On primitive prime factors of Lehmer numbers I

by

A. SCHINZEL (Warszawa)

Lehmer numbers are called terms of the sequences

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

where \( a \) and \( \beta \) are roots of the trinomial \( x^n - L x^2 + M \), and \( L \) and \( M \) are rational integers (cf. [4]). Without any essential loss of generality (cf. [9]) we can assume that

\[ L > 0, \quad M \neq 0, \quad K = L - 4M \neq 0. \] (1)

Lehmer numbers constitute a generalisation of the numbers \( a^n - b^n \) \( (a, b - \text{rational integers}) \). A prime \( p \) is called a primitive prime factor of a number \( a^n - b^n \) if

\[ p | a^n - b^n \quad \text{but} \quad p \nmid a^k - b^k \quad \text{for} \quad k < n. \]

A proper (not merely automatical) generalization of this notion for Lehmer numbers is the notion of a prime factor \( p \) such that

\[ p | P_n \quad \text{but} \quad p \nmid KLP_1 \ldots P_{n-1}. \]

or, which is easily proved to be equivalent,

\[ p | P_n \quad \text{but} \quad p \nmid P_1 \ldots P_{n-1}. \]

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 \( p | P_n \) but \( p \nmid KLP_1 \ldots P_{n-1} \).
Assume that, besides the restrictions on $L, M$ stated in (1),

\[(L, M) = 1, \quad \langle L, M \rangle \neq (1, 1), (2, 1), (3, 1)\]

(i.e. \(\beta/a\) 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:

for \(K > 0\) if \(n = 5 \neq 1, \langle L, M \rangle = (1, -1), n = 10, \langle L, M \rangle = (5, 3), n = 19, \langle L, M \rangle = (1, -5), (5, 1)\)

for \(K < 0\) if \(n \leq n_0(L, M)\)

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. Rokrkiwicz [5] generalized this theorem to so-called Lucas numbers (which correspond to Lehmer numbers for \(L \in \mathbb{Q}\) 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 \(\mathcal{R}, \mathcal{R}\):

\[\mathcal{R} = \{(L, M): (L, M) = 1, \langle L, M \rangle = (12, 25), (12, 25)\text{ or }\]
\[1 \leq |M| \leq 5, 2M + 2|L| + 1 \leq L \]
\[< \min \{64 + 2M - 2|L|, 2M + 2|L| + 4|L|^{1/4}\}\}\]

\[\mathcal{R} = \{(L, M): (L, M) = 1, \langle L, M \rangle = (4, -1), (8, 1)\text{ or }\]
\[1 \leq |M| \leq 15, L = 2M + 2|L| + 1\} \]

As can easily be verified, set \(\mathcal{R}\) consists of 184 and set \(\mathcal{R}\) of 32 pairs \((L, M)\).

For an integer \(n \neq 0\), let \(k(n)\) denote the square-free kernel of \(n\), that is a divisor by its greatest square factor. The following theorem holds.

**Theorem 1.** For \(L, M\) satisfying (1), (2), put \(n = k(M \max(K, L))\) and

\[\eta = \begin{cases} 1 & \text{if } x = 1 \pmod{4}, \\ 2 & \text{if } x = 2, 3 \pmod{4}. \end{cases} \]

If \(n \neq 1, 2, 3, 4, 6\) and \(n/\eta\) is an odd integer, then \(P_n\) has at least two primitive prime factors except:

1. for \(K > 0\) if \(n = n_0(x)\), \(\langle L, M \rangle \in \mathcal{R}_0 \subset \mathcal{R}\) or \(n = 3n_0|x|\); \(\langle L, M \rangle \in \mathcal{R}_0 \subset \mathcal{R}\) or \(n = 5, \langle L, M \rangle = (9, 1)\) or \(n = 10, \langle L, M \rangle = (5, 1)\) or \(n = 20, \langle L, M \rangle = (3, -1), (3, 1)\).

2. for \(K < 0\) if \(n \leq n_0(L, M)\).

Finite sets \(\mathcal{R}_0, \mathcal{R}_0, \eta\) and function \(n_0(L, M)\) can be effectively computed.

