Proceedings of the Steklov Institute of Mathematics, Vol. 218, 1997, pp. 146–159.
Translated from Trudy Matematicheskogo Instituta imeni V. A. Steklova, Vol. 218, 1997, pp. 151–164.

Orbits of Representation of Numbers by Local Quadratic Forms

V. G. Zhuravlev

Received February, 1997

INTRODUCTION

In this article an attempt is made to investigate the structure of orbits $\{b\}$ of primitive representations $Q[b] = A$ of numbers by integer, over the odd p-adic ring $\mathbb{Z}_p$, quadratic forms Q. Theorem 2.1 from [1], to be more precise, its p-adic analog, serves as a basis. It is proved that all orbits are divided into sets $\mathrm{pb}_{Q,A}(\{G\})$ numbered by a finite number of classes $\{G\}$ of quadratic forms from the orthogonal complement of A. This division gives a "rough" classification of the orbits. Within the indicated sets there exists a one-to-one correspondence between the orbits $\{b\}$ and $\mathrm{O}(G)$-orbits $\{C\}$ which encircle the forms A and G of the matrices C, this is a "fine" classification of the orbits $\{b\}$. In the one-dimensional case, the matrices form a set of vectors $C \bmod A$ with a natural action of the orthogonal group $\mathrm{O}(G)$ over $\mathbb{Z}_p$. If we restrict our consideration to the numbers $A = \varepsilon p^\nu$ with $\nu = 1, 2, 3$, then we shall have the cases enveloped by the Witt theorem within whose framework we remain to avoid an increase in the volume of the article.

The article consists of three sections. Following [1], in Section 1 we introduce the principal concepts and notation and define the one-to-one correspondence between the orbits $\{b\}$ and $\{C\}$. In Section 2 all vectors C that encircle A and G are found and the local invariants of the resulting forms $Q_G^A(C)$ are calculated. The main results concerning the orbits $\{b\}$ can be found in Section 3. Here the orbits $\{C\}$ are classified according to the vectors C of minimal length contained in them and the corresponding minimal forms $X = Q(C)$ and their weights w are written out. Using these forms, we can find the number of orbits $\{b\}$ for solving the quadratic equation $Q[b] = A$: the number of orbits is equal to the weighted number of representations of the form Q as the direct sum $X \oplus Y$ with the arbitrary second form Y.

Example 1. Suppose that the quadratic form Q of dimension ≥ 3 has a determinant $|Q|$ which is not divisible by p. Then the equation $Q[b] = A$ has an orbit $\{b\}$, i.e., its solutions exist and can be obtained from any fixed b_1 by means of the transformations σ from the orthogonal group $\mathrm{O}(Q)$ over $\mathbb{Z}_p$.

It is impossible to briefly formulate the conditions for the arbitrary forms Q under which one orbit $\{b\}$ remains since upon the decomposition of Q in the sum $X \oplus Y$ a strong ramification is observed, and its translation into the language of relationships between the invariants of the form Q only makes the situation still more intricate. Instead, we shall give an example of the forms Q with a large number of orbits $\{b\}$.

Example 2. The set of all solutions $(x_1, \dots, x_4)$ from the ring $\mathbb{Z}_p$ of the quadratic equation $x_1^2 + px_2^2 + p^2x_3^2 + p^3x_4^2 = p^3$ disintegrates into $(7p-3)/4$ or $(5p+1)/4$ orbits according as we have the condition $p \equiv 1$ or $-1 \pmod 4$.

1. CLASSIFICATION OF PRIMITIVE REPRESENTATIONS

All quadratic forms, lattices, and representations are defined over the local ring of integer p-adic numbers $\mathbb{Z}_p$ for an odd p.

1.1. Suppose that $Q = {}^tQ$ is a nondegenerate symmetric matrix of order n from the set of matrices $M_n(\mathbb{Z}_p)$ with coefficients from $\mathbb{Z}_p$ and $A = {}^tA$ is a similar matrix from $M_m(\mathbb{Z}_p)$ of dimension $1 \le m < n$. We shall also call them *quadratic forms*, or simply *forms*, and will investigate the primitive representations of quadratic forms by forms of larger dimensions:

$$Q[b] = {}^tbQb = A \qquad \text{for} \quad b \in M_{n,m}(\mathbb{Z}_p) \tag{1.1}$$

under the condition that $d(b) = d_p(b) = 1$, where we denote by $d(b)$ the greatest common divisor (over $\mathbb{Z}_p$) of minors of order m of the matrix b. Then we follow [1]. Primitive matrices b are pulled back to the matrices $B = (b \mid e)$ from $\mathrm{SL}_n(\mathbb{Z}_P)$, and the transformated form

$$Q_B = Q[B] = \begin{pmatrix} A & C \\ {}^tC & Q' \end{pmatrix}$$

again belongs to the class $\{Q\}$ of forms which are equivalent to Q relative to the group $\mathrm{SL}_n(\mathbb{Z}_p)$. The matrix

$$M_C = \begin{pmatrix} 1 & -A^{-1}C \\ 0 & 1 \end{pmatrix}$$

which is, in general, not p-integer, reduces the form Q_B to the form

$$Q_B[M_C] = \begin{pmatrix} A & 0 \\ 0 & G' \end{pmatrix} = A \oplus G',$$

equal to the direct sum of the forms A and $G' = Q' - A^{-1}[C]$. We fix the nonzero p-integer $a = p^\nu \cdot \{a\}$ ($p^{-\nu} = |a|_p$ means, as usual, the p-norm of a), such that the matrix $a \cdot A^{-1}$ has integer coefficients and $\nu = 0, 1, 2, \dots$ is minimal under this condition, i.e., a is a p-adic analog of the level of the quadratic form over the ring of integer rational numbers $\mathbb{Z}$. Then the form

$$a \cdot Q_B[M_C] = \begin{pmatrix} aA & 0 \\ 0 & G \end{pmatrix}$$

with the block $G = aQ' - aA^{-1}[C]$ is p-integer, and

$$|G| = a^k \frac{|Q|}{|A|}, \tag{1.2}$$

where $k = n - m$ and $|\cdot|$ denotes the determinant of the matrix. Excluding from the sequence $b \to B \to C \to G$ the dependence on the choice of the matrix B, we arrive at the representation [1, (1.16)]

$$[Q, A, a] \colon b \mapsto \{G\} = \{G(b)\},$$

where b defines the class $\{G(b)\}$ but not the form $G(b)$ itself. We denote by $\mathrm{pb}_{Q,A}$ the set of all primitive representations b (1.1) and by $\mathrm{pb}_{Q,A}(\{G\})$ the set of b corresponding to the class $\{G\}$.

