Доказательство теоремы. Рассмотрим точки $tpO_{p^2}$ $(t = 1, 2, \ldots \ldots, (p-1)/2)$. На основании следствия 5

$$u_{tp}/w_{tp} = \pm 2 \prod_{j=1}^{(p-1)/2} (a_j^p)^{\{t_j/p\}p} = \pm 2A_t^p,$$

$$v_{tp}/u_{tp}w_{tp} = \pm \prod_{j=1}^{(p-1)/2} (b_j^p)^{\{t_j/p\}p} = \pm B_t^p$$

$(t = 1, 2, \ldots, (p-1)/2)$.

В силу же следствия 2

$$\frac{2u_{sp}w_{sp}v_{rp}}{w_{p(s+r)}w_{p(s-r)}} = \frac{u_{p(s+r)}}{w_{p(s+r)}} + \frac{u_{p(s-r)}}{w_{p(s-r)}},$$

$$\frac{2u_{rp}w_{rp}v_{sp}}{w_{p(s+r)}w_{p(s-r)}} = \frac{u_{p(s-r)}}{w_{p(s-r)}} - \frac{u_{p(s+r)}}{w_{p(s+r)}}$$

$(r, s = 1, 2, \ldots, (p-1)/2, r \neq s)$.

Так как

$$u_{sp}w_{sp}v_{rp}/u_{rp}w_{rp}v_{sp} = (v_{rp}/u_{rp}w_{rp})/(v_{sp}/u_{sp}w_{sp}),$$

то

$$A_{s+r}^p + A_{s-r}^p = C_{s,r}^p, \quad A_{s-r}^p - A_{s+r}^p = D_{s,r}^p,$$

откуда, вводя новые обозначения,

(12) $$z_i^p - t_i^p = 1, \quad z_i^p + t_i^p = r_i^p \quad (i = 1, 2, \ldots, C^2_{(p-1)/2}).$$

Полученные точки кривой (12) должны быть различны, так как в противном случае точка $pO_{p^2}$ имела бы порядок меньший $p$. Далее, так как род кривой $T$ больше 0, то координаты точек $ptO_{p^2}$ $(t = 1, 2, \ldots \ldots, (p-1)/2)$ отличны от 0. Теорема доказана.

В заключение считаю своим приятным долгом выразить благодарность И. Р. Шафаревичу за ряд ценных замечаний, касающихся этой работы.

### Литература

[1] В. А. Демьяненко, *О точках конечного порядка эллиптических кривых*, Изв. АН СССР, сер. матем., 31 (6) (1967), стр. 1327–1340.

*Получено 20. 5. 1970* (90)

ACTA ARITHMETICA
XIX (1971)

# A note on the paper "Reducibility of lacunary polynomials I"

by

A. Schinzel and J. Wójcik (Warszawa)

In the paper [1] mentioned in the title the first writer has left a gap in the proof of Lemma 1. The aim of this note is to fill this gap by proving a property of normal number fields which may be of independent interest.

Let $\Omega$ be a number field of degree $|\Omega|$, $a \in \Omega$, $a \neq 0$. We denote by $\zeta_q$ a primitive $q$th root of unity and set following [1]

$$e(a, \Omega) = \begin{cases} 0 \text{ if } a = \zeta_q \text{ for some } q, \\ \text{maximal } e \text{ such that } a = \zeta_q\beta^e \text{ with suitable } q \text{ and} \\ \hfill \beta \in \Omega, \text{ otherwise.} \end{cases}$$

It is asserted in Lemma 1 of [1] that if $a \neq 0$, $f(a) = 0$, where $f(x) = \sum_{i=0}^{m} a_i x^i$ is a polynomial with integral coefficients and $\|f\| = \sum_{i=0}^{m} a_i^2$, then

(1) $$e(a, \Omega) \leqslant \tfrac{5}{2}|\Omega| \log\|f\|.$$

The proof for $a$ not being an integer is correct. The proof for $a$ being an integer is based on the following refinement of a result of Cassels ([1], p. 159).

