COLLOQUIUM MATHEMATICUM

VOL. XLV 1981 FASC. 1

ON THE COMPOSITE LEHMER NUMBERS WITH PRIME INDICES, III

BY

J. WÓJCIK (WARSZAWA)

Schinzel has deduced from his conjecture H (see [3], p. 95-96) a certain property of the so-called *Lehmer numbers*

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

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

Lehmer numbers can be also defined as follows:

$$P_1 = P_2 = 1, \quad P_n = \begin{cases} LP_{n-1} - MP_{n-2} & \text{if } n \text{ is odd,} \\ P_{n-1} - MP_{n-2} & \text{if } n \text{ is even.} \end{cases}$$

Schinzel's results are the following:

THEOREM I. *If $LM \neq 0$, $K = L - 4M \neq 0$ and none of the numbers $-KL$, $-3KL$, $-KM$, $-3KM$ is a perfect square or each of the numbers K, L is a perfect square, then there exists an integer $k > 0$ such that for each $D \neq 0$ there exists a prime q satisfying $q|P_s$, $(s, D) = 1$, where*

$$s = \frac{1}{k}\left(q - \left(\frac{KL}{q}\right)\right)$$

and $\left(\frac{KL}{q}\right)$ is Jacobi's symbol of quadratic character.

THEOREM II. *Under the assumptions of Theorem* I, *conjecture* H *implies the existence of infinitely many primes p such that $P_p(a, \beta)$ is composite.*

The afore-said conjecture H reads as follows:

H. *If $f_1, \ldots, f_k$ are irreducible polynomials with integral coefficients and positive leading coefficients such that the product $f_1(x) \ldots f_k(x)$ has no constant factor greater than 1, then there exist infinitely many positive integers x such that $f_1(x), \ldots, f_k(x)$ are primes.*

In [3] Schinzel conjectured that Theorems I and II remain valid under the single condition that α/β is not a root of unity, which is clearly necessary.

A partial result in this direction has been established in [4]. The aim of this paper is to prove the conjecture completely. We shall show

THEOREM 1. *If α and β are different from zero and α/β is not a root of unity, then there exists an integer $k > 0$ such that for every integer $D \neq 0$ there exists a prime q satisfying the condition*

$$q|P_{(q-1)/k}, \quad \left(\frac{q-1}{k}, D\right) = 1.$$

THEOREM 2. *If α and β are different from zero and α/β is not a root of unity, then conjecture H implies the existence of infinitely many primes p such that $P_p(\alpha, \beta)$ is composite.*

Remark. Theorem 1 is a little stronger than the theorem conjectured by Schinzel. Indeed, if q is sufficiently large (see the proof of Theorem 2) and $q|P_{(q-1)/k}(\alpha, \beta)$, then $(\alpha/\beta)^q \equiv \alpha/\beta \pmod{q}$ and q splits in $Q(\alpha/\beta) = Q(\sqrt{KL})$. Thus

$$\left(\frac{KL}{q}\right) = 1.$$

Theorem 1 is deduced from the following (see [5], Theorem 1)

THEOREM 1'. *Let f be an irreducible primitive polynomial with rational integer coefficients and a positive leading coefficient. Assume that f is different from x and is not a cyclotomic polynomial. Then 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 there exist infinitely many primes q satisfying the following condition:*

$q \equiv 1 \pmod{k}$, $q \equiv r \pmod{D}$, *the congruence* $f(x^k) \equiv 0 \pmod{q}$ *is soluble provided that* $(r, D) = 1$, *and* $r \equiv 1 \big(\bmod (D, k)\big)$.

The Dirichlet density σ of this set of primes satisfies the inequality

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

where

$$\varkappa = \begin{cases} 1 & \text{if } f \text{ is nonsymmetric,} \\ 2 & \text{if } f \text{ is symmetric,} \end{cases}$$

$n = \deg f$, *and $c(f)$, $C(f)$ denote certain positive integers depending on f.*

Notation. For a field $\Omega \subset K$, $N_{K/\Omega}(\cdot)$ is the norm from K to Ω, $N(\cdot) = N_{K/\Omega}(\cdot)$ if K is fixed. Q is the rational field, $\zeta_k = e^{2\pi i/k}$. If the extension k_2/k_1 is abelian, $f(k_2/k_1)$ denotes its conductor. If $\mathfrak{a}$, $\mathfrak{b}$ are ideals and F is a positive integer, then $\mathfrak{a} \sim \mathfrak{b} \pmod{F}$ means that $(\mathfrak{a}, F) = (\mathfrak{b}, F) = 1$ and $\mathfrak{a}/\mathfrak{b} = (a)$, $a \equiv 1 \pmod{F}$ and a is totally positive ($a \gg 0$). For x real, $[x]$ denotes the integer part of x. The k-th residue power symbol is denoted by $(-)_k$. For a field Ω, $|\Omega|$ denotes the absolute degree of Ω.

