References

[1] B. C. Berndt, *Classical theorems on quadratic residues*, L'Enseign. Math. 22 (1976), pp. 261–304.

[2] P. Kaplan, *Sur le 2-groupe des classes d'idéaux des corps quadratiques*, J. Reine Angew. Math. 283/284 (1976), pp. 313–363.

[3] M. A. Kenku, *Atkin-Lehner involutions and class number residuality*, Acta Arith. 33 (1977), pp. 1–9.

[4] A. Pizer, *On the 2-part of the class number of imaginary quadratic number fields*, J. Number Theory 8 (1976), pp. 184–192.

DEPARTMENT OF MATHEMATICS AND STATISTICS
CARLETON UNIVERSITY
OTTAWA, ONTARIO, CANADA K1S 5B6

Received on 1.4.1985
and in revised form on 10.6.1985 (1503)

ACTA ARITHMETICA
XLVII (1986)

Reducibility of lacunary polynomials, VI

by

A. Schinzel (Warszawa)

In this paper we shall complete the study of reducibility of non-reciprocal quadrinomials begun in [3] and continued in [6], [7].

As usual in this series of papers reducibility means reducibility over the rational field Q, polynomials have integral coefficients and for a polynomial $f \in \mathbf{Z}[x]$, $f \neq 0$, $|f|$ denotes its degree, $\|f\|$ the sum of squares of its coefficients, $Kf(x)$, called the kernel of f, the polynomial $x^{-\operatorname{ord}_x f} f$ deprived of all its cyclotomic factors. The formula

$$f(x) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} f_\sigma(x)^{e_\sigma}$$

means in addition to the equality that the polynomials f_σ are irreducible and relatively prime in pairs. We shall prove

Theorem 1. *Let a_j $(0 \leqslant j \leqslant 3)$ be non-zero integers. Then for any quadrinomial*

$$q(x) = a_0 + \sum_{j=1}^{3} a_j x^{n_j} \quad (0 < n_1 < n_2 < n_3),$$

that is not reciprocal, we have one of the following four possibilities:

(i) *$Kq(x)$ is irreducible.*

(ii) *$q(x)$ can be divided into two parts that have the highest common factor $d(x)$ being a non-reciprocal binomial. $K\big(q(x)d(x)^{-1}\big)$ is then irreducible, unless $q(x)d(x)^{-1}$ is a binomial.*

(iii) *$q(x)$ can be represented in one of the forms*

$$k(T^2 - 4TUVW - U^2V^4 - 4U^2W^4)$$
$$= k(T - UV^2 - 2UVW - 2UW^2)(T + UV^2 - 2UVW + 2UW^2),$$

$$k(U^3 + V^3 + W^3 - 3UVW)$$
$$= k(U + V + W)(U^2 + V^2 + W^2 - UV - UW - VW),$$

$$k(U^2 + 2UV + V^2 - W^2) = k(U + V + W)(U + V - W),$$

where $k = \pm(a_0, a_1, a_2, a_3)$ and T, U, V, W are monomials in $\mathbf{Z}[x]$. The factors on the right-hand side have irreducible kernels.

(iv) *$n_j = vv_j$ $(1 \leqslant j \leqslant 3)$; v and v_j are positive integers,*

$$v_3 < \exp_2(12\cdot 2^{\|q\|}\log\|q\|)$$

and $K\left(a_0+\sum_{j=1}^{3} a_j x^{v_j}\right)$ is reducible.

Moreover,

$$K\left(a_0+\sum_{j=1}^{3} a_j x^{v_j}\right) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(x)^{e_\sigma}$$

implies

$$Kq(x) \overset{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} F_\sigma(x^v)^{e_\sigma}.$$

The method of the proof of the theorem still works if the rational field is replaced by a totally real field, or a totally complex quadratic extension of such a field. In the latter case the assumption that $q(x)$ is not reciprocal should be replaced by the assumption that it is not self-inversive, i.e. $x^{|q|}q(x^{-1}) \neq \text{const}\,\bar{q}(x)$, where the bar denotes the complex conjugation. Small modifications are needed then in the parts (iii) and (iv) of the theorem. Some complications that arise in the proof are indicated briefly after Lemma 1.

Already for the rational field there remains as an open problem the reducibility of reciprocal quadrinomials. A little light on this question is shed by

THEOREM 2. *If*

$$q(x) = a_0+\sum_{j=1}^{3} a_j x^{n_j} \quad (0 < n_1 < n_2 < n_3)$$

is primitive reciprocal and

$$|a_0| = \prod_{i=1}^{k} p_i^{\alpha_i} \quad (p_i \text{ distinct primes}),$$

then the number of primitive irreducible factors of $q(x)$ with the leading coefficient different from ± 1, counted with multiplicities, does not exceed $\sum_{i=1}^{k}(\alpha_i, n_1)$.

COROLLARY 1. *If under the assumptions of Theorem 2 $|a_0| \geqslant |a_1|$ then the number of irreducible factors of $Kq(x)$, counted with multiplicities, does not exceed $\sum_{i=1}^{k}(\alpha_i, n_1)$.*

COROLLARY 2. *If under the assumption of Theorem 2 $k = 1$ and $(\alpha_1, n_1) = 1$, then $Kq(x)$ is irreducible.*

