[2] S. Knapowski, *On sing-changes in the remainder-term in the prime-number formula*, Journ. London Math. Soc. 36 (1961), pp. 451-460.

[3] — and W. Staś, *A note on a theorem of Hardy and Littlewood*, Acta Arith. 7 (1962), pp. 161-166.

[4] — and P. Turán, *Comparative prime number theory I-VIII*, Acta Math. Acad. Sc. Hungaricae (under press).

[5] P. Turán, *Eine neue Methode in der Analysis und deren Anwendungen*, Budapest 1953.

Reçu par la Rédaction le 25. 6. 1962

ACTA ARITHMETICA
VIII (1963)

On primitive prime factors of Lehmer numbers I

by

A. SCHINZEL (Warszawa)

Lehmer numbers are called terms of the sequences

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

where α and β are roots of the trinomial $z^2-L^{1/2}z+M$, and L and M are rational integers (cf. [4]). Without any essential lost of generality (cf. [9]) we can assume that

$$L>0\,,\quad M\neq 0\,,\quad K=L-4M\neq 0\,. \tag{1}$$

Lehmer numbers constitute a generalization of the numbers a^n-b^n (a, b — 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

$$p\,|\,P_n \quad \text{but} \quad p\nmid KLP_3\ldots P_{n-1}$$

or, which is easily proved to be equivalent,

$$p\,|\,P_n \quad \text{but} \quad p\nmid nP_3\ldots P_{n-1}\,.$$

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 $p\nmid KLP_3\ldots P_{n-1}$.*

Assume that, besides the restrictions on L, M stated in (1),

$$(L, M) = 1, \quad \langle L, M\rangle \neq \langle 1,1\rangle, \langle 2,1\rangle, \langle 3,1\rangle \tag{2}$$

(i.e. β/α 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 $n = 5$, $\langle L, M\rangle = \langle 1, -1\rangle$, $n = 10$, $\langle L, M\rangle = \langle 5, 1\rangle$, $n = 12$, $\langle L, M\rangle = \langle 1, -5\rangle$, $\langle 5, 1\rangle$

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

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. Rotkiewicz [5] generalized this theorem to so-called Lucas numbers (which correspond to Lehmer numbers for $L^{1/2}$ 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 $\mathfrak{M}$, $\mathfrak{N}$:

$$\begin{aligned}\mathfrak{M} = \{\langle L, M\rangle\colon (L, M) = 1;\ &\langle L, M\rangle = \langle 12, -25\rangle, \langle 112, 25\rangle \text{ or} \\ &1 \leqslant |M| \leqslant 15,\ 2M + 2|M| + 1 \leqslant L \\ &< \min(64 + 2M - 2|M|, 2M + 2|M| + 4|M|^{1/2} + 1)\},\end{aligned}$$

$$\begin{aligned}\mathfrak{N} = \{\langle L, M\rangle\colon (L, M) = 1,\ &\langle L, M\rangle = \langle 4, -1\rangle, \langle 8, 1\rangle \text{ or} \\ &1 \leqslant |M| \leqslant 15,\ L = 2M + 2|M| + 1\}.\end{aligned}$$

As can easily be verified, set $\mathfrak{M}$ consists of 184 and set $\mathfrak{N}$ of 32 pairs $\langle L, M\rangle$.

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

THEOREM 1. *For L, M satisfying* (1), (2), *put* $\varkappa = k\big(M\max(K, L)\big)$ *and*

$$\eta = \begin{cases} 1 & \text{if } \varkappa \equiv 1 \pmod 4, \\ 2 & \text{if } \varkappa \equiv 2, 3 \pmod 4. \end{cases}$$

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

1. *for $K > 0$, if $n = \eta|\varkappa|$, $\langle L, M\rangle \in \mathfrak{M}_0 \subset \mathfrak{M}$ or $n = 3\eta|\varkappa|$, $\langle L, M\rangle \in \mathfrak{N}_0 \subset \mathfrak{N}$ or $n = 5$, $\langle L, M\rangle = \langle 9, 1\rangle$ or $n = 10$, $\langle L, M\rangle = \langle 5, -1\rangle$ or $n = 20$, $\langle L, M\rangle = \langle 1, -2\rangle, \langle 9, 2\rangle$;*
2. *for $K < 0$, if $n \leqslant n_1(L, M)$.*

Finite sets $\mathfrak{M}_0$, $\mathfrak{N}_0$ and function $n_1(L, M)$ can be effectively computed.

