G–S equation and for his helpful comments also Jan Krempa for showing him connections of the G–S equation with concepts in Homological Algebra and for references on that.

M4. The very well known Hadamard estimate of the determinant of a matrix $A = (a_{i,j})_{i,j\leqslant n}$ states that

$$|\det A| \leqslant \prod_{i=1}^{n} \|\boldsymbol{a}_i\|_2,$$

where, for $i = 1, \ldots, n$, the vector $\boldsymbol{a}_i = (a_{i,1}, \ldots, a_{i,n})$ is the i-th row of the matrix A and $\|\cdot\|_2$ is the standard Euclidean norm on $\mathbb{R}^n$. The above inequality turns into an equality if all the vectors $\boldsymbol{a}_i$, $i = 1, \ldots, n$, are orthogonal. Hence the Hadamard inequality is in a sense optimal. More exactly, if we want the inequality to hold for all matrices A the Euclidean norm in the inequality can not be replaced by another norm $\|\cdot\|$ with $\|\boldsymbol{a}\| \leqslant \|\boldsymbol{a}\|_2$ for all $\boldsymbol{a} \in \mathbb{R}^n$. We can only hope for a norm which is smaller than the Euclidean norm for some vectors $\boldsymbol{a} \in \mathbb{R}^n$. It is remarkable that such a norm can be found. It is the main result of the present paper that the norm $\|\boldsymbol{a}\| = \max\Big\{\sum_{j:a_j\geqslant 0} a_j - \sum_{j:a_j<0} a_j\Big\} = \max_{I\subset\{1,\ldots,n\}}\Big|\sum_{j\in I} a_j\Big|$ fulfils

$$(*) \qquad |\det A| \leqslant \prod_{i=1}^{n} \|\boldsymbol{a}_i\|,$$

for all real matrices A. Obviously $\|\boldsymbol{a}\| < \|\boldsymbol{a}\|_2$ for some $\boldsymbol{a} \in \mathbb{R}^n$.

An elementary proof of this fact, given in the paper, can be easily explained using "the extreme points technique". Since $\det A$ is an n-linear form in the vectors $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$, to prove the inequality $(*)$ it is enough to check it for $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ being extreme points of the unit ball of the norm $\|\cdot\|$. However, these extreme points are the vectors which fulfil: they have at least one and at most two non-zero coordinates, the absolute value of non-zero coordinates is equal to 1 and the signs of non-zero coordinates alternate. For a matrix A with rows consisting of such extreme points it is very easy to see that $\det A$ is equal to 0, $+1$ or -1 and the norm of each row is equal to 1. Thus $(*)$ holds true. Also, the norm of the extreme points with two non-zero coordinates is equal to 1 while the Euclidean norm is equal to $\sqrt{2}$.

The ideas of the paper were subsequently developed by C. R. Johnson and M. Newman in their paper [11]. In particular they managed to strengthen the inequality $(*)$ to

$$|\det A| \leqslant \prod_{i=1}^{n} \|\boldsymbol{a}_i\| - \prod_{i=1}^{n} \wr\boldsymbol{a}_i\wr,$$

where $\wr\boldsymbol{a}\wr = \min\Big\{\sum_{j:a_j\geqslant 0} a_j - \sum_{j:a_j<0} a_j\Big\}$. Also other n-linear forms, like permanents, are considered in that paper.

That, for some vectors, the Hadamard Inequality can be improved was observed by A. Schinzel in the note at the end of the paper [13]. Then the observation was repeated in the proof of Theorem 2 in his paper with J. Browkin and B. Diviš [4]. The second coauthor of this paper—Bohuslav Diviš, a brilliant young number theorist, died on July 26, 1976, at age of 34. The present paper, an outgrowth from this observation, is dedicated to his memory.

M5. For a polynomial P with coefficients (a_k) comparing $\max_{x\in[-1,1]} |P(x)|$ with $\max_k |a_k|$ is a problem very often met in different branches of mathematics. Universal estimates of the ratio of these two quantities for polynomials in given classes is a subject of many papers. A lot of effort is put in finding best possible estimates in these works. The present paper concerns the case of the class, denoted by $\mathcal{P}(n)$, of polynomials which are squares of polynomials of degree $< n$ with nonnegative coefficients. In this case $\max_{x\in[-1,1]} |P(x)| = \sum_k a_k$ and it is more convenient to consider the ratio multiplied by $1/n$. The goal of the paper is to give as good as possible estimates of $A(n) = \sup\left\{\frac{\frac{1}{n}\sum_k a_k}{\max_k a_k} : P \in \mathcal{P}(n)\right\}$. One of the motivations to consider these quantities comes from the fact that if $J \subset \{0, \dots, n-1\}$ then taking $P = \sum_{k\in J} x^k$ we obtain that at least one integer has at least $A(n)$ times the cardinality of J representations as a sum of two elements from J. We refer the reader to the paper [9] by B. Green, devoted to this and more general problems.

The first step is a reduction of the problem of estimating $A(n)$ to its continuous analogue. Theorem 1 of **M5** states that $B(1 - 6/n^{1/3}) < A(n) \leqslant B$, where $B = \sup_{f\in\mathcal{F}} |f|_1/|f|_\infty$, $\mathcal{F}$ is the class of functions f which are square convolutions, $f = g * g$, of nonnegative, integrable functions g which are equal to zero outside the interval $[0, 1]$ and $|f|_p$ is the L^p norm of the function f. The problem of giving the exact value of B is still open. After the paper had appeared, A. Schinzel found out that the problem of determining $A(n)$ as well as B was posed by Leo Moser in Report of the Institute in the Theory of Numbers, University of Colorado, Boulder, June 21–July 17, 1956, Problems 28, 29. Taking $g(x) = 1/\sqrt{x}$ on $(0, 1]$ and $g(x) = 0$ outside the interval we compute that $|f|_1/|f|_\infty = 4/\pi$. And a conjecture, stated also by L. Moser, is that B is equal to $4/\pi$. It is very easy to see that $B \leqslant 2$. Thus $4/\pi \leqslant B \leqslant 2$. Any result stronger than that requires a new, nontrivial idea.

A simple and ingenious method applied in the proof of Theorem 2 allowed the authors to prove that $B \leqslant 7/4$. In Section 6 of the paper the bound $7/4$ is improved by $1/80$ and in Section 7 it is further lowered by 0.000200513…. So that the final estimate from above of B obtained in the paper is 1.7373…. The proofs of these last two estimates depend on improvements of some details in the proofs of the preceding bounds and the level of complications of the proofs of the consequent ameliorations increases very rapidly.

An estimate for B by $7/4$, and in fact by 1.74998, was obtained by B. Green in the above mentioned paper, as well. His method, based on properties of the Fourier Transform, can be easily explained. Since $|f|_2^2 \leqslant |f|_1|f|_\infty$ for each function f we get $B \leqslant C^2 \leqslant D^2$, where $C = \sup_{f\in\mathcal{F}} |f|_1/|f|_2$ and $D = \sup\{\int_{\mathbb{R}} f\,dx/|f|_2 : f \in \mathcal{G}\}$, where $\mathcal{G}$ is the class of functions f which are square convolutions, $f = g * g$, of integrable function g, which are equal to zero outside the interval $[0, 1]$. Moreover it can be easily checked that

$$D = \frac{1}{\sqrt{2\pi}} \sup\left\{\left(\int_{\mathbb{R}} g(x)dx\right)^2 / |\hat{g}|_4^2 : g \in L_1,\ g(x) = 0 \text{ for } x \notin [0, 1]\right\}$$
$$= \frac{1}{\sqrt{2\pi}} \inf\left\{|\hat{h}|_{4/3}^2 : \hat{h} \in L_{4/3},\ h(x) = 1 \text{ for } x \in [0, 1]\right\}$$

where $\hat{\phi}$ denotes the Fourier Transform of ϕ, i.e. $\hat{\phi}(x) = \frac{1}{\sqrt{2\pi}} \int_{\mathbb{R}} e^{ixy}\phi(y)dy$. From what is written in the paper of B. Green a function h with $h(x) = 1$ on $[0, 1]$ can be constructed such that $|\hat{h}|_{4/3}^4 < 7\pi/2$. This proves that $B < 7/4$. It is not clear how much we can decrease 7/4 with this method. Narrowing the gap between the lower estimate $4/\pi = 1.2732\ldots$ of B and its upper estimate 1.7373 remains an interesting problem.

References

[1] J. Aczél, J. Dhombres, *Functional Equations in Several Variables*. Encyclopedia of Mathematics and its Applications 31, Cambridge Univ. Press, Cambridge 1989.

[2] J. Aczél, J. Schwaiger, *Continuous solutions of the Gołąb–Schinzel equations on the nonnegative reals and related domains*. Österreich. Akad. Wiss. Math.-Natur. Kl. Sitzungsber. II 208 (1999), 171–177.

[3] S. Balcerzyk, *Wstęp do algebry homologicznej* (*Introduction to Homological Algebra*). Biblioteka Matematyczna 34, PWN, Warsaw 1970 (Polish).

[4] J. Browkin, B. Diviš, A. Schinzel, *Addition of sequences in general fields*. Monatsh. Math. 82 (1976), 261–268.

[5] K. S. Brown, *Cohomology of Groups*. Grad. Texts in Math. 87, Springer, New York 1994.

[6] J. Brzdęk, *On the solutions of the functional equation* $f(xf(y)^l + yf(x)^k) = tf(x)f(y)$. Publ. Math. Debrecen 38 (1991), 175–183.

[7] —, *The Gołąb–Schinzel equation and its generalizations*. Aequationes Math. 70 (2005), 14–24.

[8] J. Chudziak, *On a functional inequality related to the stability of the Gołąb–Schinzel equation*. Publ. Math. Debrecen 67 (2005), 199–208.

[9] B. Green, *The number of squares and* $B_h[g]$ *sets*. Acta Arith. 100 (2001), 365–390.

[10] P. Javor, *On the general solution of the functional equation* $f(x + yf(x)) = f(x)f(y)$. Aequationes Math. 1 (1968), 235–238.

[11] C. R. Johnson, M. Newman, *A surprising determinantal inequality for real matrices*. Math. Ann. 247 (1980), 179–185.

[12] P. Kahlig, J. Matkowski, *A modified Gołąb–Schinzel equation on a restricted domain* (*with applications to meteorology and fluid mechanics*). Österreich. Akad. Wiss. Math.-Natur. Kl. Sitzungsber. II 211 (2002), 117–136.

[13] A. Schinzel, *Reducibility of lacunary polynomials* III. Acta Arith. 34 (1978), 227–266; this collection: D7, 409–446.

[14] F. Spitzer, *Principles of random walk*. The University Series in Higher Mathematics, D. Van Nostrand, Princeton 1964.

[15] S. Wołodźko, *Solution générale de l'équation fonctionelle* $f[x+xf(y)] = f(x)f(y)$. Aequationes Math. 2 (1969), 12–29.

The influence of the Davenport–Schinzel paper in discrete and computational geometry

by Endre Szemerédi

The seminal paper of Davenport and Schinzel **M2** addressed a problem of Malanowski concerning independent solutions of a linear differential equation. They started with the observation that if $f_1, f_2, \ldots, f_n$ are everywhere defined real functions $\mathbb{R} \to \mathbb{R}$, any pair of which intersect at most k times, then their *upper envelope* $f(x) = \max\limits_{1 \leqslant i \leqslant n} f_i(x)$ has the following curious combinatorial property. If we consider the maximal connected pieces of the upper envelope that belong to the (graph of the) same function f_i and, proceeding from left to right, write down the indices of the corresponding pieces, then

1. no two consecutive indices are the same,
2. there is no alternating subsequence $\ldots a \ldots b \ldots a \ldots b \ldots$ of length $k+2$, for any $a \neq b$.

Today such a sequence is called an (n, k) *Davenport–Schinzel sequence*. In fact, it is not hard to see that every such sequence can be obtained from a sequence of functions $f_1, f_2, \ldots, f_n$ in the way described above. The classical paper **M2** gives the first nontrivial estimates for the maximum length $\lambda_k(n)$ of a Davenport–Schinzel sequence.

In [7], I managed to establish the upper bound $\lambda_k(n) = O(n \log^* n)$ for any fixed k, where $\log^* n$ denotes the iterated logarithm function, that is, the minimum height of an exponential tower $2^{2^{2^{\cdots}}}$ that exceeds n. In other words, I showed that $\lambda_k(n)$ is nearly linear. However, I was unable to prove a superlinear lower bound. Twelve years later Hart and Sharir [3] essentially settled the combinatorial question raised by Davenport and Schinzel: they showed that for any fixed k, $\dfrac{\lambda_k(n)}{n}$ is an extremely slowly growing function, closely related to the inverse of Ackermann's function. Their proof was inspired by Tarjan's brilliant analysis of the "union-find" algorithm [8].

Davenport–Schinzel sequences were rediscovered by Atallah [1], who recognized the relevance of this concept to a variety of problems in discrete and computational geometry. The simplest example comes from a two-dimensional "visibility" problem, whose relatives play an important role in computer graphics and in motion planning. Suppose we have a collection of segments $s_1, s_2, \ldots, s_n$ in the plane and we want to compute their view from

a far away stand-point. Clearly, this problem is equivalent to computing the upper envelope of n partially defined linear functions. The complexity of any algorithm for solving this problem is at least as large as and, in fact, roughly proportional to the maximum number of pieces along this upper envelope. Of course, the same segment may contribute several pieces to this upper envelope. However, it is not hard to verify that if we list from left to right the indices of the segments s_i as they appear on the upper envelope (in the same way as at the original problem addressed by Davenport and Schinzel), we obtain an $(n, 3)$ Davenport–Schinzel sequence.

In hidden surface removal and in numerous other geometric applications, one has to solve similar problems in three and higher dimensions. Unfortunately, in this case the structure of the upper envelope cannot be combinatorially coded by a single sequence. The first major achievement in this direction was due to Pach and Sharir [4]. They proved, for example, that the upper envelope of n triangles in three-dimensional space consists of at most $O(n\lambda_3(n))$, i.e., only slightly superquadratically many pieces. By the early nineties, Sharir and his coauthors established many far-reaching generalizations of this result to upper envelopes of multivariate functions. These results more or less directly led to efficient algorithms for the solution of a variety of problems in computational geometry, including visibility and "ray shooting" problems, motion planning problems, finding convex hulls, Voronoi diagrams, etc. The general framework of these applications was laid down by Schwartz and Sharir [5]. By analytically reformulating a given problem, we often obtain a number of surface patches in an arbitrarily high dimensional space, which correspond to the equations describing the geometric constraints. Thus, the original problem reduces to the computation of certain substructures (such as the upper envelope, a single cell, or a "zone" of cells) in the *arrangement* of these surface patches. The first rigorous and systematic study of the theory of arrangements was given in Edelsbrunner's monograph [2], which dealt mainly with arrangements of hyperplanes. The combinatorial and algorithmic theory of Davenport–Schinzel sequences, arrangements of more general surfaces, and their geometric and algorithmic applications was the subject of another fundamental monograph by Sharir and Agarwal [6]. It perfectly illustrates how the 1965 paper of Davenport and Schinzel on *A combinatorial problem connected with differential equations* became the starting point of a rich mathematical discipline with diverse applications in computer science.

References

[1] M. Atallah, *Some dynamic computational geometry problems*. Comput. Math. Appl. 11 (1985), 1171–1181.

[2] H. Edelsbrunner, *Algorithms in Combinatorial Geometry*. EATCS Monogr. Theoret. Comput. Sci. 10, Springer, Berlin 1987.

[3] S. Hart, M. Sharir, *Nonlinearity of Davenport–Schinzel sequences and of generalized path compression schemes*. Combinatorica 6 (1986), 151–177.

[4] J. Pach, M. Sharir, *The upper envelope of piecewise linear functions and the boundary of a region enclosed by convex plates: combinatorial analysis*. Discrete Comput. Geom. 4 (1989), 291–309.

[5] J. T. Schwartz, M. Sharir, *Algorithmic motion planning in robotics*. In: Handbook of Computer Science, Vol. A, Algorithms and Complexity, Elsevier, Amsterdam 1990, 391–430.

[6] M. Sharir, P. K. Agarwal, *Davenport–Schinzel sequences and their geometric applications*. Cambridge Univ. Press, Cambridge 1995.

[7] E. Szemerédi, *On a problem of Davenport and Schinzel*. Acta Arith. 25 (1973/74), 213–224.

[8] R. E. Tarjan, *Efficiency of a good but not linear set union algorithm*. J. Assoc. Comput. Mach. 22 (1975), 215–225.

Originally published in
Publicationes Mathematicae Debrecen 6 (1959), 113–125

Sur l'équation fonctionnelle $f[x + y \cdot f(x)] = f(x) \cdot f(y)$

avec S. Gołąb (*Cracovie*)

Dédié à Monsieur Béla Gyires
à propos de son cinquantième anniversaire

Introduction

On peut déterminer de façons diverses les sousgroupes des groupes centroaffines. En effet il faut ici résoudre certains systèmes d'équations fonctionnelles itérées.

L'ensemble des solutions du système des équations fonctionnelles dépend, comme on le sait, des hypothèses concernant la régularité des solutions cherchées. Il peut s'élargir avec l'affaiblissement des hypothèses de la régularité.

Le premier des auteurs a réduit un des problèmes, dont on parle au commencement à l'équation fonctionnelle

$$f[x + y \cdot f(x)] = f(x) \cdot f(y) \tag{1}$$

qui, étant admise la dérivabilité de la solution cherchée $f(x)$, a comme solutions les suivantes

$$f(x) \equiv 0 \qquad \text{ou} \tag{2}$$

$$f(x) = 1 + mx \quad (m = \text{constant quelconque}). \tag{3}$$

À cette occasion s'est imposé la question de la classe des solutions de l'équation (1) dans le domaine des fonctions réelles de la variable réelle ayant des propriétés de régularité plus faibles. Le travail présent — quoiqu'il ne fournit pas la solution complète de cette équation — donne quelques théorèmes dans cette direction. La question de la détermination de toutes les solutions (sans aucune hypothèse de régularité) nous semble difficile. L'équation (1) possède des solutions non mesurables. Nous donnons ici des exemples de pareilles solutions, dûs à MM. W. Sierpiński et S. Marcus.

Nous ne pouvons même pas déterminer toutes les solutions mesurables. Dans le domaine des fonctions continues il existent encore d'autres solutions outre la solution (2) et (3). Parmi les solutions nous distinguons certaine classe de celles-ci que nous nommons triviales. Ce sont les solutions, pour lesquelles les valeurs $f(x)$ sont comprises dans

l'ensemble T, qui se compose des trois nombres

$$0,\ 1,\ -1. \tag{4}$$

Si l'ensemble des valeurs de la fonction $f(x)$ donnant la solution est plus ample que T, alors il doit être infini. Ça résulte de ce que le groupe multiplicatif contenant au moins un élément différent des nombres $+1$ et -1 doit contenir déjà un nombre infini des éléments.

Dans nos considérations les soi-disant *fonctions micropériodiques* jouent un rôle special; ces sont des fonctions périodiques non triviales (non constantes), *possédant des périodes aussi petits qu'on veut* (ne possédant pas de soi-disant période principal). Les fonctions micropériodiques étaient l'objet des recherches des travaux de C. Burstin ([2]) et A. Łomnicki ([4]). En particulier, *une fonction micropériodique et continue à un point est toujors constante*.

1.

Excluons d'abord la solution qui est identique à 0. Nous affirmons, que dans ce cas il doit être

$$f(0) = 1. \tag{5}$$

En effet soit

$$f(x_0) \neq 0. \tag{6}$$

En substituant dans l'équation (1) $y = 0$, $x = x_0$ nous recevrons

$$f(x_0) = f(x_0) \cdot f(0),$$

de là, vu (6), résulte (5).

Supposons d'abord, que la solution $f(x)$ est partout dérivable. Désignons

$$m = f'(0) \tag{7}$$

et différentions (1) par rapport à x.

Nous recevons

$$f'[x + y \cdot f(x)] \cdot [1 + y \cdot f'(x)] = f'(x) \cdot f(y).$$

En substituant $x = 0$ et en tenant compte de (5) et de (7) nous recevons

$$f'(y)(1 + my) = mf(y),$$

d'où, pour $f(y) \neq 0$, nous obtenons

$$\frac{f'(y)}{f(y)} = \frac{m}{1 + my},$$

et ensuite

$$f(y) = C(1 + my),$$

où C désigne une certaine constante, mais, vu (5), on a

$$C = 1$$

et alors

$$f(x) = 1 + mx, \tag{8}$$

si $x \neq -\frac{1}{m}$. Mais, vu l'hypothèse de dérivabilité, la formule (8) doit être valable aussi pour $x = -\frac{1}{m}$ autrement dit la formule (8) est toujours juste. D'autre part on voit facilement que pour chaque valeur constante m la fonction (8) remplit l'équation (1). De cette façon nous avons déterminé toutes les solutions dérivables ([1]). Pour trouver à son tour toutes les solutions continues, nous devons d'abord démontrer certains lemmes.

2.

Lemme 1. *Si pour la solution* $f(x)$ *on a*

$$f(x_1) = f(x_2) \neq 0 \quad où \quad x_2 > x_1 \tag{9}$$

alors le nombre

$$\omega = x_2 - x_1$$

est un période de la fonction $f(x)$.

Démonstration. Supposons (9) et prenons $y = \frac{x - x_1}{f(x_1)}$; nous recevrons

$$\begin{aligned} f(x+\omega) = f(x + x_2 - x_1) &= f\Big[x_2 + \frac{x - x_1}{f(x_1)}\, f(x_1)\Big] \\ &= f[x_2 + y \cdot f(x_1)] = f[x_2 + y \cdot f(x_2)] = f(x_2) \cdot f(y) \\ &= f(x_1) \cdot f(y) = f[x_1 + y \cdot f(x_1)] = f(x) \end{aligned}$$

pour chaque x, ce qui démontre le lemme. □

Lemme 2. *Si la solution* $f(x)$ *de l'équation* (1) *est continue et périodique, alors elle est constante et égale à* 0 *ou à* 1.

([1]) Dans un certain problème de la théorie des objets géométriques M. J. Aczél a obtenu l'équation

$$C(x) \cdot C\Big[\frac{y}{C(x)}\Big] = C(x + y) \tag{1*}$$

qui peut être réduite par un simple changement de la variable à notre équation (1). L'équation (1*) possède parmi les solutions dérivables seulement les solutions

$$C(x) = 1 + mx$$

(on pourrait aussi dans ce but faire une hypothèse plus simple, p. e. que la solution possède au plus un point où elle s'annule) (Cf. [1], pp. 45–47 et [3], pp. 316–317). L'équivalence de l'équation (1*) avec notre équation n'a pas cependant lieu parce que dans nos considérations les solutions qui s'annulent dans un ensemble relativement vaste, jouent un rôle essentiel pendant que les fonctions de telle sorte ne remplient pas en principe l'équation (1*). Ainsi du théorème 1 du présent travail il suit que $C(x) = 1 + mx$ est la plus générale solution continue de (1*).

Démonstration. Soit p la période de $f(x)$. Si nous faisons abstraction de la solution $f(x)=0$, il existent des nombres x_1 et x_2, $x_1 < x_2$, $x_2 - x_1 = p$ tels, que $f(x_1) = f(x_2) \neq 0$. Nous pouvons admettre, que dans l'intérieur de l'intervalle (x_1, x_2) il y a déjà $f(x) \neq f(x_1)$ puisque autrement $f(x)$ serait constante en vertu du lemme 1 et nous n'aurions rien à démontrer.

De là $f(x) - f(x_1)$ a le même signe par exemple positif à l'intérieur (x_1, x_2), et la droite $y = f(x_1) + \varepsilon$ pour $\varepsilon > 0$ suffisamment petit, coupe le diagramme $y = f(x)$ dans les points $x_1 + \eta_1, x_2 - \eta_2$, où $\eta_1, \eta_2 > 0$, $\eta_1, \eta_2 \to 0$ quand $\varepsilon \to 0$ et

$$f(x_1 + \eta_1) = f(x_2 - \eta_2) \neq 0.$$

Les nombres $x_2 - x_1 - (\eta_1 + \eta_2) = p - (\eta_1 + \eta_2)$ en vertu du lemme 1 seront des périodes de la fonction $f(x)$, donc aussi $\eta_1 + \eta_2$ et la fonction f, comme micropério-
c dique et continue, doit être constante $f(x) \equiv c$. Mais en vertu de (1) $c = c^2$. □

Lemme 3. *Si la solution $f(x)$ n'est pas périodique, alors elle doit être invertible dans l'ensemble*

$$A = \{x : f(x) \neq 0\}.$$

C'est la conséquence immédiate du lemme 1.

Lemme 4. *Si la solution $f(x)$ est continue et n'est pas périodique, alors elle doit avoir une des formes suivantes*:

a) *$f(x)$ est négative et strictement croissante dans l'intervalle $(-\infty, x_1)$, $f(x) = 0$ dans l'intervalle $[x_1, x_2]$, $f(x)$ est positive et strictement croissante dans l'intervalle $(x_2, +\infty)$, où*

$$-\infty \leqslant x_1 \leqslant x_2 < 0.$$

b) *$f(x)$ est positive et strictement décroissante dans l'intervalle $(-\infty, x_1)$, $f(x) = 0$ dans l'intervalle $[x_1, x_2]$, $f(x)$ est négative et strictement décroissante dans l'intervalle $(x_2, +\infty)$, où*

$$0 < x_1 \leqslant x_2 \leqslant +\infty.$$

Cela résulte de ce que, $f(x)$ n'est pas constante, $f(0) = 1$, $f(x)$ est continue et invertible dans l'ensemble A.

3.

Lemme 5. *Si la fonction $f(x)$ est continue sur toute la droite et n'est pas constante, alors pour tout $x \in A$, $x \neq 0$, la valeur de $\dfrac{f(x) - 1}{x}$ est constante.*

Démonstration. Supposons que $x \in A$, $y \in A$, $xy \neq 0$ et $\dfrac{f(x) - 1}{x} \neq \dfrac{f(y) - 1}{y}$. Donc $x + y \cdot f(x) \neq y + x \cdot f(y)$, et d'autre part on a

$$f[x + y \cdot f(x)] = f(x) \cdot f(y) = f[y + x \cdot f(y)] \neq 0.$$

Donc, en vertu du lemme 1, la fonction f est périodique, ce qui, vu les hypothèses admises, n'est pas compatible avec le lemme 2. □

Lemme 6. *Les hypothèses du lemme* 5 *étant admises, le cas* $-\infty < x_1 < x_2 < \infty$ *dans le lemme* 4 *ne peut pas avoir lieu.*

Démonstration. Si $-\infty < x_1$ et $x_2 < \infty$ alors en vertu de la continuité de la fonction f aux points x_1 et x_2, nous obtenons du lemme 5

$$\frac{f(x_1) - 1}{x_1} = \frac{f(x_2) - 1}{x_2}$$

d'où, vu que $f(x_1) = f(x_2) = 0$, $x_1 = x_2$.

En outre, dans les intervalles $(-\infty, x_1)$ et (x_2, ∞) la fonction f doit être linéaire. Si $x_1 = x_2$, nous obtenons les solutions obtenues déjà dans le §1. Il nous reste donc seulement le cas, où $x_1 = -\infty < x_2 < 0$ ou bien $0 < x_1 < x_2 = +\infty$. □

Nous obtenons donc le

Théorème 1. *Les seules solutions continues de l'équation* (1) *sauf les solutions* (2) *et* (3) *sont les solutions* :

$$(10)\qquad \begin{cases} \text{a)} \quad f(x) = \begin{cases} 0 & \text{pour } x \leqslant x_2 \ (x_2 < 0) \\ 1 - \dfrac{x}{x_2} & \text{pour } x \geqslant x_2 \end{cases} \\ \text{b)} \quad f(x) = \begin{cases} 1 - \dfrac{x}{x_1} & \text{pour } x \leqslant x_1 \ (x_1 > 0) \\ 0 & \text{pour } x \geqslant x_1 \end{cases} \end{cases}$$

où x_1 *est un nombre positif quelconque,* x_2 *— un nombre négatif quelconque.*

4.

Occupons nous maintenant des solutions *triviales*. Nous appelons ainsi les solutions pour lesquelles les valeurs de $f(x)$ sont comprises dans T (voir Introduction).