THEOREM 3. *If $q(x) = a_0+\sum_{j=1}^{3} a_j x^{n_j}$ $(0 < n_1 < n_2 < n_3)$ is reciprocal and primitive, $|a_0| \geqslant |a_1|$ and $Kq(x)$ is reducible, then $|a_0| \geqslant 2$ and*

$$\frac{n_3}{2n_1} \geqslant \min_{l\in S}\max\left\{\max_{p|a_0}\frac{\operatorname{ord}_p l}{\operatorname{ord}_p a_0}+\max_{p|a_0}\frac{\operatorname{ord}_p(a_0/l)}{\operatorname{ord}_p a_0},\right.$$
$$\left.\frac{\log(|a_0|/2)}{\log l}\cdot\max_{p|a_0}\frac{\operatorname{ord}_p l}{\operatorname{ord}_p a_0},\ \frac{\log(|a_0|/2)}{\log(|a_0|/l)}\cdot\max_{p|a_0}\frac{\operatorname{ord}_p(a_0/l)}{\operatorname{ord}_p a_0}\right\},$$

where

$$S = \{l\in\mathbf{Z}\colon\ 1 < l \leqslant \sqrt{|a_0|},\ l|a_0,\ n_1\operatorname{ord}_p l \equiv 0 \bmod \operatorname{ord}_p a_0 \quad \textit{for all primes } p|a_0\}.$$

COROLLARY 3. *If under the assumptions of Theorem 3 a_0 is squarefree, we have*

$$\frac{n_3}{2n_1} \geqslant \max\left\{2,\ \min_{\substack{1<l\leqslant\sqrt{|a_0|}\\ l|a_0}}\frac{\log(|a_0|/2)}{\log l}\right\}.$$

The equality in the above estimate can be attained, as it is shown by the example

$$6x^4+x^3+x+6 = (3x^2-4x+3)(2x^2+3x+2).$$

Proofs of the theorems preceded by several lemmata are based on the results of [2], [4], [6] and [9]. At the end of the paper there is a note correcting some errors in [4]. Since this is already the third note of this sort (after [8] and the note in [6]), the author apologizes to the readers of [4] for his great inaccuracy.

LEMMA 1. *If $\langle|a_0|, |a_1|, |a_2|, |a_3|\rangle$ is a permutation of $\langle|a_0|, |a_0|, |a_i|, |a_i|\rangle$ for $i = 1$ or 2, then either $q(x)$ is reciprocal, or every irreducible reciprocal factor of $q(x)$ is cyclotomic.*

Proof. If $|a_0| = |a_{3-i}|$, $|a_3| = |a_i|$ then for any zero ζ of the factor f in question

$$a_0+a_{3-i}\zeta^{n_{3-i}} = -a_i\zeta^{n_i}-a_3\zeta^{n_3},$$
$$a_0+a_{3-i}\zeta^{-n_{3-i}} = -a_i\zeta^{-n_i}-a_3\zeta^{-n_3}.$$

If $a_0+a_{3-i}\zeta^{n_3-i}=0$, ζ is a root of unity, f is cyclotomic. If $a_0+a_{3-i}\zeta^{n_3-i}\neq 0$, we get dividing the above equations side by side:

$$\frac{a_{3-i}}{a_0}\zeta^{n_3-i}=\frac{a_3}{a_i}\zeta^{n_3+n_i},$$

$$\zeta^{n_3+n_i-n_{3-i}}=\frac{a_i a_{3-i}}{a_0 a_3}=\pm 1$$

and since $n_3+n_i>n_{3-i}$, ζ is a root of unity, f is cyclotomic.

If $|a_0|=|a_3|$, $|a_1|=|a_2|$ then in virtue of Lemma 17 of [6], proved in the above pattern, either $q(x)$ is reciprocal or $f(x)$ is cyclotomic.

Remark 1. In the case, where a_i belong to a totally complex quadratic extension K of a totally real field the above argument, when suitably modified, leads to the conclusion that either $q(x)$ is self-inversive, or every monic irreducible self-inversive factor of $q(x)$ in $K[x]$ with integer coefficients is cyclotomic. Indeed,

$$\left|\frac{a_{3-i}}{a_0}\right|=\left|\frac{a_i}{a_3}\right|=1$$

implies that all conjugates of $\bar{a}_i a_{3-i}/\bar{a}_0 a_3$ and of a_0/a_{3-i} have modulus 1 and since

$$\text{either}\quad \zeta^{n_3+n_i-n_{3-i}}=\frac{\bar{a}_i a_{3-i}}{\bar{a}_0 a_3}\quad\text{or}\quad \zeta^{n_3-i}=-\frac{a_0}{a_{3-i}}$$

all conjugates of ζ with respect to $\boldsymbol{Q}$ have modulus 1. By Kronecker's theorem either ζ is a root of unity, or ζ is not an algebraic integer.

Lemma 2. *If* $\langle|a_0|, |a_1|, |a_2|, |a_3|\rangle$ *is not a permutation of* $\langle|a_0|, |a_0|, |a_i|, |a_i|\rangle$ *for any* $i\leqslant 2$ *and* $(n_1, n_2, n_3)=1$ *then every squarefree reciprocal factor of* $q(x)$ *is of degree at most* $4\sqrt{3n_3}$.

Proof. In virtue of the well-known lemma (see, e.g. [1], Lemma 3 of Chapter VI) there exist integers $\gamma_1, \gamma_2, \gamma_3$ such that

$$\gamma_1 n_1+\gamma_2 n_2+\gamma_3 n_3=0\quad\text{and}\quad 0<\max|\gamma_i|<\sqrt{3\max\{n_1, n_2, n_3\}}.$$

In view of symmetry (we have not used the fact that $\max\{n_1, n_2, n_3\}=n_3$) we may assume that

$$\gamma_1>0,\quad \gamma_2\geqslant 0,\quad \gamma_3<0.$$

Let us consider polynomials

$$F_1(x, y)=(a_0+a_1 x+a_2 y)^{-\gamma_3}-(-a_3)^{-\gamma_3}x^{\gamma_1}y^{\gamma_2},$$
$$F_2(x, y)=(a_0+a_1 x+a_2 y)(a_0 xy+a_1 y+a_2 x)-a_3^2 xy.$$

The polynomial $F_2(x, y)$ is irreducible. Indeed, otherwise it would have a linear factor of the form

$$\text{either}\quad x-b\quad\text{or}\quad y-b\quad\text{or}\quad a_1 x+a_2 y-b.$$

Now

$x-b\,|\,F_2(x, y)$ implies $a_0+a_1 b=a_0+a_1 b^{-1}=0$; $|a_0|=|a_1|$, $|a_2|=|a_3|$;

$y-b\,|\,F_2(x, y)$ implies $a_0+a_2 b=a_0+a_2 b^{-1}=0$; $|a_0|=|a_2|$, $|a_1|=|a_3|$;

$a_1 x+a_2 y-b\,|\,F_2(x, y)$ implies $b=0$, $|a_0|=|a_3|$, $|a_1|=|a_2|$,

contrary to the assumption.