Since $|G|$ is defined by the forms A and Q, it follows that $\mathrm{pb}_{Q,A}$ is divided into a finite number of sets $\mathrm{pb}_{Q,A}(\{G\})$ which are easier to investigate:

$$\mathrm{pb}_{Q,A}=\sum_{\{G\}}\mathrm{pb}_{Q,A}(\{G\}). \tag{1.3}$$

1.2. Returning to the beginning of the section, for each solution $C \bmod A$ of the congruence

$$E[C]+G\equiv 0 \pmod{a}, \tag{1.4}$$

where $E=a\cdot A^{-1}$, $\bmod a$ is an abbreviation for $\bmod a\mathbb{Z}_p$, and $C\equiv C' \pmod{A}$ denotes the integrity of the matrix $A^{-1}(C-C')$, we define the form

$$Q_G^A(C)=\frac{1}{a}\begin{pmatrix} aA & 0\\ 0 & G\end{pmatrix}[M_C^{-1}]=\begin{pmatrix} A & C\\ {}^tC & Q'\end{pmatrix} \tag{1.5}$$

with the block $Q'=\frac{1}{a}(E[C]+G)$. Let $C_G^A(Q)$ be the set of C for which form (1.5) belongs to the class $\{Q\}$. If we now fix the class $\{G\}$ and exclude from $b\to B\to C$ the dependence on B, then we arrive at the orbits $\{C\}^+$ of the solutions C of congruence (1.4): $C\cdot S/\bmod A$ for all S from the proper orthogonal group $\mathrm{O}^+(G)$ over $\mathbb{Z}_p$. In turn, the mapping $b\to\{C\}^+$ divides the solutions b (1.1) into its own orbits $\{b\}^+$ relative to the group $\mathrm{O}^+(Q)$. The quotient mapping

$$\mathrm{pb}_{Q,A}(\{G\})\supset\{b\}^+ \underset{\sim}{\to} \{C\}^+\subset C_G^A(Q) \tag{1.6}$$

becomes a bijection (cf. [1, p. 38]). Both sets from (1.6) are empty only if the determinant $|G|$ does not satisfy condition (1.2).

If in the preceding definitions we replace the groups O^+ by complete orthogonal groups O (note that the index $[\mathrm{O}:\mathrm{O}^+]=2$ over $\mathbb{Z}_p$), then the orbits $\{\,\cdot\,\}^+$ are replaced by $\{\,\cdot\,\}$ with the preservation of the bijection (1.6):

$$\mathrm{pb}_{Q,A}(\{G\})\supset\{b\} \underset{\sim}{\to} \{C\}\subset C_G^A(Q). \tag{1.7}$$

The forms A and G can be defined (cf. with glueing [2, p. 133]) if the set $\mathrm{Ext}(G,A)$ of the encircling matrices C (1.4) is nonempty. The division (1.3) has a dual and, according to (1.2), finite partitioning

$$\mathrm{Ext}(G,A)=\sum_{\{Q\}}C_G^A(Q).$$

2. ENCIRCLING VECTORS

Let us investigate the sets $\mathrm{Ext}(G,A)$ in the one-dimensional case $m=1$ of the forms $A=p^{\nu}\cdot\{A\}$. Suppose that

$$G=\bigoplus_{\alpha}G_\alpha$$

with blocks $G_\alpha=p^\alpha\cdot G_{p^\alpha}$ of dimensions $k_\alpha=\dim G_\alpha$, $\alpha=0,1,2,\dots$, and with the determinants $|G_{p^\alpha}|$ from the group of the units $\mathbb{Z}_p^\times$. We divide the encircling vectors (in this case one-dimensional matrices) $C=(C_0\mid\dots\mid C_\alpha\mid\dots)$ into blocks C_α of length k_α respectively.

2.1. For $\nu = 1$ we have $E[C_0] \equiv -G_0 \pmod p$ according to (1.4). Therefore $k_0 = 0$ or $k_0 = 1$ and $E = \{a\}/\{A\} \sim -G_0$, where $\sim$ denotes the equivalence modulo the squares of the units $(\mathbb{Z}_p^\times)^2$. In the first case we can take $C = (0 \mid \ldots \mid 0)$, and then (1.5) implies

$$Q_G^A(C) = A \oplus \frac{1}{a} G.$$

Now if $k_0 = 1$, then $C = (\pm C_{0,\text{fix}} \mid \ldots \mid 0)$, and again, according to (1.5), we have

$$Q_G^A(C) = \begin{pmatrix} A & C_0 \\ C_0 & 0 \end{pmatrix} \oplus \frac{1}{a} G_{\neq 0} \sim 1_2^- \oplus \frac{1}{a} G_{\neq 0}, \tag{2.1}$$

where in $G_{\neq 0}$ the block G_0 is excluded, $1_2^- = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, and $\sim$ denotes the equivalence over the ring $\mathbb{Z}_p$.

Proposition 2.1. *If $A = p \cdot \{A\}$, $a = p \cdot \{a\}$, then every encircling vector C from* $\mathrm{Ext}(G, A)$ *produces the form*

$$Q_G^A(C) \sim \begin{cases} 1_2^- \oplus \dfrac{1}{a} G_{\neq 0} & \text{if } k_0 = 1,\ E \sim -G_0 \\[2mm] A \oplus \dfrac{1}{a} G & \text{if } k_0 = 0. \end{cases}$$

In this case, $\mathrm{Ext}(G, A)$ *consists of* $\mathrm{ext}(G, A) = 2$ *or* 1 *vectors respectively.*

2.2. For $\nu = 2$, we have, by analogy, $E[C_0] \equiv -G_0 \pmod{p^2}$, and again $k_0 = 0$ or $k_0 = 1$ and $E \sim -G_0$. In addition, by virtue of (1.4), we have $k_1 = 0$. In the case of $k_0 = 1$, we arrive at form (2.1).

