$$l^{l/2}\prod_{i=1}^{l}h(p_i)\geqslant n^{k-l}=\left(\frac{H(n_1,\ldots,n_m)}{D(n_1,\ldots,n_m)}\right)^{(k-l)/(k-m)}$$

which proves (3).

Acknowledgement. The authors wish to thank A. Schinzel for his attention to the work, his stimulating influence and for his help in the preparation of this article and presentation of the proof of Theorem 2.

References

[1] E. Bombieri and J. D. Vaaler, *On Siegel's lemma*, Invent. Math. 73 (1983), 11–32.

[2] S. Chaładus, *Note on a decomposition of integer vectors*, Bull. Polish Acad. Sci., Math. 35 (1987), 705–707.

[3] A. Châtelet, *Leçons sur la théorie des nombres*, Paris 1913.

[4] R. A. Rankin, *On positive definite quadratic forms*, J. London Math. Soc. 28 (1953), 309–314.

[5] A. Schinzel, *A decomposition of integer vectors, III*, Bull. Polish Acad. Sci., Math. 35 (1987), 693–703.

[6] — *A decompositon of integer vectors, IV*, J. Austral. Math. Soc. (to appear).

Received on 18.8.1989
and in revised form on 14.11.1989 (1959)

ACTA ARITHMETICA
LVII (1991)

Reducibility of lacunary polynomials, XI

by

A. Schinzel (Warszawa)

The notation of this paper is that of [1] and [3]. The aim is to improve the results of these papers by proving the following

Theorem. *Let $k > 1$ and $a_0, \ldots, a_k$ be non-zero complex numbers such that $a_0 \in \boldsymbol{Q}(a_1/a_0, \ldots, a_k/a_0) = \boldsymbol{K}_0$. The number of integer vectors $\boldsymbol{n} = [n_1, \ldots, n_k]$ such that*

$$0 < n_1 < n_2 < \ldots < n_k \leqslant N, \quad N \geqslant 3$$

and $K(a_0 + \sum_{i=1}^{k} a_i x^{n_i})$ is reducible over $\boldsymbol{K}_0$ is

$$O\left(N^{k-\min(1,3/(k-1))}\frac{(\log N)^{10}}{(\log\log N)^9}\right)$$

where for $k < 4$ the logarithmic factors can be omitted.

The above theorem constitutes an improvement upon Theorem 2 of [3] only for $k = 3, 4, 5$. However, in view of possible other applications we formulate the lemmata for arbitrary $k \geqslant 4$. The proof of Lemma 2 has been simplified by Professor J. Browkin.

Lemma 1. *Let $k \geqslant 4$, vectors $\boldsymbol{p}, \boldsymbol{q} \in \boldsymbol{Z}^k$ be linearly independent, α_i $(0 \leqslant i \leqslant k)$ be non-zero algebraic numbers such that*

$$\alpha_0 \in \boldsymbol{Q}(\alpha_1/\alpha_0, \ldots, \alpha_k/\alpha_0) = \boldsymbol{K}_0,$$

$$D(y, z) = \left(JN_{\boldsymbol{K}_0/\boldsymbol{Q}}\left(\alpha_0 + \sum_{i=1}^{k}\alpha_i y^{p_i} z^{q_i}\right), JN_{\boldsymbol{K}_0/\boldsymbol{Q}}\left(\alpha_0 + \sum_{i=1}^{k}\alpha_i y^{-p_i} z^{-q_i}\right)\right).$$

If $D(y, z) \in \boldsymbol{Q}[y, z]\setminus\boldsymbol{Q}[z]$ then either there exists a vector $\gamma \in \boldsymbol{Z}^k$ such that

$$\gamma\boldsymbol{p} = \gamma\boldsymbol{q} = 0, \quad h(\gamma) = 1$$

or there exist three linearly independent vectors $\boldsymbol{r}_1, \boldsymbol{r}_2, \boldsymbol{r}_3 \in \boldsymbol{Z}^k$ such that $\boldsymbol{r}_i\boldsymbol{p} = 0$ implies $\boldsymbol{r}_i\boldsymbol{q} = 0$ $(1 \leqslant i \leqslant 3)$,

$$(\boldsymbol{r}_i\boldsymbol{p})(\boldsymbol{r}_j\boldsymbol{q}) = (\boldsymbol{r}_j\boldsymbol{p})(\boldsymbol{r}_i\boldsymbol{q}) \quad (1 \leqslant i \leqslant j \leqslant 3)$$

and $l(\boldsymbol{r}_1) \leqslant 2$, $l(\boldsymbol{r}_2) \leqslant 2$, $l(\boldsymbol{r}_3) \leqslant 4$, *where* $l(\boldsymbol{r})$ *is the sum of the absolute values of the coordinates of* $\boldsymbol{r}$ *and* $h(\boldsymbol{r})$ *is their maximum.*

Proof. Let in the neighbourhood of $z = \infty$ one of the zeros of $D(y, z)$ be given by the Puiseux expansion

$$y(z) = c_0 z^a + \sum_{j=1}^{\infty} c_j z^{a-b_j},$$

where $0 < b_1 < b_2 < \ldots$, $c_0 \neq 0$ (since $(D(y, z), y) = 1$ we cannot have $y(z) \equiv 0$) and either $c_1 \neq 0$ or $c_j = 0$ for all $j \geqslant 1$.