Moreover, $F_2\nmid F_1$ since the highest homogeneous part of $F_2(x, y)$, which is $a_0 xy(a_1 x+a_2 y)$, does not divide the highest homogeneous part of $F_1(x, y)$, which is either $(a_1 x+a_2 y)^{-\gamma_3}$ or $-(-a_3)^{-\gamma_3}x^{\gamma_1}y^{\gamma_2}$ or finally the difference of these two. Therefore, $(F_1, F_2)=1$ and by Lemma 4 of [4]

$$\text{(1)}\qquad \operatorname{card}\{\langle\xi, \eta\rangle\in\boldsymbol{C}^2\colon F_1(\xi, \eta)=F_2(\xi, \eta)=0\}\leqslant|R|,$$

where R is the resultant of F_1 and F_2 with respect to y. Now, by Lemma 5 of [4]

$$\text{(2)}\qquad |R|\leqslant 4\max\{\gamma_1, \gamma_2, \gamma_3\}\leqslant 4\sqrt{3n_3}.$$

If $f(x)$ is a reciprocal factor of $q(x)$ and $f(\zeta)=0$ then clearly

$$a_0+a_1\zeta^{n_1}+a_2\zeta^{n_2}=-a_3\zeta^{n_3},$$

hence

$$(a_0+a_1\zeta^{n_1}+a_2\zeta^{n_2})^{-\gamma_3}=(-a_3\zeta^{n_3})^{-\gamma_3},\quad\text{i.e.}\quad F_1(\zeta^{n_1}, \zeta^{n_2})=0.$$

Also $\zeta\neq 0$,

$$a_0+a_1\zeta^{-n_1}+a_2\zeta^{-n_2}=-a_3\zeta^{-n_3},$$

hence

$$(a_0+a_1\zeta^{n_1}+a_2\zeta^{n_2})(a_0+a_1\zeta^{-n_1}+a_2\zeta^{-n_2})=a_3^2$$

thus

$$F_2(\zeta^{n_1}, \zeta^{n_2})=0.$$

If f in addition is squarefree, we have

$$\text{(3)}\qquad |f|\leqslant\sum_{\substack{\xi,\eta\\ F_1(\xi,\eta)=F_2(\xi,\eta)=0,\ \xi\eta\neq 0}}\operatorname{card}\{\zeta\in\boldsymbol{C}\colon \zeta^{n_1}=\xi,\ \zeta^{n_2}=\eta,\ \zeta^{n_3}=a_3^{-1}(-a_0-a_1\xi-a_2\eta)\}.$$

If $\zeta^{n_1} = \xi$, $\zeta^{n_2} = \eta$, $\zeta^{n_3} = a_3^{-1}(-a_0 - a_1\xi - a_2\eta)$ and $n_1 p + n_2 q + n_3 r = (n_1, n_2, n_3) = 1$ for suitable integers p, q, r, then

$$\zeta = \xi^p \eta^q a_3^{-r}(-a_0 - a_1\xi - a_2\eta)^r,$$

hence

$$\operatorname{card}\{\zeta \in C\colon \zeta^{n_1} = \xi, \zeta^{n_2} = \eta, \zeta^{n_3} = a_3^{-1}(-a_0 - a_1\xi - a_2\eta)\} \leqslant 1. \tag{4}$$

The lemma follows from (1), (2), (3) and (4).

LEMMA 3. *Let $\alpha_1, \alpha_2, \beta_0, \beta_1, \beta_2 \in \boldsymbol{Q}$, $l_1, l_2 \in \boldsymbol{C}\setminus\{0\}$, $e^{l_j} = \alpha_j$ $(1 \leqslant j \leqslant 2)$, $H(\alpha)$ be the usual height of α, $\Lambda = \beta_0 + \beta_1 l_1 + \beta_2 l_2$.*

Let V_1, V_2, W, E be positive real numbers, satisfying

$$1 \leqslant V_1 \leqslant V_2,$$

$$V_j \geqslant \max\{\log H(\alpha_j); |l_j|\} \quad (1 \leqslant j \leqslant 2),$$

$$W \geqslant \max_{1 \leqslant j \leqslant 2} \log H(\beta_j),$$

and

$$1 < E \leqslant \min\{e^{V_1}; \min_{1 \leqslant j \leqslant 2} 4V_j/|l_j|\}.$$

If $|\Lambda| \neq 0$ then

$$|\Lambda| > \exp\left(-CV_1V_2(W + \log EV_2)(\log EV_1)(\log E)^{-3}\right) \tag{5}$$

with

$$C \leqslant 2^{71}. \tag{6}$$

Proof. This is the special case $n = 2$, $D = 1$ of the theorem of Waldschmidt [9]. Unlike him we denote the principal value of logarithms by log (all logarithms are real).

