ACTA ARITHMETICA
XL (1982)

Contributions to the theory of Kummer extensions

by

J. WÓJCIK (Warszawa)

1. The congruence $f(x^k) \equiv 0 \bmod q$, where q is a prime. The present paper has emerged from the work of the writer *On the composite Lehmer numbers with prime indices* [9], [10]. It has turned out that the existence of infinitely many such numbers, so far established only conditionally is related to some phenomena concerning power residues in algebraic number fields. The aim of this paper is to study these phenomena in their own right and in full generality.

Notation. $\zeta_m = e^{2\pi i/m}$, Q is the field of rational numbers, $P_m = Q(\zeta_m)$. For an extension K/Ω where K, Ω are algebraic number fields $N_{K/\Omega}$ is the norm from K to Ω. If the field K is fixed and $\mathfrak{a}$ is an ideal of K then $N\mathfrak{a}$ denotes the absolute norm of $\mathfrak{a}$. If the extension K/Ω is abelian then $f(K/\Omega)$ is its conductor. If $\alpha \in K$, $\zeta_m \in K$, $\alpha \neq 0$, $\mathfrak{b}$ is an ideal of K then $\left(\frac{\alpha|K}{\mathfrak{b}}\right)_m$ is the mth power residue symbol (see [2], p. 49–50). This symbol can be defined for $\mathfrak{b}$ prime to $f_\alpha = f(K(\sqrt[m]{\alpha})/K)$. (In fact the symbol can be defined for $\mathfrak{b}$ with the m-power free kernel prime to f_α but for our purposes it is not needed.) f_α is also called the conductor of $\left(\frac{\alpha|K}{\mathfrak{b}}\right)_m$. $D(\alpha)$ denotes the discriminant of α. $\bar{\alpha}$ denotes the complex conjugate of α. E_m is the group of rationals congruent to 1 mod m. We call a set $G \subset Q$ a *group of rationals* mod m if (i) $E_m \subset G$, (ii) G is a multiplicative group, (iii) every element of G is prime to m (clearly G/E_m is a group of residue classes mod m). If $K \subset P_m$ then a group G of rationals mod m is said to *correspond to* K if G/E_m is the maximal subgroup of $\mathrm{Gal}(P_m/Q)$ which leaves K fixed. $[,]$ denotes the least common multiple. $|K| = (K : Q)$. For a finite set S, $|S|$ is its cardinality.

Let K be an algebraic number field. K^{mc} denotes the maximal cyclotomic extension of K. Let $\alpha \in K^{mc}$. Let us consider the equation in unknowns n, β

$$\alpha = \beta^n, \quad n \text{ natural}, \ \beta \in K^{mc}. \tag{1}$$

Put

$$c_K(a) = \begin{cases} \text{maximal } n \text{ satisfying (1)} & \text{if the equation (1) has a finite number of solutions,} \\ \infty & \text{if the equation (1) has infinitely many solutions.} \end{cases}$$

Let f be an arbitrary polynomial with rational coefficients irreducible over Q, a a root of f. Put

$$c(f) = c(a) = c_{Q(a)}(a).$$

It is easy to see that the definition of $c(f)$ does not depend on the choice of a. Let K_1 be the maximal cyclotomic subfield of $Q(a)$. Of course K_1 is also the maximal cyclotomic subfield of $Q(a')$, where a' is an arbitrary conjugate of a. This means that K_1 is uniquely determined by f.

Put

$$C(f) = C(a) = (Q(a):K_1) = n/|K_1|,$$

where n denotes the degree of f.

We shall prove the following

THEOREM 1. *Let a be an algebraic number different from zero and not a root of unity, n be degree of a. There exists a positive integer $k_0 = k_0(a)$ such that for every positive integer k divisible by k_0 and for all positive integers D and r, where $(r, D) = 1$ and $r \equiv 1 \bmod (D, k)$ there exist infinitely many prime ideals $\mathfrak{q}$ of the field $Q(a)$ such that:*

$$a \text{ is } k\text{-th power residue } \bmod \mathfrak{q}, \quad N\mathfrak{q} \equiv 1 \bmod k, \quad N\mathfrak{q} \equiv r \bmod D.$$

The Dirichlet density of this set of prime ideals is equal to

$$\frac{c(a)n}{C(a)k\varphi([k, D])}.$$

In addition to Theorem 1, we shall prove the following results:

THEOREM 2. *Let f be a polynomial with rational integral coefficients, irreducible, primitive, with the leading coefficient positive. Assume that f is different from x and is not a cyclotomic polynomial. There exists a positive integer $k_0 = k_0(f)$ such that for every positive integer k divisible by k_0 and for all positive integers D and r, where $(r, D) = 1$ and $r \equiv 1 \bmod (D, k)$ there exist infinitely many primes q satisfying the condition: the congruence $f(x^k) \equiv 0 \bmod q$ is soluble, $q \equiv 1 \bmod k$, $q \equiv r \bmod D$. The Dirichlet density σ of this set of primes satisfies the inequality*

$$\frac{c(f)}{C(f)k\varphi([k, D])} \leqslant \sigma \leqslant \frac{n}{\varkappa} \cdot \frac{c(f)}{C(f)k\varphi([k, D])}$$

where

$$\varkappa = \begin{cases} 1 & \text{if } f \text{ is not symmetric,} \\ 2 & \text{if } f \text{ is symmetric,} \end{cases}$$

n is degree of f.

A. Rotkiewicz [6] has proved the following

LEMMA. *For every natural c there exist infinitely many primes p in every arithmetical progression $ax+b$ $(x = 0, 1, 2, \ldots)$, where a and b are relatively prime positive integers such that $c|p-1$ and $p|2^{(p-1)/c}-1$.*

Using Theorem 2 we shall prove a similar result (Theorem 3 in Section 2) about the so-called Lehmer numbers.

We shall study the equation $\alpha = \vartheta^n$, where α, n are fixed, α belongs to a fixed quadratic field, n is a positive integer, ϑ is cyclotomic.

Theorem 4 gives a complete description of numbers α for which the equation is soluble for a fixed n.

LEMMA 1. *Let k_1 be an algebraic number field. If $\alpha \in k_1^{mc}$ and α is different from zero and from roots of unity then the number $c_{k_1}(\alpha)$ is a positive integer.*

Proof. It is an easy consequence of the theorem: The group of S-units (S finite) of k_1^{mc} is the direct product of the group of all roots of unity and of a free abelian group (see [5]).

LEMMA 2. *Let F be a positive integer. Let k_2 be an arbitrary algebraic number field, G_2 be a group of rationals* mod F *corresponding to $k_2 \cap P_F$. We have:*

$$G_2 = \{s \in Q: \text{there exists an ideal } \mathfrak{a} \text{ of } k_2 \text{ such that } s \equiv N\mathfrak{a} \bmod F, \ (\mathfrak{a}, F) = 1\}.$$

Proof. If $\mathfrak{p}$ is a prime ideal of $k_2 \cap P_F$ prime to F then

$$N\mathfrak{p} \in G_2. \tag{2}$$

Indeed, by Fermat's Theorem, $\beta^{N\mathfrak{p}} \equiv \beta \bmod \mathfrak{p}$ for every integer β of $k_2 \cap P_F$. Hence $\beta^{\sigma} \equiv \beta \bmod \mathfrak{p}$, where $\sigma = (\zeta_F \to \zeta_F^{N\mathfrak{p}})$, σ on $k_2 \cap P_F$ belongs to the inertia group of $\mathfrak{p}$ and the latter is identity because $\mathfrak{p} \nmid F$. Thus $N\mathfrak{p} \in G_2$.

Put

$$G = \{s \in Q: \text{there exists an ideal } \mathfrak{a} \text{ of } k_2 \text{ such that } s \equiv N\mathfrak{a} \bmod F, \ (\mathfrak{a}, F) = 1\}.$$

By Theorem 19 in [1] the extension k_2P_F/k_2 is the class field corresponding to the group of ideals mod F: $N\mathfrak{a} \equiv 1 \bmod F$. Hence

$$(G : E_F) = (k_2P_F : k_2) = (P_F : k_2 \cap P_F) = (G_2 : E_F). \tag{3}$$

By the multiplicative property of norm and by (2) $G \subset G_2$. Hence by (3) $G_2 = G$.

