ACTA ARITHMETICA
XV (1968)

On primitive prime factors of Lehmer numbers III

by

A. Schinzel (Warszawa)

§ 1. The main aim of this paper is to complete the results of [5], [7] and [8] concerning Lehmer numbers with a negative discriminant. About the case of a positive discriminant I have nothing new to say except that J. Brillhart and J. L. Selfridge have found explicitly the sets $\mathfrak{M}_0$ and $\mathfrak{N}_0$ occurring in Theorem 1 of [7]. The notation of [7] is retained. In particular $\zeta_n = e^{2\pi i/n}$,

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

where α and β are roots of the trinomial $z^2 - L^{1/2}z + M$ and L and M are rational integers. $k_e(n)$ is the eth powers-free kernel of n, n^* is the product of all distinct prime factors of n, $\bar{z}$ is the complex conjugate of z. We assume

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

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

set

$$A = \max\{12, \log M \min\{k(-K), k(L)\}\}, \quad B = \max\{12, \log M\}$$

and prove

Theorem 1. *If* $n > 3\cdot 10^{14} A^3$ *then* $P_n(\alpha,\beta)$ *has at least one primitive prime factor.*

Theorem 2. *For* L, M *satisfying* (1), (2) *set*

$$\eta = \begin{cases} 1 & \text{if} \quad k(LM) \equiv 1 \bmod 4, \\ 2 & \text{if} \quad k(LM) \equiv 2 \text{ or } 3 \bmod 4, \end{cases}$$

$$\eta_1 = \begin{cases} 1 & \text{if} \quad k(KM) \equiv 1 \bmod 4, \\ 2 & \text{if} \quad k(KM) \equiv 2 \text{ or } 3 \bmod 4; \end{cases}$$

$$\eta_2 = \begin{cases} 1 & \text{if} \quad k(KL) \equiv 1 \bmod 4, \\ 4 & \text{if} \quad k(KL) \equiv 2 \text{ or } 3 \bmod 4. \end{cases}$$

If $n>3\cdot 10^{14}A^3$ *and* $n\equiv \eta k(LM)\bmod 2\eta k(LM)$ *or* $n\equiv \eta_1 k(KM)\bmod 2\times$ $\times\eta_1 k(KM)$ *or* $n\equiv 0\bmod \eta_2 k(KL)$, *then* $P_n(\alpha,\beta)$ *has two primitive prime factors; if all three congruences hold then* $P_n(\alpha,\beta)$ *has four primitive prime factors.*

THEOREM 3. *Let* $e=3, 4$ *or* 6 *and* ζ_e *belong to the field* $\mathscr{K}(\sqrt{KL})$. *Set*

$$\eta_3=\begin{cases}1 & \text{if} \quad KL\equiv 0\bmod 27,\\ 3 & \text{if} \quad KL\not\equiv 0\bmod 27;\end{cases} \qquad \eta_4=\begin{cases}1 & \text{if} \quad K\equiv 0\bmod 8,\\ 2 & \text{if} \quad L\equiv 0\bmod 8,\\ 4 & \text{if} \quad KL\not\equiv 0\bmod 8;\end{cases}$$

$$\eta_6=\begin{cases}1 & \text{if} \quad K\equiv 0\bmod 27,\ M\equiv 1\bmod 4 \text{ or } L\equiv 0\bmod 27,\ M\equiv 3\bmod 4,\\ 2 & \text{if} \quad K\equiv 0\bmod 27,\ M\equiv 3\bmod 4 \text{ or } L\equiv 0\bmod 27,\ M\equiv 1\bmod 4,\\ 3 & \text{if} \quad K\equiv 6\bmod 9,\ M\equiv 1\bmod 4 \text{ or } L\equiv 3\bmod 9,\ M\equiv 3\bmod 4,\\ 6 & \text{if} \quad K\equiv 6\bmod 9,\ M\equiv 3\bmod 4 \text{ or } L\equiv 3\bmod 9,\ M\equiv 1\bmod 4.\end{cases}$$

If $n/\eta_e k_e(M)^*$ *is an integer relatively prime to* e,

$$n>3\cdot 10^{14}\eta_e B^3 \quad \text{and} \quad n\frac{(2n,8)}{(n^3,8)}>3\cdot 10^{14}\eta_3 B^3 \quad \text{for} \quad e=3,\ L\equiv 0\bmod 3,$$

then $P_n(\alpha,\beta)$ *has* $e+(e,2)\left[\frac{\eta_e+1}{4}\right]$ *primitive prime factors.*

Proofs of these theorems given in §§ 2, 3, 4 respectively require some facts already established in [6], [7], [8] and also an improved version of Lemma 1 of [8] stated below as Lemma 3. An application to the estimation of the greatest prime factor of a linear recurrence of the second order is given in § 5. The result obtained completes Theorem 8 of [9]. Unfortunately, the proof of a related result of [7] concerning the greatest prime factor of certain special Lehmer numbers contains a gap, which I am unable to fill in (see Corrigenda at the end of the paper).

§ 2. LEMMA 1. *For* $n\neq 1, 2, 3, 4, 6$ *primitive prime factors of* $P_n(\alpha,\beta)$ *coincide with prime factors of* $Q_n(\alpha,\beta)/(n^*, Q_n(\alpha,\beta))$ *and are of the form* $nt\pm 1$.

Proof. This follows from Theorems 3.2, 3.3 and 3.4 of [2].

LEMMA 2. *For* $n>3\cdot 10^{14}A^3$, (1) *and* (2) *imply the inequality*

$$|Q_n(\alpha,\beta)|>n|\alpha|^{\frac{11}{13}\varphi(n)}. \tag{3}$$

Proof. We have

$$|Q_n(\alpha,\beta)|=|\alpha|^{\varphi(n)}\prod_{d\mid n}\left|\left(\frac{\beta}{\alpha}\right)^d-1\right|^{\mu(n/d)}. \tag{4}$$

In order to estimate $|(\beta/\alpha)^d-1|$ we apply Theorem 2 of [9]. We set there

$$\langle\alpha',\alpha''\rangle = \begin{cases}\langle\frac{1}{2}\sqrt{Lk(K)}+\frac{1}{2}\sqrt{Kk(K)},\ \frac{1}{2}\sqrt{Lk(K)}-\frac{1}{2}\sqrt{Kk(K)}\rangle & \text{if} \quad k(-K)\leqslant k(L),\\ \langle\frac{1}{2}\sqrt{Lk(L)}+\frac{1}{2}\sqrt{Kk(L)},\ \frac{1}{2}\sqrt{Lk(L)}-\frac{1}{2}\sqrt{Kk(L)}\rangle & \text{if} \quad k(-K)>k(L);\end{cases}$$

$$\beta'=\beta''=1,$$

$\alpha', \alpha'', \beta', \beta''$ are integers of the field $\mathscr{K}(\sqrt{KL})$, and we obtain

$$\log 2\geqslant \log\left|\left(\frac{\beta}{\alpha}\right)^d-1\right|\geqslant -2^5\cdot 10^5 a_1^3(\log n+2)^2, \tag{5}$$

where

$$a_1=\max\{\pi, \log\{|eD|^{1/4}, |\alpha'\beta'|, |\alpha'\beta''|, |\alpha''\beta'|, |\alpha''\beta''|\}\}$$
$$=\max\left\{\pi, \tfrac{1}{2}\log\max\left\{|eD|^{1/2}, M\min\{k(-K), k(L)\}\right\}\right\}$$

and D is the discriminant of the field $\mathscr{K}(\sqrt{KL})$. Clearly

$$|D|\leqslant 4k(-K)k(L)$$

and an easy computation shows that

$$\tfrac{1}{4}\log 4ek(-K)k(L)\leqslant \max\left\{\pi, \tfrac{1}{2}\log M\min\{k(-K), k(L)\}\right\},$$

thus

$$a_1=\max\left\{\pi, \tfrac{1}{2}\log M\min\{k(-K), k(L)\}\right\}.$$

Since by (1) $\log|\alpha|=\frac{1}{2}\log M$ we get from (4) and (5)

$$\log|Q_n(\alpha,\beta)|-\log n|\alpha|^{\frac{11}{13}\varphi(n)}$$
$$\geqslant \tfrac{2}{13}\varphi(n)\log|\alpha|-3{,}2\cdot 10^6\cdot 2^{\nu(n)-1}a_1^3(\log n+2)^2-2^{\nu(n)-1}\log 2-\log n$$
$$\geqslant \tfrac{1}{13}\varphi(n)\log M-3{,}3\cdot 10^6\cdot 2^{\nu(n)-1}a_1^3(\log n+2)^2.$$

For $n>3\cdot 10^{14}A^3>5\cdot 10^{17}$ we have in virtue of Theorem 15 of [4]

$$\varphi(n)>\frac{n}{e^\gamma\log\log n+5/2\log\log n}>\frac{n}{e^\gamma\log\log n+0{,}675}. \tag{6}$$

On the other hand, for every n

$$2^{\nu(n)}<39\sqrt[6]{n}$$

(this can be proved elementarily). The functions

$$f_r(n)=\frac{n^{r/6}}{(e^\gamma\log\log n+0{,}675)(\log n+2)^2} \qquad (r=1 \text{ or } 5)$$

are increasing for $n>e^{13}$.

