*Сибирский математический журнал*
*Март—апрель, 2007. Том 48, № 2*

*УДК 511.512*

# ОБ АСИМПТОТИКЕ ЧИСЛА ПРИВЕДЕННЫХ ЦЕЛОЧИСЛЕННЫХ БИНАРНЫХ КВАДРАТИЧНЫХ ФОРМ С УСЛОВИЕМ ДЕЛИМОСТИ ПЕРВЫХ КОЭФФИЦИЕНТОВ

**У. М. Пачев**

**Аннотация:** Дискретным эргодическим методом для указанных в заглавии квадратичных форм получены асимптотические формулы с остаточными членами, зависящими от $L$-функции Дирихле $L(s,\chi)$ и ее поведения, связанного с некоторыми гипотезами.

**Ключевые слова:** дискретный эргодический метод, приведенная бинарная квадратичная форма, делимость коэффициентов, вектор-матрица второго порядка.

## 1. Введение. Формулировки результатов

В работе подводится некоторый итог изучению асимптотического поведения числа приведенных целочисленных бинарных квадратичных форм с условием делимости первых коэффициентов. Впервые исследования по асимптотическому подсчету числа положительных бинарных квадратичных форм с указанным условием были проведены Ю. В. Линником [1] в связи с приложениями разработанного им так называемого дискретного эргодического метода (ДЭМ) к вопросу об асимптотике числа представлений целых чисел неопределенными тернарными квадратичными формами (обзор метода и результатов его применения см. в [2]). Эти исследования были продолжены Б. Ф. Скубенко [3], А. В. Малышевым и автором в ряде работ (см., например, [4, 5]). При этом в [4, 5] соответственно в случаях положительных и неопределенных бинарных квадратичных форм получены асимптотические формулы для числа $T_1(m,q)$ целочисленных приведенных бинарных квадратичных форм определителя $m$, первые коэффициенты которых делятся на заданное нечетное число $q$.

Основной асимптотический результат о величине $T_1(m,q)$, полученный в работах [4, 5], имеет вид

$$T_1(m,q) \sim \frac{2^{\nu(q)}}{q\prod\limits_{p|q}\left(1+\frac{1}{p}\right)}T(m),$$

где $\sim$ обозначает знак асимптотической эквивалентности; $T(m)$ — число приведенных целочисленных бинарных квадратичных форм определителя $m$; $\nu(q)$ — число различных простых делителей $p \mid q$; постоянные, входящие в эту асимптотическую формулу, зависят только от $q$.

Заметим, что частный случай указанного результата, когда $q = p^k$, где $p$ — нечетное простое число, и в предположении, что $m$ нечетно, содержится в [1].

При этом вместо $T(m)$ в [4] использовалось обозначение $h(-m)$, т. е. $T(m) = h(-m)$, где $h(-m)$ — число классов положительных бинарных квадратичных форм определителя $m$.

В отличие от предшествующих исследований в настоящей работе рассматриваются одновременно оба случая как положительных, так и неопределенных бинарных квадратичных форм, причем даются оценки остаточных членов в получающихся асимптотических формулах для $T_1(m,q)$. К сожалению, остаточные члены полученных асимптотических формул зависят от $L$-функции Дирихле $L(s,\chi)$ и ее поведения, связанного с гипотезами $(\mathfrak{K})$ и $(\mathscr{G})$ (см. ниже), при этом $\chi = \chi(k)$ — вещественный характер Дирихле, отвечающий квадратичному полю $\mathbb{Q}(\sqrt{m})$ и имеющий наименьший модуль среди характеров, для которых $\chi(k) = \left(\frac{-m}{k}\right)$, если НОД$(k, 2m) = 1$.

Сначала получим с помощью ДЭМ асимптотическую формулу для $T_1(m,q)$ с остаточным членом, зависящим от неэлементарной функции $l(m)$, определяемой равенством

$$l(m) = -\frac{\log L(1,\chi)}{\log |m|}, \tag{1}$$

где

$$L(s,\chi) = \sum_{k=1}^{\infty} \frac{\chi(k)}{k^s}, \quad \operatorname{Re} s > 1,$$

— $L$-функция Дирихле.

Первая из используемых нами гипотез для $L$-функции Дирихле относится в неявном виде к «зигелеву нулю» (она существенно слабее расширенной гипотезы Римана).

