On primitive prime factors of Lehmer numbers II

by

A. SCHINZEL (Warszawa)

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,

\[ P_n(a, \beta) = \begin{cases} (a^n - \beta^n)/(a - \beta), & n \text{ odd}, \\ (a^n - \beta^n)/(a^n - \beta), & n \text{ even}, \end{cases} \]

where \(\alpha\) and \(\beta\) are roots of the trinomial \(x^3 - D^{3/2}x + M\), and \(L\) and \(M\) are rational integers, \(K = L - 4M \neq 0\). Further, \(\bar{z}\) denotes the complex conjugate of any given \(z\) and \(k_n(n)\) 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 \(D^3\) is rational, \(K^3\) is an irrational integer of the field \(K(\zeta_n)\), \(K\) is divisible by the cube of the discriminant of this field, \(n = k_n(M)\) is squarefree,

\[ n_e = \begin{cases} 2 & \text{if } e = 6, M \equiv 3 (\text{mod }4), \\ 1 & \text{otherwise}, \end{cases} \]

and \(n|n_n\), is an integer relatively prime to \(e\), then for \(n > n_4(L, M)\), \(P_n\) has at least \(e\) primitive prime factors, and \(n_4(L, M)\) can be effectively computed.

**Lemma.** Let \(e, m, n\) be positive integers, \(n|e\), and let \(\chi\) be a character \(\text{mod } n\) such that \(\chi + \chi = \chi\) and that for all \(i \neq 0 (\text{mod } e)\) characters \(\chi^i\) are primitives. Further, let

\[ \tau_i = \tau(\chi^i|n) = \sum_{(\nu|n)} \chi^i(\nu)\zeta_n, \]

let \(\chi_n\) be a character \(\text{mod } n\) induced by \(\chi\), and let \(\chi(-1)^{n/e}\) be any fixed \(e\)-th root of \(\chi(-1)\).
Then, there exist polynomials \( A_i(x, y) \) (0 ≤ i < e) with coefficients from the field \( K(\xi) \) such that

\[
\psi(x_i; x, y) = \prod_{j=0}^{n} (x - x_i - (1 - 1)\xi_j \chi_{0}(y)) \\
= A_i(x, y) + \sum_{r=1}^{e-1} \chi^{(r)}(y) A_i(x, y^r),
\]

(1)

\[
A_i(x, y) = A_i(y, x),
\]

(2)

\[
A_i(x, y) = A_{i-e}(y, x) x^{e-i} (1 - 1) (0 < i < e).
\]

Proof. In the course of this proof we shall denote by \( a_i, a_1, \ldots, b_i, b_1, \ldots, a_i, a_1, \ldots \) the numbers of the field \( K(\xi) \), by \( p(\xi, \eta, \ldots) \)

and \( s(\xi, \eta, \ldots) \) the th function of the indeterminates \( \xi, \eta, \ldots \), respectively. We have

(3)

\[
\psi(x_i; x, y) = \prod_{j=0}^{n} (x - x_i - (1 - 1)\xi_j \chi_{0}(y)) = \sum_{s=0}^{e-n} (-1)^{s+1} y^{s} \psi(x_i(1)\chi_{0}, \ldots, x_i(-1)\chi_{n})
\]

and by the Newton formulae

\[
\psi = \sum_{a_0, a_1, \ldots, a_n} \frac{a_0}{a_0} \frac{a_1}{a_1} \cdots \frac{a_n}{a_n}
\]

On the other hand,

\[
x_i(1)\chi_{0}, \ldots, x_i(-1)\chi_{n} = \sum_{r=0}^{n} x_i^{(r)}(1)\chi_{0} = \tau(x_i(1)\chi_{0}),
\]

Now, it follows from well-known results ([1], § 20, theorem IV) that under the conditions assumed with regard to character \( \chi \), \( \tau(x_i(1)\chi_{0}) \) can be different from zero only if

\[
i \equiv 0 \pmod{m} \quad \text{or} \quad m \mid n
\]

and in the latter case

\[
\tau(x_i(1)\chi_{0}) = \tau(x_i^{(1)}(1)\chi_{0}) \times \left| \frac{n}{\phi(n)} \right| \phi(n)(m, i),
\]

if \( i \equiv 0 \pmod{m} \),

\[
\tau(x_i(1)\chi_{0}) = \tau(x_i^{(1)}(1)\chi_{0}) \times \left| \frac{n}{\phi(n)} \right| \phi(n)(m, i),
\]

if \( m \mid n \).