Let us observe that the sequences \(P_n\) and \(P_n\) corresponding to \(\langle L, M \rangle\) and \(\langle \max(K, L), |M| \rangle\), respectively, are connected by the relation

\[P_n = \begin{cases} P_\eta & \text{if } M > 0 \text{ or } n \text{ even} , \\ P_\eta P_n & \text{if } M < 0 \text{ and } n \text{ odd}. \end{cases} \]

Therefore the primitive prime factors of \(P_n\) coincide with those of \(P_\eta\) if \(M > 0 \text{ or } n = 0 \pmod{4}\), with those of \(P_\eta\) if \(M < 0 \text{ and } n = 2 \pmod{4}\) and with those of \(P_\eta\) if \(M < 0 \text{ and } n = 1 \pmod{2}\). The remarks that

1. \(\langle L, M \rangle \in \mathcal{R} \text{ or } \mathcal{R}\) if and only if \(\langle \max(K, L), |M| \rangle \in \mathcal{R} \text{ or } \mathcal{R}\), respectively,

2. \(\sgn x = \sgn M\),

3. if \(x\) is even, \(\eta\)'s corresponding to \(x\) and \(\rho - x\) are equal; if \(x\) is odd, the product of these \(\eta\)'s is 2,

show that it suffices to prove the theorem for \(M > 0, x = k(M \max(K, L)) = k(LM)\).

Before proceeding further, we introduce some notation and recall some useful results from paper [6]. For any integer \(a > 0\) let

\[Q_a(x, y) = \prod_{i=0}^{n-1} (x - \zeta^n y), \]

where \(\zeta^n\) is a primitive \(n\)th root of unity. Put \(Q_a(x) = Q_a(x, 1)\) 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 \(\eta\), and write \(r = npol, A = \alpha^{2n}, B = \beta^{2n}\). To obtain conformity of notation with paper [6] one should make in the latter the following permutation of letters: \(\Phi \rightarrow \Phi, P \rightarrow R, Q \rightarrow S\).

Then by Theorem 1 of [9] and remark that \(r > 2,

\[Q_a(x) = \psi_a(x)\psi_a(-x), \]

where \((1)\)

\[\psi_a(x) = R_{\alpha}(\alpha^2 - x_{1/2}^2) \psi_{\alpha}(\alpha^2) (n \geq 0), \]

\[\prod_{(\alpha, x) = 1} (x - (r) \zeta^n) \]

\[= \prod_{(\alpha, x) = 1} (x + (r) \zeta^n) \psi_{\alpha}(\alpha^2) \]

\[\prod_{(\alpha, x) = 1} (x - (r) \zeta^n) \]

\(R, S\) are polynomials with rational integral coefficients.

(1) \((r)\) is Jacobian's symbol of quadratic character.
Let us put, similarly as in [6], for $\varepsilon = \pm 1$,

$$Q_0^\varepsilon(a, \beta) = \nu_\omega(A^{1/2}, B^{1/2}),$$

where $A^{1/2} = \frac{1}{2} \arg A$, $A^{1/2} = \frac{1}{2} \arg B$. Then, if $a, \beta$ are real, $a > \beta > 0$, we have for $\varepsilon = \pm 1$

$$Q_0^\varepsilon(a, \beta) > \left( \max \{ A^{1/2} - B^{1/2}, \{ A + B \}^{1/2} \} \right)^{\varepsilon / 2}$$

(7) $$Q_0^\varepsilon(a, \beta) > \left( \max \{ A^{1/2} - B^{1/2}, \{ A + B \}^{1/2} \} \right)^{\varepsilon / 2}$$

(8) $$Q_0^\varepsilon(a, \beta) > (2^{-1/2}(A - B)A^{1/2}B^{-1/2})^{\varepsilon / 2}$$

These inequalities were proved in [6] under the assumption that $a, \beta$ are rational integers; however, the proof does not change if $a, \beta$ are arbitrary real numbers.

Now we shall prove 3 lemmas

**Lemma 1.** If $n$ satisfies the assumptions of Theorem 1, $M > 0$, $p | Q_0(a, \beta)$ and $p$ is not a primitive prime factor of $P_n(a, \beta)$, then $p^2 | Q_0(a, \beta)$, and if $n = 2^s (r \text{ prime})$, then $p = q(n) = q(1 )$. If $n = 2^r (r \text{ prime})$, $r | Q_0(a, \beta)$ if and only if $r | L$.

**Proof.** It follows from Theorems 3.3 and 3.4 of [4] that if the assumptions of the lemmas are satisfied and $n \neq 12$, then $p^2 | Q_0(a, \beta)$ and $p = q(n)$.