Ici appartiennent surtout les deux solutions constantes et des autres, qui sont déjà discontinues.

Nous démontrerons d'abord le

Lemme 7. *Si l'ensemble* F *des valeurs de* $f(x)$*, qui est la solution de l'équation* (1) *n'est pas compris dans* T*, alors l'ensemble* F *est infini.*

Démonstration. Soit $f(x_0) \neq 0, 1, -1$.

En posant

$$\begin{aligned} f(x_0) &= a \\ x_1 &= x_0 f(x_0) + x_0 \\ x_{n+1} &= x_0 f(x_n) + x_n \end{aligned}$$

on prouve aisèment par induction que

$$f(x_n) = a^n \quad (n = 1, 2, \dots).$$

En effet, en substituant dans (1) $x = x_n$, $y = x_0$, nous avons

$$f(x_{n+1}) = f[x_n + x_0 \cdot f(x_n)] = f(x_n) \cdot f(x_0) = a^n \cdot a = a^{n+1}.$$

Comme $a \neq 0, 1, -1$, l'ensemble des valeurs de a^n est infini. □

La lemme 7 justifie l'introduction du terme "solutions triviales".

Supposons, que $f(x)$ est une solution triviale, ne prenant que les valeurs 0 et $+1$.

Une de telles solutions est la suivante :

$$f(0) = 1, \quad f(x) = 0, \quad \text{pour } x \neq 0.$$

S'il existe un $x_0 \neq 0$ tel que $f(x_0) = 1$, alors x_0 est une période de la fonction $f(x)$, car

$$f(y + x_0) = f[x_0 + y \cdot f(x_0)] = f(x_0) \cdot f(y) = f(y).$$

Désignons par Ω l'ensemble de toutes les périodes. Ω forme évidemment un groupe additif. Si $x \notin \Omega$, alors $f(x) = 0$. D'autre part si nous prenons un groupe additif quelconque Ω et posons

$$f(x) = \begin{cases} 1 & \text{quand } x \in \Omega \\ 0 & \text{quand } x \notin \Omega \end{cases} \tag{11}$$

nous obtenons une solution. Le groupe Ω peut se composer des points isolés, ou former un ensemble dense. En particulier, quand Ω se compose de tous les nombres rationnels, nous obtenons une solution discontinue à chaque point. Cette fonction est nommée fonction de Dirichlet.

Voici maintenant un exemple de solution non mesurable L de la forme (11), dû à M. W. Sierpiński.

Soit H une base de Hamel et soit b un élément donné de H. Définissons l'ensemble Ω de façon suivante :

$x \in \Omega$ si dans le développement de x de la forme $x = a_1 b_1 + a_2 b_2 + \dots + a_m b_m$, où $b_1, b_2, \dots, b_m$ sont des éléments de la base H, et $a_1, a_2, \dots, a_m$ sont des nombres rationnels, non nuls, $(b_1, b_2, \dots, b_m)$ ne contient pas l'élément b. De l'unicité des développements considérés, il résulte sans peine, que Ω est un groupe additif, et comme Ω est non mesurable L (voir [5], p. 108), la fonction f est non mesurable.

Examinons maintenant la structure des solutions triviales prenants aussi la valeur -1. Désignons

$$\Omega = \{x : f(x) = 1\}, \quad \Omega^* = \{x : f(x) = -1\}, \quad B = \{x : f(x) = 0\}.$$

L'ensemble Ω forme un groupe (composé éventuellement de 0 ou des éléments isolés) dont l'ensemble Ω^* doit être une translation. D'autre part on démontre facilement que si nous prenons un groupe additif quelconque Ω — different de l'ensemble de tous les

nombres réels, — si nous désignons par Ω^* une translation autre que Ω lui-même et par B l'ensemble $(-\infty, \infty) - (\Omega + \Omega^*)$ et si nous définissons la fonction $f(x)$ par la formule

$$f(x) = \begin{cases} 1 & \text{quand } x \in \Omega \\ -1 & \text{quand } x \in \Omega^* \\ 0 & \text{quand } x \in B \end{cases}$$

nous recevrons une solution de l'équation (1).

Le problème se pose, si l'ensemble B peut être vide. Or, la réponse est négative. Nous démontrerons que si $a \in \Omega^*$ alors $\frac{a}{2} \in B$. En effet, s'il était $\frac{a}{2} \in \Omega$ alors on aurait $\frac{a}{2} + \frac{a}{2} = a \in \Omega$, contre l'hypothèse. S'il était $\frac{a}{2} \in \Omega^*$ alors, vu que $a \in \Omega^*$, on aurait $a - \frac{a}{2} = \frac{a}{2} \in \Omega$, ce qui est impossible. Donc il doit être $\frac{a}{2} \in B$.

A. Łomnicki a démontré dans le travail cité [4] que l'ensemble des périodes d'une fonction mesurable, non constante, est de mesure nulle. Il a démontré aussi que chaque fonction mesurable, micropériodique et non constante, possède une soi-disant valeur privilégiée, c'est-à-dire il existe un nombre p tel que l'ensemble

$$E = \{x : f(x) \neq p\}$$

est de mesure nulle. Or, dans le cas de notre équation, pour chaque solution mesurable, micropériodique et non-constante, ce nombre privilégié p est égal à 0.

Pour le démontrer observons, que l'ensemble des périodes coïncide avec l'ensemble $\Omega = \{x : f(x) = 1\}$, car comme nous avons vu, $f(x_0) = 1$ entraîne $f(y + x_0) \equiv f(y)$ et si p est une période alors $f(p) = f(0) = 1$.

Si le nombre $q \neq 0$ est la valeur de la fonction $f(x)$ alors l'ensemble $Q = \{x : f(x) = q\}$ est une translation de l'ensemble Ω. Car si $f(x) = f(y) = q \neq 0$, alors en vertu du lemme 1, $x - y \in \Omega$. Puisque l'ensemble Ω en vertu du premier des théorèmes de Łomnicki est de mesure nulle, l'ensemble Q est aussi de mesure nulle, par là l'ensemble $E = A$.

5.

Occupons nous maintenant avec les solutions non micropériodiques discontinues.

Lemme 8. *Si $f(x)$ est une solution de l'équation* (1) *et s'ils existent des nombres x_1 et x_2 tels que*:

$$\begin{aligned} &f(x_1) \neq 0,\ 1,\ -1; \quad f(x_2) \neq 0, \\ &[1 - f(x_2)]x_1 \neq x_2[1 - f(x_1)], \end{aligned} \tag{12}$$

alors la fonction $f(x)$ est micropériodique.

Démonstration. Soit $y_1 = f(x_1)$, $y_2 = f(x_2)$,

$$z_0 = 0, \quad z_n = \frac{y_1^n - 1}{y_1 - 1}\, x_1\,;$$

nous affirmons, que

$$f(z_n) = y_1^n, \quad \text{pour} \quad n = 0, \pm 1, \pm 2, \ldots. \tag{13}$$

En effet, pour $n = 0$ et $n = 1$ la formule est vraie ($f(0) = 1$, $f(z_1) = y_1$). Supposons, qu'elle soit vraie pour $n \geqslant 0$ et substitutions à (1) $x = z_n$, $y = x_1$. Nous aurons :

$$f[z_n + x_1 \cdot f(z_n)] = f[z_n + x_1 y_1^n] = f(x_1) \cdot f(z_n) = y_1 \cdot y_1^n = y_1^{n+1}.$$

D'autre part

$$z_n + x_1 \cdot f(z_n) = x_1\Big[\frac{y_1^n - 1}{y_1 - 1} + y_1^n\Big] = x_1 \cdot \frac{y_1^{n+1} - 1}{y_1 - 1} = z_{n+1}.$$

Soit à son tour dans (1) $x = z_n$, $y = z_{-n}$; nous obtenons :

$$f[z_n + z_{-n} \cdot f(z_n)] = f(z_n) \cdot f(z_{-n}),$$

mais

$$z_n + z_{-n} \cdot f(z_n) = \frac{y_1^n - 1}{y_1 - 1} x_1 + \frac{y_1^{-n} - 1}{y_1 - 1} x_1 \cdot y_1^n = \frac{x_1}{y_1 - 1}\left[y_1^n - 1 + 1 - y_1^n\right] = 0.$$

De là nous avons : $f(z_{-n}) = \dfrac{1}{f(z_n)} = y_1^{-n}$ et la formule (13) se trouve démontrée. Posons maintenant dans l'équation (1) $x = z_n$, $y = x_2$, ensuite $x = x_2$, $y = z_n$. Nous aurons alors

$$f(z_n + y_1^n \cdot x_2) = f(z_n) \cdot f(x_2) = y_2 \cdot y_1^n \neq 0$$
$$f(x_2 + z_n y_2) = f(x_2) \cdot f(z_n) = y_2 \cdot y_1^n \neq 0.$$

D'où, en vertu du lemme 1, chacun des nombres

$$\omega_n = x_2 + z_n y_2 - z_n - x_2 y_1^n$$

est la période de la fonction f. Les nombres

$$\begin{aligned}\omega_{n+1} - \omega_n &= y_2(z_{n+1} - z_n) - (z_{n+1} - z_n) - x_2(y_1^{n+1} - y_1^n) \\ &= \frac{y_1^{n+1} - y_1^n}{y_1 - 1}(y_2 - 1)x_1 - x_2 y_1^n(y_1 - 1) = y_1^n\big\{(y_2 - 1)x_1 - x_2(y_1 - 1)\big\}\end{aligned}$$

sont aussi des périodes. Mais d'après l'hypothèse (12) la dernière parenthèse n'est pas nulle, donc $\omega_{n+1} - \omega_n \neq 0$. Quand $|y_1| < 1$, alors $y_1^n \to 0$ pour $n \to \infty$, quand $|y_1| > 1$, alors $y_1^n \to 0$ pour $n \to -\infty$. Il en résulte, que $f(x)$ a des périodes aussi petits qu'on veut, c'est-à-dire $f(x)$ est micropériodique, ce que nous voulions démontrer. □

Observons comme résultat secondaire, que selon que $|y_1| < 1$ ou $|y_1| > 1$ la suite z_n respectivement z_{-n} tend vers

$$\xi = \frac{x_1}{1 - f(x_1)}$$

et alors f tend vers zéro, ainsi, que, l'hypothèse de notre lemme étant admise, zéro est le point d'accumulation des valeurs de la fonction $f(x)$ quel que soit le voisinage du point ξ.

Nous avons dit plus haut, que si la solution $f(x)$ est micropériodique, alors zéro est sa valeur privilégiée. On voit, qu'aussi pour les solutions non micropériodiques zéro est une valeur "privilégiée" dans un certain sens. Le théorème suivant le démontre :

Théorème 2. *Pour que la fonction non micropériodique f soit une solution non triviale de l'équation* (1) *il faut et il suffit qu'il existe un nombre $m \neq 0$ ainsi qu'un groupe G multiplicatif, contenant outre ± 1 encore d'autres nombres et tel que*

$$f(x) = \begin{cases} 1 + mx & \textit{quand } (1 + mx) \in G \\ 0 & \textit{quand } (1 + mx) \notin G. \end{cases} \tag{14}$$

Démonstration. Nécessité. Il existe un x_0 tel, que

$$y_0 = f(x_0) \neq 0, +1, -1.$$

Évidemment $x_0 \neq 0$, puisque $f(0) = 1$. Comme $f(x)$ n'est pas micropériodique, on a en vertu du lemme 8 pour chaque x l'alternative

$$f(x) = 0 \quad \text{ou} \quad x_0[1 - f(x)] = x(1 - y_0).$$

En posant

$$m \overset{\text{def}}{=} \frac{x_0 - 1}{x_0}$$

nous avons $m \neq 0$ et on peut écrire l'alternative nommée ci-dessus dans la forme

$$f(x) = 0 \quad \text{ou} \quad f(x) = 1 + mx.$$

Il faut démontrer, que l'ensemble des y, pour lesquels $f\Big(\frac{y-1}{m}\Big) = y \neq 0$ forme un groupe multiplicatif.

Prenons deux valeurs y_1 et y_2 de l'ensemble

$$G = \Big\{y : f\Big(\frac{y-1}{m}\Big) = y \neq 0\Big\}.$$

Nous avons

$$f\Big(\frac{y_1 - 1}{m}\Big) = y_1, \quad f\Big(\frac{y_2 - 1}{m}\Big) = y_2.$$

S'il y avait

$$f\left(\frac{\frac{y_1}{y_2} - 1}{m}\right) \neq \frac{y_1}{y_2},$$

alors il devrait être

$$f\left(\frac{\frac{y_1}{y_2} - 1}{m}\right) = 0,$$

d'où nous aurions :

$$f\Big(\frac{y_1 - 1}{m}\Big) = f\left(\frac{y_2 - 1}{m} + y_2 \cdot \frac{\frac{y_1}{y_2} - 1}{m}\right) = f\left[\frac{y_2 - 1}{m} + \frac{\frac{y_1}{y_2} - 1}{m} f\Big(\frac{y_2 - 1}{m}\Big)\right]$$
$$= f\Big(\frac{y_2 - 1}{m}\Big)\Big(\frac{\frac{y_1}{y_2} - 1}{m}\Big) = 0$$

et on aboutit à une contradiction. Donc $f\left(\frac{\frac{y_1}{y_2} - 1}{m}\right) = \frac{y_1}{y_2}$ c'est-à-dire si $y_1 \in G$ et $y_2 \in G$ aussi $\frac{y_1}{y_2} \in G$ d'où il résulte que G est un groupe multiplicatif.

Suffisance. Nous vérifions que la fonction $f(x)$ remplit l'équation (1).

Quand $(1 + mx) \notin G$, alors $f(x) = 0$ et

$$f[x + y \cdot f(x)] = f(x) = 0 = f(x) \cdot f(y).$$

Quand $(1 + mx) \in G$ et $(1 + my) \in G$, alors

$$f(x) \cdot f(y) = (1 + mx) \cdot (1 + my)$$
$$1 + m[x + y \cdot f(x)] = 1 + m \cdot x + m \cdot y \cdot (1 + mx) = (1 + mx) \cdot (1 + my) \in G,$$

donc

$$f[x + y \cdot f(x)] = (1 + mx) \cdot (1 + my) = f(x) \cdot f(y).$$

Quand $(1 + mx) \in G$ et $(1 + my) \notin G$, alors $f(y) = 0$, et en même temps

$$1 + m \cdot [x + y \cdot f(x)] = 1 + mx + my \cdot (1 + mx) = (1 + mx) \cdot (1 + my) \notin G$$

d'où

$$f[x + y \cdot f(x)] = 0.$$

Par là nous avons démontré, que $f(x)$ est une solution de (1) et le théorème se trouve démontré. □

Il est à remarquer, que les solutions $f(x)$ en question sont bornées dans chaque intervalle fini. En outre chaque solution est continue au point

$$\overline{x} = -\frac{1}{m}.$$

Pour caractériser les points de discontinuité de la fonction $f(x)$ observons que, quel que soit le groupe G, un des cas suivantes subsiste :

(15) G se compose des nombres a^n ou $\pm a^n$, où a est un nombre réel $\neq 0$, et $n = 0, \pm 1, \pm 2 \ldots$.

(16) G est en même temps dense et frontière sur la demidroite $(0, \infty)$.

(17) G contient toute la demidroite $(0, \infty)$.

Dans le cas (16) la fonction f est discontinue soit sur la demidroite $(\overline{x}, \infty)$ (si $m > 0$), soit sur la demidroite $(-\infty, \overline{x})$ (si $m < 0$).

Dans le cas (17) une fonction f est de la forme $1 + mx$ (si G se compose de tous les nombres réels $\neq 0$) ou bien de la forme (10) (si G se compose de tous les nombres positifs).

Puisque toutes les solutions micropériodiques sont discontinues sur toute la droite, nous pouvons renforcer le théorème 1 de façon suivante :

Théorème 3. *Si la solution non-triviale n'est ni de la forme* (3) *ni de la forme* (10) *elle est soit discontinue sur une demidroite, soit elle est de la forme* (14) *où G remplit* (15).

Quant aux solutions de la forme (14) partout discontinues, S. Marcus a remarqué que nous pouvons obtenir une solution non mesurable de cette forme, prenant comme G le corps non-mesurable des nombres réels, dont l'existence est démontrée dans la note posthume de M. Souslin, rédigée par C. Kuratowski ([6], p. 315).

6.

Le problème se pose si l'équation (1) possède des solutions non triviales micropériodiques. Or nous démontrerons le

Théorème 4. *L'équation* (1) *possède des solutions non triviales micropériodiques.*

Nous allons construire deux groupes : un groupe additif Ω et un groupe multiplicatif G, tels que

1) Ω contient non seulement le nombre zéro, G contient non seulement les nombres 1 et -1,
2) $y \in G,\ \omega \in \Omega \implies y\omega \in \Omega$,
3) $y_1, y_2 \in G,\ (y_1 - y_2) \in \Omega \implies y_1 = y_2$.

Des paires de tels groupes existent.

Il suffit de classer dans Ω tous les nombres de la forme $r\sqrt{2}$, dans G tous les nombres $r \neq 0$, où r est un nombre rationnel quelconque.

Posons

$$f(x) = \begin{cases} y & \text{s'il existe } \omega \in \Omega \text{ tel que } y = 1 + x + \omega \in G \\ 0 & \text{si un tel } \omega \text{ n'existe pas.} \end{cases}$$

La fonction f est bien définie. En effet, supposons qu'il existe $\omega', \omega'' \in \Omega$ et $y', y'' \in G$ tels que $1 + x + \omega' = y'$, $1 + x + \omega'' = y''$; alors $y'' - y' = (\omega'' - \omega') \in \Omega$, d'où $y' = y''$. Ensuite la fonction $f(x)$ est périodique. Prenons en effet un $\omega \in \Omega$ quelconque. Si $f(x) = 0$, alors $f(x + \omega) = 0$ car s'il existait un ω' tel que $1 + (x + \omega) + \omega' \in G$, alors il existerait aussi un $\omega'' = \omega + \omega'$ tel que $1 + x + \omega'' \in G$ en contradiction avec $f(x) = 0$; or si $f(x) \neq 0$, alors $1 + x + \omega \in G$ d'où $1 + x + \omega + 0 \in G$ et alors $f(x + \omega) = 1 + x + \omega = f(x)$.

Le nombre zéro est un point d'accumulation de l'ensemble Ω pour la raison suivante. Puisque le groupe G est non-trivial, 0 est son point d'accumulation. Comme $y\omega \in \Omega$, quand $\omega \in \Omega$ alors $y \in G$, donc il existe des périodes aussi petites que l'on veut, c'est-à-dire f est micropériodique.

Nous démontrerons maintenant, que f satisfait à l'équation (1). En effet, si $f(x) = 0$, alors l'équation (1) est satisfaite d'une façon triviale. Si $f(x) = 1 + x + \omega$, alors nous distinguons deux cas : 1) ou bien $f(y) = 0$, 2) ou $f(y) = 1 + y + \omega_1$.

Dans le premier cas le second membre de l'équation est zéro. Supposons pour le moment, que le premier membre ne soit pas zéro : $f[x+y\cdot f(x)] \neq 0$, donc $1+x+yf(x)+\omega_2 \in G$, c'est-à-dire $1+x+\omega_0+y\cdot f(x)+\omega_2-\omega_0 \in G$, ou $f(x)+y\cdot f(x)+\omega_2-\omega_0 \in G$ ou (comme $f(x) \neq 0$) $1 + y + \dfrac{\omega_2 - \omega_0}{f(x)} \in G$. Mais $f(x) \in G$, $\dfrac{1}{f(x)} \in G$, $\omega_2 - \omega_0 \in G$, donc

$$\omega_1 = \frac{\omega_2 - \omega_0}{f(x)} \in \Omega$$

et comme $1 + y + \omega_1 \in G$, donc $f(y) \neq 0$ et on aboutit à une contradiction. Donc le premier membre de l'équation est aussi égal à zéro.

Dans le second cas on a

$$f(x) = 1 + x + \omega_0 \in G,$$
$$f(y) = 1 + y + \omega_1 \in G,$$

d'où

$$\begin{aligned} x + y \cdot f(x) &= f(x) - 1 - \omega_0 + [f(y) - 1 - \omega_1] \cdot f(x) \\ &= f(x) \cdot f(y) - [\omega_0 + \omega_1 f(x)] - 1, \end{aligned}$$

c'est-à-dire

$$1 + x + y \cdot f(x) = f(x) \cdot f(y) - [\omega_0 + \omega_1 \cdot f(x)].$$

Mais $f(x) \in G$, donc $\omega_1 f(x) \in \Omega$ et $\omega_2 = \omega_0 + \omega_1 \cdot f(x) \in \Omega$. Ensuite $f(x) \cdot f(y) \in G$. Alors on a $1 + x + y \cdot f(x) + \omega_2 \in G$, donc

$$f[x + y \cdot f(x)] = 1 + x + y \cdot f(x) + \omega_2 = f(x) \cdot f(y).$$

Nous avons ainsi démontré que la fonction $f(x)$ est une solution de l'équation (1).

Observons enfin que le théorème 2 nous donne la structure générale de toutes les solutions non triviales et non micropériodiques, mais le théorème 4 nous donne seulement un certain ensemble des solutions non triviales et micropériodiques, n'épuisant pas nécessairement l'ensemble de toutes les solutions de ce type.

Le problème de la forme de toutes les solutions mesurables reste aussi ouvert.

Bibliographie

[1] J. Aczél, *Beiträge zur Theorie der geometrischen Objekte* III–IV. Acta Math. Acad. Sci. Hungar. 8 (1957), 19–52.

[2] C. Burstin, *Über eine spezielle Klasse reeller periodischer Funktionen*. Monatsh. Math. Phys. 26 (1915), 229–262.

[3] M. Hosszú, *Functional equations and algebraic methods in the theory of geometric objects*. Publ. Math. Debrecen 5 (1958), 294–329.

[4] A. Łomnicki, *O wielookresowych funkcjach jednoznacznych zmiennej rzeczywistej*. Sprawozd. Tow. Nauk. Warsz. 11 (1918), 808–846.

[5] W. Sierpiński, *Sur la question de la mesurabilité de la base de M. Hamel*. Fund. Math. 1 (1920), 105–111.

[6] M. Souslin, *Sur un corps non dénombrable de nombres réels*. Fund. Math. 4 (1923), 311–315.

Originally published in
American Journal of Mathematics
LXXXVII (1965), 684–694

A combinatorial problem connected with differential equations

with H. Davenport (*Cambridge*)

1.

Let

$$F(D)f(x) = 0 \tag{1}$$

be a (homogeneous) linear differential equation with constant coefficients, of order d. Suppose that $F(D)$ has real coefficients, and that the roots of $F(\lambda) = 0$ are all real though not necessarily distinct. As is well known, any solution of (1) is of the form

$$f(x) = P_1(x)e^{\lambda_1 x} + \ldots + P_k(x)e^{\lambda_k x}, \tag{2}$$

where $\lambda_1, \ldots, \lambda_k$ are the distinct roots of $F(\lambda) = 0$ and $P_1(x), \ldots, P_k(x)$ are polynomials of degrees at most $m_1 - 1, \ldots, m_k - 1$, where $m_1, \ldots, m_k$ are the multiplicities of the roots, so that $m_1 + \ldots + m_k = d$.

Let

$$f_1(x), \ldots, f_n(x) \tag{3}$$

be n distinct (but not necessarily independent) solutions of (1). For each real number x, apart from a finite number of exceptions, there will be just one of the functions (3) which is greater than all the others. We can therefore dissect the real line into N intervals

$$(-\infty, x_1), (x_1, x_2), \ldots, (x_{N-1}, \infty)$$

such that inside any one of the intervals (x_{j-1}, x_j) a particular one of the functions (3) is the greatest, and such that this function is not the same for two consecutive intervals. It is almost obvious that N is finite, and a formal proof will be given below.

The problem of finding how large N can be, for given d and given n, was proposed to one of us (in a slightly different form) by K. Malanowski. This problem can be made to depend on a purely combinatorial problem, by the following considerations. With each $j = 1, 2, \ldots, N$ there is associated the integer $i = i(j)$ for which $f_i(x)$ is the greatest

of the functions (3) in the interval (x_{j-1}, x_j). (We write $x_0 = -\infty$ and $x_N = \infty$ for convenience.) This defines a sequence of N terms

$$i(1), i(2), \ldots, i(N), \tag{4}$$

each term being one of $1, 2, \ldots, n$. This sequence has no two consecutive terms equal, which we may express by saying that it has no immediate repetition. The sequence has the further property that it contains no subsequence of the form

$$a, b, a, b, \ldots \quad \text{with } d+1 \text{ terms and } a \neq b. \tag{5}$$

For suppose that $j_1 < j_2 < \ldots < j_{d+1}$ and that

$$i(j_1) = a, \quad i(j_2) = b, \quad i(j_3) = a, \quad \ldots.$$

Then the function $f_a(x) - f_b(x)$ is positive in (x_{j_1-1}, x_{j_1}), negative in (x_{j_2-1}, x_{j_2}), and so on. Hence this function has a zero between x_{j_1} and x_{j_2-1}, another zero between x_{j_2} and x_{j_3-1}, and so on, making at least d distinct zeros. But $f_a(x) - f_b(x)$ is itself a function of the type (2), and it is known ([1]) that any such function has at most $d-1$ zeros.

We are therefore led to the following combinatorial problem: *to find the greatest length of a sequence with no immediate repetition, each term of which is one of* $1, 2, \ldots, n$, *and which contains no subsequence of the type* (5). We shall denote this greatest length (that is, greatest number of terms) by $N_d(n)$. Any upper bound obtained for $N_d(n)$ will be valid for the number N defined earlier in relation to the differential equation (1). We do not know whether the two problems are fully equivalent, though this appears to be the case for a few small values of d and n. The combinatorial problem is plainly equivalent to the problem of the maximum number of intervals for n functions which are continuous but not necessarily of the form (2), and which have the property that any two of them are equal for at most $d-1$ values of x.

An obvious upper bound for $N_d(n)$ follows from the consideration that the pairs of integers

$$i(j), \ i(j+1), \quad \text{for } j = 1, 2, \ldots, N-1,$$

can include any given pair i_1, i_2 at most d times. Since the number of pairs i_1, i_2 with

$$1 \leqslant i_1 \leqslant n, \quad 1 \leqslant i_2 \leqslant n, \quad i_1 \neq i_2$$

is $n(n-1)$, it follows that

$$N_d(n) \leqslant dn(n-1) + 1. \tag{6}$$

The problem of evaluating $N_d(n)$ is trivial when $d = 2$, for then there is no subsequence a, b, a, and therefore any integer can occur only once. The longest sequences are simply the permutations of $1, 2, \ldots, n$, and we have

$$N_2(n) = n. \tag{7}$$

The case $d = 3$ is also simple. We prove:

([1]) See, for example, [1], Section V, Problem 75.

Theorem 1. *We have*

$$N_3(n) = 2n - 1, \tag{8}$$

and two examples of maximal sequences are

$$\begin{cases} 1, 2, 3, \ldots, n-1, n, n-1, \ldots, 3, 2, 1; \\ 1, 2, 1, 3, \ldots, 1, n-1, 1, n, 1. \end{cases} \tag{9}$$

For $d > 3$ the problem becomes much more difficult and appears to change its character. We shall concern ourselves mainly with the behaviour of $N_d(n)$ for fixed d and large n. As regards a lower bound for $N_d(n)$, we prove:

Theorem 2. *We have*

$$N_d(n) \geqslant (d^2 - 4d + 3)n - C(d) \quad \text{if } d \text{ is odd and } d > 3, \tag{10}$$

$$N_d(n) \geqslant (d^2 - 5d + 8)n - C(d) \quad \text{if } d \text{ is even and } d > 4, \tag{11}$$

where $C(d)$ depends only on d. Also $N_4(n) \geqslant 5n - C$.

As regards upper bounds, we prove:

Theorem 3. *We have*

$$N_4(n) < 2n(1 + \log n), \tag{12}$$

and, for $d > 4$,

$$N_d(n) < An \exp\bigl(B(\log n)^{1/2}\bigr), \tag{13}$$

where A, B depend only on d and

$$B = B(d) = 10(d \log d)^{1/2}. \tag{14}$$

2. Proof of Theorem 1

We give two proofs, based on different principles. Neither of them appears to be capable of extension to the case $d > 3$. In both proofs, $\mathcal{S}$ denotes a sequence of maximal length satisfying the conditions of the problem, that is, having no immediate repetition and containing no subsequence of the form a, b, a, b. We abbreviate $N_3(n)$ to $N(n)$.