LEMMA 3. *Let F be a positive integer. Let k_2 be an algebraic number field, $\beta \in k_2$, $\zeta_m \in k_2$ and $c_{k_2}(\beta) = 1$. There exists an ideal $\mathfrak{a}$ of k_2 such that*

$$\left(\frac{\beta}{\mathfrak{a}}\right)_m = \zeta_m, \quad (\mathfrak{a}, F) = 1, \quad N\mathfrak{a} \equiv 1 \bmod F.$$

Proof. We may suppose that F is divisible by all conductors of power residue symbols occurring in this proof. If the assertion of the lemma does not hold then for some natural d such that $d|m$, $d < m$ we have: If $(\mathfrak{a}, F) = 1$, $N\mathfrak{a} \equiv 1 \bmod F$ then $\left(\frac{\beta}{\mathfrak{a}}\right)_m = \zeta_d^x$ for some x depending on $\mathfrak{a}$. Hence

$$\left(\frac{\beta^d}{\mathfrak{a}}\right)_m = 1 \quad \text{for} \quad N\mathfrak{a} \equiv 1 \bmod F, \ (\mathfrak{a}, F) = 1.$$

Hence

$$\left(\frac{\beta^d|k_2P_F}{\mathfrak{b}}\right)_m = \left(\frac{\beta^d|k_2}{N_{k_2P_F/k_2}\mathfrak{b}}\right)_m = 1$$

for any ideal $\mathfrak{b}$ of k_2P_F prime to F since $N_{k_2/Q}(N_{k_2P_F/k_2}\mathfrak{b}) = N_{k_2P_F/Q}\mathfrak{b} \equiv 1 \bmod F$. This means that β^d is mth power residue for almost all prime ideals of k_2P_F and by Theorem 16.7 (I) in [4], p. 153, $\beta^d = \gamma^m$, $\gamma \in k_2P_F$. Hence $\beta = \gamma_1^{m/d}$, $\gamma_1 \in k_2^{mo}$, $m/d > 1$. This is impossible since $c_{k_2}(\beta) = 1$.

LEMMA 4. *Let F be a positive integer. Let k_2 be an algebraic number field, $\beta \in k_2$, $\zeta_m \in k_2$ and $c_{k_2}(\beta) = 1$, G_2 be a group of rationals* mod F *corresponding to $k_2 \cap P_F$. For any rational integer x and $s \in G_2$ there exists an ideal $\mathfrak{a}$ of k_2 such that*

$$\left(\frac{\beta}{\mathfrak{a}}\right)_m = \zeta_m^x, \quad (\mathfrak{a}, F) = 1, \quad N\mathfrak{a} \equiv s \bmod F.$$

Proof. We may suppose that F is divisible by $f(k_2(\sqrt[m]{\beta})/k_2)$. By Lemma 2 there exists an ideal $\mathfrak{a}_1$ of k_2 such that $s \equiv N\mathfrak{a}_1 \bmod F$, $(\mathfrak{a}_1, F) = 1$.

By Lemma 3 there exists an ideal $\mathfrak{a}_2$ of k_2 such that $\left(\frac{\beta}{\mathfrak{a}_2}\right)_m = \zeta_m$, $(\mathfrak{a}_2, F) = 1$, $N\mathfrak{a}_2 \equiv 1 \bmod F$. Put $\left(\frac{\beta}{\mathfrak{a}_1}\right)_m = \zeta_m^a$. It is enough to take $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2^{x-a}$.

Proof of Theorem 1. Let α be an algebraic number different from zero and from roots of unity, n be degree of α. Put $k_1 = Q(\alpha)$. By Lemma 1 $c_{k_1}(\alpha)$ is a positive integer, say n_1. We have

$$\alpha = \beta^{n_1}, \quad \beta \in k_1^{mo}, \quad c_{k_1}(\beta) = 1. \tag{4}$$

Hence $\beta \in k_1P_{m_1}$ for some positive integer m_1. Let K_1 be the maximal cyclotomic subfield of k_1. We have $K_1 \subset P_{m_2}$ for some positive integer m_2. Put $k_0 = [n_1, m_1, m_2]$. Let k be any positive integer divisible by k_0. Put

$$k_2 = k_1P_k, \quad \left(\frac{\gamma}{\mathfrak{a}}\right)_s = \left(\frac{\gamma|k_2}{\mathfrak{a}}\right)_s \quad \text{for } s|k, \ m = k/n_1.$$

We have $\alpha \in k_2$, $\beta \in k_2$ and

$$\left(\frac{\alpha}{\mathfrak{a}}\right)_k = \left(\frac{\beta}{\mathfrak{a}}\right)_m. \tag{5}$$

Put $(\alpha) = \mathfrak{a}/\mathfrak{b}$, $\mathfrak{a}$, $\mathfrak{b}$ integral ideals of k_2, $(\mathfrak{a}, \mathfrak{b}) = 1$.

Let D be any positive integer. Let F be a positive integer divisible by $kDN(\mathfrak{a}\mathfrak{b})$ and by all conductors of power residue symbols occurring in this proof. Let G_2 be a group of rationals mod F corresponding to the field $k_2 \cap P_F$. We have

$$\frac{|P_F|}{|k_2 \cap P_F|} = \frac{|k_2P_F|}{|k_2|} = \frac{|k_1P_kP_F|}{|k_1P_k|} = \frac{|k_1P_F|}{|k_1P_k|} = \frac{|P_F|}{|P_k|} \cdot \frac{|k_1 \cap P_k|}{|k_1 \cap P_F|} = \frac{|P_F|}{|P_k|}$$

since $k_1 \cap P_k = k_1 \cap P_F = K_1$, $K_1 \subset P_{m_2}$ $(m_2|k_0, k_0|k, k|F)$. Hence $|k_2 \cap P_F| = |P_k|$. Obviously $P_k \subset k_2 \cap P_F$. Thus $k_2 \cap P_F = P_k$.

According to the definition of G_2

$$G_2 = \{s \in Q: (s, F) = 1, \ s \equiv 1 \bmod k\}.$$

Put

$$A = \{\mathfrak{a} \text{ an ideal of } k_2: (\mathfrak{a}, F) = 1\},$$

$$H_1 = \{\mathfrak{a} \text{ an ideal of } k_2: (\mathfrak{a}, F) = 1, \ N\mathfrak{a} \equiv 1 \bmod F\},$$

$$H = \left\{\mathfrak{a} \text{ an ideal of } k_2: (\mathfrak{a}, F) = 1, \ N\mathfrak{a} \equiv 1 \bmod F, \left(\frac{\alpha}{\mathfrak{a}}\right)_k = 1\right\}.$$

By the assumption on F: A, H_1, H are groups of ideals mod F in virtue of Artin's reciprocity law. First we shall prove the theorem for $D \equiv 0 \bmod k$. Let $r \equiv 1 \bmod k$, $(r, F) = 1$. Obviously $r \in G_2$. We have $k_2^{mo} = k_1^{mo}$. Hence, by (4), $c_{k_2}(\beta) = c_{k_1}(\beta) = 1$. By Lemma 4 there exists an ideal $\mathfrak{a}_1$ of k_2 such that

$$(\mathfrak{a}_1, F) = 1, \quad N\mathfrak{a}_1 \equiv r \bmod F, \quad \left(\frac{\beta}{\mathfrak{a}_1}\right)_m = 1.$$

Let C denote the coset of A with respect to H containing $\mathfrak{a}_1$, i.e., by (5),

$$C = \left\{\mathfrak{a} \text{ an ideal of } k_2: (\mathfrak{a}, F) = 1, \ N\mathfrak{a} \equiv r \bmod F, \left(\frac{\alpha}{\mathfrak{a}}\right)_k = 1\right\}.$$

Put

$$h = (A : H). \tag{6}$$

Let $d(C)$ (similarly latter $d(C')$, $d(C'')$, $d(C''')$) denote the Dirichlet density of prime ideals belonging to C. Put

$$C' = \{\mathfrak{q}_1 \text{ a prime ideal of } k_1\colon N\mathfrak{q}_1 \equiv r \bmod F,\ a \text{ is } k\text{th power residue mod } \mathfrak{q}_1\}.$$

Let $\mathfrak{q}_1$ be a prime ideal of k_1 prime to F and $\mathfrak{q}_2$ a prime ideal of k_2 such that $\mathfrak{q}_2|\mathfrak{q}_1$. Suppose that $\mathfrak{q}_2$ is of degree one over k_1. By the definition of F $\mathfrak{q}_2$ is prime to a and to k. Hence

$$\left(\frac{a}{\mathfrak{q}_2}\right)_k = 1 \quad \text{if and only if } a \text{ is } k\text{th power residue mod } \mathfrak{q}_2. \tag{7}$$

Since $\mathfrak{q}_2$ is of degree one over k_1 we have by (7)

$$\left(\frac{a}{\mathfrak{q}_2}\right)_k = 1 \quad \text{if and only if } a \text{ is } k\text{th power residue mod } \mathfrak{q}_1. \tag{8}$$

Moreover

$$N_{k_2/Q}\mathfrak{q}_2 = N_{k_1/Q}\mathfrak{q}_1. \tag{9}$$

The extension k_2/k_1 is normal ($k_2 = k_1P_k$). Let $\tau \in \mathrm{Gal}(k_2/k_1)$. We have $\tau(a) = a$ ($k_1 = Q(a)$). If $\mathfrak{q}_2 \in C$ then $\tau\mathfrak{q}_2 \in C$. Indeed, if $\left(\frac{a}{\mathfrak{q}_2}\right)_k = 1$ then

$$\tau\left(\frac{a}{\mathfrak{q}_2}\right)_k = \left(\frac{\tau(a)}{\tau\mathfrak{q}_2}\right)_k = \left(\frac{a}{\tau\mathfrak{q}_2}\right)_k = 1.$$

