COLLOQUIUM MATHEMATICUM

VOL. LXIX 1995 FASC. 1

ON SYSTEMS OF COMPOSITE LEHMER NUMBERS WITH PRIME INDICES

BY

J. WÓJCIK*

1. Introduction. I proved in [3] two theorems about the so-called Lehmer numbers:

THEOREM I. *If α, 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*

$$q \mid P_{(q-1)/k}(\alpha, \beta), \qquad \left(\frac{q-1}{k}, D\right) = 1.$$

THEOREM II. *If α, 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.*

The Lehmer numbers are 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 the roots of the trinomial $z^2 - \sqrt{L}z + M$ and L, M are rational integers.

Here is an equivalent definition:

$$P_1 = P_2 = 1, \qquad P_n = \begin{cases} LP_{n-1} - MP_{m-2} & \text{if } n \text{ is odd,} \\ P_{n-1} - MP_{n-2} & \text{if } n \text{ is even,} \end{cases} \qquad n \geq 3.$$

Conjecture H was put forward by A. Schinzel (see [2], p. 188) and 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.

1991 *Mathematics Subject Classification*: Primary 11B39.

* J. Wójcik died on March 1, 1994 and the paper has been edited by A. Schinzel.

The aim of this paper is to extend the above results to the system of Lehmer numbers. Let $1 \le j \le s$ and let α_j, β_j be the roots of the trinomial $z^2 - \sqrt{L_j} z + M_j$, where L_j, M_j are rational integers.

We shall show

THEOREM 1. *If* $\alpha_j, \beta_j, \alpha_j - \beta_j$ $(1 \le j \le s)$ *are different from zero and the multiplicative group generated by the numbers* $\alpha_1/\beta_1, \ldots, \alpha_s/\beta_s$ *is torsion-free, then there exists a positive integer* k *such that for every positive integer* D *there exists a prime* q *satisfying the condition*

$$q \mid P_{(q-1)/k}(\alpha_1, \beta_1), \ldots, q \mid P_{(q-1)/k}(\alpha_s, \beta_s), \qquad \left(\frac{q-1}{k}, D\right) = 1.$$

THEOREM 2. *If* $\alpha_j, \beta_j, \alpha_j - \beta_j$ $(1 \le j \le s)$ *are different from zero and the multiplicative group generated by the numbers* $\alpha_1/\beta_1, \ldots, \alpha_s/\beta_s$ *is torsion-free, then Conjecture H implies the existence of infinitely many primes* p *such that the numbers* $P_p(\alpha_1, \beta_1), \ldots, P_p(\alpha_s, \beta_s)$ *are all composite.*

It is easy to see that all assumptions of Theorem 1 are essential. As to Theorem 2 we shall prove much more. Namely, we shall prove that the numbers $P_p(\alpha_1, \beta_1), \ldots, P_p(\alpha_s, \beta_s)$ are positive and divisible by the same prime not dividing $pM_1 \ldots M_s$.

The proof of Theorems 1 and 2 is based on Theorem 1 of [4] which we quote below with some changes in notation:

THEOREM 1′. *Let* K *be an algebraic number field. Let* $\alpha'_1, \ldots, \alpha'_s \in K^*$. *Assume that the multiplicative group generated by* $\alpha'_1, \ldots, \alpha'_s$ *is torsion-free. There exists a positive integer* k_0 *such that for every positive integer* k *divisible by* k_0 *and for all positive integers* F *and* t, *with* $(t, F) = 1$, $t \equiv 1 \bmod k$ *and* $F \equiv 0 \bmod k$, *there exist infinitely many prime ideals* $\mathfrak{q}$ *of degree one of* $K(\zeta_k)$ *such that*

$$\left(\frac{\alpha'_1}{\mathfrak{q}}\right)_k = 1, \ldots, \left(\frac{\alpha'_s}{\mathfrak{q}}\right)_k = 1, \qquad N\mathfrak{q} \equiv t \bmod F.$$

2. Proof of Theorems 1 and 2. Let D be any positive integer. Put $\alpha'_j = \alpha_j/\beta_j$ $(1 \le j \le s)$, $K = \mathbb{Q}(\alpha'_1, \ldots, \alpha'_s)$, $k = 2k_0$, where k_0 denotes the constant in Theorem 1′. Moreover, let $K_2 = K(\zeta_k)$, let n_2 be the degree of K_2 and $N(\cdot) = N_{K_2/\mathbb{Q}}(\cdot)$. If an extension Ω_1/Ω_2 is abelian, $f(\Omega_1/\Omega_2)$ denotes its conductor. Let g be the minimal polynomial of an integer θ such that $K_2 = \mathbb{Q}(\theta)$. Let us put

$$F = k(2n_2)! \Big| \operatorname{disc}(g) \prod_{j=1}^{s} N(f(K_2(\sqrt[k]{\alpha_j})/K_2)) \Big| D. \tag{1}$$

Further, put $\overline{F} = kF$ and $F = F_1F_2$, where F_1 contains only prime factors dividing k and $(F_2, k) = 1$.