First proof. We can suppose without loss of generality that the first term of $\mathcal{S}$ is 1. We can write $\mathcal{S}$ as

$$1, \mathcal{S}_1, 1, \mathcal{S}_2, \ldots, 1, \mathcal{S}_k, (1),$$

where each $\mathcal{S}_m$ is a sequence formed from the integers $2, 3, \ldots, n$, and where the final 1 may or may not occur. The sequences $\mathcal{S}_m$ are disjoint; for if an integer x occurred in two

of them, there would be a subsequence $1, x, 1, x$ in $\mathcal{S}$. Thus if n_m denotes the number of distinct integers in $\mathcal{S}_m$, we have

$$n_1 + n_2 + \ldots + n_k \leqslant n - 1.$$

Since S_m is a segment of $\mathcal{S}$, it satisfies the conditions of the problem, and therefore the number of terms in $\mathcal{S}_m$ is at most $N(n_m)$. It follows that

$$N(n) \leqslant k + 1 + N(n_1) + \ldots + N(n_k).$$

By induction, starting from $N(1) = 1$, we obtain

$$N(n) \leqslant k + 1 + (2n_1 - 1) + \ldots + (2n_k - 1) \leqslant 2n - 1.$$

The fact that the particular sequences (9) have the desired property is obvious, and this proves (8). □

Second proof. We begin with an observation, made to us by Mrs. Turán, that there is some one of the integers $1, 2, \ldots, n$ which occurs only once in $\mathcal{S}$. For if a is any integer which occurs twice in $\mathcal{S}$, so that

$$i(j_1) = a, \quad i(j_2) = a, \quad j_1 < j_2,$$

there must be some integer b which occurs between, say

$$i(j_3) = b, \quad j_1 < j_3 < j_2.$$

This integer b cannot occur as $i(j)$ for $j < j_1$ or $j > j_2$, for then we should have a subsequence b, a, b, a or a, b, a, b. If b occurs only once we have the result, and if not we can repeat the argument with b instead of a, and this process must terminate.

Now suppose, as we may without loss of generality, that n occurs only once in $\mathcal{S}$. If we delete the term n from $\mathcal{S}$, we obtain a sequence whose terms are formed from $1, 2, \ldots, n-1$ and which has no subsequence of the form a, b, a, b. This sequence may, however, have one immediate repetition, namely if the neighbours of n in $\mathcal{S}$ are equal:

$$\ldots, x, n', n, n', y, \ldots.$$

But this immediate repetition disappears if we delete also one of the two terms n', since $x \neq n'$ and $y \neq n'$. Hence by deleting at most two terms from $\mathcal{S}$ we can obtain an admissible sequence whose terms are formed from $1, 2, \ldots, n - 1$. It follows that

$$N(n) \leqslant N(n - 1) + 2,$$

and this again gives (8). □

3. Proof of Theorem 2

Suppose first that d is odd. Let $\mathcal{A}$ denote the sequence

$$1, 2, \ldots, n,$$

and let $\mathcal{D}$ denote the sequence

$$n-1, n-2, \ldots, 2.$$

Then the

$$\mathcal{A}, \mathcal{D}, \mathcal{A}, \mathcal{D}, \ldots, \mathcal{A}, \mathcal{D}, 1 \tag{15}$$

(which is symmetrical, in spite of its appearance) satisfies the conditions of the problem, provided each $\mathcal{A}$ and $\mathcal{D}$ is taken $(d-1)/2$ times. For if $a < b$, the successive pairs a, b in a subsequence $a, b, a, b, \ldots$ must have their a's in different $\mathcal{A}$'s, assuming (as we may) that we take the last occurrence of each a before the corresponding b. Consequently there cannot be $(d+1)/2$ such pairs. By symmetry the same holds if $a > b$.

The sequence (15) has length $(d-1)(n-1)+1$. If $d > 3$ it can be expanded into a longer sequence, which is still admissible, as follows. We replace each element in $\mathcal{A}$, say the first element 1, by

$$1, x, 1, x, \ldots, 1, x \quad \text{with } d-3 \text{ terms.}$$

Here x is an integer greater than n, and we use the same integer for all the elements of the first $\mathcal{A}$ in (15). We do the same with each $\mathcal{A}$ and $\mathcal{D}$ in (15), but using a different new integer for each of them, and finally we replace the last term 1 in (15) by

$$1, t, 1, t, \ldots, 1, t \quad \text{to } d-3 \text{ terms,}$$

where t is the same new integer as that used to expand the last $\mathcal{D}$. We now have a sequence with $n + (d-1)$ distinct terms, and of length

$$(d-3)\big((d-1)(n-1)+1\big).$$

We shall prove that this sequence satisfies the conditions of the problem, and it will follow that

$$N_d(n+d-1) \geqslant (d-1)(d-3)(n-1) + (d-3),$$

which gives (10).

We have to prove that the expanded sequence contains no subsequence $a, b, a, b, \ldots$ with $d+1$ terms. No further proof is needed if $a \leqslant n$ and $b \leqslant n$, since then the subsequence is a subsequence of (15). The result is obviously true if $a > n$ and $b > n$, that is, if a and b both belong to the set $x, y, \ldots$ of additional integers, for then there is no subsequence of the form x, y, x. Thus we can suppose that either $a \leqslant n$ and $b > n$ or $a > n$ and $b \leqslant n$, and it will be enough to treat the former case. We replace b by y for ease of comparison with the construction.

In any subsequence

$$a, y, a, y, \ldots, a, y, \tag{16}$$

all the occurrences of y must be in the expansion of the same $\mathcal{A}$ or $\mathcal{D}$ in (15), or possibly in that of the final $\mathcal{D}$ and 1. Except for the first y in (16), the a's which precede each y are in that same $\mathcal{A}$ or $\mathcal{D}$. The number of y's is therefore at most $\frac{1}{2}(d-3)+1$. Hence the length of the subsequence (16) is at most $d-1$, and this, when we allow for the possible occurrence of another a after (16), means a total length of at most d. Hence the expanded sequence has the desired property.

Suppose now that d is even. We start from the sequence

$$\mathcal{A}, \mathcal{D}, \mathcal{A}, \mathcal{D}, \ldots, \mathcal{A}, \tag{17}$$

where $\mathcal{A}$ occurs $\frac{1}{2}d$ times and $\mathcal{D}$ occurs $\frac{1}{2}d-1$ times. The longest subsequence $a, b, a, b, \ldots$ in (17) has length d, or indeed only $d-1$ if $a > b$.

We expand (17) by replacing each element a in the first $\mathcal{A}$ by

$$a, x, a, x, \ldots, a, x \quad \text{to } d-2 \text{ terms},$$

where x is an integer greater than n. We apply the same treatment to the last $\mathcal{A}$, using a different integer greater than n. We also expand the intermediate $\mathcal{A}$'s and $\mathcal{D}$'s, but here we replace each element a by

$$a, x, a, x, \ldots, a, x \quad \text{to } d-4 \text{ terms},$$

again using a different integer x for each $\mathcal{A}$ and $\mathcal{D}$. It can be proved, on the same lines as before, that the expanded sequence contains no subsequence $a, b, a, b, \ldots$ of $d+1$ terms.

The number of distinct terms in the expanded sequence is $n+d-1$, and the length is

$$> 2(d-2)n + (d-4)(d-3)(n-2) = (d^2-5d+8)n - 2(d-3)(d-4).$$

Hence

$$N_d(n+d-1) \geqslant (d^2-5d+8)n - 2(d-3)(d-4),$$

and this gives (11). If $d = 4$ we do not expand the intermediate $\mathcal{A}$'s and $\mathcal{D}$'s, and get $N_4(n) \geqslant 5n - C$. □

4.

Proof of (12). Let $\mathcal{S}$ be a sequence of maximal length for $d = 4$, this length being $N_4(n)$. Let $k(a)$ denote the number of times that a occurs in $\mathcal{S}$, for $a = 1, 2, \ldots, n$. Then

$$\sum_{a=1}^{n} k(a) = N_4(n). \tag{18}$$

If we delete a wherever it occurs in $\mathcal{S}$, we obtain a sequence formed from the $n-1$ integers other than a, and this sequence has no subsequence $a, b, a, b, \ldots$ of length greater than 4. But it may have immediate repetitions. To remove these, we must delete not only each occurrence of a but also one of the neighbours of a whenever these two neighbours are equal, as in the second proof of Theorem 1.

We now prove, for any a, that there are at most two occurrences of a, namely the first and the last, which can have equal neighbours. This is immediate, for in the contrary case we should have

$$\ldots, a, \ldots, x, a, x, \ldots, a, \ldots,$$

containing a subsequence a, x, a, x, a of 5 terms.

It follows that by deleting $k(a) + 2$ elements from $\mathcal{S}$ we can obtain an admissible sequence formed from $n - 1$ distinct integers. Hence

$$N_4(n) \leqslant N_4(n-1) + k(a) + 2.$$

Summing for $a = 1, \ldots, n$ and using (18), we obtain

$$nN_4(n) \leqslant nN_4(n-1) + N_4(n) + 2n.$$

This can be written

$$\frac{N_4(n)}{n} - \frac{N_4(n-1)}{n-1} \leqslant \frac{2}{n-1}.$$

Writing down a series of such equations and adding them, and noting that $N_4(2) = 4$, we obtain

$$\frac{N_4(n)}{n} - 2 \leqslant 2\Big(\frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n-1}\Big) < 2\int_1^{n-1} t^{-1}\,dt = 2\log(n-1).$$

This proves (12). □

5.

We now prove (13), and begin with a simple lemma. Throughout this section $\mathcal{S}$ will denote an admissible sequence for d and n, that is, a sequence formed from the integers $1, 2, \ldots, n$, with no immediate repetition, which contains no subsequence $a, b, a, b, \ldots$ of $d+1$ terms. These conditions imposed on $\mathcal{S}$ are unaffected by a permutation of $1, 2, \ldots, n$, and by choosing a suitable permutation, as in the lemma, we can simplify the later exposition.

Lemma. *After a suitable permutation of* $1, 2, \ldots, n$, *the sequence* $\mathcal{S}$ *has the following properties*:

(i) *before any occurrence of any integer* m *in* $\mathcal{S}$ *there occur all integers less than* m;

(ii) $\mathcal{S}$ *contains no subsequence*

(19) $$m, a, b, a, b, \ldots, \quad \text{to } d \text{ terms altogether,}$$

with

(20) $$m \geqslant b > a.$$

Proof. We take the first term of $\mathcal{S}$ to be 1, the second term to be 2, the next term other than 1 and 2 to be 3, and so on, numbering the terms in the order of their first appearance in $\mathcal{S}$. Plainly (i) holds.

Suppose $\mathcal{S}$ has a subsequence of the form (19), where m, a, b satisfy (20). Then before the first term, m, in (19), or possibly coinciding with it, there occurs a term b, since $b \leqslant m$. Before this term b there occurs a term a, since $a < b$. But then there is a subsequence $a, b, a, b, \ldots$ to $d+1$ terms, contrary to hypothesis. This proves the lemma. □

We remark that (ii) implies the original hypothesis that $\mathcal{S}$ contains no subsequence $a, b, a, b, \ldots$ to $d+1$ terms, since such a sequence always contains a sequence of d terms with the first term greater than the second, and this is excluded by (19) with $m = b$.

Proof of (13). For any integer m with $1 < m < n$ we pick out the first occurrence of m in $\mathcal{S}$ and dissect $\mathcal{S}$ into

$$\mathcal{S}', m, \mathcal{S}'', \tag{21}$$

so that every term in $\mathcal{S}'$ is one of $1, 2, \ldots, m-1$.

We write $\mathcal{S}''$ as

$$\mathcal{S}_1{}^{(1)}, a_1, \mathcal{S}_1{}^{(2)}, a_1, \ldots, \mathcal{S}_1{}^{(r_1)}, a_1, \mathcal{S}_2{}^{(1)}, a_2, \ldots, a_k, \mathcal{S}_k{}^{(r_k)}, a_k, \mathcal{T}, \tag{22}$$

where $a_1, \ldots, a_k$ are all the terms not exceeding m that occur in $\mathcal{S}''$, and all the terms of the sequences $\mathcal{S}_i{}^{(j)}$ and $\mathcal{T}$ are integers greater than m. Note that the integers $a_1, \ldots, a_k$ are not necessarily distinct, though $a_i \neq a_{i+1}$ as a consequence of our choice of notation.

The sequence $\mathcal{S}'$ consists of terms each of which is one of $1, 2, \ldots, m-1$, and is an admissible sequence. Hence

$$L(\mathcal{S}') \leqslant N_d(m-1), \tag{23}$$

where $L(\mathcal{S}')$ denotes the length of $\mathcal{S}'$.

The sequence $a_1, a_2, \ldots, a_k$ has each term less than or equal to m and has no immediate repetition. It also contains no subsequence $a, b, a, b, \ldots$ of d terms, for this would necessarily contain a similar subsequence of $d-1$ terms with the first term less than the second, and this, preceded by m, would contradict (ii) of the lemma. Hence

$$k \leqslant N_{d-1}(m). \tag{24}$$

The sequence

$$\mathcal{S}_1{}^{(1)}, \mathcal{S}_1{}^{(2)}, \ldots, \mathcal{S}_1{}^{(r_1)}, \mathcal{S}_2{}^{(1)}, \ldots, \mathcal{S}_2{}^{(r_2)}, \ldots, \mathcal{S}_k{}^{(1)}, \ldots, \mathcal{S}_k{}^{(r_k)}, \mathcal{T}$$

has all its terms greater than m, and is an admissible sequence except for possible immediate repetitions. These occur only when the last term of one of the above sequences is the same as the first term of the next. They can be removed by deleting at most $\sum r_i$ terms at the ends of the sequences. Hence

$$\sum_{i=1}^{k} \sum_{j=1}^{r_i} L(\mathcal{S}_i{}^{(j)}) + L(\mathcal{T}) \leqslant N_d(n-m) + \sum_{i=1}^{k} r_i. \tag{25}$$

It remains to estimate $\sum r_i$. For this we consider only the sequences $\mathcal{S}_i{}^{(j)}$ with $j > 1$. None of them can be empty, since otherwise there would be an immediate repetition of

some a_i in (22). We select from each of these sequences a term $x_i{}^{(j)}$. Among the terms

$$x_i{}^{(2)}, x_i{}^{(3)}, \ldots, x_i{}^{(r_i)}, \tag{26}$$

for given i, the same integer cannot occur more than $\frac{1}{2}d$ times, since otherwise there would be a subsequence

$$x, a_i, x, a_i, \ldots, x, a_i$$

of more than d terms. It follows that the number of distinct integers among (26) is at least $2(r_i - 1)/d$.

Let $\mathfrak{X}_i$ be a subsequence of (26) containing s_i distinct terms, where $s_i \geqslant 2(r_i - 1)/d$. The sequence

$$\mathfrak{X}_1, \mathfrak{X}_2, \ldots, \mathfrak{X}_k \tag{27}$$

is admissible for d, except for possible immediate repetitions. Since the terms of each $\mathfrak{X}_i$ are distinct among themselves, all immediate repetitions can be removed by deleting at most $k - 1$ terms. Since all the terms in (27) are greater than m, and the total number of terms is $\sum s_i$, we have

$$\sum_{i=1}^{k} s_i \leqslant N_d(n - m) + k - 1.$$

It follows that

$$2d^{-1} \sum_{i=1}^{k} (r_i - 1) \leqslant N_d(n - m) + k - 1,$$

whence

$$\sum_{i=1}^{k} r_i < \tfrac{1}{2} d N_d(n - m) + (\tfrac{1}{2}d + 1)k. \tag{28}$$

By (23), (24), (25), (28) we have

$$\begin{aligned} L(\mathcal{S}) &\leqslant L(\mathcal{S}') + 1 + \sum_{i=1}^{k} r_i + \sum_{i=1}^{k} \sum_{j=1}^{r_i} L(\mathcal{S}_i{}^{(j)}) + L(\mathcal{T}) \\ &\leqslant N_d(m - 1) + 1 + \sum_{i=1}^{k} r_i + N_d(n - m) + \sum_{i=1}^{k} r_i \\ &\leqslant N_d(m - 1) + (d + 1)N_d(n - m) + (d + 2)k \\ &\leqslant N_d(m - 1) + (d + 1)N_d(n - m) + (d + 2)N_{d-1}(m). \end{aligned}$$

Taking $\mathcal{S}$ to be a maximal sequence, we obtain the inductive inequality

$$N_d(n) \leqslant N_d(m) + (d + 1)N_d(n - m) + (d + 2)N_{d-1}(m). \tag{29}$$

Suppose that $d \geqslant 5$ and that

$$N_{d-1}(m) < A_1 m \exp(B_1\sqrt{\log m}) \tag{30}$$

for all m, where

$$B_1 = 10\big((d-1)\log(d-1)\big)^{1/2} \tag{31}$$

and A_1 depends only on d. This is a legitimate assumption when $d = 4$, by (12).

Choose A sufficiently large to ensure that the inequality

$$N_d(m) < Am \exp(B\sqrt{\log m}), \tag{32}$$

where

$$B = 10(d \log d)^{1/2}, \tag{33}$$

holds for all $m \leqslant n_0$, where $n_0 = n_0(d)$ will be chosen later (in a manner which does not depend on the choice of A). Suppose also that

$$A > 2(d+2)A_1. \tag{34}$$

Now suppose that $n > n_0$ and that (32) holds for all $m < n$; we have to prove that it holds for $m = n$. Define $C = B - B_1$. Let h be the integer defined by

$$h - 1 < n \exp\big(-C\sqrt{\log n}\big) \leqslant h. \tag{35}$$

We suppose n_0 chosen sufficiently large to ensure that $1 < h < n$. By (29),

$$\begin{aligned} N_d(n) &\leqslant N_d(n-h) + (d+1)N_d(h) + (d+2)N_{d-1}(n-h) \\ &< A(n-h)\exp\big(B\sqrt{\log n}\big) + (d+1)Ah\exp\big(B\sqrt{\log h}\big) \\ &\qquad + (d+2)A_1(n-h)\exp\big(B_1\sqrt{\log n}\big). \end{aligned}$$

This will be less than $An\exp\big(B\sqrt{\log n}\big)$, thus giving the desired conclusion, provided that

$$Ah\exp\big(B\sqrt{\log n}\big) > (d+1)Ah\exp\big(B\sqrt{\log h}\big) + (d+2)A_1 n\exp\big(B_1\sqrt{\log n}\big).$$

Since $n/h \leqslant \exp\big((B-B_1)\sqrt{\log n}\big)$ by (35), it will suffice if

$$A > (d+1)A\exp\big(-B\sqrt{\log n} + B\sqrt{\log h}\big) + (d+2)A_1.$$

By (34), this will hold if

$$1 > 2(d+1)\exp\big(-B\sqrt{\log n} + B\sqrt{\log h}\big).$$

Now, by (35),

$$\sqrt{\log n} - \sqrt{\log h} > \sqrt{\log n} - \sqrt{\log 2n - C\sqrt{\log n}} > \tfrac{1}{3}C,$$

provided n_0 is sufficiently large. Hence it suffices if

$$BC > 3\log 2(d+1).$$

By (31), (33),

$$C = B - B_1 = 10\Big((d\log d)^{1/2} - \big((d-1)\log(d-1)\big)^{1/2}\Big) > 5d^{-1/2}(\log d)^{1/2}.$$

Hence

$$BC > 50\log d,$$

and this amply suffices. This completes the proof of (13). □

Note added in proof. Since the paper was written we have improved on the results of Theorems 2 and 3.

Reference

[1] G. Pólya, G. Szegö, *Aufgaben und Lehrsätze aus der Analysis* II, zweite Auflage. Springer, Berlin 1954.

Andrzej Schinzel
Selecta

Originally published in
Demonstratio Mathematica XI (1978), 47–60

An analogue of Harnack's inequality for discrete superharmonic functions

To Professor Stefan Straszewicz
on his diamond scientific jubilee

Let $f(p)$ be a harmonic function defined on the plane and positive in the disc $D(o, R) = \{p : |p| \leqslant R\}$, where $|p|$ is the Euclidean distance from the origin o. The classical Harnack's inequality (see [2], p. 35, Th. 1.18) asserts that

$$-\frac{2|p|}{R-|p|} f(o) \leqslant f(o) - f(p) \leqslant \frac{2|p|}{R+|p|} f(o).$$

This inequality has been extended to discrete harmonic functions by S. Verblunsky [8] and R. Duffin [1]. They have proved the existence of an absolute constant A ($\leqslant 50$) such that every function $f(p)$ defined on the integral lattice $\mathbb{Z}^2$ satisfying the equation

$$\Delta f(p) = f(p+e_1) + f(p-e_1) + f(p+e_2) + f(p-e_2) - 4f(p) = 0,$$
$$e_1 = (1,0), \quad e_2 = (0,1)$$

and positive in the disc $D(o, R)$ satisfies the inequalities

$$\big|f(e_j) - f(o)\big| \leqslant \frac{A}{R} f(o) \quad (j = 1, 2).$$

An analogue of Harnack's inequality for positive superharmonic functions is easily deduced from the well known convexity properties of subharmonic functions. Indeed, let f be a superharmonic function positive in a disc $D(o, R)$ and let us set for $r \leqslant R$

$$B(r) = \sup_{|p|=r} \big(f(o) - f(p)\big).$$

$f(o) - f(p)$ is a subharmonic function, hence by a well known theorem (see [2], p. 66, Th. 2.13) $B(r)$ is a convex function of $\log r$ in the interval $1 \leqslant r \leqslant R$, i.e.

$$B(r) \leqslant \frac{\log R - \log r}{\log R} B(1) + \frac{\log r}{\log R} B(R).$$

But $\log r \geqslant 0$ and $B(R) \leqslant f(o)$. Thus for $|p| \geqslant 1$

$$f(o) - f(p) \leqslant B(1) + \frac{\log |p|}{\log R} f(o).$$

The main aim of the present paper is to prove an analogue of Harnack's inequality for discrete superharmonic functions, i.e. functions $f(p)$ defined on $\mathbb{Z}^2$ and satisfying the inequality $\Delta f(p) \leqslant 0$. We formulate it as

Theorem 1. *Let $f(p)$ be a function on $\mathbb{Z}^2$ superharmonic and non-negative in the disc $D(o, R)$. Then*

$$|f(p) - f(o)| < \frac{\pi + o(1)}{2 \log R} f(o), \quad \text{if} \quad |p| = 1,\ R \to \infty \tag{1}$$

and

$$-\frac{\log p + O(1)}{\log(R - |p|) - \log p} f(o) < f(o) - f(p) < \frac{\log |p| + O(1)}{\log R} f(o) \tag{2}$$

if $|p| \to \infty$ and $R \gg |p|$ or $R > |p|$ for the left hand side and the right hand side of (2) *respectively.*

It will be clear from Lemma 3 below that the inequalities (1) and (2) are best possible or nearly best possible. It follows from the theorem that all functions superharmonic and positive on $\mathbb{Z}^2$ are constants. This is known and apparently proved for the first time in a more general context by Kemeny and Snell [3].

Instead of the lattice $\mathbb{Z}^2$ one can consider other lattices or more generally networks. From the results on electric currents in networks due to Nash-Williams [6] one obtains the following theorem.

Theorem 2. *Let L be a regular lattice on the plane (triangular, square or hexagonal) with $o \in L$ and the minimal distance 1. If $f(p)$ defined on L satisfies*

$$\sum_{q \in L, |q-p|=1} \big(f(q) - f(p)\big) \leqslant 0 \quad \text{for all } p \in L$$

and $f(p) \geqslant 0$ for $|p| \leqslant R$ then for $|p| = 1$

$$|f(p) - f(o)| \leqslant \frac{2 + o(1)}{\log R}.$$

In particular if $f(p) \geqslant 0$ for all $p \in L$, $f(p)$ is constant.

Theorem 3 related directly to the work of Nash-Williams requires more notation and therefore, its formulation is postponed.

The present paper has originated in a problem proposed at the XXVIII Polish Mathematical Olympiad, which requires a proof of the last statement of Theorem 2 with L replaced by $\mathbb{Z}$. I thank Professor Z. Ciesielski, Dr K. Malanowski, Professor W. M. Schmidt, Dr M. Skwarczyński and Professor E. Wirsing for their valuable suggestions.

Let G be a locally finite graph, i.e. a set of points and lines joining some of these points such that every point is joined to only finitely many others (and none is joined to itself). Let c be a function with positive real values defined on the lines of G. The pair $[G, c]$ is called an *electric network*. For a set V of points of G let $\overline{V} = V \cup \{q \in G : \exists p \in V\ pq \in G\}$. V is called *connected in G* if for any two points $p, q \in V$ there exists a sequence of points $p_i \in V$ such that $p_0 = p$, $p_n = q$ and $p_i p_{i+1} \in G$. We shall call a function $f(p)$ defined on $\overline{V}$ *c-superharmonic* on V if for all $p \in V$

$$\Delta_c f(p) = \sum_{pq \in G} c_{pq}\big(f(q) - f(p)\big) \leqslant 0.$$

It is convenient to denote the set of points of G by $V(G)$, the set of lines by $E(G)$ and put $c_{pq} = 0$ if $pq \notin G$; $\alpha_p = \sum_{q \in G} c_{pq}$.

Lemma 1. *If V is a finite set of points connected in G and a function $h(p)$ is c-superharmonic on V then either $\overline{V} \neq V$ and*

$$\min_{p \in V} h(p) > \min_{p \in \overline{V} \setminus V} h(p)$$

or $h(p)$ is constant on $\overline{V}$.

Moreover, if $h(p) \geqslant 0$ for all $p \in \overline{V}$ then for any two points $p \in V$, $q \in \overline{V}$

$$h(q) \leqslant a(p, q) h(p),$$

where $a(p, q)$ is independent of h.

Proof. Let for any two points p, q, where $p \in V$, $q \in \overline{V}$, $v(p, q)$ be the minimal length n of a sequence of points $p_0, p_1, \ldots, p_{n-1} \in V$ such that

$$p_0 = p, \ p_n = q, \ p_i p_{i+1} \in G. \tag{3}$$

Let further

$$a(p, q) = \min \frac{\alpha_{p_0} \alpha_{p_1} \cdots \alpha_{p_{n-1}}}{c_{p_0 p_1} c_{p_1 p_2} \cdots c_{p_{n-1} p_n}}, \tag{4}$$

where an empty product is 1 and the minimum is taken over all sequences satisfying (3). Finally, let $m = \min_{p \in \overline{V}} h(p)$. We shall show by induction on $v(p, q)$ the following two assertions, which clearly imply the lemma.