For $k_0 = 0$ we have

$$G = \bigoplus_{\alpha \geq 2} G_\alpha.$$

Therefore $C = pC'$ according to (1.4) and $C' = (0 \mid \ldots \mid 0)$, and then $Q_G^A(C) = p^2\{a\}E \oplus \frac{1}{a} G$ or $C' = (C_2' \mid \ldots \mid C_\alpha' \mid 0 \ldots)$ with the largest α, for which the block C_α' has a nonzero $\bmod\, p$ rank $r_p(C_\alpha') \neq 0$. The definition of matrix (1.5) implies the equivalence

$$Q_G^A(C) \sim Q_G^A\bigl(p \cdot (C'\sigma / \bmod p)\bigr) \qquad \text{for every} \quad \sigma \in \mathrm{O}(G).$$

Therefore, using Witt's theorem (see, e.g., [3, 4]), we can assume that $C_\alpha' = (1\ 0 \ldots 0)$ and that the α-block of the matrix G is equal to

$$G_{p^\alpha} = \begin{cases} \begin{pmatrix} c & 0 \\ 0 & c^\perp(G_{p^\alpha}) \end{pmatrix} & \text{with } c = c_\alpha^{-1} \text{ if } G_{p^\alpha}^{-1}[{}^tC_\alpha'] = c_\alpha \not\equiv 0 \pmod p \\[2mm] \begin{pmatrix} J_2 & 0 \\ 0 & J_2^\perp(G_{p^\alpha}) \end{pmatrix} & \text{with } J_2 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \text{ if } c_\alpha \equiv 0 \pmod p. \end{cases} \tag{2.2}$$

Next we shall need the matrix realization of the orthogonal group $\mathrm{O}(Q)$ of the form that can be written as $Q = Q_1 \oplus qQ_q$, $q = p^\alpha$. The relation $Q[M] = Q$ for the matrix $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ implied $B = q \cdot B_1$ with the p-integer B_1 and

$$Q_1[A] + qQ_q[C] = Q_1, \qquad {}^tAQ_1B_1 + {}^tCQ_qD = 0, \qquad qQ_1[B_1] + Q_q[D] = Q_q. \tag{2.3}$$

We infer that the block A belongs to the group $\mathrm{O}(Q_1/\bmod q)$ and the block D belongs to the group $\mathrm{O}(Q_q/\bmod q)$ which are both orthogonal groups over the ring of residues $\mathbb{Z}_p/q\mathbb{Z}_p$. Moreover, for arbitrary A, D of this kind and for arbitrary B_1 or C, we can use (2.3) to reconstruct the whole matrix M from the group $\mathrm{O}(Q)$.

Applying successively this property of orthogonal transformations to the blocks of the matrix C', we find for it a convenient representation

$$C' = C'_{\mathrm{fix}} \cdot \sigma \qquad \text{for } C'_{\mathrm{fix}} = (\,0 \quad | \quad C'_\alpha \quad | \quad 0\,) \text{ and some } \sigma \in \mathrm{O}(G), \tag{2.4}$$

where the α-block is equal to $C'_\alpha = (1\ 0 \ldots 0)$ as before. This representation and Witt's theorem lead to the following parametrization (see (3.3)) of the orbits $\{C\}$ of solutions C of congruence (1.4) with the one-dimensional form $A = p^2 \cdot \{A\}$: $\{C\} = \{\alpha, c_\alpha\}$, where $\alpha \geq 2$ and $c_\alpha \bmod p$ is arbitrary, nontrivially representable by the form $G^{-1}_{p^\alpha}$ which is equivalent to the form G_{p^α} itself.

Represenation (2.4) makes it possible to easily calculate the blocks Q' of the forms $Q^A_G(C_{\mathrm{fix}})$ for $C_{\mathrm{fix}} = p \cdot C'_{\mathrm{fix}}$, namely,

$$Q' = \frac{p^2}{a} c' \oplus \frac{p^2}{a} c^\perp \oplus \frac{1}{a} G_{\neq\alpha} \qquad \text{for} \quad c_\alpha \not\equiv 0 \pmod p, \tag{2.5}$$

where $c' = E + p^{\alpha-2}c$, $c^\perp = c^\perp(G_{p^\alpha})$, and

$$Q' = \frac{p^2}{a} \begin{pmatrix} E & p^{\alpha-2} \\ p^{\alpha-2} & 0 \end{pmatrix} \oplus \frac{p^\alpha}{a} J_2^\perp \oplus \frac{1}{a} G_{\neq\alpha} \qquad \text{for} \quad c_\alpha \equiv 0 \pmod p,$$

where we have also used the abbreviation $J_2^\perp = J_2^\perp(G_{p^\alpha})$.

For what follows, we shall need the matrix analog of the well-known algorithm of diagonalization of quadrtic forms over the odd local ring $\mathbb{Z}_p$. The transformation

$$M = \begin{pmatrix} 1 & 0 & 0 \\ -Q_1^{-1} \cdot {}^tC & 1 & -Q_1^{-1} \cdot C_2 \\ 0 & 0 & 1 \end{pmatrix}$$

of the form

$$Q = \begin{pmatrix} A & C & C_1 \\ {}^tC & Q_1 & C_2 \\ {}^tC_1 & {}^tC_2 & Q_2 \end{pmatrix}$$

which is proper and integer under the condition $|Q_1| \not\equiv 0 \pmod p$, splits off the block Q_1. By a direct calculation we get the decomposition of the form Q in the direct sum

$$Q \sim Q_1 \oplus \begin{pmatrix} \widetilde{A} & \widetilde{C}_1 \\ {}^t\widetilde{C}_1 & \widetilde{Q} \end{pmatrix}, \tag{2.6}$$

where $\widetilde{A} = A - Q_1^{-1}[{}^tC]$, $\widetilde{C}_1 = C_1 - CQ_1^{-1}C_2$, and $\widetilde{Q} = Q_2 - Q_1^{-1}[C_2]$.

For $c_\alpha \not\equiv 0 \pmod p$ we use the relations (1.5) and (2.5) to find

$$Q^A_G(C_{\mathrm{fix}}) = E_c \oplus \frac{p^\alpha}{a} c^\perp \oplus \frac{1}{a} G_{\neq\alpha}, \qquad E_c = \begin{pmatrix} aE^{-1} & p \\ p & \frac{p^2}{a} c' \end{pmatrix}.$$

Setting

$$Q_1 = \frac{p^2}{a}c' = \frac{1}{\{a\}}c',$$

for $\alpha > 2$, we obtain, from relation (2.6), the decomposition of the form $E_c \sim \{a\}E \oplus p^\alpha\{a\}c$. For $\alpha = 2$, $c' \not\equiv 0 \pmod p$ and $c' \equiv 0 \pmod p$ we obtain, by analogy, $E_c \sim \{a\}(E+c) \oplus p^2\{a\}(E^{-1}+c^{-1})$ and $E_c \sim p \cdot 1_2^-$, respectively. If $c_\alpha \equiv 0 \pmod p$, then

$$Q_G^A(C_{\mathrm{fix}}) = E_0 \oplus \frac{p^\alpha}{a}J_2^\perp \oplus \frac{1}{a}G_{\neq\alpha}$$

with the block

$$E_0 = \begin{pmatrix} aE^{-1} & p & 0 \\ p & \{a\}^{-1}E & \{a\}^{-1}p^{\alpha-2} \\ 0 & \{a\}^{-1}p^{\alpha-2} & 0 \end{pmatrix} \sim \{a\}E \oplus \begin{pmatrix} 0 & -E^{-1}p^{\alpha-1} \\ -E^{-1}p^{\alpha-1} & -\{a\}^{-1}E^{-1}p^{\alpha-2} \end{pmatrix}.$$