Proof of Theorem 1. Put

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

where f has rational integer coefficients, $a_0 > 0$, and f is primitive.

Put further $k = 2k_0$, where k_0 denotes the constant of Theorem 1′. Let D be any positive integer. $D = D_1 D_2$, where D_1 contains only prime factors dividing k and $(D_2, k) = 1$. Let r satisfy the congruences

$$r \equiv \begin{cases} k+1 \pmod{k^2}, \\ 2 \pmod{D_2}. \end{cases}$$

D_2 is odd since k is even. Hence $(r, Dk) = 1$ and $r \equiv 1 \pmod{k}$. The polynomial f is irreducible. Since α and β are different from zero and α/β is not a root of unity, f is different from x and is not cyclotomic. By Theorem 1′ there exists a prime q not dividing the product $a_0 KLM \operatorname{disc}(a_0\alpha/\beta)$ (where $\operatorname{disc}\xi$ denotes the discriminant of ξ) such that $q \equiv r \pmod{Dk}$ and the congruence $f(x^k) \equiv 0 \pmod{q}$ is soluble for some rational integer x. Hence $\big((q-1)/k, D\big) = 1$. By Lemma 11 in [5] we obtain $q | P_{(q-1)/k}$. The theorem is proved.

LEMMA 1. *Let l be a prime. If the congruence*

$$a_0 x^n + \ldots + a_n \equiv 0 \pmod{l^2}$$

has more than n roots distinct $\pmod{l}$, *then* $a_i \equiv 0 \pmod{l^2}$ *for* $i = 0, 1, \ldots, n$.

Proof. The congruence $a_0x^n + \ldots + a_n \equiv 0 \pmod{l}$ has more than n solutions distinct $\pmod{l}$. In virtue of Lagrange's theorem, $a_0 = la_0', \ldots \ldots, a_n = la_n'$, where $a_0', \ldots, a_n'$ are rational integers. The congruence $a_0'x^n + \ldots + a_n' \equiv 0 \pmod{l}$ has more than n solutions and, as before, $a_0' = la_0'', \ldots, a_n' = la_n''$, where $a_0'', \ldots, a_n''$ are rational integers. Hence $a_0 = l^2 a_0'', \ldots, a_n = l^2 a_n''$, i.e. the assertion of the lemma holds.

LEMMA 2. *Let l be a prime. If the congruence $a_0x^n + \ldots + a_n \equiv 0$ $\pmod{l^2}$ has roots $x_1, \ldots, x_n$ distinct* $\pmod{l}$, *then the following decomposition holds:*

$$a_0x^n + \ldots + a_n \equiv a_0(x-x_1)\ldots(x-x_n) \pmod{l^2}.$$

Proof. The congruence

$$a_0x^n + \ldots + a_n - a_0(x-x_1)\ldots(x-x_n) \equiv 0 \pmod{l^2}$$

has n solutions $x_1, \ldots, x_n$ distinct $(\bmod\, l)$. By Lemma 1, all coefficients of the polynomial appearing on the left-hand side are divisible by l^2, which was to be proved.

LEMMA 3. *Let K/Ω be an abelian extension, let $\mathfrak{f}$ be its conductor, and $a \in \Omega$. If $\mathfrak{m}$ is an integral ideal of Ω prime to a and to $\mathfrak{f}$, then there exists an $\alpha \in K$ prime to $\mathfrak{m}$ such that*

$$a \equiv N_{K/\Omega}(\alpha) \pmod{\mathfrak{m}}.$$

Proof. Let $\mathfrak{p}^{\nu} \| \mathfrak{m}$ [1], $\nu > 0$, $\mathfrak{p}$ a prime ideal of Ω. By formula (5′) in [2] (Teil II, p. 26),

$$\left(\frac{a, K}{\mathfrak{p}}\right) = 1,$$

where $\left(\frac{a, K}{\mathfrak{p}}\right)$ is the norm residue symbol. By II in [2] (Teil II, p. 33), there exists an $\alpha_{\mathfrak{p}} \in K$ prime to $\mathfrak{p}$ such that

$$a \equiv N_{K/\Omega}(\alpha_{\mathfrak{p}}) \pmod{\mathfrak{p}^{\nu}}.$$

Thus for a solution of the system of congruences it suffices to take $\alpha \equiv \alpha_{\mathfrak{p}} \pmod{\mathfrak{p}^{\nu}}$ for $\mathfrak{p}^{\nu} \| \mathfrak{m}$.