If an algebraic integer $\beta$ of degree $n$ is not conjugate to $\beta^{-1}$ then

(2) $$\overline{|\beta|} > 1 + \frac{1}{5n-1},$$

where $\overline{|\beta|}$ is the maximal absolute value of the conjugates of $\beta$.

If $a$ is an integer and $a = \zeta_q\beta^e$ then $\beta$ is also an integer $(e > 0)$. However it does not follow that if $a$ is not conjugate to $a^{-1}$ then $\beta$ is not conjugate to $\beta^{-1}$. The example

$$a = -1-\sqrt{2} = \zeta_4\left(\zeta_8\sqrt{1+\sqrt{2}}\right)^2 = \zeta_4\beta^2$$

shows that even for all $i$ $\zeta_q^i\beta$ may be conjugate to $\zeta_q^{-i}\beta^{-1}$.

Therefore the inequality (2) does not follow in an obvious way (which is assumed although not asserted in [1]) from the assumption of the lemma in question and we are not able to decide whether it follows at all. However the inequality (1) is a simple consequence (see Corollary below) of the following

THEOREM. *If $a = \zeta_q\beta^c$ is not conjugate to $a^{-1}$, $\beta \in K(a)$ where $K$ is a normal field of degree $|K|$ and $(|K|, q, c) = 1$ then for some $i$, $\zeta_q^i\beta$ is not conjugate to $\zeta_q^{-i}\beta^{-1}$.*

LEMMA 1. *Let $p$ be a prime not dividing $|K|$, $\zeta_q \in K(\alpha)$, $\beta \in K(\alpha)$. If $\sigma_1, \sigma_2$ are two automorphisms of the normal closure of $K(\alpha)$, $\sigma_1(\alpha) = \sigma_2(\alpha)$, $\sigma_1(\zeta_p) = \sigma_2(\zeta_p)$ and $\sigma_1(\beta^p) = \sigma_2(\beta^p)$ then $\sigma_1(\beta) = \sigma_2(\beta)$.*

Proof. Set $\sigma = \sigma_2^{-1}\sigma_1$. Let $a$ be of degree $r$ over $K(\zeta_p)$ and let

$$\beta = a_0 + a_1\alpha + \ldots + a_{r-1}\alpha^{r-1}.$$

If $\sigma(\beta) \neq \beta$ we have $\sigma(\beta) = \zeta_p\beta \neq 0$. Therefore,

$$\sigma(\beta) = \zeta_p a_0 + \zeta_p a_1\alpha + \ldots + \zeta_p a_{r-1}\alpha^{r-1},$$

where at least one coefficient $\zeta_p a_i$, say, is non-zero. On the other hand,

$$\sigma(\beta) = \sigma(a_0) + \sigma(a_1)\alpha + \ldots + \sigma(a_{r-1})\alpha^{r-1}.$$

Since $K$ is normal, $\sigma(a_i) \in K(\zeta_p)$. It follows that

$$\sigma(a_i) = \zeta_p a_i, \qquad \sigma(a_i^p) = a_i^p.$$

$a_i^p$ belongs, therefore, to the subfield $L$, of $K(\zeta_p)$ invariant with respect to $\sigma$. We have also $\zeta_p \in L$, $a_i \notin L$ and by Abel's theorem $a_i$ is of degree $p$ over $L$. Since $L \subset L(a_i) \subset K(\zeta_p)$ it follows $|K(\zeta_p)| \equiv 0 \bmod p$ and $|K| \equiv 0 \bmod p$, contrary to the assumption.

