tive 6th root of unity. We use the simple fact that if $|a_1+a_2+a_3| = 1$, $|a_k| = 1$, $k = 1, 2, 3$ then there exist $1 \leqslant i < j \leqslant 3$ such that $a_i + a_j = 0$. This can be seen by viewing a parallelogram as four vectors with clockwise orientation in which case opposite vectors are additive inverses or in the degenerate case adjacent vectors are additive inverses. We have $1 = |\zeta^{l_1}\zeta^{l_2}\zeta^{l_3}| = |\zeta^{l_1}+\zeta^{l_2}+\zeta^{l_3}|$ and $|\zeta^{l_i}| = 1$, $i = 1, 2, 3$. So we may assume $\zeta^{l_2} = -\zeta^{l_1}$, then

$$\zeta^{l_3} = \zeta^{l_1}+\zeta^{l_2}+\zeta^{l_3} = \zeta^{l_1}\zeta^{l_2}\zeta^{l_3} = -\zeta^{2l_1}\zeta^{l_3}.$$

Consequently, $(\zeta^{l_1})^2 = -1$. Thus $\zeta^{l_1} = \pm i$, which is impossible.

Acknowledgements. The authors wish to thank Bruce C. Berndt for his encouragement and H. Edgar for carefully reading our manuscript.

References

[1] E. Artin, *Theory of Algebraic Numbers*, Göttingen 1959.
[2] J. W. S. Cassels, *On a diophantine equation*, Acta Arith. 6 (1960), 47–52.
[3] R. A. Mollin, C. Small, K. Varadarajan and P. G. Walsh, *On unit solutions of the equation* $xyz = x+y+z$ *in the ring of integers of a quadratic field*, ibid. 48 (1987), 341–345.
[4] W. Sierpiński, *On some unsolved problems of Arithmetics*, Scripta Math. 25 (1960), 125–136.
[5] — *Remarques sur le travail de M. J. W. S. Cassels "On a diophantine equation"*, Acta Arith. 6 (1961), 469–471.
[6] L. C. Zhang, *On the units of cubic and bicubic fields*, Acta Math. Sinica, New Series, 1 (1985), 22–34.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ILLINOIS
1409 West Green Street
Urbana, Illinois 61801
U.S.A.

Received on 27.6.1989 (1949)

ACTA ARITHMETICA
LVII (1991)

Note on a decomposition of integer vectors, II

by

S. Chaładus (Częstochowa) and Yu. Teterin (Leningrad)

The notation of this paper is that of [6]. For m linearly independent vectors $\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m \in \boldsymbol{Z}^k$, $H(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)$ denotes the maximum of the absolute values of all minors of order m of the matrix $\begin{pmatrix} \boldsymbol{n}_1 \\ \vdots \\ \boldsymbol{n}_m \end{pmatrix}$ and $D(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)$ the greatest common divisor of these minors. Furthermore

$$h(\boldsymbol{n}) = H(\boldsymbol{n}) \quad \text{for } \boldsymbol{n} \neq \boldsymbol{0}, \quad h(\boldsymbol{0}) = 0$$

and for $k \geqslant l \geqslant m$, $k > m$

$$c_0(k, l, m) = \sup \inf \left(\frac{D(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)}{H(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)} \right)^{(k-l)/(k-m)} \prod_{i=1}^{l} h(\boldsymbol{p}_i),$$

where the supremum is taken over all sets of linearly independent vectors $\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m \in \boldsymbol{Z}^k$ and the infimum is taken over all sets of linearly independent vectors $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_l \in \boldsymbol{Z}^k$ such that for all $i \leqslant m$

$$\boldsymbol{n}_i = \sum_{j=}^{l} u_{ij}\boldsymbol{p}_j, \quad u_{ij} \in \boldsymbol{Q}; \tag{1}$$

$\| \ \|$ denotes the usual Euclidean norm.

The aim of the paper is to prove the following two theorems.