On the other hand, as can easily be verified,

$$Q_0(a, \beta) = \sum_{\substack{k = 0 \\ k \neq 0}} a_k L^{k(n - 1)} M^d$$

where $a_k = \pm 1$, unless $n = 2^s (r \text{ prime})$. For $n = 2^s$, $a_k = \pm 1$, so that $r | Q_0(a, \beta)$ if and only if $r | L$. For $n \neq 2^s$ we have, in view of (L, M) = 1, $(p, LM) = 1$ so if $(p, \alpha) = 1$. Since all prime factors of $a$ divide $\nu_\omega(a)$, the lemma is thus proved for all $n \neq 12$.

If $n = 12$, then $Q_0(a, \beta) = L^2 - 12 M^2 + M^4$; if $p | Q_0(a, \beta)$, then in view of $(L, M) = 1$, $p = 2$ or 3. On the other hand, it follows from $12 = \nu_\omega(a)$ that $a$ is even, $\nu_\omega(a)$ is even and $p \neq 2$. Thus $p = 3$ is a primitive prime factor of $P_n(a, \beta)$, which completes the proof.

**Lemma 2.** If $n$ satisfies the assumptions of Theorem 1, $M > 0$ and $\delta = \kappa(L)^{-\omega(n/4)}$, then the numbers $\delta Q_0^\varepsilon(a, \beta)$ and $\delta Q_0^{\varepsilon - 1}(a, \beta)$ are coprime rational integers ($\delta$).

**Proof.** We show first that $\psi_\omega(a)$ (i.e.) are reciprocal polynomials. For instance, let $\nu = 3 ( \text{mod} 4 )$. We have by (5)

$$\psi_\omega(a) = \prod_{\nu = 1} (a^{\nu} + i (r | a)^{\nu} = x^{\nu} - i (r | a)^{\nu} \right) \prod_{\nu = 1} (a - i (r | a)^{\nu} = x^{\nu} - i (r | a)^{\nu} \right)$$

$$Q_0^\varepsilon(a, \beta) = \frac{1}{2} \left[ \psi_\omega(x^{\nu} + (r | a)^{\nu}, x^{\nu} - (r | a)^{\nu} \right]$$

and

$$Q_0^{\varepsilon - 1}(a, \beta) = \frac{1}{2} \left[ \psi_\omega(x^{\nu} + (r | a)^{\nu}, x^{\nu} - (r | a)^{\nu} \right]$$

Since in view of (4)

$$R_{\delta}(x) = \frac{1}{2} \left[ \psi_\omega(x^{\nu} + (r | a)^{\nu}, x^{\nu} - (r | a)^{\nu} \right]$$

it follows that polynomials $R, S$ are reciprocal. We now prove that these polynomials are of degree $\frac{1}{2} \omega(n)$ and $\frac{1}{2} \omega(n - 1)$, respectively. In fact

$$Q_0(x) = R(x) = \frac{1}{2} \omega(n),$$

whence degree $S < \omega(n)$. On the other hand, supposing that degree $S < \frac{1}{2} \omega(n)$, we find

$$E(x) = x^{2\omega(n)} + ax^{\omega(n)-1} + bx^{\omega(n)-2} + ...$$

we should find by comparing both sides of (9) that

$$2\omega(n) - \mu(r) = \omega(n)-1 = \omega(n)-1 + ...$$

$$\mu(r) = -2a = 0$$

and, in view of the definition of $\nu$, $\nu = 2 ( \text{mod} 4)$. Since $\psi_\omega(a) = \psi_\omega(x^{\nu})$, identity (9) gives again

$$\psi_\omega(x^{\nu}) = \psi_\omega(x^{\nu}) + ... = \psi_\omega(x^{\nu}) + ...$$

$$\mu(\nu) = -2b = 0$$

which is impossible, because $\nu$ is square-free.