A. If $h(p) = m$, then $h(q) = m$.

B. If $h(\overline{V}) \subset [0, \infty]$, then $h(q) \leqslant a(p, q) h(p)$.

If $v(p, q) = 0$ both A and B are obvious. Assume that they are true if $v(p, q) < n$ and let $v(p, q) = n$. Take any sequence p_i satisfying (3). From the inductive assumption applied with $q = p_{n-1}$ we get:

$$\text{if} \quad h(p) = m \quad \text{then} \quad h(p_{n-1}) = m;$$

$$\text{if} \quad h(\overline{V}) \subset [0, \infty] \quad \text{then} \quad h(p_{n-1}) \leqslant a(p, p_{n-1}) h(p). \tag{5}$$

Now, from the inequalities $c > 0$ on $E(G)$ and

$$\Delta_c h(p_{n-1}) = \sum_{r \in \overline{V}} c_{p_{n-1} r} \big(h(r) - h(p_{n-1})\big) \leqslant 0$$

we get

$$\text{if} \quad h(p) = m \quad \text{then} \quad h(q) = m;$$

$$\text{if} \quad h(\overline{V}) \subset [0, \infty] \quad \text{then} \quad h(q) \leqslant \frac{\alpha_{p_{n-1}}}{c_{p_{n-1} q}} h(p_{n-1}). \tag{6}$$

The inductive proof for A is complete, B follows by comparison of (4), (5) and (6). □

Lemma 2. *Let $V \neq \overline{V}$ be a finite set of points connected in G and $o \in V$. A function $f(p)$ c-superharmonic on V and non-negative for all $p \in \overline{V}$ satisfies for all these p the inequality*

$$f(p) \geqslant \frac{g(p, V)}{g(o, V)} f(o), \tag{7}$$

where $g(p, V)$ is the unique function defined on $\overline{V}$ such that

$$g(p, V) = 0 \quad \text{if } p \in \overline{V} \setminus V \tag{8}$$

$$\Delta_c g(p, V) = \begin{cases} -1 & \text{if } p = o \\ 0 & \text{if } p \in V,\ p \neq o. \end{cases} \tag{9}$$

Proof. A function h defined on the set $\overline{V}$ can be regarded as a point in N-dimensional Euclidean space, where N is the cardinality of V. The set S of all functions h satisfying $h(o) = 1$, $h(p) \geqslant 0$ for $p \in \overline{V}$, $\Delta_c h(p) \leqslant 0$ for $p \in V$ is closed. It is also bounded since by Lemma 1 we have

$$h(p) \leqslant a(o, p) h(o).$$

Therefore S is compact and for any $p_0 \in \overline{V}$ the functional $h(p_0)$ assumes in S its minimum m. The set $S_0 = \{h \in S : h(p_0) = m\}$ is again compact hence the functional

$$\sum_{p \in \overline{V}} h(p)$$

assumes in S_0 its minimum. Let $h_0 \in S_0$ be a function for which the minimum is assumed. We assert that it satisfies the conditions

$$h_0(p) = 0 \quad \text{if} \quad p \in \overline{V} \setminus V \tag{10}$$

$$\Delta_c h_0(o) < 0,\ \Delta_c h_0(p) = 0 \quad \text{for} \quad p \in V,\ p \neq o. \tag{11}$$

Indeed, if $h_0(p_1) \neq 0$ for a $p_1 \in \overline{V} \setminus V$, setting

$$h_1(p) = \begin{cases} h_0(p) & \text{for } p \neq p_1 \\ 0 & \text{for } p = p_1 \end{cases}$$

we find that $h_1 \in S$, $h_1(p_0) \leqslant h_0(p_0)$ and

$$\sum_{p \in \overline{V}} h_1(p) < \sum_{p \in \overline{V}} h_0(p), \tag{12}$$

contrary to the definition of h_0.

Secondly if $\Delta_c h_0(p_1) < 0$ for $p_1 \in V$, $p_1 \neq o$, we set

$$h_1(p) = \begin{cases} h_0(p) & \text{for } p \neq p_1 \\ h_0(p_1) + \alpha_{p_1}^{-1} \Delta_c h_0(p_1) = \alpha_{p_1}^{-1} \sum\limits_{q \in G} c_{pq} h_0(q) & \text{for } p = p_1. \end{cases}$$

Again $h_1 \in S$, $h_1(p_0) \leqslant h_0(p_0)$ and (12) holds.

Finally if $\Delta_c h_0(o) = 0$ we infer from Lemma 1 applied to $-h_0(p)$ that

$$\max_{p\in V} h_0(p) \leqslant \max_{p\in\overline{V}\setminus V} h_0(p) = 0$$

contrary to $h_0(o) = 1$.

It follows from (10) and (11) that the function

$$g(p, V) = \frac{h_0(p)}{|\Delta_c h_0(o)|} \tag{13}$$

satisfies the conditions (8) and (9).

If $g'(p)$ is any function satisfying the same conditions we have

$$\begin{aligned} g'(p) - g(p, V) &= 0 \quad \text{if} \quad p \in \overline{V} \setminus V, \\ \Delta_c\big(g'(p) - g(p, V)\big) &= 0 \quad \text{if} \quad p \in V, \end{aligned}$$

hence applying Lemma 1 to $g'(p) - g(p, V)$ and to $g(p, V) - g'(p)$ we get

$$\max_{p\in\overline{V}} \big|g'(p) - g(p, V)\big| \leqslant 0, \quad g'(p) = g(p, V).$$

Thus $g(p, V)$ is unique and taking $p = o$ in (11) we get independently of p_0

$$\big|\Delta_c h_0(o)\big| = \frac{h_0(o)}{g(o, V)} = \frac{1}{g(o, V)}\,. \tag{14}$$

If $f(o) = 0$ the inequality (7) is trivially satisfied. If, on the other hand, $f(o) > 0$ then $f(p)/f(o) \in S$ and for any $p \in V$ we have by (13) and (14)

$$\frac{f(p)}{f(o)} \geqslant h_0(p) = \frac{g(p, V)}{g(o, V)}\,. \qquad \square$$

Remark. Lemma 2 and at least a part of Lemma 1 can be deduced from the Maximum Principle and the Principle of Domination of the transient potential theory for Markov chains (see [4], Corollary 8-44 and Theorem 8-45). The proof obtained in this way would be about twice shorter than one given above but far from self-contained. The existence and uniqueness of $g(p, V)$ has been proved first by Nash-Williams (see [6], Lemma 4 and 9).

Lemma 3. *Let G be the two-dimensional Euclidean lattice graph, $c = 1$ on $E(G)$ and V_R the set of all points of G contained in the disc $D(o, R-1)$. Then for any $p \in V_R \setminus \{o\}$*

$$g(p, V_R) = \frac{1}{2\pi}\left(\log R - \log|p| + O\Big(\frac{1}{R}\Big) + O\Big(\frac{1}{|p|^2}\Big)\right). \tag{15}$$

Moreover

$$g(o, V_R) - g(p, V_R) = \tfrac{1}{4} \quad \textit{if} \quad |p| = 1. \tag{16}$$

Proof. McCrea and Whipple [5] and independently Stöhr [7] found a function $\phi(p)$ on $\mathbb{Z}^2$

with the following properties: $\phi(o) = 0$,

$$\Delta\phi(p) = \begin{cases} 1 & \text{for } p = o \\ 0 & \text{for } p \neq o, \end{cases}$$

$$\phi(p) = \frac{1}{2\pi}\log|p| + \frac{3}{4\pi}\log 2 + \frac{1}{2\pi}C + O\Big(\frac{1}{|p|^2}\Big),$$

where C is Euler's constant (see [7], p. 342, Theorem 1). Let us consider the function

$$h(p) = g(p, V_R) + \phi(p) - \frac{1}{2\pi}\log R - \frac{3}{4\pi}\log 2 - \frac{1}{2\pi}C. \tag{17}$$

For $p \in V_R$ we have $\Delta h(p) = 0$. If $p \in \overline{V}_R \setminus V_R$ we find $R - 1 < |p| \leqslant R$ and

$$|h(p)| = \Big|\phi(p) - \frac{1}{2\pi}\log R - \frac{3}{4\pi}\log 2 - \frac{1}{2\pi}C\Big| = O\Big(\frac{1}{R}\Big). \tag{18}$$

Hence by Lemma 1 applied to $h(p)$ and to $-h(p)$ we have $h(p) = O\Big(\frac{1}{R}\Big)$ for all $p \in \overline{V}_R$. (15) follows now from (17) and (18).

In order to prove (16) let us observe that the graph G and the set V_R are symmetric with respect to the coordinate axes, hence $g(p, V_R)$ must exhibit the same symmetry. Thus $g(p, V_R)$ has the same value for $p = \pm e_1, \pm e_2$ and (16) follows from $\Delta g(o, V_R) = -1$.□

Proof of Theorem 1. Let G be the graph described in Lemma 3, $c = 1$ on $E(G)$. A function $f(p)$ superharmonic and non-negative in $D(o, R)$ is c-superharmonic in V_R, and non-negative in $\overline{V}_R$. If $|p| = 1$ we get from Lemmata 2 and 3

$$f(o) - f(p) \leqslant \frac{g(o, V_R) - g(p, V_R)}{g(o, V_R)} = \frac{\pi + o(1)}{2\log R} f(o).$$

If $|p| \to \infty$ and $R \geqslant |p|$ we have similarly

$$f(o) - f(p) \leqslant \frac{\log|p| + O(1)}{\log R + O(1)} f(o) = \frac{\log|p| + O(1)}{\log R} f(o).$$

In order to estimate $f(o) - f(p)$ from below let us shift the roles of points o and p. Since $D(p, R - |p|) \subset D(o, R)$ we get

$$f(p) - f(o) \leqslant \frac{\pi + o(1)}{2\log(R-1)} f(p) \qquad \text{if } |p| = 1,$$

$$f(p) - f(o) \leqslant \frac{\log|p| + O(1)}{\log(R - |p|)} f(p) \qquad \text{if } |p| \to \infty \text{ and } R - |p| \geqslant |p|.$$

(1) and (2) follow now by simple algebraic transformations. □

In order to prove Theorem 2 we need a lemma due to Nash-Williams [6]. A finite sequence $Y_0, Y_1, \ldots, Y_n$ ($n \geqslant 1$) of disjoint subsets of $V(G)$ is called a *constriction of* G if $Y_0 \cup Y_1 \cup \ldots \cup Y_n = V(G)$ and $p \in Y_j$, $q \in Y_k$, $pq \in G$ implies $|j - k| \leqslant 1$. Using this notion we can state

Lemma 4. *Let V be a finite set of points connected in G, $o \in V$. For any constriction $C = \langle Y_0, Y_1, \ldots, Y_n \rangle$ of G such that $o \in Y_0$, $V(G) \setminus V \subset Y_n$ we have*

$$g(o, V) \geqslant \sum_{k=1}^{n} n_k(C)^{-1},$$

where

$$n_k(C) = \sum_{\substack{p \in Y_{k-1} \\ q \in Y_k}} c_{pq}.$$

Proof. Let $S = \big[G, c, o, V(G) \setminus V\big]$. In the language of [6] $\phi = \dfrac{g(p, V)}{g(o, V)}$ is an S-admissible G-potential and $f_{c\phi}(o) = g(o, V)^{-1}$. The lemma follows now from Lemma 5 of [6]. □

Proof of Theorem 2. Let G be a graph consisting of all points of L and all lines between points of distance 1, let $c = 1$ on $E(G)$. Take for V_R the set of all points of G contained in $D(o, R-1)$. A function satisfying the conditions of the theorem is c-superharmonic on V_R and non-negative on $\overline{V}_R$. Since G and V_R are symmetric with respect to the α_0 lines joining o to the nearest points ($\alpha_0 = 3$, 4 or 6), the function $g(p, V)$ must exhibit the same symmetry. Thus $g(p, V_R)$ takes the same value for all p with $|p| = 1$ and $\Delta_c g(o, V_R) = -1$ implies for these p

$$g(o, V_R) - g(p, V_R) = \alpha_0^{-1}.$$

Hence if $|p| = 1$ we obtain from Lemma 2

$$f(o) - f(p) \leqslant \alpha_0^{-1} g(o, V_R) f(o). \tag{19}$$

c Consider now the following constriction C of G: $Y_k = \{p \in G : d(o, p) = k\}$ $(k < [R])$, $Y_{[R]} = \{p \in G : d(o, p) \geqslant [R]\}$, where $d(o, p)$ is the minimal number n such that for suitable $p_i \in G$: $p_0 = o$, $p_n = p$, $p_i p_{i+1} \in G$.

An easy geometric argument shows that

$$n_k(C) = \begin{cases} 3 & \text{if } \alpha_0 = 3,\ k = 1, \\ 6k - 6 & \text{if } \alpha_0 = 3,\ k > 1, \\ \alpha_0(2k-1) & \text{if } \alpha_0 = 4 \text{ or } 6. \end{cases}$$

Thus in any case $n_k(C) \leqslant \alpha_0(2k-1)$ and

$$\sum_{k=1}^{[R]} n_k(C)^{-1} \geqslant \alpha_0^{-1} \int_1^{[R]+1} \frac{dt}{2t-1} = \frac{\log(2[R]+1)}{2\alpha_0}. \tag{20}$$

It follows from (19), (20) and Lemma 4 that

$$f(o) - f(p) \leqslant \frac{2}{\log(2[R]+1)} f(o). \tag{21}$$

Changing the roles of o and p and observing that $D(p, R-1) \subset D(o, R)$ we obtain

$$f(p) - f(o) \leqslant \frac{2}{\log(2[R]-1)} f(p). \tag{22}$$

The first assertion of Theorem 2 follows from (21), (22) and Lemma 4. Passing with R to infinity we get $f(p) = f(o)$ whenever $d(o, p) = |p| = 1$. By induction on $d(o, p)$ we obtain $f(p) = f(o)$ for all p. □

Our last theorem is a counterpart of Lemma 4.

Theorem 3. *Let V be a finite set of points connected in G, $o \in V$. For any constriction $C = \langle Y_0, Y_1, \dots, Y_n \rangle$ of G such that $Y_0 = \{o\}$, $Y_n = V(G) \setminus V$ we have*

$$g(o, V) \leqslant \sum_{k=1}^{n} m_0(C)^{-1} m_1(C)^{-1} \cdots m_{k-1}(C)^{-1}, \tag{23}$$

where

$$m_0(C) = \alpha_0, \quad m_k(C) = \min_{p \in Y_k} \frac{\sum\limits_{q \in Y_{k+1}} c_{pq}}{\sum\limits_{q \in Y_{k-1}} c_{pq}} \quad (k \geqslant 1),$$

the minimum is taken over fractions with non-zero denominator and if $m_k(C) = 0$, we take $m_k^{-1}(C) = \infty$.

Proof. If any of the numbers $m_k(C)$ $(k < n)$ is zero the bound is trivial.

Therefore, assume that $m_k = m_k(C) > 0$ for $k < n$ and set

$$\varrho_r = 1 - \left(1 + \sum_{s=r}^{n-1} \prod_{k=r}^{s} \frac{1}{m_k}\right)^{-1} \quad (1 \leqslant r \leqslant n).$$

We have $1 > \varrho_r > 0$ $(r < n)$, $\varrho_n = 0$, moreover it is easily verified that for $r < n$

$$m_r(1 - \varrho_{r+1}) = \varrho_r^{-1} - 1. \tag{24}$$

Let us now define for $p \in Y_k$

$$f(p) = \prod_{r=1}^{k} \varrho_r.$$

We have $f(o) = 1$, $\Delta_c f(o) = \alpha_0(\varrho_1 - 1) < 0$ and for $p \in Y_k$ $(n > k > 0)$

$$\frac{\Delta_c f(p)}{f(p)} = a_p(\varrho_k^{-1} - 1) + b_p(\varrho_{k+1} - 1), \tag{25}$$

where

$$a_p = \sum_{q \in Y_{k-1}} c_{pq}, \quad b_p = \sum_{q \in Y_{k+1}} c_{pq}.$$

It follows from (24), (25) and the definition of m_k that for $k < n$

$$\frac{\Delta_c f(p)}{f(p)} = (1 - \varrho_{k+1})(a_p m_k - b_p) \leqslant 0.$$

Thus $f(p)$ is c-superharmonic on V and since it is also non-negative we have by Lemma 2

$$f(o) - f(p) \leqslant \frac{g(o, V) - g(p, V)}{g(o, V)}\,.$$

Multiplying by c_{op} and summing over all p adjacent to o we get

$$-\Delta_c f(o) \leqslant -\Delta_c g(o, V) g(o, V)^{-1} = g(o, V)^{-1},$$

hence

$$g(o, V) \leqslant -\big(\Delta_c f(o)\big)^{-1} = m_0^{-1}(1 - \varrho_1)^{-1}$$
$$= m_0^{-1}\left(1 + \sum_{s=1}^{n-1}\prod_{k=1}^{s} m_k^{-1}\right) = \sum_{s=0}^{n-1}\prod_{k=0}^{s} m_k^{-1}. \qquad \square$$

Furthermore one can show that the equality sign holds in (23) provided $g(p, V)$ is constant on Y_k and deduce from it a formula for $g(o, V)$ analogous to Theorem 1 of [6]. We shall however not pursue the matter.

References

[1] R. J. Duffin, *Discrete potential theory*. Duke Math. J. 20 (1953), 233–251.

[2] W. K. Hayman, P. B. Kennedy, *Subharmonic Functions*, vol. I. Academic Press, London–New York 1976.

[3] J. G. Kemeny, J. L. Snell, *Potentials for denumerable Markov chains*. J. Math. Anal. Appl. 3 (1961), 196–260.

[4] J. G. Kemeny, J. L. Snell, A. W. Knapp, *Denumerable Markov Chains*. Springer, New York 1976.

[5] W. H. McCrea, F. J. W. Whipple, *Random paths in two and three dimensions*. Proc. Roy. Soc. Edinburgh 60 (1940), 281–298.

[6] C. St. J. A. Nash-Williams, *Random walk and electric currents in networks*. Proc. Cambridge Philos. Soc. 55 (1959), 181–194.

[7] A. Stöhr, *Über einige lineare partielle Differenzengleichungen mit konstanten Koeffizienten* III. Math. Nachr. 3 (1950), 330–357.

[8] S. Verblunsky, *Sur les fonctions préharmoniques*. Bull. Sci. Math. (2) 73 (1949), 148–152.

Originally published in
Colloquium Mathematicum XXXVIII (1978), 319–321

An inequality for determinants with real entries

In memory of Bohuslav Diviš

The aim of this note is to prove the following

Theorem. *For every matrix $A = (a_{ij})_{i,j\leqslant n}$ with real entries we have the inequality*

$$|\det A| \leqslant \prod_{i=1}^{n} \max\Bigg(\sum_{\substack{j=1\\ a_{ij}>0}}^{n} a_{ij},\ -\sum_{\substack{j=1\\ a_{ij}<0}}^{n} a_{ij} \Bigg). \tag{1}$$

Proof. First we consider matrices A satisfying the condition

(2) each row of A contains at most one positive and at most one negative element.

Inequality (1) takes then the form

$$|\det A| \leqslant \prod_{i=1}^{n} \max_{j} |a_{ij}|. \tag{3}$$

We prove the latter inequality by induction with respect to n. For $n = 1$ it is obvious. Assume that it is satisfied by all square matrices A satisfying (2) of degree less than n. If for some i_0 and j_0 we have $a_{i_0 j} = 0$ for all $j \neq j_0$, then

$$\det A = \pm a_{i_0 j_0} \det(a_{ij})_{\substack{i\neq i_0\\ j\neq j_0}},$$

and, by the inductive assumption,

$$\left|\det(a_{ij})_{\substack{i\neq i_0\\ j\neq j_0}}\right| \leqslant \prod_{i\neq i_0} \max_{j\neq j_0} |a_{ij}|$$

which implies (3). Therefore, suppose that for every $i \leqslant n$ and for some $k_i < l_i \leqslant n$ we have

$$a_{ik_i} a_{il_i} < 0, \quad a_{ij} = 0 \text{ for } j \neq k_i, l_i.$$

Without loss of generality we may assume that $k_1 = 1, l_1 = 2$, and

$$|a_{11}| \geqslant |a_{12}|. \tag{4}$$

We have

$$\det A = \begin{vmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & a_{22} - \dfrac{a_{21}}{a_{11}}\, a_{12} & a_{23} & \dots & a_{2n} \\ 0 & a_{32} - \dfrac{a_{31}}{a_{11}}\, a_{12} & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n2} - \dfrac{a_{n1}}{a_{11}}\, a_{12} & a_{n3} & \dots & a_{nn} \end{vmatrix} = a_{11} \det B, \tag{5}$$

where

$$B = \begin{pmatrix} a_{22} - \dfrac{a_{21}}{a_{11}}\, a_{12} & a_{23} & \dots & a_{2n} \\ a_{32} - \dfrac{a_{31}}{a_{11}}\, a_{12} & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n2} - \dfrac{a_{n1}}{a_{11}}\, a_{12} & a_{n3} & \dots & a_{nn} \end{pmatrix}.$$

The matrix B satisfies condition (2). Indeed, if $i \geqslant 2$ and $k_i > 1$, then

$$a_{i2} - \frac{a_{i1}}{a_{11}}\, a_{12} = a_{i2} \tag{6}$$

and the $(i-1)$-st row of B contains exactly two non-zero elements, namely the numbers of opposite signs: a_{ik_i} and a_{il_i}. If $k_i = 1$ and $l_i > 2$, then the $(i-1)$-st row of B contains also exactly two non-zero elements of opposite signs, namely $a_{i2} - (a_{i1}/a_{11})a_{12}$ and a_{il_i}. Besides, by (4),

$$\left| a_{i2} - \frac{a_{i1}}{a_{11}}\, a_{12} \right| = \left| \frac{a_{i1}}{a_{11}}\, a_{12} \right| \leqslant |a_{i1}|. \tag{7}$$

Finally, if $k_i = 1$ and $l_i = 2$, then the $(i-1)$-st row of B contains only one non-zero element, namely $a_{i2} - (a_{i1}/a_{11})a_{12}$. Since

$$a_{i2} - \frac{a_{i1}}{a_{11}}\, a_{12} > 0,$$

we have

$$\left| a_{i2} - \frac{a_{i1}}{a_{11}}\, a_{12} \right| < \max\left(|a_{i2}|, \left| \frac{a_{i1}}{a_{11}}\, a_{12} \right| \right) \leqslant \max\big(|a_{i2}|, |a_{i1}| \big). \tag{8}$$

By the inductive assumption, (6), (7), and (8), we have

$$|\det B| \leqslant \prod_{i=2}^{n} \max_j |a_{ij}|, \tag{9}$$

and (3) follows from (5) and (9). Thus (1) is true for all matrices A satisfying (2). In the general case we proceed by induction with respect to the number of non-zero elements of A.

If this number is 0, then $\det A = 0$ and (1) holds. Assume that (1) is true for all square matrices with less than N non-zero elements and consider a square matrix A with exactly N non-zero elements. If A satisfies (2), then (1) holds. If (2) is not fulfilled, then for a certain i_0 there exist j_1 and j_2 such that

$$j_1 \neq j_2, \quad a_{i_0 j_1} a_{i_0 j_2} > 0.$$

Assuming, without loss of generality, that $i_0 = 1$, $j_1 = 1$, and $j_2 = 2$, we have

$$\det A = \frac{a_{11}}{a_{11}+a_{12}} \begin{vmatrix} a_{11}+a_{12} & 0 & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} + \frac{a_{12}}{a_{11}+a_{12}} \begin{vmatrix} 0 & a_{11}+a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}.$$

The inductive assumption applies to the determinants on the right hand side, since the relevant matrices contain only $N-1$ non-zero elements. Hence

$$|\det A| \leqslant \left(\left| \frac{a_{11}}{a_{11}+a_{12}} \right| + \left| \frac{a_{12}}{a_{11}+a_{12}} \right| \right) \prod_{i=1}^{n} \max\left(\sum_{\substack{j=1 \\ a_{ij}>0}}^{n} a_{ij}, -\sum_{\substack{j=1 \\ a_{ij}<0}}^{n} a_{ij} \right)$$
$$= \prod_{i=1}^{n} \max\left(\sum_{\substack{j=1 \\ a_{ij}>0}}^{n} a_{ij}, -\sum_{\substack{j=1 \\ a_{ij}<0}}^{n} a_{ij} \right)$$

and the proof is complete. □

Inequality (9) gives, in general, weaker bounds than Hadamard's inequality does. There are however cases in which the situation is reverse. Such cases are considered in [1] (proof of Theorem 2) and in [2] (Note at the end of the paper).

References

[1] J. Browkin, B. Diviš, A. Schinzel, *Addition of sequences in general fields*. Monatsh. Math. 82 (1976), 261–268.

[2] A. Schinzel, *Reducibility of lacunary polynomials* III. Acta Arith. 34 (1978), 227–266; this collection: D7, 409–446.

Originally published in
Acta Arithmetica 104 (2002), 283–296

Comparison of L^1- and L^∞-norms of squares of polynomials

with W. M. Schmidt (*Boulder*)

1. Introduction

Let $\mathcal{P}(n)$ be the set of polynomials $P(X) = Q(X)^2$ where Q is a non-zero polynomial of degree $< n$ with non-negative real coefficients. We are interested in

$$A(n) = n^{-1} \sup_{P \in \mathcal{P}(n)} |P|_1/|P|_\infty,$$

where $|P|_1$ is the sum, and $|P|_\infty$ the maximum of the coefficients of P. Let $\mathcal{F}$ be the set of functions $f = g * g$ where $*$ denotes convolution and g runs through non-negative, not identically zero, integrable functions with support in $[0, 1]$. Functions in $\mathcal{F}$ have support in $[0, 2]$. We set

$$B = \sup_{f \in \mathcal{F}} |f|_1/|f|_\infty$$

where $|f|_1$ is the L^1-norm and $|f|_\infty$ the sup norm of f.

It is fairly obvious that

$$1 \leqslant A(n) \leqslant 2 - 1/n.$$

Indeed, the left inequality follows on taking

$$P = Q^2 \quad \text{with} \quad Q(X) = 1 + X + \ldots + X^{n-1},$$

the right inequality is obtained by noting that $P \in \mathcal{P}(n)$ has at most $2n - 1$ non-zero coefficients, so that $|P|_1/|P|_\infty \leqslant 2n - 1$. In a similar way one sees that

$$1 \leqslant B \leqslant 2.$$

Theorem 1. *For natural n, l,*

(i) $A(n) \leqslant A(nl)$,
(ii) $A(n) \leqslant B$,
(iii) $A(n) > B(1 - 6n^{-1/3})$.

It follows that

$$B = \lim_{n\to\infty} A(n) = \sup_n A(n).$$

The determination of B appears to be difficult.

Theorem 2. $4/\pi \leqslant B < 1.7373$.

A slightly better upper bound will in fact be proved. We should mention that Ben Green [1] showed in effect that

$$(|f|_1/|f|_2)^2 < 7/4$$

for $f \in \mathcal{F}$, where $|f|_2$ denotes the L^2-norm. In fact he has the slightly better bound 1.74998... Since $|f|_2^2 \leqslant |f|_1|f|_\infty$, this yields $B < 1.74998\ldots$, which is only slightly weaker than the upper bound in Theorem 2. However, Green's result is valid without the assumption $g \geqslant 0$.