Let $p_0 = q_0 = 0$,

$$\bigcup_{i=0}^{k} \{ap_i + q_i\} = \{w_1, \ldots, w_l\}, \quad \text{where } w_1 < w_2 < \ldots < w_l$$

and let

$$S_\lambda = \{i\colon 0 \leqslant i \leqslant k,\ ap_i + q_i = w_\lambda\}.$$

We have $l \geqslant 2$ since otherwise for all $i \leqslant k$

$$ap_i + q_i = ap_0 + q_0 = 0,$$

contrary to the linear independence of $\boldsymbol{p}$, $\boldsymbol{q}$.

From the divisibility

$$D(y, z) | \Big(JN_{K_0/Q}\big(\alpha_0 + \sum_{i=1}^{k} \alpha_i y^{p_i} z^{q_i}\big),\ JN_{K_0/Q}\big(\alpha_0 + \sum_{i=1}^{k} \alpha_i y^{-p_i} z^{-q_i}\big)\Big)$$

it follows that for some conjugates α_i', α_i'' of α_i we have

$$g(z) = \alpha_0' + \sum_{i=1}^{k} \alpha_i' y(z)^{p_i} z^{q_i} = 0,$$

$$h(z) = \alpha_0'' + \sum_{i=1}^{k} \alpha_i'' y(z)^{-p_i} z^{-q_i} = 0.$$

However,

$$g(z) = \sum_{\lambda=1}^{l} \big(\sum_{i \in S_\lambda} \alpha_i' c_0^{p_i}\big) z^{w_\lambda} + \big(\sum_{i \in S_l} \alpha_i' c_0^{p_i - 1} p_i c_1\big) z^{w_l - b_1} + o(z^{w_l - b_1}),$$

$$h(z) = \sum_{\lambda=1}^{l} \big(\sum_{i \in S_\lambda} \alpha_i'' c_0^{-p_i}\big) z^{-w_\lambda} - \big(\sum_{i \in S_1} \alpha_i'' p_i c_0^{-p_i - 1} c_1\big) z^{-w_1 - b_1} + o(z^{-w_1 - b_1}),$$

where if $c_1 = 0$ the remainder terms are missing.

If $c_1 = 0$ we have for all $\lambda \leqslant l$

$$\sum_{i \in S_\lambda} \alpha_i' c_0^{p_i} = 0; \qquad \operatorname{card} S_\lambda \geqslant 2.$$

Let

$$\boldsymbol{R} = \bigcup_{\lambda=1}^{l} \{\boldsymbol{e}_i - \boldsymbol{e}_{i_\lambda}\colon i \in S_\lambda,\ i \neq i_\lambda\}$$

where $i_\lambda = \min S_\lambda$, $\boldsymbol{e}_0 = \boldsymbol{0}$, $\boldsymbol{e}_i = [\underbrace{0, \ldots, 0, 1}_{i}, 0, \ldots, 0]$ $(1 \leqslant i \leqslant k)$.

Since the sets S_λ are disjoint, the vectors of the set $\boldsymbol{R}$ are linearly independent and every $\boldsymbol{r} \in \boldsymbol{R}$ satisfies

$$a\boldsymbol{r}\boldsymbol{p} + \boldsymbol{r}\boldsymbol{q} = 0.$$

Moreover

$$\operatorname{card} \boldsymbol{R} = \sum_{\lambda=1}^{l} (\operatorname{card} S_\lambda - 1) \geqslant \tfrac{1}{2} \sum_{\lambda=1}^{l} \operatorname{card} S_\lambda \geqslant \tfrac{1}{2}(k+1) > 2.$$

Hence for $\boldsymbol{r}_1$, $\boldsymbol{r}_2$, $\boldsymbol{r}_3$ we can take any three vectors of $\boldsymbol{R}$.

Therefore, assume that $c_1 \neq 0$. Then $g(z) = h(z) = 0$ implies

$$(1) \qquad \sum_{i \in S_l} \alpha_i' c_0^{p_i} = 0, \qquad \sum_{i \in S_1} \alpha_i'' c_0^{-p_i} = 0,$$

hence $\operatorname{card} S_l \geqslant 2$, $\operatorname{card} S_1 \geqslant 2$.

If $\operatorname{card} S_1 + \operatorname{card} S_l \geqslant 5$ we take for $\boldsymbol{r}_1$, $\boldsymbol{r}_2$, $\boldsymbol{r}_3$ any three vectors of the set

$$\{\boldsymbol{e}_i - \boldsymbol{e}_{i_l}\colon i \in S_l,\ i \neq i_l\} \cup \{\boldsymbol{e}_i - \boldsymbol{e}_{i_1}\colon i \in S_1,\ i \neq i_1\}.$$

If $\operatorname{card} S_l = \operatorname{card} S_1 = 2$ let $S_1 = \{i_1, j_1\}$, $S_l = \{i_l, j_l\}$.