Theorem 1. *For all integers k, l, m satisfying $k \geqslant l \geqslant m$, $k > m$ we have*

$$c_0(k, l, m) \leqslant \gamma_{k-m,k-l}^{1/2} \binom{k}{m}^{(k-l)/(2(k-m))}$$

where $\gamma_{k-m,k-l}$ is the Rankin constant (see [4]).

Theorem 2. *For all integers k, l, m satisfying $k \geqslant l \geqslant m$, $k > m$ and for every H there exist linearly independent vectors $\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m \in \boldsymbol{Z}^k$ such that*

$$\frac{H(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)}{D(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)} > H \tag{2}$$

and

$$\inf\left(\frac{D(n_1,\ldots,n_m)}{H(n_1,\ldots,n_m)}\right)^{(k-l)/(k-m)}\prod_{i=1}^{l}h(p_i)\geqslant l^{-l/2}. \tag{3}$$

The Rankin constant $\gamma_{n,m}$ $(0<m\leqslant n)$ can be defined as follows: let $d(f)$ denote the discriminant of a quadratic form f, i.e. the determinant of its matrix. Then $\gamma_{n,m}$ is the smallest constant with the property that each positive definite quadratic form f of rank n represents integrally some quadratic form g of rank m such that

$$0<d(g)\leqslant\gamma_{n,m}d(f)^{m/n}.$$

We define also

$$\gamma_{n,0}=\gamma_{n,n}=1.$$

The best known estimations of $\gamma_{n,m}$ are based on the relations (see [4])

$$\gamma_{n,m}=\gamma_{n,n-m},$$
$$\gamma_{n,m}\leqslant\gamma_{r,m}(\gamma_{n,r})^{m/r}\quad(m\leqslant r\leqslant n),$$
$$\gamma_{n,1}=\gamma_{n,n-1}=\gamma_n,$$
$$\gamma_{4,2}=3/2,$$

where γ_n is the Hermite constant. These relations imply

$$\gamma_{n,m}=\gamma_{n,n-m}\leqslant\Big(\prod_{i=m+1}^{n}\gamma_i^{1/(i-1)}\Big)^m.$$

As a direct consequence of Minkowski's second theorem for quadratic forms we obtain also

$$\gamma_{n,m}=\gamma_{n,n-m}\leqslant\gamma_n^m.$$

For further estimates we can apply Blichfeldt's inequality

$$\gamma_n\leqslant\frac{2}{\pi}\Gamma\left(\frac{n}{2}+2\right)^{2/n}.$$

It can also be mentioned that the same relations imply Mordell's inequality $\gamma_n\leqslant\gamma_{n-1}^{(n-1)/(n-2)}$ by putting $m=1$, $r=n-1$.

Theorem 1 extends and improves the part of Theorem 1 of [5] not covered by Theorem 1 of [6], because it can be shown using the above estimates for $\gamma_{n,m}$ that

$$\gamma_{k-m,k-l}^{1/2}\binom{k}{m}^{(k-l)/(2(k-m))}$$
$$\leqslant\min\left\{\left(\frac{2}{\sqrt{\pi}}\right)^{l-m}\Gamma\left(\frac{k-m+2}{2}\right)^{(l-m)/(k-m)}\binom{k}{m}^{1/2},\ \gamma_{k-m}^{(k-l)/2}\binom{k}{m}^{(k-l)/(2(k-m))}\right\}.$$

The bound for $c_0(k,l,m)$ given in Theorem 1 is in some cases, e.g. for $k=4$, $l=2$, $m=1$ better than the bound given in Theorem 1 of [6].

Theorem 2 shows that the exponent $(k-l)/(k-m)$ occurring in the definiton of $c_0(k,l,m)$ is the correct one (for any smaller exponent the corresponding supremum is infinite) and thus extends the result of [2] concerning the case $m=1$.

