В. Г. Журавлев, Примитивные вложения в локальные решетки простого определителя, *Алгебра и анализ*, 1999, том 11, выпуск 1, 87–117

Алгебра и анализ
Том 11 (1999), вып. 1

ПРИМИТИВНЫЕ ВЛОЖЕНИЯ В ЛОКАЛЬНЫЕ РЕШЕТКИ ПРОСТОГО ОПРЕДЕЛИТЕЛЯ

© В. Г. Журавлев

Изучаются свойства ветвлений для вложений локальных решеток или квадратичных форм над кольцом целых p-адических чисел $\mathbb{Z}_p$. Следуя аналогиям с ветвлениями абелевых расширений, находятся минимальные неразложимые вложения — аналог простых чисел и дивизоров. Доказано, что любое примитивное вложение в решетку простого определителя распадается в прямую ортогональную сумму минимальных неразложимых вложений первой и второй степеней. Как приложение, вычисляется количество орбит представлений форм над нечетным кольцом $\mathbb{Z}_p$ и доказывается глобальная формула веса представлений форм родом форм над кольцом целых рациональных чисел $\mathbb{Z}$.

§0. Введение

Рассмотрим квадратичную диофантову систему уравнений

$$\begin{gathered} x_0^2+\cdots+x_5^2=a,\quad y_0^2+\cdots+y_5^2=c,\\ x_0y_0+\cdots+x_5y_5=b,\\ x_0+\cdots+x_5=0,\quad y_0+\cdots+y_5=0, \end{gathered} \tag{1}$$

где переменные x_i, y_i и свободные члены a, b, c принадлежат кольцу целых рациональных чисел $\mathbb{Z}$. Система (1) представляет собой координатную запись матричного уравнения

$$Q[b]={}^tbQb=A \tag{2}$$

с целыми симметрическими матрицами Q, A размерностей n, m, где b пробегает целые $n\times m$— матрицы. Система уравнений (1) получается, если взять

$$Q_5=\begin{pmatrix} 2 & 1 & \dots & 1\\ 1 & 2 & \dots & 1\\ \dots & \dots & \dots & \dots\\ 1 & 1 & \dots & 2 \end{pmatrix},\qquad A=\begin{pmatrix} a & b\\ b & c \end{pmatrix} \tag{3}$$

Ключевые слова: диофантовы системы квадратичных уравнений, решетки и квадратичные формы, минимальные неразложимые вложения.

Работа выполнена при поддержке РФФИ, грант 93-011-260.

-матрицы размеров $n = 5$ и $m = 2$. Они являются матрицами квадратичных форм, и уравнение (2) можно рассматривать как представление формы A формой Q. Если A — одномерная форма, то приходим к задаче о количестве представлений $r(A, Q)$ числа A квадратичной формой Q. Эта и более общая задача о числе решений $r(A, Q)$ матричного уравнения (2) решается с помощью аналитических методов, формулы Зигеля [1], тета-рядов и операторов Гекке [2, 3] и с помощью метода Гаусса, использованного им для нахождения количества представлений числа суммой трех квадратов целых чисел.

В [4] получена некоторая общая формула веса представлений квадратичных форм родом форм. Эта формула для числа решений $r(A, Q_5)$ системы (1) принимает следующий вид:

$$r(A, Q_5) = 30 \cdot \left(3 + \left(\frac{a'}{3}\right)\right) \prod_{p|a'} \left(p + \varepsilon_1(A)\left(\frac{6}{p}\right)\right), \tag{4}$$

где a, $c > 0$ — четные числа, $ac - b^2 = a' > 0$ — нечетное бесквадратное число, не делящееся на 3, а $\varepsilon_1(A)$ равно ненулевому значению символа Лежандра $(\frac{a}{p})$ или $(\frac{c}{p})$. Определитель d формы Q_5 равен 6, и в формуле (4) предполагается отсутствие общих делителей для d и определителя $d' = a'$ формы A. Случай невзаимно-простых d и d' является трудным при любом подходе.

В данной статье, следуя методу Гаусса, доказывается формула веса представлений для форм Q и A с невзаимно-простыми определителями d и d' (теорема 7.1). Так, для системы (1) эта теорема дает формулу

$$r(A, Q_5) = 30 \cdot (9 + \varepsilon_3(A)) \prod_{p|a'} \left(p + \varepsilon_1(A)\left(\frac{6}{p}\right)\right), \tag{5}$$

где $\varepsilon_3(A)$ равно ненулевому значению $(\frac{a \cdot a'}{3})$ или $(\frac{c \cdot a'}{3})$, форма A (3) имеет нечетный бесквадратный определитель $d' = 3 \cdot a'$, т.е. d и d' имеют общий простой делитель $p = 3$.

Особенности этого случая проясняются, если от кольца $\mathbb{Z}$ перейти к кольцу целых p-адических чисел $\mathbb{Z}_p$ и рассмотреть примитивные представления

$$Q[b] = A, \quad b \in M_{n,m}(\mathbb{Z}_p) \tag{6}$$

над локальным кольцом $\mathbb{Z}_p$. Если p не делит d или d' и уравнение (6) имеет решения b, то они образуют одну двухстороннюю орбиту $\{b\}$ (предложение 1.1). Если же p делит оба определителя d, d', то имеет место явление ветвления и множественности орбит.

В статье исследуются формы Q с разложением над $\mathbb{Z}_p$ в прямую сумму

$$Q \sim Q_1 \oplus pQ_p \tag{7}$$

с невырожденными блоками Q_1, $Q_p \mod p$ и с одномерным блоком Q_p, т.е. простое p входит в определитель d формы Q в первой степени. Пусть аналогично форма $A \sim A_1 \oplus A_{\geqslant p}$, где $A_{\geqslant p} = pA_p \oplus A_2$, блок A_2 делится на p^2 и размерность формы A равна $m = m_1 + m_{\geqslant p}$ с $m_{\geqslant p} = m_p + m_2$. Тогда имеются простые условия

$$m + m_p < n - 1, \quad m_p > 1,$$

выполнение которых достаточно для существования двух типов представлений b_{I}, b_{II} (6) из разных орбит. С орбитами $\{b_1\}$, $\{b_{\mathrm{II}}\}$ связываются неэквивалентные формы G_{I}, G_{II} размерности $n-m$, и такая связь лежит в основе метода Гаусса. Формулы (4), (5) отличаются локальными множителями

$$\alpha_3(A, Q_5) = 3 + \left(\frac{a'}{3}\right) \quad \text{и} \quad \alpha_3(A, Q_5) = 9 + \varepsilon_3(A).$$

Множители $\alpha_p(A, Q)$ для простых p, делящих d и d', имеют сложную структуру, и их вычисление представляет основную трудность. Для форм Q, (7) существование ветвления проявляется в том, что $\alpha_p(A, Q)$ распадается на два слагаемых (п. 7.4)

$$\alpha_p(A, Q) = \alpha_p(A, Q, G_{\mathrm{I}}) + \alpha_p(A, Q, G_{\mathrm{II}}).$$

Вычислить же множители $\alpha_p(A, Q, G_i)$ значительно проще (§7), так как вычисление сводится к нахождению $c_p(A, Q, G_i)$ — числа решений $C \mod A$ матричного сравнения (§6)

$$qA^{-1}[C] + G_i \equiv 0 \pmod{q\mathbb{Z}_p}, \quad i = \mathrm{I}, \mathrm{II},$$

где q — p-ступень формы A.

§1. Локальные унимодулярные квадратичные формы

1.1. Вначале рассмотрим квадратичные формы с $\mathbb{Z}_p$-целыми симметрическими матрицами $Q = Q_1$ определителя $|Q_1| \not\equiv 0 \pmod p$ для *нечетного простого* p. Отождествляя квадратичные формы с их матрицами, будем говорить, что целая форма A с определителем $|A| \neq 0$ примитивно вкладывается в $Q : A \hookrightarrow Q$, если матричное уравнение

$$Q[b] = {}^tbQb = A \tag{1.1}$$

имеет *примитивное* решение b из множества $n \times m$-матриц $M_{n,m}(\mathbb{Z}_p)$, т.е. ранг $r_p(b) = \operatorname{rank}(b \bmod p) = m$. Здесь и далее предполагаются $\dim A = m$, $\dim Q = n$ и $1 \leqslant m < n$. Используя теорию приведения квадратичных форм над локальным кольцом $\mathbb{Z}_p$, $p \neq 2$ [5, с. 131], можем считать

$$A = \begin{pmatrix} A_1 & \\ & A_1^{\perp} \end{pmatrix} = A_1 \oplus A_1^{\perp}$$

прямой ортогональной суммой некоторой формы A_1 размерности 1 и ее ортогонального дополнения $A_1^{\perp}$.

1.2. Пусть $A_1 \not\equiv 0 \pmod p$. Примитивность представления b (1.1) равносильна существованию дополнительной матрицы e из $M_{n,k}(\mathbb{Z}_p)$, $k = n - m$, с условием, что *расширенная матрица* $B = (b \mid e)$ принадлежит унимодулярной группе $\mathrm{SL}_n^{\pm}(\mathbb{Z}_p)$ матриц с коэффициентами из $\mathbb{Z}_p$ и определителем ± 1. Выбираем такую дополнительную матрицу e', чтобы

$$ {}^t b_1 Q e' = 0, \quad \text{где } b = (b_1 \dots b_m) $$

— разбиение матрицы b на столбцы. Для любой фиксированной матрицы e полагаем $e' = b_1\Lambda + e$ с Λ из $M_{1,k}(\mathbb{Z}_p)$. Так как, согласно (1.1), ${}^t b_1 Q e' = A_1\Lambda + {}^t b_1 Q e$ и $A_1 \not\equiv 0 \pmod p$, то $\Lambda = -A_1^{-1} \cdot {}^t b_1 Q e$ дает нужную матрицу e'. В этом случае матрица $B' = (b \mid e')$ из группы $\mathrm{SL}_n^{\pm}(\mathbb{Z}_p)$ преобразует форму Q в *эквивалентную* ей форму $Q' = Q[B'] \sim Q$ вида

$$ Q' = A_1 \oplus A_1^{\perp}(Q'), \quad \text{где } A_1^{\perp}(Q') = \begin{pmatrix} A_1^{\perp} & * \\ * & * \end{pmatrix}. $$

Таким образом, любое вложение $b : A \hookrightarrow Q$ при подходящем выборе базисов соответствующих решеток распадается в прямую сумму

$$ b : A = A_1 \oplus A_1^{\perp} \hookrightarrow Q = A_1 \oplus A_1^{\perp}(Q), $$

т.е. $b = b_1 \oplus b_1^{\perp}$ и $b_1 : A_1 \hookrightarrow A_1$, $b_1^{\perp} : A_1^{\perp} \hookrightarrow A_1^{\perp}(Q)$ — примитивные вложения. При этом

$$ b_1 : A_1 \hookrightarrow A_1, \quad \text{где } \dim A_1 = 1,\ A_1 \not\equiv 0 \pmod p, $$

— *минимальное неприводимое вложение*. В общем случае формы $A = A_1 \oplus A_{\geqslant p}$ с блоками $|A_1| \not\equiv 0 \pmod p$ и $A_{\geqslant p} \equiv 0 \pmod p$ также будет $b = b_1 \oplus b_1^{\perp}$, и вложение b_1 распадается в прямую сумму $m_1 = \dim A_1$ одномерных минимальных неприводимых вложений.

1.3. Пусть снова $\dim A_1 = 1$ и $A_1 \equiv 0 \pmod p$. Найдем b_1' из $M_{n,1}(\mathbb{Z}_p)$ с условием ${}^t b_1' Q b = (10 \dots 0)$ или ${}^t b_1'' \cdot b = (10 \dots 0)$ для ${}^t b_1'' = {}^t b_1' \cdot Q$ и $r_p(b) = m$ (1.1). Можем считать

$$ b = \begin{pmatrix} b^{(m)} \\ * \end{pmatrix}^{(m)}_{(n-m)}, \quad |b^{(m)}| \not\equiv 0 \pmod p, $$

т.е. $b^{(m)}$ принадлежит $\mathrm{GL}_m(\mathbb{Z}_p)$. Положим ${}^t b_1'' = (\underbrace{* \cdots *}_{m} | 0 \dots 0)$, и тогда ${}^t b_1'' \cdot b = (* \cdots *) b^{(m)} = (10 \dots 0)$, и так как по условию $|Q| \not\equiv 0 \pmod p$, то $b_1' = Q^{-1} \cdot b_1''$ — требуемый столбец.

