COLLOQUIUM MATHEMATICUM

VOL. XXX 1974 FASC. 1

ON RATIONAL AUTOMORPHS OF QUADRATIC FORMS

BY

J. WÓJCIK (WARSZAWA)

1. The aim of this paper is to study lattices with the following property: the matrix formed by basic points of the lattice corresponds to a rational automorph of a quadratic form.

Definitions and notations. C_n is the n-dimensional Euclidean space. Points of C_n will be denoted by bold face letters, e.g. $\boldsymbol{x}, \boldsymbol{y}$, and treated as matrices with one column, e.g.

$$\boldsymbol{a} = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}.$$

$(\boldsymbol{x}, \boldsymbol{y})$ denotes the scalar product of $\boldsymbol{x}, \boldsymbol{y}$.

$A = [\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n]$ is the matrix whose i-th column is the point $\boldsymbol{a}_i$. If A is a matrix, then A^T is a transposed matrix. Lattices occurring in the paper are contained in C_n unless explicitly stated. A lattice K is *complete* if its basis consists of n points. In such a case, $d(K)$ is the *determinant* of K. A lattice is called *rational* or *integral* if its points are rational or integral, respectively. For $\boldsymbol{a}$ and b integral, the symbol $(\boldsymbol{a}, b) = 1$ means that numbers $a_1, \ldots, a_n, b$, where a_i's are coordinates of $\boldsymbol{a}$, are relatively prime. If K is a rational lattice, the least positive integer d such that the lattice dK is integral, where dK is the set of points $d\boldsymbol{a}$ with $\boldsymbol{a} \in K$, is called the *denominator* of K. Analogously define the denominator of a rational matrix. If d is the denominator of K, then $\boldsymbol{x}/d \in K$ is called a *generic point* of K when $(\boldsymbol{x}, d) = 1$. Every rational lattice has a generic point. Indeed, if

$$d = \prod_{i=1}^{r} p_i^{\nu_i}$$

is the denominator of a lattice K, then there exists a point $\boldsymbol{x}_i/d \in K$ such that $(\boldsymbol{x}_i, p_i) = 1$. Otherwise, the lattice $(d/p_i)K$ would be integral. It

follows that

$$\frac{1}{d}(p_2 \dots p_r x_1 + p_1 p_3 \dots p_r x_2 + \dots + p_1 \dots p_{r-1} x_r)$$

is a generic point of K.

$f(x)$ denotes an integral quadratic form in n variables, and $f(x, y)$ the corresponding bilinear form.

Z denotes the lattice of integral points of C_n. If a matrix A has n columns, then AZ denotes the lattice consisting of points Az, where $z \in Z$. If a matrix A is orthogonal (e.g. if it is an automorph of the quadratic form $\sum_{i=1}^{n} x_i^2$), then the lattice AZ is called *orthonormal*. It is simply a complete lattice with an orthonormal basis.

$\boldsymbol{Z}$ denotes the set of rational integers. If $\Lambda \subset M$, $[M:\Lambda]$ denotes the index of Λ in M.

The following theorem holds:

THEOREM 1. *Let $1 \leqslant n \leqslant 3$. A rational lattice is orthonormal if and only if it is of the form $M + \boldsymbol{Z}x$, where x is a rational point, $(x, x) \in \boldsymbol{Z}$, $M = \{u \in Z \mid (u, x) \in \boldsymbol{Z}\}$.*

LEMMA 1. *Assume that the discriminant of a quadratic form f is square-free and let x_0 be a rational point with $f(x_0) \in \boldsymbol{Z}$. Let $M = \{u \in Z \mid f(u, x_0) \in \boldsymbol{Z}\}$. The lattice $M + \boldsymbol{Z}x_0$ has the discriminant 1 and, for any two points of this lattice, the value of the bilinear form f is integral.*

Proof. If $u + tx_0$ and $v + sx_0 \in M + \boldsymbol{Z}x_0$, then

$$f(u + tx_0, v + sx_0) = f(u, v) + tf(x_0, v) + sf(u, x_0) + tsf(x_0) \in \boldsymbol{Z},$$

because of the definition of M. Clearly,

$$[M + \boldsymbol{Z}x_0 : M] = d, \tag{1}$$

where d is the least common denominator of the coordinates of x_0.

By Lemma 9 in Chapter III in [1], $[Z:M] \leqslant d$. Hence, by (1),

$$d(M + \boldsymbol{Z}x_0) \leqslant 1. \tag{2}$$

Apply to f the linear transformation

$$x = y_1 a_1 + \dots + y_n a_n = Ay,$$

where

$$A = [a_1, \dots, a_n], \qquad y = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix},$$

and the points $a_1, \ldots, a_n$ form a basis of $M + \boldsymbol{Z}x_0$. Then

$$f(x) = f(x, x) = f\Big(\sum_{i=1}^{n} y_i a_i, \sum_{j=1}^{n} y_j a_j\Big) = \sum_{i,j=1}^{n} f(a_i, a_j) y_i y_j \stackrel{\text{def}}{=} g(y).$$

In virtue of the final part of the lemma already proved, coefficients of the quadratic form g are integral. Put $d(M + \boldsymbol{Z}x_0) = |\det A| = a/b$, a, b positive integers, and $(a, b) = 1$. Hence

$$\det g = (\det A)^2 \det f = a^2 \det f / b^2 \in \boldsymbol{Z}, \qquad b^2 | \det f.$$

$b = 1$, since $\det f$ is squarefree. Thus $d(M + \boldsymbol{Z}x_0) = a \geqslant 1$. Hence, by (2), $d(M + \boldsymbol{Z}x_0) = 1$.

LEMMA 2. *Let $1 \leqslant n \leqslant 7$ and let x be a rational point such that $(x, x) \in \boldsymbol{Z}$. Then the lattice $M + \boldsymbol{Z}x$, where $M = \{u \in Z \mid (u, x) \in \boldsymbol{Z}\}$, is orthonormal.*

Proof. We have

$$M + \boldsymbol{Z}x = BZ \quad \text{for some rational matrix } B. \tag{3}$$

The quadratic form $(B\xi, B\xi)$ is positive-definite. Its discriminant equals 1, since the form is obtained from (η, η) by the substitution $\eta = B\xi$ and $|\det B| = 1$ by Lemma 1. Coefficients of the form are integral, since the value of the bilinear form $(B\xi, B\eta)$ is integral for any integral ξ, η by Lemma 1. By the well-known Hermite Theorem, there exists a unimodular matrix A such that $(BAz, BAz) = (z, z)$. It follows that the matrix BA is orthogonal. We have $Z = AZ$ since A is unimodular. Hence and by (3), we obtain $M + \boldsymbol{Z}x = BZ = BAZ$.

Proof of Theorem 1. In view of Lemma 2, it is enough to prove the necessity of the condition.

Let x be a generic point of an orthonormal lattice K. It suffices to show that, for every point a of K, there exists an integral point u and an integer t such that $a = u + tx$. Indeed, the scalar product $(x, x) \in \boldsymbol{Z}$, $u \in K$, and $(u, x) \in \boldsymbol{Z}$, since K is orthonormal. Thus $K \subset M + \boldsymbol{Z}x$. Since by Lemma 1 the determinants of both lattices are equal 1, $K = M + \boldsymbol{Z}x$.

1. $n = 1$. It suffices to take $t = 0$ and $u = a$.