On the other hand, Prof. Stanisław Kwapień (private communication) proved that

$$A(n) \geqslant B\big(1 - 3(B/4)^{1/3}n^{-1/3}\big).$$

2. Assertions (i), (ii) of Theorem 1

When R is a polynomial or power series $a_0 + a_1X + \ldots$, set $|R|_\infty$ for the maximum modulus of its coefficients. For such R, and for a polynomial S,

$$|RS|_\infty \leqslant |R|_\infty|S|_1. \tag{2.1}$$

When $P \in \mathcal{P}(n)$, say $P = Q^2$, set

$$\widetilde{Q} = (1 + X + \ldots + X^{l-1})Q(X^l) \quad \text{and} \quad \widetilde{P} = \widetilde{Q}^2.$$

Then $\deg \widetilde{Q} \leqslant l - 1 + l(n-1) = ln - 1$, so that $\widetilde{P} \in \mathcal{P}(ln)$. Further $|\widetilde{Q}|_1 = l|Q|_1$, yielding

$$|\widetilde{P}|_1 = |\widetilde{Q}|_1^2 = l^2|Q|_1^2 = l^2|P|_1. \tag{2.2}$$

For polynomials or series $R = a_0 + a_1X + \ldots$, $S = b_0 + b_1X + \ldots$ with non-negative coefficients, write $R \preceq S$ if $a_i \leqslant b_i$ $(i = 0, 1, \ldots)$. Then

$$Q(X^l)^2 \preceq |Q^2|_\infty(1 + X^l + X^{2l} + \ldots) = |P|_\infty(1 + X^l + X^{2l} + \ldots).$$

Therefore

$$\begin{aligned}\widetilde{P} &= (1 + X + \ldots + X^{l-1})^2 Q(X^l)^2 \\ &\preceq |P|_\infty(1 + X^l + X^{2l} + \ldots)(1 + X + \ldots + X^{l-1})^2 \\ &= |P|_\infty(1 + X + X^2 + \ldots)(1 + X + \ldots + X^{l-1}).\end{aligned}$$

Now (2.1) gives $|\widetilde{P}|_\infty \leqslant |P|_\infty l$. Together with (2.2) this yields $n^{-1}|P|_1/|P|_\infty \leqslant (ln)^{-1}|\widetilde{P}|_1/|\widetilde{P}|_\infty \leqslant A(nl)$. Assertion (i) follows. □

We now turn to (ii). Let $P \in \mathcal{P}(n)$ be given, say $P = Q^2$ with $Q = a_0 + a_1 X + \ldots + a_{n-1} X^{n-1}$. Let g be the function with support in $[0, 1)$ having

$$g(x) = a_i \quad \text{for } i/n \leqslant x < (i+1)/n \quad (i = 0, 1, \ldots, n-1),$$

i.e., for $\lfloor nx \rfloor = i$. Then $|g|_1 = n^{-1}|Q|_1$, so that $f = g * g$ has

$$|f|_1 = n^{-2}|Q^2|_1 = n^{-2}|P|_1. \tag{2.3}$$

Let x be given. The interval $I = [0, 1)$ is the disjoint union of the intervals (possibly empty) $I_{i,j}(x)$ $(i = 0, 1, \ldots, n-1;\ j \in \mathbb{Z})$ consisting of numbers y with

$$\lfloor ny \rfloor = i, \qquad \lfloor n(x-y) \rfloor = j - i.$$

When $y \in I_{i,j}(x)$ and $0 \leqslant i' < n$, then $y + (i' - i)/n \in I_{i',j}(x)$. Therefore $I_{i,j}(x)$ has length independent of i; denote this length by $L_j(x)$. Clearly $L_j(x) = 0$ unless $j = \lfloor nx \rfloor$ or $\lfloor nx - 1 \rfloor$. We have

$$1 = \sum_{i=0}^{n-1} \sum_j L_j(x) = n \sum_j L_j(x). \tag{2.4}$$

For $y \in I_{i,j}(x)$ with $0 \leqslant i < n$,

$$g(y)g(x-y) = \begin{cases} a_i a_{j-i} & \text{when } j - n < i \leqslant j, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore

$$\int_{I_{i,j}(x)} g(y)g(x-y)\,dy = \begin{cases} a_i a_{j-i} & \text{when } j - n < i \leqslant j, \\ 0 & \text{otherwise.} \end{cases} \tag{2.5}$$

Now

$$\sum_{i=0}^{j} a_i a_{j-i} = b_j \leqslant |P|_\infty,$$

where b_j is the coefficient of X^j in P. Taking the sum of (2.5) over $i = 0, 1, \ldots, n-1$ and $j \in \mathbb{Z}$, and observing (2.4), we obtain

$$f(x) = \int g(y)g(x-y)\,dy \leqslant |P|_\infty \sum_j L_j(x) = |P|_\infty / n.$$

Therefore $|f|_\infty \leqslant |P|_\infty / n$, so that in conjunction with (2.3),

$$n^{-1}|P|_1/|P|_\infty \leqslant |f|_1/|f|_\infty \leqslant B.$$

Assertion (ii) follows. □

3. Assertion (iii) of Theorem 1

Pick $f \in \mathcal{F}$ with $|f|_1/|f|_\infty$ close to B. We may suppose that $|f|_\infty = 1$ and $|f|_1$ is close to B, in particular that $|f|_1 \geqslant 1$. Say $f = g * g$. Then for $r < s$,

$$\Big(\int_r^s g(x)\,dx\Big)^2 \leqslant \iint\limits_{2r\leqslant x+y\leqslant 2s} g(x)g(y)\,dx\,dy = \int_{2r}^{2s} dz \int g(y)g(z-y)\,dy = \int_{2r}^{2s} f(z)\,dz \leqslant 2(s-r). \tag{3.1}$$

Setting $G(y) = \int_0^y g(y)\,dy$, so that $G(y) \leqslant \sqrt{2y}$, and using partial integration, we obtain

$$\int_0^\delta (\delta - x)g(x)\,dx = \int_0^\delta G(y)\,dy \leqslant \int_0^\delta (2y)^{1/2}\,dy < \delta^{3/2}. \tag{3.2}$$

Similarly,

$$\int_{1-\delta}^1 \big(\delta - (1-x)\big)g(x)\,dx < \delta^{3/2}.$$

With $c \in \frac{1}{2}\mathbb{Z}$ in $1 \leqslant c \leqslant (n-1)/2$ to be determined later, set

$$a_i = \frac{n}{2c}\int_{(i+1/2-c)/n}^{(i+1/2+c)/n} g(x)\,dx \qquad (0 \leqslant i < n)$$

and

$$Q(X) = \sum_{i=0}^{n-1} a_i X^i.$$

Then

$$|Q|_1 = \sum_{i=0}^{n-1} a_i = \frac{n}{2c}\int_0^1 \nu(x)g(x)\,dx$$

where $\nu(x)$ is the number of integers i, $0 \leqslant i < n$, having $(i + 1/2 - c)/n \leqslant x \leqslant (i + 1/2 + c)/n$. Then $\nu(x)$ is the number of integers i having

$$\max(0, nx - 1/2 - c) \leqslant i \leqslant \min(n-1, nx - 1/2 + c).$$

When $(c+1/2)/n \leqslant x \leqslant 1-(c+1/2)/n$, this becomes the interval $nx - 1/2 - c \leqslant i \leqslant nx - 1/2 + c$, so that $\nu(x) \geqslant 2c$, as $c \in \frac{1}{2}\mathbb{Z}$. When $x < (c+1/2)/n$, the interval becomes $0 \leqslant i \leqslant nx - 1/2 + c$, and $\nu(x) \geqslant nx + c - 1/2 = 2c - (c + 1/2 - nx)$. On the other hand when $x > 1 - (c + 1/2)/n$, then $\nu(x) \geqslant 2c - (c + 1/2 - n(1-x))$. Therefore

$$|Q|_1 \geqslant n\int_0^1 g(x)\,dx - \frac{n}{2c}\int_0^{(c+1/2)/n} (c + 1/2 - nx)g(x)\,dx - \frac{n}{2c}\int_{1-(c+1/2)/n}^1 (c + 1/2 - n(1-x))g(x)\,dx. \tag{3.3}$$

Applying (3.2) with $\delta = (c+1/2)/n$ we obtain

$$\frac{n}{2c}\int_0^{(c+1/2)/n}(c+1/2-nx)g(x)\,dx$$
$$< \frac{n^2}{2c}\big((c+1/2)/n\big)^{3/2} < n((c+1/2)/n)^{1/2}.$$

The same bound applies to the last term on the right hand side of (3.3), so that

$$|Q|_1 \geqslant n|g|_1(1-2((c+1/2)/n)^{1/2}/|g|_1).$$

Here $|g|_1 \geqslant 1$ since $|f|_1 \geqslant 1$.

The polynomial $P = Q^2$ lies in $\mathcal{P}(n)$ and has

$$|P|_1 \geqslant n^2|f|_1\big(1-4((c+1/2)/n)^{1/2}\big). \tag{3.4}$$

The coefficients of P are

$$b_l = \sum_{i+j=l} a_i a_j = \Big(\frac{n}{2c}\Big)^2 \sum_{i+j=l}\int_{(i+1/2-c)/n}^{(i+1/2+c)/n}\int_{(j+1/2-c)/n}^{(j+1/2+c)/n} g(x)g(y)\,dx\,dy.$$

Setting $z = x+y$, so that $(l+1-2c)/n \leqslant z \leqslant (l+1+2c)/n$, we obtain

$$b_l = \Big(\frac{n}{2c}\Big)^2 \int_{(l+1-2c)/n}^{(l+1+2c)/n} dz \int \mu(z,x)g(x)g(z-x)\,dx$$

where $\mu(z,x)$ is the number of integers i in $0 \leqslant i \leqslant n-1$ with $(i+1/2-c)/n \leqslant x \leqslant (i+1/2+c)/n$ and $(l-i+1/2-c)/n \leqslant z-x \leqslant (l-i+1/2+c)/n$. Thus $h = i-nx+1/2$ lies in the range

$$\max(-c, -c+l+1-nz) \leqslant h \leqslant \min(c, c+l+1-nz),$$

and $\mu(z,x) \leqslant \lambda(z)$, which is the length of the "interval" (possibly empty)

$$-c-1/2+\max(0, l+1-nz) \leqslant h \leqslant c+1/2+\min(0, l+1-nz). \tag{3.5}$$

Therefore

$$b_l \leqslant \Big(\frac{n}{2c}\Big)^2 \int dz\,\lambda(z)\int g(x)g(z-x)\,dx$$
$$= \Big(\frac{n}{2c}\Big)^2 \int \lambda(z)f(z)\,dz \leqslant \Big(\frac{n}{2c}\Big)^2 \int \lambda(z)\,dz.$$

But $\int \lambda(z)\,dz$ is the area of the domain in the (h,z)-plane given by (3.5). Here h is contained in an interval of length $2c+1$, and given h, the variable z lies in an interval of length $\leqslant (2c+1)/n$, so that

$$b_l \leqslant \Big(\frac{n}{2c}\Big)^2 \frac{(2c+1)^2}{n} = n\Big(1+\frac{1}{2c}\Big)^2.$$

Therefore $|P|_\infty \leqslant n\big(1 + 1/(2c)\big)^2$, and by (3.4),

$$A(n) \geqslant \frac{1}{n}\,|P|_1/|P|_\infty \geqslant |f|_1\left(1 - 4\left(\left(c + \frac{1}{2}\right) \Big/ n\right)^{1/2}\right) \Big/ \left(1 + \frac{1}{2c}\right)^2.$$

We now pick $c \in \frac{1}{2}\mathbb{Z}$ with $n^{1/3} - 1 \leqslant c < n^{1/3} - 1/2$. When $n \geqslant 8$, which we may clearly suppose in proving assertion (iii), then $1 \leqslant n^{1/3}/2 \leqslant c < (n-1)/2$. Since f may be chosen with $|f|_1$ arbitrarily close to B,

$$A(n) \geqslant B(1 - 4n^{-1/3})/(1 + n^{-1/3})^2 > B(1 - 6n^{-1/3}). \qquad \square$$

4. The lower bound in Theorem 2

Set $f = g * g$ where $g(x) = x^{-1/2}$ in $0 < x < 1$, and $g(x) = 0$ otherwise. Then $f \in \mathcal{F}$, and $|f|_1 = |g|_1^2 = 4$. For $0 < z \leqslant 2$,

$$f(z) = \int (z - x)^{-1/2} x^{-1/2}\, dx,$$

with the range of integration $\max(0, z-1) \leqslant x \leqslant \min(1, z)$. Setting $x = y^2 z$ we obtain

$$f(z) = 2\int \frac{dy}{(1 - y^2)^{1/2}},$$

the integration being over $y \geqslant 0$ with $1 - 1/z \leqslant y^2 \leqslant \min(1/z, 1)$. When $0 < z \leqslant 1$, this range is $0 \leqslant y \leqslant 1$, so that $f(z) = \pi$, whereas in $1 < z \leqslant 2$ the range is smaller, and $f(z) < \pi$. We may conclude that $|f|_\infty = \pi$, and $B \geqslant |f|_1/|f|_\infty = 4/\pi$. $\square$

5. The upper bound $B \leqslant 7/4$

The upper bound of Theorem 2 will be established in three stages. Here we will show that $B \leqslant 7/4 = 1.75$, and in the following stages we will prove that $B \leqslant 7/4 - 1/80 = 1.7375$, then that $B \leqslant 1.7373$.

Our problem is invariant under translations. To exhibit symmetry, we therefore redefine $\mathcal{F}$ to consist of functions $f = g * g$ with g non-zero, non-negative and integrable, with support in $[-1/2, 1/2]$, so that f has support in $[-1, 1]$. We will suppose throughout that $f \in \mathcal{F}$ with $|f|_\infty = 1$, and we will give upper bounds for $|f|_1$.

Lemma 1.

$$\int_{1/2}^{1} f(z) f(-z)\, dz \leqslant 1/4.$$

As a consequence of this lemma,

$$|f|_1 = \int_{-1}^{1} f(z)\,dz = \int_0^1 \big(f(z)+f(-z)\big)\,dz \leqslant 1 + \int_{1/2}^1 \big(f(z)+f(-z)\big)\,dz$$
$$\leqslant 1 + \int_{1/2}^1 \big(1+f(z)f(-z)\big)\,dz \leqslant \frac{3}{2}+\frac{1}{4} = \frac{7}{4},$$

so that indeed $B \leqslant 7/4$.

Proof of Lemma 1.

$$f(z) = (g*g)(z) = \int g(x)g(z-x)\,dx = 2 \int\limits_{\substack{x+y=z\\ x\leqslant y}} g(x)g(y)\,dx. \tag{5.1}$$

(It is to exhibit symmetry that we write y for $z-x$.) Similarly

$$f(-z) = 2 \int\limits_{\substack{u+v=-z\\ u\leqslant v}} g(u)g(v)\,du. \tag{5.2}$$

Here x, y, u, v may be restricted to lie in $[-1/2, 1/2]$. When $\delta \geqslant 0$ and $z \geqslant 1/2-\delta$, then $x = z-y \geqslant 1/2-\delta-1/2 = -\delta$, also $v = -u-z \leqslant 1/2-1/2+\delta = \delta$, so that

$$u \leqslant v \leqslant \delta, \qquad -\delta \leqslant x \leqslant y.$$

We obtain

$$\int_{1/2-\delta}^1 f(z)f(-z)\,dz \leqslant 4\int_{1/2-\delta}^1 dz \iint\limits_{\substack{u\leqslant v\leqslant\delta\\ -\delta\leqslant x\leqslant y\\ x+y=z\\ u+v=-z}} g(x)g(y)g(u)g(v)\,dx\,du.$$

In this integral $u \leqslant -z/2 \leqslant -1/4+\delta/2$, and $y \geqslant z/2 \geqslant 1/4-\delta/2$. Setting $w = u+y = -x-v$ we have $w \leqslant u+1/2 \leqslant 1/4+\delta/2$, and in fact $|w| \leqslant 1/4+\delta/2$. Replacing the variables x, u, z in the above integral by x, $y = z-x$, $w = u+z-x$, we obtain the bound

$$4\int_{-1/4-\delta/2}^{1/4+\delta/2} dw \iint\limits_{\substack{y+u=w\\ x+v=-w\\ -\delta\leqslant x\leqslant y\\ u\leqslant v\leqslant\delta\\ x+y\geqslant 1/2-\delta}} g(x)g(y)g(u)g(v)\,dx\,dy. \tag{5.3}$$

Let us now take $\delta = 0$. In this case

$$\int_{1/2}^1 f(z)f(-z)\,dz \leqslant 4\int_{-1/4}^{1/4} dw \iint\limits_{\substack{x+v=-w\\ y+u=w\\ u\leqslant v\leqslant 0\leqslant x\leqslant y}} g(x)g(y)g(u)g(v)\,dx\,dy.$$

Interchanging the rôles of the variables x, y, and as a result those of u, v, and replacing w by $-w$, we get an integral as before, except that the region $u \leqslant v \leqslant 0 \leqslant x \leqslant y$ is replaced by the region $v \leqslant u \leqslant 0 \leqslant y \leqslant x$. These regions are essentially disjoint, and are contained in $u \leqslant 0 \leqslant y$, $v \leqslant 0 \leqslant x$. We therefore obtain

$$\leqslant 2\int_{-1/4}^{1/4} dw \Big(\int\limits_{\substack{x+v=-w \\ v\leqslant 0\leqslant x}} g(x)g(v)\,dx \Big) \Big(\int\limits_{\substack{y+u=w \\ u\leqslant 0\leqslant y}} g(y)g(u)\,dy \Big)$$

$$= 2\int_{-1/4}^{1/4} dw\, \widetilde{f}(w)\widetilde{f}(-w)$$

with

$$\widetilde{f}(w) = \int\limits_{\substack{y+u=w \\ u\leqslant 0\leqslant y}} g(y)g(u)\,dy. \tag{5.4}$$

Thus

$$\int_{1/2}^{1} f(z)f(-z)\,dz \leqslant 4\int_{0}^{1/4} \widetilde{f}(w)\widetilde{f}(-w)\,dw. \tag{5.5}$$

It is clear from (5.1) and (5.4) that $\widetilde{f}(w) \leqslant f(w)/2 \leqslant 1/2$, so that we obtain $\leqslant 1/4$, and Lemma 1 follows. □

6. The upper bound $B \leqslant 1.7375$

With $f = g * g$ as above, and $\varepsilon = \pm 1$, set

$$I_\varepsilon = \int_0^{1/8} g(\varepsilon x)\,dx, \qquad J_\varepsilon = \iint\limits_{\substack{\varepsilon y>0,\ \varepsilon u>0 \\ \varepsilon(y+u)\leqslant 1/4}} g(y)g(u)\,dy\,du.$$

Lemma 2.

(i) $\int_{1/2}^{1} f(z)f(-z)\,dz \leqslant 1/4 - J_\varepsilon$.

(ii) *For* $0 \leqslant \delta \leqslant 1/6$,

$$\int_{1/2-\delta}^{1} f(z)f(-z)\,dz \leqslant \frac{1}{4} + \frac{\delta}{2} + \Big(\int_{-\delta}^{\delta} g(x)\,dx\Big)^2.$$

As a consequence,

$$|f|_1 = \int_0^1 \big(f(z)+f(-z)\big)\,dz = \int_0^{1/2-\delta} + \int_{1/2-\delta}^1 \tag{6.1}$$
$$\leqslant 1 - 2\delta + \int_{1/2-\delta}^1 \big(1 + f(z)f(-z)\big)\,dz$$
$$\leqslant \frac{3}{2} - \delta + \int_{1/2-\delta}^1 f(z)f(-z)\,dz \leqslant \frac{7}{4} - \frac{\delta}{2} + \Big(\int_{-\delta}^{\delta} g(x)\,dx\Big)^2.$$

Setting $\delta = 1/8$ we obtain

$$|f|_1 \leqslant \frac{27}{16} + (I_1 + I_{-1})^2 \leqslant \frac{27}{16} + 4M^2 \tag{6.2}$$

with $M = \max(I_1, I_{-1})$. On the other hand, by (i),

$$|f|_1 \leqslant \frac{3}{2} + \int_{1/2}^1 f(z)f(-z)\,dz \leqslant \frac{7}{4} - \max_{\varepsilon=\pm1} J_\varepsilon \leqslant \frac{7}{4} - M^2. \tag{6.3}$$

In conjunction with (6.2) this gives $|f|_1 \leqslant 7/4 - 1/80 = 1.7375$, so that indeed $B \leqslant 1.7375$.

Proof of Lemma 2. When $w > 0$, we cannot have $y + u = w$ and $u \leqslant y < 0$. Therefore $\widetilde{f}(w)$ as given by (5.4) is

$$\widetilde{f}(w) = \int\limits_{\substack{y+u=w\\ u\leqslant y}} g(y)g(u)\,dy - \int\limits_{\substack{y+u=w\\ 0\leqslant u\leqslant y}} g(y)g(u)\,dy = \frac{1}{2}\,f(w) - \frac{1}{2}\,\widehat{f}(w)$$

with

$$\widehat{f}(w) = \int\limits_{\substack{y+u=w\\ y,u\geqslant 0}} g(y)g(u)\,dy.$$

Now (5.5) yields

$$\int_{1/2}^1 f(z)f(-z)\,dz \leqslant \int_0^{1/4} \big(f(w) - \widehat{f}(w)\big)f(-w)\,dw \leqslant \int_0^{1/4} \big(1 - \widehat{f}(w)\big)\,dw$$
$$= \frac{1}{4} - \int_0^{1/4} dw \int\limits_{\substack{y+u=w\\ y,u\geqslant 0}} g(y)g(u)\,dy$$
$$= \frac{1}{4} - \iint\limits_{\substack{y,u\geqslant 0\\ y+u\leqslant 1/4}} g(y)g(u)\,dy\,du = \frac{1}{4} - J_1.$$

The bound $1/4 - J_{-1}$ is obtained similarly, so that assertion (i) is established.

We will now suppose $\delta > 0$, and we return to the bound (5.3). We first deal with the part where $v \leqslant x$ in the integral, so that

$$u \leqslant v \leqslant x \leqslant y. \tag{6.4}$$

After interchanging the rôles of x and y, and of u and v, and replacing w by $-w$, the integrand will be the same, but now

$$v \leqslant u \leqslant y \leqslant x. \tag{6.5}$$

The interiors of the domains (6.4), (6.5) are disjoint, and are contained in the region with $v \leqslant x$ and $u \leqslant y$, so that this part of (5.3) is

$$\begin{aligned} &\leqslant 2\int_{-1/4-\delta/2}^{1/4+\delta/2} dw \Big(\int_{\substack{x+v=-w \\ v\leqslant x}} g(x)g(v)\,dx\Big)\Big(\int_{\substack{y+u=w \\ u\leqslant y}} g(y)g(u)\,dy\Big) \\ &= \frac{1}{2}\int_{-1/4-\delta/2}^{1/4+\delta/2} dw\, f(-w)f(w) = \int_0^{1/4+\delta/2} f(w)f(-w)\,dw \leqslant 1/4+\delta/2. \end{aligned} \tag{6.6}$$

It remains for us to deal with the part of (5.3) where $x \leqslant v$ in the integral, so that $-\delta \leqslant x \leqslant v \leqslant \delta$. This part is

$$\leqslant 4\int dw \int_{\substack{x+v=-w \\ -\delta\leqslant x\leqslant v\leqslant\delta}} g(x)g(v)\,dx \int_{\substack{y+u=w \\ y\geqslant 1/2-\delta-x \\ u\leqslant\delta}} g(y)g(u)\,dy.$$

When $0 < \delta \leqslant 1/6$, then $y \geqslant 1/2 - 2\delta \geqslant \delta \geqslant u$, and the last integral is

$$\leqslant \int_{\substack{y+u=w \\ u\leqslant y}} g(y)g(u)\,dy = f(w)/2 \leqslant 1/2.$$

Therefore the part in question of (5.3) becomes

$$\leqslant 2\int dw \int_{\substack{x+v=-w \\ -\delta\leqslant x\leqslant v\leqslant\delta}} g(x)g(v)\,dx = \int dw \int_{\substack{x+v=-w \\ -\delta\leqslant x,v\leqslant\delta}} g(x)g(v)\,dx = \Big(\int_{-\delta}^{\delta} g(x)\,dx\Big)^2.$$

Together with (6.6) this gives the asserted bound for $\int_{1/2-\delta}^{1} f(z)f(-z)\,dz$. □

7. The upper bound 1.7373

In fact we will show that

$$B \leqslant 7/4 - 1/80 - \xi < 1.7373 \tag{7.1}$$

where $\xi = 0.000200513\ldots$ is a root of the transcendental equation

$$F(b(x)/a(x)) = 1/2,$$

where $a(x) = 1/10 - 2x$, $b(x) = (\sqrt{1/20 - x} - \sqrt{1/80 + x})^2/2$, and

$$F(x) = \sqrt{x^2 + x} + \log(\sqrt{x^2 + x} + \sqrt{x}).$$

The calculation of ξ has kindly been performed by Dr. A. Pokrzywa.

We will suppose that $f \in \mathcal{F}$, $|f|_\infty = 1$ and

$$|f|_1 > 7/4 - 1/80 - \xi, \tag{7.2}$$

and we will reach a contradiction, thereby establishing the truth of (7.1), and hence of Theorem 2.

Retaining earlier notation we now set $a = a(\xi)$,

$$u = I_1 + I_{-1}, \qquad v = |I_1 - I_{-1}|, \qquad m = \min(I_1, I_{-1}) = (u - v)/2,$$

and observe that $M = \max(I_1, I_{-1}) = (u+v)/2$. Also, u_0, u_1 will be the positive numbers with

$$u_0^2 = 1/20 - \xi = a/2, \qquad u_1^2 = 1/20 + 4\xi.$$

We may suppose that

$$u \geqslant u_0, \tag{7.3}$$

for otherwise (6.2) yields $|f|_1 \leqslant 27/16 + u_0^2 = 7/4 - 1/80 - \xi$, against (7.2). We further may suppose that

$$u + v \leqslant u_1, \tag{7.4}$$

for otherwise (6.3) yields $|f|_1 \leqslant 7/4 - u_1^2/4 = 7/4 - 1/80 - \xi$, contradicting (7.2). As a consequence,

$$\begin{aligned} 2u^2 - m^2/2 = 2u^2 - (u - v)^2/8 &= 3u^2/2 + u(u + v)/2 - (u + v)^2/8 \\ &\leqslant 3u^2/2 + 3u(u + v)/8 \leqslant 15u_1^2/8 < 1/10 - 2\xi = a, \end{aligned}$$

so that

$$0 = 2u_0^2 - a \leqslant 2u^2 - a < m^2/2. \tag{7.5}$$

Lemma 3.

$$\frac{7}{4} - |f|_1 \geqslant \frac{1}{4}(u^2 + v^2) + \int_{2u^2 - a}^{m^2/2} \left(\sqrt{(\eta + a)/2} - u\right) \frac{d\eta}{\sqrt{2\eta}}.$$

Proof. By (6.1) and (7.2),

$$1/80 + \xi > \delta/2 - \left(\int_{-\delta}^{\delta} g(x)\, dx\right)^2$$

for δ in $0 < \delta < 1/6$. Setting $\delta = 1/8 + \eta$ with $0 < \eta < 1/24$, this gives

$$\left(\int_{-1/8-\eta}^{1/8+\eta} g(x)\, dx\right)^2 > \eta/2 + 1/20 - \xi = (\eta + a)/2,$$

and

$$G(\eta) := \int_{1/8}^{1/8+\eta} (g(x) + g(-x))\,dx > \sqrt{(\eta + a)/2} - u. \tag{7.6}$$

On the other hand, by (6.3) and (7.2), and since $m^2/2 \leqslant u^2/8 \leqslant u_1^2/8 < 1/24 < 1/8$,

$$\begin{aligned}\frac{1}{80} + \xi &> \frac{1}{2}\sum_{\varepsilon=\pm1} J_\varepsilon = \frac{1}{2}\Big(I_1^2 + I_{-1}^2 + 2\sum_{\varepsilon=\pm1}\int_{1/8}^{1/4} g(\varepsilon x)\,dx \int_0^{1/4-x} g(\varepsilon y)\,dy\Big)\\ &\geqslant \frac{1}{2}\Big(\frac{u^2+v^2}{2} + 2\sum_{\varepsilon=\pm1}\int_{1/8}^{1/8+m^2/2} g(\varepsilon x)\,dx \int_0^{1/4-x} g(\varepsilon y)\,dy\Big)\\ &= \frac{1}{4}(u^2+v^2) + \sum_{\varepsilon=\pm1}\int_0^{m^2/2} g(\varepsilon/8 + \varepsilon\eta)\,d\eta \int_0^{1/8-\eta} g(\varepsilon y)\,dy.\end{aligned}$$

By (3.1) with $r = 1/8 - \eta$, $s = 1/8$,

$$\int_0^{1/8-\eta} g(\varepsilon y)\,dy = I_\varepsilon - \int_{1/8-\eta}^{1/8} g(\varepsilon y)\,dy \geqslant I_\varepsilon - \sqrt{2\eta} \geqslant m - \sqrt{2\eta}\,.$$

Thus

$$\begin{aligned}\frac{1}{80} + \xi &> \frac{1}{4}(u^2+v^2) + \sum_{\varepsilon=\pm1}\int_0^{m^2/2} g(\varepsilon/8 + \varepsilon\eta)\big(m - \sqrt{2\eta}\big)\,d\eta\\ &= \frac{1}{4}(u^2+v^2) + \int_0^{m^2/2} \big(g(1/8+\eta) + g(-1/8-\eta)\big)\big(m - \sqrt{2\eta}\big)\,d\eta.\end{aligned}$$

Integrating by parts we represent the last integral as

$$\int_0^{m^2/2} G(\eta)\,\frac{d\eta}{\sqrt{2\eta}} \geqslant \int_{2u^2-a}^{m^2/2} G(\eta)\,\frac{d\eta}{\sqrt{2\eta}}\,.$$

Since $m^2/2 < 1/24$ we may apply (7.6) to obtain the lemma. □

Lemma 4. *In the domain of points* (u, v) *with* (7.3), (7.4), $v \geqslant 0$, *the function*

$$H(u,v) = \frac{1}{4}(u^2+v^2) + \int_{2u^2-a}^{\frac{1}{2}(\frac{u-v}{2})^2} (\sqrt{(\eta+a)/2} - u)\,\frac{d\eta}{\sqrt{2\eta}}$$

satisfies $H(u,v) \geqslant H(u_0, u_1 - u_0)$.