The last block

$$E_0' \sim \begin{cases} p^{\alpha-1} \cdot 1_2^- & \text{if } \alpha > 2 \\ -\{a\}E \oplus p^2\{a\}E & \text{if } \alpha = 2. \end{cases}$$

Finally, it remains to calculate the number of rows of the orbits $\{\alpha, c_\alpha\}$ which have the form

$$C = (pC_2' \mid \ldots \mid pC_{\alpha-1}' \mid pC_\alpha' \mid 0 \ldots)$$

with arbitrary blocks $C_2', \ldots, C_{\alpha-1}' \bmod p$, and, consequently, the number of combinations is equal to $p^{k_{<\alpha}}$ with $k_{<\alpha} = k_2 + \cdots + k_{\alpha-1}$ and with the block C_α' which satisfies the congruence $G_{p^\alpha}^{-1}[{}^tC_\alpha'] \equiv 0 \pmod p$. According to the Witt's theorem, all solutions belong to the same orbit, and, hence, their number is equal to $o(G_{p^\alpha} / \bmod p)$, i.e., to the order of the orthogonal group $\bmod p$ for the form $G_{p^\alpha} \sim G_{p^\alpha}^{-1}$ divided by $\mathrm{stab}(C_\alpha')$, which is the order of the stabilizer of the fixed C_α'. According to the conditions $c_\alpha \not\equiv 0 \pmod p$ and $c_\alpha \equiv 0 \pmod p$, the stabilizers contain elements $o\big(c^\perp(G_{p^\alpha})/ \bmod p\big)$ and $p^{k_\alpha - 1}o\big(J_2^\perp(G_{p^\alpha})/ \bmod p\big)$, and the relations for the orders of orthogonal groups are known (see, e.g., [1, (10.2)]). We have thus proved

Proposition 2.2. *Suppose that $A = p^2\{A\}$, $E = aA^{-1}$, $a = p^2\{a\}$ is fixed, and the form $G = \bigoplus_\alpha G_\alpha$ with blocks $G_\alpha = p^\alpha \cdot G_{p^\alpha}$ of dimension k_α.*

I. *If $k_0 = 1$, $k_1 = 0$, and $E \sim -G_0$, then every encircling vector C from* $\mathrm{Ext}(G, A)$ *gives the form*

$$Q_G^A(C) \sim 1_2^- \oplus \frac{1}{a}G_{\neq 0} \qquad \textit{and} \qquad \mathrm{ext}(G, A) = 2.$$

II. *If $k_0 = k_1 = 0$, then there exists a partitioning of the set of encircling vectors from* $\mathrm{Ext}(G, A)$ *into the orbits*

$$\mathrm{Ext}(G, A) = \{0\} + \sum_{\alpha \geq 2, c_\alpha} \{\alpha, c_\alpha\} \tag{2.7}$$

with the summation over all $c_\alpha \bmod p$ which are nontrivially representable by the form G_{p^α}.

1. *The zero vector* $C = (0 \mid \dots \mid 0)$ *gives the form*

$$Q_G^A(C) \sim p^2\{a\}E \oplus \frac{1}{a}G.$$

2. *If* C *is from the orbit* $\{\alpha, c_\alpha\}$ *for* $c_\alpha \not\equiv 0 \pmod p$ *and* $c = c_\alpha^{-1}$, *then*

$$Q_G^A(C) \sim E_c \oplus \frac{p^\alpha}{a} c^\perp(G_{p^\alpha}) \oplus \frac{1}{a} G_{\neq\alpha}, \tag{2.8}$$

every vector C *performs the* 2*-encircling* E_c, *i.e., minimal form of dimension* 2 *that can be written as*

$$E_c \sim \begin{cases} \{a\}E \oplus p^\alpha\{a\}c & \text{if } \alpha > 2 \\ \{a\}(E+c) \oplus p^2\{a\}(E^{-1}+c^{-1}) & \text{if } \alpha = 2,\ c \not\equiv -E \pmod p \\ p \cdot 1_2^-, & \text{if } \alpha = 2,\ c \equiv -E \pmod p), \end{cases}$$

and the orbit $\{\alpha, c_\alpha\}$ *has the order*

$$(\alpha, c_\alpha) = p^{k_{<\alpha}} \frac{o(G_{p^\alpha} / \operatorname{mod} p)}{o(c^\perp(G_{p^\alpha}) / \operatorname{mod} p)}, \tag{2.9}$$

which depends only on the sign of $\left(\frac{c}{p}\right) = \pm 1$.

3. *Now if the vector* C *belongs to the zero orbit* $\{\alpha, 0\}$, *then*

$$Q_G^A(C) \sim E_0 \oplus \frac{p^\alpha}{a} J_2^\perp(G_{p^\alpha}) \oplus \frac{1}{a} G_{\neq\alpha},$$

where the form E_0 *is now a* 3*-encircling that can be written as*

$$E_0 \sim \begin{cases} \{a\}E \oplus p^{\alpha-1} \cdot 1_2^- & \text{if } \alpha > 2 \\ 1_2^- \oplus p^2\{a\}E & \text{if } \alpha = 2, \end{cases}$$

and

$$(\alpha, 0) = p^{k_{<\alpha}} \frac{o(G_{p^\alpha} / \operatorname{mod} p)}{p^{k_\alpha - 1} o(J_2^\perp(G_{p^\alpha}) / \operatorname{mod} p)}. \tag{2.10}$$

In all others cases $\operatorname{ext}(G, A) = 0$.