If $p_{i_1} = p_{j_1}$ we take

$$\boldsymbol{\gamma} = \boldsymbol{e}_{j_1} - \boldsymbol{e}_{i_1}.$$

If $p_{i_1} \neq p_{j_1}$, but $p_{i_l} = p_{j_l}$ we take

$$\boldsymbol{\gamma} = \boldsymbol{e}_{j_l} - \boldsymbol{e}_{i_l}.$$

If $p_{i_1} \neq p_{j_1}$, and $p_{i_l} \neq p_{j_l}$ we infer from (1) that

$$\sum_{i \in S_l} \alpha_i' p_i c_0^{p_i - 1} c_1 = \alpha_{j_l}' (p_{j_l} - p_{i_l}) c_0^{p_{j_l} - 1} c_1 \neq 0,$$

$$\sum_{i \in S_1} \alpha_i'' p_i c_0^{-p_i - 1} c_1 = \alpha_{j_1}'' (p_{j_1} - p_{i_1}) c_0^{-p_{j_1} - 1} c_1 \neq 0,$$

hence for some μ, ν

$$w_l - b_1 = w_\mu; \quad \sum_{i \in S_\mu} \alpha_i' c_0^{p_i} \neq 0;$$

$$-w_1 - b_1 = -w_\nu; \quad \sum_{i \in S_\nu} \alpha_i'' c_0^{-p_i} \neq 0.$$

It follows that $1 < \mu < l$, $1 < \nu < l$ and

$$w_l+w_1 = w_\mu+w_\nu.$$

We take

$$\boldsymbol{r}_1 = \boldsymbol{e}_{j_1}-\boldsymbol{e}_{i_1},\quad \boldsymbol{r}_2 = \boldsymbol{e}_{j_l}-\boldsymbol{e}_{i_l},\quad \boldsymbol{r}_3 = \boldsymbol{e}_{i_l}+\boldsymbol{e}_{i_1}-\boldsymbol{e}_{i_\mu}-\boldsymbol{e}_{i_\nu}.$$

Since the sets S_1, S_l, $S_\mu\cup S_\nu$ are disjoint, the vectors $\boldsymbol{r}_1$, $\boldsymbol{r}_2$, $\boldsymbol{r}_3$ are linearly independent, unless $i_\mu = i_\nu = 0$. However, in the latter case

$$\boldsymbol{r}_1[1,\dots,1] = \boldsymbol{r}_2[1,\dots,1] = 0,\quad \boldsymbol{r}_3[1,\dots,1] = 2,$$

thus the same conclusion holds.

LEMMA 2. *Let $k\geqslant 4$, $\boldsymbol{p}$, $\boldsymbol{q}$, α_i, $D(y,z)$ have the meaning of Lemma 1, $p_0 = q_0 = 0$. If $D(y,z)\in \boldsymbol{Q}[z]$ and $KD\neq 1$, then either there exists a vector $\boldsymbol{\gamma}\in \boldsymbol{Z}^k$ such that*

(2) $$0 < h(\boldsymbol{\gamma}) \leqslant C_0(\boldsymbol{\alpha}),$$

(3) $$\boldsymbol{\gamma}\boldsymbol{p} = \boldsymbol{\gamma}\boldsymbol{q} = 0,$$

or there exists a decomposition

(4) $$\{0,1,\dots,k\} = \bigcup_{\lambda=1}^{l} \boldsymbol{I}_\lambda,\quad \boldsymbol{I}_\lambda \textit{ disjoint},$$

where $[(k+1)/3]\geqslant l\geqslant 2$, $\operatorname{card}\boldsymbol{I}_\lambda\geqslant 2$ and

(5) $$p_i = p_j \quad \textit{for } i,j\in \boldsymbol{I}_\lambda \quad (1\leqslant\lambda\leqslant l).$$

Proof. Let

$$\bigcup_{i=0}^{k}\{p_i\} = \{v_1, v_2, \dots, v_l\},\quad \text{where } v_1<\dots<v_l,$$

and let

$$\boldsymbol{I}_\lambda = \{i\colon 0\leqslant i\leqslant k\colon p_i = v_\lambda\},\quad i_\lambda = \min \boldsymbol{I}_\lambda \quad (1\leqslant\lambda\leqslant l).$$

Since $p_0 = 0$ and $\boldsymbol{p}\neq \boldsymbol{0}$ we have $l\geqslant 2$.

By Gauss's lemma we obtain

$$D(z)\,|\,N_{\boldsymbol{K}_0/\boldsymbol{Q}}\,\Delta(z),$$

where $\Delta(z)$ is the content of $J\big(\sum_{j=0}^{k}\alpha_j y^{p_j}z^{q_j}\big)$ viewed as a polynomial in y. Hence $K\Delta(z)\neq 1$ and

$$\Delta(z)\,|\,J\Big(\sum_{j\in \boldsymbol{I}_\lambda}\alpha_j z^{q_j}\Big)\quad (1\leqslant\lambda\leqslant l),$$

which implies $\operatorname{card}\boldsymbol{I}_\lambda\geqslant 2$ $(1\leqslant\lambda\leqslant l)$.