Proof of Theorem 1. Let $\mathcal{N}$ be the linear subspace of $\boldsymbol{R}^k$ spanned by $\boldsymbol{n}_1,\ldots,\boldsymbol{n}_m$, $\mathcal{F}$ the orthogonal complement of $\mathcal{N}$ in $\boldsymbol{R}^k$, and $\boldsymbol{a}_1,\ldots,\boldsymbol{a}_{k-m}$ a basis of the lattice $\boldsymbol{Z}^k\cap\mathcal{F}$ and $\boldsymbol{A}=\begin{pmatrix}\boldsymbol{a}_1\\ \vdots\\ \boldsymbol{a}_{k-m}\end{pmatrix}$. Then by a known theorem (see [3], p. 53)

$$D(\boldsymbol{a}_1,\ldots,\boldsymbol{a}_{k-m})=1.$$

By the Gordan theorem (see [1], p. 28) the absolute values of the minors of order $k-m$ of the matrix $\boldsymbol{A}$ are proportional in some order to the absolute values of the minors of order m of the matrix $\begin{pmatrix}\boldsymbol{n}_1\\ \vdots\\ \boldsymbol{n}_m\end{pmatrix}$. Hence

$$H(\boldsymbol{a}_1,\ldots,\boldsymbol{a}_{k-m})=\frac{H(\boldsymbol{n}_1,\ldots,\boldsymbol{n}_m)}{D(\boldsymbol{n}_1,\ldots,\boldsymbol{n}_m)}.$$

Let us consider the positive definite quadratic form

$$f(x_1,\ldots,x_{k-m})=\|x_1\boldsymbol{a}_1+\ldots+x_{k-m}\boldsymbol{a}_{k-m}\|^2.$$

By the Cauchy–Binet formula

$$d(f)=\det\boldsymbol{A}\boldsymbol{A}^t=\sum M^2,$$

where M runs through all minors of order $k-m$ of $\boldsymbol{A}$. Hence

$$d(f)\leqslant\binom{k}{k-m}H(\boldsymbol{a}_1,\ldots,\boldsymbol{a}_{k-m})^2=\binom{k}{m}\frac{H(\boldsymbol{n}_1,\ldots,\boldsymbol{n}_m)^2}{D(\boldsymbol{n}_1,\ldots,\boldsymbol{n}_m)^2}. \tag{4}$$

By the definition of $\gamma_{n,m}$ there exist linearly independent vectors $\boldsymbol{b}_1,\ldots,\boldsymbol{b}_{k-l}\in\boldsymbol{Z}^k\cap\mathcal{F}$ such that the quadratic form

$$g(x_1,\ldots,x_{k-l})=\|x_1\boldsymbol{b}_1+\ldots+x_{k-l}\boldsymbol{b}_{k-l}\|^2$$

has determinant

$$d(g)\leqslant\gamma_{k-m,k-l}d(f)^{(k-l)/(k-m)}. \tag{5}$$

Let $\boldsymbol{B}=\begin{pmatrix}\boldsymbol{b}_1\\ \vdots\\ \boldsymbol{b}_{k-l}\end{pmatrix}$, $\mathcal{G}$ be the linear space spanned by $\boldsymbol{b}_1,\ldots,\boldsymbol{b}_{k-l}$ and $\mathcal{P}$ be the orthogonal complement of $\mathcal{G}$ in $\boldsymbol{R}^k$. Then

(6) $$\mathscr{G} \subseteq \mathscr{F}, \quad \mathscr{P} \supseteq \mathscr{N}.$$

By Theorem 2 of [1], $\mathscr{P}$ is spanned by linearly independent vectors $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_l \in \boldsymbol{Z}^k$ such that

(7) $$\prod_{i=1}^{l} h(\boldsymbol{p}_i) \leqslant \sqrt{|\det \boldsymbol{B}\,\boldsymbol{B}^t|} = d(g)^{1/2}.$$

Inequalities (4), (5), (7) imply

$$\prod_{i=1}^{l} h(\boldsymbol{p}_i) \leqslant \gamma_{k-m,k-l}^{1/2} \binom{k}{m}^{(k-l)/(2(k-m))} \left(\frac{H(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)}{D(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)}\right)^{(k-l)/(k-m)}$$

and (6) implies (1). Hence by the definition of $c_0(k, l, m)$

$$c_0(k, l, m) \leqslant \gamma_{k-m,k-l}^{1/2} \binom{k}{m}^{(k-l)/(2(k-m))}$$

and the proof of Theorem 1 is complete.