LEMMA 4. *If $q(x)$ is not reciprocal and $Kq(x)$ has an irreducible reciprocal factor, then either there is a linear relation*

$$\gamma_1 n_1 + \gamma_2 n_2 + \gamma_3 n_3 = 0 \tag{7}$$

with $\gamma_i \in \boldsymbol{Z}$ and

$$0 < \max_{1 \leqslant i \leqslant 3} |\gamma_i| \leqslant \max_{0 \leqslant j \leqslant 3} \frac{\log a_j^2}{\log 2}, \tag{8}$$

or

$$\frac{n_3}{(n_1, n_2, n_3)} < e^{200}(\log \|q\|)^5. \tag{9}$$

Proof. Let

$$d = (n_1, n_2, n_3), \quad n_j' = n_j/d \quad (j = 1, 2, 3).$$

If

$$K\left(a_0 + \sum_{j=1}^{3} a_j x^{n_j'}\right) \overset{\text{can}}{=} \text{const} \prod_{\varrho=1}^{r} f_\varrho(x)^{e_\varrho},$$

where none of the polynomials f_ϱ is reciprocal, then for each $\varrho \leqslant r$ we have

$$\left(f_\varrho, x^{|f_\varrho|} f_\varrho(x^{-1})\right) = 1$$

and thus

$$\left(f_\varrho(x^d), x^{d|f_\varrho|} f_\varrho(x^{-d})\right) = 1.$$

Hence

$$Kq(x) = \text{const} \prod_{\varrho=1}^{r} f_\varrho(x^d)^{e_\varrho}$$

has no irreducible reciprocal factor, contrary to the assumption. Therefore, we can assume without loss of generality that $(n_1, n_2, n_3) = 1$. If the reciprocal factor in question, say $f(x)$, is primitive with the leading coefficient different from ± 1, then in virtue of Lemma 13 of [6] there is a linear relation (7) with the coefficients γ_i satisfying (8). If the leading coefficient of f is ± 1, we use Lemmata 1 and 2 and infer that

$$|f| \leqslant 4\sqrt{3n_3}. \tag{10}$$

In virtue of Dobrowolski's theorem (see [2], p. 329) f, which is non-cyclotomic and has the leading coefficient ± 1, satisfies

$$\prod_{f(\zeta)=0} \max(1, |\zeta|) > 1 + \frac{1}{1200}\left(\frac{\log\log 4\sqrt{3n_3}}{\log 4\sqrt{3n_3}}\right)^3. \tag{11}$$

Hence there exists a zero ζ of f such that

$$\log|\zeta| > \frac{1}{1201 \cdot 4\sqrt{3n_3}}\left(\frac{\log\log 4\sqrt{3n_3}}{\log 4\sqrt{3n_3}}\right)^3 > \frac{1}{n_3^{3/5}} \tag{12}$$

for $n_3 > \exp 200$.

We have however

$$a_0 + \sum_{j=1}^{3} a_j \zeta^{n_j} = a_0 + \sum_{j=1}^{3} a_j \zeta^{-n_j} = 0. \tag{13}$$

It follows that

$$|a_0| \leqslant (|a_1|+|a_2|+|a_3|)\,|\zeta|^{-n_1},$$
$$|a_3| \leqslant (|a_0|+|a_1|+|a_2|)\,|\zeta|^{n_2-n_3},$$

hence in view of (12)

$$|a_0\zeta^{-n_3}|+|a_1\zeta^{n_1-n_3}| \leqslant \left(\frac{|a_1|(|a_1|+|a_2|+|a_3|)}{|a_0|}+|a_0|\right)|\zeta|^{-n_3}$$
$$\leqslant (|a_1|^2+|a_1a_2|+|a_1a_3|+|a_0|^2)\exp(-n_3^{2/5}),$$
$$|a_2\zeta^{-n_2}|+|a_3\zeta^{-n_3}| \leqslant \left(\frac{|a_2|(|a_0|+|a_1|+|a_2|)}{|a_3|}+|a_3|\right)|\zeta|^{-n_3}$$
$$\leqslant (|a_0a_2|+|a_1a_2|+|a_2|^2+|a_3|^2)\exp(-n_3^{2/5}).$$

Now, from (13)

$$|\zeta|^{n_2-n_3} = \left|\frac{a_3}{a_2}\right|+O\left(\frac{|a_0|^2+|a_1|^2+|a_1a_2|+|a_1a_3|}{|a_2|}\right)\exp(-n_3^{2/5}),$$
$$|\zeta|^{-n_1} = \left|\frac{a_0}{a_1}\right|+O\left(\frac{|a_0a_2|+|a_1a_2|+|a_2|^2+|a_3|^2}{|a_1|}\right)\exp(-n_3^{2/5}),$$

where the constant in the O symbol is 1 (so in the sequel). It follows from the inequality

$$\bigl|\log|z_1|-\log|z_2|\bigr| \leqslant \frac{|z_1-z_2|}{\min\{|z_1|,\,|z_2|\}}$$

that

$$(n_2-n_3)\log|\zeta| = \log\left|\frac{a_3}{a_2}\right|+O(|a_0|^2+|a_1|^2+|a_1a_2|+|a_1a_3|)\,\|q\|\exp(-n_3^{2/5}),$$
$$-n_1\log|\zeta| = \log\left|\frac{a_0}{a_1}\right|+O(|a_0a_2|+|a_1a_2|+|a_2|^2+|a_3|^2)\,\|q\|\exp(-n_3^{2/5}),$$

whence

$$(14)\qquad \left|n_1\log\left|\frac{a_3}{a_2}\right|+(n_2-n_3)\log\left|\frac{a_0}{a_1}\right|\right| = |\Lambda| \leqslant \frac{5}{2}\|q\|^2 n_3\exp(-n_3^{2/5}).$$

The case $|a_3/a_2| = |a_0/a_1| = 1$ is excluded by Lemma 1. Thus $\max\limits_{0\leqslant i\leqslant 3}|a_i| \geqslant 2$, $\|q\| \geqslant 7$ and, what is more important, $|\Lambda|$ can be estimated from below. If

$$\left|\frac{a_3}{a_2}\right| = 1,\quad \left|\frac{a_0}{a_1}\right| \neq 1 \quad\text{or}\quad \left|\frac{a_3}{a_2}\right| \neq 1,\quad \left|\frac{a_0}{a_1}\right| = 1,$$

we have

$$(15)\qquad |\Lambda| \geqslant \|q\|^{-1/2}.$$

If $|a_3/a_2| \neq 1$ and $|a_0/a_1| \neq 1$, we apply Lemma 3 taking there

$$\alpha_1 = \left|\frac{a_3}{a_2}\right|,\quad \alpha_2 = \left|\frac{a_0}{a_1}\right|,\quad \beta_0 = 0,\quad \beta_1 = n_1,\quad \beta_2 = n_2-n_3,$$
$$l_1 = \log\left|\frac{a_3}{a_2}\right|,\quad l_2 = \log\left|\frac{a_0}{a_1}\right|,$$
$$V_1 = V_2 = \log\|q\|,\quad W = \log n_3,\quad E = 7.$$