Remark. For applications, we must know the distribution by classes $1^{\eta_1} \oplus p^\alpha \cdot 1^{\eta_2}$, where $\eta = (\eta_1, \eta_2) = (\pm, \pm)$ and $\left(\frac{1^-}{p}\right) = -1$, of the forms of the second kind from (2.8). We denote by (η) the number of residues $c \not\equiv 0 \pmod p$ under the conditions

$$\left(\frac{\{a\}(E+c)}{p}\right) = \eta_1, \qquad \left(\frac{\{a\}(E^{-1}+c^{-1})}{p}\right) = \eta_2.$$

By analogy [5, p. 86], we calculate

$$(\eta) = \begin{cases} \frac{1}{4}\left(p - 2 - 3\left(\frac{-1}{p}\right)\right) & \text{if } \eta_1 = \eta_2 = \left(\frac{-\{a\}E}{p}\right) \\ \frac{1}{4}\left(p - 2 + \left(\frac{-1}{p}\right)\right) & \text{in the other cases.} \end{cases}$$

2.3. As we shall see later, the primitive representations of cubes $A = p^3\{A\}$ is the last case, where we can directly use Witt's theorem. If $k_0 = 1$, then the two dimensions $k_1 = k_2 = 0$, and we again arrive at relation (2.1).

Let $k_0 = k_1 = k_2 = 0$ and, hence, $G = G_3 \oplus G_4 \oplus \cdots$. By virtue of (1.4), $C = p^2C'$ with any $C' \bmod p$, i.e., $C' = (0 \mid \ldots \mid 0)$. Then

$$Q_G^A(C) = p^3\{a\}E \oplus \frac{1}{a}G,$$

or $C' = (C_3' \mid \ldots \mid C_\alpha' \mid 0 \ldots)$ with the largest $\alpha \geq 3$, when the rank $r_p(C_\alpha') \neq 0$.

In the case of $C' \not\equiv 0 \pmod p$, we can assume that the α-block has form (2.2) and the vector $C' = C'_{\text{fix}}$, where $C'_{\text{fix}} = (0 \mid C_\alpha' \mid 0)$ and $C_\alpha' = (1\,0 \ldots 0)$.

For $c_\alpha \not\equiv 0 \pmod p$, by virtue of (1.5), we have

$$Q' = \frac{1}{\{a\}}c' \oplus \frac{p^\alpha}{a}c^\perp \oplus \frac{1}{a}G_{\neq\alpha},$$

where $c' = pE + p^{\alpha-3}c$, and therefore, for $C_{\text{fix}} = p^2C'_{\text{fix}}$, we have

$$Q_G^A(C_{\text{fix}}) \sim E_c \oplus \frac{p^\alpha}{a}c^\perp \oplus \frac{1}{a}G_{\neq\alpha} \qquad \text{with} \quad E_c = \begin{pmatrix} aE^{-1} & p^2 \\ p^2 & \{a\}^{-1}c' \end{pmatrix}$$

as 2-encircling whose decomposition can be found by means of algorithm (2.6). Thus $c' = pc''$ and $c'' \equiv E \not\equiv 0 \pmod p$ for $\alpha > 4$, whence it follows that

$$E_c \sim p\frac{c''}{\{a\}} \oplus p\widetilde{A}, \qquad \widetilde{A} = \frac{a}{p}E^{-1} - \frac{\{a\}}{c''}p^2 \sim p^{\alpha-2}\{a\}c,$$

and, hence, $E_c \sim p\{a\}E \oplus p^{\alpha-1}\{a\}c$. The other cases can be considered by analogy. For $c_\alpha \equiv 0 \pmod p$ we obtain

$$Q_G^A(C_{\text{fix}}) \sim E_0 \oplus \frac{p^\alpha}{a}J_2^\perp \oplus \frac{1}{a}G_{\neq\alpha}$$

with the block

$$E_0 = \begin{pmatrix} aE^{-1} & p^2 & 0 \\ p^2 & \{a\}^{-1}Ep & \{a\}^{-1}p^{\alpha-3} \\ 0 & \{a\}^{-1}p^{\alpha-3} & 0 \end{pmatrix}$$

as a 3-encircling now, just as in item 2.2.

The case $k_0 = k_1 = 0$ and $k_2 = 1$, is a new one, where, in accordance with (1.4), $C_2 = pC_2'$ and $C_2' \bmod p^2$ satisfies the congruence $E[C_2'] \equiv -G_{p^2} \pmod p$. We can assume here that $E = -G_{p^2}$ and C_2' has the form $C'_{2,\text{fix}} = 1 + pC_2''$ with any $C_2'' \bmod p$. Therefore $C = pC'$, where $C' = (C_2' \mid 0 \ldots)$ or $C' = (C_2' \mid pC_3' \mid \ldots \mid pC_\alpha' \mid 0 \ldots)$ with the α-block $C_\alpha' = (1\,0 \ldots 0)$. In this case, the block G_{p^α} has form (2.2). The vectors $C' = (C_2' \mid 0 \ldots)$ give the form

$$Q_G^A(C) \sim E_C \oplus \frac{1}{a}G_{>2}, \qquad \text{where} \quad E_C = \begin{pmatrix} aE^{-1} & pC_2' \\ pC_2' & \{a\}^{-1}c' \end{pmatrix}$$

and $c' = 2EC_2'' + pEC''^2_2$. If $c' \not\equiv 0 \pmod p$, i.e., $C_2'' \not\equiv 0 \pmod p$, then

$$E_C \sim 1 \oplus p^2 \cdot (-1) \qquad \text{or} \qquad E_C \sim -1 \oplus p^2 \cdot 1,$$

and every form appears $2 \cdot (p-1)/2 = p-1$ times. Now if $c' \equiv 0 \pmod p$, then $E_C \sim p \cdot 1_2^-$ and the form on the right appears twice.

The maximal 4-encirclings give the vectors $C' = (C_2' \mid \dots \mid pC_\alpha' \mid 0 \dots)$ from the $\mathrm{O}(G)$-orbit of the vector

$$C'_{\text{fix}} = (1 \mid 0 \dots \mid pC'_\alpha \mid 0 \dots) \qquad \text{with} \qquad C'_\alpha = (1\ 0 \dots 0) \tag{2.11}$$

and the form G_{p^α} of the kind (2.2) in the case of $c_\alpha \equiv 0 \pmod p$:

$$E_0 = \begin{pmatrix} aE{-}1 & p & p^2 & 0 \\ p & & & \\ p^2 & & \{a\}^{-1}E_0' & \\ 0 & & & \end{pmatrix}$$

with the block

$$E_0' = \begin{pmatrix} 0 & E & 0 \\ E & pE & p^{\alpha-3} \\ 0 & p^{\alpha-3} & 0 \end{pmatrix}.$$

Setting

$$Q_1 = \frac{1}{\{a\}} \begin{pmatrix} 0 & E \\ E & pE \end{pmatrix},$$

in the relation (2.6), we find the decomposition for E_0.