Добавляя к b (1.1) столбец b_1', получаем $b' = (b_1 b_1' \mid b_2 \dots b_m)$ и $Q[b'] = \left(\begin{smallmatrix} A_1 & 1 \\ 1 & 0 \end{smallmatrix}\right) \oplus A_1^{\perp}$. Покажем, что ранг $r_p(b') = m + 1$. Предположим противное $b_1' \equiv \lambda_1 b_1 + \dots +$

$\lambda_m b_m \pmod p$, где $r_p(b) = m$. Имеем ${}^t b_1' \cdot Q b_1 \equiv \lambda_1 Q[b_1] + \cdots + \lambda_m b_m Q b_1 \equiv \lambda_1 A_1 \equiv 0 \pmod p$, что противоречит равенству ${}^t b_1' \cdot Q b_1 = 1$. По доказанному $r_p(b') = m+1$, и, значит, существует расширенная матрица вида $B = (b' \mid e)$ из $\mathrm{SL}_n^{\pm}(\mathbb{Z}_p)$.

Далее действуем по аналогии с п. 1.2, полагая $e' = (b_1 b_1') \cdot \Lambda + e$ с целой $2 \times (k-1)$-матрицей Λ. Условие ${}^t(b_1 b_1') \cdot Q e' = 0$ теперь приводит к выбору $\Lambda = -\begin{pmatrix} A_1 & 1 \\ 1 & * \end{pmatrix}^{-1} \cdot {}^t(b_1 b_1') Q e$. Итак, найдем базис из столбцов матрицы $B' = (b' | e')$, в котором форма Q приобретает вид

$$Q' = Q[B'] = \begin{pmatrix} A_1 & 1 \\ 1 & * \end{pmatrix} \oplus \begin{pmatrix} A_1^{\perp} & * \\ * & * \end{pmatrix} \quad \text{с } A_1 \equiv 0 \pmod p.$$

Первую форму можно привести к более *каноническому виду* $J(A_1) = \begin{pmatrix} A_1 & 1 \\ 1 & 0 \end{pmatrix}$, если сделать замену $b_1'' = \lambda b_1 + b_1'$ и потребовать, чтобы $Q[b_1''] = A_1 \lambda^2 + 2\lambda + Q[b_1'] = 0$. Это уравнение имеет решение λ из $\mathbb{Z}_p$, поскольку простое p нечетное. Новое скалярное произведение ${}^t b_1'' \cdot Q b_1 = \lambda A_1 + 1 \equiv 1 \pmod p$, и поэтому для $b_1' = (\lambda A_1 + 1)^{-1} \cdot b_1''$ получаем нужную форму $Q[(b_1 b_1')] = J(A_1)$.

1.4. Это, переходя к обозначениям п. 1.2 $A = A_1 \oplus A_{\geqslant p}$, означает, что вложение $b : A \hookrightarrow Q$ (1.1) распадается в прямую ортогональную сумму $b = b_1 \oplus b_{\geqslant p} \oplus b^{\perp}$:

$$b : A = A_1 \oplus A_{\geqslant p} \hookrightarrow Q = A_1 \oplus J(A_{\geqslant p}) \oplus Q^{\perp}, \tag{1.2}$$

где $J(A_{\geqslant p}) = \begin{pmatrix} A_{\geqslant p} & 1 \\ 1 & 0 \end{pmatrix}$ — *гиперболическая форма* размерности $2m_{\geqslant p}$, $m_{\geqslant p} = \dim A_{\geqslant p}$ и $Q^{\perp} = Q \ominus J(A)$ с $J(A) = A_1 \oplus J(A_{\geqslant p})$. Здесь *разность* $X \ominus Y$ есть любая форма Z из разложения $X \sim Y \oplus Z$. Вложение $b_1 \oplus b_{\geqslant p} = b_{\min}$ является минимальным вложением $b_{\min} : A \hookrightarrow A_1 \oplus J(A_{\geqslant p})$ формы A *размерности* $m_1 + 2m_{\geqslant p}$. Если блоки A_1 и $A_{\geqslant p}$ разложить на одномерные составляющие $A_1 = \bigoplus\limits_j A_{1j}$, $A_{\geqslant p} = \bigoplus\limits_j A_{\geqslant p,j}$, то $b_{\min}$ разложится в прямую сумму *минимальных неразложимых вложений* вида

$$A_{1j} \hookrightarrow A_{1j}, \quad A_{\geqslant p,j} \hookrightarrow J(A_{\geqslant p,j}) \tag{1.3}$$

размерностей 1 и 2.

1.5. Если уравнение (1.1) разрешимо, то, согласно (1.2), можем считать $b = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ с единичным блоком размерности $m = \dim A$ и форма Q имеет вид

$$Q = \begin{pmatrix} A & C \\ {}^t C & Q' \end{pmatrix} \quad \text{с блоками } C = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},\ Q' = \begin{pmatrix} 0 & \\ & Q^{\perp} \end{pmatrix}. \tag{1.4}$$

В матрице C единичный блок имеет размерность $m_{\geqslant p} = \dim A_{\geqslant p}$, и C называется *сцепляющей матрицей* (подробности см. [4]). Все примитивные решения

$b : Q[b] = A$ разбиваются на *классы* $\mathrm{pb}(A, Q, \{G\})$, нумеруемые классами $\{G\}$ форм

$$G = aQ' - aA^{-1}[C], \tag{1.5}$$

где $a = \operatorname{level} A$ — некоторая фиксированная *ступень* (*p-ступень*) матрицы A. По определению $a = p^{\nu}\{a\}$ — ненулевое целое число из $\mathbb{Z}_p$, где $p^{-\nu} = |a|_p$ обозначает *p-норму*, для которого матрица $a \cdot A^{-1}$ целая и $\nu = 0, 1, 2, \ldots$ минимальное с таким свойством. Классы эквивалентности форм $\{G\}$ рассматриваются относительно $\mathrm{SL}^{\pm}(\mathbb{Z}_p)$. Разложение (1.2) показывает, что в случае $Q = Q_1$ возможен лишь один класс $\{G\}$ формы

$$G = -aA^{-1}_{\geqslant p} \oplus aQ^{\perp} \tag{1.6}$$

при условии существования разности $Q^{\perp} = Q \ominus J(A)$ или, более кратко, если $J(A) \leqslant Q$.

Пусть C — произвольная матрица $C \mod A$, удовлетворяющая *матричному сравнению*

$$aA^{-1}[C] \equiv -G \pmod{a}. \tag{1.7}$$

Здесь сравнение $C \equiv C' \pmod{A}$ означает, что матрица $A^{-1}(C - C')$ целая, а $\mod a$ — сокращение $\mod a \cdot \mathbb{Z}_p$. Тогда C определяет примитивное вложение формы A в целую невырожденную форму вида

$$Q^A_G(C) = \begin{pmatrix} A & \\ & \frac{1}{a}G \end{pmatrix}[M_C^{-1}] = \left(\begin{array}{c|c} A & C \\ \hline {}^tC & A^{-1}[C] + \frac{1}{a}G \end{array}\right), \tag{1.8}$$

где матрица $M_C = \left(\begin{smallmatrix} 1 & -A^{-1} \cdot C \\ 0 & 1 \end{smallmatrix}\right)$ может быть нецелой. Все формы G (1.5), отвечающие примитивным вложениям b (1.1), и, в частности, форма (1.6) имеют определитель

$$|G| = a^{n-m}|Q|/|A|. \tag{1.9}$$

Многие вопросы о представлениях b (1.1) сводятся к соответствующим свойствам сцепляющих матриц C. Так, число $c(A, Q, G)$ решений $C \in C(A, Q, G)$ матричного сравнения (1.7) с условием $Q^A_G(C) \sim Q$ является *локальным множителем* $c_p(A, Q, G)$ в формуле веса примитивных представлений над кольцом целых рациональных чисел $\mathbb{Z}$ формы A родом $[Q]$ формы Q, отвечающих роду формы G [4, с. 43, 51]. Также существует *биекция*

$$\mathrm{pb}(A, Q, \{G\}) \supset \{b\} \xrightarrow[\sim]{[A,Q,G]/\bmod A} \{C\} \subset C(A, Q, G) \tag{1.10}$$

между *двухсторонними орбитами*

$$\{b\} = \{\sigma b U : \sigma \in O(Q), U \in O(A)\},$$
$$\{C\} = \{{}^tUCV \bmod A : U \in O(A), V \in O(G)\},$$

где $O(\cdot) = O_{\mathbb{Z}_p}(\cdot)$ обозначает *группу целых автоморфизмов* соответствующей квадратичной формы. Биекция (1.10) сохраняется при дроблении орбит $\{\cdot\}$ на *односторонние орбиты* $[b]$ относительно группы $O(Q)$ и $[C]$ относительно $O(G)$ [4, с. 38]. Отметим, что из (1.10) вытекает конечность числа орбит примитивных вложений $b : A \hookrightarrow Q$.

1.6. Рассмотрим сравнение (1.7) с формой G (1.6). Так как решения $C \mod A$ и $A = A_1 \oplus A_{\geqslant p}$ п. 1.4, то полагаем $C = \begin{pmatrix} 0 & 0 \\ C_1 & C_2 \end{pmatrix}$, и тогда

$$aA_{\geqslant p}^{-1}[C_1] \equiv aA_{\geqslant p}^{-1} \pmod a, \quad \text{где } C_1 \bmod A_{\geqslant p}, \tag{1.11}$$

и

$${}^tC_1 \cdot aA_{\geqslant p}^{-1}C_2 \equiv 0 \pmod a.$$

Согласно [4, с. 58], $|C_1| \not\equiv 0 \pmod p$, т.е. C_1 принадлежит $\mathrm{GL}(\mathbb{Z}_p)$, и поэтому $aA_{\geqslant p}^{-1}C_2 \equiv 0 \pmod a$ или $C_2 \equiv 0 \pmod{A_{\geqslant p}}$). Множество решений сравнения (1.11) образует *ортогональную группу* $O(aA_{\geqslant p}^{-1}, A_{\geqslant p})$. Ее *порядок* $o(aA_{\geqslant p}^{-1}, A_{\geqslant p})$ вычислен в [4, с. 79]. Приведенные рассуждения показывают, что решения C сравнения (1.7) имеют вид $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} V$ с $V = \begin{pmatrix} \overline{C}_1 & 0 \\ 0 & 1 \end{pmatrix}$ из группы $O(G)$ и с блоком $\overline{C}_1 \equiv C_1 \pmod A_{\geqslant p}$, где C_1 пробегает группу $O(aA_{\geqslant p}^{-1}, A_{\geqslant p})$. При этом использовано свойство *эпиморфности* гомоморфизма [6, с. 125]

$$O(aA_{\geqslant p}^{-1}) \xrightarrow{\bmod A_{\geqslant p}} O(aA_{\geqslant p}^{-1}, A_{\geqslant p}). \tag{1.12}$$

Таким образом, решения C сравнения (1.7) образуют одну орбиту $[C_{\mathrm{fix}}]$ с представителем $C_{\mathrm{fix}} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ (1.4), и число решений равно порядку $o(aA_{\geqslant p}^{-1}, A_{\geqslant p})$. Для всех C квадратичная форма $Q_G^A(C)$ эквивалентна форме Q (1.4), и, значит, $c(A, Q, G)$ равно числу решений сравнения (1.7). Итак, доказано

Предложение 1.1. *Пусть форма $Q = Q_1$ имеет определитель $|Q_1| \not\equiv 0 \pmod p$ для $p \neq 2$. Тогда существует примитивное представление $b : Q[b] = A$ только в случае $J(A) \leqslant Q$. Решения образуют одну орбиту $[b]$, и соответствующие вложения $b : A \hookrightarrow Q$ распадаются в прямую сумму минимальных неразложимых вложений* (1.3) *степени* 1 *и* 2. *Локальные множители $c(A, Q, G) \neq 0$ только для форм G, эквивалентных форме* (1.6), *и в этом случае*

$$c(A, Q, G) = o(aA_{\geqslant p}^{-1}, A_{\geqslant p}). \tag{1.13}$$

Замечание. Единственность орбиты $[b]$ вытекает уже из единственности разложения (1.2). В п. 1.5, 1.6 на простом примере показан общий метод, используемый в дальнейшем в существенно более сложной ситуации.

§2. Квадратичные системы сравнений

2.1. Воспользуемся предложением 1.1 и найдем число решений $b \bmod p^\delta$ матричного сравнения

$$Q[b] \equiv A \pmod{p^\delta}, \quad \text{где } r_p(b) = m,\ \delta \geqslant 1. \tag{2.1}$$

Обозначим $\mathrm{PN}(A, Q/p^\delta)$ множество решений b этой системы.