If $a_1 = \pi$ we find

$$\frac{\frac{1}{13}\varphi(n)\log M}{2^{\nu(n)-1}a_1^3(\log n+2)^2} > \frac{\log 2}{254\pi^3}f_5(n) \geqslant \frac{\log 2}{254\pi^3}f_5(5\cdot 10^{17}) > 10^{6,56} > 3{,}3\cdot 10^6.$$

If $a_1 = \frac{1}{2}\log M \min\{k(-K), k(L)\} \geqslant \pi$ we find $n > 24\cdot 10^{14}a_1^3$,

$$\log M \geqslant \frac{2\pi-\log 2}{4\pi}\log M \min\{-K, L\} \geqslant \frac{2\pi-\log 2}{2\pi}a_1,$$

hence

$$\begin{aligned}\frac{\frac{1}{13}\varphi(n)\log M}{2^{\nu(n)-1}a_1^3(\log n+2)^2} &> \frac{2\pi-\log 2}{507\pi a_1^2}f_5(n) \geqslant \frac{2\pi-\log 2}{507\pi a_1^2}f_5(24\cdot 10^{14}a_1^3)\\ &= \frac{2\pi-\log 2}{507\pi}(24\cdot 10^{14})^{2/3}f_1(24\cdot 10^{14}a_1)\\ &\geqslant \frac{2\pi-\log 2}{507\pi}(24\cdot 10^{14})^{2/3}f_1(24\cdot 10^{14}\pi^3) > 10^{6,53} > 3{,}3\cdot 10^6.\end{aligned}$$

This completes the proof.

Proof of Theorem 1 follows at once from Lemmata 1 and 2.

§ 3. LEMMA 3. *Let e, n be positive integers, $n > 2$, $(e, 2n) = 1$ or 2. Let χ be a character* mod $n(e, n)$ *of order e with the conductor f, where* $\left(\frac{n(e,n)}{f}, e\right) = 1$. *Set*

$$\psi_n(\chi; x, y) = \prod_{\substack{r=1\\(r,n)=1}}^{n}(x-\chi(r)\zeta_{n(e,n)}^r y).$$

Then

$$Q_n(x^e, y^e) = \prod_{\varepsilon^e=1}\psi_n(\chi; x, \varepsilon y), \tag{7}$$

$$\bar{\psi}_n(\chi; x, y) = \chi(-1)^{\varphi(n)/e}\psi_n(\chi; y, x), \tag{8}$$

$$\psi_n(\chi; x, y) = R_0(x^e, y^e) + \sum_{i=1}^{e-1}\tau(\chi^i)x^{e-i}y^i R_i(x^e, y^e), \tag{9}$$

where R_i are polynomials over $\mathscr{K}(\zeta_e)$ and $\tau(\chi^i)$ are normalized primitive Gaussian sums belonging to characters χ^i.

Proof. Formula (7) follows at once, since

$$\prod_{\varepsilon^e=1}\psi_n(\chi; x, \varepsilon y) = \prod_{\substack{r=1\\(r,n)=1}}^{n}\prod_{\varepsilon^e=1}(x-\chi(r)\zeta_{n(e,n)}^r\varepsilon y) = \prod_{\substack{r=1\\(r,n)=1}}^{n}(x^e-\zeta_{n(e,n)}^{re}y^e).$$

To prove formula (8) we notice that

$$\chi = \chi_{(e^3,n^2)}\chi_{n/(e^2,n)}, \tag{10}$$

where $\chi_{(e^3,n^2)}$ and $\chi_{n/(e^2,n)}$ are characters mod (e^3, n^2) and mod $n/(e^2, n)$, respectively, the former primitive;

$$\prod_{\substack{r=1\\(r,n)=1}}^{n} r \equiv \begin{cases} 3 \bmod 8 & \text{if } n = 4,\ e = 2,\\ 1 \bmod (e^3, n^2) & \text{otherwise;}\end{cases}$$

$$\prod_{\substack{r=1\\(r,n)=1}}^{n} r \equiv \begin{cases} -1 \bmod n & \text{if } n \text{ has a primitive root,}\\ 1 & \text{otherwise.}\end{cases}$$

Besides

$$\prod_{\substack{r=1\\(r,n)=1}}^{n}\zeta_{n(e,n)}^{-r} = (-1)^{\varphi(n)/(e,n)};$$

$$\frac{\varphi(n)}{e} \equiv \begin{cases} 1 \bmod 2 & \text{if } n = 4,\ e = 2,\\ \frac{p-1}{e} \bmod 2 & \text{if } n = p^\mu,\ p \text{ odd},\\ \frac{p-1}{2} \bmod 2 & \text{if } n = 2p^\mu,\ p \text{ odd},\ e \text{ even},\\ 0 \bmod 2 & \text{otherwise.}\end{cases}$$

It follows hence

$$\prod_{\substack{r=1\\(r,n)=1}}^{n}\bar{\chi}(r)\zeta_{n(e,n)}^{-r} = \begin{cases} -\chi(3) = \chi(-1)^{\frac{\varphi(n)}{e}} & \text{if } n = 4,\ e = 2,\\ \chi(-1) = (-1)^{\frac{p-1}{e}} = (-1)^{\left(\frac{p-1}{e}\right)^2} = \chi(-1)^{\frac{\varphi(n)}{e}} & \text{if } n = p^\mu,\ p \text{ odd},\\ \chi_{n/2}(-1)(-1)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}} = 1 = \chi(-1)^{\frac{\varphi(n)}{e}} & \\ \qquad\qquad \text{if } n = 2p^\mu,\ p \text{ odd},\ e \text{ even},\\ \chi(-1) = 1 = \chi(-1)^{\frac{\varphi(n)}{e}} & \text{if } n = 2p^\mu,\ p, e \text{ odd},\\ \chi(1) = 1 = \chi(-1)^{\frac{\varphi(n)}{e}} & \text{otherwise}\end{cases}$$

and we get

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

In the proof of (9) we shall denote by $a_1, a_2, \ldots, b_1, b_2, \ldots, c_1, c_2, \ldots$ numbers of the field $\mathscr{K}(\zeta_e)$, by $p_i(\xi, \eta, \ldots)$ and $s_i(\xi, \eta, \ldots)$ the ith fundamental symmetric function and the sum of ith powers of the indeterminates $\xi, \eta, \ldots$, respectively. We have

$$\psi_n(\chi; x, y) = \sum_{j=0}^{\varphi(n)} (-1)^j x^{\varphi(n)-j} y^j p_j\left(\chi(1)\zeta_{n(e,n)}, \ldots, \chi(-1)\zeta_{n(e,n)}^{-1}\right) \tag{11}$$

and by Newton's formulae

$$p_j = \sum_{a_1+2a_2+\ldots+ka_k=j} a_{a_1 a_2 \ldots a_k} s_1^{a_1} s_2^{a_2} \ldots s_k^{a_k}. \tag{12}$$

On the other hand, in the notation of [1], § 20,

$$s_i\left(\chi(1)\zeta_{n(e,n)}, \ldots, \chi(-1)\zeta_{n(e,n)}^{-1}\right) = \frac{1}{(n,e)} \tau(\chi^i \mid \zeta_{n(e,n)}^{i}). \tag{13}$$

This is obvious if $(n, e) = 1$; if $(n, e) = 2$ we have by (10)

$$\chi(r+n) = \chi_{(8,n^2)}(r+n)\chi_{n/(n,4)}(r+n) = -\chi_{(8,n^2)}(r)\chi_{n/(n,4)}(r) = -\chi(r); \tag{14}$$
$$2\sum_{\substack{r=1\\(r,n)=1}}^{n} \chi^i(r)\zeta_{2n}^{ri} = \sum_{\substack{r=1\\(r,n)=1}}^{n} \chi^i(r)\zeta_{2n}^{ri} + \sum_{\substack{r=1\\(r,n)=1}}^{n} \chi^i(r+n)\zeta_{2n}^{(r+n)i} = \tau(\chi^i \mid \zeta_{2n}^{i}).$$

Now, by the reduction theory for Gaussian sums, we have

$$\tau(\chi^i \mid \zeta_n^i) = b_i \tau(\chi^i),$$

on the other hand, by the theory of Jacobi sums

$$\tau(\chi^i) = c_i \tau(\chi)^i \quad \text{with} \quad c_i \neq 0.$$

It follows by (13)

$$s_1^{a_1} s_2^{a_2} \ldots s_k^{a_k} = b_{a_1 a_2 \ldots a_k} \tau(\chi^{a_1+2a_2+\ldots+ka_k}). \tag{15}$$

Formulae (11), (12) and (15) give (9) with

$$R_i(x, y) = \sum_{\substack{0\leqslant j\leqslant\varphi(n)\\ a_1+2a_2+\ldots+ka_k=j\equiv i(\mathrm{mod}\,e)}} (-1)^j a_{a_1 a_2 \ldots a_k} b_{a_1 a_2 \ldots a_k} x^{\frac{\varphi(n)+i-j}{e} - \left[\frac{i+e-1}{e}\right]} y^{\frac{j-i}{e}}.$$

Corollary 1. *Let $n > 2$, χ be a quadratic character* mod $n(n, 2)$ *with the conductor f, where $n(n, 2)/f$ is odd and let ψ_n have the meaning of Lemma 3. Then*

$$Q_n(x^2, y^2) = \psi_n(\chi; x, y)\psi_n(\chi; x, -y), \tag{16}$$

$$\psi_n(\chi; x, y) = R(x^2, y^2) - \sqrt{\chi(-1)f}\, xy S(x^2, y^2), \tag{17}$$

where R and S are polynomials with rational coefficients and

$$R(x, y) = \chi(-1)^{\frac{1}{2}\varphi(n)} R(y, x), \quad S(x, y) = \chi(-1)^{\frac{1}{2}\varphi(n)+1} S(y, x). \tag{18}$$

Besides, for n even, $\varepsilon = \pm 1$

$$\psi_n(\chi; x, \varepsilon y) = \prod_{\substack{r=1\\ \chi(r)=\varepsilon}}^{2n} (x - \zeta_{2n}^{r} y). \tag{19}$$

Proof. Formulae (16), (17) and (18) follow from (7), (9) and (8), respectively on taking into account that $\tau(\chi) = \sqrt{\chi(-1)f}$ is irrational. Besides for n even, $\varepsilon = \pm 1$

$$\varepsilon\chi(r)\zeta_{2n}^{r} = \zeta_{2n}^{r + \frac{1-\varepsilon\chi(r)}{2} n}$$

and in virtue of (14) the sequence

$$r + \frac{1-\varepsilon\chi(r)}{2} n \qquad (1 \leqslant r < n,\ (r, n) = 1)$$

is a permutation of the sequence r $(1 \leqslant r < 2n, \chi(r) = \varepsilon)$, which implies (19).