In order to prove Theorem 2 we introduce the following notation.

For a matrix $\boldsymbol{P} \in \mathscr{M}_{l,k}(\boldsymbol{Z})$ we denote by $\boldsymbol{P}(j_1, j_2, \ldots, j_{k-l})$ the square matrix of order l obtained from $\boldsymbol{P}$ by omitting the columns $j_1 < j_2 < \ldots < j_{k-l}$ and by $SQ(\boldsymbol{P})$ the set of the matrices $\boldsymbol{P}(j_1, j_2, \ldots, j_{k-l})$ corresponding to all sequences $j_1, j_2, \ldots, j_{k-l}$ such that $1 \leqslant j_1 < j_2 < \ldots < j_{k-l} \leqslant k$.

Let us order the set $SQ(\boldsymbol{P})$ lexicographically, i.e. let $\boldsymbol{P}(j_1, j_2, \ldots, j_{k-l})$ precedes $\boldsymbol{P}(j'_1, j'_2, \ldots, j'_{k-l})$ if the first nonzero difference $j'_s - j_s$, $s = 1, 2, \ldots, k-l$, is positive. Finally, let $\boldsymbol{A} \in \mathscr{M}_{l+1,k}$ be the matrix obtained from $\boldsymbol{P}$ by adding the vector $\boldsymbol{n} = [1, n, \ldots, n^{t-1}, 0, \ldots, 0] \in \boldsymbol{Z}^k$ $(t \leqslant k)$ as the first row.

LEMMA. *Let $1 \leqslant i_1 < i_2 < \ldots < i_{k-l} \leqslant t$. If the rank of $\boldsymbol{A}$ is at most l and every matrix in $SQ(\boldsymbol{P})$ which precedes $\boldsymbol{P}(i_1, i_2, \ldots, i_{k-l})$ is singular then for every $s = 0, 1, \ldots, k-l$ and every sequence $j_{s+1}, j_{s+2}, \ldots, j_{k-l}$ of positive integers such that*

$$i_s < j_{s+1} < j_{s+2} < \ldots < j_{k-l} \leqslant k$$

we have

(8) $$\det \boldsymbol{P}(i_1, \ldots, i_s, j_{s+1}, \ldots, j_{k-l}) \equiv 0 \pmod{n^s}.$$

In particular

$$\det \boldsymbol{P}(i_1, i_2, \ldots, i_{k-l}) \equiv 0 \pmod{n^{k-l}}.$$

Proof. We proceed by induction on s. The case $s = 0$ is obvious. If $l = k$ we put $SQ(\boldsymbol{P}) = \{\boldsymbol{P}\}$. Assume that our lemma is true with s replaced by $s-1$. Let us apply to the matrix $\boldsymbol{A}(i_1, \ldots, i_{s-1}, j_{s+1}, \ldots, j_{k-l})$ the Laplace expansion with respect to the first row. In the expansion the summands involving determinants of the matrices preceding $\boldsymbol{P}(i_1, i_2, \ldots, i_s, j_{s+1}, \ldots, j_{k-l})$ are equal to zero. Leaving out of account these summands we obtain

$$\begin{aligned}
0 &= \det \boldsymbol{A}(i_1, \ldots, i_{s-1}, j_{s+1}, \ldots, j_{k-l}) \\
&= (-1)^{i_s - s} n^{i_s - 1} \det \boldsymbol{P}(i_1, \ldots, i_s, j_{s+1}, \ldots, j_{k-l}) \\
&\quad + \sum_{r=i_s+1}^{\min\{t, j_{s+1}-1\}} (-1)^{r-s} n^{r-1} \det \boldsymbol{P}(i_1, \ldots, i_{s-1}, r, j_{s+1}, \ldots, j_{k-l}) \\
&\quad + \sum_{\sigma=s+1}^{k-l} \sum_{r=j_\sigma+1}^{\min\{t, j_{\sigma+1}-1\}} (-1)^{r-\sigma} n^{r-1} \det \boldsymbol{P}(i_1, \ldots, i_{s-1}, j_{s+1}, \ldots, j_\sigma, r, j_{\sigma+1}, \ldots, j_{k-l}),
\end{aligned}$$