Если положить $b' = b + p^\delta b_1$ и $M^s = M + {}^tM$, то

$$Q[b'] \equiv Q[b] + p^\delta({}^tb_1 Q \cdot b)^s \equiv A \pmod{p^{\delta+1}}$$

равносильно сравнению $({}^tb_1 Q \cdot b)^s \equiv M \pmod p$ с целой симметрической матрицей $M = p^{-\delta}(A - Q[b])$. По условию b примитивно и, значит, $b = U\begin{pmatrix}1\\0\end{pmatrix}$ для некоторой матрицы U из $\mathrm{GL}(\mathbb{Z}_p)$. Пусть

$${}^tb_1' = (\underset{(m)}{{}^tb_{11}'} \mid \underset{(k)}{{}^tb_{12}'}) = {}^tb_1 QU, \quad \text{где } |QU| \not\equiv 0 \pmod p.$$

Тогда последнее сравнение равносильно $(b_{11}')^s \equiv M \pmod p$, и блок b_{12}' может быть любой $k \times m$-матрицей $\bmod p$. Разложим $b_{11}' = S + S_-$ на симметрическую $S = {}^tS$ и кососимметрическую $S_- = -{}^tS_-$ части. Первая однозначно определена $S \equiv 1/2M \pmod p$, $p \neq 2$, а S_- — любая кососимметрическая $m \times m$-матрица $\bmod p$. Таким образом, справедлива

Лемма 2.1. *Если $Q = Q_1$, то отображение $\iota = \iota_\delta^{\delta+1}$ для $\delta \geqslant 1$, переводящее $b \bmod p^{\delta+1} \to b \bmod p^\delta$, задает эпиморфизм*

$$\mathrm{PN}(A, Q/p^\delta) \xleftarrow{\iota} \mathrm{PN}(A, Q/p^{\delta+1}). \tag{2.2}$$

Все b из левой части имеют одно и то же число прообразов $|\iota^{-1}(b)| = p^{\langle m\rangle + mk}$, где $\langle m\rangle = m(m-1)/2$, $k = n - m$.

Следствие 2.1. *Пусть $\mathrm{PN}(A, Q)$ обозначает множество примитивных решений $b : Q[b] = A$ в кольце $\mathbb{Z}_p$, $p \neq 2$, и ι_δ — отображение $b \to b \bmod p^\delta$ для $\delta \geqslant 1$. Тогда*

$$\mathrm{PN}(A, Q/p^\delta) \xleftarrow{\iota_\delta} \mathrm{PN}(A, Q) \tag{2.3}$$

эпиморфно.

2.2. По (2.3) для любого решения b сравнения (2.1) существует решение $\overline{b} \equiv b \pmod{p^\delta}$ уравнения $Q[\overline{b}] = A$ (1.1), и обратно. Следовательно, по предложению 1.1 сравнение (2.1) разрешимо только при условии $J(A) \leqslant Q$. Далее, любое $\overline{b} = \overline{\sigma} \cdot \overline{b}_1$ для фиксированного $\overline{b}_1$ (1.1) и некоторого преобразования $\overline{\sigma}$ из $O(Q)$. Отсюда заключаем $b \equiv \sigma b_1 \pmod{p^\delta}$, где $\sigma = \overline{\sigma} \bmod p^\delta$ принадлежит *ортогональной группе* $O(Q/p^\delta) = \mathrm{PN}(Q, Q/p^\delta)$, т.е. сравнение (2.1) имеет одну *орбиту* $[b/p^\delta] = [b \bmod p^\delta]$.

2.3. Вычислим число решений $\mathrm{pn}(A, Q/p^\delta)$ сравнения (2.1). По только что доказанному и лемме 2.1 записываем

$$\mathrm{pn}(A, Q/p^\delta) = p^{(\delta-1)(\langle m\rangle + mk)}\,\mathrm{pn}(A, Q/p) \tag{2.4}$$

для любого $\delta \geqslant 1$, при этом

$$\mathrm{pn}(A, Q/p) = o(Q/p)/\,\mathrm{stab}(b/p).$$

Здесь $o(Q/p)$ — порядок *ортогональной группы* $O(Q/p)$ матриц $U : Q[U] \equiv Q \pmod{p}$ (см., например, [4, с. 82]), а $\mathrm{stab}(b/p)$ — порядок *стабилизатора* некоторого фиксированного решения $b : Q[b] \equiv A \pmod{p}$.

Согласно (1.2), можем считать, что форма Q имеет вид

$$Q \equiv A_1 \oplus J(m_{\geqslant p}) \oplus Q^\perp \pmod{p},$$

где $J(m_{\geqslant p}) = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ — гиперболическая форма размерности $2m_{\geqslant p}$ с $m_{\geqslant p} = \dim A_{\geqslant p}$ и $|Q^\perp| \not\equiv 0 \pmod{p}$. Пусть

$$b = b_{\mathrm{fix}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}, \qquad \sigma = \begin{pmatrix} \alpha & a & b & c \\ a_1 & A & B & E \\ b_1 & C & D & G \\ c_1 & E_1 & G_1 & F \end{pmatrix} \in O(Q/p)$$

разбиты на блоки аналогично форме Q. Из условия $\sigma b \equiv b \pmod{p}$ вытекает $\alpha, A \equiv 1$ и $a, a_1, b_1, c_1, C, E \equiv 0 \pmod{p}$. Затем условие $Q[\sigma] \equiv Q \pmod{p}$ добавляет сравнения $D \equiv 1$, $b, c, G \equiv 0 \pmod{p}$ и

$$B^s \equiv -Q^\perp[G_1],\ Q^\perp[F] \equiv Q^\perp,\ E + {}^tG_1 Q^\perp \cdot F \equiv 0 \pmod{p}. \tag{2.5}$$

Полагая $B = S + S_-$ (ср. п. 2.1), видим, что $S \equiv -1/2 Q^\perp[G_1] \pmod{p}$, а составляющая $S_- \equiv -{}^tS_- \pmod{p}$ может быть произвольной. Теперь алгоритм решения системы сравнений (2.5) следующий:

1) выбираем любые F из $O(Q^\perp/p)$ и матрицу $E \pmod p$ размеров $m_{\geqslant p} \times (n - m - m_{\geqslant p})$;

2) G_1 однозначно определяется третьим сравнением из (2.5), так как $|Q^\perp| \cdot |F| \not\equiv 0 \pmod p$;

3) наконец, для B находим симметрическую составляющую S.

Это приводит к следующей формуле для стабилизатора

$$\operatorname{stab}(b/p) = p^{\langle m_{\geqslant p}\rangle + m_p(n-m-m_{\geqslant p})} o(Q^\perp/p), \tag{2.6}$$

где форма $Q^\perp = Q \ominus J(A)$ (1.2). Интересно сравнить получающуюся формулу для числа $\operatorname{pn}(A, Q/p)$ вложений $A \hookrightarrow Q \pmod p$ с [7, с. 202].

Из п. 2.2 и 2.3 вытекает

Предложение 2.1. *Для формы $Q = Q_1$ с определителем $|Q_1| \not\equiv 0 \pmod p$, $p \neq 2$, сравнение (2.1) разрешимо тогда и только тогда, когда $J(A) \leqslant Q$. В этом случае оно имеет одну орбиту $[b/p^\delta]$ из $\operatorname{pn}(A, Q/p^\delta)$ (2.4), (2.6) решений.*

Замечание. При $\delta = 1$ получаем теорему Витта [7, с. 165, 173], в которой необходимое условие $m + m_{\geqslant p} \leqslant n$ существования вложения $A \hookrightarrow Q \pmod p$ усилено необходимым и достаточным условием $J(A) \leqslant Q$.

2.4. В формуле Зигеля [1] вес представлений формы родом выражается в виде произведения *локальных плотностей*

$$\alpha_p(A, Q) = p^{-\delta(nm - [m])} n(A, Q/p^\delta),$$

где $[m] = m(m+1)/2$, $n(A, Q/p^\delta)$ — число всех решений сравнения (2.1) и $\delta \gg 0$ — достаточно большое целое число. Примитивную локальную плотность $p\alpha_p(A, Q)$ определим по аналогии, используя число примитивных решений $\operatorname{pn}(A, Q/p^\delta)$. Для нее в случае формы $Q = Q_1$ с $|Q_1| \not\equiv 0 \pmod p$, $p \neq 2$, предложение 2.1 дает явную формулу

$$p\alpha_p(A, Q) = p^{-(n-m)(m+m_{\geqslant p}) - \langle m\rangle + [m_{\geqslant p}]} \frac{o(Q/p)}{o(Q^\perp/p)}. \tag{2.7}$$

В частном случае $|A| \not\equiv 0 \pmod p$ все решения b сравнения (2.1) примитивны. Их общее число равно

$$n(A, Q/p^\delta) = p^{(\delta-1)(\langle m\rangle + m(n-m))} \frac{o(Q/p)}{o(Q^\perp/p)}, \tag{2.8}$$

а локальная плотность —

$$\alpha_p(A, Q) = p^{-m(n-m) - \langle m\rangle} \frac{o(Q/p)}{o(Q^\perp/p)} \tag{2.9}$$

(ср. [8, §9], где исследуются тернарные формы).

§3. Локальные ортогональные преобразования

3.1. Выясним некоторые свойства ортогональных преобразований $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ из группы $O(Q)$ квадратичной формы $Q = \left(\begin{smallmatrix} Q_1 & \\ & qQ_q \end{smallmatrix}\right)$ размерности n и ступени $q \equiv 0 \pmod p$ с невырожденными блоками $|Q_1|$, $|Q_q| \not\equiv 0 \pmod p$, $p \neq 2$, размерностей n_1 и n_q. В этих обозначениях условие $Q[M] = Q$ принимает вид

$$Q_1[A] + qQ_q[C] = Q_1, \quad {}^tAQ_1B + q\,{}^tCQ_qD = 0, \quad Q_1[B] + qQ_q[D] = qQ_q. \tag{3.1}$$

3.2. Пусть целая $n \times m$-матрица $b = \left(\begin{smallmatrix} b' \\ b'' \end{smallmatrix}\right)$ имеет блок b' ранга $r_p(b') = m$ и пусть $b' = U\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ для некоторого U из $\mathrm{GL}_{n_1}(\mathbb{Z}_p)$. Найдем M, преобразующую b в $M \cdot b = \left(\begin{smallmatrix} * \\ 0 \end{smallmatrix}\right)$ с нулевым нижним блоком

$$Cb' + Db'' = 0, \tag{3.2}$$

т.е. $CU\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) = -Db''$. Вначале заметим, что расширенное последнее равенство $CU\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = (-Db''0)$ равносильно

$$C = C(D) = (-Db''0)U^{-1},$$

т.е. для любого D существует $C = C(D)$ с условием (3.2).

Согласно (3.1), $B = qB_1$, $B_1 = -({}^tAQ_1)^{-1} \cdot {}^tCQ_qD$. Поэтому блок $B = B(A, C, D)$ однозначно определяется остальными блоками и (3.1) преобразуется в систему

$$Q_1[A] + qQ_q[C] = Q_1, \quad qQ_1[B_1(A, C, D)] + Q_q[D] = Q_q.$$

Подставляя в нее $C = C(D)$, получаем систему

$$Q_1[A] + qR_1(D) = Q_1, \quad qR_q(A, D) + Q_q[D] = Q_q. \tag{3.3}$$

Здесь $R_q(A, D) = |A|^{-2} \cdot R'_q(A, D)$, $R'_q(A, D)$ и $R_1(D)$ — симметрические матричные полиномы от элементов $\{a_{ij}\}$, $\{d_{ij}\}$ и по первому равенству (3.3) $|A| \not\equiv 0 \pmod p$. Поэтому

$$R_1(D) \equiv R_1(D_1), \; R_q(A, D) \equiv R_q(A_1, D_1) \pmod{p^\alpha},$$

если $A \equiv A_1$, $D \equiv D_1 \pmod{p^\alpha}$ и A, D удовлетворяют системе (3.3).

Ее разрешимость докажем индукцией по α. Для $\alpha \geqslant 1$ из равенства $q = p^\alpha\{q\}$ единичные матрицы $A = 1$, $D = 1$ удовлетворяют сравнениям (3.3) $\bmod p^\alpha$. Пусть теперь A_0, D_0 — некоторые решения сравнения (3.3) $\bmod p^\alpha$ для степени p^α, делящей ступень q. Тогда матрицы $A = A_0 + p^\alpha A_1$, $D = D_0 + p^\alpha D_1$ будут решениями системы (3.3) $\bmod p^{\alpha+1}$ в том и только в том случае, когда A_1, D_1 удовлетворяют системе

$$Q_1[A_0] + p^\alpha({}^tA_0Q_1A_1)^s + qR_1(D_0) \equiv Q_1 \pmod{p^{\alpha+1}},$$
$$qR_q(A_0, D_0) + Q_q[D_0] + p^\alpha({}^tD_0Q_qD_1)^s \equiv Q_q \pmod{p^{\alpha+1}}$$

или, что равносильно,

$$({}^tA_0Q_1A_1)^s \equiv S_1,\ ({}^tD_0Q_qD_1)^s \equiv S_q \pmod p$$

с целыми симметрическими матрицами S_1, S_q. Очевидно, можем взять

$$A_1 \equiv 1/2({}^tA_0Q_1)^{-1}S_1,\ D_1 \equiv 1/2({}^tD_0Q_q)^{-1}S_q \pmod p,$$

поскольку $|A_0|$, $|D_0| \not\equiv 0 \pmod p$ по (3.3) $\bmod p^\alpha$ и $|Q_1|$, $|Q_q| \not\equiv 0 \pmod p$ по условию.