Lemma 4. *Let χ be a quadratic character* mod n *with the conductor f and*

$$\Phi_n^{(\varepsilon)}(\chi; x, y) = \omega_n^{\varepsilon}(\chi) \prod_{\substack{r=1\\ \chi(r)=\varepsilon}}^{n} (x - \zeta_n^{r} y),$$

where $\varepsilon = \pm 1$ and

$$\omega_n(\chi) = \begin{cases} \prod_{\substack{r=1\\ \chi(r)=1}}^{n} \zeta_n^{r} & \text{if } f = 3, \\ 1 & \text{otherwise.} \end{cases}$$

Then

$$Q_n(x,y) = \Phi_n^{(1)}(\chi;x,y)\Phi_n^{(-1)}(\chi;x,y), \tag{20}$$

$$\Phi_n^{(\varepsilon)}(\chi;x,y) = T(x,y) - \varepsilon\sqrt{\chi(-1)f}\,U(x,y), \tag{21}$$

where T, U are polynomials with rational coefficients and

$$T(x,y) = x^{2^{\nu-2}}, \qquad U(x,y) = y^{2^{\nu-2}} \quad \text{if} \quad f = 4,\ n = 2^\nu,$$
$$T(x,y) = -T(y,x), \qquad U(x,y) = U(y,x)$$
$$\text{if } f = 8,\ n = 2^\nu,\ \chi(1) = -1 \text{ or } f = 4,\ n = 2^\mu q^\nu \text{ or } f = q,\ n = q^\nu,\ q \text{ prime} \equiv 3 \bmod 4, \tag{22}$$
$$T(x,y) = T(y,x), \qquad U(x,y) = \chi(-1)\,U(y,x) \quad \text{otherwise.}$$

Besides we have

$$\Phi_n^{(\varepsilon)}(\chi;x^2,y^2) = \begin{cases} \Phi_n^{(\varepsilon\chi(2))}(\chi;x,y)\,\Phi_n^{(\varepsilon\chi(2))}(\chi;x,-y) & (n \text{ odd}), \\ \Phi_{2n}^{(\varepsilon)}(\chi;x,y) & (n \text{ even},\ f \neq 3). \end{cases} \tag{23}$$

Proof. Let $n = 2^\mu m$, where m/f is odd. If f is odd, there exists an integer s such that $\chi(s) = 1$,

$$(s-1,m) = \sigma = \begin{cases} 3 & \text{if } f = 3, \\ 1 & \text{otherwise.} \end{cases}$$

Hence

$$(s-1)\sum_{\substack{r=1\\ \chi(r)=\varepsilon}}^{m(n,2)} r = \sum_{\substack{r=1\\ \chi(r)=\varepsilon}}^{m(n,2)} sr - \sum_{\substack{r=1\\ \chi(r)=\varepsilon}}^{m(n,2)} r \equiv 0 \bmod m(n,2)$$

and

$$\sigma\sum_{\substack{r=1\\ \chi(r)=\varepsilon}}^{n} r \equiv 0 \bmod n \quad \text{if } n \text{ is odd},$$

$$\sigma\sum_{\substack{r=1\\ \chi(r)=\varepsilon}}^{2m} r \equiv \tfrac{1}{2}\varphi(m) \bmod 2m \quad \text{if } n \text{ is even}.$$

In the latter case

$$\sigma\sum_{\substack{r=1\\ \chi(r)=\varepsilon}}^{n} r = \sigma\sum_{\substack{r=1\\ \chi(r)=\varepsilon}}^{2m}\sum_{k=0}^{2^{\mu-1}-1} r + 2km = \sigma 2^{\mu-1}\sum_{\substack{r=1\\ \chi(r)=\varepsilon}}^{2m} r + \sigma\varphi(m)m\sum_{k=0}^{2^{\mu-1}-1} k$$

$$\equiv 2^{\mu-2}\varphi(m)m + 2^{\mu-2}\varphi(m)m(2^{\mu-1}-1) \equiv 2^{2\mu-3}\varphi(m)m \equiv \frac{\varphi(n)n}{4} \bmod n.$$

It follows that for f odd

$$\prod_{\substack{r=1\\ \chi(r)=\varepsilon}}^{n} \zeta_n^{r\sigma} = (-1)^{\frac{(n-1)\varphi(n)}{2}}. \tag{24}$$

In particular $\omega_n(\chi)^6 = 1$ and $\omega_n(\chi)$ belongs to $\mathscr{K}\left(\sqrt{\chi(-1)f}\right)$. Moreover for n odd $\omega_n(\chi) = \omega_n(\chi)^{2\chi(2)}$, thus

$$\Phi_n^{(\varepsilon)}(\chi;x^2,y^2)$$
$$= \omega_n^\varepsilon(\chi)\prod_{\substack{r=1\\ \chi(r)=\varepsilon\chi(2)}}^{n}(x^2-\zeta_n^{2r}y^2) = \omega_n^{2\varepsilon\chi(2)}\prod_{\substack{r=1\\ \chi(r)=\varepsilon\chi(2)}}^{n}(x-\zeta_n^r y)\prod_{\substack{r=1\\ \chi(r)=\varepsilon\chi(2)}}^{n}(x+\zeta_n^r y)$$
$$= \Phi_n^{(\varepsilon\chi(2))}(\chi;x,y)\,\Phi_n^{(\varepsilon\chi(2))}(\chi;x,-y),$$

which proves (23) for n odd. For n even, $f \neq 3$ we have

$$\Phi_n^{(\varepsilon)}(\chi;x^2,y^2) = \prod_{\substack{r=1\\ \chi(r)=\varepsilon}}^{n}(x^2-\zeta_n^r y^2) = \prod_{\substack{r=1\\ \chi(r)=\varepsilon}}^{n}(x-\zeta_{2n}^r y)(x-\zeta_{2n}^{r+n}y)$$
$$= \prod_{\substack{r=1\\ \chi(r)=\varepsilon}}^{2n}(x-\zeta_{2n}^r y) = \Phi_{2n}^{(\varepsilon)}(\chi;x,y).$$

Since (20) is obvious, it remains to prove (21) and (22). For f odd χ is induced by $(r|f)$, thus (21) follows from Lemma 1 of [6] and the remark after formula (20) there. Further, by (24)

$$\overline{\Phi}_n^{(\varepsilon)}(\chi;x,y) = \omega_n(\chi)^{-\varepsilon}(-1)^{\varphi(n)/2}\prod_{\substack{r=1\\ \chi(r)=\varepsilon}}^{n}\zeta_n^{-r}\prod_{\substack{r=1\\ \chi(r)=\varepsilon}}^{n}(y-\zeta_n^r x)$$
$$= (-1)^{\varphi(n)/2}\prod_{\substack{r=1\\ \chi(r)=\varepsilon}}^{n}\zeta_n^{-r\sigma}\Phi_n^{(\varepsilon)}(\chi;y,x) = (-1)^{n\varphi(n)/2}\Phi_n^{(\varepsilon)}(\chi;y,x),$$

which implies (22) since $\frac{1}{2}n\varphi(n)$ is odd only for $n = q^\nu$, q prime $\equiv 3 \bmod 4$.

For f even by (23) and (19)

$$\Phi_n^{(\varepsilon)}(\chi;x,y) = \Phi_m^{(\varepsilon)}(\chi;x^{2^\mu},y^{2^\mu}) = \begin{cases} x^{2^\mu} - \varepsilon\zeta_4 y^{2^\mu} & \text{if } m = 4, \\ \psi_{m/2}(\chi;x^{2^\mu},\varepsilon y^{2^\mu}) & \text{if } m > 4 \end{cases}$$

and the lemma follows from Corollary 1 since

$$\chi(-1)^{\frac{1}{2}\varphi(m/2)} = \begin{cases} -1 & \text{if } f = 8,\ n = 2^\nu,\ \chi(-1) = -1 \\ & \text{or } f = 4,\ n = 2^\mu q^\nu,\ q \text{ prime} \equiv 3 \bmod 4, \\ 1 & \text{otherwise.} \end{cases}$$

Remark. Lemma 4 can also be deduced from the results of [3]. One has only to rectify the formulae for λ_{3N} and λ_{4N} given on p. 192 there.