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

$$P_n = \begin{cases} \overline{P}_n & \text{if } M > 0 \text{ or } n \text{ even}, \\ \overline{P}_{2n}/\overline{P}_n & \text{if } M < 0 \text{ and } n \text{ odd}. \end{cases}$$

Therefore the primitive prime factors of P_n coincide with those of $\overline{P}_n$ if $M > 0$ or $n \equiv 0 \pmod 4$, with those of $\overline{P}_{\frac{1}{2}n}$ if $M < 0$ and $n \equiv 2 \pmod 4$ and with those of $\overline{P}_{2n}$ if $M < 0$ and $n \equiv 1 \pmod 2$. The remarks that

1. $\langle L, M\rangle \in \mathfrak{M}$ or $\mathfrak{N}$ if and only if $\langle \max(K, L), |M|\rangle \in \mathfrak{M}$ or $\mathfrak{N}$, respectively,
2. $\operatorname{sgn}\varkappa = \operatorname{sgn} M$,
3. if $\varkappa$ is even, η's corresponding to $\varkappa$ and $-\varkappa$ are equal; if $\varkappa$ is odd, the product of these η's is 2,

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

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

$$Q_n(x, y) = \prod_{\substack{r=1 \\ (r,n)=1}}^{n} (x - \zeta_n^r y),$$

where ζ_n is a primitive nth root of unity. Put $Q_n(x) = Q_n(x, 1)$ 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 $\eta\varkappa$, and write $\nu = \eta\varkappa l$, $A = \alpha^{n/\nu}$, $B = \beta^{n/\nu}$. To obtain conformity of notation with paper [6] one should make in the latter the following permutation of letters: $\Phi \to Q$, $P \to R$, $Q \to S$.

Then by Theorem 1 of [6] and remark that $\nu > 2$,

$$Q_\nu(x^2) = \psi_{\nu,\varkappa}(x)\psi_{\nu,\varkappa}(-x), \tag{3}$$

where (¹)

$$\psi_{\nu,\varkappa}(x) = R_{\varkappa l,\varkappa}(x^2) - \varkappa^{1/2} x S_{\varkappa l,\varkappa}(x^2) \quad (\varkappa^{1/2} > 0), \tag{4}$$

$$= \begin{cases} \prod\limits_{(r,\varkappa l)=1} \big(x - (r|\varkappa)\zeta_{\varkappa l}^r\big) & \text{if } \varkappa \equiv 1 \pmod 4, \\ \prod\limits_{(r,\varkappa l)=1} \big(x + i(r|\varkappa)\zeta_{\varkappa l}^r\big) & \text{if } \varkappa \equiv 3 \pmod 4, \\ \prod\limits_{\substack{(r,4\varkappa l)=1 \\ (\varkappa|r)=1}} (x - \zeta_{4\varkappa l}^r) & \text{if } \varkappa \equiv 2 \pmod 4 \end{cases} \tag{5}$$

and R, S are polynomials with rational integral coefficients.

(¹) $(r|\varkappa)$ is Jacobi's symbol of quadratic character.

Let us put, similarly as in [6], for $\varepsilon = \pm 1$,

$$Q_n^{(\varepsilon)}(\alpha, \beta) = \psi_{\nu,\varkappa}(A^{1/2}, \varepsilon B^{1/2}) , \tag{6}$$

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

$$|Q_n^{(\varepsilon)}(\alpha, \beta)| > \left(\max\left(A^{1/2} - B^{1/2}, \left(\tfrac{1}{8}A + \tfrac{1}{8}B\right)^{1/2}\right)\right)^{\varphi(\nu)} , \tag{7}$$

$$|Q_n^{(\varepsilon)}(\alpha, \beta)| > \left(2^{-1/2}(A-B)A^{\frac{1}{2}q(l)-\frac{3}{2}}\right)^{\varphi(\nu')} \qquad \left(l \geqslant 3,\ \nu' = \nu/q(l)\right) . \tag{8}$$

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

Now we shall prove 3 lemmas

LEMMA 1. *If n satisfies the assumptions of Theorem 1, $M > 0$, $p \mid Q_n(\alpha, \beta)$ and p is not a primitive prime factor of $P_n(\alpha, \beta)$, then $p^2 \nmid Q_n(\alpha, \beta)$, and if $n \neq 2r^a$ (r prime), then $p = q(n) = q(l)$. If $n = 2r^a$ (r prime), $r \mid Q_n(\alpha, \beta)$ if and only if $r \mid L$.*