Proof.

$$2H(u,v) = \frac{1}{2}(u^2+v^2) + \int_{2u^2-a}^{\frac{1}{2}(\frac{u-v}{2})^2} \sqrt{\frac{\eta+a}{\eta}}\,d\eta - u(u-v) + 2u\sqrt{4u^2-2a}.$$

Hence

$$2\frac{\partial H(u,v)}{\partial v} = v+u+\left(\frac{(u-v)^2+8a}{(u-v)^2}\right)^{1/2}\cdot\frac{v-u}{4}$$
$$= v+u-\frac{1}{4}\big((u-v)^2+8a\big)^{1/2}.$$

We claim that this partial derivative is $\leqslant 0$ in our domain. For otherwise $16(u+v)^2 - ((u-v)^2+8a) > 0$, or $15(u+v)^2+4uv-8a > 0$. But $u+v \leqslant u_1$ and $4uv \leqslant 4u(u_1-u) \leqslant 4u_0(u_1-u_0)$ since $u \geqslant u_0 > u_1/2$. Therefore $15u_1^2+4u_0u_1-4u_0^2-8a > 0$. Substituting the values for a, u_0, u_1 gives

$$4u_0u_1 \geqslant 1/4 - 80\xi.$$

Squaring, we get

$$16(1/20+4\xi)(1/20-\xi) > (1/4-80\xi)^2,$$

which is not true. Thus our claim is proven, and

$$H(u,v) \geqslant H(u,u_1-u). \tag{7.7}$$

Next,

$$2H(u,u_1-u) = -u^2+\frac{1}{2}u_1^2+\int_{2u^2-a}^{\frac{1}{2}(\frac{2u-u_1}{2})^2}\sqrt{\frac{\eta+a}{\eta}}\,d\eta+2u\sqrt{4u^2-2a}\,,$$

so that

$$2\frac{d}{du}H(u,u_1-u) = -2u+\left(\frac{(2u-u_1)^2+8a}{(2u-u_1)^2}\right)^{1/2}\cdot\frac{2u-u_1}{2}-\left(\frac{2u^2}{2u^2-a}\right)^{1/2}\cdot 4u$$
$$+2(4u^2-2a)^{1/2}+8u^2(4u^2-2a)^{-1/2}$$
$$= -2u+\frac{1}{2}\sqrt{(2u-u_1)^2+8a}+2\sqrt{4u^2-2a}\,.$$

We claim that this derivative is $\geqslant 0$ for $u_0 \leqslant u \leqslant u_1$. For otherwise $16u^2 \geqslant (2u-u_1)^2+8a$, so that $12u^2+4uu_1-u_1^2 > 8a$. But this entails $15u_1^2 > 8a$, i.e.,

$$15(1/20+4\xi) > 4/5+16\xi,$$

which is not true. Thus our claim is correct, and

$$H(u,u_1-u) \geqslant H(u_0,u_1-u_0),$$

which together with (7.7) establishes the lemma. □

It is now easy to arrive at the desired contradiction to (7.2). By Lemmas 3 and 4,

$$7/4-|f|_1 \geqslant H(u_0,u_1-u_0)$$
$$= \frac{1}{4}(u_0^2+(u_1-u_0)^2)+\int_{2u_0^2-a}^{\frac{1}{2}(u_0-\frac{1}{2}u_1)^2}\left(\frac{1}{2}\sqrt{\frac{\eta+a}{\eta}}-\frac{u_0}{\sqrt{2\eta}}\right)d\eta.$$

Here $2u_0^2 - a = 0$ and $\frac{1}{2}\big(u_0 - \frac{1}{2}u_1\big)^2 = b(\xi) = b$, say, and

$$\int_0^x \sqrt{\frac{\eta + a}{\eta}}\, d\eta = aF(x/a), \qquad \int_0^x \frac{d\eta}{\sqrt{2\eta}} = \sqrt{2x}\,.$$

Therefore

$$\begin{aligned} 7/4 - |f|_1 &\geqslant \frac{1}{4}(2u_0^2 - 2u_0u_1 + u_1^2) + \frac{a}{2}F(b/a) - u_0(u_0 - u_1/2) \\ &= -u_0^2/2 + u_1^2/4 + \frac{a}{2}\,F(b/a) = -\frac{1}{80} + \frac{3}{2}\,\xi + \frac{a}{2}\,F(b/a) = 1/80 + \xi, \end{aligned}$$

contrary to (7.2). □

Added in proof. Dr. Erik Bajalinov has checked that for $n \leqslant 26$ and $n = 31, 36, 41, 46, 51$: $A(n) < 4/\pi$, which suggests that $B = 4/\pi$.

Addendum*

The following problem equivalent to the problem considered in this paper has been proposed by L. Moser at the Institute in the Theory of Numbers (Boulder, Colorado 1959), see Report of the said Institute, p. 342, Problem 29:

Let $f(x) \geqslant 0$, $f(x) = 0$ *outside* $(0, 1)$, $\int_0^1 f(x)\,dx = 1$. *Let*

$$g(t) = \int_0^t f(x)\,f(t - x)\,dx.$$

Find $M = \min\limits_f \max\limits_t g(t)$. Conjecture: $M = \pi/4$.

Reference

[1] B. Green, *The number of squares and* $B_h[g]$ *sets*. Acta Arith. 100 (2001), 365–390.

* Added in 2006

Unsolved problems and unproved conjectures

Unsolved problems and unproved conjectures proposed by Andrzej Schinzel in the years 1956–2006 arranged chronologically

1 (conjecture) For every positive integer m there exist $n_0(m)$ and $n_1(m)$ such that for $n > n_0(m)$ or $n > n_1(m)$ the equation

$$\frac{m}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$$

is solvable in positive integers x, y, z or in integers x, y, z respectively.
(formulated in [5])

2 (problem) Does the number of integer solutions of the equation $x_1 + x_2 + \ldots + x_s = x_1 x_2 \cdots x_s$ satisfying $1 \leqslant x_1 \leqslant x_2 \leqslant \ldots \leqslant x_s$ tend to infinity with s ? (formulated in [6])

3 (conjecture) For every even k the equation $\varphi(x + k) = \varphi(x)$ has infinitely many solutions. (paper 21)

4 (conjecture) If k is a positive integer and $f_1(x), f_2(x), \ldots, f_k(x)$ irreducible polynomials with integer coefficients and the leading coefficient positive such that $f_1(x) f_2(x) \cdots f_k(x)$ has no fixed divisor > 1, then there exist infinitely many positive integers x such that all numbers $f_i(x)$ $(1 \leqslant i \leqslant k)$ are primes. (paper 22=J1)

5 (conjecture) For all positive integers k and n, where $n > 1$, $k \leqslant n$, $(k, n) = 1$, there exists at least one prime $p \equiv k \pmod{n}$, $p < n^2$. (paper 22=J1)

6 (conjecture) For every integer $k > 34$, $k \neq p^\alpha$ (p prime) there exists an integer n such that $n - i \nmid \binom{n}{i}$ for all $i \leqslant k$. (paper 26=H1)

7 (conjecture) Every integer $n \not\equiv 0, 4, 7 \pmod 8$, $n > 130$, is a sum of three positive squares. (paper 33=A4)

8 (conjecture) Every integer $n \not\equiv 0, 4, 7 \pmod 8$, $n > 627$, is a sum of three distinct squares. (paper 33=A4)

9 (conjecture) For every positive integer k

$$\liminf_{n\to\infty} \frac{\overbrace{\sigma\sigma\cdots\sigma}^{k \text{ times}}(n)}{n} < \infty. \qquad ([3])$$

10 (conjecture) The product $p_1 p_2 \cdots p_{k-1} p_{k+1}$, where p_i is the i-th prime, is the least positive integer $g(k)$ with the property that for every integer n sufficiently large at least one of the numbers $n+1, n+2, \ldots, n+g(k)$ has more than k prime divisors. ([4])

11 (problem) Apart from 2, 3, 5 and 3, 4, 5, 7, 11 does there exist a sequence $a_1 < a_2 < \ldots < a_r$ of positive integers such that

$$a_r < [a_i, a_j] \quad (1 \leqslant i < j \leqslant r) \quad \text{and} \quad \sum_{i=1}^{r} \frac{1}{a_i} > 1 \, ? \qquad \text{(paper 35)}$$

12 (conjecture) For every $k \neq 1$ and $l \geqslant 0$ there exists an integer m such that the equations $\varphi(x) = m$ and $\sigma(y) = m$ have exactly k and l solutions respectively. (paper 46=J2)

13 (conjecture) For every $x \geqslant 8$ there is a prime between x and $x + (\log x)^2$. (paper 46=J2)

14 (problem) For every pair of relatively prime integers with $|a| > |b| > 0$ does there exist n such that $a^n - b^n$ has three primitive prime factors? (paper 53=I1)

15 (problem) Does there exist a pair a, b (as above) with $ab \neq \pm c^h$ $(h \geqslant 2)$ such that $a^n - b^n$ has three primitive prime factors for infinitely many n? (paper 53=I1)

16 (problem) Does there exist a pair a, b (as above) with $ab \neq \pm 2c^2, \pm c^h$ $(h \geqslant 2)$ such that the greatest prime factor of $a^n - b^n$ is greater than $2n$ for all sufficiently large n? (paper 53=I1)

17 (problem) Does there exist a polynomial $f \in \mathbb{Q}[x_1, x_2, \ldots, x_n, y, z]$ such that for all integer systems $(x_1, \ldots, x_n)$ the equation

$$f(x_1, x_2, \ldots, x_n, y, z) = 0 \qquad (1)$$

is soluble in integers y, z and for no rational functions

$$\varphi, \psi \in \mathbb{Q}(x_1, x_2, \ldots, x_n) \qquad (2)$$

the identity

$$f(x_1, x_2, \ldots, x_n, \varphi, \psi) = 0 \qquad (3)$$

holds? (paper 56=E1, cf. also 69=F1)

18 (problem) Does there exist a polynomial

$$f \in \mathbb{Q}[x_1, x_2, \ldots, x_n, y, z]$$

such that for all rational systems $(x_1, \ldots, x_n)$ the equation (1) is soluble in rational y, z and for no rational functions φ, ψ satisfying (2) the identity (3) holds? (paper 56=E1)

19 Let distinct polynomials $f_1, \ldots, f_k$ $(k \geqslant 0)$ satisfy the assumptions of conjecture 4. Let g be a polynomial with integral coefficients and the leading coefficient positive.

(conjecture) Let n be a positive integer such that $n - g(x)$ is irreducible and $\prod_{i=1}^{k} f_i(x)(n - g(x))$ has no fixed divisor > 1. Denote by $N(x) = N$ the number of

positive integers x such that $n - g(x) > 0$ and by $P(n)$ the number of x's such that all numbers $f_1(x)$, $f_2(x)$, ..., $f_k(x)$ and $n - g(x)$ are primes. Then for large n we have

$$P(n) \sim \frac{N}{\log^{k+1} N} (h_0 h_1 \cdots h_k)^{-1} \prod_p \Big(1 - \frac{\omega(p)}{p}\Big)\Big(1 - \frac{1}{p}\Big)^{-k-1},$$

where $h_0 = \deg g$, $h_i = \deg f_i$ and $\omega(p)$ is the number of solutions of the congruence $\prod_{i=1}^{k} f_i(x)(n - g(x)) \equiv 0 \pmod p$. (paper 60=J3)

20 (problem) Does there exist infinitely many solutions of the equation $(x^2-1)(y^2-1) = (z^2-1)^2$ with x even, y, z odd or at least one solution with $|x|$, $|y|$, $|z|$ even and distinct? (paper 61)

21 (problem) Assume that $f \in \mathbb{Z}[x]$ and $f(x)$ is representable as a sum of two integral cubes for all sufficiently large integer x. Does it follow that $f(x) = u(x)^3 + v(x)^3$, where u, v are integer valued polynomials? (paper 66=A6)

22 (problem) Is the inequality

$$\sigma\varphi(n) \geqslant \frac{1}{2} n$$

true for all n ? (paper 67=G5)

23 (conjecture) There exists a constant $c > 0$ such that for every algebraic integer $\alpha \neq 0$ of degree n, that is not a root of unity,

$$\boxed{|\alpha|} > 1 + \frac{c}{n}. \quad \text{(paper 68=C1)}$$

24 A factorization of a polynomial in $\mathbb{Q}[x]$ into a product of a constant and of coprime powers of polynomials irreducible over $\mathbb{Q}$ is called *standard*. For a given polynomial $f \neq 0$, Kf denotes the factor of f of the greatest possible degree whose no root is 0 or a root of 1 and whose leading coefficient is equal to the leading coefficient of f. If $\phi \in \mathbb{Q}[x_1^{\pm 1}, \ldots, x_k^{\pm 1}] \setminus \{0\}$, then

$$J\phi = \phi \prod_{i=1}^{k} x_i^{-\operatorname{ord}_{x_i} \phi}.$$

(conjecture) Let $F(y_1, \ldots, y_k)$ be a polynomial irreducible over $\mathbb{Q}$ which does not divide $y_1 \cdots y_k J(y_1^{\delta_1} y_2^{\delta_2} \cdots y_k^{\delta_k} - 1)$ for any integers $\delta_1, \ldots, \delta_k$ not all zero.

For every system of k positive integers $n_1, \ldots, n_k$ there exists an integral non-singular matrix $[\nu_{ij}]$ $(1 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant k)$ satisfying the following conditions:

(i) $0 \leqslant \nu_{ij} \leqslant C_1(F)$ $(1 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant k)$;

(ii) $n_i = \sum_{j=1}^{k} \nu_{ij} u_j$ $(1 \leqslant i \leqslant k)$, u_j integers $\geqslant 0$ $(1 \leqslant j \leqslant k)$;

(iii) if

$$JF\Big(\prod_{j=1}^{k} y_j^{\nu_{1j}}, \prod_{j=1}^{k} y_j^{\nu_{2j}}, \ldots, \prod_{j=1}^{k} y_j^{\nu_{kj}}\Big) = \text{const} \prod_{s=1}^{r} F_s(y_1, \ldots, y_k)^{e_s}$$

is a standard factorization, then either

$$KF(x^{n_1}, \ldots, x^{n_k}) = \text{const} \prod_{s=1}^{r} KF_s(x^{u_1}, \ldots, x^{u_k})^{e_s}$$

is a standard factorization or $\alpha_1 n_1 + \ldots + \alpha_k n_k = 0$, where α_i are integers not all zero and $|\alpha_i| \leqslant C_0(F)$ $(1 \leqslant i \leqslant k)$. $C_0(F)$ and $C_1(F)$ are constants independent of $n_1, \ldots, n_k$. (paper 73=D2, cf. also paper 96=D4)

25 (conjecture) In every finite covering system of congruences $a_i \pmod{m_i}$ $(m_i > 1)$ we have $m_i \mid m_j$ for at least one pair $\langle i, j \rangle$ with $i \neq j$. (paper 86=D3)

26 Let S be the set of all polynomials with integral coefficients and the leading coefficient positive.

(problem) Does there exist for every polynomial $f(x) \in S$ and every $\varepsilon > 0$ a polynomial $h(x) \in S$ of degree d such that the degree of each irreducible factor of $f(h(x))$ is less than εd ? (paper 87, §5=J4).

27 (problem) Does there exist an identity $\sum_{i=1}^{4} f_i^3(x) = Px + Q$, where $f_i \in \mathbb{Z}_3[x]$, $P, Q \in \mathbb{Z}_3$, $P \neq 0$, $Q \equiv 4 \pmod 9$? (paper 89)

28 (conjecture) Every genus of primitive binary quadratic forms with discriminant D represents a positive integer $\leqslant c(\varepsilon)|D|^{\varepsilon}$ for every $\varepsilon > 0$. (paper 99)

29 (problem) To estimate the number of irreducible non-cyclotomic factors of a polynomial $f \in \mathbb{Z}[x]$ by a function of $\|f\|$ alone, where $\|f\|$ is the sum of squares of the coefficients of f. (paper 105=C6)

30 (problem) Let K be an algebraic number field. Does there exist a sequence $\{\alpha_i\}$ of integers in K such that for every ideal $\mathfrak{q}$ of K, integers $\alpha_1, \alpha_2, \ldots, \alpha_{N(\mathfrak{q})}$ represent all residue classes modulo $\mathfrak{q}$?

(formulated in [7], earlier for $K = \mathbb{Q}(i)$ proposed orally by J. Browkin)

31 (problem) To improve the estimate $(\log n)^2 / \log\log n$ for the number of non-zero coefficients of the cyclotomic polynomial with a square-free index n. (formulated in [1])

32 (conjecture) If a polynomial $P(x)$ with rational coefficients has at least three simple zeros, then the equation $y^2 z^3 = P(x)$ has only finitely many solutions in integers x, y, z with $yz \neq 0$. (paper 115=A8)

33 (problem) Given a, b with $|a| \neq |b|$, do there exist infinitely many quotients r such that for suitable integers m, n: $m/n = r$ and $K(ax^{m+n} + bx^m + bx^n + a)$ is reducible?

(paper 121=D7, the operation K is defined in 24 above)

34 (conjecture) Let $F \in \mathbb{Z}[x, y]$ be a form such that

$$F(x, y) = F_1(ax + by, cx + dy) \text{ for any } F_1 \in \mathbb{Z}[x, y] \text{ and any } a, b, c, d \in \mathbb{Z}$$

$$\text{implies } \begin{vmatrix} a & b \\ c & d \end{vmatrix} = \pm 1.$$

If $f \in \mathbb{Z}[t_1, \ldots, t_r]$ has the fixed divisor equal to its content and the equation

$$F(x, y) = f(t_1, \ldots, t_r) \tag{4}$$

is soluble in integers x, y for all integral vectors $[t_1, \dots, t_r]$, then there exist polynomials $X, Y \in \mathbb{Z}[t_1, \dots, t_r]$ such that identically

$$F\big(X(t_1, \dots, t_r), Y(t_1, \dots, t_r)\big) = f(t_1, \dots, t_r). \tag{5}$$ (paper 128=J5)

35 (conjecture) Let $F \in \mathbb{Z}[x, y]$ be any form and $f \in \mathbb{Z}[t_1, \dots, t_r]$ any polynomial. If the equation (4) is soluble in integers x, y for all integer vectors $[t_1, \dots, t_r]$, then there exist polynomials $X, Y \in \mathbb{Q}[t_1, \dots, t_r]$ satisfying (5). (paper 128=J5)

36 (problem) Does the divisibility $\phi(n) + 1 \mid n$ imply $n = p$ or $2p$, where p is a prime? (formulated in [2], p. 52)

37 (conjecture) If $F \in \mathbb{Z}[x, y, t]$ is irreducible, the highest homogeneous part F_0 of F with respect to x, y is reducible over $\mathbb{Q}(t)$ and every arithmetic progression contains an integer t^* such that $F(x, y, t^*) = 0$ is solvable in integers x, y, then there exist polynomials $X, Y \in \mathbb{Q}[t]$ such that $F\big(X(t), Y(t), t\big) = 0$. (paper 132=A12)

38 (problem) Let $\boldsymbol{a}(0) = [a_1(0), \dots, a_n(0)] \in \mathbb{R}^n$ and an infinite sequence

$$\boldsymbol{a}(t) = [a_1(t), \dots, a_n(t)]$$

be formed by means of the formulae

$$a_i(t+1) = |a_i(t) - a_{i+1}(t)|,$$

where the addition of indices is $\bmod n$. Is it true that for every n and every $\boldsymbol{a}(0) \in \mathbb{R}^n$ either $\lim\limits_{t\to\infty} a(t) = 0$ or there exists $c \in \mathbb{R}$ such that $a(t) \in \{0, c\}^n$ for all sufficiently large t? (paper 155)

39 Given m linearly independent vectors $\boldsymbol{n}_1, \dots, \boldsymbol{n}_m \in \mathbb{Z}^k$, let $H(\boldsymbol{n}_1, \dots, \boldsymbol{n}_m)$ denote the maximum of the absolute values of all minors of order m of the matrix

$$\begin{pmatrix} \boldsymbol{n}_1 \\ \vdots \\ \boldsymbol{n}_m \end{pmatrix}$$

and $D(\boldsymbol{n}_1, \dots, \boldsymbol{n}_m)$ the greatest common divisor of these minors. Furthermore, let

$$c_0(k, l, m) = \sup \inf \left(\frac{D(\boldsymbol{n}_1, \dots, \boldsymbol{n}_m)}{H(\boldsymbol{n}_1, \dots, \boldsymbol{n}_m)} \right)^{(k-l)/(k-m)} \prod_{i=1}^{l} H(p_i),$$

where the supremum is taken over all sets of linearly independent vectors $\boldsymbol{n}_1, \dots, \boldsymbol{n}_m \in \mathbb{Z}^k$ and the infimum is taken over all sets of linearly independent vectors $\boldsymbol{p}_1, \dots, \boldsymbol{p}_l \in \mathbb{Z}^k$ such that

$$\boldsymbol{n}_i = \sum_{j=1}^{l} u_{ij} p_j, \quad u_{ij} \in \mathbb{Q}.$$

(problem) Is $\limsup\limits_{k,l\to\infty} c_0(k, l, m)$ finite? (paper 166=L2)

40 (problem) Given an integer $m \geqslant 3$, does there exist a number K such that every polynomial in $\mathbb{Q}[x]$ with m non-zero coefficients has a factor irreducible over $\mathbb{Q}$ with at most K non-zero coefficients? (paper 168, for $m = 3$ already paper 56=E1)

41 (conjecture) If $f_i(x) = a_i x^2 + b_i x + c_i \in \mathbb{Z}[x]$ $(i = 1, 2, 3)$, $\sqrt{a_1 a_2 a_3} \notin \mathbb{Q}$, then the number $N(x)$ of integers x_3 such that $|x_3| \leqslant x$ and the equation $f_3(x_3) = f_1(x_1) f_2(x_2)$ is soluble in integers x_1, x_2, satisfies $N(x) \ll x^{\varepsilon}$ for every $\varepsilon > 0$. (paper 170)

42 (conjecture) For every algebraic number field K there exist sets $F_{\nu,\mu} \subset K^2$ $(\nu \in \mathbb{N}, \mu \in \mathbb{N})$ such that

$$\bigcup_{\langle \nu,\mu \rangle} \bigcup_{\langle a,b \rangle \in F_{\mu,\nu}(K)} \{x^{\nu} + a x^{\mu} + b\} \quad \text{is finite}$$

and if $x^n + a x^m + b$, where $n \geqslant 2m > 0$, $\langle a, b \rangle \in K^{*2}$, is reducible over K, at least one of the following conditions is satisfied:

(i) $x^{n/(n,m)} + a x^{m/(n,m)} + b$ has a proper linear or quadratic factor over K,

(ii) there exists an integer l such that $\langle n/l, m/l \rangle = \langle 2p, p \rangle$ (p prime), $\langle 6, 1 \rangle$, $\langle 6, 2 \rangle$, $\langle 7, 1 \rangle$, $\langle 8, 2 \rangle$, $\langle 8, 4 \rangle$, $\langle 9, 3 \rangle$, $\langle 10, 2 \rangle$, $\langle 10, 4 \rangle$, $\langle 12, 2 \rangle$, $\langle 12, 3 \rangle$, $\langle 12, 4 \rangle$, $\langle 15, 5 \rangle$, $\langle 7, 2 \rangle$, $\langle 7, 3 \rangle$, $\langle 8, 1 \rangle$, $\langle 9, 1 \rangle$, $\langle 14, 2 \rangle$, $\langle 21, 7 \rangle$,

(iii) there exists an integer l such that $\langle n/l, m/l \rangle =: \langle \nu, \mu \rangle \in \mathbb{Z}^2$ and $a = u^{\nu-\mu} a_0(v)$, $b = u^{\nu} b_0$, where $\langle a_0, b_0 \rangle \in F_{\nu,\mu}$.

Consequence 1. For every algebraic number field K there exists a constant $C_1(K)$ such that if $n_1 > C_1(K)$ and $a, b \in K^*$ then $x^n + a x^m + b$ is reducible over K if and only if (i) holds.

Consequence 2. For every algebraic number field K there exists a constant $C_2(K)$ such that if $a, b \in K$ then $x^n + a x^m + b$ has in $K[x]$ an irreducible factor with at most $C_2(K)$ non-zero coefficients.

Consequence 3. There are only finitely many integers b such that for some $n \neq 2m$, $x^n + b x^m + 1$ is reducible over $\mathbb{Q}$. (paper 175=D10)

43 (problem) What is the least positive integer n such that all integers $2^k n - 1$ $(k = 1, 2, \ldots)$ are composite? (paper 179=G6)

44 (problem) Have the integers not of the form $n - \varphi(n)$ a positive lower density? (paper 179=G6)

45 (conjecture) Let k, m, a, b be positive integers, $m > kb$. There are no polynomials $F_1, F_2, \ldots, F_k \in \mathbb{Z}[x]$ with the leading coefficient positive such that

$$\frac{m}{ax + b} = \sum_{i=1}^{k} \frac{1}{F_i(x)}\,. \qquad \text{(paper 198=A15)}$$

46 (problem) Do there exist two trinomials $T_i \in \mathbb{C}[x]$ $(i = 1, 2)$ such that (T_1, T_2) has more than six non-zero coefficients? (paper 199=D16)

47 (conjecture) For every algebraic number field K and $d = 1, 2$ there exist sets $F^d_{\nu,\mu}(K) \subset \mathbb{N}^2 \times \{x^d + \ldots + c_d : c_1, c_d \in K\}$ such that the set

$$\bigcup_{\nu,\mu,F} \bigcup_{\langle a,b,F\rangle \in F^d_{\nu,\mu}} \{x^\nu + ax^\mu + b\}$$

is finite and if $n, m \in \mathbb{N}, n > m, n_1 = n/(n,m), m_1 = m/(n,m), a, b \in K^*$, F is a monic factor of $x^{n_1} + ax^{m_1} + b$ in $K[x]$ of maximal possible degree $d \in \{1, 2\}$, $n_1 > 6$, then $(x^n + ax^m + b)F(x^{(n,m)})^{-1}$ is reducible over K if and only if there exists an integer l such that $\langle n/l, m/l\rangle =: \langle \nu, \mu\rangle \in \mathbb{N}^2$ and $a = u^{\nu-\mu}a_0$, $b = u^\nu b_0$, $F = u^{(\nu,\mu)d}F_0(x/u^{(\nu,\mu)})$, where $u \in K^*$, $\langle a_0, b_0, F_0\rangle \in F^d_{\nu,\mu}(K)$.

(paper 200=D14, for $d = 1$ already paper 197=D13)

48 (conjecture) For every field K such that $\operatorname{char} K > d$ every polynomial $F \in K[x_1, x_2]$ can be represented as $\sum_{\mu=1}^{d} f_\mu(\alpha_{\mu_1}x_1 + \alpha_{\mu_2}x_2)$, where $f_\mu \in K[z]$, $\alpha_{\mu_i} \in K$ $(1 \leqslant \mu \leqslant d, 1 \leqslant i \leqslant 2)$. (paper 208=E8)

49 (problem) Let K be a real quadratic field, β be a primitive integer of K, p a rational prime and $\mathcal{M}$ the set of Mahler measures of all algebraic numbers. Do the conditions $\beta \in \mathcal{M}$ and p splits in K imply $p\beta \in \mathcal{M}$ in general, or for $\beta = (1 + \sqrt{17})/2$, $p = 2$ in particular? (paper 211=C10)

50 (problem) Let K be a field of characteristic 0, n a positive integer. Is it true that a monic polynomial $f \in K[x]$ of degree n with exactly k distinct zeros is determined up to finitely many possibilities by any k of its non-zero proper coefficients? (paper 213)

51 (problem) Let $f \in \mathbb{Z}[x]$ have the leading coefficient positive and assume that the congruence $f(x) \equiv y^2 \pmod m$ is solvable for every positive integer m. Does there exist an odd integer $k > 0$ and integers $x_1, \ldots, x_k$ such that $\prod_{i=1}^{k} f(x_i)$ is a square? (paper 214=A16)

52 (problem) Let f be a non-singular binary form over $\mathbb{C}$. Can the existence of a non-trivial automorph of f be characterized in terms of invariants of f exclusively? (paper 219=E9)

53 (conjecture) The explicit value for the maximal order of the group of weak automorphs divided by the group of trivial automorphs of a binary form f of degree n defined over a field of characteristic π, where $0 < \pi \leqslant n$. (paper 219=E9)

54 (problem) How to compute $l(P)$ for cubic polynomials P over $\mathbb{R}$, in particular for $P(x) = 2x^3 + 3x^2 + 4$? Here $l(P) = \inf L(PG)$, where $L(F)$ is the length of F and G runs through all monic polynomials over $\mathbb{R}$. (paper 221=D17)

55 (problem) Is it true that $l(P) \in K(P)$ for all $P \in \mathbb{R}[x]$ with no zeros inside the unit circle? Here $l(P)$ has the meaning of Problem 54 and $K(P)$ is the field generated by the coefficients of P. (paper 221=D17)

56 (conjecture) Let k, n and b_i $(1 \leqslant i \leqslant k)$ be positive integers, and let a_i $(1 \leqslant i \leqslant k)$ be any integers. The number $N(n; a_1, b_1, \ldots, a_k, b_k)$ of solutions of the congruence

$$\sum_{i=1}^{k} a_i x_i \equiv 0 \pmod{n} \quad \text{in the box } 0 \leqslant x_i \leqslant b_i$$

satisfies the inequality $N(n; a_1, b_1, \ldots, a_k, b_k) \geqslant 2^{1-n} \prod_{i=1}^{k} (b_i + 1)$. (paper 222)

References

[1] J. H. Conway, A. J. Jones, *Trigonometric Diophantine equations* (*On vanishing sums of roots of unity*). Acta Arith. 30 (1976), 229–240.