2. $n = 2$. Let

$$x = \begin{bmatrix} x/d \\ y/d \end{bmatrix}, \qquad x, y, d \in \boldsymbol{Z}, \ (x, y, d) = 1,$$

d being the denominator of K, and let

$$a = \begin{bmatrix} a/d \\ b/d \end{bmatrix}, \qquad \text{where } a, b \in \boldsymbol{Z}.$$

Since the scalar products $(x, x), (a, x) \in \boldsymbol{Z}$, we have

$$x^2 + y^2 \equiv 0 \pmod{d^2}, \qquad ax + by \equiv 0 \pmod{d^2}. \tag{4}$$

Since $(x, y, d) = 1$, we get

$$(x, d) = (y, d) = 1. \tag{5}$$

Let t be a solution of the congruence

$$a \equiv tx \pmod{d}. \tag{6}$$

It follows, by (4) and (5), that $tx^2 + by \equiv 0 \pmod{d}$, $by \equiv ty^2 \pmod{d}$, and $b \equiv ty \pmod{d}$. Hence, by (6),

$$\boldsymbol{a} = \begin{bmatrix} a/d \\ b/d \end{bmatrix} = \begin{bmatrix} u + t(x/d) \\ v + t(y/d) \end{bmatrix} = \boldsymbol{u} + t\boldsymbol{x}, \quad \text{where } \boldsymbol{u} = \begin{bmatrix} u \\ v \end{bmatrix}, \ u, v \in \boldsymbol{Z}.$$

3. $n = 3$. Let

$$\boldsymbol{x} = \begin{bmatrix} x/d \\ y/d \\ z/d \end{bmatrix}, \quad x, y, z, d \in \boldsymbol{Z}, \ (x, y, z, d) = 1,$$

d being the denominator of K. We have

$$\boldsymbol{a} = \begin{bmatrix} a/d \\ b/d \\ c/d \end{bmatrix}, \quad a, b, c \in \boldsymbol{Z}.$$

Since the scalar products $(\boldsymbol{x}, \boldsymbol{x})$, $(\boldsymbol{a}, \boldsymbol{x})$, $(\boldsymbol{a}, \boldsymbol{a}) \in \boldsymbol{Z}$, we have

$$\begin{aligned} x^2 + y^2 + z^2 &\equiv 0 \pmod{d^2}, \\ ax + by + cz &\equiv 0 \pmod{d^2}, \\ a^2 + b^2 + c^2 &\equiv 0 \pmod{d^2}. \end{aligned} \tag{7}$$

Let

$$p^\nu \| d, \quad \nu > 0, \ p \text{ prime}. \tag{8}$$

Since $(x, y, z, d) = 1$, we can assume that

$$p \nmid x. \tag{9}$$

Let $t(p)$ be a solution of the congruence

$$a \equiv t(p)x \pmod{p^{2\nu}}. \tag{10}$$

It follows, by (7), that

$$t(p)x^2 + by + cz \equiv 0 \pmod{p^{2\nu}}, \quad t^2(p)x^2 + b^2 + c^2 \equiv 0 \pmod{p^{2\nu}}.$$

Hence, by the first congruence of (7), we get a system of congruences

$$by + cz \equiv t(p)A \pmod{p^{2\nu}}, \quad b^2 + c^2 \equiv t^2(p)A \pmod{p^{2\nu}},$$

where $A = y^2 + z^2$.

Multiplying the last congruence by z^2, taking $cz \equiv t(p)A - by \pmod{p^{2\nu}}$, and using the fact that $p \nmid A$, we get, by (7) and (9), after some transformations,

$$(b - t(p)y)^2 \equiv 0 \pmod{p^{2\nu}}, \quad b \equiv t(p)y \pmod{p^\nu}. \tag{11}$$

Analogously,

$$c \equiv t(p)z \pmod{p^\nu}. \tag{12}$$

From (10) we get

$$a \equiv t(p)x \pmod{p^\nu}. \tag{13}$$

Put $t \equiv t(p) \pmod{p^\nu}$ for each p satisfying (8). It follows, by (13), (11) and (12), that $a \equiv tx \pmod{d}$, $b \equiv ty \pmod{d}$, and $c \equiv tz \pmod{d}$. We have

$$\boldsymbol{a} = \begin{bmatrix} a/d \\ b/d \\ c/d \end{bmatrix} = \begin{bmatrix} u + t(x/d) \\ v + t(y/d) \\ w + t(z/d) \end{bmatrix} = \boldsymbol{u} + t\boldsymbol{x}, \quad \text{where } \boldsymbol{u} = \begin{bmatrix} u \\ v \\ w \end{bmatrix}, \ u, v, w \in \boldsymbol{Z}.$$

The proof of Theorem 1 is complete.

Theorem 1 implies easily the following

COROLLARY 1. *Let $1 \leqslant n \leqslant 3$. For every rational point $\boldsymbol{x}$ such that $(\boldsymbol{x}, \boldsymbol{x}) \in \boldsymbol{Z}$, there exists exactly one orthonormal lattice for which $\boldsymbol{x}$ is a generic point.*

Proof. One such lattice is $M + \boldsymbol{Z}\boldsymbol{x}$, where $M = \{\boldsymbol{u} \in Z \mid (\boldsymbol{u}, \boldsymbol{x}) \in \boldsymbol{Z}\}$. On the other hand, an orthonormal lattice for which $\boldsymbol{x}$ is a generic point must be of this form, since for $\boldsymbol{x}$ in Theorem 1 one can take any generic point of the lattice, as is clear from the proof of this theorem. An application of Lemmas 1 and 2 to some diophantine equations is given in Section 3.

2. Let K be an arbitrary lattice, and K_0 its sublattice consisting of all integral points of K. The factor group of K modulo K_0 will be called, briefly, the *factor group of* K, and the corresponding cosets — the *cosets of* K. We call K *cyclic* if its factor group is cyclic (see Jones [2]). The lattice $M + \boldsymbol{Z}\boldsymbol{x}$, where $M = \{\boldsymbol{u} \in Z \mid f(\boldsymbol{u}, \boldsymbol{x}) \in \boldsymbol{Z}\}$, $f(\boldsymbol{x}) \in \boldsymbol{Z}$, and $\boldsymbol{x}$ is rational, will be called *cyclic induced by the quadratic form* f.

It is clear from Lemma 1 and Lemma 4 below that this lattice K has the following properties:

(i) $\boldsymbol{x}$ is a generic point of K;

(ii) K is cyclic;

(iii) the value of the bilinear form for any two points of K is integral and contains every rational lattice with the same properties.

Lemma 2 asserts that if $n \leqslant 7$, then every cyclic lattice induced by the sum of n squares is orthonormal, and Theorem 1 says that if $n \leqslant 3$,

then orthonormal lattices coincide with cyclic lattices induced by

$$f = \sum_{i=1}^{n} x_i^2.$$

A connection of cyclic lattices induced by a form f with rational automorphs of f is the main object of this section. Namely, we establish the following two theorems:

THEOREM 2. *Let $A_1, \ldots, A_m$ be rational matrices such that the product $A_1 \ldots A_m$ is defined. Assume the denominators of matrices A_i $(1 \leqslant i \leqslant m)$ are relatively prime in pairs. If lattices $A_i Z$ $(1 \leqslant i \leqslant m)$ are cyclic, then the lattice $A_1 \ldots A_m Z$ is also cyclic.*

THEOREM 3. *Let $S = U_1 \ldots U_m$ be the factorization of a rational automorph S of a form f into rational reflexions. If the denominators of reflexions U_i $(1 \leqslant i \leqslant m)$ are relatively prime in pairs, then the lattice SZ is cyclic, and if, besides, the discriminant of f is squarefree, the lattice is cyclic induced by f.*

Theorem 3 is in a sense a converse to Lemma 2 for a general form f. Proofs of Theorems 2 and 3 will be preceded by some lemmas.