Proof. It follows from Theorems 3.3 and 3.4 of [4] that if the assumptions of the lemma are satisfied and $n \neq 12$, then $p^2 \nmid Q_n(\alpha, \beta)$ and $p = q(n)$. On the other hand, as can easily be verified,

$$Q_n(\alpha, \beta) = \sum_{i=0}^{\frac{1}{2}\varphi(n)} a_i L^{\frac{1}{2}\varphi(n)-i} M^i$$

where $a_0 = 1$ and $a_{\frac{1}{2}\varphi(n)} = \pm 1$, unless $n = 2r^a$ (r prime). For $n = 2r^a$, $a_{\frac{1}{2}\varphi(n)} = \pm r$, so that $r \mid Q_n(\alpha, \beta)$ if and only if $r \mid L$. For $n \neq 2r^a$ we have, in view of $(L, M) = 1$, $(p, LM) = 1$ so $(p, \varkappa) = 1$. Since all prime factors of n divide $\eta\varkappa l$, the lemma is thus proved for all $n \neq 12$.

If $n = 12$, then $Q_n(\alpha, \beta) = L^2 - 4LM + M^2$; if p is an imprimitive prime factor of $P_n(\alpha, \beta)$, then $L \equiv kM \pmod{p}$ for some $k \leqslant 4$. Hence, if $p \mid Q_n(\alpha, \beta)$, then in view of $(L, M) = 1$, $p = 2$ or 3. On the other hand, it follows from $12 = \eta\varkappa l$ that $\varkappa$ is even, LM is even and $p \neq 2$. Thus $p = 3 = l$ and $p^2 \nmid Q_n(\alpha, \beta)$, which completes the proof.

LEMMA 2. *If n satisfies the assumptions of Theorem 1, $M > 0$ and $\delta = k(L)^{-\{\varphi(n)/4\}}$, then the numbers $\delta Q_n^{(1)}(\alpha, \beta)$ and $\delta Q_n^{(-1)}(\alpha, \beta)$ are coprime rational integers* (¹).

Proof. We show first that $\psi_{\nu,\varkappa}(x)$ $(\nu > 1)$ are reciprocal polynomials. For instance, let $\varkappa \equiv 3 \pmod 4$. We have by (5)

$$\psi_{\nu,\varkappa}(x^{-1}) = \prod_{(r,\varkappa l)=1} \left(x^{-1} + i(r|\varkappa)\zeta_{\varkappa l}^{r}\right) = x^{-\varphi(\nu)} \prod_{(r,\varkappa l)=1} \left(i(r|\varkappa)\zeta_{\varkappa l}^{r}\right) \prod_{(r,\varkappa l)=1} \left(x - i(r|\varkappa)\zeta_{\varkappa l}^{-r}\right)$$
$$= x^{-\varphi(\nu)} i^{\varphi(\nu)} (-1)^{\frac{1}{2}\varphi(\nu)} \prod_{(r,\varkappa l)=1} \left(x + i(-r|\varkappa)\zeta_{\varkappa l}^{-r}\right) = x^{-\varphi(\nu)} \psi_{\nu,\varkappa}(x) .$$

(¹) $[x]$ and $\{x\}$ denote the integral and the fractional part of x, respectively.

Since in view of (4)

$$R_{\varkappa l,\varkappa}(x) = \tfrac{1}{2}\left(\psi_{\nu,\varkappa}(x^{1/2}) + \psi_{\nu,\varkappa}(-x^{1/2})\right)$$

$$S_{\varkappa l,\varkappa}(x) = \frac{1}{2(\varkappa x)^{1/2}}\left(\psi_{\nu,\varkappa}(x^{1/2}) - \psi_{\nu,\varkappa}(-x^{1/2})\right) ,$$

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

$$Q_\nu(x) = R^2(x) - \varkappa x S^2(x) , \tag{9}$$

whence degree $S <$ degree $R = \frac{1}{2}$ degree $Q_\nu = \frac{1}{2}\varphi(\nu)$. On the other hand, supposing that degree $S < \frac{1}{2}\varphi(\nu) - 1$,

$$R(x) = x^{\frac{1}{2}\varphi(\nu)} + a x^{\frac{1}{2}\varphi(\nu)-1} + b x^{\frac{1}{2}\varphi(\nu)-2} + \dots$$

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

$$x^{\varphi(\nu)} - \mu(\nu) x^{\varphi(\nu)-1} + \dots = x^{\varphi(\nu)} + 2a x^{\varphi(\nu)-1} + \dots ,$$

whence $\mu(\nu) = -2a = 0$ and, in view of the definition of ν, $\varkappa \equiv 2 \pmod 4$. Since $Q_\nu(x) = Q_{\frac{1}{2}\nu}(x^2)$, identity (9) gives again

$$x^{\varphi(\nu)} - \mu(\tfrac{1}{2}\nu) x^{\varphi(\nu)-2} + \dots = x^{\varphi(\nu)} + 2b x^{\varphi(\nu)-2} + \dots ,$$

$\mu(\frac{1}{2}\nu) = -2b = 0$, which is impossible, because $\frac{1}{2}\nu$ is square-free.