It follows from the above that $(x + y)^{2\omega(n)} E(x, y) = (x + y)^{-\omega(n)} S(x, y)$ are homogeneous symmetric functions of $x, y$ of dimension 0; so they are rationally expressible in terms of $(x + y)^{2}$ and any, and thus $(A + B)^{2\omega(n)} E(A, B), (A + B)^{-\omega(n)} S(A, B)$ are rationally expressible by $(A + B)^{2}$ and $AB$. In their turn $(A + B)^{2}$, $AB$ and $(A + B)(a + \beta)$ are rationally expressible by $(a + \beta)^{2}$ and $a\beta$. Therefore numbers

$$A^2 E(A, B) = (a + \beta)^{2\omega(n)} \left( \frac{A + B}{a + \beta} \right)^{2\omega(n)}$$

$$A^2 S(A, B) = (a + \beta)^{2\omega(n)} \left( \frac{A + B}{a + \beta} \right)^{2\omega(n)}$$

are rationally expressible by $(a + \beta)^{2}$ and $a\beta$ and $a\beta - M$ and as such are rational.

Since for $\varepsilon = \pm 1$

$$\delta Q_0^\varepsilon(a, \beta) = \delta R(A, B) \pm \frac{A + B}{a + \beta} \delta \left( \frac{A + B}{a + \beta} \right)^{2\omega(n)}$$

and numbers

$$\frac{A + B}{a + \beta}, \left( \frac{A + B}{a + \beta} \right)^{2\omega(n)} = \pm \frac{A^2}{a\beta} \delta, \left( \frac{A + B}{a + \beta} \right)^{2\omega(n)} = \pm \frac{LM \delta}{\kappa(L, M)}$$

(9) [5] and (v) denote the integral and the fractional part of $\alpha$, respectively.
are rational, the numbers \( \delta Q^0(a, \beta) \) are also rational. If \( \varphi(n) = 0 \) (mod 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 \( \varphi(n) \neq 0 \) (mod 4) and \( k(L) \neq 1 \). Since \( n \neq 1, 2, 4 \), we have

\[
 n = r^a \quad \text{or} \quad n = 2^a, \quad r \text{ prime } 3 \text{ (mod 4)}.
\]

Since \( k(L) \neq n, k(L) \) is odd, we get \( k(L) = n = 2^a \). We have to prove that the numbers \( r^{-1/2} Q^0(a, \beta) \) are algebraic integers. First, since \( \delta = 1 \), it is clear from formula (4) that their difference is integral. Now in view of the formula (3) and (6)

\[
 Q(a, \beta) = Q^0(a, \beta) Q^B(a, \beta);
\]

their product is therefore \( r^{-1/2} Q(a, \beta) \) and is integral by Lemma 1. Thus the numbers \( r^{-1/2} Q(a, \beta) \) are themselves integral. So we have proved that the numbers \( \delta Q^0(a, \beta) (e = \pm 1) \) are rational integers. It remains to prove that they are coprime.

By identity (3) the resultant \( R \) of polynomials \( \psi(x), \psi(-x) \) divides the discriminant of \( Q_a(x) \) and therefore also the discriminant of \( x^a - 1 \), which is \( (2)^{2a} \). There exist polynomials \( \chi^0(x), \chi^{(-1)}(x) \) such that

\[
 \chi^0(x) \psi(x) + \chi^{(-1)}(x) \psi(-x) = R
\]

identically in \( x \). The coefficients of \( \chi^0(x), \chi^{(-1)}(x) \) are expressible integrally in terms of the coefficients of \( \psi(x) \) and therefore are algebraic integers. On making the above relation homogeneous in \( x, y \) and putting \( x = \lambda \), \( y = \delta \), we deduce that any common prime factor of \( \delta Q^0(a, \beta) \) and \( \delta Q^B(a, \beta) \) must divide \( 2a \). By Lemma 1 and (10) each prime factor of \( \delta Q^0(a, \beta) (e = \pm 1) \) is a primitive prime factor of \( P_a \), except possibly for \( p(n) \), which then occurs to the first power only. Since no prime factor of \( 2a \) can be a primitive prime factor of \( P_a \), \( \delta Q^0(a, \beta) \) is relatively prime. The proof of the lemma is thus complete.

**Lemma 3.** If \( \chi(r) \) is an arbitrary character (mod \( m \), \( m > 1 \) and \( |x| = 1 \), then

\[
\Pi = \prod_{\chi(r) = \text{cong to } 0} |x - \chi(r)| < \exp(2m^{1/3} \log^2 m).
\]

**Proof.** We can assume without the loss of generality that \( \arg \alpha = 2\pi/m \). Let \( \epsilon \) be the least positive exponent such that \( \chi^{(1)} = \chi \). If \( \epsilon = 1 \) much stronger estimation for \( \Pi \) is known (cf. [1]), if \( \epsilon = \varphi(m) \), the lemma is satisfied trivially, and thus we can assume \( \varphi(m) > \epsilon > 0 \).