LEMMA 3. *Let K be an arbitrary lattice. If there exists a point $\boldsymbol{y}$ such that $\boldsymbol{a} = \boldsymbol{v} + s\boldsymbol{y}$ for every $\boldsymbol{a} \in K$ and suitable integrals $\boldsymbol{v}$ and s, then K is cyclic.*

Proof. For $\boldsymbol{a} \in K$, denote by $\{\boldsymbol{a}\}$ the coset of $\boldsymbol{a}$. We have

$$\boldsymbol{a} = \boldsymbol{v} + s\boldsymbol{y}, \quad \boldsymbol{v}, s \text{ integral}. \tag{14}$$

Let s_0 be the least positive integer for which there exists a point $\boldsymbol{x} \in K$ such that

$$\boldsymbol{x} = \boldsymbol{v}_0 + s_0\boldsymbol{y}, \quad \boldsymbol{v}_0 \text{ integral}. \tag{15}$$

The expression s/s_0 must be integral. Otherwise, we should have $s = qs_0 + r$, $0 < r < s_0$, $q, r \in \boldsymbol{Z}$, $\boldsymbol{a} - q\boldsymbol{x} = \boldsymbol{v} - q\boldsymbol{v}_0 + r\boldsymbol{y} \in K$, contrary to the definition of s_0. By (14) and (15) we get $\boldsymbol{a} = \boldsymbol{u} + t\boldsymbol{x}$, where $\boldsymbol{u} = \boldsymbol{v} - (s/s_0)\boldsymbol{v}_0$, $t = s/s_0$ integral, $\boldsymbol{x} \in K$, $\boldsymbol{u} \in K$. It follows that $\{\boldsymbol{a}\} = t\{\boldsymbol{x}\}$.

LEMMA 4. *Let K be a cyclic rational lattice and $\boldsymbol{x}$ a generic point of it. For every $\boldsymbol{a} \in K$, there exists an integral point $\boldsymbol{u}$ and an integer t such that $\boldsymbol{a} = \boldsymbol{u} + t\boldsymbol{x}$.*

Proof. It is enough to show that the coset $\{\boldsymbol{x}\}$ generates the factor group of K. Let d be the denominator of K. The d cosets $t\{\boldsymbol{x}\}$, where $0 \leqslant t < d$, are distinct. There are no other cosets, since, for every $\boldsymbol{a} \in K$, the point $d\boldsymbol{a}$ is integral and K is cyclic.

LEMMA 5. *Assume that the discriminant of a quadratic form f is squarefree. If a rational complete lattice K is cyclic, its determinant equals* 1, *and*

if the value of the bilinear form f for any two points of K is integral, then the lattice K is cyclic induced by f.

Proof. Let $\{x\}$ be a generator of the factor group of K. Let $L = M + \mathbf{Z}x$, where $M = \{u \in Z \mid f(u, x) \in \mathbf{Z}\}$. According to the definition of x, we have, for an arbitrary $a \in K$, $a = u + tx$, where u and t integral, $u \in K$. Hence $f(u, x) \in \mathbf{Z}$ and $K \subset L$. Since $x \in K$, x is rational, and $f(x) \in \mathbf{Z}$, we have, by Lemma 1, $d(K) = d(L) = 1$. This gives $K = L$.

LEMMA 6. *Assume that the discriminant of f is squarefree and let S be a rational automorph of f. If the lattice SZ is cyclic, then it is cyclic included by f.*

Proof. It is well known that the lattice SZ has the discriminant 1 and the value of the bilinear form f for any two of its points is integral. Lemma 6 follows now from Lemma 5.

LEMMA 7. *Let A be a rational matrix. If the lattice AZ is cyclic, then the lattice A^TZ is also cyclic.*

Proof. Let

$$A = [a_1, \ldots, a_n],$$

where

$$a_i = u_i + t_i x$$

with

$$x = \begin{bmatrix} x_1/d \\ \vdots \\ x_m/d \end{bmatrix}, \quad u_i = \begin{bmatrix} u_{i1} \\ \vdots \\ u_{im} \end{bmatrix}, \quad u_{ij}, x_i, d, t_i \in \mathbf{Z}.$$

Let

$$A^T = [b_1, \ldots, b_m],$$

where

$$b_i = v_i + x_i y,$$

with

$$y = \begin{bmatrix} t_1/d \\ \vdots \\ t_n/d \end{bmatrix}, \quad v_i = \begin{bmatrix} u_{1i} \\ \vdots \\ u_{ni} \end{bmatrix} \quad (1 \leqslant i \leqslant m).$$

For $a = a_1 b_1 + \ldots + a_m b_m$, $a_i \in \mathbf{Z}$, we get $a = v + sy$, where $v = a_1 v_1 + \ldots + a_m v_m$ and $s = a_1 x_1 + \ldots + a_m x_m$ are integral. The assertion of Lemma 7 follows now from Lemma 3.

LEMMA 8. *Let A and B be rational matrices for which the product BA is defined. Let d_1 and d_2 be the denominators of lattices AZ and B^TZ, respectively, and $\bar{x}/d_1$ and $\bar{y}/d_2$ their respective generic points. Assume that $((\bar{x}, \bar{y}), d_1, d_2) = 1$. If the lattices AZ and B^TZ are cyclic, then the lattice BAZ is also cyclic.*

Proof. Let p be a prime satisfying the condition

$$p^{\nu} \| d_1 d_2, \quad \nu > 0. \tag{16}$$

Let

$$B^T = [\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n]. \tag{17}$$

By Lemma 4,

$$\boldsymbol{b}_i = \boldsymbol{v}_i + s_i(\bar{\boldsymbol{y}}/d_2) = (d_2\boldsymbol{v}_i + s_i\bar{\boldsymbol{y}})/d_2, \quad \boldsymbol{v}_i, s_i \text{ integral}. \tag{18}$$

Put

$$\boldsymbol{y} = \begin{bmatrix} y_1/d_1d_2 \\ \vdots \\ y_n/d_1d_2 \end{bmatrix},$$

where y_i are integers satisfying the condition

$$y_i \equiv \begin{cases} d_2(\boldsymbol{v}_i, \bar{\boldsymbol{x}}) + s_i(\bar{\boldsymbol{y}}, \bar{\boldsymbol{x}}) \pmod{p^{\nu}} & \text{if } p \nmid (\bar{\boldsymbol{y}}, \bar{\boldsymbol{x}}) \text{ or } p \nmid d_2, \\ s_i \pmod{p^{\nu}} & \text{if } p \mid (\bar{\boldsymbol{y}}, \bar{\boldsymbol{x}}) \text{ and } p \mid d_2, \end{cases} \tag{19}$$

for each p satisfying (16). Let

$$\boldsymbol{a} = BA\boldsymbol{z} = B\boldsymbol{b} = \begin{bmatrix} a_1/d_1d_2 \\ \vdots \\ a_n/d_1d_2 \end{bmatrix}, \quad \boldsymbol{z} \in Z, \ \boldsymbol{b} = A\boldsymbol{z}, \ a_i \in \boldsymbol{Z}.$$

It follows, by (17), that

$$a_i/d_1d_2 = (\boldsymbol{b}_i, \boldsymbol{b}). \tag{20}$$

By Lemma 4, $\boldsymbol{b} = \boldsymbol{u} + t(\bar{\boldsymbol{x}}/d_1) = (d_1\boldsymbol{u} + t\bar{\boldsymbol{x}})/d_1$, $\boldsymbol{u} \in Z$, $t \in \boldsymbol{Z}$. Hence, by (18) and (20), we get

$$\begin{aligned} a_i &= (d_2\boldsymbol{v}_i + s_i\bar{\boldsymbol{y}}, d_1\boldsymbol{u} + t\bar{\boldsymbol{x}}) \\ &= d_1d_2(\boldsymbol{v}_i, \boldsymbol{u}) + s_id_1(\bar{\boldsymbol{y}}, \boldsymbol{u}) + t[d_2(\boldsymbol{v}_i, \bar{\boldsymbol{x}}) + s_i(\bar{\boldsymbol{y}}, \bar{\boldsymbol{x}})]. \end{aligned} \tag{21}$$