LEMMA 2. *The theorem holds for $q = 2^\nu$.*

Proof. Set $\zeta_q = \zeta$. If $e \not\equiv 0 \bmod 2$ we have for suitable $i$

$$\alpha = \zeta\beta^c = (\zeta^i\beta)^c,$$

hence $\zeta^i\beta$ is not conjugate to $\zeta^{-i}\beta^{-1}$. Assume that $e \equiv 0 \bmod 2$, $|K| \not\equiv 0 \bmod 2$ and that for each $i$ there exists an automorphism $\sigma_i$ of the normal closure of $K(\alpha)$ such that

$$\sigma_i(\zeta^i\beta) = \zeta^{-i}\beta^{-1}.$$

If $\sigma_i(\zeta) = \zeta^{s_i}$ we have

$$\sigma_i^t(\beta) = \zeta^{-i(s_i^t+1)}\beta^{-1} \qquad (t \text{ odd}),$$

$$\sigma_i^t(\alpha) = \begin{cases} \zeta^{s_i^t - ie(s_i^t+1)}\beta^{-c} & \text{for } t \text{ odd}, \\ \zeta^{s_i^t - ie(s_i^t-1)}\beta^{c} & \text{for } t \text{ even}. \end{cases}$$



If $s_i \equiv -1 \bmod q$ then setting $t = 1$ we get $\sigma_i(\alpha) = \alpha^{-1}$, contrary to the assumption. This remark implies the validity of the lemma for $\nu = 1, 2$. Indeed, if $\nu = 1$ then $s_i \equiv -1 \bmod 2$. If $\nu = 2$ then either $s_0 \equiv -1 \bmod 4$ or $s_1 \equiv -1 \bmod 4$. Otherwise $s_0 \equiv s_1 \equiv 1 \bmod 4$,

$$\sigma_0(\alpha) = \zeta\beta^{-e} = \sigma_1(\alpha), \qquad \sigma_0(\beta^2) = \beta^{-2} = \sigma_1(\beta^2)$$

and by Lemma 1

$$\sigma_0(\beta) = \sigma_1(\beta), \qquad \beta^{-1} = -\beta^{-1},$$

which is impossible.

In order to prove the lemma for $\nu \geqslant 3$ we prove first the three assertions:

(i) *if $\nu \geqslant 3$, $2^{\nu-3} \| i-j$ then either $s_i \equiv -1 \bmod 4$ or $s_j \equiv -1 \bmod 4$,*

(ii) *if $\nu \geqslant 4$, $2^{\nu-4} \| i-j$, $s_i \equiv 3 \bmod 8$ then $s_j \equiv -1 \bmod 4$,*

(iii) *if $1 < l < \nu$, $2^{\nu-1-l} \| i-j$, $2^l \| s_i+1$ then $2^l \nmid s_j+1$.*

(i). We have $\sigma_i\sigma_j(\alpha) = \zeta^{s_is_j - je(s_j+1)s_i + ie(s_i+1)}\beta^c$. Since $2(i-j)(s_i+1)\times(s_j+1) \equiv 0 \bmod 2^\nu$ it follows that $\sigma_i\sigma_j(\alpha) = \sigma_j\sigma_i(\alpha)$ and $\sigma_i\sigma_j(\beta^2) = \sigma_j\sigma_i(\beta^2)$, thus by Lemma 1 $\sigma_i\sigma_j(\beta) = \sigma_j\sigma_i(\beta)$. Hence $(i-j)(s_i+1)(s_j+1) \equiv 0 \bmod 2^\nu$, $(s_i+1)(s_j+1) \equiv 0 \bmod 8$ and either $s_i \equiv -1 \bmod 4$ or $s_j \equiv -1 \bmod 4$.

(ii). If $s_i \equiv 3 \bmod 8$ then $2(i-j)(s_i+1)(s_j+1) \equiv 0 \bmod 2^\nu$, $\sigma_i\sigma_j(\alpha) = \sigma_j\sigma_i(\alpha)$, $\sigma_i\sigma_j(\beta^2) = \sigma_j\sigma_i(\beta^2)$ thus by Lemma 1 $\sigma_i\sigma_j(\beta) = \sigma_j\sigma_i(\beta)$, $(i-j)\times(s_i+1)(s_j+1) \equiv 0 \bmod 2^\nu$, $(s_i+1)(s_j+1) \equiv 0 \bmod 16$, $s_j \equiv -1 \bmod 4$.