If for some distinct λ, $\mu\leqslant l$ we have

$$\operatorname{card}\boldsymbol{I}_\lambda+\operatorname{card}\boldsymbol{I}_\mu\leqslant 5,$$

we take in Theorem 1 of [5] after a suitable renumbering of the variables x_i

$$P = \alpha_{i_\lambda}+\sum_{i\in \boldsymbol{I}_\lambda\setminus\{i_\lambda\}}\alpha_i x_i,\quad Q = \alpha_{i_\mu}+\sum_{i\in \boldsymbol{I}_\mu\setminus\{i_\mu\}}\alpha_i x_i,$$

$$n_i = q_i-q_{i_\lambda}\ (i\in \boldsymbol{I}_\lambda\setminus\{i_\lambda\}),\quad n_i = q_i-q_{i_\mu}\ (i\in \boldsymbol{I}_\mu\setminus\{i_\mu\})$$

and obtain the existence of integers γ_i $(i\in \boldsymbol{I}_\lambda\cup \boldsymbol{I}_\mu\setminus\{i_\lambda, i_\mu\})$ such that

$$0<\max|\gamma_i|\leqslant C_1(\boldsymbol{\alpha}),$$

$$\sum_{i\in \boldsymbol{I}_\lambda\setminus\{i_\lambda\}}\gamma_i(q_i-q_{i_\lambda})+\sum_{i\in \boldsymbol{I}_\mu\setminus\{i_\mu\}}\gamma_i(q_i-q_{i_\mu}) = 0.$$

Taking

$$\boldsymbol{\gamma} = \sum_{i\in \boldsymbol{I}_\lambda\cup \boldsymbol{I}_\mu\setminus\{i_\lambda,i_\mu\}}\gamma_i\boldsymbol{e}_i-\Big(\sum_{i\in \boldsymbol{I}_\lambda\setminus\{i_\lambda\}}\gamma_i\Big)\boldsymbol{e}_{i_\lambda}-\Big(\sum_{i\in \boldsymbol{I}_\mu\setminus\{i_\mu\}}\gamma_i\Big)\boldsymbol{e}_{i_\mu}$$

we find (2) and (3) with $C_0(\boldsymbol{\alpha}) = 2C_1(\boldsymbol{\alpha})$.

If for all distinct λ, $\mu\leqslant l$ we have

$$\operatorname{card}\boldsymbol{I}_\lambda+\operatorname{card}\boldsymbol{I}_\mu\geqslant 6$$

then in particular for every $\lambda\leqslant l$

$$\operatorname{card}\boldsymbol{I}_\lambda+\operatorname{card}\boldsymbol{I}_{\lambda+1}\geqslant 6$$

where $\boldsymbol{I}_{l+1} = \boldsymbol{I}_1$. On summing over λ we obtain

$$6l\leqslant \sum_{\lambda=1}^{l}\operatorname{card}\boldsymbol{I}_\lambda+\sum_{\lambda=1}^{l}\operatorname{card}\boldsymbol{I}_{\lambda+1} = 2(k+1)$$

which gives the desired bound for l.

Before proceeding further we recall the definition of $c_0(k)$ from [1]:

$$c_0(k) = \sup_{\substack{\boldsymbol{n}\in \boldsymbol{Z}^k\\ \boldsymbol{n}\neq \boldsymbol{0}}}\inf\frac{h(\boldsymbol{p})\,h(\boldsymbol{q})}{h(\boldsymbol{n})^{(k-2)/(k-1)}},$$

where the infimum is taken over all pairs of linearly independent vectors $\boldsymbol{p},\boldsymbol{q}\in \boldsymbol{Z}^k$ such that $\boldsymbol{n} = u\boldsymbol{p}+v\boldsymbol{q}$, $u, v\in \boldsymbol{Q}$. The next lemma is an improvement of Lemma 2 of [1].

LEMMA 3. *Let $k\geqslant 4$, α_j have the meaning of Lemma 1, $\boldsymbol{m} = [m_1,\dots,m_k]$. If $0 = m_0<m_1<\dots<m_k$, $(m_1,\dots,m_k) = 1$ and $KN_{\boldsymbol{K}_0/\boldsymbol{Q}}\big(\sum_{j=0}^{k}\alpha_j x^{m_j}\big)$ has a squarefree reciprocal factor $f(x)$, then either*

(6) $$\deg f\leqslant c_0(k)\,[\boldsymbol{K}_0:\boldsymbol{Q}]^2\, m_k^{(k-2)/(k-1)}$$

or there exists a vector $\boldsymbol{\gamma}\in \boldsymbol{Z}^k$ such that

(7) $$0<h(\boldsymbol{\gamma})\leqslant C_0(\boldsymbol{\alpha})\quad \textit{and}\quad \boldsymbol{\gamma}\boldsymbol{m} = 0$$

or there exist three linearly independent vectors $\boldsymbol{r}_1$, $\boldsymbol{r}_2$, $\boldsymbol{r}_3\in \boldsymbol{Z}^k$ such that