[2] R. K. Guy, *Unsolved Problems in Number Theory*, Springer, New York 1981.

[3] A. Schinzel, *Ungelöste Problem* Nr. 30. Elem. Math. 14 (1959), 60–61.

[4] —, *Ungelöste Problem* Nr. 31. Elem. Math. 14 (1959), 82–83.

[5] W. Sierpiński, *Sur les décompositions de nombres rationnels en fractions primaires*. Mathesis 65 (1956), 16–32; see also Oeuvres choisies, T. I, Varsovie 1974, 169–184.

[6] E. Trost, *Ungelöste Problem* Nr. 14. Elem. Math. 11 (1956), 135.

[7] R. Wasén, *Remark on a problem of Schinzel*. Acta Arith. 29 (1976), 425–426.

Publication list of Andrzej Schinzel

Publication list of Andrzej Schinzel

A. Research papers

(papers not reviewed are marked with letters A, B, ...)

If a paper is reprinted in this collection, the number of its beginning page is put in the last column.

[12] *O liczbach pierwszych, dla których suma dzielników sześcianu jest pełnym kwadratem* (*On prime numbers such that the sums of the divisors of their cubes are perfect squares*), Wiadom. Mat. (2) 1 (1956), 203–204 (Polish), MR0110663 (22 #1538).

[13] *O pewnym przypuszczeniu dotyczącym rozkładów na sumę trzech kwadratów* (*On a certain conjecture concerning partitions into sums of three squares*), Wiadom. Mat. (2) 1 (1956), 205, MR0113856 (22 #4687).

[14] *Sur l'équation* $x^z - y^t = 1$, *où* $|x - y| = 1$, Ann. Polon. Math. 3 (1956), 5–6, MR0082506 (18,561d).

[15] (with W. Sierpiński) *Sur l'équation* $x^2+x+1 = 3y^2$, Colloq. Math. 4 (1956), 71–73, MR0077552 (17,1055j).

[16] *Generalization of a theorem of B. S. K. R. Somayajulu on the Euler's function* $\varphi(n)$, Ganita 5 (1954), 123–128, MR0083999 (18,791a).

[17] *Sur un problème concernant la fonction* $\varphi(n)$, Czechoslovak Math. J. 6 (1956), 164–165, MR0084005 (18,792b). 875

[18] (with W. Sierpiński) *Sur les sommes de quatre cubes*, Acta Arith. 4 (1958), 20–30, MR0095158 (20 #1664).

[19] (with Y. Wang) *A note on some properties of the functions* $\varphi(n)$, $\sigma(n)$ *and* $\theta(n)$, Ann. Polon. Math. 4 (1958), 201–213, MR0095149 (20 #1655); *Announcement*, Bull. Acad. Polon. Sci. Cl. III 4 (1956), 207–209, MR0079024 (18,17c); *Corrigendum*, Ann. Polon. Math. 19 (1967), 115, MR0209240 (35 #142).

[20] *Sur l'existence d'un cercle passant par un nombre donné de points aux coordonnées entières*, Enseignement Math. (2) 4 (1958), 71–72, MR0098059 (20 #4522). 17

[21] *Sur l'équation* $\varphi(x+k) = \varphi(x)$, Acta Arith. 4 (1958), 181–184, MR0106867 (21 #5597).

[22] (with W. Sierpiński) *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. 4 (1958), 185–208; *Erratum* 5 (1959), 259, MR0106202 (21 #4936). 1113

[23] *Sur un problème concernant le nombre de diviseurs d'un nombre naturel*, Bull. Acad. Polon. Sci. Sér. Sci. Math. Astr. Phys. 6 (1958), 165–167, MR0106203 (21 #4937).

[24] *Sur l'équation diophantienne* $x^x y^y = z^z$, Acta Scient. Mat. Univ. Szehuensis (1958), 81–83 (Chinese), Ref. Zh. 1959 #4439.

[24A] *Uwagi o zadaniu 420*, Matematyka XI-3 (1958), 60–62.

[25] *Sur les nombres composés n qui divisent* $a^n - a$, Rend. Circ. Mat. Palermo (2), 7 (1958), 37–41, MR0106201 (21 #4935).

[26] *Sur un probléme de P. Erdős*, Colloq. Math. 5 (1958), 198–204, MR0099950 (20 #6386). 903

[27] *Sur les diviseurs naturels des polynômes*, Matematiche (Catania) 12 (1957), 18–22, MR0130248 (24 #A114).

[28] *Démonstration d'une conséquence de l'hypothèse de Goldbach*, Compositio Math. 14 (1959), 74–76, MR0103870 (21 #2633).

[29] (with S. Gołąb) *Sur l'équation fonctionnelle* $f[x + y \cdot f(x)] = f(x) \cdot f(y)$, Publ. Math. Debrecen 6 (1959), 113–125, MR0107101 (21 #5828). 1314

[30] (with A. Mąkowski) *Sur l'équation indéterminée de R. Goormaghtigh*, Mathesis 68 (1959), 128–142, MR0118701 (22 #9472).

[31] *O okresowości pewnych ciągów liczb naturalnych* (*On the periodicity of certain sequences of natural numbers*), Wiadom. Mat. (2) 2 (1959), 269–272, MR0117182 (22 #7965).

[32] *Sur une conséquence de l'hypothèse de Goldbach*, Bulgar. Akad. Nauk. Izv. Mat. Inst. 4 (1959), no. 1, 35–38, MR0141628 (25 #5026).

[33] *Sur les sommes de trois carrés*, Bull. Acad. Polon. Sci. Sér. Sci. Math. Astr. Phys. 7 (1959), 307–310, MR0111728 (22 #2590). 18

[34] *Sur quelques propositions fausses de P. Fermat*, C. R. Acad. Sci. Paris 249 (1959), 1604–1605, MR0106875 (21 #5605).

[35] (with G. Szekeres) *Sur un probléme de M. Paul Erdős*, Acta Sci. Math. Szeged 20 (1959), 221–229, MR0112864 (22 #3710).

[36] (with A. Białynicki-Birula and J. Browkin) *On the representation of fields as finite unions of subfields*, Colloq. Math. 7 (1959), 31–32, MR0111739 (22 #2601).

[37] (with A. Wakulicz) *Sur l'équation* $\varphi(x + k) = \varphi(x)$ *II*, Acta Arith. 5 (1959), 425–426, MR0123506 (23 #A831).

[38] (with W. Sierpiński) *Sur les congruences* $x^x \equiv c \pmod m$ *et* $a^x \equiv b \pmod p$, Collect. Math. 11 (1959), 153–164, MR0113838 (22 #4670).

[39] *O równaniu diofantycznym* $\sum_{k=1}^{n} A_k x_k^{\vartheta_k} = 0$ (*On the Diophantine equation* $\sum_{k=1}^{n} A_k x_k^{\vartheta_k} = 0$), Prace Mat. 4 (1960), 45–51, MR0131395 (24 #A1247).; *Corrigendum*, Comment. Math. Prace Mat. 44 (2004), 283–284, MR2118015 (2005i:11045) 22

[40] *O równaniu* $x^4 + ax^2y^2 + by^4 = z^2$, Prace Mat. 4 (1960), 52–56, MR0131396 (24 #A1248).

[41] (with B. Rokowska) *Sur un problème de M. Erdős*, Elem. Math. 15 (1960), 84–85, MR0117188 (22 #7970).

[42] (with J. Browkin) *On the equation* $2^n - D = y^2$, Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys. 8 (1960), 311–318, MR0130215 (24 #A82).

[43] *On the congruence* $a^x \equiv b \pmod p$, Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys. 8 (1960), 307–309, MR0125070 (23 #A2377). 909

[44] *On some problems of the arithmetical theory of continued fractions*, Acta Arith. 6 (1961), 393–413, MR0125814 (23 #A3111). 131

[45] (with P. Erdős) *Distributions of the values of some arithmetical functions*, Acta Arith. 6 (1961), 473–485, MR0126410 (23 #A3706). 877

[46] *Remarks on the paper "Sur certaines hypothèses concernant les nombres premiers"*, Acta Arith. 7 (1961), 1–8, MR0130203 (24 #A70). 1134

[47] (with H. Davenport and D. J. Lewis) *Equations of the form* $f(x) = g(y)$, Quart. J. Math. Oxford Ser. (2) 12 (1961), 304–312, MR0137703 (25 #1152).

[48] *The intrinsic divisors of Lehmer numbers in the case of negative discriminant*, Ark. Mat. 4 (1962), 413–416, MR0139567 (25 #2999).

[49] *On the composite integers of the form* $c(ak+b)! \pm 1$, Nordisk Mat. Tidskr. 10 (1962), 8–10, MR0139565 (25 #2997). 912

[50] *On some problems of the arithmetical theory of continued fractions II*, Acta Arith. 7 (1962), 287–298, MR0139566 (25 #2998); *Corrigendum* 47 (1986), 295, MR0870671 (88b:11007). 149

[51] *Remark on the paper of K. Prachar "Über die kleinste Primzahl einer arithmetischen Reihe"*, J. Reine Angew. Math. 210 (1962), 121–122, MR0150115 (27 #118).

[52] (with W. Sierpiński) *Sur les triangles rectangulaires dont les deux cotés sont des nombres triangulaires*, Bull. Soc. Math. Phys. Serbie 13 (1961), 145–147, Zbl. 0131.28304.

[53] *On primitive prime factors of* $a^n - b^n$, Proc. Cambridge Philos. Soc. 58 (1962), 555–562, MR0143728 (26 #1280). 1036

[54] *Solution d'un problème de K. Zarankiewicz sur les suites de puissances consécutives de nombres irrationnels*, Colloq. Math. 9 (1962), 291–296, MR0141637 (25 #5035); *Correction* 12 (1964), 289, MR0174554 (30 #4755). 295

[55] *Remarque au travail de W. Sierpiński sur les nombres* $a^{2^n}+1$, Colloq. Math. 10 (1963), 137–138, MR0148601 (26 #6108).

[56] *Some unsolved problems on polynomials*, Neki nerešeni problemi u matematici, Matematička Biblioteka 25, Beograd 1963, 63–70, Zbl. 0122.25401. . 703

[57] *On primitive prime factors of Lehmer numbers* I, Acta Arith. 8 (1963), 213–223, MR0151423 (27 #1408). 1046

[58] *On primitive prime factors of Lehmer numbers* II, Acta Arith. 8 (1963), 251–257, MR0151424 (27 #1409). 1059

[59] *Reducibility of polynomials in several variables*, Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys. 11 (1963), 633–638, MR0159816 (28 #3032). 709

[60] *A remark on a paper of Bateman and Horn*, Math. Comp. 17 (1963), 445–447, MR0153647 (27 #3609). 1142

[61] (with W. Sierpiński) *Sur l'équation diophantienne* $(x^2-1)(y^2-1) = \left[\left(\frac{y-x}{2}\right)^2 - 1\right]^2$, Elem. Math. 18 (1963), 132–133, MR0163881 (29 #1180).

[62] (with M. Bhaskaran) *A new elementary estimation for the sum of real characters*, Prace Mat. 8 (1963), 99–102, MR0182614 (32 #97).

[63] (with A. Rotkiewicz) *Sur les nombres pseudopremiers de la forme* $ax^2 + bxy + cy^2$, C. R. Acad. Sci. Paris 258 (1964), 3617–3620, MR0161828 (28 #5032).

[64] (with H. Davenport) *Two problems concerning polynomials*, J. Reine Angew. Math. 214/215 (1964), 386–391, MR0162789 (29 #93); *Corrigendum* 218 (1965), 220, MR0174553 (30 #4754).

[65] (with J. Mikusiński) *Sur la réductibilité de certains trinômes*, Acta Arith. 9 (1964), 91–95, MR0163906 (29 #1205).

[66] (with H. Davenport and D. J. Lewis) *Polynomials of certain special types*, Acta Arith. 9 (1964), 107–116, MR0163880 (29 #1179). 27

[67] (with A. Mąkowski) *On the functions $\varphi(n)$ and $\sigma(n)$*, Colloq. Math. 13 (1964), 95–99, MR0173660 (30 #3870). 890

[68] (with H. Zassenhaus) *A refinement of two theorems of Kronecker*, Michigan Math. J. 12 (1965), 81–85, MR0175882 (31 #158). 175

[69] *On Hilbert's Irreducibility Theorem*, Ann. Polon. Math. 16 (1965), 333–340, MR0173658 (30 #3868). 839

[70] *On the composite Lehmer numbers with prime indices*, Prace Mat. 9 (1965), 95–103, MR0174520 (30 #4721).

[71] (with A. Mąkowski) *Sur l'équation indéterminée de R. Goormaghtigh* II, Mathesis 70 (1965), 94–96, Zbl. 0127.01903.

[72] (with H. Davenport) *A note on sequences and subsequences*, Elem. Math. 20 (1965), 63–64, Zbl. 0132.25101.

[73] *On the reducibility of polynomials and in particular of trinomials*, Acta Arith. 11 (1965), 1–34, MR0180549 (31 #4783); *Errata*, ibid., 491, MR0197448 (33 #5613); *Corrigenda*, Acta Arith. 16 (1969), 159. 301

[74] (with B. J. Birch, S. Chowla and M. Hall Jr.) *On the difference $x^3 - y^2$*, Norske Vid. Selsk. Forh. (Trondheim) 38 (1965), 65–69, MR0186620 (32 #4079).

[75] *Uwaga do artykułu H. Steinhausa "Pogadanka (trochę historyczna)"* (*A remark to the paper by H. Steinhaus "A chat (slightly historical)"*), Wiadom. Mat. (2) 8 (1965), 143–144, Zbl. 0149.28202.

[76] (with S. Hartman, J. Mycielski, and S. Rolewicz) *Concerning the characterization of linear spaces*, Colloq. Math. 13 (1965), 199–208, MR0183808 (32 #1284).

[77] (with H. Davenport) *A combinatorial problem connected with differential equations*, Amer. J. Math. 87 (1965), 684–694, MR0190010 (32 #7426). .. 1327

[78] (with W. Sierpiński) *Sur les puissances propres*, Bull. Soc. Roy. Sci. Liège 34 (1965), 550–554, MR0186649 (32 #4107).

[79] *On a theorem of Bauer and some of its applications*, Acta Arith. 11 (1966), 333–344, MR0190130 (32 #7544); *Corrigendum* 12 (1967), 425, MR0210684 (35 #1570). 179

[80] (with D. J. Lewis and H. Zassenhaus) *An extension of the theorem of Bauer and polynomials of certain special types*, Acta Arith. 11 (1966), 345–352, MR0190131 (32 #7545). 190

[81] (with H. Davenport and D. J. Lewis) *Quadratic Diophantine equations with a parameter*, Acta Arith. 11 (1966), 353–358, MR0184902 (32 #2373).

[82] (with H. Davenport) *A note on certain arithmetical constants*, Illinois J. Math. 10 (1966), 181–185, MR0188193 (32 #5632).

[83] *On sums of roots of unity. Solution of two problems of R. M. Robinson*, Acta Arith. 11 (1966), 419–432, MR0201418 (34 #1302). 197

[84] (with H. Davenport) *Diophantine Approximation and sums of roots of unity*, Math. Ann. 169 (1967), 118–135, MR0205926 (34 #5751).

[85] *Reducibility of polynomials of the form $f(x) - g(y)$*, Colloq. Math. 18 (1967), 213–218, MR0220703 (36 #3755). 715

[86] *Reducibility of polynomials and covering systems of congruences*, Acta Arith. 13 (1967), 91–101, MR0219515 (36 #2596). 333

[87] *On two theorems of Gelfond and some of their applications*, Acta Arith. 13 (1967), 177–236, MR0222034 (36 #5086); *Corrigendum* 16 (1969), 101, MR0246840 (40 #109); *Addendum* 56 (1996), 181, MR1075643. 1145

[88] (with A. Grużewski) *Sur les itérations d'une fonction arithmétique*, Prace Mat. 11 (1968), 279–282, MR0224548 (37 #147).

[89] *On sums of four cubes of polynomials*, J. London Math. Soc. 43 (1968), 143–145, MR0223340 (36 #6388).

[90] (with L. P. Postnikova) *O primitivnyh delitelyah vyraženiya $a^n - b^n$ v polyah algebraičeskih čisel* (*Primitive divisors of the expression $a^n - b^n$ in algebraic number fields*), Mat. Sb. (N.S.) 75 (1968), 171–177; Math. USSR-Sb. 4 (1968), 153–159, MR0223330 (36 #6378).

[91] *On primitive prime factors of Lehmer numbers* III, Acta Arith. 15 (1968), 49–70, MR0232744 (38 #1067); *Corrigendum* 16 (1969), 101, MR0246840 (40 #109). 1066

[92] *An improvement of Runge's theorem on Diophantine equations*, Comment. Pontificia Acad. Sci. 2 (1969), No. 20, MR0276174 (43 #1922). 36

[93] (with W. Narkiewicz) *Ein einfacher Beweis des Dedekindschen Differentensatzes*, Colloq. Math. 20 (1969), 65–66, MR0240071 (39 #1425).

[94] *Remarque sur le travail précédent de T. Nagell*, Acta Arith. 15 (1969), 245–246, MR0246854 (40 #123).

[95] *A remark on a paper of Mordell*, J. London Math. Soc. (2) 1 (1969), 765–766, MR0249358 (40 #2603).

[96] *Reducibility of lacunary polynomials* I, Acta Arith. 16 (1969), 123–159, MR0252362 (40 #5583). 344

[97] *Reducibility of lacunary polynomials* II, Acta Arith. 16 (1970), 371–392, MR0265323 (42 #233). 381

[98] *A refinement of a theorem of Gerst on power residues*, Acta Arith. 17 (1970), 161–168, MR0284417 (44 #1644).

[99] (with A. Baker) *On the least integers represented by the genera of binary quadratic forms*, Acta Arith. 18 (1971), 137–144, MR0319896 (47 #8437).

[100] (with J. Wójcik) *A note on the paper "Reducibility of lacunary polynomials I"*, Acta Arith. 19 (1971), 195–201, MR0289463 (44 #6653). 403

[101] (with W. Brostow) *On interesting walks in a graph*, J. Statist. Phys. 4 (1972), 103–110, MR0309794 (46 #8899).

[102] *Integer points on conics*, Comment. Math. Prace Mat. 16 (1972), 133–135, *Erratum* 17 (1973), 305, MR0321868 (48 #233).

[103] (with M. Fried) *Reducibility of quadrinomials*, Acta Arith. 21 (1972), 153–171, MR0313219 (47 #1774); *Corrigendum and addendum*, ibid. 99 (2001), 409–410, MR1845693. 720

[104] *On a theorem of Bauer and some of its applications* II, Acta Arith. 22 (1973), 221–231, MR0330105 (48 #8443). 210

[105] *On the product of the conjugates outside the unit circle of an algebraic number*, Acta Arith. 24 (1973), 385–399, MR0360515 (50 #12963); *Addendum* 26 (1975), 329–331, MR0371853 (51 #8070). 221

[106] *A contribution to combinatorial geometry*, Demonstratio Math. 6 (1973), 339–342, MR0350607 (50 #3099).

[107] *On two conjectures of P. Chowla and S. Chowla concerning continued fractions*, Ann. Mat. Pura Appl. (4) 98 (1974), 111–117, MR0340187 (49 #4943). 161

[108] *Primitive divisors of the expression $A^n - B^n$ in algebraic number fields*, J. Reine Angew. Math. 268/269 (1974), 27–33, MR0344221 (49 #8961). .. 1090

[109] *A general irreducibility criterion*, J. Indian Math. Soc. (N.S.) 37 (1973), 1–8, MR0429849 (55 #2859). 739

[110] *On power residues and exponential congruences*, Acta Arith. 27 (1975), 397–420, MR0379432 (52 #337). 915

[111] *On linear dependence of roots*, Acta Arith. 28 (1975), 161–175, MR0389835 (52 #10665). 238

[112] *Traces of polynomials in algebraic numbers*, Norske Vid. Selsk. Skr. (Trondheim) 1975, no. 6, 3 pp., MR0412143 (54 #270)

[113] (with D. M. Goldfeld) *On Siegel's zero*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) 2 (1975), 571–583, MR0404213 (53 #8016). 1199

[114] *On the number of irreducible factors of a polynomial*, in: Topics in Number Theory, Colloq. Math. Soc. János Bolyai 13, North-Holland, Amsterdam 1976, 305–314, MR0435027 (55 #7989).

[115] (with R. Tijdeman) *On the equation $y^m = P(x)$*, Acta Arith. 31 (1976), 199–204, MR0422150 (54 #10142). 41

[116] (with J. Browkin and B. Diviš) *Addition of sequences in general fields*, Monatsh. Math. 82 (1976), 261–268, MR0432581 (55 #5568).

[117] *Abelian binomials, power residues and exponential congruences*, Acta Arith. 32 (1977), 245–274, MR0429819 (55 #2829); *Addendum* 36 (1980), 101–104, MR0576586 (81g:12005). 939

[118] (with T. Shorey, A. J. van der Poorten and R. Tijdeman) *Applications of the Gel′fond-Baker method to Diophantine equations*, in: Transcendence Theory: Advances and Applications (ed. by A. Baker and D. Masser), Academic Press, London 1977, 59–77, MR0472689 (57 #12383).

[119] (with H. L. Montgomery) *Some arithmetic properties of polynomials in several variables*, ibid., 195–203, MR0472757 (57 #12447). 747

[120] *An analogue of Harnack's inequality for discrete superharmonic functions*, Demonstratio Math. 11 (1978), 47–60, MR0486564 (58 #6287). 1338

[121] *Reducibility of lacunary polynomials* III, Acta Arith. 34 (1978), 227–266, MR0506160 (58 #22012). 409

[122] *An inequality for determinants with real entries*, Colloq. Math. 38 (1978), 319–321, MR0485920 (58 #5714). 1347

[123] (with G. Baron) *An extension of Wilson's theorem*, C. R. Math. Rep. Acad. Sci. Canada 1 (1979), 115–118, MR0519537 (80e:05025). 971

[124] (with R. Perlis) *Zeta function and the equivalence of integral forms*, J. Reine Angew. Math. 309 (1979), 176–182, MR0542046 (80j:12008). 47

[125] (with L. A. Rubel and H. Tverberg) *On difference polynomials and hereditarily irreducible polynomials*, J. Number Theory 12 (1980), 230–235, MR0578817 (81i:12024). 755

[126] (with D. J. Lewis) *Quadratic Diophantine equations with parameters*, Acta Arith. 37 (1980), 133–141, MR0598871 (81m:10030). 54

[127] (with H. P. Schlickewei and W. M. Schmidt) *Small solutions of quadratic congruences and small fractional parts of quadratic forms*, Acta Arith. 37 (1980), 241–248, MR0598879 (81m:10063).

[128] *On the relation between two conjectures on polynomials*, Acta Arith. 38 (1980), 285–322, MR0602194 (82g:12004). 1154

[129] (with J. Browkin) *On Sylow 2-subgroups of K_2O_F for quadratic number fields F*, J. Reine Angew. Math. 331 (1982), 104–113, MR0647375 (83g:12011). 253

[130] (with K. Győry and P. Kiss) *On Lucas and Lehmer sequences and their applications to Diophantine equations*, Colloq. Math. 45 (1981), 75–80, MR0652603 (83g:10009).

[131] (with J. W. S. Cassels) *Selmer's conjecture and families of elliptic curves*, Bull. London Math. Soc. 14 (1982), 345–348, MR0663485 (84d:14028). . 62

[132] *Families of curves having each an integer point*, Acta Arith. 40 (1982), 399–420, MR0667049 (83k:12003). 67

[132A] (with F. Laubie) *Sur le théorème de Gordan-Igusa*, Publ. Dept. Math. Limoges, Fasc. 4 (1982), 50–53.

[133] *An application of Hilbert's irreducibility theorem to Diophantine equations*, Acta Arith. 41 (1982), 203–211, MR0674833 (83k:12004).

[134] (with E. Dobrowolski and W. Lawton) *On a problem of Lehmer*, in: Studies in Pure Mathematics. To the memory of Paul Turán (ed. by P. Erdős), Birkhäuser, Basel 1983, 135–144, MR0820217 (87e:11120).

[134A] *Généralisation d'un résultat de Smyth aux polynômes à plusieurs variables*, Publ. Math. Univ. Pierre et Marie Curie 64 (1983/84), Fasc. 1, exposé no. 4.

[135] *On the number of irreducible factors of a polynomial* II, Ann. Polon. Math. 42 (1983), 309–320, MR0728089 (86k:11056).

[136] (with J. Wróblewski) *On ideals in the ring of polynomials in one variable over a Dedekind domain*, Studia Sci. Math. Hungar. 16 (1981), 415–425, MR0729304 (84m:13021).

[137] *Hasse's principle for systems of ternary quadratic forms and for one biquadratic form*, Studia Math. 77 (1983), 103–109, MR0743067 (85h:11018). 87

[138] *Reducibility of lacunary polynomials* IV, Acta Arith. 43 (1984), 313–315, MR0738143 (85g:11091). 447

[139] *Reducibility of lacunary polynomials* V, Acta Arith. 43 (1984), 425–440, MR0756292 (86d:11083).

[140] *The number of zeros of polynomials in valuation rings of complete discretely valued fields*, Fund. Math. 124 (1984), 41–97, MR0818607 (87g:12005).

[141] *Reducibility of polynomials in several variables* II, Pacific J. Math. 118 (1985), 531–563, MR0789192 (86i:12005).

[142] *The fundamental lemma of Brun's sieve in a new setting*, Rocky Mountain J. Math. 15 (1985), 573–578, MR0823268 (87h:11087).

[143] *Systems of exponential congruences*, Demonstratio Math. 18 (1985), 377–394, MR0816042 (87c:11036). 975

[144] *A non-standard metric in the group of reals*, Colloq. Math. 50 (1986), 241–248, MR0857859 (88h:54057).

[145] *Reducibility of lacunary polynomials VI*, Acta Arith. 47 (1986), 277–293, MR0870670 (88e:11104).

[146] *Reducibility of lacunary polynomials* VII, Monatsh. Math. 102 (1986), 309–337, MR0866132 (88e:11105); *Errata*, Acta Arith. 53 (1989), 95, MR1045457 (91a:11049).

[147] (with A. Rotkiewicz) *On the Diophantine equation* $x^p + y^{2p} = z^2$, Colloq. Math. 53 (1987), 147–153, MR0890851 (88e:11017).

[148] *A decomposition of integer vectors* I, Bull. Polish Acad. Sci. Math. 35 (1987), 155–159, MR0908163 (88m:11050).

[149] *On the number of terms of a power of a polynomial*, Acta Arith. 49 (1987), 55–70, MR0913764 (89a:12007). 450

[150] *Second order strong divisibility sequences in an algebraic number field*, Arch. Math. (Brno) 23 (1987), 181–186, MR0930320 (89c:11028).