Hence by (8) and (9) we have: If $\mathfrak{q}_2$ is a prime ideal of k_2 of degree one over k_1 and $\mathfrak{q}_2 \in C$ then there exist exactly $|k_2|/|k_1|$ prime ideals $\tau\mathfrak{q}_2$ ($\tau \in \mathrm{Gal}(k_2/k_1)$) of degree one over k_1 belonging to C and dividing a certain prime ideal $\mathfrak{q}_1$ of k_1 belonging to C' ($\mathfrak{q}_1 = N_{k_2/k_1}\mathfrak{q}_2$). Conversely, if $\mathfrak{q}_1$ is a prime ideal of k_1 and $\mathfrak{q}_1 \in C'$, then $\mathfrak{q}_1$ splits completely in k_2 and each of its prime divisor $\mathfrak{q}_2$ of k_2 belongs to C. This follows easily from (8), (9) and from Theorem 19 in [1]. Hence by Hecke's theorem and by (6)

$$\frac{1}{h} = d(C) = \lim_{s\to 1+0} \frac{\sum_{\mathfrak{q}_2\in C} \frac{1}{(N\mathfrak{q}_2)^s}}{\log\frac{1}{s-1}} = (|k_2|/|k_1|) \lim_{s\to 1+0} \frac{\sum_{\mathfrak{q}_1\in C'} \frac{1}{(N\mathfrak{q}_1)^s}}{\log\frac{1}{s-1}} = (|k_2|/n)\,d(C'), \tag{10}$$

($|k_1| = n$), where $\mathfrak{q}_2$ are prime ideals of k_2 of degree one over k_1.

Thus

$$d(C') = \frac{n}{h|k_2|}. \tag{11}$$

By Lemma 2 the quotient group A/H_1 is isomorphic with G_2/E_F. By Galois theory

$$(A : H_1) = (G_2 : E_F) = (P_F : k_2 \cap P_F) = (P_F : P_k) = |P_F|/|P_k|.$$

We have

$$n_1 = c_{k_1}(a) = c_{Q(a)}(a) = c(a).$$

By (5) and by Lemma 4 ($s = 1$)

$$(H_1 : H) = m = k/n_1 = k/c(a).$$

By (6)

$$h = (A : H) = (A : H_1)(H_1 : H) = \frac{|P_F|}{|P_k|} \cdot \frac{k}{c(a)}. \tag{12}$$

We have $(k_1 : K_1) = (Q(a) : K_1) = n/|K_1| = C(a)$ (see the begining of the paper). Further $K_1 \subset P_{m_2} \subset P_k$ since $m_2|k_0$, $k_0|k$. Hence $k_1 \cap P_k = K_1$ and

$$\frac{|k_2|}{|P_k|} = \frac{|k_1P_k|}{|P_k|} = \frac{|k_1|}{|k_1 \cap P_k|} = \frac{n}{|K_1|} = C(a).$$

Hence, by (12),

$$h|k_2| = |P_F| \cdot \frac{k}{c(a)} \frac{|k_2|}{|P_k|} = \varphi(F) \cdot \frac{k}{c(a)} \cdot C(a).$$

By (11)

$$d(C') = \frac{c(a)n}{C(a)k\varphi(F)}. \tag{13}$$

Suppose that $D \equiv 0 \bmod k$. Put

$$C'' = \{\mathfrak{q} \text{ a prime ideal of } k_1\colon N\mathfrak{q} \equiv r \bmod D,\ a \text{ is } k\text{th power residue mod } \mathfrak{q}\},$$

where $(r, D) = 1$ and $r \equiv 1 \bmod k$.

Let P be the group of all residue classes mod F prime to F and P_1 its subgroup of residue classes mod F congruent to $1 \bmod D$. Since for each rational integer ξ prime to D there exists a rational integer η prime to F satisfying $\eta \equiv \xi \bmod D$, we have $(P : P_1) = \varphi(D)$. Hence the number of residue classes mod F that are congruent to $r \bmod D$ is equal to $\varphi(F)/\varphi(D)$ and all the classes are congruent to $1 \bmod k$ because of $D \equiv 0 \bmod k$.

It follows that the C'' apart from at most finite number of prime ideals $\mathfrak{q}$ dividing F is the theoretic set union of $\varphi(F)/\varphi(D)$ disjoint sets of the type C'.

Hence, by (13), $d(C'') = \frac{\varphi(F)}{\varphi(D)} d(C')$ and

$$d(C'') = \frac{c(\alpha)n}{C(\alpha)k\varphi(D)}. \tag{14}$$

Thus we have proved the theorem for $D \equiv 0 \bmod k$.

Let D be any positive integer. Put

$$C''' = \{\mathfrak{q} \text{ a prime ideal of } k_1\colon N\mathfrak{q} \equiv 1 \bmod k,\ N\mathfrak{q} \equiv r \bmod D,\ \alpha \text{ is } k\text{th power residue mod } \mathfrak{q}\},$$

where $(r, D) = 1$ and $r \equiv 1 \bmod (D, k)$.

There exist rational integers x, y such that $r = 1 + kx + Dy$. Obviously,

$$C''' = \{\mathfrak{q} \text{ a prime ideal of } k_1\colon N\mathfrak{q} \equiv 1 + kx \bmod [k, D],\ \alpha \text{ is } k\text{th power residue mod } \mathfrak{q}\}.$$

By (14) (theorem for $D \equiv 0 \bmod k$),

$$d(C''') = \frac{c(\alpha)n}{C(\alpha)k\varphi([k, D])}.$$

The theorem is proved.

LEMMA 5. *Let $f(x)$ be an irreducible polynomial: $a_0x^n + \ldots + a_n$, $a_0, \ldots, a_n \in \mathbf{Z}$, $a_0 \neq 0$, α be its root. Let q be a prime number prime to $a_0D(a_0\alpha)$. The condition $q \mid f(x^k)$ is satisfied for some rational integer x if and only if there exists in $\mathbf{Q}(\alpha)$ a prime ideal $\mathfrak{q}$ of degree one dividing q such that α is k-th power residue* mod $\mathfrak{q}$.

Proof. Necessity. Put $k_1 = \mathbf{Q}(\alpha)$, $N = N_{k_1/\mathbf{Q}}$. We have

$$f(x^k) = a_0N(x^k - \alpha) = N(a_0x^k - a_0\alpha)/a_0^{n-1}, \tag{15}$$

$a_0\alpha$ is algebraic integer. Suppose that $q \mid f(x^k)$ for some rational integer x. Then, by (15), $q \mid N(a_0x^k - a_0\alpha)$. Hence $(q, a_0x^k - a_0\alpha) \neq 1$. Let $\mathfrak{q} \mid (q, a_0x^k - a_0\alpha)$, where $\mathfrak{q}$ is a prime ideal of k_1. Obviously $\mathfrak{q} \mid q$. Hence $(\mathfrak{q}, a_0) = 1$. We have

$$a_0\alpha \equiv a_0x^k \bmod \mathfrak{q}. \tag{16}$$

Let β be any integer of k_1. Of course $k_1 = \mathbf{Q}(a_0\alpha)$. Since $(q, D(a_0\alpha)) = 1$ we have:

$$\beta = \sum_{i=0}^{n-1} c_i(a_0\alpha)^i \equiv \sum_{i=0}^{n-1} d_i(a_0x^k)^i \bmod \mathfrak{q},$$

where c_i are rational numbers with denominators dividing $D(a_0\alpha)$ and d_i are rational integers such that $d_i \equiv c_i \bmod q$. β is congruent to a rational integer mod $\mathfrak{q}$. This means that $\mathfrak{q}$ is a prime ideal of degree one. By (16) $x^k \equiv \alpha \bmod \mathfrak{q}$ since $(q, a_0) = 1$. Thus α is kth power residue mod $\mathfrak{q}$.

Sufficiency. Suppose that $\mathfrak{q}$ is a prime ideal of degree one in k_1 such that $\mathfrak{q} \mid q$ and α is kth power residue mod $\mathfrak{q}$. Then there exists a rational integer x such that $x^k \equiv \alpha \bmod \mathfrak{q}$. Hence $a_0x^k \equiv a_0\alpha \bmod \mathfrak{q}$, $a_0\alpha$ is algebraic integer. We have $\mathfrak{q} \mid N(a_0x^k - a_0\alpha)$. Hence and by (15) $\mathfrak{q} \mid f(x^k)$ since $\mathfrak{q} \mid q$ and $(q, a_0) = 1$. Thus $q \mid f(x^k)$. The lemma is proved.

Proof of Theorem 2. Let $f(x) = a_0x^n + \ldots + a_n$ be a polynomial satisfying the assumptions of theorem. Let α be any of its roots. By the assumptions of the theorem α is different from zero and is not a root of unity. Put $k_1 = \mathbf{Q}(\alpha)$.

