References

[1] C. Chevalley, *Class field theory*, Nagoya University (1953-1954), p. 38.

[2] H. Yokoi, *On the ring of integers in an algebraic number field as a representation module of Galois group*, Nagoya Math. J. 16 (1960), pp. 83-90.

DEPARTMENT OF MATHEMATICS
NAGOYA INSTITUTE OF TECHNOLOGY

Reçu par la Rédaction le 8. 7. 1962

ACTA ARITHMETICA
VIII (1963)

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,

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

where α and β are roots of the trinomial $z^2-L^{1/2}z+M$, and L and M are rational integers, $K=L-4M\neq 0$. Further, $\bar{z}$ denotes the complex conjugate of any given z and $k_e(n)$ denotes a positive integer n divided by the greatest eth power dividing it. The main result of the paper runs as follows.

Theorem. *Let $(L,M)=1$, $e=3$, 4 or 6. If $L^{1/2}$ is rational, $K^{1/2}$ is an irrational integer of the field $K(\zeta_e)$, K is divisible by the cube of the discriminant of this field, $\varkappa_e=k_e(M)$ is squarefree,*

$$\eta_e=\begin{cases}2 & \text{if } e=6,\ M\equiv 3 \pmod 4,\\ 1 & \text{otherwise},\end{cases}$$

and $n/\eta_e\varkappa_e$ is an integer relatively prime to e, then for $n>n_e(L,M)$, P_n has at least e primitive prime factors, and $n_e(L,M)$ can be effectively computed.

Lemma 1. *Let e,m,n be positive integers, $m|n$, and let χ be a character* $\bmod m$ *such that $\chi^{e+1}=\chi$ and that for all $i\not\equiv 0 \pmod e$ characters χ^i are primitive. Further, let*

$$\tau_i=\tau(\chi^i|\zeta_m)=\sum_{\substack{r=1\\(r,m)=1}}^{m}\chi^i(r)\zeta_m^r,$$

let χ_n be a character $\bmod n$ *induced by χ, and let $\chi(-1)^{1/e}$ be any fixed e-th root of $\chi(-1)$.*

Then, there exist polynomials $A_i(x, y)$ $(0 \leq i < e)$ with coefficients from the field $K(\zeta_e)$ such that

$$\psi(\chi_n;\, x, y) = \prod_{\substack{r=1 \\ (r,n)=1}}^{n} \big(x - \chi(-1)^{1/e}\chi(r)\zeta_n^r y\big)$$

$$= A_0(x^e, y^e) + \sum_{i=1}^{e-1} \chi(-1)^{i/e}\tau_i x^{e-i} y^i A_i(x^e, y^e)\,,$$

(1) $$\bar{A}_0(x, y) = A_0(y, x)\,,$$

(2) $$\bar{A}_i(x, y) = A_{e-i}(y, x)\chi^{i-1}(-1) \qquad (0 < i < e)\,.$$

Proof. In the course of this proof we shall denote by $a_1, a_2, \ldots$ $\ldots, b_1, b_2, \ldots, c_1, c_2, \ldots$ the numbers of the field $K(\zeta_e)$, by $p_i(\xi, \eta, \ldots)$ and $s_i(\xi, \eta, \ldots)$ the ith fundamental symmetric function and the sum of the ith powers of the indeterminates $\xi, \eta, \ldots$, respectively. We have

(3) $$\psi(\chi_n;\, x, y) = \sum_{j=0}^{\varphi(n)} (-1)^j x^{\varphi(n)-j} y^j p_j\big(\chi_n(1)\zeta_n, \ldots, \chi_n(-1)\zeta_n^{-1}\big)$$

and by the Newton formulae

$$p_j = \sum_{a_1+2a_2+\ldots+ka_k=j} a_{a_1,a_2,\ldots,a_k} s_1^{a_1} s_2^{a_2} \ldots s_k^{a_k}\,.$$

On the other hand,

$$s_i\big(\chi_n(1)\zeta_n, \ldots, \chi_n(-1)\zeta_n^{-1}\big) = \sum_{\substack{r=1 \\ (r,n)=1}}^{n} \chi_n^i(r)\zeta_n^{ri} = \tau(\chi_n^i|\zeta_n^i)\,.$$