LEMMA 4. *Let k_2 be an abelian field, and k a positive integer. Assume that N_1 denotes the degree of k_2, and $g(x)$ is the minimal polynomial of an integer θ such that $k_2 = Q(\theta)$. If an integral ideal $\mathfrak{a}$ of k_2 and a positive integer F satisfy the condition*

$$\text{(i)} \qquad \begin{gathered} F \equiv 0 \ \big(\bmod\, k(2N_1)!\operatorname{disc} g\big), \quad N\mathfrak{a} \equiv 1 \pmod{k}, \\ (\mathfrak{a}, F) = 1, \quad \left(\frac{N\mathfrak{a}-1}{k}, F\right) = 1, \end{gathered}$$

then there exists a polynomial $f_1(x)$ such that the polynomials $f_1(x)$ and $f_2(x) = \big(f_1(x)-1\big)/k$ satisfy the assumptions of conjecture H. Moreover, if $q = f_1(x)$ is prime for some positive integer x, then $q = N\mathfrak{q}$, $\mathfrak{q} \sim \mathfrak{a}^{-1} \pmod{F}$, where $\mathfrak{q}$ is a prime ideal of degree 1 in k_2.

Proof. By Nagell's theorem there exists a prime $l > FN\mathfrak{a}$ such that the following congruences are soluble:

$$\text{(1)} \qquad g(x) \equiv 0 \pmod{l}, \qquad \Phi_{N_1}(y) \equiv 0 \pmod{l}, \qquad f(z) \equiv 0 \pmod{l},$$

[1] $\mathfrak{p}^{\nu} \| \mathfrak{m}$ means that $\mathfrak{p}^{\nu} | \mathfrak{m}$ and $\mathfrak{p}^{\nu+1} \nmid \mathfrak{m}$.

where Φ_{N_1} is the N_1-th cyclotomic polynomial, and $f(z) = z^{N_1}+N\mathfrak{a}+l$. Every prime factor of Φ_{N_1} either divides N_1 or satisfies $l \equiv 1 \pmod{N_1}$, and since the first case is excluded by $l > F$, $N_1|F$, we infer that $l \equiv 1 \pmod{N_1}$ and the congruence $f(z) \equiv 0 \pmod{l}$ has N_1 solutions distinct $(\mathrm{mod}\, l)$, say $z_1, \dots, z_{N_1}$. The existence of rational integers $z'_1, \dots, z'_{N_1}$ with $z'_i \equiv z_i \pmod{l}$ and $f(z'_i) \equiv 0 \pmod{l^2}$ follows now from Hensel's lemma, and Lemma 2 gives

(2) $$f(z) \equiv \prod_{i=1}^{N_1} (z-z'_i) \pmod{l^2}.$$

Since $(\mathfrak{a}, kl^2F) = 1$, there exists an integral ideal $\mathfrak{b}_1$ of k_2 such that

(3) $$\mathfrak{a}\mathfrak{b}_1 = \gamma_1, \quad (\mathfrak{b}_1, N\mathfrak{a}) = 1, \quad \gamma_1 \equiv 1 \pmod{kl^2F}, \quad \gamma_1 \gg 0.$$

Since $l \nmid \mathrm{disc}\, g$, l must be prime to $\mathrm{disc}\, k_2$ and the solvability of $g(x) \equiv 0 \pmod{l}$ implies that l splits completely in k_2:

(4) $$l = \mathfrak{l}_1 \dots \mathfrak{l}_{N_1},$$

$\mathfrak{l}_i$ being distinct and of degree 1.

By Chinese remainder theorem, for k_2 there exists an integer γ_2 $(\gamma_2 \in k_2)$ satisfying the system of congruences

(5) $$\gamma_2 \equiv \begin{cases} 1 \pmod{kF}, \\ -z'_i \pmod{\mathfrak{l}_i^2} \quad (i=1, \dots, N), \end{cases}$$

(5′) $$N(\gamma_2) \equiv 2/N\mathfrak{b}_1 \pmod{N\mathfrak{a}}, \quad \gamma_2 \gg 0,$$

where z'_i are rational integers occurring in factorization (2). (Note that if γ_2 is not totally positive, then $\gamma_2+xkl^2FN\mathfrak{a}$ is totally positive for a sufficiently large positive integer x.) Congruence (5′) is soluble in virtue of Lemma 3, since $(N\mathfrak{a}, 2N\mathfrak{b}_1 \mathrm{disc}\, k_2) = 1$ by (3), (i) and $\mathrm{disc}\, k_2 | \mathrm{disc}\, g$.