(iii). Let $s_i \equiv -5^{\alpha_i}$, $s_j \equiv -5^{\alpha_j} \bmod 2^\nu$. If $2^l \| s_i+1$, $2^l \| s_j+1$ then $5^{\alpha_i} \equiv 2^l+1 \bmod 2^{l+1}$, $5^{\alpha_j} \equiv 2^l+1 \bmod 2^{l+1}$, hence $2^{l-2} \| \alpha_i$, $2^{l-2} \| \alpha_j$, $(\alpha_j, 2^{\nu-2}) | \alpha_i$. It follows that the congruence

$$t\alpha_j \equiv \alpha_i \bmod 2^{\nu-2}$$

is soluble. Its root $t$ must be odd since otherwise $l-1 \leqslant \nu-2$ implies $\alpha_i \equiv t\alpha_j \equiv 0 \bmod 2^{l-1}$, which is impossible. Thus we have for an odd $t$

$$s_j^t \equiv s_i \bmod 2^\nu.$$

Since $2(i-j)(s_i+1) \equiv 0 \bmod 2^\nu$ we get $\sigma_j^t(\alpha) = \sigma_i(\alpha)$, $\sigma_j^t(\beta^2) = \sigma_i(\beta^2)$, thus by Lemma 1 $\sigma_j^t(\beta) = \sigma_i(\beta)$, $(i-j)(s_i+1) \equiv 0 \bmod 2^\nu$, which is impossible.

Let $l$ be the greatest integer not exceeding $\nu$ such that $s_i \equiv -1 \bmod 2^l$ for suitable $i$. Since $s_i \not\equiv -1 \bmod 2^\nu$ for all $i$ we have $l < \nu$ and by (i) $l > 1$.

Consider first the case $\nu = 3$. Then $q = 8$, $l = 2$, $s_i \equiv 3 \bmod 8$. Taking in (iii) $l = 2$, $\nu = 3$, $j = i-1$ or $i+1$ we get $s_{i-1} \equiv s_{i+1} \equiv 1 \bmod 4$.

If $s_{i-1} \equiv s_{i+1} \bmod 8$ then $2[(i+1)-(i-1)](s_{i-1}+1) \equiv 4(s_{i-1}+1) \equiv 0 \bmod 8$, hence $\sigma_{i-1}(\alpha) = \sigma_{i+1}(\alpha)$, $\sigma_{i-1}(\beta^2) = \sigma_{i+1}(\beta^2)$ and by Lemma 1 $\sigma_{i-1}(\beta) = \sigma_{i+1}(\beta)$, $2(s_{i-1}+1) \equiv 0 \bmod 8$ which is impossible.

In the remaining cases: $s_{i-1} \equiv 1$, $s_i \equiv 3$, $s_{i+1} \equiv 5 \bmod 8$ and $s_{i-1} \equiv 5$, $s_i \equiv 3$, $s_{i+1} \equiv 1$ we have $s_{i-1}s_is_{i+1} \equiv -1$, $s_i \equiv 3 \bmod 8$.

It follows

$$\sigma_{i-1}\sigma_i\sigma_{i+1}(\alpha) = \zeta^{s_{i-1}s_is_{i+1}-e[(i+1)s_{i-1}s_is_{i+1}+s_{i-1}s_i-s_{i-1}+i-1]}\beta^{-e}$$
$$= \zeta^{-1-e(-i-1+3s_{i-1}-s_{i-1}+i-1)}\beta^{-e}$$
$$= \zeta^{-1-2e(s_{i-1}-1)}\beta^{-e} = \zeta^{-1}\beta^{-e} = \alpha^{-1},$$

since $2(s_{i-1}-1) \equiv 0 \bmod 8$.