We get $\Lambda = 0$ or

$$(16)\qquad |\Lambda| > \exp\bigl(-2^{69}(\log\|q\|)^2(\log n_3+\log\log\|q\|+\log 7)$$
$$\times(\log\log\|q\|+\log 7)\bigr),$$

which is clearly weaker than (15). Combining (14) and (16), we obtain

$$\log\frac{5}{2}\|q\|^2+\log n_3-n_3^{2/5} > -2^{69}(\log\|q\|)^2(\log n_3+\log\log\|q\|+\log 7)$$
$$\times(\log\log\|q\|+\log 7),$$

whence by a tedious computation follows (9).

If, on the other hand, $\Lambda = 0$, we have

$$\left|\frac{a_3}{a_2}\right|^{n_1} = \left|\frac{a_0}{a_1}\right|^{n_2-n_3}.$$

Since $|a_3/a_2| = |a_0/a_1| = 1$ is excluded, there exists a prime p which occurs in the factorization of either a_3/a_2 or a_0/a_1 with a non-zero exponent. Thus we get

$$(17)\qquad n_1\operatorname{ord}_p(a_3/a_2) = (n_3-n_2)\operatorname{ord}_p(a_0/a_1)$$

and since

$$\operatorname{ord}_p a_i \leqslant \max_{0\leqslant j\leqslant 3}\frac{\log|a_j|}{\log 2}\qquad (0\leqslant i\leqslant 3),$$

(17) represents a relation (7) with the condition (8).

Remark 2. By applying the arguments used in the proof of Theorem 4 in [6] and Lemma 13 in [4] and taking into account the estimate for $e(\alpha,\Omega)$ implied by Dobrowolski's theorem, one can show that the conditions (7) and (8) imply (9), moreover we have under the assumption of the lemma

$$\frac{n_3}{(n_1,\,n_2,\,n_3)} < C(\varepsilon)(\log\|q\|)^{4+\varepsilon}$$

for every $\varepsilon > 0$ and a suitable constant $C(\varepsilon)$.

Lemma 5. *If $q(x)$ is not reciprocal and either $Kq(x)$ has no irreducible reciprocal factors, or the conditions* (7) *and* (8) *hold, then we have the alternative* (i)–(iv).

Proof is identical with the proof of Theorem 4 in [6], except the last paragraph which is not needed.

Proof of the theorem. If $Kq(x)$ has no irreducible reciprocal factor the theorem follows from Lemma 5. If $Kq(x)$ has an irreducible reciprocal factor $f(x)$, then in virtue of Lemma 4 we have either (7) and (8) or (9). In the former case the theorem follows again from Lemma 5. In the latter case we write

$$q(x) = F(x^{(n_1,n_2,n_3)}),$$

where

$$F(x) = a_0 + \sum_{j=1}^{3} a_j x^{n_j/(n_1,n_2,n_3)}.$$

We now apply to $F(x)$ Theorem 1 of [4] and infer the existence of integers v and u such that

$$0 < v < \exp(10|F|\log 2|F|\log\|F\|)^2, \quad (n_1, n_2, n_3) = uv,$$

and

$$KF(x^v) \overset{\mathrm{can}}{=} \mathrm{const}\prod_{\sigma=1}^{s} F_\sigma(x)^{e_\sigma}$$

implies

$$KF(x^n) \overset{\mathrm{can}}{=} \mathrm{const}\prod_{\sigma=1}^{s} F_\sigma(x^u)^{e_\sigma}.$$

Taking

$$v_j = vn_j/(n_1, n_2, n_3), \quad v = u$$

we find (iv), since

$$\begin{aligned} v_3 &= v\frac{n_3}{(n_1, n_2, n_3)} \\ &\leqslant e^{200}(\log\|q\|)^5\exp\big(10e^{200}\log\|q\|(201+5\log\log\|q\|)\log\|q\|\big)^2 \\ &< \exp_2(12\cdot 2^{\|q\|}\log\|q\|), \end{aligned}$$

where the last inequality follows from $\|q\| \geqslant 7$. This completes the proof.

Remark 3. Theorem 4 in [6] includes an estimate for the number of irreducible factors of $Kq(x)$, namely

$$(18) \qquad \Omega(Kq(x)) = \sum_{\sigma=1}^{s} e_\sigma \leqslant \left(\frac{1}{2\log\theta_0} + \frac{1}{2\log 2}\right)\log\|q\|, \qquad \theta_0^3 - \theta_0 - 1 = 0$$

proved under the assumptions of that theorem, more stringent than these of the present Theorem 1. The above estimate is valid without any assumption about $q(x)$ for the number of irreducible factors of $Kq(x)$ that are either non-reciprocal or primitive with the leading coefficient different from ±1. In fact, using the theorems of Landau and Smyth more carefully than in [6], one can eliminate the summand $1/(2\log 2)$ in (18). However to estimate the number of irreducible factors of $Kq(x)$ that are reciprocal and monic is more difficult; Theorem 1 furnishes an exceedingly large bound $\exp_2(12\cdot 2^{\|q\|}\log\|q\|)$. Using Remark 2 and Theorem 1 of [6] one can get

$$\Omega(Kq(x)) \leqslant C_1(\varepsilon)(\log\|q\|)^{4+\varepsilon}$$

for every $\varepsilon > 0$ and a suitable $C_1(\varepsilon)$, but also this estimate does not seem sharp.