Now, it follows from well-known results ([1], § 20, theorem IV) that under the conditions assumed with regard to character χ, $\tau(\chi_n^i|\zeta_n^i)$ can be different from zero only if

$$i \equiv 0 \ (\mathrm{mod}\, e) \quad \text{ or } \quad m \,\Big|\, \frac{n}{(n, i)}$$

and in the latter case

$$\tau(\chi_n^i|\zeta_n^i) = \tau(\chi^i|\zeta_m^i) \times \begin{cases} \pm\mu\left(\dfrac{n}{(n, i)}\right)\cdot\dfrac{\varphi(n)\varphi\big(m/(m, i)\big)}{\varphi(m)\varphi\big(n/(n, i)\big)}\,, & \text{if} \quad i \equiv 0 \ (\mathrm{mod}\, e)\,, \\ \mu\left(\dfrac{n}{(n, i)m}\right)\chi^i\left(\dfrac{n}{(n, i)m}\right)\chi^{-i}\left(\dfrac{ia}{(n, i)}\right)\dfrac{\varphi(n)}{\varphi\big(n/(n, i)\big)}\,, & \\ & \text{if} \quad m \,\Big|\, \dfrac{n}{(n, i)}\,, \end{cases}$$

where $\zeta_m^a = \zeta_n^{n/m}$.

This implies that

(4) $$p_j\big(\chi_n(1)\zeta_n, \ldots, \chi_n(-1)\zeta_n^{-1}\big) = \sum_{a_1+2a_2+\ldots+ka_k=j} b_{a_1,a_2,\ldots,a_k}\tau_1^{a_1}\tau_2^{a_2}\ldots\tau_k^{a_k}\,.$$

Now, it follows from other well-known results ([1], § 20, theorem VIII) that for suitable c_j, $\tau_j = c_j\tau_1^j$; thus if

$$a_1 + 2a_2 + \ldots + ka_k = j \equiv i \ (\mathrm{mod}\, e)\,,$$

we have

(5) $$\tau_1^{a_1}\tau_2^{a_2}\ldots\tau_k^{a_k} = c_{a_1,a_2,\ldots,a_k}\tau_i\,.$$

Formulae (3), (4), (5) give

(6) $$\psi(\chi_n;\, x, y) = A_0(x^e, y^e) + \sum_{i=1}^{e-1} \chi(-1)^{i/e}\tau_i x^{e-i} y^i A_i(x^e, y^e)\,,$$

where

$$A_0(x, y) = \sum_{\substack{0 \leq j \leq \varphi(n) \\ a_1+2a_2+\ldots+ka_k=j\equiv 0 \ (\mathrm{mod}\, e)}} (-1)^j\chi(-1)^{j/e} b_{a_1,\ldots,a_k} c_{a_1,\ldots,a_k}\tau_0 x^{(\varphi(n)-j)/e} y^{j/e}\,,$$

$$A_i(x, y) =$$

$$\sum_{\substack{0 < j \leq \varphi(m) \\ a_1+2a_2+\ldots+ka_k=j\equiv i \ (\mathrm{mod}\, e)}} (-1)^j\chi(-1)^{(j-i)/e} b_{a_1,\ldots,a_k} c_{a_1,\ldots,a_k} x^{(\varphi(n)-e+i-j)/e} y^{(j-i)/e}$$

$$(0 < i < e)$$

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

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

$$\prod_{\substack{r=1 \\ (r,n)=1}}^{n} \bar{\chi}(r) = \bar{\chi}\Big(\prod_{\substack{r=1 \\ (r,n)=1}}^{n} r\Big) = \chi(-1)^{\varphi(n)/e}\,.$$

It follows that

$$\bar{\psi}(\chi_n;\, x, y) = \prod_{\substack{r=1 \\ (r,n)=1}}^{n} \big(x - \chi(-1)^{-1/e}\bar{\chi}(r)\bar{\zeta}_n^r y\big)$$

$$= \prod_{\substack{r=1 \\ (r,n)=1}}^{n} \big(-\chi(-1)^{-1/e}\bar{\chi}(r)\bar{\zeta}_n^r\big) \prod_{\substack{r=1 \\ (r,n)=1}}^{n} \big(y - \chi(-1)^{1/e}\chi(r)\zeta_n^r x\big)$$

$$= \chi(-1)^{-\varphi(n)/e} \prod_{\substack{r=1 \\ (r,n)=1}}^{n} \bar{\chi}(r)\psi(\chi_n;\, y, x) = \psi(\chi_n;\, y, x)\,.$$

Applying formula (6) successively to $\psi(\chi_n; x, y)$ and $\psi(\chi_n; y, x)$ and taking into account the well-known equality

$$\bar{\tau}_i = \chi(-1)^i \tau_{e-i} \tag{7}$$

we find (1) and (2).