Put

$$s \equiv \begin{cases} t + d_1(\bar{\boldsymbol{y}}, \boldsymbol{u})(\bar{\boldsymbol{y}}, \bar{\boldsymbol{x}})^{-1} \pmod{p^{\nu}} & \text{if } p \nmid (\bar{\boldsymbol{y}}, \bar{\boldsymbol{x}}), \\ t \pmod{p^{\nu}} & \text{if } p \mid (\bar{\boldsymbol{y}}, \bar{\boldsymbol{x}}), p \nmid d_2, \\ d_1(\bar{\boldsymbol{y}}, \boldsymbol{u}) + t(\bar{\boldsymbol{y}}, \bar{\boldsymbol{x}}) \pmod{p^{\nu}} & \text{if } p \mid (\bar{\boldsymbol{y}}, \bar{\boldsymbol{x}}), p \mid d_2, \end{cases} \tag{22}$$

for each p satisfying (16). For each p in question we have

$$p^{\nu} \mid d_1 \text{ for } p \nmid d_2; \quad p^{\nu} \mid d_2 \text{ for } p \mid (\bar{\boldsymbol{y}}, \bar{\boldsymbol{x}}), \ p \mid d_2. \tag{23}$$

Indeed, by the assumption, the condition $p \mid (\bar{\boldsymbol{y}}, \bar{\boldsymbol{x}})$, $p \mid d_2$, implies $p \nmid d_1$.

We get, by (19), (22), (23) and (21), for each p satisfying (16), $a_i \equiv sy_i \pmod{p^{\nu}}$, whence $a_i \equiv sy_i \pmod{d_1d_2}$, $a_i/d_1d_2 = v_i + sy_i/d_1d_2$, $v_i \in \boldsymbol{Z}$.

Taking

$$\boldsymbol{v} = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix},$$

we get $\boldsymbol{a} = \boldsymbol{v} + s\boldsymbol{y}$, where $\boldsymbol{v} \in Z$, $s \in \boldsymbol{Z}$. By Lemma 3, the lattice BAZ is cyclic.

Proof of Theorem 2. We proceed by induction on m. For $m = 1$, the theorem is obvious. Assume its validity for $m-1$, $m > 1$. Let $A_1, \ldots, A_m$ satisfy the assumptions of Theorem 2. By the inductive assumption, the lattice $BZ = A_2 \ldots A_m Z$ is cyclic. By Lemma 7, the lattice $A_1^T Z$ is also cyclic. Since the denominators of lattices $A_1^T Z$ and BZ are relatively prime, we infer, by Lemma 8, that the lattice $A_1 BZ$ is cyclic.

Proof of Theorem 3. It is enough to prove that a lattice UZ, where U denotes a rational reflexion of f, is cyclic. Indeed, in such a case, by Theorem 2, a lattice SZ is cyclic, and if the discriminant of f is squarefree, in virtue of Lemma 6, it is cyclic induced by f. Put

$$U = U(\boldsymbol{t}) = I - \boldsymbol{t}\boldsymbol{t}^T A / f(\boldsymbol{t}) = [\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n], \qquad \boldsymbol{t} = \begin{bmatrix} t_1 \\ \vdots \\ t_n \end{bmatrix}, \quad A = [a_{ji}],$$

where $f(\boldsymbol{t}) \neq 0$, $t_i \in \boldsymbol{Z}$, $a_{ij} \in \boldsymbol{Z}$, and I is the identity matrix (see [6], p. 11 and p. 123). We have $\boldsymbol{a}_i = \boldsymbol{v}_i + s_i \boldsymbol{y}$, where

$$\boldsymbol{y} = \begin{bmatrix} t_1/f(\boldsymbol{t}) \\ \vdots \\ t_n/f(\boldsymbol{t}) \end{bmatrix} \quad \text{and} \quad \boldsymbol{v}_i = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix}$$

with 1 appearing at i-th place, and $s_i = t_1 a_{1i} + \ldots + t_n a_{ni}$.

For $\boldsymbol{a} = b_1 \boldsymbol{a}_1 + \ldots + b_n \boldsymbol{a}_n$, $b_i \in \boldsymbol{Z}$, we get $\boldsymbol{a} = \boldsymbol{v} + s\boldsymbol{y}$, where $\boldsymbol{v} = b_1 \boldsymbol{v}_1 + \ldots + b_n \boldsymbol{v}_n \in Z$, and $s = b_1 s_1 + \ldots + b_n s_n \in \boldsymbol{Z}$. By Lemma 3, the lattice UZ is cyclic.

For an orthogonal matrix S, the matrix $S^T = S^{-1}$ is also orthogonal, hence, by Lemmas 7 and 6, we get

COROLLARY 2. *If S is a rational orthogonal matrix and the lattice SZ is cyclic induced by the form*

$$f = \sum_{i=1}^{n} x_i^2,$$

then the lattice $S^T Z = S^{-1} Z$ is also cyclic induced by f.

Remark 1. The assumption of Lemma 8 that $((\bar{x}, \bar{y}), d_1, d_2) = 1$ does not depend upon the choice of generic points. Indeed, if $\bar{\bar{x}}/d_1$ and

$\bar{\bar{y}}/d_2$ are also generic points of lattices AZ and B^TZ, respectively, then, by Lemma 4, $\bar{\bar{x}} = ud_1 + t\bar{x}$ and $\bar{\bar{y}} = vd_2 + s\bar{y}$, $u, v \in Z$, $s, t \in Z$. Since $(d_1, t) = (d_2, s) = 1$, we have

$$(\bar{\bar{x}}, \bar{\bar{y}}), d_1, d_2) = (ts(\bar{x}, \bar{y}), d_1 d_2) = ((\bar{x}, \bar{y}), d_1 d_2) = 1.$$

Remark 2. If the assumption of Theorem 3 is not satisfied, then the lattice SZ need not to be cyclic.

Example. Let $f(x) = x_1^2 + x_2^2 + x_3^2 + x_4^2$,

$$\bar{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x^4 \end{bmatrix}, \quad S = \begin{bmatrix} -\frac{1}{7} & -\frac{4}{7} & -\frac{4}{7} & -\frac{4}{7} \\ -\frac{4}{7} & \frac{1}{7} & \frac{4}{7} & -\frac{4}{7} \\ -\frac{4}{7} & \frac{4}{7} & -\frac{4}{7} & \frac{1}{7} \\ -\frac{4}{7} & -\frac{4}{7} & \frac{1}{7} & \frac{4}{7} \end{bmatrix} = U_1 U_2,$$

where

$$U_1 = \begin{bmatrix} -\frac{1}{7} & -\frac{4}{7} & -\frac{4}{7} & -\frac{4}{7} \\ -\frac{4}{7} & \frac{5}{7} & -\frac{2}{7} & -\frac{2}{7} \\ -\frac{4}{7} & -\frac{2}{7} & \frac{5}{7} & -\frac{2}{7} \\ -\frac{4}{7} & -\frac{2}{7} & -\frac{2}{7} & \frac{5}{7} \end{bmatrix} = U(t_1),$$

$$U_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{3}{7} & \frac{6}{7} & -\frac{2}{7} \\ 0 & \frac{6}{7} & -\frac{2}{7} & \frac{3}{7} \\ 0 & -\frac{2}{7} & \frac{3}{7} & \frac{6}{7} \end{bmatrix} = U(t_2),$$

$$t_1 = \begin{bmatrix} 2 \\ 1 \\ 1 \\ 1 \end{bmatrix} \quad \text{and} \quad t_2 = \begin{bmatrix} 0 \\ 2 \\ -3 \\ 1 \end{bmatrix}.$$