Lemma 6. *If $q(x)$ is reciprocal and primitive, $f(x)$ is primitive with the leading coefficient l and $f(x)|q(x)$, then for every prime $p|a_0$*

$$(19) \qquad n_1 \operatorname{ord}_p l \equiv 0 \bmod \operatorname{ord}_p a_0.$$

Moreover, we have for every prime p

$$(20) \qquad |Kf|\operatorname{ord}_p a_0 \geqslant n_1 \operatorname{ord}_p l + n_1 \operatorname{ord}_p f(0).$$

Proof. Both sides of the formulae (19) and (20) behave as additive functions of f, hence it is enough to show them for all irreducible f. For f cyclotomic the formulae are true since $l = 1$, $f(0) = \pm 1$, therefore we assume that f is irreducible and $Kf = f$. Let ζ be a zero of such an f and let

$$(21) \qquad (\zeta) = \frac{\mathfrak{m}}{\mathfrak{n}},$$

where $\mathfrak{m}$, $\mathfrak{n}$ are ideals of $\boldsymbol{Q}(\zeta)$ and $(\mathfrak{m}, \mathfrak{n}) = 1$. We have

$$f(x) = lN(x-\zeta),$$

where N denotes the norm from $\boldsymbol{Q}(x, \zeta)$ to $\boldsymbol{Q}(x)$ or from $\boldsymbol{Q}(\zeta)$ to $\boldsymbol{Q}$, hence by Gauss's lemma

$$(22) \qquad 1 = |l|(N\mathfrak{n})^{-1}, \quad |l| = N\mathfrak{n}, \quad |f(0)| = N\mathfrak{m}.$$

On the other hand, for every prime ideal $\mathfrak{p}|\mathfrak{n}$ we have

$$\operatorname{ord}_\mathfrak{p} a_3\zeta^{n_3} < \operatorname{ord}_\mathfrak{p} a_0, \quad \text{because} \quad a_3 = \pm a_0,$$

$$\operatorname{ord}_\mathfrak{p} a_2\zeta^{n_2} < \operatorname{ord}_\mathfrak{p} a_1\zeta^{n_1}, \quad \text{because} \quad a_2 = \pm a_1,\ n_2 > n_1,$$

hence

$$q(\zeta) = a_0 + \sum_{j=1}^{3} a_j \zeta^{n_j} = 0$$

implies

$$\operatorname{ord}_{\mathfrak{p}} a_3 \zeta^{n_3} = \operatorname{ord}_{\mathfrak{p}} a_2 \zeta^{n_2}$$

and thus

$$\operatorname{ord}_{\mathfrak{p}} a_3 - \operatorname{ord}_{\mathfrak{p}} a_2 = (n_3 - n_2) \operatorname{ord}_{\mathfrak{p}} \mathfrak{n} > 0. \tag{23}$$

Since $(a_2, a_3) = 1$, $n_3 - n_2 = n_1$, we get

$$\operatorname{ord}_{\mathfrak{p}} a_2 = 0, \quad n_1 \operatorname{ord}_{\mathfrak{p}} \mathfrak{n} \equiv 0 \bmod \operatorname{ord}_p a_0.$$

Hence, by (22)

$$n_1 \operatorname{ord}_p l = \sum_{\mathfrak{p}|p} n_1 \operatorname{ord}_{\mathfrak{p}} \mathfrak{n} \cdot \operatorname{ord}_p N\mathfrak{p} \equiv 0 \bmod \operatorname{ord}_p a_0$$

which proves (19). Since by (23)

$$\operatorname{ord}_{\mathfrak{p}} a_0 = n_1 \operatorname{ord}_{\mathfrak{p}} \mathfrak{n}$$

for every prime ideal $\mathfrak{p}|\mathfrak{n}$, we get

$$\mathfrak{n}^{n_1} | a_0.$$

Since $x^{|f|} f(1/x) | q(x)$, the role of $\mathfrak{m}$ and $\mathfrak{n}$ is symmetrical, hence also

$$\mathfrak{m}^{n_1} | a_0.$$

Since $(\mathfrak{m}, \mathfrak{n}) = 1$, the last two divisibilities give

$$(\mathfrak{m}\mathfrak{n})^{n_1} | a_0$$

and on taking norms we get by (22)

$$\big(f(0)\, l\big)^{2n_1} | a_0^{|f|},$$

which implies (20).

LEMMA 7. *If $q(x)$ is reciprocal and $|a_0| \geqslant |a_1|$, then all zeros of $q(x)$ lie on the unit circle. Moreover, if f is primitive with the leading coefficient l and $f(x)|q(x)$, then*

$$|Kf| \log(|a_0|/2) \leqslant n_3 \log |l|.$$

Proof. If $|a_0| \geqslant |a_1|$ then also $|a_0| + |a_3| \geqslant |a_1| + |a_2|$ and in virtue of Lemma 14 of [6] all zeros of $q(x)$ lie on the unit circle. In proving the second part of the lemma we may assume without loss of generality that f is irreducible, non cyclotomic, $f(\zeta) = 0$ and (21) holds. It follows from $q(\zeta) = 0$ that

$$a_0(1 + \varepsilon\zeta^{n_3}) = -a_1(\zeta^{n_1} + \varepsilon\zeta^{n_2}),$$

where

$$\varepsilon = a_3/a_0 = a_2/a_1 = \pm 1.$$

Hence

$$a_0(1 + \varepsilon\zeta^{n_3})\mathfrak{n}^{n_3} = -a_1(\zeta^{n_1} + \varepsilon\zeta^{n_1})\mathfrak{n}^{n_3},$$

$$a_0 | a_1(\zeta^{n_1} + \varepsilon\zeta^{n_2})\mathfrak{n}^{n_3}$$

and since $(a_0, a_1) = 1$ we have

$$a_0 | (\zeta^{n_1} + \varepsilon\zeta^{n_2})\mathfrak{n}^{n_3}.$$

On taking norms we get by (22)

$$a_0^{|f|} | l^{n_3} N(\zeta^{n_1} + \varepsilon\zeta^{n_2}).$$

Since f is non-cyclotomic, ζ is not a root of unity, hence $\zeta^{n_1} + \varepsilon\zeta^{n_2} \neq 0$ and

$$N(\zeta^{n_1} + \varepsilon\zeta^{n_2}) \neq 0.$$

On the other hand, since all the conjugates of ζ lie on the unit circle,

$$|N(\zeta^{n_1} + \varepsilon\zeta^{n_2})| \leqslant 2^{|f|}.$$

The last three formulae imply

$$|a_0|^{|f|} \leqslant |l|^{n_3} 2^{|f|},$$

which gives the second part of the lemma.