3.3. Для приложений важен еще случай $r_p(b'') = m$, $b' \equiv 0 \pmod q$, когда требуется, чтобы произведение $M \cdot b = \begin{pmatrix} 0 \\ * \end{pmatrix}$ имело верхний нулевой блок $Ab' + Bb'' = 0$, где $b' = qb_1'$ и $B = qB_1$ по (3.1), т.е.

$$Ab_1' + B_1b'' = 0, \quad \text{где } r_p(b'') = m. \tag{3.4}$$

Аналогично п. 3.2 для любого A существует $B_1 = B_1(A)$ — решение (3.4). Далее, согласно (3.1), ${}^tAQ_1 \cdot B_1 + {}^tCQ_qD = 0$. Отсюда ${}^tC = -{}^tAQ_1B_1 \cdot (Q_qD)^{-1}$ и, значит, целая матрица $C = C(A, B_1, D)$ однозначно определяется блоками A, B_1, D. Поэтому система (3.1) принимает вид

$$Q_1[A] + qR_1(A, D) = Q_1, \quad qR_q(A) + Q_q[D] = Q_q,$$

аналогичный (3.3). Итак, доказана

Лемма 3.1. *Пусть форма $Q = Q_1 \oplus qQ_q$ имеет невырожденные* $\bmod p$ *блоки Q_1, Q_q и ступень $q \equiv 0 \pmod p$, $p \neq 2$, и пусть целая матрица $b = \begin{pmatrix} b' \\ b'' \end{pmatrix}$ ширины m разбита на блоки аналогичным образом. Тогда имеют место следующие утверждения.*

1. *Если ранг $r_p(b') = m$, то найдется матрица $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ из ортогональной группы $O(Q)$ с условием $Cb' + Db'' = 0$.*

2. *Если же ранг $r_p(b'') = m$ и $b' \equiv 0 \pmod p$, то найдется M из $O(Q)$ с условием $Ab' + Bb'' = 0$.*

§4. Квадратичные формы простого определителя: m–случай

4.1. Вернемся к уравнению $Q[b] = A$ (1.1), в котором форма Q теперь будет иметь вид $Q = Q_1 \oplus pQ_p$ с невырожденными блоками $|Q_1|, |Q_p| \not\equiv 0 \pmod p$, $p \neq 2$, размерностей $\dim Q_1 = n-1$ и $\dim Q_p = 1$. Форму A размерности $\dim A = m$, $1 \leqslant m < n$, запишем в приведенном виде [5, с. 131] $A = A_1 \oplus A_{\geqslant p}$ с блоками $|A_1| \not\equiv 0$, $A_{\geqslant p} \equiv 0 \pmod p$ и

$$A_{\geqslant p} = \bigoplus_i A_i \quad \text{с } A_i = A_{\geqslant p,i} = p^{\alpha_i}\{A_i\},\ \alpha_i \geqslant 1, \tag{4.1}$$

где матрицы $\{A_i\}$ имеют определители $|\{A_i\}| \not\equiv 0 \pmod p$. Если $b = \begin{pmatrix} b' \\ b'' \end{pmatrix}$ из (1.1) разбить на блоки высоты $n-1$ и 1, то ранг b' может быть равен $r_p(b') = m-1$ или m.

4.2. Рассмотрим случай $r_p(b') = m$. По лемме 3.1.1 орбита $[b]$ п. 1.5 содержит представителя с нулевым нижним блоком. Поэтому можно считать

$$Q[b] = Q_1[b'] = A, \quad \text{где } b = \begin{pmatrix} b' \\ 0 \end{pmatrix} \text{ и } b' \text{ примитивно}, \tag{4.2}$$

а по предложению 1.1 — считать

$$Q_1 = \left(\begin{array}{cc|c} A_1 & & \\ & A_{\geqslant p} \quad \begin{matrix} 1 \\ 0 \end{matrix} & \\ & \begin{matrix} 1 & 0 \end{matrix} & \\ \hline & & Q_1^\perp \end{array}\right) = \begin{pmatrix} J(A) & \\ & Q_1^\perp \end{pmatrix}, \qquad b' = b'_{\text{fix}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}. \tag{4.3}$$

При этом матричное уравнение (4.2) имеет решения (все они принадлежат одной орбите $[b']$) только, когда существует блок $Q_1^\perp = Q_1 \ominus J(A)$. Следовательно,

$$Q = J(A) \oplus Q^\perp \quad \text{с блоком } Q^\perp = Q_1^\perp \oplus pQ_p = Q \ominus J(A), \tag{4.4}$$

и орбита $[b]$ содержит представителя $b = b_{\text{fix}} = \begin{pmatrix} b'_{\text{fix}} \\ 0 \end{pmatrix}$.

Для ортогонального преобразования M из $O(Q)$ в матрице $M \cdot b$ верхний блок равен $b'_1 = Ab' + Bb''$. Так как по (3.1) A принадлежит группе $O(Q_1/p)$ и $B \equiv 0 \pmod p$, то $r_p(b'_1) = r_p(b')$ и, следовательно, $r_p(b')$ есть *инвариант* орбиты $[b]$.

4.3. Разложение (4.4) формы

$$Q = \begin{pmatrix} A & C \\ {}^tC & Q' \end{pmatrix}, \quad \text{где } C = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},\ Q' = \begin{pmatrix} 0 & 0 \\ 0 & Q^\perp \end{pmatrix},$$

аналогично разложению (1.4), и доказательство п. 1.5 и 1.6 формулы (1.13) для локального множителя $c(A, Q, G)$ сохраняется.

Из приведенных рассуждений вытекает

Предложение 4.1. *Для формы $Q = Q_1 \oplus pQ_p$ уравнение $Q[b] = A$ имеет решение $b = \begin{pmatrix} b' \\ b'' \end{pmatrix}$ с условием $r_p(b') = m$ тогда и только тогда, когда $J(A) \leqslant Q$. Если это неравенство выполняется, то все решения лежат в одной орбите $[b]$ и каждое вложение b: $A \hookrightarrow Q$ разлагается в прямую сумму минимальных неразложимых вложений* (1.3) *размерностей* 1 *и* 2. *Локальный множитель $c(A, Q, G)$ п.* 1.5 *равен*

$$c(A, Q, G) = o(aA^{-1}_{\geqslant p}, A_{\geqslant p}), \tag{4.5}$$

если $G \sim -aA^{-1}_{\geqslant p} \oplus aQ^{\perp}$, где $Q^{\perp}$ — форма из разложения (4.4), *и $c(A, Q, G) = 0$ в остальных случаях.*

§5. Квадратичные формы простого определителя: $m - 1$-случай

5.1. В случае $r_p(b') = m-1$ воспользуемся переставляющей столбцы с номерами i, m матрицей $P = P_{im}$. Если b — какое-то решение уравнения (1.1), то $Q[bP] = A[P]$ и bP представляет форму $A[P] \sim A$. Используя инвариантность $r_p(b')$, можем считать

$$b = (b_1 b_2) = \begin{pmatrix} b'_1 & b'_2 \\ b''_1 & b''_2 \end{pmatrix},$$

где блок b'_1 имеет размеры $(n-1) \times (m-1)$ и ранг $r_p(b'_1) = m - 1$,

$$A = \begin{pmatrix} A^{(i)} & \\ & A'_i \end{pmatrix} \quad \text{с блоком } A^{(i)} = \begin{pmatrix} A_1 & \\ & A^{(i)}_{\geqslant p} \end{pmatrix}$$

и одномерным блоком $A'_i = A_{\geqslant p, i} \equiv 0 \pmod p$.

5.2. В приведенных обозначениях имеем

$$Q[b] = Q[(b_1 b_2)] = \begin{pmatrix} Q[b_1] & {}^t b_1 Q b_2 \\ * & Q[b_2] \end{pmatrix} = \begin{pmatrix} A^{(i)} & 0 \\ 0 & A'_i \end{pmatrix}.$$

Тогда $Q[b_1] = A^{(i)}$, ранг $r_p(b'_1) = m - 1$, и мы приходим к ситуации §4, что позволяет предположить

$$Q = \left(\begin{array}{cccc|c} A_1 & & & & \\ & A^{(i)}_{\geqslant p} & 1 & & \\ & 1 & 0 & & \\ & & & Q_1^{\perp} & \\ \hline & & & & pQ_p \end{array}\right), \qquad b = (b_1 b_2) = \left(\begin{array}{cc|c} 1 & 0 & \overline{b}_1 \\ 0 & 1 & \overline{b} \\ 0 & 0 & \overline{b}' \\ 0 & 0 & b^{\perp} \\ \hline 0 & 0 & b_p \end{array}\right). \tag{5.1}$$

Здесь блок $Q_1^{\perp} = Q_1 \ominus J(A^{(i)})$; и поскольку $r_p(b') = r_p((b'_1 b'_2)) = m-1$ и $r_p(b) = m$, то блоки $\overline{b}', b^{\perp} \equiv 0$ и $b_p \not\equiv 0 \pmod p$.

5.3. Рассмотрим локальную форму $Q_1^{\perp} \oplus pQ_p$ и примитивное представление $\binom{b^{\perp}}{b_p}$, в котором $b^{\perp} \equiv 0$, $b_p \not\equiv 0 \pmod p$. По лемме 3.1.2 орбита $\left[\binom{b^{\perp}}{b_p}\right]$ содержит представителя с нулевым блоком $b^{\perp} = 0$. Но тогда и в орбите $[b]$ содержится представитель с блоком $b^{\perp} = 0$.

Снова воспользуемся явным видом (5.1) формы Q и запишем

$$ {}^t b_1 Q b_2 = \begin{pmatrix} A_1 \overline{b}_1 \\ A^{(i)}_{\geqslant p} \cdot \overline{b} + \overline{b}' \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, $$

т.е. $\overline{b}' = -A^{(i)}_{\geqslant p} \cdot \overline{b}$ и $\overline{b}_1 = 0$, так как определитель $|A_1| \not\equiv 0 \pmod p$. Наконец, вычисляя значение $Q[b_2]$, получаем еще одно соотношение между блоками столбца b_2:

$$ Q[b_2] = -A^{(i)}_{\geqslant p}[\overline{b}] + pQ_p[b_p] = A'_i. $$

Таким образом, можем считать, что форма Q имеет вид (5.1) и представление b (5.1) имеет блоки $\overline{b}_1 = 0$, $b^{\perp} = 0$, а остальные блоки связаны двумя соотношениями $\overline{b}' = -A^{(i)}_{\geqslant p} \cdot \overline{b}$ и

$$ A^{(i)}_{\geqslant p}[\overline{b}] + A'_i = pQ_p[b_p], \quad \text{где } b_p \not\equiv 0 \pmod p. \tag{5.2} $$

5.4. Далее следуем схеме п. 1.5. Для этого расширим b до матрицы $B = (be)$ из $\mathrm{SL}^{\pm}_n(\mathbb{Z}_p)$ с помощью $n \times k$-матрицы e, в которой на уровне $\binom{\overline{b}'}{b^{\perp}}$ стоит единичная матрица $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, а остальные строки нулевые. В преобразованной форме $Q[B] = \left(\begin{smallmatrix} A & C \\ {}^t C & Q' \end{smallmatrix}\right)$ блоки C и Q' имеют вид

$$ C = {}^t bQe = \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ {}^t\overline{b} & 0 \end{pmatrix}, \qquad Q' = Q[e] = \begin{pmatrix} 0 & 0 \\ 0 & Q_1^{\perp} \end{pmatrix}, $$

и $Q[B]$ раскладывается в прямую сумму форм

$$ Q[B] = A_1 \oplus \left(\begin{array}{cc|c} A^{(i)}_{\geqslant p} & 0 & 1 \\ 0 & A'_i & {}^t\overline{b} \\ \hline 1 & \overline{b} & 0 \end{array}\right) \oplus Q_1^{\perp}. $$

5.5. Используя п. 5.4, вычисляем по формуле (1.5) форму

$$\frac{1}{a}G = \frac{1}{a}G_i \oplus \dot{Q}_1^{\perp}, \quad \text{где } \frac{1}{a}G_i = -A_{\geqslant p}^{(i)-1} - A_i'^{-1}[{}^t\overline{b}], \tag{5.3}$$

и переходим к *основной задаче* — найти все классы $\{G\}$ форм G, когда $\overline{b}$ пробегает решения уравнения (5.2).