Consider next the case $\nu \geqslant 4$. Let $2^{\nu-1-l}\|i-j$, $2^k\|s_j+1$. For suitably chosen $j$ we have $k > 1$. Indeed, if $l > 2$ then $\nu-1-l < \nu-3$, $2^{\nu-1-l}\|i-j-2^{\nu-3}$ and by (i) $s_j \equiv -1 \bmod 4$ or $s_{j+2^{\nu-3}} \equiv -1 \bmod 4$.

If $l = 2$ and $s_j \equiv 1 \bmod 4$ then by (i) $s_{j+2^{\nu-3}} \equiv -1 \bmod 4$, by (ii) $s_{j+2^{\nu-4}} \equiv -1 \bmod 4$, because $s_{j+2^{\nu-3}} \not\equiv -1 \bmod 8$ and again by (ii) $s_j \equiv -1 \bmod 4$, a contradiction.

By the definition of $l$ we have $k \leqslant l$ and by (iii) $k \neq l$. Thus we get $1 < k < l < \nu$. Let

$$s_i \equiv -5^{a_i} \bmod 2^\nu, \quad s_j \equiv -5^{a_j} \bmod 2^\nu.$$

It follows

$$5^{a_i} \equiv 1 \bmod 2^l, \quad 5^{a_j} \equiv 2^k+1 \bmod 2^{k+1};$$

$$2^{l-2}|a_i, \quad 2^{k-2}\|a_j; \quad (a_j, 2^{\nu-2})|a_i$$

and the congruence

$$ta_j + a_i \equiv 0 \bmod 2^{\nu-2}$$

is soluble. Since $k < l$ its root $t$ must be even. Thus we have for an even $t$

$$s_i s_j^t \equiv -1 \bmod 2^\nu.$$

Since $2^{\nu-1-l}|i-j$, $2^l|s_i+1$ we get

$$j(s_is_j^t - s_i) + i(s_i+1) \equiv (i-j)(s_i+1) \equiv 0 \bmod 2^{\nu-1}$$

and

$$\sigma_i\sigma_j^t(\alpha) = \zeta^{s_is_j^t - e[j(s_is_j^t-s_i)+i(s_i+1)]}\beta^{-e} = \alpha^{-1},$$

which is impossible.

Lemma 3. *The theorem holds for $q = p^\nu$, where $p$ is an odd prime.*

Proof. Set $\zeta_q = \zeta$. If $e \not\equiv 0 \bmod p$ we have for suitable $i$

$$\alpha = \zeta\beta^e = (\zeta^i\beta)^e,$$

hence $\zeta^i\beta$ is not conjugate to $\zeta^{-i}\beta^{-1}$. Assume that $e \equiv 0 \bmod p$, $|\boldsymbol{K}| \not\equiv 0 \bmod p$ and that for each $i$ there exists an automorphism $\sigma_i$ of the normal closure of $\boldsymbol{K}(\alpha)$ such that

$$\sigma_i(\zeta^i\beta) = \zeta^{-i}\beta^{-1}.$$



If $i \equiv 0 \bmod p^{\nu-1}$, $t$ is odd then

$$\sigma_i^t(\beta) = \zeta_q^{-i(s_i^t+1)}\beta^{-1}, \quad \sigma_i^t(\alpha) = \zeta_q^{s_i^t}\beta^{-e}.$$