LEMMA 5. *If* $n \equiv \eta k(LM) \bmod 2\eta k(LM)$, χ *is the character* $\bmod \eta n$ *induced by* $\left(k(LM)|r\right)$,

$$Q_n^{(\varepsilon)}(\alpha,\beta) = \psi_n(\chi; \sqrt{\alpha}, \varepsilon\sqrt{\beta}) \quad (\varepsilon = \pm 1) \tag{25}$$

and

$$\delta = k(L)^{\{\frac{1}{2}\varphi(n)\}},$$

then $\delta^{-1}Q_n^{(1)}(\alpha,\beta)$ *and* $\delta^{-1}Q_n^{(-1)}(\alpha,\beta)$ *are relatively prime rational integers dividing* $Q_n(\alpha,\beta)$.

Proof. The assertion is proved as Lemma 1 in [7]. One has only to verify that $Q_n^{(\varepsilon)}(\alpha,\beta)$ defined by formula (6) there coincide with $Q_n^{(\varepsilon)}(\alpha,\beta)$ defined here. Alternatively one can proceed as below in the proof of Lemma 6.

LEMMA 6. *If* $n \equiv \eta_1 k(KM) \bmod 2\eta_1 k(KM)$, χ_1 *is the character* $\bmod \eta_1 n$ *induced by* $\left(k(KM)|r\right)$,

$$Q_n'^{(\varepsilon)}(\alpha,\beta) = \psi_n(\chi_1; \sqrt{\alpha}, \varepsilon\sqrt{\beta}) \quad (\varepsilon = \pm 1) \tag{26}$$

and

$$\delta_1 = k(K)^{\{\frac{1}{2}\varphi(n)\}},$$

then $\delta_1^{-1}Q_n'^{(1)}(\alpha,\beta)$ *and* $\delta_1^{-1}Q_n'^{(-1)}(\alpha,\beta)$ *are relatively prime rational integers dividing* $Q_n(\alpha,\beta)$.

Proof. Since $\chi_1(-1) = -1$, it follows from (17) and (18) that the functions $R(x,y)(x-y)^{\frac{1}{2}\varphi(n)}$ and $S(x,y)(x-y)^{\frac{1}{2}\varphi(n)-1}$ are symmetric of even degree thus are expressible rationally by $(x+y)^2$ and xy. Hence the numbers $R(\alpha,\beta)K^{\frac{1}{2}\varphi(n)}$ and $S(\alpha,\beta)K^{\frac{1}{2}\varphi(n)-1}$ are rational. Since

$$\sqrt{\chi_1(-1)f(\chi_1)\alpha\beta K} = \eta_1 k(KM)\sqrt{\frac{KM}{k(KM)}}$$

is rational, it follows from (17) and (26) that the numbers $K^{\frac{1}{2}\varphi(n)}\psi_n(\chi_1; \sqrt{\alpha}, \varepsilon\sqrt{\beta})$ and also $\delta_1 Q_n'^{(\varepsilon)}(\alpha,\beta)$ are rational.

They are also obviously algebraic integers, thus they are rational integers. $\delta_1^2 Q_n'^{(\varepsilon)}(\alpha,\beta)^2$ are perfect squares and since they are divisible by a square-free number δ_1^2 they are divisible by its square δ_1^4. Thus $\delta_1^{-1}Q_n'^{(\varepsilon)}(\alpha,\beta)$ are rational integers ($\varepsilon = \pm 1$). Finally, they are relatively prime. Indeed, the resultant of $\psi_n(\chi_1; x, y)$ and $\psi_n(\chi_1; x, -y)$ by (16) divides the discriminant of $Q_n(x^2, y^2)$ and *a fortiori* $(2n)^{2n}$. Since by (2) $(\alpha,\beta) = 1$, it follows from (26) that any common prime factor of $\delta_1^{-1}Q_n'^{(1)}(\alpha,\beta)$ and $\delta_1^{-1}Q_n'^{(-1)}(\alpha,\beta)$ divides $2n$. On the other hand, by

Lemma 1 any prime factor of $2n$ divides $Q_n(\alpha,\beta)$ at most in first power. Since by (16) and (26)

$$Q_n(\alpha,\beta) = Q_n'^{(1)}(\alpha,\beta)Q_n'^{(-1)}(\alpha,\beta),$$

we reach the desired conclusion.

LEMMA 7. *If* $n > 4$, $n \equiv 0 \bmod \eta_2 k(KL)$, χ_2 *is the character* $\bmod n$ *induced by* $\left(k(KL)|r\right)$, $\varepsilon = \pm 1$,

$$Q_n''^{(\varepsilon)}(\alpha,\beta) = \begin{cases} \zeta_8^{\varepsilon}\Phi_n^{(\varepsilon)}(\chi_2; \alpha, \beta) & \text{if } n = 2^\nu,\ k(KL) = -1, \\ \Phi_n^{(-\varepsilon)}(\chi_2; \alpha, \beta) & \text{if } k(KL) \equiv 5 \bmod 8, \\ \Phi_n^{(\varepsilon)}(\chi_2; \alpha, \beta) & \text{otherwise}; \end{cases} \tag{27}$$

$$\delta_2 = \begin{cases} \sqrt{2} & \text{if } n = 2, \quad k(KL) = -1, \\ \sqrt{-2} & \text{if } n = 2^\nu, \quad k(KL) = -2, \\ \sqrt{-1} & \text{if } n = 2^\mu q^\nu, \quad k(KL) = -1, \\ \sqrt{k(K)} & \text{if } n = q^\nu, \quad k(KL) = -q,\ q \text{ prime} \equiv 3 \bmod 4, \\ \sqrt{k(L)} & \text{if } n = 2q^\nu, \quad k(KL) = -q, \\ 1 & \text{otherwise}, \end{cases}$$

then $\delta_2^{-1}Q_n''^{(1)}(\alpha,\beta)$ *and* $\delta_2^{-1}Q_n''^{(-1)}(\alpha,\beta)$ *are relatively prime rational integers dividing* $Q_n(\alpha,\beta)$.

Proof. It is enough to prove that $\delta_2 Q_n''^{(\varepsilon)}(\alpha,\beta)$ is rational for $\varepsilon = \pm 1$; the remainder can be proved like the corresponding part of Lemma 6.

If $n = 2^\nu$ ($\nu \geqslant 3$), $k(KL) = -1$ we have by (22)

$$\begin{aligned} \delta_2 Q_n''^{(\varepsilon)}(\alpha,\beta) &= \sqrt{2}\,\zeta_8^{\varepsilon}(\alpha^{2^{\nu-2}} - \zeta_4\beta^{2^{\nu-2}}) \\ &= \alpha^{2^{\nu-2}} + \beta^{2^{\nu-2}} + \varepsilon\sqrt{-KL}\,\frac{\alpha^{2^{\nu-2}} - \beta^{2^{\nu-2}}}{\alpha^2 - \beta^2}, \end{aligned}$$

thus $\delta_2 Q_n''^{(\varepsilon)}(\alpha,\beta)$ can be expressed rationally in terms of $(\alpha+\beta)^2 = L$ and $\alpha\beta = M$ and is rational.

If $n = 2^\nu$, $k(KL) = -2$ or $n = 2^\mu q^\nu$, $k(KL) = -1$ it follows from (22) that $T(x,y)(x^2-y^2)$ and $U(x,y)$ are symmetric functions of even degree, hence $T(\alpha,\beta)\sqrt{KL}$ and $U(\alpha,\beta)$ are rational. Since

$$\sqrt{\chi_2(-1)f(\chi_2)KL} = k(KL)\sqrt{\frac{\eta_2 KL}{k(KL)}} \tag{28}$$

and $\delta_2 = \sqrt{k(KL)}$, it follows from (21) and (27) that $\sqrt{KL}\,\Phi_n^{(\varepsilon)}(\chi_2; \alpha, \beta)$ and $\delta_2 Q_n''^{(\varepsilon)}(\alpha,\beta)$ are rational.

If $n = q^r$, $k(KL) = -q$ it follows from (22) that $T(x,y)(x-y)$ and $U(x,y)(x+y)^{-1}$ are symmetric functions of even degree, hence $\sqrt{k(K)}\,T(\alpha,\beta)$ and $\sqrt{k(K)}\,U(\alpha,\beta)/\sqrt{KL}$ are rational. In the remaining cases by (22) $T(x,y)(x+y)^{\frac{1}{2}\varphi(n)}$ and $U(x,y)(x+y)^{\frac{1}{2}\varphi(n)}(x^2-y^2)^{-1}$ are symmetric functions of even degree, thus

$$k(L)^{\{\frac{1}{2}\varphi(n)\}}T(\alpha,\beta) \quad \text{and} \quad k(L)^{\{\frac{1}{2}\varphi(n)\}}U(\alpha,\beta)/\sqrt{KL}$$

are rational. The desired conclusion follows from (21), (27) and (28).