Lattices U_1Z and U_2Z have the common denominator 7. The point

$$x = \begin{bmatrix} -\frac{1}{7} \\ -\frac{4}{7} \\ -\frac{4}{7} \\ -\frac{4}{7} \end{bmatrix}$$

is a generic point of the lattice SZ. This lattice is not cyclic. For otherwise, since it contains the point

$$a = \begin{bmatrix} -\frac{4}{7} \\ \frac{1}{7} \\ \frac{4}{7} \\ -\frac{4}{7} \end{bmatrix},$$

we would have, by Lemma 4, $a = u + tx$, $u \in Z$, $t \in Z$. But the calculation of the first two coordinates gives $-4 = 7u_1 - t$ are $1 = 7u_2 - 4t$, $u_1 u_2 \in Z$, which is impossible.

3. We now give the promised applications to diophantine equations.

THEOREM 4. *Let $3 \leqslant n \leqslant 7$. For every positive integer m, there exist coprime positive integers $x_1, \ldots, x_n$ such that $m^2 = x_1^2 + \ldots + x_n^2$ except for the following cases:*

$n = 3$, $m \equiv 0 \pmod 2$, $m = 1, 5$;

$n = 4$, $m \equiv 0 \pmod 4$, $m = 1, 3$;

$n = 5$, $m = 1, 2, 3$;

$n = 6$, $m = 1, 2, 4$;

$n = 7$, $m = 1, 2, 3$.

This theorem can be deduced from the theorem of Gauss on sums of three squares and from the formula of Jacobi for the number of de-

compositions into sum of four squares. For $n = 3$, the theorem follows easily from Corollary 1 of [3] (see also [4]). However, the proof given here does not use these results and, moreover, it gives a method of construction of the required decomposition of m^2.

LEMMA 9. *Let $2 \leqslant n \leqslant 7$. Let p be a prime and let $\mu_2, \ldots, \mu_n$ and $a_2, \ldots, a_n$ be integers such that $\mu_i \geqslant 0$, $p \nmid a_i$,*

$$\left(-\sum_{i=2}^{n} p^{2\mu_i} a_i^2/p\right) = 1 \quad \text{for } p > 2,$$

where (a/p) is the symbol of Legendre,

$$-\sum_{i=2}^{n} p^{2\mu_i} a_i^2 \equiv 1 \pmod 8 \quad \text{for } p = 2.$$

Let a positive integer ν satisfy the inequality

$$\nu > \max_{2 \leqslant j \leqslant n,\, 0 \leqslant \xi < p^{\mu_j}} \left\{ \max\left(\mu_j, \operatorname{ord}_p \left[\left(\sum_{i=2}^{n} b_{j\xi i} p^{\mu_i} a_i \right)^2 + b_{j\xi}^2 \sum_{i=2}^{n} p^{2\mu_i} a_i^2 \right] - \mu_j \right) \right\}, \tag{24}$$

where

$$b_{j\xi}^2 + \sum_{i=2}^{n} b_{j\xi i}^2 = p^{2\mu_j}, \quad b_{j\xi} \neq 0, \quad b_{j\xi j} = 0, \quad b_{j\xi i} \equiv \xi p^{\mu_i} a_i \pmod{p^{\mu_j}}.$$

Then $p^{2\nu}$ is the sum of n squares of coprime positive integers.

Proof. The assumption together with the well-known properties of quadratic congruences implies the solvability of the congruence

$$x^2 + \sum_{i=2}^{n} p^{2\mu_i} a_i^2 \equiv 0 \pmod{p^{2\nu}}. \tag{25}$$

Put

$$\boldsymbol{x} = \begin{bmatrix} x/p^{\nu} \\ p^{\mu_2} a_2/p^{\nu} \\ \vdots \\ p^{\mu_n} a_n/p^{\nu} \end{bmatrix}.$$

Congruence (25) means that $(\boldsymbol{x}, \boldsymbol{x}) \in \boldsymbol{Z}$. Hence, in virtue of Lemma 2, the lattice $M + \boldsymbol{Z}\boldsymbol{x}$, where $M = \{\boldsymbol{u} \in Z \mid (\boldsymbol{u}, \boldsymbol{x}) \in \boldsymbol{Z}\}$, has an orthonormal basis. Let one of its elements be given by

$$\begin{bmatrix} (p^{\nu} u + t x)/p^{\nu} \\ (p^{\nu} u_2 + t p^{\mu_2} a_2)/p^{\nu} \\ \vdots \\ (p^{\nu} u_n + t p^{\mu_n} a_n)/p \end{bmatrix}, \tag{26}$$

where $u, u_j, t \in \mathbf{Z}$, $0 \leqslant t < p^\nu$, and, besides,

$$ux + \sum_{i=2}^{n} u_i p^{\mu_i} a_i \equiv 0 \pmod{p^\nu}. \tag{27}$$

We have

$$(p^\nu u + tx)^2 + \sum_{i=2}^{n} (p^\nu u_i + t p^{\mu_i} a_i)^2 = p^{2\nu}. \tag{28}$$

We prove that none of the terms occurring on the left-hand side of (28) can vanish. Let, e.g., $p^\nu u + tx = 0$. Hence, by (26) and $p \nmid x$, we have $t \equiv 0 \pmod{p^\nu}$, $t = 0$. After substitution into (28), we get

$$u^2 + \sum_{i=2}^{n} u_i^2 = 1.$$

If $u = \pm 1$, $u_j = 0$, $j = 2, \ldots, n$, then substituting into (27) we get $\pm x \equiv 0 \pmod{p^\nu}$, which is impossible.

If $u = 0$, $u_j = \pm 1$, $u_2 = \ldots = u_{j-1} = u_{j+1} = \ldots = u_n = 0$, then, analogously, we have $\pm p^{\mu_j} a_j \equiv 0 \pmod{p^\nu}$, which is impossible, since $\nu > \max(\mu_2, \ldots, \mu_n)$.

Thus we have

$$p^\nu u + tx \neq 0. \tag{29}$$

Assume now that

$$p^\nu u_j + t p^{\mu_j} a_j = 0 \quad \text{for a certain } j. \tag{30}$$

Hence, by (26), $p^{\nu-\mu_j} | t$, $t = \xi p^{\nu-\mu_j}$, $0 \leqslant \xi < p^{\mu_j}$. After substitution into (28) we have

$$(p^{\mu_j} u + \xi x)^2 + \sum_{i=2}^{n} (p^{\mu_j} u_i + \xi p^{\mu_i} a_i)^2 = p^{2\mu_j}. \tag{31}$$

Put

$$b_{j\xi} = p^{\mu_j} u + \xi x, \qquad b_{j\xi i} = p^{\mu_j} u_i + \xi p^{\mu_i} a_i. \tag{32}$$

Hence

$$u = (b_{j\xi} - \xi x)/p^{\mu_j}, \qquad u_i = (b_{j\xi i} - \xi p^{\mu_i} a_i)/p^{\mu_j}.$$

Substituting into (27), we have

$$(b_{j\xi} - \xi x)x + \sum_{i=2}^{n} (b_{j\xi i} - \xi p^{\mu_i} a_i) p^{\mu_i} a_i \equiv 0 \pmod{p^{\nu+\mu_j}}$$

or

$$b_{j\xi} x - \xi \left(x^2 + \sum_{i=2}^{n} p^{2\mu_i} a_i^2\right) + \sum_{i=2}^{n} b_{j\xi i} p^{\mu_i} a_i \equiv 0 \pmod{p^{\nu+\mu_j}}.$$