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

$$\tau(\chi^i|\zeta_m) = \zeta_e^{\delta_i}\chi(-1)^{ie/(4,e^2)}\bar{\omega}^{(e-i)/e}\omega^{i/e} \qquad (0 < i < e).$$

Here $\arg\omega^{1/e} = \dfrac{1}{e}\arg\omega$, $\arg\bar{\omega}^{1/e} = \dfrac{1}{e}\arg\bar{\omega} + \dfrac{e-1}{e}2\pi$, $\chi(-1)^{1/(4,e^2)}$ *is any fixed $(4, e^2)$-th root of $\chi(-1)$ and*

$$\bar{\zeta}_e^{\delta_i} = \zeta_e^{\delta_{e-i}}\chi(-1)^{\frac{1}{(4,e^2)}[e^2+i(4,e^2)]}. \tag{8}$$

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

$$\tau(\chi_j|\zeta_{p_j})^e = \chi_j(-1)^{e^2/(4,e^2)}\bar{\pi}_j^{e-1}\pi_j, \tag{9}$$

whence by (7)

$$\tau(\chi_j^{e-1}|\zeta_{p_j})^e = \chi_j(-1)^{e^2/(4,e^2)}\bar{\pi}_j\pi_j^{e-1}. \tag{10}$$

Further, it follows from the connection between $\tau(\chi_j|\zeta_{p_j})$ and $\tau(\chi_j^i|\zeta_{p_j})$ (cf. [1], § 20, theorem IX) that

$$\tau(\chi_j^2|\zeta_{p_j})^e = \bar{\pi}_j^{e-2}\pi_j^2, \tag{11}$$

$$\tau(\chi_j^{e-2}|\zeta_{p_j})^e = \bar{\pi}_j^2\pi_j^{e-2}. \tag{12}$$

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

$$\tau(\chi_j^3|\zeta_{p_j})^6 = \chi_j(-1)\bar{\pi}_j^3\pi_j^3. \tag{13}$$

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

$$\tau(\chi_j^i|\zeta_{p_j})^e = \chi(-1)^{ie^2/(4,e^2)}\bar{\pi}_j^{e-i}\pi_j^i \qquad (e = 3, 4, \text{ or } 6). \tag{14}$$

(¹) An irrational prime π of the field $K(\zeta_e)$ is normalized if $\pi = A + B\zeta_3$, $A \equiv -1 \pmod 3$, $B \equiv 0 \pmod 3$ for $e = 3$ or 6, and $\omega = A + B\zeta_4$, $A \equiv B + 1 \pmod 4$, $B \equiv 0 \pmod 2$ for $e = 4$.

Put

$$\zeta_m = \prod_{j=1}^{k}\zeta_{p_j}, \qquad \chi = \prod_{j=1}^{k}\chi_j.$$

It follows from the properties of characters χ_j that χ^i are primitive characters $\bmod m$ for all $i \not\equiv 0 \pmod e$. Besides, we find from (14) and a well-known theorem ([1], § 20, theorem VI) that

$$\tau(\chi^i|\zeta_m)^e = \chi(-1)^{ie^2/(4,e^2)}\bar{\omega}^{e-i}\omega^i.$$

It follows hence that

$$\tau(\chi^i|\zeta_m) = \zeta_e^{\delta_i}\chi(-1)^{ie/(4,e^2)}\bar{\omega}^{(e-i)/e}\omega^{i/e},$$

and by (7)

$$\bar{\zeta}_e^{\delta_i} = \chi(-1)^{\frac{1}{(4,e^2)}[e^2+i(4,e^2)]}\zeta^{\delta_{e-i}},$$

which completes the proof.

Proof of the theorem. Since $k_e(\alpha\bar{\alpha}) = \varkappa_e$, there exist two integers α_1 and ω of the field $K(\zeta_e)$ such that $\alpha = \alpha_1^e\omega$ and $\omega\bar{\omega} = \varkappa_e$.