(8) $$l(\mathbf{r}_1) \leqslant 2, \quad l(\mathbf{r}_2) \leqslant 2, \quad l(\mathbf{r}_3) \leqslant 4$$

and

(9) $$\max\{|\mathbf{r}_1\mathbf{m}|, |\mathbf{r}_2\mathbf{m}|, |\mathbf{r}_3\mathbf{m}|\} \leqslant 4\sqrt{c_0(k)}\, m_k^{(k-2)/2(k-1)}(\mathbf{r}_1\mathbf{m}, \mathbf{r}_2\mathbf{m}, \mathbf{r}_3\mathbf{m}),$$

or there exists a decomposition

$$\{0, 1, \ldots, k\} = \bigcup_{\lambda=1}^{l} \mathbf{I}_\lambda, \quad \mathbf{I}_\lambda \text{ disjoint},$$

where $2 \leqslant l \leqslant [(k+1)/3]$, $\operatorname{card} \mathbf{I}_\lambda \geqslant 2$ $(1 \leqslant \lambda \leqslant l)$ *and*

(10) $$\frac{\max\limits_{\lambda \leqslant l, i, j \in \mathbf{I}_\lambda} |m_j - m_i|}{\text{g.c.d.}\limits_{\lambda \leqslant l, i, j \in \mathbf{I}_\lambda} (m_j - m_i)} \leqslant 2c_0(k)\, m_k^{(k-2)/(k-1)}.$$

Proof. By the definition of $c_0(k)$ and by Theorem 2 of [2] there exist linearly independent vectors $\mathbf{p}, \mathbf{q} \in \mathbf{Z}^k$ such that

(11) $$\mathbf{m} = u_0\mathbf{p} + v_0\mathbf{q}$$

where

(12) $$h(\mathbf{p})\, h(\mathbf{q}) \leqslant c_0(k)\, m_k^{(k-2)/(k-1)}$$

and $u_0, v_0 \in \mathbf{Z}$. By Theorem 1 of [2]

(13) $$c_0(k) \leqslant 2.$$

In view of symmetry between $\mathbf{p}$ and $\mathbf{q}$ we may assume that

$$h(\mathbf{p}) \leqslant h(\mathbf{q}),$$

hence

(14) $$h(\mathbf{p}) \leqslant \sqrt{c_0(k)}\, m_k^{(k-2)/2(k-1)}.$$

It follows from $(m_1, \ldots, m_k) = 1$ that $(u_0, v_0) = 1$. If we had $v_0 = 0$ it would follow that $u_0 = \pm 1$, $h(\mathbf{n}) = h(\mathbf{p})$ and thus by (13) and (14)

$$m_k = h(\mathbf{m}) \leqslant c_0(k)^{(k-1)/k} \leqslant 2^{(k-1)/k} < 1,$$

which contradicts $m_k \geqslant k \geqslant 4$. Therefore,

(15) $$(u_0, v_0) = 1, \quad v_0 \neq 0.$$

Let us consider polynomials

$$G = JN_{K_0/Q}\Big(\sum_{j=0}^{k} \alpha_j y^{p_j} z^{q_j}\Big),$$

$$H = JN_{K_0/Q}\Big(\sum_{j=0}^{k} \alpha_j y^{-p_j} z^{-q_j}\Big),$$

$$D = (G, H).$$

We distinguish three cases:

(i) $D \in \mathbf{Q}[z]$, $KD(z) = 1$,

(ii) $D \in \mathbf{Q}[z]$, $KD(z) \neq 1$,

(iii) $D \in \mathbf{Q}[y, z] \setminus \mathbf{Q}[z]$.

In the case (i) we infer from (15) as in [1], p. 316 (with the simplification resulting from $w_0 = 1$) that

$$\deg f \leqslant 8\,[K_0 : Q]^2\, h(\mathbf{p})\, h(\mathbf{q}),$$

which implies (6) in view of (12).

In the case (ii) by Lemma 2 either there exists a vector $\boldsymbol{\gamma} \in \mathbf{Z}^k$ satisfying (2) and (3) or there exists a decomposition (4) satisfying (5). In the former case $\boldsymbol{\gamma}$ satisfies (7) in view of (11). In the latter case the decomposition in question satisfies (10) since by (5) and (11)

$$m_j - m_i = v_0(q_j - q_i) \quad (i, j \in \mathbf{I}_\lambda,\ 1 \leqslant \lambda \leqslant l)$$

while by (12)

$$\max_{i<j} |q_j - q_i| \leqslant 2c_0(k)\, m_k^{(k-2)/(k-1)}.$$

In the case (iii) by Lemma 1 either there exists a vector $\boldsymbol{\gamma} \in \mathbf{Z}^k$ satisfying (2) and (3) (provided $C_0(\boldsymbol{\alpha}) \geqslant 1$) or there exist three linearly independent vectors $\mathbf{r}_1$, $\mathbf{r}_2$, $\mathbf{r}_3$ such that $\mathbf{r}_i\mathbf{p} = 0$ implies $\mathbf{r}_i\mathbf{q} = 0$ $(1 \leqslant i \leqslant 3)$,

$$(\mathbf{r}_i\mathbf{p})(\mathbf{r}_j\mathbf{q}) = (\mathbf{r}_j\mathbf{p})(\mathbf{r}_i\mathbf{q}) \quad (1 \leqslant i \leqslant j \leqslant 3)$$

and (8) holds. In the former case $\boldsymbol{\gamma}$ satisfies (7) in view of (11). In the latter case we find by (11)

$$(\mathbf{r}_i\mathbf{p})(\mathbf{r}_j\mathbf{m}) - (\mathbf{r}_j\mathbf{p})(\mathbf{r}_i\mathbf{m})$$
$$= (\mathbf{r}_i\mathbf{p})(\mathbf{r}_j u_0\mathbf{p} + \mathbf{r}_j v_0\mathbf{q}) - (\mathbf{r}_j\mathbf{p})(\mathbf{r}_i u_0\mathbf{p} + \mathbf{r}_i v_0\mathbf{q}) = 0 \quad (1 \leqslant i \leqslant j \leqslant 3).$$