By the assumption $2v > v + \mu_j$, we have, in virtue of (25),

$$b_{j\xi}x + \sum_{i=2}^{n} b_{j\xi i}p^{\mu_i}a_i \equiv 0 \pmod{p^{v+\mu_j}}$$

or

$$b_{j\xi}^2x^2 \equiv \Big(\sum_{i=2}^{n} b_{j\xi i}p^{\mu_i}a_i\Big)^2 \pmod{p^{v+\mu_j}}.$$

On the other hand, in virtue of (25),

$$b_{j\xi}^2x^2 \equiv -b_{j\xi}^2\sum_{i=2}^{n} p^{2\mu_i}a_i^2 \pmod{p^{v+\mu_j}}.$$

Hence

$$0 < A_{j\xi} = \Big(\sum_{i=2}^{n} b_{j\xi i}p^{\mu_i}a_i\Big)^2 + b_{j\xi}^2\sum_{i=2}^{n} p^{2\mu_i}a_i^2 \equiv 0 \pmod{p^{v+\mu_j}}, \tag{33}$$

since $b_{j\xi} \neq 0$ by (29) and (32). In virtue of (30) and (32), $b_{j\xi j} = 0$ and $b_{j\xi i} \equiv \xi p^{\mu_i}a_i \pmod{p^{\mu_j}}$. By (31),

$$b_{j\xi}^2 + \sum_{i=2}^{n} b_{j\xi i}^2 = p^{2\mu_j}.$$

By (33), for some j, ξ, we infer that $v \leqslant \operatorname{ord}_p A_{j\xi} - \mu_j$, contrary to the assumption.

We have shown that the lattice $M + \boldsymbol{Z}\boldsymbol{x}$ has an orthonormal basis with non-zero coordinates. Let this basis consist of the points

$$\begin{bmatrix} a_{1i}/p^v \\ \vdots \\ a_{ni}/p^v \end{bmatrix}, \quad i = 1, \ldots, n.$$

Since the denominator of the lattice is p^v, we have $p \nmid a_{ij}$ for some i, j. Hence $p^{2v} = a_{1j}^2 + \ldots + a_{nj}^2$, $(a_{1j}, \ldots, a_{nj}) = 1$, $a_{kj} \neq 0$, $k = 1, \ldots, n$. The proof of the lemma is complete.

LEMMA 10. *Let $2 \leqslant n \leqslant 7$. If an odd prime p divides the sum of n squares of positive integers non-divisible by p, then, for every positive integer v, p^{2v} is the sum of n squares of coprime positive integers.*

Proof. Let $p \mid a_1^2 + \ldots + a_n^2$, $p \nmid a_i$, $i = 1, \ldots, n$. The numbers a_j, $\mu_j = 0$ $(2 \leqslant j \leqslant n)$ satisfy the assumptions of Lemma 9. The assertion of Lemma 10 follows, since the right-hand side of (24) equals 0.

LEMMA 11. *Let p be an odd prime, and k an integer non-divisible by p. Then there exist integers x, y such that $p \nmid xy$, $p \mid x^2 + y^2 + k$, except for the cases $p = 5$, $k \equiv \pm 1 \pmod 5$, and $p = 3$, $k \equiv -1 \pmod 3$.*

Proof. Let W be the number of quadratic residues in the sequence

$$0^2+k,\ 1^2+k,\ \ldots,\ (p-1)^2+k \tag{34}$$

if $p \equiv 1 \pmod 4$, and the number of quadratic non-residues if $p \equiv -1 \pmod 4$. We have to prove that $W > 1$.

Let R or N be the number of residues or non-residues modulo p, respectively, in sequence (34). It is well known that

$$\sum_{x=0}^{p-1}\left(\frac{x^2+k}{p}\right) = -1.$$

Hence

$$R = \begin{cases} \dfrac{p-3}{2} & \text{for } \left(\dfrac{-k}{p}\right) = 1, \\ \dfrac{p-1}{2} & \text{for } \left(\dfrac{-k}{p}\right) = -1, \end{cases} \qquad N = \begin{cases} \dfrac{p-1}{2} & \text{for } \left(\dfrac{-k}{p}\right) = 1, \\ \dfrac{p+1}{2} & \text{for } \left(\dfrac{-k}{p}\right) = -1. \end{cases}$$

Thus $W \geqslant (p-3)/2 > 1$ for $p > 5$.

If $p = 5$, $k \equiv \pm 2 \pmod 5$, then $W = R = 2 > 1$, and if $p = 3$, $k \equiv 1 \pmod 3$, then $W = N = 2 > 1$. The proof is complete.

LEMMA 12. *Theorem 4 holds for $m = p^\nu$, where p is a prime, and ν is a positive integer.*

Proof. Case 1. $p > 2$, $p \neq 5$ for $n = 3$, $p \neq 3$ for $n = 4, 5, 7$.

In virtue of Lemma 11, each of the following congruences is solvable in integers x and y non-divisible by p:

for $p \neq 5, 2$,

$$x^2+y^2+1 \equiv 0 \pmod p;$$

for $p > 3$,

$$x^2+y^2+2 = x^2+y^2+1^2+1^2 \equiv 0 \pmod p,$$

$$x^2+y^2+3 = x^2+y^2+1^2+1^2+1^2 \equiv 0 \pmod p,$$

$$x^2+y^2+27 = x^2+y^2+1^2+1^2+3^2+4^2 \equiv 0 \pmod p,$$

$$x^2+y^2+8 = x^2+y^2+1^2+1^2+1^2+1^2+2^2 \equiv 0 \pmod p.$$

Moreover, $1^2+1^2+1^2+1^2+1^2+1^2 \equiv 0 \pmod 3$.

The above-given congruences show that p divides the sum of n squares of positive integers non-divisible by p. In virtue of Lemma 10, $p^{2\nu}$ is the sum of n squares of coprime positive integers.

Case 2. $\nu > 2$; $p = 5$, $n = 3$; $p = 3$, $n = 4$. $\nu > 3$; $p = 2, 3$; $n = 5, 7$. $\nu > 6$; $p = 2$, $n = 6$.

Put

$$\mu_2 = 0,\ \mu_3 = a_2 = a_3 = 1 \quad \text{for } n = 3,\ p = 5,\ v > 2;$$

$$\mu_2 = \mu_3 = 0,\ a_2 = a_3 = a_4 = \mu_4 = 1 \quad \text{for } n = 4,\ p = 3,\ v > 2;$$

$$\mu_2 = \mu_3 = 0,\ \mu_4 = \mu_5 = a_2 = a_3 = a_4 = a_5 = 1 \quad \text{for } n = 5,\ p = 3,\ v > 3;$$

$$\mu_2 = \mu_3 = \mu_4 = 0,\ a_2 = a_3 = a_4 = a_5 = \mu_5 = 1 \quad \text{for } n = 5,\ p = 2,\ v > 3;$$

$$\mu_2 = \mu_3 = \mu_4 = 0,\ \mu_5 = a_2 = a_3 = a_4 = a_5 = a_6 = 1,\ \mu_6 = 2 \quad \text{for } n = 6,\ p = 2,\ v > 6;$$

$$\mu_2 = \mu_3 = \mu_4 = \mu_5 = \mu_6 = 0,\ a_2 = a_3 = a_4 = a_5 = a_6 = a_7 = \mu_7 = 1 \quad \text{for } n = 7,\ p = 3,\ v > 3;$$

$$\mu_2 = \mu_3 = \mu_4 = 0,\ \mu_5 = \mu_6 = \mu_7 = a_2 = a_3 = a_4 = a_5 = a_6 = a_7 = 1 \quad \text{for } n = 7,\ p = 2,\ v > 3.$$

As one can easily see, numbers a_j, μ_j, p and v satisfy the assumptions of Lemma 9. In virtue of that lemma, p^{2v} is the sum of n squares of coprime positive integers.