It follows from the above that $(x+y)^{-\frac{1}{2}\varphi(\nu)} R(x, y)$, $(x+y)^{1-\frac{1}{2}\varphi(\nu)} S(x, y)$ are homogeneous symmetric functions of x, y of dimension 0; so they are rationally expressible in terms of $(x+y)^2$ and xy, and thus $(A+B)^{-\frac{1}{2}\varphi(\nu)} \times R(A, B)$, $(A+B)^{-1-\frac{1}{2}\varphi(\nu)} S(A, B)$ are rationally expressible by $(A+B)^2$ and AB. In their turn $(A+B)^2$, AB and $(A+B)/(\alpha+\beta)$ are rationally expressible by $(\alpha+\beta)^2$ and $\alpha\beta$. Therefore numbers

$$\delta R(A, B) = (\alpha+\beta)^{2\left[\frac{\varphi(\nu)}{4}\right]} \left(\frac{A+B}{\alpha+\beta}\right)^{\frac{1}{2}\varphi(\nu)} (A+B)^{-\frac{1}{2}\varphi(\nu)} R(A, B) ,$$

$$\delta \frac{S(A+B)}{A+B} = (\alpha+\beta)^{2\left[\frac{\varphi(\nu)}{4}\right]} \left(\frac{A+B}{\alpha+\beta}\right)^{\frac{1}{2}\varphi(\nu)} (A+B)^{-1-\frac{1}{2}\varphi(\nu)} S(A, B)$$

are rationally expressible by $(\alpha+\beta)^2 = L$ and $\alpha\beta = M$ and as such are rational.

Since for $\varepsilon = \pm 1$

$$\delta Q_n^{(\varepsilon)}(\alpha, \beta) = \delta R(A, B) \pm \frac{A+B}{\alpha+\beta}\left(\frac{AB}{\alpha\beta}\right)^{1/2} \left(\varkappa(\alpha+\beta)^2\alpha\beta\right)^{1/2} \delta \frac{S(A, B)}{A+B}$$

and numbers

$$\frac{A+B}{\alpha+\beta}, \quad \left(\frac{AB}{\alpha\beta}\right)^{1/2} = \pm(\alpha\beta)^{(n-\nu)/2\nu}, \quad \left(\varkappa(\alpha+\beta)^2\alpha\beta\right)^{1/2} = \varkappa\left(\frac{LM}{k(LM)}\right)^{1/2}$$

are rational, the numbers $\delta Q_n^{(\varepsilon)}(\alpha, \beta)$ are also rational. If $\varphi(n) \equiv 0 \pmod 4$ 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 $\varphi(n) \not\equiv 0 \pmod 4$ and $k(L) \neq 1$. Since $n \neq 1, 2, 4$, we have

$$n = r^a \quad \text{or} \quad n = 2r^a, \qquad r \text{ prime} \equiv 3 \pmod 4).$$

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

$$Q_n(\alpha, \beta) = Q_n^{(1)}(\alpha, \beta) Q_n^{(-1)}(\alpha, \beta); \tag{10}$$

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

By identity (3) the resultant R of polynomials $\psi_{\nu,\varkappa}(x)$, $\psi_{\nu,\varkappa}(-x)$ divides the discriminant of $Q_\nu(x^2)$ and therefore also the discriminant of $x^{2\nu} - 1$, which is $(2\nu)^{2\nu}$. There exist polynomials $\chi^{(1)}(x)$, $\chi^{(-1)}(x)$ such that

$$\chi^{(1)}(x)\psi_{\nu,\varkappa}(x) + \chi^{(-1)}(x)\psi_{\nu,\varkappa}(-x) = R$$