Let t satisfy the congruences

$$t \equiv \begin{cases} k + 1 \bmod k^2, \\ 2 \bmod F_2. \end{cases}$$

Now, F_2 is odd since k is even. Hence

$$(t, \overline{F}) = 1, \quad t \equiv 1 \bmod k \quad \text{and} \quad \left(\frac{t-1}{k}, F\right) = 1. \tag{2}$$

By Theorem 1′ there exists a prime ideal $\mathfrak{q}_0$ of degree one of K_2 such that

$$\left(\frac{\alpha_1'}{\mathfrak{q}_0}\right)_k = 1, \ldots, \left(\frac{\alpha_s'}{\mathfrak{q}_0}\right)_k = 1, \quad N\mathfrak{q}_0 \equiv t \bmod \overline{F}, \tag{3}$$
$$N\mathfrak{q}_0 \text{ is sufficiently large so that } \mathfrak{q}_0 \nmid \beta_j(\alpha_j - \beta_j).$$

By (1)–(3),

$$\begin{aligned} &F \equiv 0 \bmod k(2n_2)!\,\mathrm{disc}(g), \quad N\mathfrak{q}_0 \equiv 1 \bmod k, \\ &(\mathfrak{q}_0, F) = 1, \quad \left(\frac{N\mathfrak{q}_0 - 1}{k}, F\right) = 1. \end{aligned} \tag{4}$$

Put $q = N\mathfrak{q}_0$. Then q is a prime. By (3) and Euler's criterion,

$$(\alpha_j/\beta_j)^{(q-1)/k} \equiv \left(\frac{\alpha_j'}{\mathfrak{q}_0}\right)_k = 1 \bmod \mathfrak{q}_0.$$

Hence $\mathfrak{q}_0 \mid P_{(q-1)/k}(\alpha_j, \beta_j)$ and

$$q \mid P_{(q-1)/k}(\alpha_j, \beta_j) \quad (1 \le j \le s).$$

Further, by (4) and (1), $\left(\frac{q-1}{k}, D\right) = 1$, which proves Theorem 1.

Next we shall prove Theorem 2. By Lemma 5 of [4] and by (4) there exists a polynomial $f_1(x)$ such that the polynomials $f_1(x)$ and $f_2(x) = (f_1(x) - 1)/k$ satisfy the assumption of Conjecture H. By this conjecture there exist infinitely many positive integers x such that $q = f_1(x)$ and $p = f_2(x)$ are primes. Again by Lemma 5 of [4],

$$q = N\mathfrak{q}', \quad \mathfrak{q}' \sim \mathfrak{q}_0^{-1} \bmod F, \tag{5}$$

where $\mathfrak{q}'$ is a prime ideal of degree one of K_2.

By (5), (3), (1) and Euler's criterion,

$$(\alpha_j/\beta_j)^{(q-1)/k} \equiv \left(\frac{\alpha_j'}{\mathfrak{q}'}\right)_k = \left(\frac{\alpha_j'}{\mathfrak{q}_0}\right)_k^{-1} = 1 \bmod \mathfrak{q}'$$

in view of Artin's reciprocity law. Hence $\mathfrak{q}' \mid P_{(q-1)/k}(\alpha_j, \beta_j)$ and

$$q \mid P_p(\alpha_j, \beta_j) \qquad (1 \le j \le s) \tag{6}$$

because $(q-1)/k = p$.

Put $\Delta_j = L_j - 4M_j$ $(1 \le j \le s)$. We may assume without loss of generality that $L_j > 0$ for each j. Assume that $\Delta_1 > 0, \ldots, \Delta_u > 0$, $\Delta_{u+1} < 0, \ldots, \Delta_s < 0$.

For $1 \le j \le u$ by inequality (5) of [1] we have

$$|P_p(\alpha_j, \beta_j)| \ge \left(\frac{1+\sqrt{5}}{2}\right)^{p-2} \tag{7}$$

and for $u+1 \le j \le s$ by inequality (5′) of [1] we obtain

$$|P_p(\alpha_j, \beta_j)| \ge (\sqrt{2})^{p-\log^3 p} \qquad \text{for } p > N(\alpha_j, \beta_j). \tag{8}$$

By (7) and (8) for sufficiently large p we have

$$|P_p(\alpha_j, \beta_j)| > kp + 1 = q$$

and (6) implies that the numbers $P_p(\alpha_j, \beta_j)$ are composite. ∎

REFERENCES

[1] A. Schinzel, *On the composite Lehmer numbers with prime indices*, *I*, Prace Mat. 9 (1965), 95–103.

[2] A. Schinzel et W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. 4 (1958), 185–208, Correction, ibid. 5 (1959), 259.

[3] J. Wójcik, *On the composite Lehmer numbers with prime indices*, *III*, Colloq. Math. 45 (1981), 81–90.

[4] —, *On a problem in algebraic number theory*, Math. Proc. Cambridge Philos. Soc., to appear.

Reçu par la Rédaction le 15.6.1994