Proof of Theorem 2. In order to prove the first part of the theorem it is enough to show in view of Lemmata 1, 5, 6 and 7 that for $n > 3\cdot 10^{14}A^3$

$$\min\{|Q_n^{(\varepsilon)}(\alpha,\beta)|, |Q_n'^{(\varepsilon)}(\alpha,\beta)|, |Q_n''^{(\varepsilon)}(\alpha,\beta)|\} > n \qquad (\varepsilon = \pm 1). \tag{29}$$

Now by (25)-(27), (19) and Lemma 3 of [7] we have

$$\max\{|Q_n^{(-\varepsilon)}(\alpha,\beta)|, |Q_n'^{(-\varepsilon)}(\alpha,\beta)|, |Q_n''^{(-\varepsilon)}(\alpha,\beta|\} < |\alpha|^{\frac{1}{2}\varphi(n)}\exp(4n^{\frac{1}{2}}\log^2 n). \tag{30}$$

Since $|\alpha| = \sqrt{M} \geqslant \sqrt{2}$ we get by (3) and (6) for $n > 3\cdot 10^{14}A^3$

$$\begin{aligned}
&\log\min\{|Q_n^{(\varepsilon)}(\alpha,\beta)|, |Q_n'^{(\varepsilon)}(\alpha,\beta)|, |Q_n''^{(\varepsilon)}(\alpha,\beta)|\} - \log n \\
&\quad = \log|Q_n(\alpha,\beta)| - \log\max\{|Q_n^{(-\varepsilon)}(\alpha,\beta)|, |Q_n'^{(-\varepsilon)}(\alpha,\beta)|, |Q_n''^{(-\varepsilon)}(\alpha,\beta)|\} - \log n \\
&\quad > \tfrac{11}{13}\varphi(n)\log|\alpha| - \tfrac{1}{2}\varphi(n)\log|\alpha| - 4n^{1/2}\log^2 n \\
&\quad > \frac{9\log 2}{52}\,n^{1/2}\log^2 n\left(g(n) - \frac{208}{9\log 2}\right),
\end{aligned}$$

where

$$g(n) = \frac{n^{1/2}}{(e^\gamma \log\log n + 0{,}675)\log^2 n}. \tag{31}$$

$g(n)$ is an increasing function for $n > e^5$ and

$$g(3\cdot 10^{14}A^3) > g(5\cdot 10^{17}) > 5\cdot 10^4 > \frac{208}{9\log 2}, \tag{32}$$

thus (29) follows.

To prove the second part of the theorem we show that if n satisfies all three congruences $n \equiv \eta k(KL) \bmod 2\eta k(LM)$, $n \equiv \eta_1 k(KM) \bmod 2\eta_1 \times$ $\times k(KM)$ and $n \equiv 0 \bmod \eta_2 k(KL)$ then

$$Q_n^2(\alpha,\beta) = \prod_{\substack{\varepsilon=\pm 1\\ \theta=\pm 1}} Q_n^{(\varepsilon,\theta)}(\alpha,\beta), \tag{33}$$

where

$$Q_n^{(\varepsilon,\theta)}(\alpha,\beta) = \frac{\delta_0 Q_n^2(\alpha,\beta)}{Q_n^{(-\varepsilon)}(\alpha,\beta)Q'^{(-\theta)}(\alpha,\beta)Q''^{(-\varepsilon\theta)}(\alpha,\beta)}, \tag{34}$$

$$\delta_0 = \begin{cases} \sqrt{-1} & \text{if } n = 4q^r,\ q \text{ prime} \equiv 3 \bmod 4, \\ 1 & \text{otherwise;} \end{cases}$$

$Q_n^{(\varepsilon,\theta)}(\alpha,\beta)$ are rational integers relatively prime in pairs except for $n = q^r$ or $2q^r$, when two of them have the greatest common factor q.

It follows from Lemmata 5, 6 and 7 that for $\varepsilon = \pm 1$, $\theta = \pm 1$

$$(\delta\delta_1\delta_2)^{-1}Q_n^{(-\varepsilon)}(\alpha,\beta)Q_n'^{(-\theta)}(\alpha,\beta)Q_n''^{(-\varepsilon\theta)}(\alpha,\beta)$$

is rational. On the other hand

$$\delta\delta_1\delta_2 = \begin{cases} (-1)^n q & \text{if } n = q^r \text{ or } 2q^r, \\ \delta_0 & \text{otherwise.} \end{cases}$$

This implies that $Q_n^{(\varepsilon,\theta)}(\alpha,\beta)$ is rational. Moreover, since $\chi_2 = \chi\chi_1$, we have by (25)-(27), (19) and (23) for n odd

$$\begin{aligned}
Q_n^{(\varepsilon,\theta)}(\alpha,\beta) &= \frac{\delta_0 Q_n^{(\varepsilon)}(\alpha,\beta)Q_n'^{(\theta)}(\alpha,\beta)}{Q_n''^{(-\varepsilon\theta)}(\alpha,\beta)} \\
&= \frac{\delta_0\psi_n(\chi;\sqrt{\alpha},\varepsilon\sqrt{\beta})\psi_n(\chi_1;\sqrt{\alpha},\theta\sqrt{\beta})}{\Phi_n^{(-\varepsilon\theta)}(\chi\chi_1;\sqrt{\alpha},\sqrt{\beta})\Phi_n^{(-\varepsilon,\theta)}(\chi\chi_1,\sqrt{\alpha},\sqrt{\beta})} \\
&= \delta_0\omega_n^{\varepsilon\theta}(\chi\chi_1)\prod_{\substack{r=1\\ \chi(r)=\varepsilon\\ \chi_1(r)=\theta}}^{n}(\sqrt{\alpha}-\zeta_n^r\sqrt{\beta})\prod_{\substack{r=1\\ \chi(r)=-\varepsilon\\ \chi_1(r)=-\theta}}^{n}(\sqrt{\alpha}+\zeta_n^r\sqrt{\beta}),
\end{aligned}$$

for n even

$$\begin{aligned}
Q_n^{(\varepsilon,\theta)}(\alpha,\beta) &= \frac{\delta_0 Q_n^{(\varepsilon)}(\alpha,\beta)Q_n'^{(\theta)}(\alpha,\beta)}{Q_n''^{(-\varepsilon\theta)}(\alpha,\beta)} \\
&= \frac{\delta_0\Phi_{2n}^{(\varepsilon)}(\chi;\sqrt{\alpha},\sqrt{\beta})\Phi_{2n}^{(\theta)}(\chi_1;\sqrt{\alpha},\sqrt{\beta})}{\Phi_{2n}^{(-\varepsilon\theta)}(\chi\chi_1;\sqrt{\alpha},\sqrt{\beta})} = \delta_0\prod_{\substack{r=1\\ \chi(r)=\varepsilon\\ \chi_1(r)=\theta}}^{2n}(\sqrt{\alpha}-\zeta_n^r\sqrt{\beta}).
\end{aligned}$$

Therefore $Q_n^{(\varepsilon,\theta)}(\alpha,\beta)$ is an algebraic integer and hence a rational integer. Since

$$\begin{aligned}
Q_n^{(\varepsilon,\theta)}(\alpha,\beta)Q_n^{(\varepsilon,-\theta)}(\alpha,\beta) &= Q_n^{(\varepsilon)}(\alpha,\beta)^2\delta_0^2, \\
Q_n^{(\varepsilon,\theta)}(\alpha,\beta)Q_n^{(-\varepsilon,\theta)}(\alpha,\beta) &= Q_n'^{(\theta)}(\alpha,\beta)^2\delta_0^2, \\
Q_n^{(\varepsilon,\theta)}(\alpha,\beta)Q_n^{(-\varepsilon,-\theta)}(\alpha,\beta) &= Q_n''^{(\varepsilon\theta)}(\alpha,\beta)^2\delta_0^2
\end{aligned} \tag{35}$$

the greatest common factor of $Q_n^{(e_1,\theta_1)}(\alpha,\beta)$ and $Q_n^{(e_2,\theta_2)}(\alpha,\beta)$ divides at least two of the numbers

$$\left(Q_n^{(1)}(\alpha,\beta)^2, Q_n^{(-1)}(\alpha,\beta)^2\right), \quad \left(Q_n'^{(1)}(\alpha,\beta)^2, Q_n'^{(-1)}(\alpha,\beta)^2\right), \quad \left(Q_n''^{(1)}(\alpha,\beta)^2, Q_n''^{(-1)}(\alpha,\beta)^2\right)$$

equal $|\delta^2|$, $|\delta_1^2|$, $|\delta_2^2|$, respectively. However these numbers are $\{1,q,q\}$, $\{q,1,q\}$ or $\{1,1,1\}$ according to whether $n=q^r$, $2q^r$ or otherwise. It follows that $Q_n^{(e,\theta)}(\alpha,\beta)$ are relatively prime in pairs except for $n=q^r$ or $2q^r$, when (35) shows that two of them have the greatest common factor q.

Now, by (3), (6), (30)-(32) and (34) we have for $n>3\cdot 10^{14}A^3$

$$\begin{aligned}\log|Q_n^{(e,\theta)}(\alpha,\beta)|-\log n^2 &> \frac{22}{13}\varphi(n)\log|\alpha|-\frac{3}{2}\varphi(n)\log|\alpha|-12\,n^{1/2}\log^2 n\\ &\geqslant \frac{5}{52}\varphi(n)\log 2-12\,n^{1/2}\log^2 n\\ &> \frac{5\log 2}{52}n^{1/2}\log^2 n\left(g(n)-\frac{624}{5\log 2}\right)>0.\end{aligned}$$

In virtue of (33) and Lemma 1 the theorem follows.