Let $k_0 = k_0(\alpha) = k_0(f)$ be the constant given in Theorem 1. Let k be any positive integer divisible by k_0. Put

$$C = \{\mathfrak{q} \text{ a prime ideal of } k_1\colon N\mathfrak{q} \equiv 1 \bmod k,\ N\mathfrak{q} \equiv r \bmod D,\ \alpha \text{ is } k\text{th power residue mod } \mathfrak{q}\},$$

$$B = \{q \text{ a prime number: } q \equiv 1 \bmod k,\ q \equiv r \bmod D, \text{ the congruence } f(x^k) \equiv 0 \bmod q \text{ is soluble}\},$$

where $(r, D) = 1$ and $r \equiv 1 \bmod (D, k)$.

It follows easily from Lemma 5: If $q \in B$ and q is prime to $a_0D(a_0\alpha)$ then there exists a prime ideal $\mathfrak{q}$ of degree one in k_1 such that $\mathfrak{q} \mid q$ and $\mathfrak{q} \in C$.

Conversely, if $\mathfrak{q}$ is a prime ideal of degree one in k_1 prime to $a_0D(a_0\alpha)$ and $\mathfrak{q} \in C$ then $q = N\mathfrak{q} \in B$. Hence

$$d(C) = \lim_{s \to 1+0} \frac{\sum_{\mathfrak{q} \in C} \frac{1}{(N\mathfrak{q})^s}}{\log \frac{1}{s-1}} = \lim_{s \to 1+0} \frac{\sum_{q \in B} \frac{\nu_q}{q^s}}{\log \frac{1}{s-1}}, \tag{17}$$

where $\mathfrak{q}$ are prime ideals of degree one in k_1 and $\nu_q > 0$ is the number of prime ideals of degree one in k_1 dividing q and belonging to C. q and $N\mathfrak{q}$ are prime to $a_0D(a_0\alpha)\operatorname{disc}(\bar{k}_1/\mathbf{Q})$ and to α, where $\bar{k}_1$ denotes the normal closure of k_1.

Let τ be any isomorphism of k_1 such that

$$\tau(\alpha) = \begin{cases} \alpha & \text{if } f \text{ is not symmetric,} \\ \alpha \text{ or } \alpha^{-1} & \text{if } f \text{ is symmetric} \end{cases} \tag{18}$$

($\tau = 1$ or $\tau(\alpha) = \alpha^{-1}$).

Put

$$\varkappa = \begin{cases} 1 & \text{if } f \text{ is not symmetric,} \\ 2 & \text{if } f \text{ is symmetric.} \end{cases}$$

τ is an automorphism of k_1; moreover, if $\mathfrak{q}$ is a prime ideal of degree one in k_1 dividing a prime q and belonging to C and $\mathfrak{q}$ is prime to α, then $\tau\mathfrak{q}$ has the same property. Indeed, if $x^k \equiv \alpha \bmod \mathfrak{q}$ $(x \in \boldsymbol{Q})$ then by (18) $x^k \equiv \tau(\alpha) = \alpha^{\pm 1} \bmod \tau\mathfrak{q}$ and since $(\tau\mathfrak{q}, \alpha) = 1$ we have $x^{\pm k} \equiv \alpha \bmod \tau\mathfrak{q}$. $\alpha \neq \alpha^{-1}$ since α is not a root of unity. The number of automorphisms satisfying (18) is equal to $\varkappa$. If $\tau(\alpha) = \alpha^{-1}$ and $\mathfrak{q}$ is a prime ideal of degree one in k_1 such that $q = N\mathfrak{q}$ is prime to $\operatorname{disc}(\bar{k}_1/\boldsymbol{Q})$ then

$$\tau\mathfrak{q} \neq \mathfrak{q}. \tag{19}$$

Indeed, $\tau \neq 1$ and the decomposition $q = \mathfrak{q} \cdot \tau\mathfrak{q} \cdot \tau_3\mathfrak{q} \dots \tau_n\mathfrak{q}$ holds in $\bar{k}_1$, where $1, \tau, \tau_3, \dots, \tau_n$ are isomorphisms of k_1. (19) follows at once from Dedekind's theorem. Hence

$$\varkappa \leqslant \nu_q \leqslant n. \tag{20}$$

Since f is irreducible and $f(0) \neq 0$, $f(x^k)$ has no multiple roots. Let K be the splitting field of $f(x^k)$. Let Φ_1 be the Galois group of K represented as permutation group of nk roots of $f(x^k)$. Let Φ_2 be the Galois group of $P_{[k,D]}$.

The Galois group $\bar{\Phi}$ of $K_1 = KP_{[k,D]}$ is some subgroup of the direct product $\Phi_1\Phi_2$. Put

$$\mathscr{U} = \{\sigma \in \bar{\Phi}\colon \sigma = \sigma_1\sigma_2,\ \sigma_1 \in \Phi_1,\ \sigma_2 \in \Phi_2,\ \sigma_1 \text{ fixes at least one root of } f(x^k),\ \sigma_2 = (\zeta_k \to \zeta_k^r, \zeta_D \to \zeta_D^r)\}.$$

$\mathscr{U}$ has the property: $\tau\mathscr{U}\tau^{-1} = \mathscr{U}$ for every $\tau \in \bar{\Phi}$. It is easy to see that $q \in B, (q, \operatorname{disc} K_1) = 1$ if and only if $\left(\frac{K_1}{q}\right) = \langle\sigma\rangle$ where $\sigma \in \mathscr{U}$. Hence and by Tchebotarev's density theorem the set B has Dirichlet's density, say $d(B)$, and $d(B)$ is equal to $|\mathscr{U}|/|\bar{\Phi}|$. (In particular, if $\mathscr{U}$ is empty then $d(B) = 0$.) By (17) and (20):

$$\varkappa \lim_{s \to 1+0} \frac{\sum_{q \in B} \frac{1}{q^s}}{\log \frac{1}{s-1}} \leqslant d(C) \leqslant n \lim_{s \to 1+0} \frac{\sum_{q \in B} \frac{1}{q^s}}{\log \frac{1}{s-1}},$$

where q are prime numbers prime to $a_0 D(a_0\alpha) \cdot \operatorname{disc}(\bar{k}_1/\boldsymbol{Q})$ and to α. Hence $\varkappa d(B) \leqslant d(C) \leqslant n d(B)$ and

$$\frac{1}{n} d(C) \leqslant d(B) \leqslant \frac{1}{\varkappa} d(C). \tag{21}$$

By the definition of $c(f)$ and $C(f)$: $c(\alpha) = c(f)$, $C(\alpha) = C(f)$. This and Theorem 1 give:

$$d(C) = \frac{nc(f)}{C(f)k\varphi([k, D])}.$$

By (21)

$$\frac{c(f)}{C(f)k\varphi([k, D])} \leqslant d(B) \leqslant \frac{n}{\varkappa} \cdot \frac{c(f)}{C(f)k\varphi([k, D])}.$$

The theorem is proved.

2. Application to Lehmer numbers. We shall give some application to Lehmer numbers. Lehmer numbers can be defined as follows:

$$P_n(\alpha, \beta) = \begin{cases} (\alpha^n - \beta^n)/(\alpha - \beta) & \text{if } n \text{ is odd,} \\ (\alpha^n - \beta^n)/(\alpha^2 - \beta^2) & \text{if } n \text{ is even,} \end{cases}$$

where α, β are roots of the trinomial $z^2 - \sqrt{L}z + M$ and L, M are rational integers.

Put for the moment $P'_n = P_n(\alpha, \beta)$. Lehmer numbers can be also defined as follows

$$P'_1 = P'_2 = 1,$$

$$P'_n = \begin{cases} LP'_{n-1} - MP'_{n-2} & \text{if } n \text{ is odd,} \\ P'_{n-1} - MP'_{n-2} & \text{if } n \text{ is even.} \end{cases}$$

Suppose that α, β are different from zero and α/β is not a root of unity. Put $k_1 = \boldsymbol{Q}(\alpha/\beta) = \boldsymbol{Q}(\sqrt{K\bar{L}})$, where $K = L - 4M$.

Since $c_{k_1}(\alpha/\beta)$ is a positive integer (Lemma 1) we may put

$$\alpha/\beta = \zeta_w^l \Xi^T, \tag{22}$$

where w is the number of roots of unity in k_1, $\Xi \in k_1$, Ξ is quotient of two conjugate integers of k_1 if k_1 is quadratic, T is maximal positive integer satisfying (22), $t \in \boldsymbol{Z}$. Below dash denotes the conjugate if k_1 is quadratic.

THEOREM 3. *If α, β defined above are different from zero and α/β is not a root of unity then there exists a positive integer k_0 such that for every positive integer k divisible by k_0 and for all positive integers D and r, where $(D, r) = 1$ and $r \equiv 1 \bmod (D, k)$ there exist infinitely many primes q satisfying the condition:*

$$q \equiv r \bmod D, \quad q \equiv 1 \bmod k, \quad q \mid P_{(q-1)/k}(\alpha, \beta).$$

The Dirichlet density of this set of primes is equal to $\frac{wT}{k\varphi([k, D])}$, where w, T are given in (22).