[151] *Reducibility of lacunary polynomials* VIII, Acta Arith. 50 (1988), 91–106, MR0945276 (89f:11144).

[152] *A decomposition of integer vectors* III, Bull. Polish Acad. Sci. Math. 35 (1987), 693–703, MR0961707 (90m:11096).

[153] (with E. Wirsing) *Multiplicative properties of the partition function*, Proc. Indian Acad. Sci. Math. Sci. 97 (1987), 297–303, MR0983622 (90b:11102). 1211

[154] *Reducibility of lacunary polynomials* IX, in: New Advances in Transcendence Theory (ed. by A. Baker), Cambridge Univ. Press, Cambridge 1988, 313–336, MR0972008 (90a:11117).

[155] (with M. Misiurewicz) *On n numbers on a circle*, Hardy-Ramanujan J. 11 (1988), 30–39, MR1011768 (90i:11024).

[155A] *Postscript to the paper A. Rotkiewicz and W. Złotkowski "On the Diophantine equation* $1 + p^{\alpha_1} + \ldots + p^{\alpha_k} = y^2$*"*, in: Number Theory, Colloq. Math. Soc. János Bolyai 51, North-Holland, Amsterdam 1989, 929–936, MR1058252 (91e:11032).

[156] *Reducibility of lacunary polynomials* X, Acta Arith. 53 (1989), 47–97, MR1045456 (91e:11119).

[157] *An analog of Hilbert's irreducibility theorem*, Number Theory (ed. by R. A. Mollin), Walter de Gruyter, Berlin 1990, 509–514, MR1106684 (92h:12003).

[158] (with J. L. Nicolas) *Localisation des zéros de polynômes intervenant en théorie du signal*, in: Cinquante ans de polynômes, Lecture Notes in Math. 1415, Springer, Berlin 1990, 167–179, MR1044112 (90k:30007).

[159] *Un critère d'irréductibilité de polynômes*, ibid., 212–224, MR1044116 (91k:12002).

[160] (with P. Erdős) *On the greatest prime factor of* $\prod_{k=1}^{x} f(k)$, Acta Arith. 55 (1990), 191–200, MR1061638 (91h:11100).

[161] *Postscript to the paper of A. Mąkowski "On Stroeker's equation"*, in: Algebra and Number Theory (ed. by A. Grytczuk), Pedagog. Univ. Zielona Góra, Zielona Góra 1990, 41–42, MR1114364 (92f:11046).

[162] *Special Lucas sequences, including the Fibonacci sequence modulo a prime*, in: A Tribute to Paul Erdős (ed. by A. Baker, B. Bollobás and A. Hajnal), Cambridge Univ. Press, Cambridge 1990, 349–357, MR1117027 (92f:11029).

[163] *Reducibility of lacunary polynomials* XI, Acta Arith. 57 (1991), 165–175, MR1092768 (92f:11139).

[164] (with S. Chaładus) *A decomposition of integer vectors* II, Pliska Stud. Math. Bulgar. 11 (1991), 15–23, MR1106550 (92g:11065). 1249

[165] *A class of polynomials*, Math. Slovaca 41 (1991), 295–298, MR1126666 (92m:11024). 846

[166] *A decomposition of integer vectors* IV, J. Austral. Math. Soc. Ser. A 51 (1991), 33–49, MR1119686 (92f:11086). 1259

[167] (with H. Niederreiter and L. Somer) *Maximal frequencies of elements in second-order linear recurring sequences over a finite field*, Elem. Math. 46 (1991), 139–143, MR1119645 (92k:11017).

[168] (with A. Choudhry) *On the number of terms in the irreducible factors of a polynomial over* $\boldsymbol{Q}$, Glasgow Math. J. 34 (1992), 11–15, MR1145626 (92m:11022).

[168A] *O pewnym zadaniu Wacława Sierpińskiego* (*On certain problem of Wacław Sierpiński*), Gradient 1 (1992), No. 2, 6–9.

[169] *Differences between values of a quadratic form*, Acta Math. Univ. Comenian. (N.S.) 61 (1992), 91–93, MR1205863 (93m:11028).

[170] (with U. Zannier) *Distribution of solutions of Diophantine equations* $f_1(x_1)f_2(x_2) = f_3(x_3)$*, where* f_i *are polynomials*, Rend. Sem. Mat. Univ. Padova 87 (1992), 39–68, MR1183901 (93h:11040).

[171] (with A. Grytczuk) *On Runge's theorem about Diophantine equations*, in: Sets, Graphs and Numbers, Colloq. Math. Soc. János Bolayi 60, North Holland, Amsterdam 1992, 329–356, MR1218200 (94i:11025). 93

[172] (with J. Wójcik) *On a problem in elementary number theory*, Math. Proc. Cambridge Philos. Soc. 112 (1992), 225–232, MR1171159 (93e:11006). .. 987

[173] *On an analytic problem considered by Sierpiński and Ramanujan*, in: New Trends in Probability and Statistics, vol. 2, VSP Utrecht 1992, 165–171, MR1198499 (93j:11062). 1217

[174] *An extension of the theorem on primitive divisors in algebraic number fields*, Math. Comp. 61 (1993), 441–444, MR1189523 (93k:11107). 1098

[175] *On reducible trinomials*, Dissert. Math. (Rozprawy Mat.) 329 (1993), 83 pp., MR1254093 (95d:11146); *Errata*, Acta Arith. 73 (1995), 399–400, MR1366047. 466

[176] (with K. Győry) *On a conjecture of Posner and Rumsey*, J. Number Theory 47 (1994), 63–78, MR1273456 (95k:11027). 549

[177] (with U. Zannier) *Distribution of solutions of Diophantine equations* $f_1(x_1)f_2(x_2) = f_3(x_3)$*, where* f_i *are polynomials* II, Rend. Sem. Mat. Univ. Padova 92 (1994), 29–46, MR1320476 (96a:11032).

[178] (with T. Šalat) *Remarks on maximum and minimum exponents in factoring*, Math. Slovaca 44 (1994), 505–514, MR1338424 (96f:11017a); *Errata*, ibid. 45 (1995), 317, MR1361826 (96f:11017b).

[179] (with J. Browkin) *On integers not of the form* $n - \varphi(n)$, Colloq. Math. 68 (1995), 55–58, MR1311762 (95m:11106). 895

[180] (with U. Zannier) *The least admissible value of the parameter in Hilbert's Irreducibility Theorem*, Acta Arith. 69 (1995), 293–302, MR1316481 (96f:12002). 849

[181] (with I. Z. Ruzsa) *An application of Kloosterman sums*, Compositio Math. 96 (1995), 323–330, MR1327149 (96a:11099).

[181A] (with U. Zannier) *Appendix to the paper of M. Nair and A. Perelli "A sieve fundamental lemma for polynomials in two variables"*, in: Analytic Number Theory, Progr. Math. 139, Birkhäuser Boston 1996, 685–702, MR1409386 (97j:11045).

[182] *O pokazatel′nyh sravneniyah* (*On exponential congruences*), Diofantovy Priближeniya, Mat. Zapiski 2, 121–126, MGU, Moskva 1996, Ref. Zh. 1998 #1A149. 996

[183] (with J. Browkin, M. Filaseta and G. Greaves) *Squarefree values of polynomials and the abc-conjecture*, in: Sieve Methods, Exponential Sums, and their Applications in Number Theory, London Math. Soc. Lecture Notes Ser. 237, Cambridge Univ. Press, Cambridge 1996, 65–85, MR1635726 (99d:11101).

[184] *On the Mahler measure of polynomials in many variables*, Acta Arith. 79 (1997), 77–81, MR1438118 (97k:11036).

[185] *Triples of positive integers with the same sum and the same product*, Serdica Math. J. 22 (1996), 587–588, MR1483607 (98g:11033).

[186] *A class of algebraic numbers*, in: Number Theory, Tatra Mt. Math. Publ. 11, Bratislava 1997, 35–42, MR1475503 (98i:11089). 264

[187] *On homogeneous covering congruences*, Rocky Mountain J. Math. 27 (1997), 335–342, MR1453107 (98b:11003).

[188] *On pseudosquares*, New Trends in Probability and Statistics, vol. 4, VSP Utrecht 1997, 213–220, MR1653611 (99i:11071).

[189] (with D. Barsky and J. P. Bézivin) *Une caractérisation arithmétique de suites récurrentes linéaires*, J. Reine Angew. Math. 494 (1998), 73–84, MR1604460 (99j:11011). 1001

[190] (with I. Aliev and S. Kanemitsu) *On the metric theory of continued fractions*, Colloq. Math. 77 (1998), 141–146, MR1622796 (99d:11087).

[191] *A property of the unitary convolution*, Colloq. Math. 78 (1998), 93–96, MR1658143 (99k:11010).

[192] *On Pythagorean triangles*, Ann. Math. Sil. 12 (1998), 31–33, MR1673056 (99k:11044).

[193] (with J. Urbanowicz and P. van Wamelen) *Class numbers and short sums of Kronecker symbols*, J. Number Theory 78 (1999), 62–84, MR1706925 (2000g:11103). 1224

[194] (with S. Chaładus) *On a linear Diophantine equation*, Österreich. Akad. Wiss. Math.-Natur. Kl. Sitzungsber. II 207 (1998), 95–101, MR1749915 (2001e:11026).

[194A] *Remark on a paper of T. W. Cusick*, Biuletyn WAT 48 (1999), No. 10, 5–9.

[195] *Reducibility of lacunary polynomials* XII, Acta Arith. 90 (1999), 273–289, MR1715532 (2001b:11099). 563

[196] (with A. Rotkiewicz) *On Lucas pseudoprimes with a prescribed value of the Jacobi symbol*, Bull. Polish Acad. Sci. Math. 48 (2000), 77–80, MR1751157 (2001a:11013).

[197] *On reducible trinomials* II, Publ. Math. Debrecen 56 (2000), 575–608, MR1766001 (2001k:11207); *Corrigendum*, Acta Arith. 115 (2004), 403, MR2099832. 580

[198] *On sums of three unit fractions with polynomial denominators*, Funct. Approx. Comment. Math. 28 (2000), 187–194, MR1824003 (2002a:11029). . 116

[199] *On the greatest common divisor of two univariate polynomials* II, Acta Arith. 98 (2001), 95–106, MR1831458 (2002k:12002); *Corrigendum*, Acta Arith. 115 (2004), 403, MR2099832. 646

[200] *On reducible trinomials* III, Period. Math. Hungar. 43 (2001), 43–69, MR1830565 (2002g:11145). 605

[201] (with A. Paszkiewicz) *On the least prime primitive root modulo a prime*, Math. Comp. 71 (2002), 1307–1321, MR1898759 (2003d:11006).

[202] *On the greatest common divisor of two univariate polynomials* I, in: A Panorama of Number Theory or the View from Baker's Garden (ed. by G. Wüstholz), Cambridge Univ. Press, Cambridge 2002, 337–352, MR1975461 (2004a:11021). 632

[203] *On a decomposition of polynomials in several variables* II, Colloq. Math. 92 (2002), 67–79, MR1899238 (2003i:11048).

[204] (with W. M. Schmidt) *Comparison of L^1- and L^∞-norms of squares of polynomials*, Acta Arith. 104 (2002), 283–296, MR1914723 (2003f:11035). ... 1350

[204A] *Appendix to the paper "Diophantine Equations and Bernoulli Polynomials" by Yu. F. Bilu, B. Brindza, P. Kirschenhofer, Á. Pintér and R. F. Tichy*, Compositio Math. 131 (2002), 185–187, MR1898434 (2003a:11025).

[205] *An extension of some formulae of Lerch*, Acta Math. Inform. Univ. Ostraviensis 10 (2002), 111–116, MR1943030 (2003i:11050).

[206] *A property of polynomials with an application to Siegel's lemma*, Monatsh. Math. 137 (2002), 239–251, MR1942622 (2004h:11022). 1274

[207] (with A. Paszkiewicz) *Numerical calculation of the density of prime numbers with a given least primitive root*, Math. Comp. 71 (2002), 1781–1797, MR1933055 (2003g:11109).

[208] *On a decomposition of polynomials in several variables*, J. Théor. Nombres Bordeaux 14 (2002), 647–666, MR2040699 (2005e:11031). 760

[209] (with M. Skałba) *On power residues*, Acta Arith. 108 (2003), 77–94, MR1971083 (2005a:11005). 1012

[210] (with M. Filaseta) *On testing the divisibility of lacunary polynomials by cyclotomic polynomials*, Math. Comp. 73 (2004), 957–965, MR2031418 (2004m:11207).

[211] *On values of the Mahler measure in a quadratic field* (*solution of a problem of Dixon and Dubickas*), Acta Arith. 113 (2004), 401–408, MR2079812 (2005h:11242). 272

[212] *On the congruence* $u_n \equiv c \pmod{\mathfrak{p}}$*, where* u_n *is a recurring sequence of the second order*, Acta Acad. Paedagog. Agriensis Sect. Mat. (N.S.) 30 (2003), 147–165, MR2054724 (2005a:11004).

[213] (with K. Győry, L. Hajdu, Á. Pintér) *Polynomials determined by a few of their coefficients*, Indag. Math. (N.S.) 15 (2004), 209–221, MR2071857 (2005d:11036).

[214] (with M. Skałba) *On equations* $y^2 = x^n + k$ *in a finite field*, Bull. Pol. Acad. Sci. Math. 52 (2004), 223–226, MR2127058 (2005j:11046). 124

[215] (with Th. Bolis) *Identities which imply that a ring is Boolean*, Bull. Greek Math. Soc. 48 (2003), 1–5, MR2230423 (2007a:16042).

[216] (with I. Aliev, W. M. Schmidt) *On vectors whose span contains a given linear subspace*, Monatsh. Math. 144 (2005), 177–191, MR2130272 (2005m:11128). 1288

[217] *Self-inversive polynomials with all zeros on the unit circle*, Ramanujan J. 9 (2005), 19–23, MR2166374 (2006d:30008).

[218] (with S. Kanemitsu, Y. Tanigawa) *Sums involving the Hurwitz zeta-function values*, in: Zeta functions, topology and quantum physics, Dev. Math. 14, Springer, New York 2005, 81–90, MR2179274 (2006g:11179).

[219] *On weak automorphs of binary forms over an arbitrary field*, Dissert. Math. (Rozprawy Mat.) 434 (2005), MR2229645 (2007a:11051). 779

[220] *Reducibility of symmetric polynomials*, Bull. Pol. Acad. Sci. Math. 53 (2005), 251–258, MR2213603 (2007b:12005). 828

[221] *On the reduced length of a polynomial with real coefficients*, Funct. Approx. Comment. Math. 35 (2006), 271–306, MR2271619. 658

[222] (with M. Zakarczemny) *On a linear homogeneous congruence*, Colloq. Math. 106 (2006), 283–292.

[223] *Reducibility of a special symmetric form*, Acta Math. Univ. Ostraviensis 14 (2006), 71–74.

B.1. Lectures on own or joint work

[1] *Reducibility of lacunary polynomials*, in: 1969 Number Theory Institute, Proc. Sympos. Pure Math. 20, Amer. Math. Soc., Providence 1971, 135–149, MR0323749 (48 #2105).

[2] *Reducibility of polynomials*, in: Computers in Number Theory (ed. by B. J. Birch and A. O. L. Atkin), Academic Press, London 1971, 73–75, MR0314733 (47 #3285).

[3] *Reducibility of polynomials*, in: Actes du Congrès International des Mathèmaticiens (Nice 1970), t. I, Gauthier-Villars, Paris 1971, 491–496, MR0424768 (54 #12726).
[4] *Privodimost' četyrehčlenov*, Trudy Mat. Inst. Steklov. 132 (1973), 143–144, MR0332707 (48 #11033); English version (*Reducibility of quadrinomials*): Proc. Steklov Inst. Math. 132 (1973), 163–165, MR0369228 (51 #5463).
[5] *Les extensions pures et les résidus des puissances*, Astérisque 24–25 (1975), 69–74, MR0379433 (52 #338).
[6] *Les résidus de puissances et les congruences exponentielles*, Astérisque 41–42 (1977), 103–109, MR0447173 (56 #5488).
[7] *Diophantine equations with parameters*, in: Journées Arithmétiques 1980, London Math. Soc. Lecture Notes 56, Cambridge 1982, 211–217, Zbl. 0539.10017.
[8] *Le nombre de zéros des polynômes dans les anneaux de valuation des corps complets valués discrètement*, Groupe d'étude d'Analyse Ultramétrique (Y. Amice, G. Christol, P. Robba), 9^{e} année 1981/82, exposé no. 6, Inst. Henri Poincaré, Paris, 1983, MR0720554 (85c:11118).
[9] *Reducible lacunary polynomials*, Séminaire de Théorie des Nombres Univ. de Bordeaux, Année 1983–1984, exposé no 29, Univ. Bordeaux I, Talence, 1984, MR0784075.
[10] *On reducible trinomials*, Publ. Math. Univ. Pierre et Marie Curie no. 108 (1993), exposé no. 10.

B.2. Other papers

[1] (with W. Sierpiński) *O równaniu* $x^2 - 2y^2 = k$, Wiadom. Mat. (2) 7 (1964), 229–232, MR0184904 (32 #2375).
[2] (with S. Bergman et al.) *Kazimierz Zarankiewicz*, Colloq. Math. 12 (1964), 277–288, MR0174454 (30 #4658); Polish version — Wiadom. Mat. (2) 9 (1967), 175–185, MR0209106 (35 #10).
[3] *Liczb teoria*, Wielka Encyklopedia Powszechna PWN 6, Warszawa 1965, 501–503.
[4] *O różnych działach teorii liczb*, Wiadom. Mat. (2) 9 (1967), 187–197, MR0227081 (37 #2666); Bulgarian version — Fiz.-Mat. Spis. Bulgar. Akad. Nauk. 13 (46) (1970), 130–138, MR0396377 (53 #244).
[5] *O pracach Michała Kaleckiego z teorii liczb*, Ekonomista 1970, 1021–1022.
[6] *Równania diofantyczne*, Wiadom. Mat. (2) 12 (1971), 227–232, MR0453627 (56 #11889); Serbian version — Uvodenje mladih u naučni rad VI, Matematička Biblioteka 41, Beograd 1965, 29–34.
[7] *Życiorys Wacława Sierpińskiego*, Wiadom. Mat. (2) 12 (1971), 303–308, MR0396189 (53 #57).
[8] *Wacław Sierpiński's papers on the theory of numbers*, Acta Arith. 21 (1972), 7–13, MR0300846 (46 #9b); French version—W. Sierpiński "Oeuvres choisies", t. I, Warszawa 1973, 65–72, MR0414302 (54 #2405); Polish version—Wiadom. Mat. (2) 26 (1984), 24–31.
[9] (with J. Oderfeld) *O pracach matematycznych Michała Kaleckiego*, Wiadom. Mat. (2) 16 (1973), 71–73, MR0453459 (56 #11722).

[10] *Postęp w teorii liczb w latach 1966–1978*, Wiadom. Mat. (2) 22 (1979), 1–11, MR0571455 (83e:10002).

[11] *O pracach H. Iwańca dotyczących metody sita*, Wiadom. Mat. 22 (1979), 13–16, MR0571456 (82f:01140).

[12] *Ułamki łańcuchowe*, Delta nr 5 (65) (1979), 1–3.

[13] *Wacław Sierpiński a szkoła średnia*, Matematyka 33 (1980), 68–69.

[14] *Commentary to the Bulgarian edition of Dirichlet's "Vorlesungen über Zahlentheorie"*, Sofia 1980, 567–578.

[15] *Wacław Sierpiński*, Matematyka 35 (1982), 126–128.

[16] *Paul Turán's work in number theory*, in: Topics in Classical Number Theory, Colloq. Math. Soc. János Bolyai 34, North-Holland 1984, 31–48, MR0781134 (86e:11002).

[17] *Związki między własnościami lokalnymi a globalnymi w teorii równań diofantycznych*, Wiadom. Mat. (2) 25 (1984), 169–175, MR0786112 (87b:11027).

[18] *Rola Wacława Sierpińskiego w historii matematyki polskiej*, Wiadom. Mat. (2) 26 (1984), 1–9, MR0778895 (86i:01054a).

[19] *Teoria rozmieszczenia liczb pierwszych*, Delta nr 4 (136) 1985, 12.

[20] *Propozycje terminologiczne*, Wiadom. Mat. (2) 27 (1986), 148–149, MR0888159 (88f:00021).

[21] *Sprostowanie*, Matematyka 40 (1987), 271.

[22] *50 tomów Acta Arithmetica*, Wiadom. Mat. 28 (1988), 81–83, MR0986063 (90c:01046).

[23] *Rozwój teorii liczb pierwszych w XIX w.*, Matematyka XIX wieku (ed. by S. Fudali), Szczecin 1988, 29–33.

[24] *Postęp w teorii liczb w latach 1978–1988*, Wiadom. Mat. (2) 29 (1990), 3–10, *Addendum*, ibid. 276, MR1111891 (92k:11003).

[25] *Rekordy i otwarte problemy w teorii liczb*, Delta nr 3 (202), 1991, 1–3.

[26] *Wacław Sierpiński*, Matematyka przełomu XIX i XX wieku, Prace Naukowe Uniwersytetu Śląskiego nr 1253, Katowice 1992, 9–15, MR1196940 (93k:01078).

[27] *Progress in number theory during the years 1989–1992*, Discuss. Math. 13 (1993), 75–80, MR1249152 (94m:11003); Polish version – Gradient 1 (1992), No. 7, 1–7.

[28] *Historia teorii liczb w Polsce w latach 1851–1950*, Wiadom. Mat. 30 (1993), 19–50, MR1281604.

[29] *Prawda i istnienie w matematyce*, Nauka – Religia – Dzieje, VII Seminarium Interdyscyplinarne w Castel Gandolfo, Kraków 1994, 65–76.

[30] *Solved and unsolved problems on polynomials*, in: Panoramas of Mathematics, Banach Center Publ. 34, Warsaw 1995, 149–159, MR1374345 (97a:12001).

[31] *O liczbach Fermata*, Gradient 5 (1996), 92.

[32] *Arithmetical properties of polynomials*, The Mathematics of Paul Erdős, I, Algorithms Combin. 13, Springer, Berlin 1997, 151–154, MR1425182 (97k:11035).

[33] *Teoria liczb w Polsce w latach 1851–1950*, Matematyka Polska w Stuleciu 1851–1950, Uniwersytet Szczeciński – Materiały Konferencyjne nr 16, Szczecin 1995, 61–67.

[34] *Sierpiński Wacław*, Polski Słownik Biograficzny, tom 37/3, Warszawa – Kraków 1997, 356–359.

[35] *Pál Erdős 1913–1996*, Nauka 1997, Nr 3, 253–255.

[36] *O liczbach doskonałych parzystych*, Matematyka 50 (1997), 270.

[37] *Sto lat twierdzenia o liczbach pierwszych*, Wiadom. Mat. (2) 33 (1997), 91–98, MR1615772 (99b:11001).

[38] *Jan Wójcik i jego prace z teorii liczb*, ibid., 199–204, MR1615831 (99m:01087).

[39] *IX Problem Hilberta*, Problemy Hilberta w pięćdziesięciolecie śmierci ich twórcy, Warszawa 1997, 119–122, MR1632441.

[40] *XII Problem Hilberta*, ibid. 147–151, MR1632444.

[41] *The Warsaw period of Voronoi's creative work*, Voronoi's Impact on Modern Science, Book I, Proc. Institute of Mathematics of the National Academy of Sciences of Ukraine 21, Kyiv 1998, 29–33; Ukrainian version: Вплив наукового доробку Г. Вороного на сучасну науку, Kyiv 2003, 43–47.

[42] *Reducibility of polynomials over Kroneckerian fields*, Number Theory. Diophantine, Computational and Algebraic Aspects (ed. by K. Győry, A. Pethő and V. T. Sós), Walter de Gruyter, Berlin 1998, 473–477, MR1628863 (99i:11097).

[43] *O tak zwanym twierdzeniu Chińczyków*, Gradient 7 (1998), 214–215.

[44] *Georgij Woronoj – mistrz Wacława Sierpińskiego*, XII Szkoła Historii Matematyki, Krynica 19–25 maja 1998, Kraków 1999, 155–161.

[45] *The Mahler measure of polynomials*, in: Number Theory and its Applications, Lecture Notes in Pure and Appl. Math. 204, Marcel Dekker 1999, 171–183, MR1661667 (99k:11041).

[46] *50 lat Olimpiady Matematycznej*, Matematyka 52 (1999), 350–352.

[47] *Exponential congruences*, Number Theory and its Applications, Kluwer Academic Publishers, Dordrecht 1999, 303–308, MR1738825 (2001e:11031).

[48] *Pięćdziesiąt lat Olimpiady Matematycznej*, Gradient 8 (1999), 323–332; Wiadom. Mat. (2) 36 (2000), 155–161.

[49] *Remark to the article of G. N. Sakovich "У світи математики"*, 6 (2000), no. 3, 46 (Ukrainian).

[50] *Teoria liczb w "Disquisitiones Arithmeticae"*, Matematyka czasów Gaussa, 137–141, Zielona Góra 2001, MR1847691.

[51] *Erdős's Work on Finite Sums of Unit Fractions*, Paul Erdős and his Mathematics I (ed. V. T. Sós), vol. I, Budapest 2002, 629–636, MR1954717 (2003k:11055).

[52] *Teoria liczb w pracach Kummera, Kroneckera, Dedekinda i Webera*, Matematyka czasów Weierstrassa, Szczecin 2002, 85–93.

[53] *Reducibility of polynomials in one variable over the rationals*, IV International Conference "Modern Problems of Number Theory and its Applications", dedicated to 180^{th} anniversary of P. C. Chebysheff and 110 anniversary of I. M. Vinogradov, Current Problems, Part II, Moskva 2002, 143–150.

[54] *Monadologia E. Kählera*, Nauka – Religia – Dzieje, XI Seminarium w Castel Gandolfo 7–9 sierpnia 2001, Kraków 2002, 119–122.

[55] *Niektóre osiągnięcia teorii liczb w XX wieku*, Matematyka 55 (2002), 68–70.

[56] *Przegląd osiągnięć teorii liczb w XX wieku*, Wiadom. Mat. (2) 38 (2002), 179–188, MR1985661 (2004b:11002).

[57] *Sto tomów Acta Arithmetica*, Wiadom. Mat. (2) 38 (2002), 189–192.

[58] *Wacław Sierpiński*, Słownik Biograficzny Matematyków Polskich, Tarnobrzeg 2003, 214–216.
[59] *Algorytm Euklidesa i jego uogólnienia*, Zeszyty Naukowe Uniwersytetu Opolskiego, Matematyka 31, Opole 2003, 163–169.
[60] *Nieskończoność w matematyce*, Nauka – Religia – Dzieje, XII Seminarium w Castel Gandolfo 5–7 sierpnia 2003, Kraków 2004, 109–116.
[61] *Progress in the number-theoretic problems considered by Bouniakowsky*, Віктор Якович Буняковский (до 200 ричча з дня народжения), Proc. Institute of Mathematics of the National Academy of Sciences of Ukraine, vol. 53, Kyiv 2004, 94–100.
[62] *Całki pseudoeliptyczne i równanie Pella dla wielomianów*, Matematyka abelowa w dwóchsetlecie urodzin Nielsa Henrika Abela (1802–1829), Nowy Sącz 2004, 45–48.
[63] *Podręczniki algebry Netta i Webera*, Sławne dzieła matematyczne i rocznice, Białystok 2005, 153–157.
[64] (with W. M. Schmidt) *The mathematical work of Eduard Wirsing*, Funct. Approx. Comment. Math. 35 (2006), 7–18; *Corrigendum*, ibid. 36 (2006), 133.

C. Books

[1] *Wacław Sierpiński*, Warszawa 1976, 1–50.
[2] *Selected Topics on Polynomials*, XXII+250 pp., University of Michigan Press, Ann Arbor 1982, MR0649775 (84k:12010).
[3] *Polynomials with Special Regard to Reducibility*, X+558 pp., Encyclopaedia of Mathematics and its Applications 77, Cambridge Univ. Press, Cambridge 2000, MR1770638 (2001h:11135).

ISBN 978-3-03719-038-8

www.ems-ph.org