identically in x. The coefficients of $\chi^{(1)}$, $\chi^{(-1)}$ are expressible integrally in terms of the coefficients of $\psi_{\nu,\varkappa}(x)$ and therefore are algebraic integers. On making the above relation homogeneous in x, y and putting $x = A^{1/2}$, $y = B^{1/2}$, we deduce that any common prime factor of $\delta Q_n^{(1)}(\alpha, \beta)$ and $\delta Q_n^{(-1)}(\alpha, \beta)$ must divide $2\nu M$. By Lemma 1 and (10) each prime factor of $\delta Q_n^{(\varepsilon)}(\alpha, \beta)$ $(\varepsilon = \pm 1)$ is a primitive prime factor of P_n except possibly for $q(n)$, which then occurs to the first power only. Since no prime factor of $2\nu M$ can be a primitive prime factor of P_n, numbers $\delta Q_n^{(1)}(\alpha, \beta)$, $\delta Q_n^{(-1)}(\alpha, \beta)$ are 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*

$$\Pi = \prod_{\chi(r) = \mathrm{const} \neq 0} |x - \zeta_m^r| < \exp(2m^{1/2}\log^2 m).$$

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

[1] The idea of this proof is due to P. Erdös. An earlier proof of the writer led to a weaker estimation for Π.

Let the product Π be taken over r such that $\chi(r) = \zeta_e^{j_0}$. Order these integers r according to the magnitude of $\left\{\frac{r}{m} - \frac{1}{2\pi}\arg x\right\}$ so that

$$\left\{\frac{r_1}{m} - \frac{1}{2\pi}\arg x\right\} < \ldots < \left\{\frac{r_k}{m} - \frac{1}{2\pi}\arg x\right\} \qquad \left(k = \frac{\varphi(m)}{e}\right).$$

Denote by N_i and $N_{i,j}$ $(1 \leqslant i \leqslant k,\ 0 \leqslant j < e)$ the number of all non-negative integers $r < m$ such that $\left\{\frac{r}{m} - \frac{1}{2\pi}\arg x\right\} \leqslant \left\{\frac{r_i}{m} - \frac{1}{2\pi}\arg x\right\}$ and $\chi(r) = 0$ or $\chi(r) = \zeta_e^j$, respectively. We have

$$\left|(m - \varphi(m))\left\{\frac{r_i}{m} - \frac{1}{2\pi}\arg x\right\} - N_i\right| < 2^{\nu(m)} \leqslant m^{1/2} \tag{11}$$

$$\left|\sum_{j=0}^{e-1} N_{i,j} - m\left\{\frac{r_i}{m} - \frac{1}{2\pi}\arg x\right\} + N_i\right| < 1. \tag{12}$$

$(1 \leqslant i \leqslant k)$

On the other hand, from a well-known theorem of Schur [8] (for imprimitive characters see [3]), which we apply successively to characters $\chi(r), \chi^2(r), \ldots, \chi^{e-1}(r)$, we get

$$\left|\zeta_e^{-hj_0}\sum_{j=0}^{e-1} N_{i,j}\zeta_e^{hj}\right| < m^{1/2}\log m \qquad (1 \leqslant h < e,\ 1 \leqslant i \leqslant k). \tag{13}$$

Adding inequalities (11), (12), (13), we find

$$\left|eN_{i,j_0} - \varphi(m)\left\{\frac{r_i}{m} - \frac{1}{2\pi}\arg x\right\}\right| < em^{1/2}\log m \qquad (1 \leqslant i \leqslant k).$$

Since $N_{i,j_0} = i$, putting for brevity $\pi\left\{\frac{r_i}{m} - \frac{1}{2\pi}\arg x\right\} - \pi\frac{i}{k} = \varrho_i$ we get for each $i \leqslant k$

$$|\varrho_i| \leqslant \pi k^{-1} m^{1/2}\log m.$$

Now, if $\arg\zeta_k = 2\pi/k$, we find

$$\begin{aligned}
\prod_{i=1}^{k-1} |x - \zeta_m^{r_i}|\,|1 - \zeta_k^i|^{-1} &= \prod_{i=1}^{k-1}\left|\sin\left(\frac{1}{2}\arg x - \pi\frac{r_i}{m}\right)\right|\left|\sin\pi\frac{i}{k}\right|^{-1} \\
&= \prod_{i=1}^{k-1}\left|\sin\left(\pi\frac{i}{k} + \varrho_i\right)\right|\left|\sin\pi\frac{i}{k}\right|^{-1} = \prod_{i=1}^{k-1}\left(|\cos\varrho_i| + |\sin\varrho_i|\left|\cot\pi\frac{i}{k}\right|\right) \\
&\leqslant \prod_{i=1}^{[k/2]}\left(1 + (\pi k^{-1}m^{1/2}\log m)\frac{k}{\pi i}\right)^2 \leqslant \exp\left(2m^{1/2}\log m\sum_{i=1}^{[k/2]}\frac{1}{i}\right) \\
&\leqslant \exp\left(2m^{1/2}\log m\left(1 + \log\frac{k}{2}\right)\right).
\end{aligned}$$