Hence either $\max\{|\mathbf{r}_2\mathbf{m}|, |\mathbf{r}_3\mathbf{m}|\} \neq 0$, thus $\max\{|\mathbf{r}_2\mathbf{p}|, |\mathbf{r}_3\mathbf{p}|\} \neq 0$ and by (8) and (14)

$$\frac{\max\{|\mathbf{r}_1\mathbf{m}|, |\mathbf{r}_2\mathbf{m}|, |\mathbf{r}_3\mathbf{m}|\}}{(\mathbf{r}_1\mathbf{m}, \mathbf{r}_2\mathbf{m}, \mathbf{r}_3\mathbf{m})} = \frac{\max\{|\mathbf{r}_1\mathbf{p}|, |\mathbf{r}_2\mathbf{p}|, |\mathbf{r}_3\mathbf{p}|\}}{(\mathbf{r}_1\mathbf{p}, \mathbf{r}_2\mathbf{p}, \mathbf{r}_3\mathbf{p})} \leqslant 4h(\mathbf{p})$$
$$\leqslant 4\sqrt{c_0(k)}\, m_k^{(k-2)/2(k-1)},$$

which implies (9), or $\mathbf{r}_2\mathbf{m} = \mathbf{r}_3\mathbf{m} = 0$, thus

$$\max\{|\mathbf{r}_1\mathbf{m}|, |\mathbf{r}_2\mathbf{m}|, |\mathbf{r}_3\mathbf{m}|\} = (\mathbf{r}_1\mathbf{m}, \mathbf{r}_2\mathbf{m}, \mathbf{r}_3\mathbf{m}),$$

which again gives (9).

Proof of the theorem. It is enough to prove the theorem for the case where $a_0, a_1, \ldots, a_k$ are algebraic numbers, since then the general case follows in view of Lemma 5 of [3]. Replacing a_i by α_i in order to conform the notation to that of [1] let us assume that $\alpha_0, \ldots, \alpha_k$ are algebraic and that

$$\alpha_0 \in \boldsymbol{Q}(\alpha_1/\alpha_0, \ldots, \alpha_k/\alpha_0) = \boldsymbol{K}_0.$$

If

$$0 = n_0 < n_1 < \ldots < n_k \leqslant N \tag{16}$$

and $K\left(\sum_{j=0}^{k} \alpha_j x^{n_j}\right)$ is reducible over $\boldsymbol{K}_0$ we infer from

$$K\left(\sum_{j=0}^{k} \alpha_j x^{n_j}\right) = A_1(x) A_2(x), \quad A_i \in \boldsymbol{K}_0[x], \quad \deg A_i \geqslant 1$$

that

$$KN_{\boldsymbol{K}_0/\boldsymbol{Q}}\left(\sum_{j=0}^{k} \alpha_j x^{n_j}\right) = \prod_{i=1}^{2} N_{\boldsymbol{K}_0/\boldsymbol{Q}} A_i(x),$$

hence

$$KN_{\boldsymbol{K}_0/\boldsymbol{Q}}\left(\sum_{j=0}^{k} \alpha_j x^{n_j}\right) \text{ is reducible over } \boldsymbol{Q}. \tag{17}$$

Let us denote by $\boldsymbol{S}$ the set of all integer vectors $[n_1, n_2, \ldots, n_k] = \boldsymbol{n}$ satisfying (16) and (17) and decompose it into two subsets $\boldsymbol{T}$ and $\boldsymbol{U}$ assigning a vector $\boldsymbol{n}$ to $\boldsymbol{T}$ if $KN_{\boldsymbol{K}_0/\boldsymbol{Q}}\left(\sum_{j=0}^{k} \alpha_j x^{n_j}\right)$ has in $\boldsymbol{Z}[x]$ at least one irreducible reciprocal factor and to $\boldsymbol{U}$ if all its irreducible factors in $\boldsymbol{Z}[x]$ are non-reciprocal.

It is shown on p. 332 of [1] that

$$\operatorname{card} \boldsymbol{U} = O(N^{k-1}),$$

thus it remains to estimate card $\boldsymbol{T}$. For $k = 2$ the required estimate

$$\operatorname{card} \boldsymbol{T} = O(N)$$

is proved on p. 331 of [1].