Put

(6) $$\gamma = \gamma_1\gamma_2.$$

Let μ be any totally positive integer generating k_2 and let z be a positive integer different from all numbers

(7) $$\frac{\gamma^{(i)}-\gamma}{(N\mathfrak{a})^2kFl^2(\mu-\mu^{(i)})} \quad (i = 2, \dots, N_1),$$

where $\xi^{(i)}$ denotes the i-th conjugate of ξ with respect to Q, $\mu^{(1)} = \mu$, $\gamma^{(1)} = \gamma$.

Put

(8) $$\Gamma = \gamma+kF(N\mathfrak{a})^2l^2z\mu.$$

Condition (7) means that $\Gamma \neq \Gamma^{(i)}$ for $i = 2, \ldots, N_1$, thus Γ generates k_2. Moreover, $\Gamma \gg 0$.

Put

$$f_1(x) = \frac{N(FN\mathfrak{a}x+\Gamma)}{N\mathfrak{a}} \quad \text{and} \quad f_2(x) = \frac{f_1(x)-1}{k}.$$

By (8), (6) and (3) we have

$$\Gamma = \mathfrak{a}\mathfrak{b}, \tag{9}$$

where $\mathfrak{b}$ is an integral ideal of k_2. Hence

$$N(\Gamma) = N\mathfrak{a}N\mathfrak{b}. \tag{10}$$

By (8), (6), (3) and (5) we obtain

$$\Gamma \equiv \gamma = \gamma_1\gamma_2 \equiv 1 \pmod{kF}, \qquad N(\Gamma) \equiv 1 \pmod{kF}. \tag{11}$$

By (10),

$$N(FN\mathfrak{a}x+\Gamma) \equiv N(\Gamma) \equiv 0 \pmod{N\mathfrak{a}},$$

which means that the polynomial $f_1(x)$ has rational integer coefficients.

We have $f_2(x) = f_3(x)/kN\mathfrak{a}$, where $f_3(x) = N(FN\mathfrak{a}x+\Gamma)-N\mathfrak{a}$. Since $k|F$, we get

$$f_3(x) \equiv N(\Gamma)-N\mathfrak{a} = N\mathfrak{a}\,(N\mathfrak{b}-1) \equiv 0 \pmod{kN\mathfrak{a}}$$

because $N\mathfrak{b} \equiv 1 \pmod{k}$ by (10), (11) and (i). This means that $f_2(x)$ has rational integer coefficients. The polynomials $f_1(x)$ and $f_2(x)$ have positive leading coefficients. The leading coefficient c of $f_1(x)f_2(x)$ is given by

$$c = \frac{1}{k}F^{2N_1}(N\mathfrak{a})^{2N_1-2}. \tag{12}$$

By (10),

$$f_1(0) = N\mathfrak{b} \quad \text{and} \quad f_2(0) = \frac{N\mathfrak{b}-1}{k}. \tag{13}$$

By (10), (8), (6), (3) and (5),

$$N\mathfrak{a}N\mathfrak{b} = N(\Gamma) \equiv N(\gamma) = N\mathfrak{a}N\mathfrak{b}_1N(\gamma_2) \equiv 2N\mathfrak{a}\left(\mathrm{mod}\,(N\mathfrak{a})^2\right).$$

Hence

$$N\mathfrak{b} \equiv 2 \pmod{N\mathfrak{a}}. \tag{14}$$

By (10), (11) and (i),

$$(N\mathfrak{b}, F) = \left(\frac{N\mathfrak{a}-1}{k}, F\right) = 1. \tag{15}$$

By (10) we have the identity

$$\frac{N(\Gamma)-1}{k} = N\mathfrak{b}\frac{N\mathfrak{a}-1}{k}+\frac{N\mathfrak{b}-1}{k}.$$

Hence, by (11), (13), (15), (14) and (i) we obtain

$$(16) \qquad \big(f_1(0)f_2(0), FN\mathfrak{a}\big) = 1$$

since $2|F$. By (12) this means that the polynomial $f_1(x)f_2(x)$ is primitive. Further, since $(2N_1)!|F$, from (16) we get $\big(f_1(0)f_2(0), (2N_1)!\big) = 1$. In virtue of Lagrange's theorem this implies that $f_1(x)f_2(x)$ has no fixed factor greater than 1. The polynomial $f_1(x)$ is irreducible since Γ generates the field k_2.