LEMMA 6. *Let k_1 be an algebraic number field. If e is a positive integer and $\gamma \in k_1^{mc}$ then $c_{k_1}(\gamma^e) = ec_{k_1}(\gamma)$.*

Proof. If γ is zero or a root of unity the lemma holds. Suppose that γ is different from zero and from roots of unity. Let $n = c_{k_1}(\gamma)$, $m = c_{k_1}(\gamma^e)$. By Lemma 1, m, n are positive integers. We have $\gamma = \beta^n$ and $\gamma^e = \delta^m$ with $\beta, \delta \in k_1^{mc}$. It follows that $\gamma^e = \beta^{ne}$ and hence $m \geqslant ne$. There exist integers a, b such that $(e, m) = ae + bm$. Then $\gamma^{(e,m)} = \gamma^{ae+bm} = (\delta^a\gamma^b)^m$ and consequently $\gamma = \varepsilon^{m/(e,m)}$ for some $\varepsilon \in k_1^{mc}$. Thus $\frac{m}{(e,m)} \leqslant n$ and $m \leqslant (e, m)n \leqslant en$. Hence $m = en$.

LEMMA 7 (A. Schinzel). *Let k_1 be a field. n a positive integer not divisible by the characteristic of k_1. A binomial $x^n - \alpha$ has over k_1 an abelian Galois group if and only if $\alpha^{w_n} = \gamma^n$, where $\gamma \in k_1$ and w_n is the number of n-th roots of unity contained in k_1.*

Proof. Sufficiency. If $\alpha^{w_n} = \gamma^n$, $\gamma \in k_1$ then $\sqrt[n]{\alpha} = \zeta_{nw_n}^a \sqrt[w_n]{\gamma}$, $\sqrt[w_n]{\gamma} \in k_1^{ab}$ $(\zeta_{w_n} \in k_1)$ where k_1^{ab} denotes the maximal abelian extension of k_1. Thus $\sqrt[n]{\alpha} \in k_1^{ab}$ and $k_1(\sqrt[n]{\alpha}, \zeta_n)/k_1$ is abelian.

Necessity. Assume that the Galois group of $x^n - \alpha$ is abelian. Let $\alpha^{w_n} = \gamma^{n_0}$, $\gamma \in k_1$, $n_0 \in \boldsymbol{N}$, $n_0 | n$, n_0 maximal. Obviously $n_0 \leqslant n$, $w_n | n_0$. We are to prove that $n_0 = n$. Suppose that $n_0 < n$. Let $p | \frac{n}{n_0}$, p a prime. Put: $p^\omega \| w_n$, $t = p^{\omega+1}n_0/w_n$, $k_2 = k_1(\zeta_{p^{\omega+1}})$, $k_3 = k_1(\sqrt[p^{\omega+1}]{\gamma}) \subset k_1(\sqrt[t]{\alpha}, \zeta_{tw_n}) \subset k_1(\sqrt[n]{\alpha}, \zeta_{tw_n}) \subset k_1^{ab}(\sqrt[n]{\alpha} \in k_1^{ab})$. By the definition of n_0: $(k_3 : k_1) = p^{\omega+1}$. Hence $\zeta_{p^{\omega+1}} \in k_3$ and $k_1 \subset k_2 \subset k_3$. Further $\zeta_{p^\omega} \in k_1$, $\zeta_{p^{\omega+1}} \notin k_1$ because $p^{\omega+1} | n$, $p^\omega \| w_n$.

1. $\omega = 0$. Then $(k_2 : k_1) | p - 1$. Hence $k_2 = k_1$ and $\zeta_p \in k_1$, a contradiction.

2. $\omega > 0$. We have $(k_3 : k_2) < p^{\omega+1}$ and $k_3 = k_2(\sqrt[p^{\omega+1}]{\gamma})$. Hence $\gamma = \gamma_1^p$, $\gamma_1 \in k_2$. Thus $k_1(\sqrt[p]{\gamma}) \subset k_2 = k_1(\sqrt[p]{\zeta_{p^\omega}})$. Hence $\gamma = \zeta_{p^\omega}^a \gamma_2^p$, $\gamma_2 \in k_1$ and $\alpha^{w_n} = \gamma_2^{pn_0}$, $pn_0 | n$ contrary to the definition of n_0.

Remark 1. Lemma 7 is the main part of Theorem 2 in [7] and also Theorem 2.1 of [8], but the proof given above is definitely shorter.

LEMMA 8. *Let k_1 be an algebraic number field and let l denote an arbitrary prime. If $\Xi \in k_1$, $\zeta_{l^{n-1}} \in k_1$, $\zeta_{l^n} \notin k_1$ for a certain n and Ξ is not of the form $\zeta_{l^{n-1}}^a \gamma^l$, $\gamma \in k_1$, then Ξ is not the l^n-th power in k_1^{mc}.*

Proof. Suppose that $\Xi = \Xi_1^{l^n}$, where $\Xi_1 \in k_1^{mc}$. Evidently the splitting field L_1 of the polynomial $x^{l^n} - \Xi$ is contained in k_1^{mc}. Consequently L_1 is an abelian extension of k_1. By Lemma 7 we have $\Xi^{l^{n-1}} = \gamma^{l^n}$ with $\gamma \in k_1$. Consequently $\Xi = \zeta_{l^{n-1}}^a \gamma^l$.

LEMMA 9. *Let k_1 be a quadratic field, $\omega \in k_1$. If $N(\omega) < 0$ then ω is not the square of a cyclotomic number.*

Proof. Since $N(\omega) < 0$, the field k_1 is real. We may assume that $\omega > 0$ changing the sign of ω, if necessary. It follows that $\omega' < 0$, where $N(\omega) = \omega\omega'$. Moreover, ω is not a square in k_1 because $N(\omega) < 0$. Suppose that ω is the square of a cyclotomic number ξ. Evidently ξ is real and $\boldsymbol{Q}(\xi)$ is a normal extension of degree 4. Let σ be an automorphism of the field $\boldsymbol{Q}(\xi)$ satisfying $\sigma(\omega) = \omega'$.

Applying σ to $\xi^2 = \omega$ we obtain $(\sigma(\xi))^2 = \omega' < 0$. This is impossible since $\sigma(\xi)$ is a real number.

LEMMA 10. *Let k_1 be a quadratic field, σ a nontrivial automorphism of it. Let w denote the number of roots of unity in k_1. If $\gamma \in k_1$ and $\gamma \neq 0$ then $\gamma^{1-\sigma}$ is the w-th power of a cyclotomic number.*

Proof. 1. k_1 is real. Then $w = 2$ and $\gamma^{1-\sigma} = (\sqrt{N(\gamma)}/\gamma^\sigma)^2$.

2. k_1 is imaginary. Let γ_1 be a root of the polynomial $x^w - \gamma^{1-\sigma}$. Then $\gamma_1^{w(1+\sigma)} = \gamma^{(1-\sigma)(1+\sigma)} = 1$. Hence $\gamma_1^{1+\sigma} = 1$ since $\gamma_1^{1+\sigma} = |\gamma_1|^2 > 0$. Hence $\gamma_1^\sigma = \gamma_1^{-1}$. Let τ be the generating element of $\mathrm{Gal}(k_1(\gamma_1)/k_1)$. We have $\tau(\gamma_1) = \zeta_w^a \gamma_1$. It is enough to prove that σ and τ commute.

Indeed,

$$\sigma\tau(\gamma_1) = \sigma(\zeta_w^a\gamma_1) = \zeta_w^{-a}\gamma_1^{-1} = (\zeta_w^a\gamma_1)^{-1} = (\tau(\gamma_1))^{-1} = \tau(\gamma_1^{-1}) = \tau\sigma(\gamma_1).$$

LEMMA 11. *Let k_1 be a quadratic field and $\Xi_1 \in k_1$, n be a positive integer. Assume that either n is odd or k_1 is imaginary. If $N(\Xi_1) = 1$ and Ξ_1 is an n-th power in k_1 then Ξ_1 is of the form $(\xi/\xi')^n$, $\xi \in k_1$.*

Proof. Assume that $\Xi_1 = \Xi_2^n$, $\Xi_2 \in k_1$. Hence $N(\Xi_1) = N(\Xi_2)^n = 1$. Since every norm is rational and also nonnegative if k_1 is imaginary we have $N(\Xi_2) = 1$. By Hilbert's Theorem 90 $\Xi_2 = \xi/\xi'$, $\xi \in k_1$. Hence $\Xi_1 = (\xi/\xi')^n$.

LEMMA 12. *Let k be a positive integer and α, β satisfy the assumptions of Theorem 3. Put*

$$f(x) = \begin{cases} a_0(x - \alpha/\beta) & \text{if } \alpha/\beta \text{ is rational,} \\ a_0(x - \alpha/\beta)(x - \beta/\alpha) & \text{if } \alpha/\beta \text{ is irrational.} \end{cases}$$

Suppose that f has rational integral coefficients, $a_0 > 0$, f is primitive, q is a prime number prime to $a_0 KLMD(a_0\alpha/\beta)$. Assume that $q \equiv 1 \bmod k$. The divisibility $q | f(x^k)$ is satisfied for some rational integer x if and only if $q | P_{(q-1)/k}(\alpha, \beta)$.