\( \epsilon \) The idea of this proof is due to P. Erdős. An earlier proof of the writer led to a weaker estimation for \( \Pi \).
Since on the other hand, \(\prod_{i=1}^{k-1} (1 - z_i) = k\) and \(k = \varphi(m)/\{e < m/2\}\), we get
\[
H \leq 2 \prod_{i=1}^{k-1} \left(1 - \frac{z_i}{n-1}\right) \prod_{i=1}^{k-1} \left(1 - \frac{z_i}{n-1}\right) \leq \exp\left(2m^{1/2} \log^2 \left(1 + \log^2 \frac{m}{n}\right)\right) \leq \exp\left(2m^{1/2} \log^2 \left(\frac{m}{n}\right)\right).
\]

This proves the lemma.

Proof of the theorem. 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
\[
|Q_{\alpha, \beta}^n(a, \beta)| > \begin{cases} 
1, & \text{if } q(l) < q(n) \text{ and } e = 2^r, r \text{ as below}, \\
q(l), & \text{if } q(l) = q(n) \text{ and } e = 2^r, r \text{ as above}, \\
q(l), & \text{if } n = 2^r, r = k(L) \text{ prime } \equiv 3 \pmod{4}, \\
q(l), & \text{if } n = 2^r, r \text{ as above}. 
\end{cases}
\]

The proof of this inequality is different if \(a, \beta\) are real (\(K > 0\)) and if they are complex (\(K < 0\)); consequently the proof is divided into 2 parts.

1. \(K > 0\). If \(n > q = q(n)\), we apply (7) and find
\[
|Q_{\alpha, \beta}^n(a, \beta)| > \begin{cases} 
(2 - \frac{1}{2})^{\psi(n)} (\varphi(n) + \varphi(2n)), & \text{if } a = \frac{1}{n} - \frac{1}{2}, \\
\varphi(n), & \text{if } a = \frac{1}{n} - \frac{1}{2}, \frac{1}{n} - \frac{1}{2} > 1. 
\end{cases}
\]

Now, as can easily be verified, \(\varphi(n) + \varphi(2n) > 2\varphi(n)\) for all \(L, M\), so that
\[
|Q_{\alpha, \beta}^n(a, \beta)| > \begin{cases} 
\varphi(n), & \text{if } n = 2^r, r = k(L) \text{ prime } \equiv 3 \pmod{4}, \\
\varphi(n), & \text{if } n = 2^r, r \text{ as above}. 
\end{cases}
\]

and inequality (14) holds. Thus we can assume that \(n = r, A = \alpha, B = \beta\).

We shall consider successively \(l = 1, 2, 3 \) and \(l \geq 5\).

If \(l = 1,\) we have to prove
\[
|Q_{\alpha, \beta}^n(a, \beta)| > 1 \text{ if } n = 2^r, r \text{ as below}, 
\]
\[
|Q_{\alpha, \beta}^n(a, \beta)| > 1 \text{ if } n = 2^r, r \text{ as above}.
\]

Now, if \(|Q_{\alpha, \beta}^n(a, \beta)| \leq 1\), we have by inequality (7)
\[
1 > \alpha^{18} - \frac{18}{1} = \frac{18}{1}, 
\]
so that \(L < 4M + 4M^{1/3} + 1, L < 64\). Since \(4M < L\), we get \(M = \{e < m/2\}\) and \(\{e < m/2\}\). It remains to consider the case \(n = 2^r, r \text{ prime } \equiv 3 \pmod{4}, r \geq 7\) (since \(n = 6\), \(k(L) = r, k(M) = 1\)). By (7) we have
\[
|Q_{\alpha, \beta}^n(a, \beta)| > \left(\max(L^{1/2} - 2M^{1/2}, 1)^{1/2}\right)^{1/2}.
\]

Since \(r = r - 1\), it suffices to establish the inequality
\[
\max(L^{1/2} - 2M^{1/2}, 1)^{1/2} > r^{(r-1)}.
\]

Since \(r \geq 7, r^{(r-1)} < 7^{18} < 2^{30}\), 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 \(\langle L, M \rangle \in \mathbb{R}\\ or \langle L, M \rangle = (112, 25)\).