Proof of Theorem 2. Let

$$q(x) = f_0 \prod_{j=1}^{h} f_j^{\beta_j},$$

where f_j are primitive irreducible polynomials with the leading coefficients $l_j > 1$ $(j = 1, 2, \ldots, h)$. We have for each prime $p_i | a_0$

$$\alpha_i \geqslant \sum_{j=1}^{h} \beta_j \operatorname{ord}_{p_i} l_j,$$

hence

$$(\alpha_i, n_1) \geqslant \sum_{j=1}^{h} \beta_j \frac{(\alpha_i, n_1) \operatorname{ord}_{p_i} l_j}{\alpha_i}$$

and

$$\sum_{i=1}^{k} (\alpha_i, n_1) \geqslant \sum_{j=1}^{h} \beta_j \sum_{i=1}^{k} \frac{(\alpha_i, n_1) \operatorname{ord}_{p_i} l_j}{\alpha_i}.$$

By Lemma 6 each inner sum on the right-hand side is an integer. It is also positive since $l_j > 1$. Hence

$$\sum_{i=1}^{k} (\alpha_i, n_1) \geqslant \sum_{j=1}^{k} \beta_j.$$

Proof of Corollary 1. If $|a_0| \geqslant |a_1|$ then by Lemma 7 all zeros of $q(x)$ lie on the unit circle. By the theorem of Kronecker those among them that are algebraic integers are roots of unity, hence $Kq(x)$ has no monic factor.

Proof of Corollary 2. If $k = 1$ and $(\alpha_1, n_1) = 1$ then by Corollary 1 the number of irreducible factors of $Kq(x)$, counted with multiplicities, does not exceed 1.

Proof of Theorem 3. Assume that $Kq(x) = f_1 f_2$, where f_1, f_2 are non-constant polynomials with the leading coefficients l_1, l_2, respectively. We have

$$|a_0| = |a_3| = |l_1 l_2| \tag{24}$$

and by Corollary 1

$$|l_i| > 1 \quad (i = 1, 2). \tag{25}$$

In view of symmetry we may assume

$$1 < l_1 \leqslant \sqrt{|a_0|}.$$

By Lemma 6

$$n_1 \operatorname{ord}_p l_1 \equiv 0 \bmod \operatorname{ord}_p a_0$$

for every prime $p | a_0$, hence $l_1 \in S$.

By Lemma 7 every zero of f lies on the unit circle, hence

$$f_i(0) = \pm l_i \quad (i = 1, 2).$$

Again, by Lemma 6

$$|Kf_i| \geqslant 2n_1 \max_{p|a_0} \frac{\operatorname{ord}_p l_i}{\operatorname{ord}_p a_0} \quad (i = 1, 2).$$

Thus

$$\frac{n_3}{2n_1} \geqslant \frac{|Kf_1| + |Kf_2|}{2n_1} \geqslant \sum_{i=1}^{2} \max_{p|a_0} \frac{\operatorname{ord}_p l_i}{\operatorname{ord}_p a_0}. \tag{26}$$

On the other hand, by Lemma 7

$$|Kf_i| \log(|a_0|/2) \leqslant n_3 \log |l_i| \quad (i = 1, 2).$$

By (24) and (25) we have $|a_0| \geqslant 2$, hence

$$n_3 \log |l_i| \geqslant |Kf_i| \log \frac{|a_0|}{2} \geqslant 2n_1 \log \frac{|a_0|}{2} \max_{p|a_0} \frac{\operatorname{ord}_p l_i}{\operatorname{ord}_p a_0}$$

and

$$\frac{n_3}{2n_1} \geqslant \frac{\log(|a_0|/2)}{\log |l_i|} \max_{p|a_0} \frac{\operatorname{ord}_p l_i}{\operatorname{ord}_p a_0} \quad (i = 1, 2).$$

Thus by (24) and (26)

$$\frac{n_3}{2n_1} \geqslant \max \Big\{ \max_{p|a_0} \frac{\operatorname{ord}_p l_1}{\operatorname{ord}_p a_0} + \max_{p|a_0} \frac{\operatorname{ord}_p (a_0/l_1)}{\operatorname{ord}_p a_0}, \\ \frac{\log(|a_0|/2)}{\log l_1} \max_{p|a_0} \frac{\operatorname{ord}_p l_1}{\operatorname{ord}_p a_0}, \frac{\log(|a_0|/2)}{\log(|a_0|/l_1)} \max_{p|a_0} \frac{\operatorname{ord}_p (a_0/l_1)}{\operatorname{ord}_p a_0} \Big\}.$$

Since $l_1 \in S$ the theorem follows.

Proof of Corollary 3. If a_0 is squarefree, we have for every $l \in S$

$$\max_{p|a_0} \frac{\operatorname{ord}_p l}{\operatorname{ord}_p a_0} = \max_{p|a_0} \frac{\operatorname{ord}_p (a_0/l)}{\operatorname{ord}_p a_0} = 1 \quad \text{and} \quad \log l \leqslant \log(|a_0|/l)$$

hence the simplification of the theorem.