**Гипотеза** $(\mathfrak{K})$**.** *Пусть $\chi = \chi(k)$ — вещественный характер Дирихле, имеющий наименьший модуль среди характеров, для которых*

$$\chi(k) = \left(\frac{-m}{k}\right), \quad \text{если НОД}(k, 2m) = 1.$$

*Тогда при $|m| \to \infty$*

$$l(m) \ll -\frac{1}{\log\log |m|}, \tag{2}$$

*где постоянные, входящие в символ $\ll$, абсолютные.*

Заметим, что оценка (2) в гипотезе $(\mathfrak{K})$ равносильна оценке

$$L(1,\chi) \gg |m|^{-\frac{c}{\log\log|m|}}, \tag{3}$$

где $c$ — некоторая положительная постоянная. Теорема Зигеля (см., например, [6, 7]) дает вместо (3) лишь оценку

$$L(1,\chi) \gg |m|^{-\varepsilon},$$

где постоянные, входящие в $\gg$, зависят только от $\varepsilon > 0$.

Во второй гипотезе речь идет об области, свободной от нулей $L(s,\chi)$.

**Гипотеза** $(\mathscr{G})$**.** *В области*

$$|s-1| < \frac{(\log\log|m|)^2 \log\log\log|m|}{\sqrt{\log|m|}} \tag{4}$$

*комплексного переменного $s$ нет нулей $L(s,\chi)$.*

Заметим, что гипотеза $(\mathfrak{K})$ следует из гипотезы $(\mathscr{G})$ (см. [8]).

Сформулируем теперь полученные основные результаты (необходимые для понимания определения из теории бинарных квадратичных форм и арифметики матриц второго порядка см. ниже или в [9, 10]).

**Теорема 1.** *Пусть $m \neq 0$ — целое число; $\sqrt{|m|} \notin \mathbb{Q}$; $q$ — целое число, причем* НОД$(q, 2m) = 1$*; $u$ — целое число, для которого*

$$u^2 + m \equiv 0 (\bmod q). \tag{5}$$

Для произвольной целой матрицы второго порядка $Q$ нормы $q$ обозначим через $r(m; Q, u)$ число приведенных целочисленных собственно примитивных вектор-матриц $L$ нормы $m$, для которых выполняется делимость справа $u + L/Q$. Тогда при $|m| \to \infty$

$$r(m; Q, u) = \frac{T(m)}{\sigma_0(q)} \{1 + O(\gamma(m))\}, \tag{6}$$

где $T(m)$ — число приведенных целочисленных собственно примитивных бинарных квадратичных форм определителя $m$; $\sigma_0(q)$ — число неассоциированных слева примитивных матриц нормы $q$;

$$\gamma(m) = \sqrt{\left(l(m) + \frac{1}{\log\log|m|}\right) \log \left| l(m) + \frac{1}{\log\log|m|} \right|}, \tag{7}$$

постоянная, входящая в символ $O$, зависит только от $q$.

Опираясь на теорему 1, получаем следующий результат.

**Теорема 2.** *Пусть $m \neq 0$ — целое число; $\sqrt{|m|} \notin \mathbb{Q}$; $q > 0$ — целое число, причем* НОД$(q, 2m) = 1$ *и $\left(\frac{-m}{p}\right) = 1$ для всех простых $p \mid q$. Тогда при $|m| \to \infty$*

$$T_1(m, q) = \frac{2^{\nu(q)}}{q \prod\limits_{p|q} \left(1 + \frac{1}{p}\right)} T(m) \{1 + O(\gamma(m))\}, \tag{8}$$

*где $\gamma(q)$ — число различных простых делителей числа $q$; постоянная, входящая в асимптотическую формулу (8), зависит только от $q$.*

Этот результат приводится в предварительном сообщении [11].

В следующих теоремах используются сформулированные гипотезы о поведении $L$-функции Дирихле.

**Теорема 3.** *Пусть в условиях теоремы 2 выполнена гипотеза $(\mathfrak{K})$, т. е. $l(m) \ll \frac{1}{\log\log|m|}$. Тогда при $|m| \to \infty$*

$$T_1(m, q) = \frac{2^{\nu(q)}}{q \prod\limits_{p|q} \left(1 + \frac{1}{p}\right)} T(m) \left\{1 + O\left(\sqrt{\frac{\log\log\log|m|}{\log\log|m|}}\right)\right\}, \tag{9}$$

*постоянные, входящие в асимптотическую формулу (9), зависят только от $q$.*

С использованием гипотезы $(\mathscr{G})$ получаем следующий результат.

**Теорема 4.** *Пусть в условиях теоремы 2 выполнена гипотеза $(\mathscr{G})$, т. е. в области*

$$|s - 1| < \frac{(\log\log|m|)^2 \log\log\log|m|}{\sqrt{\log|m|}}$$

*комплексной переменной $s$ нет нулей $L(s, \chi)$. Тогда при $|m| \to \infty$*

$$T_1(m, q) = \frac{2^{\nu(q)}}{q \prod\limits_{p|q} \left(1 + \frac{1}{p}\right)} T(m) \left\{1 + O\left(\frac{1}{(\log|m|)^{\frac{1}{4}}}\right)\right\}, \tag{10}$$

*постоянные, входящие в (10), зависят только от $q$.*

## 2. Вспомогательные результаты из арифметики матриц второго порядка

Прежде чем приступить к доказательствам теорем 1–4, приведем необходимые понятия и вспомогательные результаты из арифметики матриц второго порядка, используемые нами в дальнейшем (подробности см. в [9]).