On the other hand, by the assumption about K we have

$$K \equiv 0 \pmod{27} \quad (e = 3 \text{ or } 6), \qquad K \equiv 0 \pmod{64} \quad (e = 4).$$

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

$$(M, e) = (\alpha\bar{\alpha}, e) = 1$$

and *a fortiori* $(\varkappa_e, e) = 1$, $(\alpha_1, e) = 1$.

It follows from the latter equality that $\operatorname{Im}\alpha_1^e \equiv 0 \bmod (1-\zeta_e^2)^2$. Since also $\operatorname{Im}\alpha \equiv 0 \bmod (1-\zeta_e^2)^2$, we get $\operatorname{Im}\omega \equiv 0 \bmod (1-\zeta_e^2)^2$. Since $\omega\bar{\omega}$ is squarefree, ω is not divisible by any rational prime and thus ω or $-\omega$ is a product of normalized irrational primes. But $P_n(-\alpha_1^e\omega, -\bar{\alpha}_1^e\bar{\omega}) = \pm P_n(\alpha, \beta)$, therefore we can assume that ω itself has the said property. Applying Lemma 2 to ω we find a character χ satisfying the conditions of Lemma 1 and such that formulae (1), (2) hold. Let χ_{n/η_e} be the induced character $\bmod n/\eta_e$ (by the assumption $\varkappa_e | n/\eta_e$), and let $\chi(-1)^{1/e}$ be any fixed eth root of $\chi(-1)$.

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

$$Q_n^{(i)}(\alpha, \beta) = \psi(\chi_{n/\eta_e}; \alpha^{1/e}, \beta^{1/e}),$$

where

$$\alpha^{1/e} = \alpha_1\omega^{1/e}, \qquad \beta^{1/e} = \overline{\alpha^{1/e}}.$$

Since $\beta = \overline{\alpha}$, we find from Lemma 1 and Lemma 2

$$(15)\qquad Q_n^{(i)}(\alpha, \beta) = A_0(\alpha, \overline{\alpha}) + \sum_{i=1}^{e-1} \zeta_e^{\delta_i} \chi(-1)^{\frac{i}{e}} \chi(-1)^{i\frac{e}{(4,e^2)}} \overline{\omega}^{\frac{e-i}{e}} \omega^{\frac{i}{e}} (\alpha_1^e \omega)^{\frac{e-i}{e}} (\overline{\alpha}_1^e \overline{\omega})^{\frac{i}{e}} A_i(\alpha, \overline{\alpha})$$

$$= A_0(\alpha, \overline{\alpha}) + \tfrac{1}{2}\omega\overline{\omega} \sum_{i=1}^{e-1} \Big(\zeta_e^{\delta_i} \chi(-1)^{\frac{i}{e}} \chi(-1)^{i\frac{e}{(4,e^2)}} \alpha_1^{e-i} \overline{\alpha}_1^{i} A_i(\alpha, \overline{\alpha}) + $$

$$+ \zeta_e^{\delta_{e-i}} \chi(-1)^{\frac{e-i}{e}} \chi(-1)^{(e-i)\frac{e}{(4,e^2)}} \alpha_1^{i} \overline{\alpha}_1^{e-i} A_{e-i}(\alpha, \overline{\alpha})\Big) .$$

Now, by formula (1)

$$\overline{A_0(\alpha, \overline{\alpha})} = \overline{A}_0(\overline{\alpha}, \alpha) = A_0(\alpha, \overline{\alpha}) ,$$

and by formulae (2) and (8)

$$\overline{\zeta_e^{\delta_i} \chi(-1)^{\frac{i}{e}} \chi(-1)^{i\frac{e}{(4,e^2)}} \alpha_1^{e-i} \overline{\alpha}_1^{i} A_i(\alpha, \overline{\alpha})}$$

$$= \zeta_e^{\delta_{e-i}} \chi(-1)^{\frac{e^2+i(4,e^2)}{(4,e^2)}} \chi(-1)^{-\frac{i}{e}} \chi(-1)^{-i\frac{e}{(4,e^2)}} \overline{\alpha}_1^{e-i} \alpha_1^{i} \overline{A}_i(\overline{\alpha}, \alpha)$$

$$= \zeta_e^{\delta_{e-i}} \chi(-1)^{\frac{e-i}{e}} \chi(-1)^{(e-i)\frac{e}{(4,e^2)}} \alpha_1^{i} \overline{\alpha}_1^{e-i} A_{e-i}(\alpha, \overline{\alpha})$$