Proof. Assume that $q \equiv 1 \bmod k$. By Lemma 5, $q|f(x^k)$ for some $x \in \boldsymbol{Z}$ if and only if there exists a prime ideal $\mathfrak{q}$ of k_1 of degree one dividing q such that α/β is kth power residue mod $\mathfrak{q}$. If $\alpha/\beta \equiv x^k \bmod \mathfrak{q}$ $(x \in \boldsymbol{Z})$ then $(\alpha/\beta)^{(q-1)/k} \equiv 1 \bmod \mathfrak{q}$. Hence $q|P_{(q-1)/k}(\alpha, \beta)$ since $(q, KL) = 1$.

Let $q|P_{(q-1)/k}(\alpha, \beta)$. Since $(q, M) = 1$ it follows that

$$(\alpha/\beta)^{(q-1)/k} \equiv 1 \bmod \mathfrak{q}, \tag{23}$$

where $\mathfrak{q}$ is a prime ideal of k_1 dividing q. Hence

$$(\alpha/\beta)^q \equiv \alpha/\beta \bmod \mathfrak{q}. \tag{24}$$

Put $\Xi = a_0\alpha/\beta$. Ξ is algebraic integer. By (24) and Fermat's theorem $\Xi^q \equiv \Xi \bmod \mathfrak{q}$. Since $k_1 = Q(\Xi)$ and $(q, D(\Xi)) = 1$ it follows that $\gamma^q \equiv \gamma \bmod \mathfrak{q}$ for any integer γ of k_1. This means that $\mathfrak{q}$ is of degree one. Hence by Euler's criterion and by (23) α/β is kth power residue mod $\mathfrak{q}$. The lemma is proved.

Proof of Theorem 3. Let f be a polynomial as in Lemma 12. Let t, T, Ξ have the same meaning as in (22). Let n, $\varkappa$ have the meaning of Theorem 1. f is of degree one or symmetric of degree two. In each case: $n/\varkappa = 1$. Since k_1 is cyclotomic we have $C(f) = 1$. By Theorem 2 and Lemma 12 there exists a positive integer k_0 such that for every positive integer k divisible by k_0 and for all positive integers D, r satisfying: $(D, r) = 1$ and $r \equiv 1 \bmod (D, k)$ there exist infinitely many primes q satisfying the condition: $q \equiv r \bmod D$, $q \equiv 1 \bmod k$, $q|P_{(q-1)/k}(\alpha, \beta)$. The Dirichlet density of this set of primes is equal to $\dfrac{c(f)}{k\varphi([k, D])}$. It is enough to prove that $c(f) = wT$. Obviously $k_1^{\mathrm{mc}} = \boldsymbol{Q}^{\mathrm{mc}}$ and $c_{k_1}(*) = c_{\boldsymbol{Q}}(*)$. Let us put $N(*) = N_{k_1/\boldsymbol{Q}}(*)$. By (22) and Lemma 6:

$$c(f) = c_{k_1}(\alpha/\beta) = c_{\boldsymbol{Q}}(\Xi^T) = c_{\boldsymbol{Q}}(\Xi)T.$$

It is enough to prove that

$$c_{\boldsymbol{Q}}(\Xi) = w. \tag{25}$$

We shall prove

(i) *If l is a prime and $l \nmid w$ then Ξ is not the l-th power of a cyclotomic number.*

First we shall prove that Ξ is not an lth power in k_1. If $\alpha/\beta \in \boldsymbol{Q}$ this follows from the definition of Ξ and T. If $\alpha/\beta \notin \boldsymbol{Q}$ then by Lemma 11 $(\Xi_1 = \Xi, n = l)$, by the definition of Ξ and since l is odd, Ξ is not an lth power in k_1. Obviously $\zeta_l \notin k_1$. Now (i) follows at once from Lemma 8 $(n = 1)$.

1. $w = 2$. By (i)

$$c_{\boldsymbol{Q}}(\Xi) = 2^u, \quad u \geqslant 0. \tag{26}$$

If Ξ is not of the form $\pm\omega^2$, $\omega \in k_1$, then by Lemma 8 $(l = n = 2)$ Ξ is not the biquadrate of a cyclotomic number. Hence $u \leqslant 1$.

Assume now that $\Xi = \pm\omega^2$, $\omega \in k_1$. By the definition of Ξ and T it follows that k_1 is quadratic and $N(\Xi) = 1$. Hence $N(\omega) = \pm 1$. It follows that $N(\omega) = -1$. Otherwise by Hilbert's Theorem 90 we would have $\omega = \xi/\xi'$, $\xi \in k_1$, $\Xi = \pm(\xi/\xi')^2$ contrary to the definition of Ξ and T. By Lemma 6, $c_{\boldsymbol{Q}}(\Xi) = c_{\boldsymbol{Q}}(\omega^2) = 2c_{\boldsymbol{Q}}(\omega)$. Hence and by (26) $c_{\boldsymbol{Q}}(\omega) = 2^{u-1}$. By Lemma 9 ω is not the square of a cyclotomic number. Hence $u = 1$. In each case

$$u \leqslant 1. \tag{27}$$

On the other hand, $\Xi = \gamma/\delta = \omega_1/\delta^2 = (\sqrt{\omega_1}/\delta)^2$, where γ, δ are integesr of k_1, $\omega_1 = \gamma\delta$ is rational integer. Hence Ξ is the square of a cyclotomic number. This means that $u \geqslant 1$. By (26) and (27) $u = 1$, and $c_{\boldsymbol{Q}}(\Xi) = 2$. Thus (25).

2. $w = 4$. We have $k_1 = P_4 = \boldsymbol{Q}(\sqrt{-1})$. By (i)

$$c_{\boldsymbol{Q}}(\Xi) = 2^u, \quad u \geqslant 0. \tag{28}$$

By Lemma 11 $(\Xi_1 = i^x\Xi, n = 2)$ none of the numbers $i^x\Xi$ is a square in P_4. By Lemma 8 $(l \neq 2, n = 3)$ Ξ is not the eighth power of a cyclotomic number.

Hence

$$u \leqslant 2. \tag{29}$$

By (22) $\Xi = \gamma/\overline{\gamma}$, $\gamma \in P_4$. By Lemma 10 Ξ is the biquadrate of a cyclotomic number. This means that $u \geqslant 2$. By (29) and (28) $u = 2$ and $c_{\boldsymbol{Q}}(\Xi) = 4$. Thus (25).

3. $w = 6$. We have $k_1 = P_3 = P_6 = \boldsymbol{Q}(\sqrt{-3})$. By (i)

$$c_{\boldsymbol{Q}}(\Xi) = 2^u 3^v, \quad u, v \geqslant 0. \tag{30}$$

By Lemma 11 $(\Xi_1 = \zeta_6^x\Xi, n = 2, 3)$ none of the numbers $\zeta_6^x\Xi$ is a square or a cube in P_6. By Lemma 8 $(n = 2; l = 2, 3)$ Ξ is neither the biquadrate nor the ninth power of a cyclotomic number. Hence

$$u \leqslant 1, \quad v \leqslant 1. \tag{31}$$

By (22) $\Xi = \gamma/\overline{\gamma}$, $\gamma \in P_6$. By Lemma 10 Ξ is the sixth power of a cyclotomic number. This means that $u \geqslant 1$, $v \geqslant 1$. By (31) and (30) $u = v = 1$ and $c_{\boldsymbol{Q}}(\Xi) = 6$. Thus (25).

Example 1. Theorems 1, 2 and 3 are not true for all positive integers k. Put in Theorem 3: $k = 2$, $\alpha = 2$, $\beta = 1$. Then we have $P_n(\alpha, \beta) = 2^n - 1 = M_n$, where n is odd and M_n denotes the nth Mersenne number. It follows easily from quadratic reciprocity law that there is no prime q satisfying the condition: $q|M_{(q-1)/2}$, $q \equiv 3 \bmod 8$ although $3 \equiv 1 \bmod (8, 2)$.

EXAMPLE 2. Put in Theorem 3: $k=4$, $\alpha=-1+2i$, $=-1-2i$. It follows easily from the biquadratic reciprocity law and from the formula $(\alpha/\beta)^{(q-1)/4}\equiv\left(\frac{\alpha|P_4}{q}\right)_4 \bmod q$ (see [9], p. 112) that there is no prime q satisfying the condition $q|P_{(q-1)/4}(\alpha,\beta)$, $q\equiv 9 \bmod 20$ although $9\equiv 1 \bmod (20,4)$.

EXAMPLE 3. Put in Theorem 3: $k=6$, $\alpha=1+3\varrho$, $\beta=1+3\varrho^2$ ($\varrho=e^{2\pi i/3}$). It follows easily from the cubic reciprocity law and from the formula

$$(\alpha/\beta)^{(q-1)/3}\equiv\left(\frac{\alpha|P_3}{q}\right)_3 \bmod q$$

(see [9], p. 113) that there is no prime q satisfying the condition: $q|P_{(q-1)/6}(\alpha,\beta)$, $q\equiv 31 \bmod 42$ although $31\equiv 1 \bmod (42,6)$.