Пусть $\overline{b}' = \sigma\overline{b}$ для некоторого σ из ортогональной группы $O(A_{\geqslant p}^{(i)})$. Тогда

$$A_{\geqslant p}^{(i)-1} + A_i'^{-1}[{}^t\overline{b}'] = (A_{\geqslant p}^{(i)-1} + A_i'^{-1}[{}^t\overline{b}])[{}^t\sigma],$$

и поэтому

$$G' \sim G, \quad \text{если } \overline{b}' \in [\overline{b}] \tag{5.4}$$

— орбите $\overline{b}$ относительно группы $O(A_{\geqslant p}^{(i)})$.

Еще одно свойство форм G вытекает из сравнения

$$G_i' \equiv G_i \pmod{a}, \quad \text{если } \overline{b}' \equiv \overline{b} \pmod{A_i'}. \tag{5.5}$$

Заметим, что по (5.3) ступень форм G_i, G_i' меньше ступени a формы A п. 1.5, т.е. они не делятся на a. Упростим обозначения $G = G_i$, $G' = G_i'$. Пусть

$$G' = \begin{pmatrix} G_1' & C \\ {}^tC & G_{\geqslant p}' \end{pmatrix} \equiv \begin{pmatrix} G_1 & 0 \\ 0 & G_{\geqslant p} \end{pmatrix} = G \pmod{a},$$

где $|G_1| \not\equiv 0$, $G_{\geqslant p} \equiv 0 \pmod{p}$. Тогда $G_1' \equiv G_1 \pmod{p}$, поэтому $|G_1'| \not\equiv 0 \pmod{p}$ и $G_1' \sim G_1$. С помощью матрицы

$$M = \begin{pmatrix} 1 & -G'^{-1} \cdot C \\ 0 & 1 \end{pmatrix}$$

из $\mathrm{SL}(\mathbb{Z}_p)$ получаем эквивалентность

$$G' \sim G'[M] = G_1' \oplus G_{\geqslant p}'', \quad \text{где } G_{\geqslant p}'' = G_{\geqslant p}' - G_1'^{-1}[C],$$

и $G_{\geqslant p}'' \equiv G_{\geqslant p}' \equiv G_{\geqslant p} \pmod{a}$, так как по предположению $C \equiv 0 \pmod{a}$. Итак, доказано, что формы G', G имеют один и тот же инвариант $\{G_1\}$. Форму G' можем считать имеющей вид $G' = G_1 \oplus G_{\geqslant p}''$ с блоком $G_{\geqslant p}'' \equiv G_{\geqslant p} \pmod{a}$. Отсюда по индукции получаем свойство (5.5).

Согласно свойствам (5.4) и (5.5), если мы интересуемся лишь классами $\{G_i\}$ форм G_i из разложения (5.3), то можем решение $\overline{b}$ уравнения (5.2) заменить

любым представителем *орбиты* $[\overline{b}/A_i']$, состоящей из столбцов $\sigma \cdot \overline{b} \mod A_i'$ с σ из ортогональной группы $O(A^{(i)}_{\geqslant p})$.

В уравнении (5.2) уточним обозначения для формы

$$A^{(i)}_{\geqslant p} = \underset{j}{\oplus} A^{(i)}_j,$$

где блоки $A^{(i)}_j$ имеют следующий вид:

$$A^{(i)}_j = A_j = p^{\alpha_j}\{A_j\} = p^{\alpha_j} \cdot A_{p^{\alpha_j}}, \qquad \text{если } \alpha_j \neq \alpha_i, \tag{5.6}$$

$$A^{(i)}_j = A_i \ominus A_i' = p^{\alpha_i}(\{A_i\} \ominus \{A_i'\}) = p^{\alpha_i}\{A^{(i)}_j\}, \quad \text{если } \alpha_j = \alpha_i, \tag{5.7}$$

при этом

$$A_i = p^{\alpha_i} \begin{pmatrix} \{A_i\} \ominus \{A_i'\} & 0 \\ 0 & \{A_i'\} \end{pmatrix} \quad \text{с } A_i' = p^{\alpha_i} \cdot \{A_i'\}$$

— одномерным блоком.

Будем различать два случая $\alpha_i = 1$ и $\alpha_i \geqslant 2$.

5.6. Если $\alpha_i = 1$, то $\overline{b} \mod p$ и имеются две возможности: $b \equiv 0 \pmod p$, и тогда мы берем $b = 0$; или $\overline{b} \not\equiv 0 \pmod p$. Пусть $\overline{b}$ разбито на блоки аналогично форме $A^{(i)}_{\geqslant p}$ и первый ненулевой блок $b_j \not\equiv 0 \pmod p$. Следовательно, в форме $A^{(i)}_{\geqslant p}$ соответствующий блок $A^{(i)}_j$ также ненулевой. По формуле (5.3) получаем $-\frac{1}{a}G_i \sim A^{(i)-1}_{\geqslant p}$, если $\alpha_i = 1$, $\overline{b} \equiv 0 \pmod p$. Для $\alpha_i = 1$ по определениям (5.6) и (5.7) форма

$$A^{(i)}_{\geqslant p} = A^{(i)}_1 \oplus A_2 \oplus \ldots, \quad \text{где } A^{(i)}_1 = pA_p \ominus A_i'.$$

Подставляя $\overline{b} = 0$ в равенство (5.2), замечаем $A_i' = pQ_p[b_p]$ с $b_p \not\equiv 0 \pmod p$, т.е. $A_i' \sim pQ_p$. Здесь $a \sim b$ для a, b из поля p-адических чисел $\mathbb{Q}_p$ означает, что a/b есть квадрат некоторой единицы кольца $\mathbb{Z}_p$. Поэтому в случае $\alpha_i = 1$ и $\overline{b} \equiv 0 \pmod p$ имеем

$$-\frac{1}{a}G_i \sim (pA_p \ominus pQ_p)^{-1} \oplus A_2^{-1} \oplus \ldots \tag{5.8}$$

5.7. Если же в $\overline{b}$ существует блок $b_j \not\equiv 0 \pmod p$, то, согласно предложению 3.1.1 и п. 5.5, можем считать в $\overline{b}$ все блоки нулевыми, кроме блока b_j. Затем по предложению 1.1 можем считать $b_j = (10\ldots0)$,

$$\{A^{(i)}_j\} = \begin{pmatrix} c_1 & 0 \\ 0 & c_1^{\perp} \end{pmatrix} \quad \text{для } c_1 \not\equiv 0 \pmod p,\ c_1^{\perp} = \{A^{(i)}_j\} \ominus c_1 \tag{5.9}$$

или

$$\{A_j^{(i)}\} = \left(\begin{array}{cc|c} c_1 & 1 & \\ 1 & 0 & \\ \hline & & J(c_1)^{\perp} \end{array}\right) \quad \text{для } c_1 \equiv 0 \pmod p,\ J(c_1)^{\perp}\{A_j^{(i)}\} \ominus J(c_1), \quad (5.10)$$

где

$$A_{\geqslant p}^{(i)}[\overline{b}] = A_j^{(i)}[b_j] = p^{\alpha_j} \cdot c_1 = c \quad \text{или} \quad \{A_j^{(i)}\}[b_j] = c_1.$$

В этих условиях равенство (5.2) принимает вид

$$c + A_i' = pQ_p[b_p], \quad \text{где } b_p \not\equiv 0 \pmod p,\ A_i' = p \cdot \{A_i'\}, \quad (5.11)$$

а для формы G_i из (5.3) выполняется разложение в прямую сумму

$$-\frac{1}{a}G_i = A_1^{(i)-1} \oplus \cdots \oplus A_{ij}^{-1} \oplus A_{j+1}^{(i)-1} \oplus \ldots \quad (5.12)$$

с блоком $A_{ij}^{-1} = A_j^{(i)-1} \oplus \left(\begin{smallmatrix} A_i'^{-1} & 0 \\ 0 & 0 \end{smallmatrix}\right)$. Этот блок по формуле (5.9) для $c_1 \not\equiv 0 \pmod p$ равен

$$A_{ij}^{-1} = (p^{-\alpha_j} \cdot c_1^{-1} + A_i'^{-1}) \oplus p^{-\alpha_j} \cdot c_1^{\perp -1}, \quad (5.13)$$

а по формуле (5.10) в случае $c_1 \equiv 0 \pmod p$ равен

$$A_{ij}^{-1} = p^{-\alpha_j} \begin{pmatrix} p^{\alpha_j} \cdot A_i'^{-1} & 1 \\ 1 & -c_1 \end{pmatrix} \oplus p^{-\alpha_j} J(c_1)^{\perp -1}. \quad (5.14)$$

5.8. Разберем случай $c_1 \not\equiv 0 \pmod p$. Ввиду условия (5.11) для первого блока из разложения (5.13) имеет место эквивалентность

$$p^{-\alpha_j} \cdot c_1^{-1} + A_i'^{-1} \sim p^{-\alpha_j} \cdot Q_p / c_1 \{A_i'\}.$$

Отсюда и из (5.13) заключаем, что форма

$$A_{ij} \sim p^{\alpha_j}(c_1\{A_i'\}/Q_p \oplus c_1^{\perp}), \quad \text{где } c_1^{\perp} = \{A_j^{(i)}\} \ominus c_1.$$

Для $\alpha_j = \alpha_i = 1$ по определению (5.7) форма $\{A_j^{(i)}\}$ равна $\{A_j\} \ominus \{A_i'\}$, и тогда

$$A_{ij} \sim p^{\alpha_j}(\{A_j\} \ominus Q_p).$$

Если же $\alpha_j > \alpha_i = 1$, то по (5.11) $\{A_i'\} \sim Q_p$ и по определению (5.6) $\{A_j^{(i)}\} = \{A_j\}$. Следовательно,

$$A_{ij} \sim p^{\alpha_j}\{A_j\} = A_j.$$

Из этих соотношений и формулы (5.12) для формы G_i в случае $\alpha_i = 1$ вытекает эквивалентность (5.8).

5.9. Для $c_1 \equiv 0 \pmod p$ получаем

$$p^{-\alpha_j}\begin{pmatrix} p^{\alpha_j}\cdot A_i^{'-1} & 1 \\ 1 & -c_1 \end{pmatrix} \sim p^{-\alpha_j}\cdot J_1, \quad \text{где } J_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

— двумерная гиперболическая форма. Отсюда, (5.14) и (5.10), выводим

$$A_{ij} \sim p^{\alpha_j} J_1 \oplus p^{\alpha_j} J(c_1)^{\perp} = p^{\alpha_j}(J_1 \oplus (\{A_j^{(i)}\} \ominus J(c_1))),$$

т.е. снова

$$A_{ij} \sim p^{\alpha_j}\{A_j^{(i)}\} = A_j^{(i)}.$$

Так как $c_1 \equiv 0 \pmod p$, то по (5.11) $\{A_i'\} \sim Q_p$ или $A_i' \sim pQ_p$.

Если $\alpha_j = \alpha_i = 1$, то $A_{ij} \sim A_j^{(i)}$ и по определению (5.7) $A_{ij} \sim pA_p \ominus pQ_p$. Если же $\alpha_j > \alpha_i = 1$, то по определению (5.6) $A_{ij} \sim A_j^{(i)} = A_j$ и по (5.7) $A_1^{(i)} = pA_p \ominus pQ_p$. Как видим, в обоих случаях для формы G_i получается эквивалентность (5.8). Значит, (5.8) всегда имеет место для $\alpha_i = 1$.