Case 3. $v = 1$, $p = 2$, $n = 4$. $v = 2$; $p = 5$, $n = 3$; $p = 3$, $n = 4$. $v = 2, 3$; $p = 2, 3$; $n = 5, 7$. $v = 3, 4, 5, 6$; $p = 2$, $n = 6$.

The following equalities complete the proof of the lemma:

$$2^2 = 1^2+1^2+1^2+1^2,\ 5^4 = 12^2+15^2+16^2,\ 3^4 = 2^2+2^2+3^2+8^3,$$

$$2^4 = 1^2+1^2+1^2+2^2+3^2,\ 2^6 = 1^2+1^2+1^2+5^2+6^2,$$

$$3^4 = 1^2+2^2+2^2+6^2+6^2,$$

$$3^6 = 1^2+2^2+12^2+16^2+18^2,\ 2^4 = 1^2+1^2+1^2+1^2+2^2+2^2+2^2,$$

$$2^6 = 1^2+1^2+1^2+2^2+2^2+2^2+7^2,\ 3^4 = 1^2+1^2+1^2+1^2+2^2+3^2+8^2,$$

$$3^6 = 1^2+1^2+1^2+1^2+1^2+18^2+20^2,\ 2^6 = 1^2+1^2+1^2+3^2+4^2+6^2,$$

$$2^8 = 1^2+1^2+1^2+3^2+10^2+12^2,\ 2^{10} = 1^2+1^2+3^2+4^2+6^2+31^2,$$

$$2^{12} = 1^2+3^2+5^2+10^2+31^2+60^2.$$

LEMMA 13. *Let $3 \leqslant n \leqslant 7$, p be a prime, and v a positive integer. Assume $p > 2$ for $n = 3$; $v = 1$ for $p = 2$, $n = 4$. Then p^{2v} is the sum of n squares of coprime integers.*

Proof. This is an immediate consequence of Lemma 12 and of the equalities $5^2 = 3^2+4^2$, $3^2 = 1^2+2^2+2^2$, $2^2 = 1^2+1^2+1^2+1^2$ and $2^4 = 1^2+1^2+1^2+1^2+2^2+3^2$.

LEMMA 14. *Let $2 \leqslant n \leqslant 7$, p be a prime, and v, d positive integers, $p \nmid d$. Assume that p^{2v} is the sum of n squares of coprime positive integers and d^2 is the sum of n squares of coprime integers. Then $p^{2v}d^2$ is the sum of n squares of coprime positive integers.*

Proof. Let

$$p^{2\nu} = y_1^2 + \ldots + y_n^2, \quad y_i > 0,\ i = 1, \ldots, n,\ (y_1, \ldots, y_n) = 1. \tag{35}$$

Put

$$\boldsymbol{y} = \begin{bmatrix} y_1/p^\nu \\ \vdots \\ y_n/p^\nu \end{bmatrix}.$$

Equality (35) means that $(\boldsymbol{y}, \boldsymbol{y}) = 1 \in \boldsymbol{Z}$. In virtue of Lemma 2, the lattice $M + \boldsymbol{Z}\boldsymbol{y}$, where $M = \{\boldsymbol{u} \in Z \mid (\boldsymbol{u}, \boldsymbol{y}) \in \boldsymbol{Z}\}$, has an orthonormal basis. Let this basis consist of the points

$$\begin{bmatrix} a_{1i}/p^\nu \\ \vdots \\ a_{ni}/p^\nu \end{bmatrix}, \quad a_{ij} \in \boldsymbol{Z},\ i, j = 1, \ldots, n. \tag{36}$$

Let

$$d^2 = x_1^2 + \ldots + x_n^2, \quad (x_1, \ldots, x_n) = 1. \tag{37}$$

Since the denominator of the lattice $M + \boldsymbol{Z}\boldsymbol{y}$ is p^ν, we can assume without loss of generality that $p \nmid a_{1n}$. We can also assume $p \nmid x_n$. Further, permuting, if necessary, the numbers a_{1j} $(j = 1, \ldots, n-1)$ (this corresponds to a permutation of points (36)) and also the numbers x_j $(j = 1, \ldots, n-1)$ and changing the sign of x_n, we can achieve that

$$a_{11}x_1 + \ldots + a_{1n}x_n \not\equiv 0 \pmod{p}. \tag{38}$$

Indeed, if $p > 2$, then at least one of the numbers $a_{11}x_1 + \ldots + a_{1n}x_n$, $a_{11}x_1 + \ldots - a_{1n}x_n$ is non-divisible by p, since their difference $2a_{1n}x_n$ is non-divisible by p.

If $p = 2$, then d is odd. It implies that at least one of the numbers x_j is even, since otherwise, by (37), $1 \equiv d^2 \equiv n \pmod 8$, contrary to the assumption.

We assume without loss of generality that the numbers $x_1, \ldots, x_s$ and $a_{11}, \ldots, a_{1r}$ are even, and $x_{s+1}, \ldots, x_n$ and $a_{1,r+1}, \ldots, a_{1n}$ are odd, where

$$0 < s < n,\ 0 \leqslant r < n,\ n-s \text{ odd},\ n-r \text{ even},\ r+2 \leqslant n,\ r \neq s. \tag{39}$$

Put

$$x_j' = x_j \quad \text{for } j \neq 1, s+1, \qquad a_{1j}' = a_{1j} \quad \text{for } j \neq 2, r+1,$$

$$x_1' = \begin{cases} x_1 & \text{for } s > r, \\ x_{s+1} & \text{for } s < r, \end{cases} \qquad a_{12}' = \begin{cases} a_{12} & \text{for } s > r, \\ a_{1,r+1} & \text{for } s < r, \end{cases}$$

$$x_{s+1}' = \begin{cases} x_{s+1} & \text{for } s > r, \\ x_1 & \text{for } s < r, \end{cases} \qquad a_{1,r+1}' = \begin{cases} a_{1,r+1} & \text{for } s > r, \\ a_{12} & \text{for } s < r. \end{cases}$$

We have, in virtue of (39),

$$\sum_{j=1}^{n} a'_{1j}x'_j = \begin{cases} \sum_{j=1}^{n} a_{1j}x_j \equiv \sum_{j=s+1}^{n} a_{1j}x_j \equiv n-s \equiv 1 \pmod 2 & \text{for } s > r, \\ a_{11}x_2 + a_{1,r+1}x_1 + a_{12}x_{r+1} + \sum_{\substack{j=3 \\ j\neq r+1}}^{n} a_{1j}x_j & \text{for } r > s = 1, \\ a_{11}x_{s+1} + a_{1,r+1}x_2 + a_{1,s+1}x_1 + a_{12}x_{r+1} + \sum_{\substack{j=3 \\ j\neq s+1,r+1}}^{n} a_{1j}x_j & \text{for } r > s > 1. \end{cases}$$

Moreover, for $r > s \geqslant 1$, we have

$$\sum_{j=1}^{n} a'_{1j}x'_j \equiv \sum_{j=r+2}^{n} a_{1j}x_j \equiv n-r-1 \equiv 1 \pmod 2.$$

Since basis (36) is orthonormal, we have, by (37),

$$p^{2\nu}d^2 = p^{2\nu}\sum_{i=1}^{n} x_i^2 = \sum_{i=1}^{n}\Big(\sum_{j=1}^{n} a_{ij}x_j\Big)^2 = \sum_{i=1}^{n} z_i^2.$$

In virtue of (38),

$$p \nmid z_1. \tag{40}$$

Hence we have $(z_1, \ldots, z_n) = 1$; for, otherwise, $|\det(a_{ij})| = p^{n\nu}$ and

$$z_i = \sum_{j=1}^{n} a_{ij}x_j \equiv 0 \pmod q \quad \text{for } q \neq p,\ i = 1, \ldots, n,$$

would imply $x_j \equiv 0 \pmod q$, contrary to (37).