Since, on the other hand, $\prod_{i=1}^{k-1}|1-\zeta_k^i| = k$ and $k = \varphi(m)/e < m/2$, we get

$$\Pi \leqslant 2\prod_{i=1}^{k-1}\left(|x-\zeta_m^{ri}||1-\zeta_k^i|^{-1}\right)\prod_{i=1}^{k-1}|1-\zeta_k^i|$$
$$\leqslant m\exp\left(2m^{1/2}\log m\left(1+\log\frac{m}{4}\right)\right) \leqslant \exp(2m^{1/2}\log^2 m)\,.$$

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

$$(14)\qquad |Q_n^{(\varepsilon)}(\alpha,\beta)| > \begin{cases} 1\,, & \text{if}\quad q(l)<q(n) \text{ and } n\neq 2r^\alpha,\ r \text{ as below}\,,\\ r^{1/2}\,, & \text{if}\quad n=2r^\alpha,\ r=k(L) \text{ prime} \equiv 3 \pmod 4\,,\\ q(l)\,, & \text{if}\quad q(l)=q(n) \text{ and } n\neq 2r^\alpha,\ r \text{ as above}\,.\end{cases}$$

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

1. $K>0$. If $n>\nu=\eta\varkappa l$, thus $n\geqslant 3\nu$, we apply (7) and find

$$|Q_n^{(\varepsilon)}(\alpha,\beta)| > (A^{1/2}-B^{1/2})^{\varphi(\nu)} \geqslant (\alpha^{3/2}-\beta^{3/2})^{\varphi(\nu)}$$
$$= \left(KL^{1/2}+M(L^{1/2}-2M^{1/2})\right)^{\frac12\varphi(\eta\varkappa)\varphi(l)} > (KL^{1/2})^{\frac12\varphi(\eta\varkappa)\varphi(l)}\,.$$

Now, as can easily be verified, $(KL^{1/2})^{\frac12\varphi(\eta\varkappa)}>2$ for all L, M, so that

$$|Q_n^{(\varepsilon)}(\alpha,\beta)| > 2^{\varphi(l)} \geqslant 2^{q(l)-1} \geqslant q(l)$$

and inequality (14) holds. Thus we can assume that $n=\nu$, $A=\alpha$, $B=\beta$. We shall consider successively $l=1$, $l=3$ and $l\geqslant 5$.

If $l=1$, we have to prove

$$(15)\qquad |Q_n^{(\varepsilon)}(\alpha,\beta)| > 1 \quad \text{if } n\neq 2r\,,\ r \text{ as below}\,,$$
$$|Q_n^{(\varepsilon)}(\alpha,\beta)| > r^{1/2} \quad \text{if } n=2r\,,\ r=k(L) \text{ prime} \equiv 3 \pmod 4\,.$$

Now, if $|Q_n^{(\varepsilon)}(\alpha,\beta)|\leqslant 1$, we have by inequality (7)

$$1 > \alpha^{1/2}-\beta^{1/2} = (L^{1/2}-2M^{1/2})^{1/2}\,,\qquad 1>\tfrac18\alpha+\tfrac18\beta = \tfrac18 L^{1/2}\,,$$

so that $L<4M+4M^{1/2}+1$, $L<64$. Since $4M<L$, we get $M\leqslant 15$ and $\langle L, M\rangle \in \mathfrak{M}$. It remains to consider the case $n=2r$, r prime $\equiv 3 \pmod 4$, $r\geqslant 7$ (since $n\neq 6$), $k(L)=r$, $k(M)=1$. By (7) we have

$$|Q_n^{(\varepsilon)}(\alpha,\beta)| > \left(\max(L^{1/2}-2M^{1/2},\ \tfrac18 L^{1/2})\right)^{\frac12\varphi(\nu)}\,.$$

Since $\varphi(\nu)=r-1$, it suffices to establish the inequality

$$(16)\qquad \max(L^{1/2}-2M^{1/2},\ \tfrac18 L^{1/2}) > r^{1/(r-1)}\,.$$

Since $r\geqslant 7$, $r^{1/(r-1)}\leqslant 7^{1/6}<2^{1/2}$, 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 $\langle L, M\rangle\in\mathfrak{M}$ or $\langle L, M\rangle = \langle 112, 25\rangle$.