5.10. Проверим, что (5.8) также имеет место и для $\alpha_i \geqslant 2$. Теперь, согласно п. 5.5, $\overline{b} \mod p^{\alpha_i}$ и $\overline{b}$ удовлетворяет равенству (5.2), в котором $A_i' \equiv 0 \pmod{p^2}$. Поэтому

$$A_{\geqslant p}^{(i)}[\overline{b}] \equiv pQ_p[b_p] \pmod{p^2}, \quad \text{где } b_p \not\equiv 0 \pmod p.$$

Согласно (5.6), блок $A_1^{(i)} = pA_p$. Пусть b_1 — блок из $\overline{b}$, отвечающий блоку pA_p. Тогда $A_{\geqslant p}^{(i)}[\overline{b}] \equiv pA_p[b_1] \pmod{p^2}$, и по предыдущему сравнению

$$A_p[b_1] = c_1, \quad \text{где } c_1 \not\equiv 0 \pmod p,\ c_1 \sim Q. \tag{5.15}$$

По условию $|A_p| \not\equiv 0 \pmod p$, поэтому из (5.15) следует $b_1 \not\equiv 0 \pmod p$. Согласно п. 5.5 и лемме 3.1.1, можем считать, что блок ${}^t b_1 = (10\ldots0)$, остальные блоки в $\overline{b}$ нулевые, и

$$A_p = \begin{pmatrix} c_1 & 0 \\ 0 & c_1^{\perp} \end{pmatrix}, \quad \text{где } c_1 \not\equiv 0 \pmod p,\ c_1^{\perp} = A_p \ominus c_1.$$

В этих условиях имеем $A_{\geqslant p}^{(i)}[\overline{b}] = pA_p[b_1] = pc_1 = c$, где $c \sim pQ_p$. Поэтому форма G_i из (5.3) разлагается в прямую сумму

$$-\frac{1}{a}G_i = \begin{pmatrix} p^{-1}\cdot c_1^{-1} + A_i^{'-1} & 0 \\ 0 & p^{-1}\cdot c_1^{\perp -1} \end{pmatrix} \oplus A_2^{-1} \oplus \cdots \oplus A_i^{(i)-1} \oplus \ldots,$$

где $p^{-1}\cdot c_1^{-1} + A_i^{'-1} \sim A_i^{'-1}$ в силу сравнения $A_i' \equiv 0 \pmod{p^2}$, $p\cdot c_1^{\perp} = pA_p \ominus c \sim pA_p \ominus pQ_p$, и по определению (5.7) блок $A_i^{(i)} = A_i \ominus A_i'$. Отсюда для $\alpha_i \geqslant 2$ получаем разложение

$$-\frac{1}{a}G_i \sim A_i^{'-1} \oplus (pA_p \ominus pQ_p)^{-1} \oplus A_2^{-1} \oplus \cdots \oplus (A_i \ominus A_i')^{-1} \oplus \ldots,$$

эквивалентное разложению (5.8). Тем самым (5.8) доказано для любого α_i.

5.11. Возвращаемся к форме G из (5.3) со вторым блоком $Q_1^\perp = Q_1 \ominus J(A^{(i)})$ из разложения (5.1). По определению из п. 5.1 имеем

$$J(A^{(i)}) = A_1 \oplus \begin{pmatrix} A^{(i)}_{\geqslant p} & 1 \\ 1 & 0 \end{pmatrix} \sim A_1 \oplus J(m_{\geqslant p} - 1),$$

где последний блок обозначает гиперболическую форму $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ размера $2(m_{\geqslant p} - 1)$ для $m_{\geqslant p} = \dim A_{\geqslant p}$ (4.1). Это означает, что класс $\{J(A^{(i)})\}$, а значит, и $\{Q_1^\perp\}$ не зависят от выбора A_i' с условием $A_i' \equiv 0 \pmod p$.

Подставляя (5.8) в разложение (5.3), получаем следующий результат.

Лемма 5.1. *Пусть форма $Q = Q_1 \oplus pQ_p$ и примитивное представление $b : Q[b] = A$ имеют верхний $(n-1) \times m$-блок b' ранга $r_p(b') = m - 1$. Тогда все такие b принадлежат единственному классу* $\mathrm{pb}(A, Q, \{G\})$ *п. 1.5 с формой G, удовлетворяющей условию*

$$-\frac{1}{a}G \sim \left(\begin{array}{c|c} (A_{\geqslant p} \ominus pQ_p)^{-1} & \\ \hline & -Q_1^\perp \end{array}\right) \quad c\ Q_1^\perp \sim Q_1 \ominus \begin{pmatrix} A_1 & 0 \\ 0 & J(m_{\geqslant p} - 1) \end{pmatrix}. \tag{5.16}$$

§6. Сплетающие матрицы и локальные множители

6.1. Вопрос о формах G решен, и можем перейти к *матричному сравнению*

$$A^{-1}[C] \equiv -\tfrac{1}{a}G \pmod{\mathbb{Z}_p}, \tag{6.1}$$

где G — форма из (5.16), и решения C рассматриваются по $\bmod A$. Любая сцепляющая матрица C дает целую невырожденную форму $Q_G^A(C)$ (1.8) с определителем $|Q_G^A(C)| = |A| \cdot |\frac{1}{a}G|$. Согласно определению (5.16) формы G, имеем

$$(-1)^{n-m}\left|\frac{1}{a}G\right| = \left(\frac{|A_{\geqslant p}|}{|p \cdot Q_p|}\right)^{-1} \cdot (-1)^{(n-1)+(m_1+2(m_{\geqslant p}-1))} \frac{|Q_1|}{|A_1| \cdot |J(m_{\geqslant p} - 1)|},$$

т.е.

$$\left|\frac{1}{a}G\right| = \frac{|Q_1| \cdot |pQ_p|}{|A_1| \cdot |A_{\geqslant p}|} = \frac{|Q|}{|A|}.$$

Следовательно, определитель форм (1.8) равен

$$|Q_G^A(C)| = |Q|.$$

Из классификации квадратичных форм над нечетным локальным кольцом $\mathbb{Z}_p$ [5, с. 131] и из равенства определителей заключаем, что

$$Q_G^A(C) \sim Q \quad \text{или} \quad Q_G^A(C) \sim Q^- = Q_1^- \oplus pQ_p^-,$$

где Q_1^-, Q_p^- — произвольные целые формы размерностей $n-1, 1$ с определителями $|Q_1^-| = 1^- \cdot |Q_1|$, $|Q_p^-| = 1^- \cdot |Q_p|$. Здесь 1^- — фиксированная единица кольца $\mathbb{Z}_p$, $p \neq 2$, для которой *символ Лежандра* $\left(\frac{1^-}{p}\right) = -1$. Форма Q^- удовлетворяет условиям предложения 4.1 и леммы 5.1. Предположим, что $Q^-[b] = A$ для некоторого примитивного b, отвечающего матрице C — решению сравнения (6.1) с формой G и (5.16). По предложению 4.1 ранг $r_p(b')$ равняться m не может. Остается возможность $r_p(b') = m-1$. В этом случае по лемме 5.1 b принадлежит классу $\mathrm{pb}(A, Q^-, \{G^-\})$ для формы G^- из (5.16), где блоки Q_p, Q_1 заменены на Q_p^-, Q_1^-. Поскольку формы G и G^- неэквивалентны, то мы приходим к следующему выводу:

$$Q_G^A(C) \sim Q \tag{6.2}$$

для любого решения C сравнения (6.1) с формой G из (5.16).

Пусть $Q[b] = A$ с $r_p(b') = m-1$ и C — решение сравнения (6.1). Тогда, согласно (1.10) и (6.2), имеет место *биекция* между двухсторонними орбитами

$$\{b\} \xrightarrow{\sim} \{C\}. \tag{6.3}$$

В частности, отсюда вытекает существование указанных представлений b в случае разрешимости сравнения (6.1).

6.2. Найдем все двухсторонние орбиты $\{C\}$ п. 1.5 решений C сравнения (6.1). Поскольку решения рассматриваются по $\bmod A$, то, не уменьшая общности, будем считать

$$A = A_{\geqslant p} = \begin{pmatrix} A_2 & 0 \\ 0 & A_1 \end{pmatrix}, \tag{6.4}$$

где блок $A_1 = pA_p$ с $|A_p| \not\equiv 0 \pmod p$ и блок $A_2 \equiv 0 \pmod{p^2}$. Обозначим

$$E = aA^{-1} = \begin{pmatrix} aA_2^{-1} & 0 \\ 0 & aA_1^{-1} \end{pmatrix} = \begin{pmatrix} E_2 & 0 \\ 0 & E_1 \end{pmatrix},$$

где a — ступень (1.5) формы A. В этих обозначениях сравнение (6.1) с формой G (5.16) принимает вид

$$\begin{pmatrix} E_2 & 0 \\ 0 & E_1 \end{pmatrix} \left[\left(\begin{array}{cc|c} C_1 & C_2 & D_1 \\ C_3 & C_4 & D_2 \end{array} \right) \right] \equiv \left(\begin{array}{cc|c} E_2 & 0 & \\ 0 & E_1' & \\ \hline & & 0 \end{array} \right) \pmod a, \tag{6.5}$$

где, согласно (6.4) и (5.16), блок $E_1' = a(pA_p \ominus pQ_p)^{-1}$. Из (6.5) следует $E_2[C_1] + E_1[C_3] \equiv E_2 \pmod a$, и по условию форма $E_1 \equiv 0 \pmod{a/p}$. Следовательно, $E_2[C_1] \equiv E_2 \pmod{a/p}$, и при этом ступень целой формы E_2 не делится на a/p. Тогда в силу [4, с. 58] определитель $|C_1| \not\equiv 0 \pmod p$. Заметим, что в определении орбиты $\{C\}$ п. 1.5 матрица ${}^tU$ принадлежит ортогональной группе $O(E)$. Так как сейчас важны не сами решения C (6.1), а лишь их орбиты $\{C\}$, то по (1.12) и лемме 3.1.1 можем считать $C_1 = 1$, $C_3 = 0$. В этих условиях по (6.5) ${}^tC_1E_2C_2 \equiv E_2C_2 \equiv 0 \pmod a$, т.е. $C_2 \equiv 0 \pmod{A_2}$, и считаем $C_2 = 0$. Аналогично можем считать $D_1 = 0$.

Относительно блока C_4 сравнение (6.5) дает $E_1[C_4] \equiv E_1' \pmod a$ или

$$A_p^{-1}[C_4] \equiv (A_p \ominus Q_p)^{-1} \pmod p, \quad \text{где } C_4 \pmod p.$$

По предложению 2.1 решение C_4 существует тогда и только тогда, когда существует разность форм $A_p \ominus Q_p$, т.е. когда выполняется неравенство $Q_p \leqslant A_p$. В силу эпиморфности отображения ι_1 (2.3) можем считать $A_p^{-1}[C_4] = (A_p \ominus Q_p)^{-1}$, а по предложению 1.1 — считать, что

$$A_p = \left(\begin{array}{c|} A_p \ominus Q_p \\ \hline Q_p \end{array}\right), \qquad C_4 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Подставляя в E_1 форму A_p, из (6.5) выводим $D_2 = \begin{pmatrix} 0 \\ D_2' \end{pmatrix}$, где блок D_2 разбит аналогично C_4 и $Q_p^{-1}[D_2'] \equiv 0 \pmod p$. Так как $|Q_p| \not\equiv 0 \pmod p$ и $D_2' \mod p$, то можем взять $D_2' = 0$. Таким образом, если G — форма из (5.16), то сравнение (6.1) разрешимо, и все его решения $C \mod A$ принадлежит *одной* двухсторонней орбите $\{C_{\text{fix}}\}$ с фиксированным представителем

$$C_{\text{fix}} = \left(\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \hline 0 & 0 & 0 \end{array}\right).$$

6.3. Для того чтобы разложить вложение $b : A \hookrightarrow Q$ с $r_p(b') = m - 1$ на минимальные неразложимые вложения, достаточно для сцепляющей матрицы C_{fix} вычислить квадратичную форму $Q_G^A(C_{\text{fix}})$ (1.8) для G из (5.16). Для этого вернемся к общим обозначениям п. 4.1 формы

$$A = A_1 \oplus A_{\geqslant p}, \quad A_{\geqslant p} = pA_p \oplus A_2,$$

где $|A_1|$, $|A_p| \not\equiv 0 \pmod p$, $A_2 \equiv 0 \pmod{p^2}$, и блок A_p имеет такой же вид, как и в п. 6.2. В сравнении (6.1) $C \mod A$, и поэтому, переходя к общему случаю формы A, нужно во всех матрицах C из п. 6.2 добавить сверху нулевой блок

высоты $m_1 = \dim A_1$ и то же самое сделать с C_{fix}. С учетом этого замечания по формуле (1.8) прямым вычислением получаем разложение

$$Q_G^A(C_{\text{fix}}) = A_1 \oplus \begin{pmatrix} A_2 & 1 \\ 1 & 0 \end{pmatrix} \oplus \begin{pmatrix} pA_p \ominus pA_p & 1 \\ 1 & 0 \end{pmatrix} \oplus pQ_p \oplus Q_1^{\perp}, \tag{6.6}$$

где $Q_1^{\perp}$ — форма из (5.16). Если воспользоваться обозначениями из (1.2), то разложение (6.6) примет более компактный вид

$$Q_G^A(C_{\text{fix}}) = J(A \ominus pQ_p) \oplus pQ_p \oplus Q_1^{\perp}. \tag{6.7}$$

Сравнивая (6.6) и (6.7) с (1.2), видим, что при разложении в прямую сумму вложений $b : A \hookrightarrow Q$ в форму $Q = Q_1 \oplus pQ_p$ с условием $r_p(b') = m-1$ появляется новое *одномерное минимальное неразложимое вложение*

$$p \cdot \varepsilon \hookrightarrow p \cdot \varepsilon, \quad \text{где } \varepsilon \text{ — единица } \mathbb{Z}_p. \tag{6.8}$$