EXAMPLE 4. Put in Theorem 3: $\alpha=(1+\sqrt{5})/2$, $\beta=(1-\sqrt{5})/2$. Since $\alpha+\beta=1$ we have $P_n(\alpha,\beta)=u_n$, where u_n denotes Fibonacci sequence. The value of k_0 in Theorem 3 can be obtained by arguments given at the begining of the proof of Theorem 1 (see the begining of the proof of Theorem 3)

$$k_0=[n_1,m_1,m_2]=[2,20,20]=20.$$

We have $w=2$, $T=1$, $k_1=Q(\sqrt{5})$. By Theorem 3 there exist infinitely many primes q such that $q|u_{(q-1)/20}$, $q\equiv 21 \bmod 40$. The Dirichlet density of this set of primes is equal to $1/160$.

Remark 2. For any α, β in Theorem 3 the constant $k_0=k_0(\alpha,\beta)$ may be given explicitly. This will be an object of an another paper.

3. On the equation $\alpha=\vartheta^n$. Let $\alpha\in Q$. From Lemma 7 it follows at once the known fact: α is the nth power of a cyclotomic number if and only if one of the following conditions is satisfied for a suitable $\gamma\in Q$:

(a) $n\equiv 1 \bmod 2$, $\alpha=\gamma^n$, (b) $n\equiv 0 \bmod 2$, $\alpha=\varepsilon\gamma^{n/2}$, where $\varepsilon^2=1$.

We shall study in this section the equation $\alpha=\vartheta^n$, where α belongs to a fixed quadratic field, n is a positive integer, ϑ is a cyclotomic number. From Lemma 7 we shall deduce

THEOREM 4. *Let K be a quadratic field, f its conductor. The equation $\alpha=\vartheta^n$, $\alpha\in K$, n a positive integer, ϑ cyclotomic, holds if and only if one of the following conditions is satisfied for a suitable $c\in Q$, $\gamma,\delta\in K$:*

(i) $n\equiv 1 \bmod 2$, $\alpha=\varepsilon(\delta/\delta')^{n/w_n}\gamma^n$,

(ii) $n\equiv 0 \bmod 2$, $\alpha=\varepsilon(\delta/\delta')^{n/w_n}c^{n/2}\gamma^n$,

(iii) $n\equiv 0 \bmod 2$, *K is real*, $f=a^2+b^2$, $a,b\in Z$, $\alpha=\varepsilon(\sqrt{f}(a+\sqrt{f}))^{n/2}\times c^{n/2}\gamma^n$, *where w_n is the number of n-th roots of unity contained in K*, $\varepsilon^{w_n}=1$, *δ' denotes the conjugate of δ.*

LEMMA 13. *Let K be a quadratic field, f its conductor. Let $\beta\in K$. If β is the square of a cyclotomic number then one of the following conditions is satisfied for a suitable $c\in Q$ and a suitable $\gamma\in K$:*

(iv) $\beta=c\gamma^2$,

(v) *K is real*, $f=a^2+b^2$, $a,b\in Z$, $\beta=c\sqrt{f}(a+\sqrt{f})\gamma^2$.

Proof. The assertion of the lemma is obvious if β is a square in K. Assume that β is not a square in K. Then the polynomial $x^2-\beta$ is irreducible over K.

Put $\beta=\vartheta^2$, $\vartheta\in Q^{mc}$. The field $K(\vartheta)$ is biquadratic and abelian. We consider 2 cases:

Case 1: $K(\vartheta)$ is not cyclic. Then by Galois theory $K(\sqrt{\beta})=K(\vartheta)=K\cdot Q(\sqrt{c})=K(\sqrt{c})$, $c\in Q$. Hence $\beta=c\gamma^2$, $\gamma\in K$. Thus (iv).

Case 2: $K(\vartheta)$ is cyclic. We have $L=K(\vartheta)=Q(\vartheta)$ since $\beta\notin Q$. Let σ be the generating element of $\mathrm{Gal}(L/Q)$. Then σ^2 is the generating element of $\mathrm{Gal}(L/K)$. Obviously $\sigma(\beta)=\beta'$. We have $\sigma^2(\beta)=\beta=(\sigma^2(\vartheta))^2=\vartheta^2$. Hence $\sigma^2(\vartheta)=-\vartheta$ since $\sigma^2\neq 1$. Further we have $\sigma^2(\sigma(\vartheta)/\vartheta)=\sigma^3(\vartheta)/\sigma^2(\vartheta)=\sigma(-\vartheta)/(-\vartheta)=\sigma(\vartheta)/\vartheta$. This means that $\sigma(\vartheta)/\vartheta\in K$ thus $\sigma(\vartheta)=\gamma_1\vartheta$ with $\gamma_1\in K$. Further $\sigma^2(\vartheta)=\sigma(\gamma_1\vartheta)=\sigma(\gamma_1)\gamma_1\vartheta=N(\gamma_1)\vartheta=-\vartheta$. Hence $N(\gamma_1)=-1$. The field K is real and $K=Q(\sqrt{f})$. There exist rational numbers x, y such that $x^2-fy^2=-1$. Hence every odd prime factor of f is congruent to 1 mod 4 and $f=a^2+b^2$, $a,b\in Z$. Put $\gamma_2=(a-\sqrt{f})/b$. We have $N(\gamma_2)=-1$ and $N(\gamma_1/\gamma_2)=1$. By Hilbert's Theorem 90: $\gamma_1/\gamma_2=\gamma'/\gamma$, $\gamma\in K$. Further

$$\beta'/\beta=(\sigma(\vartheta))^2/\vartheta^2=\gamma_1^2=\gamma_2^2\gamma'^2/\gamma^2=\frac{-\sqrt{f}(a-\sqrt{f})\gamma'^2}{\sqrt{f}(a+\sqrt{f})\gamma^2}.$$

Hence $\beta=c\sqrt{f}(a+\sqrt{f})\gamma^2$ where $c\in Q$ since $c'=c$ (see also [3], (22), p. 36). Thus (v).

Remark 3. We have also proved the known fact: *If $K(\sqrt{\beta})$ is cyclic and $\sqrt{\beta}\notin K$ then K is real.*

LEMMA 14. *Let K be a quadratic field. Let $\beta\in K$. If β is the cube of a cyclotomic number then*

$$\beta=(\delta/\delta')\gamma^3,\quad \gamma,\delta\in K.$$

Proof. The assertion of the lemma is obvious if β is a cube in K. Assume that β is not a cube in K. Then the polynomial $x^3-\beta$ is irreducible over K. Put $\beta=\vartheta^3$, $\vartheta\in Q^{mc}$. The field $L=K(\vartheta)$ is abelian. It is the splitting field of $x^3-\beta$ over K. By Lemma 7 $w_3=3$. Hence $K=P_3=Q(\sqrt{-3})$. We have $L=P_3(\vartheta)$ and $|L|=6$. The field L is cyclic of degree six. Let σ be the generating element of $\mathrm{Gal}(L/Q)$. Then σ^2 is the

generating element of $\mathrm{Gal}(L/P_3)$. We may put $\sigma^2(\vartheta) = \varrho\vartheta$ ($\varrho = e^{2\pi i/3}$). Obviously $\sigma(\varrho) = \varrho^2$. We have $\sigma^2(\vartheta\cdot\sigma(\vartheta)) = \sigma^2(\vartheta)\cdot\sigma^3(\vartheta) = \varrho\vartheta\cdot\sigma(\varrho\vartheta) = \varrho\vartheta\varrho^2\sigma(\vartheta) = \vartheta\cdot\sigma(\vartheta)$. This means that $\vartheta\cdot\sigma(\vartheta)\in P_3$. Further $\beta = (\delta/\delta')\gamma^3$, where $\delta = \sigma(\beta) = \beta'\in P_3$, $\gamma = \dfrac{\beta}{\vartheta\sigma(\vartheta)}\in P_3\ (= K)$. The lemma is proved.

LEMMA 15. *Let K be a quadratic field, f its conductor. If $\beta = \vartheta_1^{w_n}$ $\beta\in K$, ϑ_1 a cyclotomic number then one of the following conditions is satisfied for a suitable $c\in Q$, γ, $\delta\in K$:*

(vi) $n\equiv 1 \bmod 2$, $\beta = (\delta/\delta')\gamma^{w_n}$,

(vii) $n\equiv 0 \bmod 2$, $\beta = (\delta/\delta')c^{w_n/2}\gamma^{w_n}$,

(viii) $n\equiv 0 \bmod 2$, *K is real*, $f = a^2+b^2$, $a, b\in Z$, $\beta = c\sqrt{f}(a+\sqrt{f})\gamma^2$.

Proof. $w_n = 1$. (vi) holds trivially.

$w_n = 2$. By Lemma 13 we have (vii) or (viii).

$w_n = 3$. By Lemma 14 we have (vi).