This implies that

(4)

\[
\psi(x_i(1)\chi_{0}, \ldots, x_i(-1)\chi_{n}) = \sum_{\eta_i + \eta_2 + \cdots + \eta_n = f} b_{\eta_0, \eta_1, \ldots, \eta_n} \eta_0 \eta_1 \cdots \eta_n.
\]

Now, it follows from other well-known results ([1], § 20, theorem VIII) that for suitable \( \theta_i, \tau_i, \eta_i \), thus if

\[
a_1 + 2a_2 + \cdots + ka_k = j \pmod{e},
\]

we have

(5)

\[
\psi(x_i; x, y) = A_i(x, y) + \sum_{i=0}^{e-1} \chi^{(i)}(y) A_i(x, y^i),
\]

where

\[
A_i(x, y) = \sum_{a_0, a_1, \ldots, a_n} (-1)^{e-n-a_0} b_{a_0, a_1, \ldots, a_n} e^{e-n} \tau_0 \tau_1 \cdots \tau_n,
\]

\[
A_i(x, y) = \sum_{a_0, a_1, \ldots, a_n} (-1)^{e-n-a_0} b_{a_0, a_1, \ldots, a_n} e^{e-n} \tau_0 \tau_1 \cdots \tau_n (0 < i < e)
\]

are polynomials with coefficients from the field \( K(\xi) \).

To prove formulae (1) and (2), notice that

\[
\prod_{i=1}^{n} (x - x_i) = x^{(n)}(x) = x^{(-1)^{n} x_{0}} x^{(-1)^{n} x_{0}}
\]

It follows that

\[
\psi(x_i; x, y) = \prod_{i=1}^{n} (x - x_i)^{(-1)^{n} x_{0}} x^{(-1)^{n} x_{0}}
\]

\[
= \prod_{i=1}^{n} (x - x_i)^{(-1)^{n} x_{0}} x^{(-1)^{n} x_{0}} \prod_{i=1}^{n} (y - x_{0})^{(-1)^{n} x_{0}}
\]

\[
= x^{(-1)^{n} x_{0}} \prod_{i=1}^{n} (x - x_i) = \psi(x_i; y, x).
\]
Applying formula (6) successively to $\psi(x; \pm x, y)$ and $\psi(y; y, x)$ and taking into account the well-known equality

$$
\psi(\pm x; \pm x, y) = (-1)^j \psi(\mp x; \pm x, y)
$$

we find (1) and (2).

**Lemma 2.** If $e = 3, 4$ or 6 and $\omega$ is a product of normalized irrational primes of the field $K(\zeta_e)$ such that $m = \omega \bar{\omega}$ is squaresafe and $(m, e) = 1$, then there exists a primitive root of unity $\zeta_m$ and a character $\chi$ satisfying the condition of Lemma 1 such that

$$
\tau(\zeta_m) = \zeta_m^{1/2} \chi(\zeta_m^{1/2})
$$

Here $\arg \omega = \frac{1}{e} \arg \omega$, $\arg \bar{\omega} = \frac{1}{e} \arg \bar{\omega}$ and $\zeta_m(1) = (\zeta_m^{1/2})^e$ is any fixed $\zeta_m$-th root of unity.

(4, $\mathfrak{c}$)-th root of $\chi(\zeta_m)$ and

$$
\chi(\zeta_m)^{1/2} = \zeta_m^{1/2} \chi(\zeta_m^{1/2})
$$

Proof. Let $\omega = \pi_1 \pi_2 \ldots \pi_k$ be the factorization of $\omega$ in the field $K(\zeta_e)$ into normalized irrational primes. Since $\omega \bar{\omega}$ is squaresafe, numbers $p_j = \pi_j \pi_j$ ($j < k$) are distinct rational primes, and since $(\omega \bar{\omega}, e) = 1$, $p_j \bar{p}_j$. Now, for $e = 3, 4, 6$ there exist two characters $\chi \mod p_j$, such that $\chi^p_j = \chi$ and all $\chi^p_j (0 < i < e)$ are primitive. It follows from the formula, given in (1), § 20.4 that for one of these characters, which we denote by $\chi_i$,

$$
\tau(\chi_i) = \chi_i(\zeta_m^{1/2}) = (-1)^{1/2 \log \zeta_m \log \pi_j} - 1, \chi_i
$$

whence by (7)

$$
\tau(\chi_i) = \chi_i(\zeta_m^{1/2}) = (-1)^{1/2 \log \zeta_m \log \pi_j} - 1.
$$