6.4. Осталось вычислить локальный множитель $c(A, Q, G)$ для формы G (5.16). В преобразованиях п. 6.2 решений C сравнения (6.1) к виду C_{fix} были использованы лишь преобразования из ортогональной группы $O(E)$. Поэтому, согласно свойству (6.2) и определению локального множителя из п. 1.5, будем использовать формулу

$$c(A, Q, G) = o(aA_{\geqslant p}^{-1}, A_{\geqslant p}) / \operatorname{stab}(C_{\text{fix}}). \tag{6.9}$$

Здесь $\operatorname{stab}(C_{\text{fix}})$ — *порядок стабилизатора* матрицы C_{fix} п. 6.2 в группе $O(aA_{\geqslant p}^{-1}, A_{\geqslant p})$, где в обозначениях п. 6.2 $aA_{\geqslant p}^{-1} = E$,

$$E = \left(\begin{array}{c|cc} E_2 & & \\ \hline & E_1' & 0 \\ & 0 & a(pQ_p)^{-1} \end{array}\right) \quad \text{и} \quad M = \left(\begin{array}{c|cc} \alpha & a & b \\ \hline a_1 & A & B \\ b_1 & C & D \end{array}\right) \tag{6.10}$$

из группы $O(E)$ разбито на блоки аналогично E. Если

$$MC_{\text{fix}} \equiv C_{\text{fix}} \pmod{A_{\geqslant p}} \quad \text{для } A_{\geqslant p} = \begin{pmatrix} A_2 & 0 \\ 0 & pA_p \end{pmatrix},$$

то $\alpha \equiv 1$, $a \equiv 0 \pmod{A_2}$ и $a_1 \equiv 0$, $b_1 \equiv 0$, $A \equiv 1$, $C \equiv 0 \pmod{p}$, т.е.

$$M = \left(\begin{array}{c|cc} 1 & 0 & b \\ \hline 0 & 1 & B \\ 0 & 0 & D \end{array}\right) \quad \text{и} \quad E[M] \equiv E \pmod{a},\ M \bmod A_{\geqslant p}.$$

Используя вид формы E (6.10), из последнего сравнения получаем $E_2 b \equiv 0$, $E_1' B \equiv 0 \pmod{a}$, поэтому можем взять $b = 0$, $B = 0$. Теперь для блока D вытекает сравнение $Q_p^{-1}[D] \equiv Q_p^{-1} \pmod{p}$, где $D \pmod{p}$, $p \neq 2$. Так как $D \equiv \pm 1 \pmod{p}$, доказано

$$\operatorname{stab}(C_{\text{fix}}) = 2.$$

Теорема 6.1. 1. *Для формы $Q = Q_1 \oplus pQ_p$ уравнение $Q[b] = A$ имеет примитивное решение с условием $r_p(b') = m-1$ тогда и только тогда, когда существует форма G* (5.16), *т.е. когда*

$$A_1 \oplus J(m_{\geqslant p} - 1) \leqslant Q_1, \qquad Q_p \leqslant A_p. \tag{6.11}$$

2. *Если условия* (6.11) *выполнены, то все решения b лежат в одной двухсторонней орбите $\{b\}$, и каждое вложение $b : A \hookrightarrow Q$ разлагается в прямую сумму минимальных неразложимых вложений вида* (1.3) *и единственного вложения* (6.8) *с $\varepsilon \sim Q_p$.*

3. *Локальный множитель $c(A, Q, G) \neq 0$ только для формы G из* (5.16), *для которой он равен*

$$c(A, Q, G) = o(aA_p^{-1}, A_{\geqslant p})/2. \tag{6.12}$$

Доказательство. Утверждение 1) следует из леммы 5.1, п. 6.2 и формулы (6.2); 2) — из биекции (6.3), п. 6.2 и из разложений (6.6), (6.7). Утверждение 3) вытекает из 1) и п. 6.4. •

6.5. Пусть $b : A \hookrightarrow Q$ — примитивное вложение. Обозначим b_{I}, b_{II} вложения $b = \begin{pmatrix} b' \\ * \end{pmatrix}$, у которых блок b' высоты $n-1$ имеет ранг $r_p(b') = m$ и $m-1$ соответственно. Из предложений 4.1 и 6.1 вытекает

Следствие 6.1. 1. *Если $Q = Q_1 \oplus pQ_p$, то число двухсторонних орбит $\{b\}$ примитивных представлений $b : Q[b] = A$ над кольцом $\mathbb{Z}_p$, $p \neq 2$, равно числу разложений*

$$Q \sim X \oplus Y, \tag{6.13}$$

где X — произвольное минимальное вложение $A \hookrightarrow X$ формы A. Каждое такое X есть прямая сумма минимальных неразложимых вложений первого типа

$$\varepsilon \hookrightarrow \varepsilon, p^j \cdot \varepsilon \hookrightarrow J(p^j \cdot \varepsilon) = \begin{pmatrix} p^j \cdot \varepsilon & 1 \\ 1 & 0 \end{pmatrix}, \tag{6.14}$$

где ε — единица кольца $\mathbb{Z}_p$ и $j \geqslant 1$, и вложений второго типа

$$p \cdot \varepsilon \hookrightarrow p \cdot \varepsilon \quad \text{для } \varepsilon \sim Q_p. \tag{6.15}$$

2. *Имеет место биекция*

$$X_i \underset{\sim}{\longrightarrow} \{b_i\}, \quad i = \mathrm{I}, \mathrm{II}, \tag{6.16}$$

где X_{I} является суммой вложений первого типа (6.14), *а X_{II} содержит вложение второго типа* (6.15).

Пусть в обозначениях п. 6.3 форма A размерности m имеет разложение $A = A_1 \oplus A_{\geqslant p}$ с $A_{\geqslant p} = pA_p \oplus A_2$ и ее блоки A_p, $A_{\geqslant p}$ имеют размерности m_p, $m_{\geqslant p}$. Из следствия 6.1 легко получаются следующие *достаточные условия*:

существует вложение первого типа $b_{\mathrm{I}} : A \hookrightarrow Q$, если

$$m + m_{\geqslant p} < n - 1, \tag{6.17}$$

и — второго типа $b_{\mathrm{II}} : A \hookrightarrow Q$, если

$$m + m_{\geqslant p} < n + 1, \quad m_p > 1. \tag{6.18}$$

Таким образом, если $m + m_{\geqslant p} < n - 1$ и $m_p > 1$, то форма A *свободно*, т.е. более чем одним способом, вкладывается в Q. В противном случае A не вкладывается в Q или вкладывается *жестко*.

Пример 1. Выясним, какие невырожденные формы A размерности $m = 2$ примитивно вкладываются в форму

$$Q = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 3 \end{pmatrix} \quad \text{над кольцом } \mathbb{Z}_7.$$

Имеем $d = |Q| = 7$ и верхний 2×2-минор $|Q_1| = 3$ является невычетом mod 7. Следовательно, форма $Q \sim Q_1 \oplus pQ_p$ над $\mathbb{Z}_7$ имеет блоки $Q_1 = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 2 \end{smallmatrix}\right)$, $n_1 = 2$, и $Q_p = 7 \cdot 3^{-1}$, $n_p = 1$, и ее *p-адический символ* [9, с. 477] равен $7_Q = 1^{-2}7^{-1}$. Если $A = A_1$, $|A_1| \not\equiv 0 \pmod 7$, то по лемме 6.1 $X = X_{\mathrm{I}} = A_1$ и $\left(\frac{|A_1|}{7}\right) = -1$, т.е. $7_A = 1^{-2}$. Если же $A \equiv 0 \pmod 7$, то возможно только $A = p \cdot A_p$, и A всегда вкладывается в X_{II}, т.е. $7_A = 7^{\pm 2}$. Аналогично рассматривается оставшийся случай $A = A_1 \oplus pA_p$, когда $7_A = 1^{\pm 1}7^{-1}$ и $X = X_{\mathrm{II}}$. Итак, в форму Q над $\mathbb{Z}_7$ примитивно вкладываются только бинарные формы A с p-адическими символами

$$7_A = 1^{-2}, 1^{\pm 1}7^{-1}, 7^{\pm 2}$$

с минимальными вложениями типа X_{I}, X_{II}, X_{II} соответственно. Поэтому в Q любая бинарная форма A может вкладываться только жестко.

Пример 2. Решим обратную задачу. Какова бинарная невырожденная форма A, если она *свободно* вкладывается над $\mathbb{Z}_5$ в форму

$$Q = \begin{pmatrix} 2 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 2 \end{pmatrix} \underset{\sim}{\mathrm{SL}_4^{\pm}(\mathbb{Z})} \begin{pmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -1 & 0 \\ 0 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix}$$

(см. подробности в п. 7.6). Ее определитель $d = |Q| = 5$ и верхний главный 3×3-минор $\equiv 4 \pmod 5$. Отсюда заключаем, что $5_Q = 1^{+3}5^{+1}$. Поскольку существуют минимальные вложения двух типов $A \hookrightarrow X_{\mathrm{I}}$ и $A \hookrightarrow X_{\mathrm{II}}$, то из (6.14), (6.15) следует $5_A = 1^{\varepsilon_1 \cdot 1}5^{+1}$ и из (6.14) — дополнительное условие $\varepsilon_1\left(\frac{-1}{5}\right) = +1$. Это однозначно определяет p-адический символ $5_A = 1^{+1}5^{+1}$, а следовательно, и класс $\{A\}$ формы A, свободно вкладывающейся в форму Q. В качестве представителя класса $\{A\}$ можно взять бинарную форму $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 5 \end{smallmatrix}\right)$.

§7. Представление форм родом квадратичных форм

7.1. Объединяя (4.5) и (6.12), получаем для локальных множителей общую формулу

$$c_p(A, Q, G_i) = \frac{1}{(2)} o(aA^{-1}_{\geqslant p}, A_{\geqslant p}),$$

при этом $(2) = 1$ или 2 для $i = \mathrm{I}$ или II соответственно, и по (4.4) и (5.16)

$$G_{\mathrm{I}} = -aA^{-1}_{\geqslant p} \oplus Q_1^{\perp} \oplus apQ_p, \tag{7.1}$$

$$G_{\mathrm{II}} = -a(A_{\geqslant p} \ominus pQ_p)^{-1} \oplus aQ_1^{\perp}, \tag{7.2}$$

где $Q_1^{\perp} = Q_1 \ominus J(A)$ в первом случае и $Q_1^{\perp} = Q_1 \ominus (A_1 \oplus J(m_{\geqslant p} - 1))$ — во втором. Согласно §12, 13 [4], формулу для локального множителя можно переписать в виде

$$c_p(A, Q, G_i) = \frac{1}{(2)} |A|_p^{-(m_{\geqslant p}-1)/2} m_p(aA^{-1}_{\geqslant p})^{-1}, \tag{7.3}$$

где $|A|_p = |\det A|_p$ и $|\cdot|_p$ — *p-норма* поля $\mathbb{Q}_p$, т.е. $|p|_p = p^{-1}$, и *p-масса* $m_p(G)$ для формы $G = \bigoplus\limits_q qG_q$, $\dim G_q = k_q$ с $q = p^{\alpha}$, $p \neq 2$, равна

$$m_p(G) = \prod_q M_p(G_q) \prod_{q<q'} (q'/q)^{k_q \cdot k_{q'}/2}. \tag{7.4}$$

Здесь

$$M_p(G_q) = \mathrm{std}_p(k_q, E_q(G)) \quad \text{с } E_q(G) = \varepsilon_q(G)\left(\frac{(-1)^{k_q/2}}{p}\right),$$

где $\varepsilon_q(G) = \left(\frac{|G_q|}{p}\right)$ — *знак* блока G_q, и для $k = 2s-1$ или $k = 2s$, $k > 0$,

$$\operatorname{std}_p(k,E)^{-1} = 2(1-p^{-2})\dots(1-p^{-2(s-1)})(1-E_1p^{-s}),$$

где $E_1 = 0$ или $E_1 = 1$ для k нечетных или четных соответственно.