Suppose now that \(l = 3\). If \(q(n) > 3\) it is again sufficient to prove (15). By (8) we have
\[
|Q_{\alpha, \beta}^n(a, \beta)| > 2^{30} q(n) \geq 1
\]

unless \(1 > 2^{30} q(n) \geq 2^{30} K^{18}, i.e. K = 1\). Since, as we already know,
\[
|Q_{\alpha, \beta}^n(a, \beta)| > 1 \text{ unless } \langle L, M \rangle \in \mathbb{R}\\ or \langle L, M \rangle = (3, 1, 1).
\]

It remains to consider \(l \geq 5\). Here we notice first that for all \(\langle L, M \rangle\) in question
\[
2^{30} K^{18} a \geq 5 \text{ or } \langle L, M \rangle = (9, 1),
\]
\[
2^{30} K^{18} a \geq 5 \text{ or } \langle L, M \rangle = (3, 1, 1),
\]
\[
2^{30} K^{18} a \geq 5 \text{ or } \langle L, M \rangle = (9, 2).
\]

It follows that, if \(\langle L, M \rangle = (3, 1, 1), (9, 1, 1), (9, 2),
\]
\[
(2 - \frac{1}{2})^{\psi(n)} > 5,
\]
hence also for all \(l \geq 5\)
\[
(2 - \frac{1}{2})^{\psi(n)} > q(n),
\]
and inequality (14) follows by (8).

If \(\langle L, M \rangle = (5, 1, 1), (9, 1, 1), (9, 2),\) we find directly
\[
(2 - \frac{1}{2})^{\psi(n)} > 1;
\]
hence (17) holds if \(q(n) > 1\). It remains to consider the cases \(\langle L, M \rangle = (5, 1, 1), (9, 1, 1), (9, 2),\) \(l = 5\) or 15. Their direct examination leads to the exceptions stated in the theorem. The proof for \(K > 0\) is complete.
On primitive prime factors of Lehmer numbers I

2. $K < 0$. By the fundamental lemma of [7]

$$|Q(x, y)| > |a^{(m-n)}| \log n$$

for $n > N(x, y)$.

On the other hand, by (5) and (6), $Q(x, y)$ can easily be represented as the products of $B^{(m-n)}$ and 2 or 1 expressions of the form

$$\prod_{\chi(r) = \chi(m)} |x - r|,$$

where $x = -A^{1/2}B^{-1/2} + iA^{1/2}B^{-1/2}$, and $\chi(r)$ is a real character mod $n = x$ or $4x$, respectively. Since $|A^{1/2}B^{-1/2}| = 1$, $m < 2n$, we get by Lemma 3

$$|Q(x, y)| < |a^{(m-n)}| \exp(4(2n)^{1/2}(\log 2n)^2).$$

It follows from (10), (18), and (19), that for $n > N(a, b)$

$$|Q(a, b)| > |a^{(m-n)}| \exp(-4(2n)^{1/2}(\log 2n)^2).$$

Since, however, if $K < 0, |a| > 2^{1/2}$ and for $n > 10^{10}$

$$\log 2^{1/2}(4\psi(x) - 2^{1/2}(\log x)^2 - 4(2n)^{1/2}(\log 2n)^2) > \log x,$$

we find for $n > \max(N(a, b), 10^{10})$

$$|Q(a, b)| > n,$$

which completes the proof.

Let us remark that Theorem 1 implies the following.

**Corollary.** If $k = 1$, $K > 0$, $n$ is odd, then $P_n$ has at least two primitive prime factors, except for $n = 5, 7, 11, 19, 18, 18$.

It follows that all terms from the fifth onwards of the above sequences $P_n$ are composite.

**Theorem 2.** If $k = \max(K, L) = \pm 1, \pm 2$, then $\lim_{n \to \infty} q(P_n) / n = 2$.

The theorem follows at once from two lemmas.

**Lemma 4.** If $P_n$ is an arbitrary Lehmer sequence and $n$ runs through all numbers $k = 0 \mod 4$, then

$$\lim_{n \to \infty} q(P_n) / n = 2.$$

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 $k = 0 \mod 4$, then

$$\lim_{n \to \infty} q(P_n) / n = 2.$$

**References**


*Reçu par la Rédaction le 30. 6. 1963*