Since k_2 is normal, there exists an automorphism σ_i of k_2 such that

$$\sigma_i \mathfrak{l}_i = \mathfrak{l}_1, \quad \sigma_1 = 1 \quad (i = 1, \ldots, N_1),$$

where $\mathfrak{l}_i$ are prime ideals of k_2 occurring in factorization (4). By (8), (6), (3) and (5) we obtain

$$\Gamma \equiv -z_i' \,(\mathrm{mod}\, \mathfrak{l}_i^2) \quad (i = 1, \ldots, N_1).$$

Hence

$$\sigma_i \Gamma \equiv -z_i' \,(\mathrm{mod}\, \mathfrak{l}_1^2) \quad (i = 1, \ldots, N_1).$$

According to the definition of $f_3(x)$ we get further

$$f_3(x) = \prod_{i=1}^{N_1} (FN\mathfrak{a}x + \sigma_i\Gamma) - N\mathfrak{a} \equiv \prod_{i=1}^{N_1} (FN\mathfrak{a}x - z_i') - N\mathfrak{a}$$

$$\equiv (FN\mathfrak{a})^{N_1} x^{N_1} + l \,(\mathrm{mod}\, \mathfrak{l}_1^2)$$

by (2) and the definition of $f(z)$. Thus

$$f_3(x) \equiv (FN\mathfrak{a})^{N_1} x^{N_1} + l \,(\mathrm{mod}\, l^2),$$

since l is unramified in k_2. $N_1 = \deg f_3$ and, besides, as we know, $l > FN\mathfrak{a}$.

In virtue of Eisenstein's criterion the polynomial $f_2(x) = f_3(x)/kN\mathfrak{a}$ is irreducible. Thus we have shown that the polynomials $f_1(x)$ and $f_2(x)$ satisfy the assumptions of conjecture H. If $q = f_1(x)$ is prime for a certain $x > 0$, then $q = N\mathfrak{q}$, where $\mathfrak{q} = (FN\mathfrak{a}x + \Gamma)/\mathfrak{a}$ is an integral ideal of k_2 by (9), hence a prime ideal of degree 1. We have $\mathfrak{q} \sim \mathfrak{a}^{-1} \,(\mathrm{mod}\, F)$ by (11) and $\Gamma \gg 0$. The lemma is proved.

Proof of Theorem 2. Let k be a positive integer given in Theorem 1. Let us put

$$K = L - 4M, \quad k_1 = Q\left(\frac{a}{\beta}\right) = Q(\sqrt{KL}), \quad k_2 = k_1 Q(\zeta_k),$$

$$N_1 = |k_2|, \quad N(\cdot) = N_{k_2/Q}(\cdot).$$

Let g be the minimal polynomial of an integer θ such that $k_2=Q(\theta)$ and put

$$F=k(2N_1)!\,|(\operatorname{disc} g)KLM|\,N\left(f\left(\frac{k_2(\sqrt[k]{\alpha/\beta})}{k_2}\right)\right).$$

By Theorem 1 there exists a prime q_0 such that

$$(17)\qquad q_0|P_{(q_0-1)/k}(\alpha,\beta),\qquad \left(\frac{q_0-1}{k},F\left[\frac{F-1}{k}\right]!\right)=1.$$

Since $P_1=1$, it follows that $(q_0-1)/k>1$. Hence, by (17) and the definition of F,

$$(18)\qquad q_0>F\geqslant 2kKLM.$$

By (17),

$$(19)\qquad \left(\frac{\alpha}{\beta}\right)^{(q_0-1)/k}\equiv 1\ (\operatorname{mod} q_0).$$

Hence

$$(20)\qquad \left(\frac{\alpha}{\beta}\right)^{q_0}\equiv\frac{\alpha}{\beta}\ (\operatorname{mod} q_0).$$