Proposition 2.3. *Let $A = p^3\{A\}$ and $E = aA^{-1}$ for $a = p^3\{a\}$.*

I. *If $k_0 = 1$, $k_1 = k_2 = 0$, and $E \sim -G_0$, then the encircling vectors C from* $\mathrm{ext}(G, A)$ *give the form*

$$Q_G^A(C) \sim 1_2^- \oplus \frac{1}{a} G_{\neq 0} \qquad \textit{and} \qquad \mathrm{ext}(G, A) = 2.$$

II. *If $k_0 = k_1 = k_2 = 0$, then the set of encircling vectors from* $\mathrm{Ext}(G, A)$ *decompose, just as in* (2.7), *into orbits $\{0\}$ and $\{\alpha, c_\alpha\}$, where $\alpha \geq 3$.*

1. *The vector $C = (0 \mid \dots \mid 0)$ gives the form*

$$Q_G^A(C) \sim p^3\{a\}E \oplus \frac{1}{a} G.$$

2. *If C belongs to the orbit $\{\alpha, c_\alpha\}$ with $c_\alpha \not\equiv 0 \pmod p$ and $c = c_\alpha^{-1}$, then the form*

$$Q_G^A(C) \sim E_c \oplus \frac{p^\alpha}{a} c^\perp(G_{p^\alpha}) \oplus \frac{1}{a} G_{\neq \alpha}$$

with the 2-encirclings

$$E_c \sim \begin{cases} p\{a\}E \oplus p^{\alpha-1}\{a\}c & \textit{if } \alpha > 4 \\ p\{a\}(E + c) \oplus p^{\alpha-1}\{a\}(E^{-1} + c^{-1}) & \textit{if } \alpha = 4,\ c \not\equiv -E \pmod p \\ p^2 \cdot 1_2^- & \textit{if } \alpha = 4,\ c \equiv -E \pmod p \\ \{a\}c \oplus p^3\{a\}E & \textit{if } \alpha = 3, \end{cases}$$

and the orbit $\{\alpha, c_\alpha\}$ *is of order* (α, c_α) (2.9).

3. *In the case of a vector from the orbit* $\{\alpha, 0\}$, *the form*

$$Q_G^A(C) \sim E_0 \oplus \frac{p^\alpha}{a} J_2^\perp(G_{p^\alpha}) \oplus \frac{1}{a} G_{\neq\alpha}$$

with 3-*encirclings*

$$E_0 \sim \begin{cases} p\{a\}E \oplus p^{\alpha-2} \cdot 1_2^- & \text{if } \alpha > 4 \\ p \cdot 1_2^- \oplus p^3\{a\}E & \text{if } \alpha = 4 \\ 1_2^- \oplus p^3\{a\}E & \text{if } \alpha = 3, \end{cases}$$

and the order of orbit $(\alpha, 0)$ *is equal to* (2.10).

III. *Finally, let* $k_0 = k_1 = 0$, $k_2 = 1$, *and* $E \sim -G_{p^2}$. *Then the set of encircling vectors from* $\mathrm{Ext}(G, A)$ *has partitioning* (2.7), *where the zero orbit* $\{0\}$ *consists of* $C = (pC_1' \mid 0 \dots)$ *with the block* $C_2' \bmod p^2$ *and* $E[C_2'] \equiv -G_{p^2} \pmod p$, *and* $\{\alpha, c_\alpha\}$ *with* $\alpha \geq 3$ *is an* $\mathrm{O}(G)$-*orbit of the vector* $C_{\mathrm{fix}} = p \cdot C_{\mathrm{fix}}'$ (2.11).

1. *The vectors* C *from the orbit* $\{0\}$ *lead to the form*

$$Q_G^A(C) \sim E_C \oplus \frac{1}{a} G_{>2}, \tag{2.12}$$

where the blocks $E_C \sim 1 \oplus p^2 \cdot (-1)$, $E_c \sim -1 \oplus p^2 \cdot 1$, *and* $E_C \sim p \cdot 1_2^-$ *appear* $p-1$, $p-1$, *and* 2 *times, respectively.*

2. *For* C, *from the orbit* $\{\alpha, c_\alpha\}$ *with* $c_\alpha \not\equiv 0 \pmod p$ *we have*

$$Q_G^A(C) \sim E_c \oplus \frac{p^\alpha}{a} c^\perp(G_{p^\alpha}) \oplus \frac{1}{a} G_{\neq 2,\alpha} \tag{2.13}$$

with 3-*encircling*

$$E_c \sim 1_2^- \oplus p^{\alpha-1}\{a\}c, \qquad \alpha \geq 3,$$

and with the order of the orbit (α, c_α) *twice exceeding the order* (2.9).

3. *Now if* C *belongs to the orbit* $\{\alpha, 0\}$, *then*

$$Q_G^A(C) \sim E_0 \oplus \frac{p^\alpha}{a} J_2^\perp(G_{p^\alpha}) \oplus \frac{1}{a} G_{\neq 2,\alpha} \tag{2.14}$$

with a 4-*encircling*

$$E_0 \sim 1_2^- \oplus p^{\alpha-1} \cdot 1_2^-, \qquad \alpha \geq 3,$$

and now the order of the orbit $(\alpha, 0)$ *twice exceeds the order* (2.10).

In all the other cases $\mathrm{ext}(G, A) = 0$.

3. ORBITS OF ONE-DIMENSIONAL REPRESENTATIONS

The existence of the one-to-one correspondence (1.7) between the orbits $\{b\}$ of the primitive solutions of (1.1) and the orbits $\{C\}$ of the solutions $C \bmod A$ of congruence (1.4) imply the finiteness of the number of orbits $\{b\}$. In Section 2 we classified the orbits $\{C\}$ in the case of one-dimensional matrices $A = p^\nu\{A\}$ with $\nu \leq 3$. Preserving the possibility of classifying the orbits $\{b\}$, we shall restrict ourselves to the calculation of the number of these orbits.