$w_n = 4$. We have $K = P_4 = Q(\sqrt{-1})$. We consider 2 cases:

Case 1: β is a square in P_4. Then

$$\beta = \beta_1^2 = \vartheta_1^4, \qquad \beta_1\in P_4, \qquad \vartheta_1\in Q^{\mathrm{mc}}. \tag{32}$$

Hence $\beta_1 = \vartheta_2^2$, $\vartheta_2\in Q^{\mathrm{mc}}$. By Lemma 13 $\beta_1 = c\gamma^2$, $c\in Q$, $\gamma\in P_4\ (= K)$. By (32) $\beta = c^2\gamma^4$ thus (vii).

Case 2: β is not a square in P_4. Then the polynomial $x^4-\beta$ is irreducible over P_4. Put $\beta = \vartheta_1^4$, $\vartheta_1\in Q^{\mathrm{mc}}$. The field $L = P_4(\vartheta_1)$ is abelian. $|L| = 8$. L is not cyclic. Otherwise the biquadratic cyclic subfield of L would contain the real quadratic field (Remark 3). On the other hand L contains P_4 which is impossible. Since the extension L/P_4 is cyclic and of degree four the group $\mathrm{Gal}(L/Q)$ contains an element of order 4. Hence the group $\mathrm{Gal}(L/Q)$ is of the type $(4,2)$. On the other hand a biquadratic cyclic field does not contain ζ_4 because it contains a real quadratic field. Hence by Galois theory

$$L = K_1P_4 \quad \text{and} \quad K_1\cap P_4 = Q, \tag{33}$$

where K_1 is a cyclic biquadratic field.

Let σ be the generating element of $\mathrm{Gal}(L/P_4)$. Let σ_1 be the generating element of $\mathrm{Gal}(L/K_1)$. By Galois theory and by (33)

$$\mathrm{Gal}(L/Q) = \mathrm{Gal}(L/P_4)\,\mathrm{Gal}(L/K_1).$$

σ is of order four and σ_1 is of order two. σ, σ_1 are generating elements of $\mathrm{Gal}(L/Q)$.

We may put $\sigma(\vartheta_1) = i\vartheta_1$. We have $\sigma_1(i) = -i$ (otherwise by Galois theory and by (33) we would have $\sigma_1 = 1$ which is impossible). We have

$$\begin{aligned}\sigma(\vartheta_1\cdot\sigma_1(\vartheta_1)) &= \sigma(\vartheta_1)\sigma\sigma_1(\vartheta_1) = i\vartheta_1\cdot\sigma_1\sigma(\vartheta_1) = i\vartheta_1\cdot\sigma_1(i\vartheta_1)\\ &= i\vartheta_1(-i)\sigma_1(\vartheta_1) = \vartheta_1\sigma_1(\vartheta_1)\end{aligned}$$

and

$$\sigma_1(\vartheta_1\sigma_1(\vartheta_1)) = \sigma_1(\vartheta_1)\cdot\sigma_1^2(\vartheta_1) = \vartheta_1\sigma_1(\vartheta_1).$$

This means that $c_1 = \vartheta_1\sigma_1(\vartheta_1)\in Q$.

Further

$$N_{P_4/Q}(\beta c_1^2(c_1/\beta)^4) = N_{P_4/Q}(c_1^6/\beta^3) = N_{P_4/Q}(\sigma_1(\vartheta_1^6)/\vartheta_1^6) = (\sigma_1(\vartheta_1^6)/\vartheta_1^6)^{1+\sigma_1} = 1.$$

By Hilbert's Theorem 90:

$$\beta c_1^2(c_1/\beta)^4 = \delta/\bar{\delta}, \qquad \delta\in P_4\ (= K).$$

Hence $\beta = (\delta/\bar{\delta})c^2\gamma^4$, where $c = c_1^{-1}\in Q$, δ, $\gamma = \beta/c_1\in P_4(= K)$. Thus (vii).

$w_n = 6$. We have $K = P_6 = Q(\sqrt{-3})$. By Lemma 13

$$\beta = c_1\gamma_1^2, \qquad c_1\in Q, \qquad \gamma_1\in K. \tag{34}$$

By Lemma 14

$$\beta = (\delta/\delta')\gamma_2^3, \qquad \delta, \gamma_2\in K. \tag{35}$$

Put $c = c_1N(\delta)$, $\gamma_3 = \gamma_1/c\delta$, $\gamma_4 = \gamma_2/c$. By (34) and (35)

$$\frac{1}{c^3}(\delta'/\delta)\beta = \gamma_3^2 = \gamma_4^3, \qquad \gamma_3, \gamma_4\in K.$$

Hence $\dfrac{1}{c^3}(\delta'/\delta)\beta = \gamma^6$, $c\in Q$, $\gamma\in K$ thus (vii). The lemma is proved.

Proof of Theorem 4. Necessity. Assume that $a = \vartheta^n$, $\vartheta\in Q^{\mathrm{mc}}$. $KP_n(\vartheta)$ is the splitting field of x^n-a over K. $KP_n(\vartheta)$ is abelian. By Lemma 7 $a^{w_n} = \beta^n$, $\beta\in K$. Hence

$$a = \varepsilon\beta^{n/w_n} = \vartheta^n, \qquad \varepsilon^{w_n} = 1. \tag{36}$$

Thus $\beta = \vartheta_1^{w_n}$, $\vartheta_1\in Q^{\mathrm{mc}}$. Necessity of the condition follows at once from Lemma 15 and from (36).

Sufficiency. Assume first (i) or (ii). If $c\in Q$ then $\sqrt{c}$ is cyclotomic. Since $w_n|w$ by Lemma 10 δ'/δ is the w_n-th power of a cyclotomic number. Hence a is the nth power of a cyclotomic number.

Assume that (iii) holds. It is enough to prove that $\sqrt{f}(a+\sqrt{f})$ is a square in Q^{mc}. By Lemma 10:

$$\frac{a+bi}{a-bi} = \theta^4, \qquad \theta\in Q^{\mathrm{mc}}.$$

Hence $(a+bi)\sqrt{f} = A^2$, $A \in Q^{mc}$ and $(a-bi)\sqrt{f} = \bar{A}^2$. Hence $A\bar{A} = f$ since f is positive. Hence

$$\sqrt{f}(a+\sqrt{f}) = \frac{(a+bi)\sqrt{f}+(a-bi)\sqrt{f}+2f}{2} = \frac{A^2+\bar{A}^2+2A\bar{A}}{2} = \left(\frac{A+\bar{A}}{\sqrt{2}}\right)^2,$$

where $(A+\bar{A})/\sqrt{2} \in Q^{mc}$. The proof is complete.

References

[1] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil I: *Klassenkörpertheorie*, Teil Ia: *Beweise zu Teil I*, Würzburg–Wien 1970.

[2] — *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil II: *Reziprozitätsgesetz*, Würzburg–Wien 1970.

[3] — *Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörper*, Abh. Deutsche Akad. Wiss. Berlin, Jahrgang 1948, No 2, Berlin 1950.

[4] Henry B. Mann, *Introduction to algebraic number theory*, Columbus 1955.

[5] Warren May, *Unit groups of infinite abelian extensions*, Proc. Amer. Math. Soc. 25 (1970), pp. 680–683.

[6] A. Rotkiewicz, *On the prime factor of the number* $2^{p-1}-1$, Glasgow Mathematical Journal 9 (1968), pp. 83–86.

[7] A. Schinzel, *Abelian polynomials, power residues and exponential congruences*, Acta Arith. 32 (1977), pp. 245–274.

[8] W. Y. Vélez, *On normal binomials*, Acta Arith. 36 (1980), pp. 113–124.

[9] J. Wójcik, *On the composite Lehmer numbers with prime indices II*, Prace Mat. 9 (1965), pp. 105–113.

[10] — *On the composite Lehmer numbers with prime indices III*, Colloq. Math. (in press).

Received on 31. 8. 1978
and in revised form on 18. 7. 1979 (1099)

ACTA ARITHMETICA
XL (1982)

Kummer congruences for the coefficients of Hurwitz series

by

CHIP SNYDER (Orono, Maine)*

1. Introduction. In L. Carlitz [3], it is shown that Hurwitz series $f(x)$ satisfying the differential equation

$$(f')^2 = 1 + \sum_{i=1}^{4} a_i f^i \qquad (a_i \in Z)$$

possess Kummer congruences. (These concepts are defined below.) However once the polynomial function on the right-hand side of the above equation has degree greater than four, Carlitz's methods fail to yield information about Kummer congruences. Nevertheless, he believed that when $f(x)$ satisfies

$$(f')^2 = 1+f^6$$

then f has Kummer congruences.

In this article we refine the machinery developed by Carlitz and solve the above problem in the affirmative. Moreover we show that of all Hurwitz series $f(x)$ satisfying in particular

$$(f')^2 = 1+f^m$$

for m an integer greater than 4, only for $m = 6$ does f have Kummer congruences.

Although this is the only application of the machinery developed that is given, the methods may be applied to other Hurwitz series satisfying more general differential equations.

2. An analysis of the Ω_p operator. Let R be an integral domain containing Z, the rational integers.

* Partially supported by University of Maine Summer Faculty Research Grant.