7.2. Используя разложение (7.1), по формуле (7.4) записываем

$$m_p(G_{\mathrm{I}}) = m_p(-aA_{\geqslant p}^{-1})M_p(\{a\}Q_1^{\perp})M_p(\{a\}Q_p)\Pi_1\cdot\Pi_2,$$

где

$$\Pi_1 = |A|_p^{-(n-1-2m+m_1)/2}, \qquad \Pi_2 = |A|_p^{-1/2}\cdot p^{(n-m-1)/2}.$$

Так как $m_p(-G) = m_p(G)$, по (7.3) получаем

$$c_p(A,Q,G_{\mathrm{I}})m_p(G_{\mathrm{I}}) = \frac{1}{2}|A|_p^{-n'/2}p^{n'/2}M_p(\{a\}Q_1^{\perp}), \tag{7.5}$$

где $n' = n-m-1$. С помощью разложения (7.2) аналогично получаем

$$m_p(G_{\mathrm{II}}) = |A\ominus pQ_p|_p^{-(n+1-2m+m_1)/2}m_p(a(A_{\geqslant p}\ominus pQ_p)^{-1})M_p(\{a\}Q_1^{\perp}).$$

Пусть $A_{\geqslant p} = pA_p\oplus A_2$ с блоком $A_2 \equiv 0 \pmod{p^2}$. Тогда выполняется разложение $aA_{\geqslant p}^{-1} = aA_2^{-1}\oplus(a/p)A_p^{-1}$, и по формуле (7.4) находим

$$m_p(aA_{\geqslant p}^{-1}) = \left|\frac{1}{p}A_2\right|_p^{-m_p/2}m_p(aA_2^{-1})M_p(\{a\}A_p^{-1}).$$

Наконец, разложение $a(A_{\geqslant p}\ominus pQ_p)^{-1} = aA_2^{-1}\oplus(a/p)A_p'^{-1}$ с блоком $A_p' = A_p\ominus Q_p$ приводит к формуле

$$m_p(a(A_{\geqslant p}\ominus pQ_p)^{-1}) = \left|\frac{1}{p}A_2\right|_p^{-m_p'/2}m_p(aA_2^{-1})M_p(\{a\}A_p'^{-1}).$$

Теперь исключаем из двух последних равенств множитель $m_p(aA_2^{-1})$ и из (7.3) выводим формулу

$$\begin{aligned} &c_p(A,Q,G_{\mathrm{II}})m_p(G_{\mathrm{II}})\\ &\quad= \frac{1}{2}|A|_p^{-(n-m)/2}\left|\frac{1}{p}A_2\right|_p^{1/2}p^{-(n+1-2m+m_1)/2}\\ &\qquad\times M_p(\{a\}(A_p\ominus Q_p)^{-1})M_p(\{a\}A_p^{-1})^{-1}M_p(\{a\}Q_1^{\perp}). \end{aligned} \tag{7.6}$$

7.3. Собственно для приложений локальные множители $c_p(A,Q,G)$ нужны в виде следующей комбинации:

$$\alpha_p(A,Q,G) = c_p(A,Q,G)m_p(G)/\operatorname{std}(n-m,d_A), \tag{7.7}$$

где $d_A = |G|$ — определитель (1.9), а в знаменателе — *стандартное значение* p-массы $m_p(G)$ [4, с. 86], определяемое формулой

$$\operatorname{std}_p(n,d)^{-1} = 2(1-p^{-2})\dots(1-p^{-2(s-1)})(1-\varepsilon\, p^{-s})$$

для $n = 2s-1$ или $2s > 0$, $\varepsilon = \left(\frac{(-1)^s\cdot d}{p}\right)$ для четного n и p, не делящих $2d$, а в остальных случаях — $\varepsilon = 0$. Для форм $Q = Q_1 \oplus pQ_p$ числители в (7.7) вычисляются по формулам (7.5) и (7.6).

7.4. Простейшие нетривиальные формулы дают квадратичные формы

$$A = A_1 \oplus pA_p \quad \text{с } \dim A_p = m_p = 1 \tag{7.8}$$

и $n-m \geqslant 3$ нечетным, т.е. A имеет такой же вид, как и форма Q. При ограничениях (7.8) форма G_{I} (7.1) всегда существует, а G_{II} (7.2) — только при совпадении знаков $\varepsilon_p(A) = \varepsilon_p(Q)$ (см. п. 7.1). Используя п. 7.3 и формулы (7.5) и (7.6), прямым вычислением находим

$$\alpha_p(A,Q,G_{\mathrm{I}}) = (p^{n'}-1)/2$$

и

$$\alpha_p(A,Q,G_{\mathrm{II}}) = 1, \quad \text{если } \varepsilon_p(A) = \varepsilon_p(Q).$$

Таким образом, *сумма* $\alpha_p(A,Q)$ этих двух множителей при условии (7.8) равна

$$\alpha_p(A,Q) = (p^{n'} + \varepsilon_p(A)\,\varepsilon_p(Q))/2, \quad \text{где } n' = n-m-1. \tag{7.9}$$

7.5. Пусть положительно определенные $\mathbb{Z}$-*целые* квадратичные формы Q и A размерностей n и m имеют ступени a_Q и a и удовлетворяют условиям:

$$d = |Q| = a_Q, \qquad |A| = a, \tag{7.10}$$

при этом a *бесквадратное*; p^2 не делит d и $p \neq 2$, если простое p делит a и d. Последнее условие означает, что форма Q эквивалентна $Q_1 \oplus pQ_p$ над $\mathbb{Z}_p$, $p \neq 2$, и блок Q_p имеет размерность 1.

Если *четная* форма $Q = Q_{\text{чет}}$, т.е. форма с четной диагональю, представляет над кольцом целых чисел $\mathbb{Z}$ форму A, то A также четная. Пусть дополнительно $n - m \geqslant 3$ нечетное и $d \not\equiv 0 \pmod 4$, то [4, с. 99–100]

$$\alpha_2(A, Q) = 2^{-n'/2-1}.$$

Еще нам потребуется *стандартная масса* $\mathrm{std}(n)$ [10] для нечетных n. Приведем значения $\mathrm{std}(n)$ для небольших n:

$$\mathrm{std}(1) = 2, \quad \mathrm{std}(3)^{-1} = 2 \cdot 3, \quad \mathrm{std}(5)^{-1} = 2^4 \cdot 3^2 \cdot 5,$$
$$\mathrm{std}(7)^{-1} = 2^6 \cdot 3^4 \cdot 5 \cdot 7, \quad \mathrm{std}(9)^{-1} = 2^{10} \cdot 3^5 \cdot 5^2 \cdot 7.$$

Вес представлений $n(A, [Q])$ формы A *родом* $[Q]$ формы Q равен числу $r(A, Q)$ всех целых представлений b из $M_{n,m}(\mathbb{Z})$ формы $A = Q[b]$ с весом $o_{\mathbb{Z}}(Q)^{-1}$, когда $\{Q\}$ пробегает все $\mathrm{SL}_n^{\pm}(\mathbb{Z})$-классы рода $[Q]$. В случае одноклассного рода вес равен

$$n(A, [Q]) = n(A, Q) = r(A, Q)/o_{\mathbb{Z}}(Q).$$

Из формулы (7.9) и [4, с. 102] вытекает

Теорема 7.1. *Пусть целые четные положительно определенные формы* $Q = Q_{\text{чет}}$, $A = A_{\text{чет}}$ *удовлетворяют условиям* (7.10) *и пусть разность их размерностей* $n - m \geqslant 3$ *нечетная. Тогда вес представлений* $n(A, [Q])$ *формы* A *родом* $[Q]$ *равен*

$$n(A, [Q]) = \mathrm{std}(n-m) 2^{-\alpha(d)} \alpha_2(A, Q) \times \prod_{\substack{p \mid (a,d) \\ p \neq 2}} (p^{n'} + \varepsilon_p(A)\,\varepsilon_p(Q)) \prod_{\substack{p \mid d \\ p \nmid 2a}} (q^{n'/2} + \delta_p) \prod_{\substack{p \mid a \\ p \nmid 2d}} (p^{n'/2} + \varepsilon_p), \tag{7.11}$$

при этом $\alpha(d)$ *— количество нечетных простых делителей* d, $n' = n - m - 1$, $q = |Q|_p^{-1}$ *и*

$$\delta_p = \varepsilon_1(Q)\Big(\frac{(-1)^{n'/2} a}{p}\Big), \qquad \varepsilon_p = \varepsilon_1(A)\Big(\frac{(-1)^{n'/2-1} d}{p}\Big),$$

где $\varepsilon_1(Q) = \big(\frac{|Q_1|}{p}\big)$ *и* $\varepsilon_1(A) = \big(\frac{|A_1|}{p}\big)$ *— знаки единичных блоков* Q_1 *и* A_1.

Замечание. Имеются формулы веса $n(A, [Q])$ для всех квадратичных форм Q, A с условием (7.10) (ср. [4, теорема 13.1]).

7.6. Конкретные примеры приведем для квадратичных форм, отвечающих *решеткам корней с нулевой суммой* A_n. По определению A_n является n-мерной подрешеткой кубической решетки $\mathbb{Z}^{n+1}$, состоящей из векторов x с нулевой суммой координат $x_0 + x_1 + \cdots + x_n = 0$. Ее матрица Грама

$$Q_n = \begin{pmatrix} 2 & 1 & \dots & 1 \\ 1 & 2 & \dots & 1 \\ \dots & \dots & \dots & \dots \\ 1 & 1 & \dots & 2 \end{pmatrix}$$

четная, имеет определитель $d_n = n+1$ и порядок группы целых автоморфизмов $o(Q_n) = o_{\mathbb{Z}}(Q_n) = 2\cdot(n+1)!$ Род $[Q_n]$ одноклассный для $n \leqslant 7$. Нам потребуются знаки форм Q_n для $n = 4, 5 : \varepsilon_1(Q_4) = +1$, $\varepsilon_5(Q_4) = +1$, $\varepsilon_1(Q_5) = -1$, $\varepsilon_3(Q_5) = +1$.

7.7. Пример 1. Пусть $Q = Q_4$, $A = a = 2 \cdot 5 \cdot a_1$, где $a_1 \geqslant 1$ — бесквадратное число, не делящееся на 2 и 5. В данном случае $d = d_4 = 5$, $O(Q_4) = 2 \cdot 5!$, и в обозначениях теоремы 7.1 имеем

$$n - m = 3, \quad n' = 2, \quad \varepsilon_5(A) = -\Big(\frac{a_1}{5}\Big), \quad \varepsilon_p = \Big(\frac{5}{p}\Big) = \Big(\frac{p}{5}\Big)$$

для p, делящих a_1. Отсюда и из (7.11) получаем формулу

$$r(A, Q_4) = 5\Big(25 - \Big(\frac{a_1}{5}\Big)\Big) \prod_{p|a_1} \Big(p + \Big(\frac{p}{5}\Big)\Big) \tag{7.12}$$

для числа решений системы уравнений

$$x_0^2 + x_1^2 + \cdots + x_4^2 = 10a_1, \quad x_0 + x_1 + \cdots + x_4 = 0, \quad x_i \in \mathbb{Z},$$

где $a_1 \geqslant 1$ нечетное бесквадратное, не делящееся на 5.

Пример 2. Теперь возьмем $Q = Q_5$ и $A = \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ — четную положительно определенную форму с определителем $|A| = a = 3 \cdot a'$, где a' — бесквадратное с условием $(a', 6) = 1$. Имеем $d = d_5 = 2 \cdot 3$, $o(Q_5) = 2 \cdot 6!$ Разность размерностей $n - m = 3$ и $n' = 2$ не изменились, и по (7.11) число целых представлений бинарной формы A формой Q_5 равно $r(A, Q_5)$ (5).

Список литературы

[1] Siegel C. L., *Über die analytische Theorie der quadratischen Formen*, Ann. of Math. (2) **36** (1935), 527–606.

[2] Андрианов А. Н., Журавлев В. Г., *Модулярные формы и операторы Гекке*, Наука, М., 1990.

[3] Журавлев В. Г., *Мультипликативная арифметика тета-рядов нечетных квадратичных форм*, Изв. РАН. Сер. мат. **59** (1995), № 3, 77–140.

[4] Журавлев В. Г., *Представление формы родом квадратичных форм*, Алгебра и анализ **8** (1996), № 1, 21–112.

[5] Касселс Дж., *Рациональные квадратичные формы*, Мир, М., 1982.

[6] Никулин В. В., *Целочисленные симметрические билинейные формы и некоторые их геометрические приложения*, Изв. АН СССР. Сер. мат. **43** (1979), № 1, 111–177.

[7] Артин Э., *Геометрическая алгебра*, Наука, М., 1969.

[8] Elstrodt J., Grunewald F., Mennicke J., *Arithmetic applications of the hyperbolic lattice point theorem*, Proc. London Math. Soc. (3) **57** (1988), no. 2, 239–283.

[9] Конвей Дж., Слоэн Н., *Упаковки шаров, решетки и группы.* Т. 1, 2, Мир, М., 1990.

[10] Conway J. H., Sloane N. J., *Low-dimensional lattices.* IV. *The mass formula*, Proc. Roy. Soc. London Ser. A **419** (1988), no. 1857, 259–286.

Поступило 24 ноября 1997 г.

Владимирский государственный
педагогический университет
кафедра алгебры
600024, г. Владимир, пр. Строителей, 11 Россия
E-mail: zhuravl@vgpu.elcom.ru