Further, it follows from the connection between $\tau(\chi_i \zeta_2)$ and $\tau(\chi_i \zeta_2)$ (cf. [1], § 20, theorem IX) that

$$
\tau(\chi_i \zeta_2) = \pi_j \pi_j^{-2} + \chi_i(\zeta_m^{1/2})
$$

Finally, formula (7) implies that for $e = 6$

$$
\tau(\chi_i \zeta_2) = \chi_i(\zeta_m^{1/2})
$$

Formulae (9)-(13) can be written together as follows:

$$
\tau(\chi_i \zeta_2) = \chi_i(\zeta_m^{1/2}) (e = 3, 4, or 6).
$$

Put

$$
\zeta_m = \prod_{j=1}^k \zeta_j, \quad \chi = \prod_{j=1}^k \chi_j.
$$

It follows from the properties of characters $\chi$, that $\chi^p$ are primitive characters $\mod m$ for all $i \neq 0 (\mod e)$. Besides, we find from (14) and a well-known theorem ([1], § 20, theorem VIII) that

$$
\tau(\chi_i \zeta_m) = \tau(\chi_i \zeta_m) \chi_i(\zeta_m^{1/2}) = \chi_i(\zeta_m^{1/2})
$$

It follows hence that

$$
\tau(\chi_i \zeta_m) = \chi_i(\zeta_m^{1/2}) \chi_i(\zeta_m^{1/2}) = \chi_i(\zeta_m^{1/2})
$$

and by (7)

$$
\chi_i(\zeta_m^{1/2}) = \chi_i(\zeta_m^{1/2}) \chi_i(\zeta_m^{1/2}) = \chi_i(\zeta_m^{1/2})
$$

which completes the proof.

Proof of the theorem. Since $k_0(\alpha \beta) = k_0 \alpha \beta$, there exist two integers $\alpha$ and $\beta$ of the field $K(\zeta_e)$ such that $\alpha = a \alpha_0$ and $\alpha_0 = \beta \beta_0$. On the other hand, by the assumption about $K$ we have

$$
K = 0 (\mod 27) \quad (e = 3 or 6), \quad K = 0 (\mod 64) \quad (e = 4).
$$

Therefore, since $K = L - 4 M, (L, M) = 1$,

$$(M, e) = (a \alpha_0, e) = 1$$

and $a \text{ fortiori} (a \alpha_0, e) = 1$.

It follows from the latter equality that $K_0 = 0 \mod (1 - \zeta_6)$. Since also $K_0 = 0 \mod (1 - \zeta_6)$, we get $K = 0 \mod (1 - \zeta_6)$. Since $\omega$ is squaresafe, $a \alpha_0$ is not divisible by any rational prime and thus $\omega = \omega$ is a product of normalized irrational primes. But $P_\alpha = \omega \omega_0$, $P_\alpha \omega_0 = \pm P_\alpha(a \beta, \beta)$, therefore we can assume that $\omega$ itself has the said property. Applying Lemma 2 to $\omega$ we find a character $\chi$ satisfying the conditions of Lemma 1 and such that formulae (1), (2) hold. Let $\chi_0 \omega_0$ be the induced character $\mod \bar{\omega}_0$ (by the assumption $\chi_0 \mod \bar{\omega}_0$, and let $(-1)^{1/2}$ be any fixed $\mathfrak{c}$-th root of $\chi(\zeta_m)$.

Now, for $i = 0, 1, \ldots, e - 1$, put

$$
Q^0_e(a \beta, \beta) = \psi(\chi_0 \omega_0 ^{a \beta}, \beta),
$$

where

$$
\alpha^{1/2} = a, \omega_0^{1/2}, \quad \beta^{1/2} = \alpha^{1/2}.
$$
Further, it follows from (16) as in the analogous situation in [3], that the common prime factors of any two numbers \( Q^m(a, \beta) \) must divide the discriminant of \( x_{m} - 1 \), equal to \( e_{m} \). However, by Lemma 1 of [3], no prime factor of \( e_{m} \) can divide \( Q_m(a, \beta) \) with an exponent \( > 1 \). Thus the numbers \( Q^m(a, \beta) \) are relatively prime in pairs, and in order to prove the theorem it suffices, again by Lemma 1 of [3], to establish the inequality

\[
|Q^m(a, \beta)| > n \quad (0 < i < \epsilon).
\]

To this end, notice that by Lemma 3 of [3]

\[
\log |Q^m(a, \beta)| < \frac{\varphi(n)}{e} \log |a| + 2en^{1/4} \log^2 n.
\]

On the other hand, by the fundamental lemma of [2], we have for \( n > N(a, \beta) \)

\[
\log |Q^m(a, \beta)| > \left( \frac{\varphi(n)}{e} - 2en^{1/4} \log^2 n \right) \log |a| - 2e(e-1)n^{1/2} \log^2 n.
\]

Since \( \frac{\varphi(n)}{e} \) is odd and for \( n > 10^8 \)

\[
\left( \frac{\varphi(n)}{e} - 2en^{1/4} \log^2 n \right) \log^2 n - 2e(e-1)n^{1/2} \log^2 n > \log n \quad (e \leq 6)
\]

inequality (18) certainly holds for

\[
\frac{\varphi(n)}{e} - 2en^{1/4} \log^2 n > \log n
\]

and the theorem is proved.

References