It remains to show that $z_i \neq 0$ $(i = 1, \ldots, n)$. Suppose that $z_i = 0$ for a certain i. Since points (36) belong to the lattice $M + \boldsymbol{Z}y$, we have $a_{ij} = u_{ij}p^{\nu} + t_j y_i$, $u_{ij}, t_j \in \boldsymbol{Z}$. Hence

$$z_i = \sum_{j=1}^{n} a_{ij}x_j = p^{\nu}\sum_{j=1}^{n} u_{ij}x_j + y_i\sum_{j=1}^{n} t_j x_j = 0.$$

In virtue of (40), $p \nmid \sum_{j=1}^{n} t_j x_j$. This implies that $y_i \equiv 0 \pmod{p^{\nu}}$. Since $y_i > 0$, we have $y_i \geqslant p^{\nu}$. Hence $y_1^2 + \ldots + y_n^2 > p^{2\nu}$, contrary to (35).

Proof of Theorem 4. If m does not satisfy the assumptions of the theorem, it can be verified that m^2 is not the sum of n squares of coprime positive integers. Assume that m satisfies the assumptions of the theorem. We proceed by induction with respect to the number $\omega(m)$ of distinct prime factors of m. Clearly, $\omega(m) > 0$.

The validity of the theorem for $\omega(m) = 1$ follows from Lemma 12.

Let $\omega(m) = 2$, $m = p^\nu q^\mu$, p, q — primes. Assume, first, that at least one of the powers $p^{2\nu}$, $q^{2\mu}$, say $p^{2\nu}$, is the sum of n squares of coprime positive integers. Since m satisfies the assumptions of the theorem, we have $q > 2$ for $n = 3$, and $\mu = 1$ for $q = 2$, $n = 4$. In virtue of Lemma 13, $q^{2\mu}$ is the sum of n squares of coprime integers. In virtue of Lemma 14, m^2 is the sum of n squares of coprime positive integers. Assume now that none of the numbers $p^{2\nu}$, $q^{2\nu}$ is the sum of n squares of coprime positive integers. Since m satisfies the assumption of the theorem, we infer from Lemma 12 that $m = 6$, $n = 5, 7$. The equalities $6^2 = 1^2+1^2+3^2+3^2+4^2$ and $6^2 = 1^2+1^2+2^2+2^2+3^2+4^2$ complete the proof for $\omega(m) = 2$.

Assume that the theorem holds for $\omega(m) = k \geqslant 2$ and let $\omega(m) = k+1 \geqslant 3$. It is easy to see that there exist a prime p and a positive integer ν satisfying the assumptions of Lemma 12 and such that $m = p^\nu d$, $p \nmid d$. In virtue of Lemma 12, $p^{2\nu}$ is the sum of n squares of coprime positive integers. Since $\omega(d) = k \geqslant 2$ and m satisfies the assumptions of the theorem, the number d also satisfies them. By the inductive assumption, d^2 is the sum of n squares of coprime positive integers. In virtue of Lemma 14, m^2 is the sum of n squares of coprime positive integers.

We have also

THEOREM 5. *Let $n \geqslant 5$. For every positive integer m, there are coprime positive integers $x_1, \ldots, x_n$ such that $m^2 = x_1^2+\ldots+x_n^2$ except for the case where m^2 belongs to the sequence* $1, 2, 3, \ldots, n-1, n+1, n+2, n+4, n+5, n+7, n+10, n+13$.

Remark 3. This theorem is an easy consequence of Theorem 9 of G. Pall and Theorem 8 given in [4], p. 378-379, and of arguments used in the proofs of these theorems. Those arguments, however, are based ultimately on the Gauss theorem on sum of three squares.

We say that a *positive integer* $m \in S_n$ if it is the sum of n squares of positive integers, and $m \in \bar{S}_n$ if it is the sum of n coprime positive integers.

LEMMA 15. *Let $n \geqslant 8$. If $m \in S_{n-4}$ and $m > n+13$, then $m \in \bar{S}_n$.*

Proof. It is enough to prove that there holds at least one of the following decompositions:

$$m = \begin{cases} x^2+A, & \text{where } x > 3,\ A \in S_{n-5}, \\ 2\cdot 3^2+B, & \text{where } B \in S_{n-6}, \\ 4\cdot 2^2+C, & \text{where } C \in S_{n-8}. \end{cases} \tag{41}$$

Indeed, by Theorem 4, we have $x^2 \in \bar{S}_5$, $2\cdot 3^2 = 2\cdot 1^2+4\cdot 2^2 \in \bar{S}_6$, $4\cdot 2^2 = 7\cdot 1^2+3^2 \in \bar{S}_8$ and in any case $m \in \bar{S}_n$.

If none of decompositions (41) holds, then $m = a\cdot 1^2+b\cdot 2^2+c\cdot 3^2$, $a+b+c = n-4$, $0 \leqslant a$, $0 \leqslant b \leqslant 3$, $0 \leqslant c \leqslant 1$. Hence

$$m = a+4b+9c = n-4+3b+8c \leqslant n-4+9+8 = n+13,$$

contrary to the assumption.

LEMMA 16. *Let* $n \geqslant 5$. *If* $m^2 > n+13$, *then* $m^2 \in \bar{S}_n$.

Proof. We proceed by induction on n.

For $n = 5, 6, 7$, the lemma follows from Theorem 4.

For $n = 8$, we have $m^2 > 21$, $m > 4$. If m is odd, then, by Theorem 4, $m^2 \in \bar{S}_4$, If $m = 2m_1$, then $m^2 = 4m_1^2 \in S_4$. Thus, in any case, $m^2 \in S_4$. In virtue of Lemma 15, $m^2 \in \bar{S}_8$.

Now assume that the lemma holds for $n-4$, where $n \geqslant 9$. By the assumption, $m^2 > n-4+13$. By the inductive assumption, $m^2 \in \bar{S}_{n-4}$. By Lemma 15, $m^2 \in \bar{S}_n$.

Proof of Theorem 5. In virtue of Lemma 16, it is enough to prove the theorem for $m^2 \leqslant n+13$, but in that case very elementary arguments of Pall do apply (cf. [4], p. 378-379).

REFERENCES

[1] J. W. S. Cassels, *An introduction to the geometry of numbers*, Berlin-Göttingen-Heidelberg 1959.

[2] A. J. Jones, *Cyclic overlattices, I*, Acta Arithmetica 17 (1970), p. 303-314.

[3] A. Schinzel, *Sur les sommes de trois carrés*, Bulletin de l'Académie Polonaise des Sciences, Série des sciences mathématiques, astronomiques et physiques, 7 (1959), p. 307-309.

[4] W. Sierpiński, *Elementary theory of numbers*, Warszawa 1964.

[5] F. Steiger, *Über die Grundlösung der Gleichung* $a^2+b^2+c^2 = d^2$, Elemente der Mathematik 11 (1956), p. 105-108.

[6] G. L. Watson, *Integral quadratic forms*, Cambridge 1960.

Reçu par la Rédaction le 25. 9. 1972