COROLLARY 2. *If $e=1,2,3,4$ or 6, ζ_e belongs to the field $\mathscr{K}(\sqrt{KL})$ and $n>3\cdot 10^{14}A^3$ then $\alpha^n-\zeta_e^i\beta^n$ has a rational prime factor of the form $\frac{e}{(i,e)}nt\pm 1$, relatively prime to $\alpha^e-\beta^e$.*

Proof. For $e=1$ or 2 the corollary follows at once from the divisibility $Q_{ne}(\alpha,\beta)\,|\,\alpha^n-\zeta_e\beta^n$, Lemma 1 and Lemma 2.

For $e>2$ since

$$\zeta_e^i=\zeta_{e/(i,e)}^{i/(i,e)},$$

it is enough to consider the case $i=\pm 1$. Then

$$Q_{ne}'^{(i)}(\alpha,\beta)\,|\,\alpha^n-\zeta_e^i\beta^n, \quad Q_{ne}''^{(i)}(\alpha,\beta)\,|\,Q_{ne}(\alpha,\beta)$$

and the corollary follows from Lemma 1 and (29).

§ 4. In this and the next section we call an integer $a+b\zeta_e$ of the field $\mathscr{K}(\zeta_e)$ *normalized* if $e=3$ or 6, $a\equiv -1 \bmod 3$, $b\equiv 0 \bmod 3$ or $e=4$, $a\equiv 1 \bmod 4$, $b\equiv 0 \bmod 4$, *semi-normalized* if either $a+b\zeta_e$ or $-(a+b\zeta_e)$ is normalized. Two normalized integers of $\mathscr{K}(\zeta_e)$ which divide each other are equal.

LEMMA 8. *Let $e=3$, 4 or 6 and ω be a semi-normalized integer of $\mathscr{K}(\zeta_e)$ such that $(\omega,\overline{\omega})=1$. Then there exists a character χ of order e, even for $e=6$, such that*

$$f(\chi)=\begin{cases}4k_e(\omega\overline{\omega})^* & \text{if } e=6,\ \omega\overline{\omega}\equiv 3 \bmod 4,\\ k_e(\omega\overline{\omega})^* & \text{otherwise,}\end{cases}$$

$$\tau(\chi^i)=c_i^e\overline{\omega}^{e-i}\omega^i, \quad \text{where} \quad c_i\in\mathscr{K}(\zeta_e).$$

Proof. Let $\omega=\pm\omega_0^e\prod_{k=1}^{e-1}\omega_k^k$, where each ω_k is a product of distinct normalized irrational primes of $\mathscr{K}(\zeta_e)$ and ω_k's are relatively prime in pairs. In virtue of Lemma 2 of [8] there exists for each ω_k a character χ_k of order e such that

$$f(\chi_k^i)=\omega_k\overline{\omega}_k, \quad \tau(\chi_k^i)=\chi_k(-1)^{\frac{ei}{(2,e)}}\overline{\omega}_k^{e-i}\omega_k^i \quad (0<i<e).$$

Consider the character $\chi_0=\prod_{k=1}^{e-1}\chi_k^k$. In virtue of well known theorems we have

$$f(\chi_0)=\prod_{k=1}^{e-1}\omega_k\overline{\omega}_k=k_e(\omega\overline{\omega})^*,$$

$$\begin{aligned}\tau(\chi_0^i)=\prod_{k=1}^{e-1}\tau(\chi_k^{ki})^e &= \prod_{\substack{k=1\\ ki\not\equiv 0 \bmod e}}^{e-1}\chi_k(-1)^{\frac{eki}{(2,e)}}\overline{\omega}_k^{e-e\left\{\frac{ki}{e}\right\}}\omega_k^{e\left\{\frac{ki}{e}\right\}}\\ &= \chi_0(-1)^{\frac{ei}{(2,e)}}\prod_{k=1}^{e-1}\overline{\omega}_k^{ke-ki}\omega_k^{ki}\prod_{\substack{k=1\\ ki\not\equiv 0 \bmod e}}^{e-1}\overline{\omega}_k^{-ke+e+e\left[\frac{ki}{e}\right]}\omega_k^{-e\left[\frac{ki}{e}\right]}\times\\ &\qquad\times\prod_{\substack{k=1\\ ki\equiv 0 \bmod e}}^{e-1}\overline{\omega}_k^{-ke+ki}\omega_k^{ki}\\ &= \chi_0(-1)^{\frac{ei}{(2,e)}}c_i^e\overline{\omega}^{e-i}\omega^i,\end{aligned}$$

where

$$c_i=\pm\omega_0^{-1}\prod_{k=1}^{e-1}\overline{\omega}_k^{-k-\left[-\frac{ki}{e}\right]}\omega_k^{-\left[\frac{ki}{e}\right]}.$$

For $e=3$ or 4 we have $\chi_0(-1)^{e/(2,e)}=1$. For $e=6$

$$\chi_0(-1)=\prod_{k=1}^{5}\chi_k(-1)^k=(-1)^{(f(\chi_1\chi_3\chi_5)-1)/6},$$

thus $\chi_0(-1)=-1$ only if $f(\chi_1\chi_3\chi_5)=k(\omega\overline{\omega})\equiv\omega\overline{\omega}\equiv 3 \bmod 4$.

Set now

$$\chi=\begin{cases}\chi_4\chi_0 & \text{if } e=6,\ \omega\overline{\omega}\equiv 3 \bmod 4,\\ \chi_0 & \text{otherwise,}\end{cases}$$

where χ_4 is the primitive character mod 4. For $e=6$, $\omega\overline{\omega} \equiv 3 \bmod 4$ we have

$$\chi(-1)=1, \quad f(\chi)=4k_e(\omega\overline{\omega})^*,$$
$$\tau(\chi^i)^e=\tau(\chi_4^i)^e\tau(\chi_0^i)^e=(-1)^i\chi_0(-1)^i c_i^e\overline{\omega}^{e-i}\omega^i=c_i^e\overline{\omega}^{e-i}\omega^i.$$

Thus the character χ satisfies the conditions of the lemma.

LEMMA 9. *Let e, ω and χ have the meaning of Lemma 8 and ε run through e-th roots of unity. If $m(m,e)/f(\chi)$ is an integer relatively prime to e,*

$$Q_m^{(e)}(\omega,\overline{\omega})=\chi(-1)^{\varphi(m)/2e}\psi_m(\chi;\omega^{1/e},\varepsilon\overline{\omega}^{1/e}), \tag{36}$$

χ is considered as a character mod $m(m,e)$ *and $m>3\cdot 10^{14}\max^3\{12,\log\omega\overline{\omega}\}$, then $Q_m^{(e)}(\omega,\overline{\omega})$ are rational integers, relatively prime in pairs and*

$$|Q_m^{(e)}(\omega,\overline{\omega})|>m.$$

Proof. We have $\chi(-1)^{\varphi(m)/2}=1$ and by Lemma 8

$$\left(\tau(\chi^i)(\omega^{1/e})^{e-i}(\varepsilon\overline{\omega}^{1/e})^i\right)^e=c_i^e(\omega\overline{\omega})^e,$$

thus

$$\chi(-1)^{\varphi(m)/2e}\in\mathscr{K}(\zeta_e) \quad \text{and} \quad \tau(\chi^i)(\omega^{1/e})^{e-i}(\varepsilon\overline{\omega}^{1/e})^i\in\mathscr{K}(\zeta_e).$$

It follows hence that

$$\chi(-1)^{\varphi(m)/2e}R_0(\omega,\overline{\omega})\in\mathscr{K}(\zeta_e)$$

and

$$\chi(-1)^{\varphi(m)/2e}\tau(\chi^i)(\omega^{1/e})^{e-i}(\varepsilon\overline{\omega}^{1/e})^iR_i(\omega,\overline{\omega})\in\mathscr{K}(\zeta_e) \quad (0<i<e),$$

thus by (9) and (36)

$$Q_m^{(e)}(\omega,\overline{\omega})\in\mathscr{K}(\zeta_e).$$

On the other hand, $Q_m^{(e)}(\omega,\overline{\omega})$ is real because by (8)

$$\begin{aligned}\overline{\chi(-1)^{\varphi(m)/2e}\psi_m(\chi;\omega^{1/e},\varepsilon\overline{\omega}^{1/e})}&=\chi(-1)^{-\varphi(m)/2e}\psi_m(\chi;\overline{\omega}^{1/e},\varepsilon^{-1}\omega^{1/e})\\&=\chi(-1)^{\varphi(m)/2e}\psi_m(\chi;\varepsilon^{-1}\omega^{1/e},\overline{\omega}^{1/e})\\&=\chi(-1)^{\varphi(m)/2e}\psi_m(\chi;\omega^{1/e},\varepsilon\overline{\omega}^{1/e}).\end{aligned}$$

Since $Q_m^{(e)}(\omega,\overline{\omega})$ is obviously an algebraic integer it is a rational integer. To prove that $Q_m^{(e)}(\omega,\overline{\omega})$ and $Q_m^{(\theta)}(\omega,\overline{\omega})$ are relatively prime for $\varepsilon\neq\theta$ we notice that by (7) the resultant of $\psi_m(\chi;x,\varepsilon y)$ and $\psi_m(\chi;x,\theta y)$ divides the discriminant of $Q_m(x^e,y^e)$ and *a fortiori* $(em)^{em}$. Since $(\omega,\overline{\omega})=1$ it follows by (36) that any common prime factor of $Q_m^{(e)}(\omega,\overline{\omega})$ and $Q_m^{(\theta)}(\omega,\overline{\omega})$ divides em. On the other hand, by Lemma 1, any prime factor of $6m$ divides $Q_m(\omega,\overline{\omega})$ at most in first power. Since

$$Q_m(\omega,\overline{\omega})=\prod_e Q_m^{(e)}(\omega,\overline{\omega}) \tag{37}$$

we reach the desired conclusion.