We have

$$\sigma_0\sigma_{p^{\nu-1}}(\alpha) = \zeta^{s_0s_{p^{\nu-1}}}\beta^e = \sigma_{p^{\nu-1}}\sigma_0(\alpha),$$

$$\sigma_0\sigma_{p^{\nu-1}}(\zeta_p) = \sigma_{p^{\nu-1}}\sigma_0(\zeta_p), \quad \sigma_0\sigma_{p^{\nu-1}}(\beta^p) = \sigma_{p^{\nu-1}}\sigma_0(\beta^p),$$

thus by Lemma 1

$$\sigma_0\sigma_{p^{\nu-1}}(\beta) = \sigma_{p^{\nu-1}}\sigma_0(\beta); \quad p^{\nu-1}(s_0+1)(s_{p^{\nu-1}}+1) \equiv 0 \bmod p^\nu.$$

Hence either $s_0 \equiv -1 \bmod p$ or $s_{p^{\nu-1}} \equiv -1 \bmod p$ and we assume without loss of generality that the first congruence holds. Then $s_0^{p^{\nu-1}} \equiv -1 \bmod p^\nu$, $\sigma_0^{p^{\nu-1}}(\alpha) = \alpha^{-1}$, which is impossible.

Proof of the theorem. We proceed by induction with respect to $\omega(q)$ the number of distinct prime factors of $q$. If $\omega(q) = 0$ the theorem is trivial. If $\omega(q) = 1$ the theorem holds in virtue of Lemmata 2 and 3. Suppose that the theorem holds for $\omega(q) < n$ and consider $\omega(q) = n > 1$. Let $p$ be the least prime factor of $q$, $q = p^\nu q_1$, $e = p^\mu e_1$, where $p \nmid q_1e_1$. If $\mu = 0$ then for suitable $\zeta_{p^\nu}$, $\zeta_{q_1}$ we have

$$\alpha = \zeta_q\beta^e = \zeta_{q_1}(\zeta_{p^\nu}\beta)^e.$$

Since $\zeta_q = \alpha\beta^{-e} \in \boldsymbol{K}(\alpha)$ we have $\zeta_{p^\nu} \in \boldsymbol{K}(\alpha)$, $\zeta_{p^\nu}\beta \in \boldsymbol{K}(\alpha)$ and by the inductive assumption for some $i$

$$\zeta_{q_1}^i\zeta_{p^\nu}\beta \text{ is not conjugate to } \zeta_{q_1}^{-i}\zeta_{p^\nu}^{-1}\beta^{-1},$$

which was to be proved.

If $\mu > 0$, by the assumption $|\boldsymbol{K}| \not\equiv 0 \bmod p$. We have for suitable $\zeta_{p^\nu}$, $\zeta_{q_1}$

$$\alpha = \zeta_q\beta^e = \zeta_{p^\nu}(\zeta_{q_1}\beta^{e_1})^{p^\mu}.$$

Since $\zeta_{q_1}\beta^{e_1} \in \boldsymbol{K}(\alpha)$ it follows by the inductive assumption that for some $i$

$$\alpha_1 = \zeta_{p^\nu}^i\zeta_{q_1}\beta^{e_1} \text{ is not conjugate to } \alpha_1^{-1}.$$

However we have for suitable $j$

$$\alpha_1 = \zeta_{q_1}(\zeta_{p^\nu}^j\beta)^{e_1}$$

and $\zeta_{p^\nu}^j\beta \in \boldsymbol{K}(\zeta_{p^\nu}, \alpha_1)$. Indeed, $\beta \in \boldsymbol{K}(\alpha)$ and $\alpha = \zeta_{p^\nu}^{1-ip^\mu}\alpha_1^{p^\mu}$. Moreover since $(|\boldsymbol{K}|, q, e) = 1$ and $p$ is the least prime factor of $q$

$$\big(|\boldsymbol{K}(\zeta_{p^\nu})|, q_1, e_1\big) \,\big|\, \big(p^{\nu-1}(p-1)|\boldsymbol{K}|, q_1, e_1\big) = 1.$$

By the inductive assumption we have for some $k$:

$$\zeta_{q_1}^k\zeta_{p^\nu}^j\beta \text{ is not conjugate to } \zeta_{q_1}^{-k}\zeta_p^{-j}\beta^{-1}$$

which was to be proved.