Suppose now that $l=3$. If $q(n)>3$ it is again sufficient to prove (15). By (8) we have

$$|Q_n^{(\varepsilon)}(\alpha,\beta)| > 2^{-1/2}(\alpha-\beta) \geqslant 1$$

unless $1>2^{-1/2}(\alpha-\beta) = 2^{-1/2}K^{1/2}$, i.e. $K=1$. Since, as we already know, $|Q_n^{(\varepsilon)}(\alpha,\beta)|>1$ unless $\langle L, M\rangle\in\mathfrak{M}$, we find that, if $q(n)>3$, inequality (14) holds unless

$$\langle L, M\rangle \in \mathfrak{N}\,.$$

We have yet to consider the case $q(n)=l=3$, i.e. $n=12$, $k(LM)=2$. We find directly

$$Q_{12}^{(\varepsilon)}(\alpha,\beta) = L-\varepsilon 2^{1/2}L^{1/2}M^{1/2}-M$$

and since $M<\frac14 L$,

$$|Q_n^{(\varepsilon)}(\alpha,\beta)| > (\tfrac34-2^{-1/2})L\,.$$

Thus $|Q_n^{(\varepsilon)}(\alpha,\beta)|>3$ unless $L\leqslant 12(3-2^{3/2})^{-1}<75$. By an enumeration of cases we find that $|Q_n^{(\varepsilon)}(\alpha,\beta)|>3$ unless $\langle L, M\rangle\in\mathfrak{N}$ or $\langle L, M\rangle = \langle 8, 1\rangle$.

It remains to consider $l\geqslant 5$. Here we notice first that for all $\langle L, M\rangle$ in question

$$2^{-1/2}K^{1/2}\alpha\geqslant 5 \ \text{ or }\ \varkappa\geqslant 2 \ \text{ or }\ \langle L, M\rangle = \langle 9, 1\rangle\,,$$
$$2^{-1/2}K^{1/2}\alpha\geqslant 5^{1/2} \ \text{ or }\ \varkappa\geqslant 5 \ \text{ or }\ \langle L, M\rangle = \langle 9, 2\rangle\,,$$
$$2^{-1/2}K^{1/2}\alpha\geqslant 5^{1/4} \ \text{ or }\ \langle L, M\rangle = \langle 5, 1\rangle\,,\ \langle 9, 2\rangle\,.$$

It follows that, if $\langle L, M\rangle \neq \langle 5, 1\rangle, \langle 9, 1\rangle, \langle 9, 2\rangle$,

$$(2^{-1/2}K^{1/2}\alpha)^{\varphi(\eta\varkappa)} > 5;$$

hence also for all $l\geqslant 5$

$$(17)\qquad (2^{-1/2}K^{1/2}\alpha^{(q(l)-3)/2})^{\varphi(\eta\varkappa)} > q(l)\,,$$

and inequality (14) follows by (8).

If $\langle L, M\rangle = \langle 5, 1\rangle, \langle 9, 1\rangle, \langle 9, 2\rangle$, we find directly

$$(2^{-1/2}K^{1/2}\alpha^2)^{\varphi(\eta\varkappa)} > 7;$$

hence (17) holds if $q(l)\geqslant 7$. It remains to consider the cases $\langle L, M\rangle = \langle 5, 1\rangle, \langle 9, 1\rangle, \langle 9, 2\rangle$, $l=5$ or 15. Their direct examination leads to the exceptions stated in the theorem. The proof for $K>0$ is complete.

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

$$(18) \qquad |Q_n(\alpha, \beta)| > |\alpha|^{\varphi(n)-2^{\nu(n)}\log^3 n} \quad \text{for} \quad n > N(\alpha, \beta).$$

On the other hand, by (5) and (6), $Q_n^{(e)}(\alpha, \beta)$ can easily be represented as the products of $B^{\frac{1}{2}\varphi(\nu)}$ and 2 or 1 expressions of the form

$$\prod_{\chi(r)=\mathrm{const}\neq 0} |x-\zeta_m^r|, \quad \text{where} \quad x = -A^{1/2}B^{-1/2},\ \pm iA^{1/2}B^{-1/2},$$

and $\chi(r)$ is a real character $\bmod m = \varkappa$ or $4\varkappa$, respectively. Since $|A^{1/2}B^{-1/2}| = 1$, $m \leqslant 2n$, we get by Lemma 3

$$(19) \qquad |Q_n^{(e)}(\alpha, \beta)| < |\alpha|^{\frac{1}{2}\varphi(n)} \exp\left(4(2n)^{1/2}(\log 2n)^2\right).$$