Now, if $(m,e)=1$

$$Q_m^{(e)}(\omega,\overline{\omega})=\overline{\omega}^{\varphi(m)/e}\prod_{\theta^e=1}\prod_{\substack{r=1\\ \chi(r)=\theta}}^{m}\left(\frac{\omega^{1/e}}{\varepsilon\theta\overline{\omega}^{1/e}}-\zeta_m^r\right).$$

If $(m,e)=2$ we have $f(\chi)\equiv 0 \bmod 4$ and by Lemma 8 $\chi=\chi_4\chi_0$, where χ_0 is a character mod $m/2$. Hence

$$\begin{aligned}Q_m^{(e)}(\omega,\overline{\omega})&=\prod_{\substack{r=1\\(r,m)=1}}^{m}\left(\omega^{1/e}-\chi(r)\zeta_{2m}^r\varepsilon\overline{\omega}^{1/e}\right)\\&=\prod_{\substack{r=1\\(r,m)=1}}^{m}\left(\omega^{1/e}-\chi\big(r(4+m/2)\big)\zeta_{2m}^{r(4+m/2)}\varepsilon\overline{\omega}^{1/e}\right)\\&=\prod_{\substack{r=1\\(r,m)=1}}^{m}\left(\omega^{1/e}-\chi(4+m/2)\chi_4(r)\chi_0(r)\zeta_4^r\zeta_{m/2}^r\varepsilon\overline{\omega}^{1/e}\right)\\&=\prod_{\substack{r=1\\(r,m/2)=1}}^{m/2}\left(\omega^{1/e}-\chi(4+m/2)\zeta_4\chi_0(r)\zeta_{m/2}^r\varepsilon\overline{\omega}^{1/e}\right)\\&=\overline{\omega}^{\varphi(m)/e}\prod_{\theta^e=1}\prod_{\substack{r=1\\ \chi_0(r)=\theta}}^{m/2}\left(\frac{\omega^{1/e}}{\varepsilon\theta\overline{\omega}^{1/e}}\overline{\chi}(4+m/2)\zeta_4^{-1}-\zeta_{m/2}^r\right).\end{aligned}$$

Therefore, by Lemma 3 of [7]

$$|Q_m^{(e)}(\omega,\overline{\omega})|\leqslant|\overline{\omega}|^{\varphi(m)/e}\exp(2em^{1/2}\log^2 m).$$

On the other hand, since $k\big((\omega+\overline{\omega})^2\big)=1$ we have by Lemma 3 for $m>3\cdot 10^{14}\max^3\{12,\log\omega\overline{\omega}\}>5\cdot 10^{17}$

$$Q_m(\omega,\overline{\omega})|>m|\overline{\omega}|^{\frac{11}{13}\varphi(m)}.$$

It follows by (6), (31), (32) and (37) that for m in question

$$\begin{aligned}\log|Q_m^{(e)}(\omega,\overline{\omega})|-\log m&>\frac{11}{13}\varphi(m)\log|\overline{\omega}|-\frac{e-1}{e}\varphi(m)\log|\overline{\omega}|-\\&\qquad-2e(e-1)m^{1/2}\log^2 m\\&\geqslant\frac{1}{78}\varphi(m)\log|\overline{\omega}|-60\,m^{1/2}\log^2 m\\&\geqslant\frac{\log 2}{156}m^{1/2}\log^2 m\left(g(m)-\frac{9360}{\log 2}\right)>0.\end{aligned}$$

This completes the proof.

Proof of Theorem 3. We set for $e = 3$ or 6

$$\langle \omega, m\rangle = \begin{cases} \langle \alpha, n\rangle & \text{if} \quad K \equiv 0 \bmod 27, \\ \left\langle \zeta_4 \alpha, n \dfrac{(2n,8)}{(n^3,8)} \right\rangle & \text{if} \quad L \equiv 0 \bmod 27, \\ \langle \zeta_3^s \alpha, n/3\rangle & \text{if} \quad K \equiv 6 \bmod 9, \\ \left\langle \zeta_{12}^s \alpha, \dfrac{n}{3} \cdot \dfrac{(2n,8)}{(n^3,8)} \right\rangle & \text{if} \quad L \equiv 6 \bmod 9; \end{cases}$$

for $e = 4$

$$\langle \omega, m\rangle = \begin{cases} \langle \alpha, n\rangle & \text{if} \quad K \equiv 0 \bmod 8, \\ \langle \zeta_4 \alpha, n/2\rangle & \text{if} \quad L \equiv 0 \bmod 8, \\ \langle \zeta_8^s \alpha, n/4\rangle & \text{if} \quad KL \not\equiv 0 \bmod 8. \end{cases}$$

It can be verified that for a suitably chosen $s = \pm 1$, ω is a semi-normalized integer of $\mathscr{K}(\zeta_e)$ and $m > 3 \cdot 10^{14} B^3$. Moreover

$$Q_n(\alpha, \beta) = \begin{cases} Q_m(\omega, \overline{\omega}) & \text{if} \quad KL \equiv 0 \bmod e^3/(8, e^3), \\ Q_m(\omega, \overline{\omega}) Q_m(\zeta_e^s \omega, \zeta_e^{-s} \overline{\omega}) & \text{otherwise.} \end{cases} \tag{38}$$

Since $\omega\overline{\omega} = M$ and $(n/\eta_e k_e(M)^*, e) = 1$, ω and m satisfy the assumptions of Lemma 9. Therefore by (37) $Q_m(\omega, \overline{\omega})$ has e pairwise relatively prime factors $> m$ and by Lemma 1 $Q_m(\omega, \overline{\omega})$ has e distinct prime factors $\equiv \pm 1 \bmod m$. These primes clearly do not divide n and again by Lemma 1 they are primitive prime factors of $P_n(\alpha, \beta)$. If $KL \equiv 0 \bmod e^3/(8, e^3)$ we have $e = e + (e, 2)[(\eta_e + 1)/4]$ and the theorem is proved. Otherwise the resultant of $Q_m(x, y)$ and $Q_m(\zeta_e^s x, \zeta_e^{-s} y)$ divides the discriminant of their product $Q_n(x, y)$ and *a fortiori* n^n. The same applies to the greatest common divisor of $Q_m(\omega, \overline{\omega})$ and $Q_m(\zeta_e^s \omega, \zeta_e^{-s} \overline{\omega})$. Therefore, the primitive prime factors mentioned beforehand do not divide $Q_m(\zeta_e^s \omega, \zeta_e^{-s} \overline{\omega})$. By Lemma 2 we have for $m > 3 \cdot 10^{14} B^3$

$$|Q_m(\zeta_e^s \omega, \zeta_e^{-s} \overline{\omega})| > m,$$

thus for $e = 3$ we get from Lemma 1 and (38)

$$4 = e + (e, 2)\left[\frac{\eta_e + 1}{4}\right]$$

primitive prime factors of $P_n(\alpha, \beta)$.

Finally if $e = 4$ or 6 and $KL \not\equiv 0 \bmod e^3/8$, $P_m(\zeta_e^s \omega, \zeta_e^{-s} \overline{\omega})$ has by Theorem 2 two primitive prime factors. These factors by Lemma 1 divide

$Q_m(\zeta_e^s \omega, \zeta_e^{-s} \overline{\omega})$, thus we get from (38)

$$e + 2 = e + (e, 2)\left[\frac{\eta_e + 1}{4}\right]$$

primitive prime factors of $P_n(\alpha, \beta)$.

§ 5. THEOREM 4. *Let u_n be a recurrence of the second order given by the formula $u_n = \Omega\omega^n + \Omega'\omega'^n$, where ω and ω' satisfy $z^2 - Pz + Q = 0$, P, Q, u_0, u_1 are rational integers*

$$\Delta = P^2 - 4Q < 0, \quad P^2 \neq Q,\ 2Q,\ 3Q \tag{39}$$

and ω/ω', Ω/Ω' are multiplicatively dependent. If e is the number of roots of unity contained in $\mathscr{K}(\sqrt{\Delta})$, u and v are the least in absolute value integers satisfying

$$(\omega/\omega')^{eu/2} = (-\Omega/\Omega')^{ev/2}, \quad v > 0, \tag{40}$$

$n > 0$ and $nv + u > 3 \cdot 10^{14} \max^3\{12, \log 2Q^2 (P^2, Q)^{-1}\}$, then

$$q(u_n) \geqslant nv + u - 1$$

(q denotes the greatest prime factor).

Proof. Let r and s be integers such that

$$ru - sv = \sigma = (u, v).$$

It follows from (40) that $(\omega/\omega')^{u/\sigma}(-\Omega/\Omega')^{-v/\sigma}$ is a root of unity, hence by the definition of e

$$\left(\frac{\omega}{\omega'}\right)^{eu/\sigma} \left(-\frac{\Omega}{\Omega'}\right)^{-ev/\sigma} = 1$$

and by the choice of u and v, $\sigma \leqslant 2$.