Note concerning the paper [4]

1. The proof given on p. 133 that (12) has at most k linearly independent solutions should be modified as follows.

"Let r be the rank of the matrix $[c_{pq}]$ and assume that the vectors $[c_{1s}, \ldots, c_{p_0 s}]$ $(1 \leqslant s \leqslant r)$ are linearly independent, while

$$c_{pq} = \sum_{s=1}^{r} \gamma_{qs} c_{ps}$$

for all $p \leqslant p_0$, $q \leqslant k$ and suitable $\gamma_{qs} \in \boldsymbol{Q}$.

If we had $k+1$ linearly independent solutions $a_1, \ldots, a_{k+1}$ of (12) then taking as $\xi_1, \ldots, \xi_{k+1}$ real numbers linearly independent over $\boldsymbol{Q}$ we should find the set of reals $\sum_{m=1}^{k+1} a_{mi} \xi_m$ $(0 \leqslant i \leqslant l)$, where all the differences would span over $\boldsymbol{Q}$ a space of dimension at least $r+1$, while the differences occurring only once

$$\sum_{m=1}^{k+1} (a_{mj_p} - a_{mi_p}) \xi_m = \sum_{m=1}^{k+1} \xi_m \Big(\sum_{q=1}^{k} c_{pq} a_{m,l+q} \Big) \\ = \sum_{s=1}^{r} c_{ps} \Big(\sum_{q=1}^{k} \gamma_{qs} \sum_{m=1}^{k+1} a_{m,l+q} \xi_m \Big)$$

would span a space of dimension at most r, contrary to the theorem of Straus [11]".

The same modification should be made in the proof of Lemma 2 in [5]. The proof of the same assertion given in the remark on p. 134 of [4] is correct and rather simpler than the above proof.

2. On p. 134 of [4] the estimate for $h(\Lambda')$ is derived incorrectly from Hadamard's inequality. The correct application of this inequality gives

$$h(\Lambda') \leqslant (2+\max\{kc^2, 4\})^{(l+\varrho)/2},$$

hence

$$h(\Lambda') \leqslant (2k+k\max\{c^2, 2\})^{(l+\varrho)/2},$$

unless $k = 1$, $c = 1$. In that case the last inequality follows from inequality (99) in [6]. Thus the estimate for $h(\gamma)$ on p. 134 and in the last line of Lemma 7 in [4] should read

$$h(\gamma) \leqslant k^{k-1}(k\max\{c^2, 2\}+2k)^{(l+1)(k-1)/2},$$

that is just what is used to estimate $h(\gamma)$ on p. 127.

3. On p. 152 of [4] in Lemma 13 the assumption $F(x^{n_1}, x^{n_2}) \neq 0$ is lacking. Moreover, the argument below formula (75) needs an amplification. It assumes silently that every zero $\xi \neq 0$ of $\left(\frac{JF}{KF}\right)(x^{n_1}, x^{n_2})$ is a zero of $\frac{JF(x^{n_1}, x^{n_2})}{KF(x^{n_1}, x^{n_2})}$, which is true but not obvious. When one refers to the definition of KF given on p. 123 one has to show that for an irreducible F the divisibility $F(x_1, x_2)|J(x_1^{\delta_1}x_2^{\delta_2}-1)$ implies $KF(x^{n_1}, x^{n_2}) = \text{const}$. This is obvious if $n_1\delta_1+n_2\delta_2 \neq 0$, but if $n_1\delta_1+n_2\delta_2 = 0$ one needs the fact implied by Lemma 11 of [6] that

$$F(x_1, x_2) = \text{const}\, J\Phi(x_1^{\delta_1/(\delta_1,\delta_2)} x_2^{\delta_2/(\delta_1,\delta_2)})$$

for a polynomial $\Phi|z^{(\delta_1,\delta_2)}-1$. If $\delta_1 n_1+\delta_2 n_2 = 0$ we get

$$F(x^{n_1}, x^{n_2}) = \text{const}.$$

References

[1] J. W. S. Cassels, *An introduction to Diophantine approximation*, Cambridge 1957.

[2] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. 34 (1979), pp. 391–401.

[3] M. Fried and A. Schinzel, *Reducibility of quadrinomials*, ibid. 21 (1972), pp. 153–171.

[4] A. Schinzel, *Reducibility of lacunary polynomials I*, ibid. 16 (1969), pp. 123–159.

[5] — *Reducibility of lacunary polynomials*, Proc. Symposia Pure Math. 20 (1971), pp. 135–149.

[6] — *Reducibility of lacunary polynomials III*, Acta Arith. 34 (1978), pp. 227–266.

[7] — *Reducibility of lacunary polynomials, V*, ibid. 43 (1984), pp. 424–440.

[8] A. Schinzel and J. Wójcik, *A note on the paper "Reducibility of lacunary polynomials I"*, ibid. 19 (1971), pp. 195–201.

[9] M. Waldschmidt, *A lower bound for linear forms in logarithms*, ibid. 37 (1980), pp. 257–283.

Corrections to [4], [6] and [7]

[4], p. 152, formula (75), for $T_1 = L(x_1, x_2)V^{-1}$, $U_1 = L(x_1, x_2)V^{-1}$
read $T_1 = LF(x_1, x_2)V^{-1}$, $U_1 = LF(x_1^{-1}, x_2^{-1})V^{-1}$.
p. 153, formula (76) before "with" insert "$=0$"
lines 9–10 for R_{ij} read R_i, for S_{ij} read S_i, for x_j read x_1,
line 13 for S_{ij} read S_i, for i, j read i;
[6]. p. 229 line 14 for $\Omega(q(x))$ read $\Omega(Kq(x))$,
p. 261 line 10 for (86) read (85);
[7], p. 435 line 9 for $[a_0, \ldots, a_{n-1}]$ read $[a_0, \ldots, a_{n-1}]$ not in $\Omega(p)$ for any p.

Received on 21.6.1985 (1521)