Let us consider the case $k = 3$. Then by Lemma 7 of [4] if $\boldsymbol{n} \in \boldsymbol{T}$ then either

$$J\left(\sum_{j=0}^{3} \alpha_j x^{-n_j}\right) = k_0 \sum_{j=0}^{3} \alpha_j^{\sigma} x^{n_j} \tag{18}$$

for an automorphism σ of $\boldsymbol{K}_0$ and a $k_0 \in \boldsymbol{K}_0$, or there is a permutation $\langle g, h, i, j\rangle$ of $\langle 0, 1, 2, 3\rangle$ such that

$$\frac{\max\{|n_i - n_g|, |n_j - n_h|\}}{(n_i - n_g, n_j - n_h)} < B_3(\boldsymbol{\alpha}), \tag{19}$$

where $B_3(\boldsymbol{\alpha})$ is a number depending only on $\boldsymbol{\alpha}$. Now (16) and (18) imply

$$n_1 + n_2 = n_3$$

and the number of vectors $\boldsymbol{n} \in \boldsymbol{Z}^3$ satisfying (16) and the above is $O(N^2)$. On the other hand for a vector $\boldsymbol{n}$ satisfying (16) and (19) the coordinates $n_{\min(g,i)}$, $n_{\min(h,j)}$ can be chosen in at most N ways (one of them is 0) and then by Lemma 6 of [1] with $r = 2$, $A = N$, $B = B_3(\boldsymbol{\alpha})$ the remaining coordinates in at most $2B_3(\boldsymbol{\alpha}) N$ ways. Hence

$$\operatorname{card} \boldsymbol{T} = O(N^2)$$

as required.

Assume now that $k \geqslant 4$, $\boldsymbol{n} \in \boldsymbol{T}$ and let

$$(n_1, \ldots, n_k) = d, \quad n_j = dm_j \quad (0 \leqslant j \leqslant k),$$

$$F(x) = KN_{\boldsymbol{K}_0/\boldsymbol{Q}}\left(\sum_{j=0}^{k} \alpha_j x^{m_j}\right).$$

We have

$$KN_{\boldsymbol{K}_0/\boldsymbol{Q}}\left(\sum_{j=0}^{k} \alpha_j x^{n_j}\right) = F(x^d).$$

If we had $f(x) \neq Jf(x^{-1})$ for every irreducible factor f of F in $\boldsymbol{Z}[x]$ it would follow from $(f(x), Jf(x^{-1})) = 1$, $(f(x^d), Jf(x^{-d})) = 1$ that F has in $\boldsymbol{Z}[x]$ no irreducible reciprocal factor, contrary to $\boldsymbol{n} \in \boldsymbol{T}$. Therefore $F(x)$ has an irreducible reciprocal factor $f \in \boldsymbol{Z}[x]$.

If $\deg f > 8c_0(k)[\boldsymbol{K}_0:\boldsymbol{Q}]^2 m_k^{(k-2)/(k-1)}$, then in virtue of Lemma 3 either there exists a vector $\boldsymbol{\gamma} \in \boldsymbol{Z}^k$ satisfying (7) or there exist three linearly independent vectors $\boldsymbol{r}_1, \boldsymbol{r}_2, \boldsymbol{r}_3 \in \boldsymbol{Z}^k$ satisfying (8) and (9) or there exists a decomposition

$$\{0, 1, \ldots, k\} = \bigcup_{\lambda=1}^{l} \boldsymbol{I}_\lambda, \quad \boldsymbol{I}_\lambda \text{ disjoint}, \tag{20}$$

where

$$2 \leqslant l \leqslant \left[\frac{k+1}{3}\right], \quad \operatorname{card} \boldsymbol{I}_\lambda \geqslant 2 \quad (1 \leqslant \lambda \leqslant l) \tag{21}$$

and (10) holds.

If $\deg f \leqslant 8c_0(k)[\boldsymbol{K}_0:\boldsymbol{Q}] m_k^{(k-2)/(k-1)}$ then in the notation of [1] explained there on p. 329

$$\boldsymbol{m} = [m_1, \ldots, m_k] \in \bigcup_{\nu=3}^{7} \boldsymbol{S}_\nu(N/d).$$

Let us denote by $\boldsymbol{S}(M; \boldsymbol{\gamma})$ the set of all vectors $\boldsymbol{m} \in \boldsymbol{Z}^k$ satisfying $\boldsymbol{\gamma}\boldsymbol{m} = 0$ and

$$0 = m_0 < m_1 < \ldots < m_k \leqslant M, \tag{22}$$

by $S(M; r_1, r_2, r_3)$ the set of all vectors $m \in Z^k$ satisfying (9) and (20), by $S(M; I_1, I_2, \ldots, I_l)$ the set of all vectors $m \in Z^k$ satisfying (10) and (22).