Мы будем рассматривать бинарную квадратичную форму

$$\varphi = \varphi(x, y) = \alpha x^2 + 2\beta xy + \gamma y^2 \tag{11}$$

с коэффициентами $\alpha$, $\beta$, $\gamma \in \mathbb{Q}$, при этом $\alpha$ — первый коэффициент формы (11), на котором будет сосредоточено наше основное внимание; $d = d(\varphi) = \alpha\gamma - \beta^2$ — ее определитель. Условия приведенности квадратичной формы (11) определителя $d$ в случаях $d > 0$ и $d < 0$ соответственно имеют вид

$$2|\beta| < \alpha < \gamma, \quad 0 < 2\beta < \alpha = \gamma, \quad 0 < 2\beta = \alpha < \gamma, \tag{12}$$

$$0 \le \beta < \sqrt{-d}, \quad \sqrt{-d} - \beta < |\alpha| < \sqrt{-d} + \beta. \tag{13}$$

Две формы $\varphi$ и $\varphi'$ называются *эквивалентными* (точнее, *целочисленно эквивалентными*), если $\varphi$ переходит в $\varphi'$ целочисленной линейной подстановкой $U$ переменных с $\det U = \pm 1$.

Форму $\varphi = (\alpha, \beta, \gamma)$ называем *целочисленной* (или *классически целочисленной*), если ее коэффициенты $\alpha$, $\beta$, $\gamma \in \mathbb{Z}$ — целые числа. Множество всех эквивалентных между собой целочисленных бинарных квадратичных форм образует класс форм заданного определителя $d$, число которых конечно. В случае положительных бинарных квадратичных форм, т. е. при $d > 0$ в каждом классе содержится только одна приведенная форма вида (12).

В отличие от них, т. е. в случае $d < 0$, имеется (см. [10, гл. IV]) конечное число различных целочисленных приведенных неопределенных бинарных квадратичных форм, эквивалентных данной форме:

$$\varphi_1, \varphi_2, \ldots, \varphi_{2n}; \quad \varphi_i = \varphi_{i+2nk}, \quad k \in \mathbb{Z}; \tag{14}$$

они образуют период (цикл) приведенных форм; элементы периода (14) упорядочены так, что $\varphi_i$ и $\varphi_{i+1}$ — соседние формы (см. [10, гл. IV]). Число этих периодов равно числу классов неопределенных бинарных квадратичных форм.

Мы рассматриваем также квадратные матрицы $A = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}$ второго порядка над полем рациональных чисел, $\alpha_{ij} \in \mathbb{Q}$, $(i, j = 1, 2)$. Число $N(A) = \det A = \alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21}$ называем (по аналогии с алгеброй кватернионов) *нормой матрицы* $A$.

След матрицы $A$, как обычно, определяется равенством $\operatorname{Sp} A = \alpha_{11} + \alpha_{22}$. Если $\operatorname{Sp} A = 0$, то $A$ называем *вектор-матрицей.* Любую матрицу $A$ можно представить единственным способом в виде $A = l + L$, где $l = lE$ — скалярная матрица, $L$ — вектор-матрица, причем число $l$ определяется равенством $l = \frac{1}{2}\operatorname{Sp} A$.

Вектор-матрицу

$$L = \begin{pmatrix} \beta & -\alpha \\ \gamma & -\beta \end{pmatrix}, \quad \alpha, \beta, \gamma \in \mathbb{Q} \tag{15}$$

(ясно, что это общий вид вектор-матриц), сопоставляем с бинарной квадратичной формой $\varphi = \alpha x^2 + 2\beta xy + \gamma y^2$. В связи с этим можно говорить о положительной или неопределенной вектор-матрице.

Вектор-матрица (15) называется *приведенной*, если соответствующая ей форма $\varphi = (\alpha, \beta, \gamma)$ является приведенной, т. е. выполняется одно из условий (12) или (13). Матрицу

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \tag{16}$$

называем *целой* (см. [9]), если $a_{ij} \in \mathbb{Z}$ $(i, j = 1, 2)$. Говорим, что целая матрица (16) *примитивна*, если НОД$(a_{11}, a_{12}, a_{21}, a_{22}) = 1$. В кольце $M_2(\mathbb{Z})$ целых матриц второго порядка определяем ассоциированность матриц слева и справа.