It follows further from (40) that

$$\left(\frac{\omega}{\omega'}\right)^{\sigma e/2} = \left(-\frac{\Omega}{\Omega'}\right)^{erv/2} \left(\frac{\omega'}{\omega}\right)^{esv/2},$$

whence

$$\frac{\omega^e}{\omega'^e} = \left(\left(\frac{\Omega}{\Omega'}\right)^r \left(\frac{\omega'}{\omega}\right)^s\right)^{ev/\sigma}. \tag{41}$$

The number $(\Omega/\Omega')^r(\omega'/\omega)^s$ is a quotient of two conjugates in $\mathscr{K}(\sqrt{\Delta})$ and is different from ± 1 since by (39) ω/ω' is not a root of unity. Therefore, it can be represented in the form $\dfrac{(L^{1/2} + K^{1/2})/2}{(L^{1/2} - K^{1/2})/2}$, where L, K are rational integers, $L > 0$, $K < 0$, $\mathscr{K}(\sqrt{KL}) = \mathscr{K}(\sqrt{\Delta})$ and $(4L, L - K) = 4$. Set

$$L - K = 4M, \quad (L^{1/2} + K^{1/2})/2 = \alpha, \quad (L^{1/2} - K^{1/2})/2 = \beta.$$

α^e and β^e are relatively prime integers of $\mathscr{K}(\sqrt{\Delta})$ semi-normalized if $\mathscr{K}(\sqrt{\Delta}) = \mathscr{K}(\zeta_e)$. Also $\omega^e(P^2, Q)^{-e/2}$ and $\omega'^e(P^2, Q)^{-e/2}$ are such integers and since by (41)

$$\frac{\omega^e(P^2, Q)^{-e/2}}{\omega'^e(P^2, Q)^{-e/2}} = \frac{\alpha^{ev/\sigma}}{\beta^{ev/\sigma}},$$

we get

$$\omega^e(P^2, Q)^{-e/2} = \pm\alpha^{ev/\sigma}, \qquad \omega'^e(P^2, Q)^{-e/2} = \pm\beta^{ev/\sigma},$$

$$\omega = \zeta_{2e}^{-\mu}(P^2, Q)^{1/2}\alpha^{v/\sigma}, \qquad \omega' = \zeta_{2e}^{\mu}(P^2, Q)^{1/2}\beta^{v/\sigma}. \tag{42}$$

Since $(\Omega^2\Delta, \Omega'^2\Delta) = \big((2u_1 - Pu_0)^2, u_1^2 - Pu_1u_0 + Qu_0^2\big) = \Delta_1$ is a rational integer and by (40)

$$\left(\frac{\Omega^2\Delta/\Delta_1}{\Omega'^2\Delta/\Delta_1}\right)^{ev/2} = \left(\frac{\alpha}{\beta}\right)^{euv/\sigma},$$

it follows as before that

(43)

$$\langle\Omega(\omega-\omega'), \Omega'(\omega'-\omega)\rangle = \begin{cases} \langle\zeta_{2e}^{-\nu}\Delta_1^{1/2}\alpha^{u/\sigma}, \zeta_{2e}^{\nu}\Delta_1^{1/2}\beta^{u/\sigma}\rangle & \text{if} \quad u \geqslant 0, \\ \langle\zeta_{2e}^{-\nu}\Delta_1^{1/2}\beta^{|u|/\sigma}, \zeta_{2e}^{\nu}\Delta_1^{1/2}\alpha^{|u|/\sigma}\rangle & \text{if} \quad u < 0. \end{cases}$$

Thus we obtain

$$u_n = \zeta_{2e}^{-(n-1)\mu-\nu}\Delta_1^{1/2}(P^2, Q)^{(n-1)/2}(\alpha\beta)^{(|u|-u)/2\sigma}\,\frac{\alpha^{(nv+u)/\sigma} - \zeta_e^{n\mu+\nu}\beta^{(nv+u)/\sigma}}{\alpha^{v/\sigma} - \zeta_e^{\mu}\beta^{v/\sigma}}.$$

Since ω/ω' is not a root of unity, by (41) α/β also is not such a root, hence $\langle L, M\rangle \neq \langle 1, 1\rangle, \langle 2, 1\rangle, \langle 3, 1\rangle$. Further, it follows from (42) that

$$M = \alpha\beta \leqslant \omega\omega'(P^2, Q)^{-1} = Q(P^2, Q)^{-1}.$$

Since $\min\{-K, L\} \leqslant 2M$, we get

$$A \leqslant \max\{12, \log 2Q^2(P^2, Q)^{-2}\}$$

and in virtue of Corollary 2 $\alpha^{(nv+u)/\sigma} - \zeta_e^{n\mu+\nu}\beta^{(nv+u)/\sigma}$ has a rational prime factor p of the form $\dfrac{e}{(n\mu+\nu, e)}\cdot\dfrac{nv+u}{\sigma}t \pm 1$ relatively prime to $\alpha^e - \beta^e$.

Since $\big((nv+u)/\sigma, v/\sigma\big) = 1$, the highest common factor of $\alpha^{(nv+u)/\sigma} - \zeta_e^{n\mu+\nu}\beta^{(nv+u)/\sigma}$ and $\alpha^{v/\sigma} - \zeta_e^{\mu}\beta^{v/\sigma}$ divides $\alpha^e - \beta^e$. Thus p is relatively prime to $\alpha^{v/\sigma} - \zeta_e^{\mu}\beta^{v/\sigma}$, we have $p \mid u_n$ and

$$q(u_n) \geqslant p \geqslant nv + u - 1$$

except possibly if

$$\sigma = 2, \qquad \eta\mu + \nu \equiv 0 \bmod e. \tag{44}$$

In that case we have by the choice of u, v

$$\left(\frac{\omega}{\omega'}\right)^{eu/4} \neq \left(-\frac{\Omega}{\Omega'}\right)^{ev/4},$$

hence by (42), (43)

$$nv/2 \not\equiv \mu u/2 \bmod 2$$

and by (38) $(nv+u)/\sigma$ is odd. The prime p being of the form $(nv+u)t/2 \pm 1$ must be at least $nv+u-1$, which completes the proof.

References

[1] H. Hasse, *Vorlesungen über Zahlentheorie*, Berlin 1964.

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

[3] T. Nagell, *Contributions à la théorie des corps et des polynômes cyclotomiques*, Ark. Math. 5 (1964), pp. 153-192.

[4] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), pp. 64-94.

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

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

[7] — *On primitive prime factors of Lehmer numbers I*, Acta Arith. 8 (1963), pp. 213-223.

[8] — *On primitive prime factors of Lehmer numbers II*, Acta Arith. 8 (1963), pp. 251-257.

[9] — *On two theorems of Gelfond and some of their applications*, Acta Arith. 13 (1967), pp. 177-236.

Corrigenda to [5], [7] and [8]

[5] p. 414 line -4 replace $-\nu(n)$ by $-2^{\nu(n)}$,
line -3 replace $[N_0(N_0+1)/2]+1$ by $[N_0(N_0+1)/2]+2$;

[7] p. 214 line 7 replace $\langle 1, -5\rangle$ by $\langle 1, -1\rangle$.

In Theorem 2 and Lemmata 4 and 5 the assertion $\varlimsup\limits_{n} \dfrac{q(P_n)}{n} \geqslant 2$ must be replaced by a weaker one: $q(P_n) \geqslant n+1$ for $n > n_0$. Indeed, if $n+1$ and $n-1$ are both primes and $(KL \mid n \pm 1) = \pm 1$ one can not conclude as in the last sentence on p. 223 that at least one of two primitive prime factors of P_n is $\geqslant 2n-1$.

[8] In Lemma 1 the assumption must be added: $n > 2$ and the convention made: $\tau_i = 1$ for $i \equiv 0 \pmod e$.

In the footnote on p. 254, replace $A \equiv B+1 \pmod 4$ by $A \equiv 1 \pmod 4$.
The formula for $Q_n^{(i)}(\alpha, \beta)$ on p. 255 must be replaced by

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

and the corresponding change must be made in formula (15), p. 256, which as it stands applies to $Q_n^{(0)}(\alpha, \beta)$.
In formula (16) replace $\psi(\chi_{n/\eta_e}^i; x, y)$ by $\psi(\chi_{n/\eta_e}; x, \zeta_e^i y)$.

Reçu par la Rédaction le 30. 12. 1967

ACTA ARITHMETICA
XV (1968)

A note on solid partitions

by

LORNE HOUTEN (Pullman, Wash.)

1. The purpose of this paper is to extend some of the results of [2] to solid partitions.

2. We define a solid partition of a positive integer n to be a representation of n as the solution to a Diophantine equation of the form

$$n = \sum_{i,j,k=1}^{\infty} n_{i,j,k}$$

where the $n_{i,j,k}$ are non-negative integers satisfying $n_{i,j,k} \geqslant n_{i+1,j,k}$, $n_{i,j,k} \geqslant n_{i,j+1,k}$, and $n_{i,j,k} \geqslant n_{i,j,k+1}$. We may represent such a partition as a three dimensional array obtained by placing the non-zero part $n_{i,j,k}$ in a position $i-1$ units to the right of, j units below and k units underneath some origin. For example, the solid partitions of 4 are:

First Plane	4	31	3 1	3	22	2 2	2	211	21 1	2 1 1
Second Plane				1			2			
Third Plane										
Fourth Plane										