For a given set $A \subset Z^k$ let $dA = \{da: a \in A\}$. We have

$$(23)\quad T \subset \bigcup_{d=1}^{[N/2]} \Big(\bigcup\nolimits_0 dS(N/d; \gamma) \cup \bigcup\nolimits_1 dS(N/d; r_1, r_2, r_3) \cup \bigcup\nolimits_2 dS(N/d; I_1, \ldots, I_l) \cup \bigcup_{v=3}^{7} dS_v(N/d)\Big),$$

where $\bigcup_0$ is taken over all vectors $\gamma \in Z^k$ satisfying (7), $\bigcup_1$ is taken over all triples of linearly independent vectors $r_1, r_2, r_3 \in Z^k$ satisfying (8) and (9), $\bigcup_2$ is taken over all decompositions (20) satisfying (21). Moreover in the notation of [1]

$$(24)\quad S_3(M) \subset \bigcup_{\substack{0<h(\gamma)<C_2(\alpha)\\ \gamma \in Z^k}} S(M; \gamma),$$

$$(25)\quad S_7(M) \subset \bigcup_{\substack{0<h(\gamma)<C_8(\alpha)\\ \gamma \in Z^k}} S(M; \gamma).$$

We have for $\gamma \neq 0$

$$\operatorname{card} S(M, \gamma) = O(M^{k-1}),$$

hence

$$(26)\quad \operatorname{card} \bigcup\nolimits_0 dS(N/d; \gamma) = O((N/d)^{k-1})$$

and by (24), (25)

$$(27)\quad \operatorname{card} S_v(N/d) = O((N/d)^{k-1}) \quad \text{for } v = 3, 7.$$

Further, for r_1, r_2, r_3 linearly independent, $l(r_i) \leqslant 4$

$$\operatorname{card} S(M; r_1, r_2, r_3) \leqslant M^{k-3} \operatorname{card} V,$$

where

$$V = \{[\varrho_1, \varrho_2, \varrho_3] \in Z^3: \max_{1 \leqslant i \leqslant 3} |\varrho_i| \leqslant 4M, \quad \max_{1 \leqslant i \leqslant 3} |\varrho_i| \leqslant 4\sqrt{c_0(k)}\, M^{(k-2)/(k-1)} (\varrho_1, \varrho_2, \varrho_3)\}.$$

Indeed, since $\dim(r_1, r_2, r_3) = 3$ there exists a set $I \subset \{1, 2, \ldots, k\}$ such that $\operatorname{card} I = k-3$ and $r_i m$ $(1 \leqslant i \leqslant 3)$ together with m_i $(i \in I)$ uniquely determine m.

For $m \in S(M; r_1, r_2, r_3)$ we have $[r_1 m, r_2 m, r_3 m] \in V$, while for $i \in I$ $m_i \in \{1, \ldots, M\}$.

Now, by Lemma 6 of [1] applied with $r = 3$, $A = 4M$, $B = 4\sqrt{c_0(k)} \times M^{(k-2)/2(k-1)}$

$$\operatorname{card} V \leqslant 2AB^2 = 128\, c_0(k)\, M^{(2k-3)/(k-1)}.$$

Hence

$$\operatorname{card} S(M; r_1, r_2, r_3) = O(M^{k-1}),$$

$$(28)\quad \operatorname{card} \bigcup\nolimits_1 dS(N/d; r_1, r_2, r_3) = O((N/d)^{k-1}).$$

By the estimate proved on p. 330 of [1]

$$\operatorname{card} S(M; I_1, \ldots, I_l) \leqslant c_3(k)\, M^{k-(k-l)/(k-1)}$$

and since by (21) $k-l \geqslant k-[(k+1)/3] \geqslant 3$

$$(29)\quad \operatorname{card} \bigcup\nolimits_2 dS(N/d; I_1, \ldots, I_l) = O((N/d)^{k-3/(k-1)}).$$

Finally by the estimates proved on p. 331 of [1]

$$\operatorname{card} S_4(M) + \operatorname{card} S_5(M) = O\left(M^{k-3/(k-1)} \frac{(\log M)^{10}}{(\log\log eM)^9}\right)$$

hence

$$(30)\quad \operatorname{card} dS_4\left(\frac{N}{d}\right) + \operatorname{card} dS_5\left(\frac{N}{d}\right) = O\left(\left(\frac{N}{d}\right)^{k-3/(k-1)} \frac{(\log N)^{10}}{(\log\log N)^9}\right).$$

It now follows from (23) and (26)–(30) that

$$\operatorname{card} T = O\left(N^{k-3/(k-1)} \frac{(\log N)^{10})}{(\log\log N)^9}\right),$$

which completes the proof.

References

[1] A. Schinzel, *Reducibility of lacunary polynomials, VII*, Monatsh. Math. 102 (1986), 309–337.

[2] — *A decomposition of integer vectors, I*, Bull. Polish Acad. Sci., Math. 35 (1987), 155–159.

[3] — *Reducibility of lacunary polynomials, VIII*, Acta Arith. 50 (1988), 91–106.

[4] — *Reducibility of lacunary polynomials, IX*, in *New Advances in Transcendence Theory* (ed. A. Baker), Cambridge University Press, 1988, 313–336.

[5] — *Reducibility of lacunary polynomials, X*, Acta Arith. 53 (1989), 47–97.

Corrections to [1] (see also Note at the end of [5])

p. 329 line −2: for $\subset S_7(M)$ read $\cup S_7(M)$

p. 330 formula (51): for S, S_4, S_5, S_8 read dS, dS_4, dS_5, dS_8 for $N/4$ read N/d.

line −14: for $\max\{g, h\}$. read $\max\{g, i\}$

line −10: for $1/2(k-1)$ read $k/2(k-1)$

Received on 19.9.1989
and in revised form on 13.11.1989 (1968)