Remark 1. An examination of the proof shows that if $K$ is abelian the assumption $(|K|, q, e) = 1$ can be replaced by $(|K|, q, e) \equiv 1 \bmod 2$.

COROLLARY. *If $a \in \Omega$ is an integer not conjugate to $a^{-1}$, $a \neq 0$ and $f(a) = 0$, where $f$ is a polynomial with integer coefficients then*

$$e(a, \Omega) \leqslant \tfrac{5}{2}|\Omega| \log \|f\|.$$

Proof. Suppose first that $\Omega = Q(a)$, set $e(a, \Omega) = e$ and let $\beta$ be an integer of $Q(a)$ such that $a = \zeta_q \beta^e$. It follows that

$$\log \overline{|a|} = e \log \overline{|\beta|}. \tag{3}$$

By the inequality of Carmichael–Masson $\overline{|a|} \leqslant \|f\|^{1/2}$ we have

$$\log \overline{|a|} \leqslant \tfrac{1}{2} \log \|f\|. \tag{4}$$

On the other hand, by the theorem $\zeta_q^i \beta$ is not conjugate to $\zeta_q^{-i} \beta^{-1}$ for some $i$. Since $\zeta_q^i \beta \in Q(a)$ we have by the inequality (2)

$$\overline{|\beta|} = \overline{|\zeta_q^i \beta|} > 1 + \frac{1}{5|Q(a)| - 1},$$

thus

$$\log \overline{|\beta|} > \frac{1}{5|Q(a)|}$$

and by (3) and (4)

$$e \leqslant \tfrac{5}{2}|Q(a)| \log \|f\|.$$

In the general case we use the following assertion of Lemma 1 of [1] independent of (1). If $\Omega_1 \supset \Omega$ then

$$e(a, \Omega_1) \leqslant \frac{|\Omega_1|}{|\Omega|} e(a, \Omega).$$

Taking $\Omega_1 = \Omega$, $\Omega = Q(a)$ we get

$$e(a, \Omega) \leqslant \frac{|\Omega|}{|Q(a)|} \cdot \tfrac{5}{2}|Q(a)| \log \|f\| = \tfrac{5}{2}|\Omega| \log \|f\|,$$

q.e.d.

Remark 2. The recent unpublished work of C. J. Smyth on the product of conjugates of an algebraic integer lying outside the unit circle allows one to strenghten considerably the Corollary and the relevant results of [1]. This will form an object of another paper.

**Reference**

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



**Corrigenda to [1]**

p. 123 line 1 from below for $J(x^{-1})$ read $Jf(x^{-1})$;

p. 150 lines 9–6 from below should read

$$\log 4 + 5 \cdot 2^{\|F\|^4 - 1} + 2\|F\|^2 \log 8 |F|^* \leqslant (\|F\|^2 - 1) \exp(21 |F|^{*\|F\| - 1} \log \|F\|)$$

and obtain

$$\begin{aligned} h(N) &\leqslant 4 \exp_2 (21 |F|^{*\|F\|-1} \log \|F\|) \exp(5 \cdot 2^{\|F'\|^2 - 1} + 2\|F'\| \log |F'|^*) \\ &< \exp(\log 4 + \exp(21 |F|^{*\|F\|-1} \log \|F\|)) \times \\ &\quad \times (\exp 5 \cdot 2^{\|F\|^4 - 1} + \ldots; \end{aligned}$$

p. 151 line 13 for exp read $\exp_{2k-4}$.

p. 157 line 14 for $\sum_{j=0}^{k} a_j \prod_{i=1}^{l} z^{\mu_{ij}}$ read $a_0 + \sum_{j=1}^{k} a_j \prod_{i=1}^{l} z_i^{\mu_{ij}}$.

(118) *Received on 17. 10. 1970*