We have

$$K=L-4M,\qquad M=\alpha\beta,\qquad \alpha=\frac{\sqrt{L}+\sqrt{K}}{2},\qquad \beta=\frac{\sqrt{L}-\sqrt{K}}{2},$$

$$\sqrt{KL}=2M\frac{\alpha}{\beta}-L+2M$$

for a suitable choice of square roots. Hence, by (20) and Fermat's theorem,

$$(21)\qquad (\sqrt{KL})^{q_0}\equiv(2M)^{q_0}\left(\frac{\alpha}{\beta}\right)^{q_0}-(L-2M)^{q_0}\equiv\sqrt{KL}\ (\operatorname{mod} q_0).$$

On the other hand,

$$(22)\qquad (\sqrt{KL})^{q_0}\equiv\left(\frac{KL}{q_0}\right)\sqrt{KL}\ (\operatorname{mod} q_0).$$

Since q_0 is odd,

$$\left(\frac{KL}{q_0}\right)=1.$$

This means that q_0 splits in $k_1=Q(\sqrt{KL})$; q_0 splits also in $Q(\zeta_k)$ since $q_0\equiv 1\ (\operatorname{mod} k)$ by (17). Thus q_0 splits in the composed field $k_2=k_1Q(\zeta_k)$ (see [2], Teil I, p. 50, 17).

There exists a prime ideal $\mathfrak{a}$ of k_2 such that

$$q_0 = N\mathfrak{a}. \tag{23}$$

Obviously, k_2 is abelian. By (17), (18) and the definition of F, condition (i) of Lemma 4 holds. In view of Lemma 4, the conjecture H implies that there exist infinitely many positive integers x such that $q = f_1(x)$ and $p = f_2(x)$ are primes. Again by Lemma 4,

$$q = N\mathfrak{q}, \quad \mathfrak{q} \sim \mathfrak{a}^{-1} \,(\mathrm{mod}\, F), \tag{24}$$

where $\mathfrak{q}$ is a prime ideal of degree 1 in k_2.

By Euler's criterion, (19), (23), and (18) we have

$$\left(\frac{a/\beta}{\mathfrak{a}}\right)_k = 1. \tag{25}$$

By (24) and (23) we get $q \equiv q_0^{-1} (\mathrm{mod}\, F)$, $q \equiv 1 \,(\mathrm{mod}\, k)$ (k_2 contains ζ_k). Hence by (18) and the definition of F, $(q, kKLM) = 1$. By (24) and (25),

$$\left(\frac{a}{\beta}\right)^{(q-1)/k} \equiv \left(\frac{a/\beta}{\mathfrak{q}}\right)_k = \left(\frac{a/\beta}{\mathfrak{a}}\right)_k^{-1} \equiv 1 \;(\mathrm{mod}\, \mathfrak{q})$$

in virtue of Artin's reciprocity law and Euler's criterion. Hence $\mathfrak{q} | P_{(q-1)/k}(a, \beta)$. Since $(q-1)/k = p$, by (24) we obtain

$$q | P_p(a, \beta). \tag{26}$$

For a moment we may assume without loss of generality that $L > 0$. Then for $K > 0$, in virtue of inequality (5) in [3], we have

$$|P_p(a, \beta)| \geqslant \left(\frac{1+\sqrt{5}}{2}\right)^{p-2}$$

and for $K < 0$, in virtue of (5′) also in [3], we obtain

$$|P_p(a, \beta)| \geqslant (\sqrt{2})^{p-\log^3 p} \quad \text{for } p > N(a, \beta). \tag{27}$$

Thus, in any case, for p large enough we have $|P_p(a, \beta)| > kp+1 = q$, and (26) implies that $P_p(a, \beta)$ is composite. Thus the assertion of Theorem 2 follows.

Remark. Using Baker's theorem [1] one can obtain an inequality stronger than (27), namely

$$|P_p(a, \beta)| \geqslant (\sqrt{2})^{p-c_1 \log p},$$

where $c_1 = c_1(a, \beta)$, $p \geqslant 2$, provided $L > 0$, $K < 0$, $M \neq 0$, and a/β is not a root of unity.

REFERENCES

[1] A. Baker, *A sharpening of the bounds for linear forms in logarithms*, Acta Arithmetica 21 (1972), p. 117-129.

[2] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil I, Ia, Teil II, Würzburg-Wien 1970.

[3] A. Schinzel, *On the composite Lehmer numbers with prime indices, I*, Prace Matematyczne 9 (1965), p. 95-103.

[4] J. Wójcik, *On the composite Lehmer numbers with prime indices, II*, ibidem 9 (1965), p. 105-113.

[5] — *Contributions to the Kummer extensions*, Acta Arithmetica 40 (1980), p. 155-174.

Reçu par la Rédaction le 15. 6. 1978