so that all the terms of sum (15) are real. Therefore, the numbers $Q_n^{(i)}(\alpha, \beta)$ are real. On the other hand, they are of course algebraic integers and by (15) they belong to the field $K\big(\zeta_e, \chi(-1)^{1/e}\big)$. Thus, if $\chi(-1) = 1$, they must be rational integers. If $\chi(-1) = -1$, $e = 4$ or 6 and $(m-1)/e$ is odd. Since $M \equiv m \pmod{2e}$, $(M-1)/e$ must be odd. This gives, for $e = 4$, $M \equiv 5 \pmod 8$, which is incompatible with the condition that $L^{1/2}$ is rational, $K \equiv 0 \pmod{64}$. Thus $e = 6$, and we conclude that in this case numbers $Q_n^{(i)}(\alpha, \beta)$ are real integers of the field $K(\zeta_{12})$. Taking the relative conjugates of the numbers $Q_n^{(i)}(\alpha, \beta)$ with respect to the field $K(\zeta_4)$, we find as in the case of complex conjugates, that they are equal. This proves that $Q_n^{(i)}(\alpha, \beta)$ $(0 \leqslant i < e)$ are rational integers in every case.

On the other hand, since $(n/\eta_e, e) = 1$, we have

$$(16)\qquad \prod_{i=0}^{e-1} \psi(\chi_{n/\eta_e}^{i}; x, y) = \prod_{\substack{r=1\\ (r, n/\eta_e)=1}}^{n/\eta_e} \big(x^e - \chi(-1)\zeta_{n/\eta_e}^{re} y^e\big) = Q_{n/\eta_e}\big(x^e, \chi(-1)y^e\big) .$$

It follows from the definition of η_e that $\eta_e = 1$ unless $\chi(-1) = -1$, and in this case $\eta_e = 2$. Therefore, we get from formula (16)

$$(17)\qquad \prod_{i=0}^{e-1} Q_n^{(i)}(\alpha, \beta) = Q_{n/\eta_e}\big(\alpha, \chi(-1)\beta\big) = Q_n(\alpha, \beta) .$$

Further, it follows from (16) as in the analogous situation in [3], that the common prime factors of any two numbers $Q_n^{(i)}, Q_n^{(j)}$ $(0 \leqslant i < j < e)$ must divide the discriminant of $x^{en} - 1$, equal to en^{en}. However, by Lemma 1 of [3], no prime factor of en can divide $Q_n(\alpha, \beta)$ with an exponent > 1. Thus the numbers $Q_n^{(i)}(\alpha, \beta)$ $(0 \leqslant i < e)$ are relatively prime in pairs, and in order to prove the theorem it suffices, again by Lemma 1 of [3], to establish the inequality

$$(18)\qquad |Q_n^{(i)}(\alpha, \beta)| > n \qquad (0 \leqslant i < e) .$$

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

$$(19)\qquad \log |Q_n^{(i)}(\alpha, \beta)| < \frac{\varphi(n)}{e} \log|\alpha| + 2en^{1/2}\log^2 n .$$

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

$$(20)\qquad \log|Q_n(\alpha, \beta)| > \big(\varphi(n) - 2^{\nu(n)}\log^3 n\big)\log|\alpha| .$$

It follows from (17), (19) and (20) that for $n > N(\alpha, \beta)$

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

Since $|\alpha| \geqslant 2^{1/2}$ and for $n > 10^{60}$

$$\left(\frac{\varphi(n)}{e} - 2^{\nu(n)}\log^3 n\right)\frac{\log 2}{2} - 2e(e-1)n^{1/2}\log^2 n > \log n \qquad (e \leqslant 6)$$

inequality (18) certainly holds for

$$n > \max\big(10^{60}, N(\alpha, \beta)\big)$$

and the theorem is proved.

References

[1] H. Hasse, *Vorlesungen über Zahlentheorie*, Berlin 1950.

[2] A. Schinzel, *The intrinsic divisors of Lehmer numbers in the case of negative discriminant*, Ark. Math. 4 (1962), pp. 413-416.

[3] — *On primitive prime factors of Lehmer numbers I*, Acta Arith. this volume, pp. 213-223.

Reçu par la Rédaction le 20. 7. 1962