3.1. Suppose that in the notation of Section 2 $C = (C_0 \mid \ldots \mid C_\alpha \mid \ldots)$ and $G = G(C) \oplus G_{\mathrm{res}}$, where $G(C)$ is the direct sum of the blocks G_α, for which $G_\alpha \not\equiv 0 \pmod{p^\nu}$. Then, similarly, $Q' \sim Q'(C) \oplus \frac{1}{a} G_{\mathrm{res}}$, and therefore, the form (1.5) decomposes in the direct sum

$$Q_G^A(C) \sim Q(C) \oplus \frac{1}{a} G_{\mathrm{res}}, \qquad Q(C) = \begin{pmatrix} A & C_{\not\equiv 0} \\ {}^t C_{\not\equiv 0} & Q'(C) \end{pmatrix}. \tag{3.1}$$

Thus, choosing $C = (0 \mid \ldots \mid 0)$ and $C = (C_{0,\mathrm{fix}} \mid 0 \ldots)$ for $A = p\{A\}$, we get, according to Proposition 2.1, the forms $Q(C) = A$ and $Q(C) = 1_2^-$. From this and from decomposition (3.1) we obtain

Proposition 3.1. *The number of orbits $\{b\}$ of the solutions of* (1.1) *with $A = p\{A\}$ is equal to the weighted number of decompositions $Q \sim X \oplus Y$, where the forms X have the following appearance and weights:*

$$pX_1 = p\{A\}, \quad w_1 = 1, \qquad X_{20} = 1_2^-, \quad w_{20} = 1.$$

Remark. The "weighted" number means that every decomposition is counted the number of times corresponding to w. In the next items we shall encounter nonidentity weights, and this explains the use of this terms (for the sake of uniformity).

3.2. If $A = p^2\{A\}$, then the encircling vectors C of form (2.4) are added:

$$C_{\mathrm{fix}} = pC'_{\mathrm{fix}} = (0 \mid \ldots \mid pC'_\alpha \mid 0 \ldots)$$

with the block $C'_\alpha = (1\, 0 \ldots 0)$ and $\alpha \geq 2$.

Lemma 3.1. *For the fixed form G the enumerated vectors give a complete system of representatives of all diferent orbits $\{C\}$ of the solutions $C \bmod p^2$ of the congruence $E[C] \equiv -G \pmod{p^2}$.*

Proof. According to (2.4), we have reprsentatives C of all orbits, and, consequently, it remains to show that these orbits are different. For G of dimension $k_0 = 1$ we have one vector $C_{0,\mathrm{fix}}$, and there is nothing to prove. Let $k_0 = 0$ ($k_1 = 0$ always). According to [1, (10.7)], in the orthogonal group $\mathrm{O}(G)$ any matrix $\sigma = (x_{ij})$ with the partition into blocks consistent with the partition into blocks of the form

$$G = \bigoplus_{\alpha \geq 2} p^\alpha G_{p^\alpha}, \qquad |G_{p^\alpha}| \not\equiv 0 \pmod{p},$$

can be written as

$$\sigma = \begin{pmatrix} x_{22} & px'_{23} & \ldots & p^{\alpha-2}x'_{2\alpha} & \ldots \\ x_{32} & x_{33} & \ldots & p^{\alpha-3}x'_{3\alpha} & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ x_{\alpha 2} & x_{\alpha 3} & \ldots & x_{\alpha\alpha} & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots \end{pmatrix}. \tag{3.2}$$

All blocks x_{ij}, x'_{ij} have p-integer coefficients and the diagonal blocks x_{ii} belong to the groups $\mathrm{O}(G_{p^i} / \bmod p)$. Since (3.2) yields the congruence

$$C \cdot \sigma = (\ldots \mid pC'_\alpha x_{\alpha\alpha} \mid 0 \ldots) \pmod{p^2}, \tag{3.3}$$

α and $c_\alpha \bmod p$, where $G_{p^\alpha}^{-1}[{}^t C'_\alpha] = c_\alpha$, parametrize the orbits $\{C\}$. We have proved the lemma.

From Lemma 3.1 and Proposition 2.2 we obtain

Proposition 3.2. *Equation* (1.1) *with* $A = p^2\{A\}$ *has the number of orbits* $\{b\}$ *which is equal to the weighted number of decompositions* $Q \sim X \oplus Y$, *where the forms* X *have the following appearance and weights:*

(1) *one-dimensional forms*

$$p^2 X_1 = p^2\{A\}, \qquad w_1 = 1;$$

(2) *two-dimensional forms*

$$X_{20} = 1_2^-, \quad pX_{20} = p \cdot 1_2^-, \qquad w_{20} = 1,$$
$$X_{22}^{\eta} = 1^{\eta_1} \oplus p^2 \cdot 1^{\eta_2}, \qquad w_{22}^{\eta} = (\eta),$$
$$X_{2\alpha} = \{A\} \oplus p^{\alpha} \cdot 1^{\pm} \qquad \text{for} \quad \alpha > 2, \qquad w_{2\alpha} = \frac{p-1}{2};$$

(3) *three-dimensional forms*

$$X_{32} = 1_2^- \oplus p^2 \cdot \{A\}, \qquad w_{32} = 1,$$
$$X_{3\alpha} = \{A\} \oplus p^{\alpha} \cdot 1_2^- \qquad \text{for} \quad \alpha \geq 2, \qquad w_{3\alpha} = 1.$$

3.3. For $A = p^3\{A\}$, in addition to vectors C of types 1 and 2

$$(C_{0,\mathrm{fix}} \mid 0 \dots) \quad \text{and} \quad (0 \mid \dots \mid 0), \quad (0 \mid \dots \mid p^2 C'_{\alpha} \mid 0 \dots)$$

with $\alpha \geq 3$ in the case of the form

$$G = \bigoplus_{\alpha \geq 2} p^{\alpha} G_{p^{\alpha}},$$

where $k_0 = k_1 = 0$, $k_2 = 1$, and $G_{p^2} \sim -E$, there appear the vectors of the third type

$$(C_2 \mid 0 \dots) \qquad \text{with} \qquad C_2 = p(C'_{2,\mathrm{fix}} + pC''_2), \qquad C''_2 \bmod p, \tag{3.4}$$

and

$$(C_2 \mid \dots \mid p^2 C'_{\alpha} \mid 0 \dots) \qquad \text{with} \qquad C'_{\alpha} = (1\, 0 \dots 0) \quad \text{and} \quad \alpha \geq 4. \tag{3.5}$$

Here the value $\alpha = 3$ is excluded. Obviously, orbits of different types are different themselves since every type has its own form G. The reasoning for vectors of the first two types repeats the reasoning from item 3.2 for the case $A = p^2\{A\}$.