It follows from (10), (18) and (19), that for $n > N(\alpha, \beta)$

$$|Q_n^{(e)}(\alpha, \beta)| > |\alpha|^{\frac{1}{2}\varphi(n)-2^{\nu(n)}\log^3 n} \exp\left(-4(2n)^{1/2}(\log 2n)^2\right).$$

Since, however, if $K < 0$, $|\alpha| \geqslant 2^{1/2}$ and for $n > 10^{40}$

$$\frac{\log 2}{2}\left(\tfrac{1}{2}\varphi(n) - 2^{\nu(n)}\log^3 n\right) - 4(2n)^{1/2}(\log 2n)^2 > \log n,$$

we find for $n > \max\left(N(\alpha, \beta), 10^{40}\right)$

$$|Q_n^{(e)}(\alpha, \beta)| > n,$$

which completes the proof.

Let us remark that Theorem 1 implies the following

COROLLARY. *If $k(LM) = 1$, $K > 0$, n is odd > 3, then P_n has at least two primitive prime factors, except for $n = 5$, $\langle L, M\rangle = \langle 9, 1\rangle$.*

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

THEOREM 2. *If $k\left(M\max(K, L)\right) = \pm 1, \pm 2$, then* $\varliminf_n \frac{q(P_n)}{n} \geqslant 2$.

The theorem follows at once from two lemmas.

LEMMA 4. *If P_n is an arbitrary Lehmer sequence and n runs through all numbers $\not\equiv 0 \pmod 4$, then*

$$\varliminf_n \frac{q(P_n)}{n} \geqslant 2.$$

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 $\equiv 0 \pmod{\varkappa}$, $\varkappa = k\left(M\max(K, L)\right)$, then*

$$\varliminf_n \frac{q(P_n)}{n} \geqslant 2.$$

Proof. By Lemma 4 we can suppose $n \equiv 0 \pmod 4$. If $\varkappa$ is odd, then P_n has at least one primitive prime factor q for n large enough, by the theorem quoted in the introduction. q is of the form $nk + (KL \mid q)$ and so $q \equiv (KL \mid q) \bmod 4\varkappa$. Hence $(LM \mid q) = 1$, which in view of the formula

$$(20) \qquad (\alpha/\beta)^{\frac{1}{2}q - \frac{1}{2}(KL\mid q)} \equiv (LM \mid q) \bmod q$$

implies that $P_{\frac{1}{2}q-\frac{1}{2}(KL\mid q)}$ is divisible by q. Since q is a primitive prime factor of P_n, we cannot have $q - (KL \mid q) = n$, whence $q \geqslant 2n-1$.

The same argument applies if $\varkappa$ is even and $n/2\varkappa$ is even. If the latter ratio is odd, then by Theorem 1 for n large enough P_n has at least two primitive prime factors. One at least of these is $\geqslant 2n-1$, which completes the proof.

References

[1] P. T. Bateman, *Note on the coefficients of the cyclotomic polynomial*, Bull. Amer. Math. Soc. 55 (1949), pp. 1180-1181.

[2] L. K. Durst, *Exceptional real Lehmer sequences*, Pacific J. Math. 9 (1959), pp. 437-441.

[3] E. Landau, *Abschätzungen von Charakter summen, Einheiten und Klassenzahlen*, Nachr. Gottingen (1918), pp. 79-97.

[4] D. H. Lehmer, *An extended theory of Lucas functions*. Ann. of Math. (2) 31 (1930), pp. 419-448.

[5] A. Rotkiewicz, *On Lucas numbers with two intrinsic divisors*, Bull. Acad. Polon. Sci. Sér. Math. Astr. Phys. 10 (1962), pp. 229-232.

[6] A. Schinzel, *On primitive prime factors of a^n-b^n*, Proc. Cambridge Philos. Soc. 58 (1962), pp. 555-562.

[7] — *The intrinsic divisors of Lehmer numbers in the case of negative discriminant*, Ark. Mat. 4 (1962), pp. 413-416.

[8] I. Schur, *Einige Bemerkungen zu der vorstehenden Arbeit des Herrn G. Polya: Ueber die Verteilung der quadratichen Reste und Nichtreste*, Nachr. Gottingen (1918), pp. 30-36.

[9] M. Ward, *The intrinsic divisors of Lehmer numbers*, Ann. of Math. (2) 62 (1955), pp. 230-236.

Reçu par la Rédaction le 30. 6. 1962