where by convention $j_{k-l+1} = k+1$. The determinants that occur in either sum are divisible by n^{s-1}, by the inductive assumption. Hence

$$n^{i_s - 1} \det \boldsymbol{P}(i_1, \ldots, i_s, j_{s+1}, \ldots, j_{k-l}) \equiv 0 \pmod{n^{i_s + s - 1}}$$

and (8) follows.

Remark. The above proof follows the proof of the lemma in [2], which corresponds to the case $t = k$.

Proof of Theorem 2. We define the vectors $\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m$ as follows:

$$\boldsymbol{n}_1 = [1, n, \ldots, n^{k-m}, 0, \ldots, 0], \quad \boldsymbol{n}_i = [\underbrace{0, \ldots, 0, 1}_{k-m+i}, 0, \ldots, 0] \quad (2 \leqslant i \leqslant m),$$

where $n > H$ is a positive integer. Clearly

(9) $$H(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m) = n^{k-m}, \quad D(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m) = 1,$$

thus (2) is satisfied. Suppose that linearly independent vectors $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_l \in \boldsymbol{Z}^k$ satisfy (1) and put

$$\boldsymbol{P} = \begin{bmatrix} \boldsymbol{p}_1 \\ \vdots \\ \boldsymbol{p}_l \end{bmatrix}, \quad \boldsymbol{A}_i = \begin{bmatrix} \boldsymbol{n}_i \\ \boldsymbol{p}_1 \\ \vdots \\ \boldsymbol{p}_l \end{bmatrix} \quad (1 \leqslant i \leqslant m).$$

The matrix $\boldsymbol{P}$ is of rank l and so by (1) are $\boldsymbol{A}_i$ $(1 \leqslant i \leqslant m)$. Let $\boldsymbol{P}(i_1, i_2, \ldots, i_{k-l})$ be the first non-singular matrix in $SQ(\boldsymbol{P})$. If $i_{k-l} > k-m+1$ we expand $\det \boldsymbol{A}_{i_{k-l}-k+m}(i_1, i_2, \ldots, i_{k-l-1})$ with respect to the first row and obtain

$$0 = \det \boldsymbol{A}_{i_{k-l}-k+m}(i_1, i_2, \ldots, i_{k-l-1}) = (-1)^{i_{k-l}-k+l} \boldsymbol{P}(i_1, i_2, \ldots, i_{k-l}),$$

thus since the right hand side is different from zero, we have a contradiction. Therefore, $i_{k-l} \leqslant k-m+1$ and applying Lemma with $\boldsymbol{A} = \boldsymbol{A}_1$, $t = k-m+1$ we obtain

$$\det \boldsymbol{P}(i_1, i_2, \ldots, i_{k-l}) \equiv 0 \pmod{n^{k-l}},$$

$$|\det \boldsymbol{P}(i_1, i_2, \ldots, i_{k-l})| \geqslant n^{k-l}.$$

Hence, by the Hadamard inequality and by (9)

$$l^{l/2}\prod_{i=1}^{l} h(\boldsymbol{p}_i) \geqslant n^{k-l} = \left(\frac{H(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)}{D(\boldsymbol{n}_1, \ldots, \boldsymbol{n}_m)}\right)^{(k-l)/(k-m)}$$

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 $K\left(a_0 + \sum_{i=1}^{k} a_i x^{n_i}\right)$ 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, $\alpha_i (0 \leqslant i \leqslant k)$ 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 $\boldsymbol{\gamma} \in \boldsymbol{Z}^k$ such that

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

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 $\boldsymbol{r}_i \boldsymbol{q} = 0 (1 \leqslant i \leqslant 3)$,

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