According to (3.2), the matrices σ from the orthogonal group $\mathrm{O}(G)$ transform the vector C (3.5) into the vector $C \cdot \sigma$ of the form

$$(pC'_2 x_{22} + p^2 C'_{\alpha} x_{\alpha 2} \mid \dots \mid p^{\alpha-1} C'_{\alpha} x'_{2\alpha} + p^2 C'_{\alpha} x_{\alpha\alpha} \mid p^{\alpha} C'_2 x'_{2,\alpha+1} + p^3 C'_{\alpha} x_{\alpha,\alpha+1} \mid \dots).$$

Therefore, if we a priori assume the fulfillment of the condition $\alpha > 3$, then the number α of the last, $\bmod p$ nondegenerate block C'_{α} is an invariant of the orbit $\{C\}$. Since, in addition, the congruence of α-blocks $C \cdot \sigma \equiv p^2 C'_{\alpha} x_{\alpha\alpha} \pmod{p^3}$ is fulfilled for $x_{\alpha\alpha} \in \mathrm{O}(G_{p^{\alpha}} / \bmod p)$, it follows that $c_{\alpha} \bmod p$ is also an invariant of the orbit. Relation (2.3) show that in the orbit $\{C\}$ the block C'_2 of the vector C is defined only $\bmod p$, and, hence, we can take $C'_2 = C'_{2,\mathrm{fix}}$. Consequently, for

$\alpha \geq 4$ every form $Q(C) = E_c$ from decomposition (2.13) writen as $1_2^- \oplus p^{\alpha-1} \cdot 1^{\pm}$ has the weight $(p-1)/2$, and the form $Q(C) = E_0$ from decomposition (2.14) written as $1_2^- \oplus p^{\alpha-1} \cdot 1_2^-$ has the identity weight.

Now if $\alpha = 3$, then, using the defining relationships (2.3) between the blocks of orthogonal matrices, we can show that there exists a matrix σ from the group $\mathrm{O}(G)$ with the block x'_{23}: 3-block $C \cdot \sigma \equiv 0 \pmod{p^3}$. In this case, the orbit $\{C\}$ contains a vector C of form (3.4). Suppose that the congruence

$$C \cdot \sigma \equiv (pC'_2 x_{22} \mid p^2 C'_2 x'_{23} \mid 0 \ldots) \equiv C \pmod{p^3}$$

is satisfied for this vector and for the arbitrary matrix σ (3.2) from $\mathrm{O}(G)$. Then $x'_{23} \equiv 0 \pmod{p}$ by virtue of the condition $C'_2 \not\equiv 0 \pmod{p}$. From this and from the first relation of (2.3) we have the congruence

$$G_{p^2}[x_{22}] \equiv G_{p^2} \pmod{p^2},$$

and, hence, the block $x_{22} \equiv \pm 1 \pmod{p^2}$ since the form G_{p^2} is one-dimensional. Therefore, for all σ of this kind, the 2-block of the transformed vector $C \cdot \sigma$ satisfies the congruence 2-block $C \cdot \sigma \equiv \pm pC'_2 \pmod{p^3}$. This proves that the vectors C of form (3.4) belong to different orbits and the corresponding forms $Q(C) = E_C$ from decomposition (2.12) written as $1 \oplus p^2 \cdot (-1)$ and $-1 \oplus p^2 \cdot 1$ have the weight $(p-1)/2$ each. We have proved

Proposition 3.3. *The number of orbits* $\{b\}$ *of the solutions of* (1.1) *in the case* $A = p^3\{A\}$ *coincides with the weighted number of decompositions* $Q \sim X \oplus Y$, *where the forms* X *have the following appearance and weights:*

(1) *one-dimensional forms*

$$p^3 X_1 = p^3\{A\}, \qquad w_1 = 1;$$

(2) *two-dimensional forms*

$$\begin{gathered} X_{20} = 1_2^-, \quad pX_{20}, \quad p^2 X_{20}, \qquad w_{20} = 1, \\ X_{22}^1 = \pm 1 \oplus p^2(\mp 1), \qquad w_{22}^1 = p-1, \\ pX_{22}^\eta = p(1^{\eta_1} \oplus p^2 \cdot 1^{\eta_2}), \qquad w_{22}^\eta = (\eta), \\ X_{23} = 1^{\pm} \oplus p^3\{A\}, \qquad w_{23} = \frac{p-1}{2}, \\ pX_{2\alpha} = p(\{A\} \oplus p^\alpha \cdot 1^{\pm}) \qquad \text{for} \quad \alpha \geq 3, \qquad w_{2\alpha} = \frac{p-1}{2}; \end{gathered}$$

(3) *three-dimensional forms*

$$\begin{gathered} pX_{32} = p(1_2^- \oplus p^2\{A\}), \qquad w_{32} = 1, \\ X_{33} = 1_2^- \oplus p^3\{A\}, \qquad w_{33} = 1, \\ pX_{3\alpha} = p(\{A\} \oplus p^\alpha \cdot 1_2^-) \qquad \text{for} \quad \alpha \geq 2, \qquad w_{3\alpha} = 1, \\ X_{3\alpha} = 1_2^- \oplus p^\alpha \cdot 1^{\pm} \qquad \text{for} \quad \alpha \geq 3, \qquad w_{3\alpha} = \frac{p-1}{2}; \end{gathered} \tag{3.6}$$

(4) *four-dimensional forms*

$$X_{4\alpha} = 1_2^- \oplus p^\alpha \cdot 1_2^- \qquad for \quad \alpha \geq 2, \qquad w_{4\alpha} = 1.$$

Remark. In the case of primitive representations of cubes $A = p^3\{A\}$ a new phenomenon appears. The three-dimensional quadratic forms $Q = Q(C)$, which are equivalent to the form $X_{33} = 1_2^- \oplus p^3\{A\}$ from (3.6), admit two types of the so-called minimal primitive representations of the numbers $A = p^3\{A\}$, corresponding, respectively, to the forms G from item 1.1 which can be written as

$$G \sim p^3 \cdot 1_2^- \qquad \text{and} \qquad G \sim p^2(-\{a\}\{A\}) \oplus p^4\{a\}\{A\}.$$

The total number of all orbits $\{b\}$ of solutions of equation $Q[b] = p^3\{A\}$ is, according to Proposition 3.3, equal to $p+2$. Out of this number, $1 + (p-1)/2 = (p+1)/2$ orbits $\{b\}$ belong to the minimal representations and $(p+3)/2$ orbits belong to the other types.

ACKNOWLEDGMENTS

The work was supported by the Russian Foundation for Fundamental Research (project no. 96-01-00502).

REFERENCES

1. Zhuravlev, V. G., Representing of the Form by the Genus of Quadratic Forms, *Algebra i Analiz*, 1996, vol. 8, no. 1, pp. 21–112.
2. Conway, J. H. and Sloane, N. J. A., *Sphere Packings, Lattices and Groups*, Springer, 1988.
3. Artin, E., *Geometric Algebra*, Princeton Univ., 1957.
4. Cassels, J., *Rational Quadratic Forms*, London Academic, 1978.
5. Vinogradov, I. M., *Osnovy teorii chisel* (Foundations of Number Theory), Moscow: Nauka, 1953.

Translated by I. Aleksandrova