Матрицу $A_1$ называем *ассоциированной слева с матрицей* $A \in M_2(\mathbb{Z})$, если найдется такая целая матрица $U$ с нормой $N(U) = \pm 1$, для которой $A_1 = UA$. Аналогично будем говорить, что $A_1$ *ассоциирована справа с* $A$, если найдется $V \in M_2(\mathbb{Z})$ с нормой $N(V) = \pm 1$ так, что $A_1 = A \cdot V$.

Определим также понятие делимости матриц справа и слева. Пусть $A$, $B \in M_2(\mathbb{Z})$, причем $B$ — неособая матрица, т. е. $N(B) \neq 0$. Будем говорить, что $A$ *делится справа на* $B$, и записывать $A/B$, если $AB^{-1}$ — целая матрица, т. е. $AB^{-1} \in M_2(\mathbb{Z})$. Аналогично $A$ *делится слева на* $B$, записывается $B \backslash A$, если $B^{-1}A \in M_2(\mathbb{Z})$.

Приведем также используемые нами результаты из арифметики матриц второго порядка.

**Предложение 1.** *Пусть $q > 0$ — нечетное число. Обозначим через $\sigma_0(q)$ число неассоциированных слева примитивных матриц второго порядка нормы $q$. Тогда*

$$\sigma_0(q) = q \prod_{p|q} \left(1 + \frac{1}{p}\right). \tag{17}$$

Доказательство см. в [9] (см. также [5], где дается более простое доказательство с использованием канонических треугольных матриц из [12]).

Большую роль в ДЭМ играет следующий матричный аналог основной теоремы арифметики.

**Предложение 2.** *Пусть $A$ — целая матрица нормы $N(A) = a \neq 0$, и пусть $a = b \cdot c$, где $b$, $c$ — целые числа. Тогда найдутся такие целые матрицы $B$ и $C$, что $A = B \cdot C$, $N(B) = b$, $N(C) = c$. При этом если*

$$A = B_1 C_1, \quad B_1, C_1 \in M_2(\mathbb{Z}), \quad N(B_1) = b, \quad N(C_1) = c,$$

*то $B_1$ ассоциирована справа с $B$.*

Доказательство см. в [9]. По индукции предложение 2 обобщается на несколько сомножителей.

Для полноты изложения воспроизведем использованные в [5] понятия и результаты с необходимыми уточнениями (см. также [13]).

Вектор-матрицу

$$L = \begin{pmatrix} b & -a \\ c & -b \end{pmatrix}, \quad L \in M_2(\mathbb{Z}),$$

нормы $N(L) = ac - b^2$ называем *собственно примитивной*, если НОД$(a, 2b, c) = 1$. Ясно, что число собственно примитивных приведенных вектор-матриц нормы $m$ равно $T(m)$.

При применении ДЭМ наибольшую трудность доставляет случай неопределенных бинарных квадратичных форм, требующий отдельного рассмотрения некоторых дополнительных сведений по сравнению со случаем положительных бинарных квадратичных форм.

Соответственно периоду неопределенных форм (14) рассматриваем период вектор-матриц $L = L_1, L_2, \ldots, L_{2n}$, который можно продолжить периодично $(\operatorname{mod} 2n)$ влево и вправо, причем

$$L_{i+1} = \begin{pmatrix} 0 & -1 \\ 1 & k_i \end{pmatrix} L_i \begin{pmatrix} 0 & -1 \\ 1 & k_i \end{pmatrix}^{-1} \quad (i = 0, \pm 1, \pm 2, \ldots),$$

где $k_i$ — некоторые целые числа.

Как и в [1, 13], введем в рассмотрение матрицы

$$E^{(i)} = \begin{pmatrix} 0 & -1 \\ 1 & k_1 \end{pmatrix}^{-1} \cdot \ldots \cdot \begin{pmatrix} 0 & -1 \\ 1 & k_{i-1} \end{pmatrix} \quad (i = 1, \ldots, 2n),$$

$E^{(0)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$; $k_1, \ldots, k_{i-1}$ — целые числа, так что

$$E^{(i)} L (E^{(i)})^{-1} = L_i \quad (i = 1, \ldots, 2n),$$

где $2n$ — длина периода вектор-матрицы $L$.

Для целых вектор-матриц $L$ и $L'$ найдется (см. [1]) целая матрица $A$ с условием $ALA^{-1} = L'$ (такое свойство относится к теории поворотов вектор-матриц). Обозначим $E_L = \tilde{t} - \tilde{u}L$, где $\tilde{t}$, $\tilde{u}$ — наименьшее целое положительное решение уравнения Пелля $t^2 + mu^2 = 1$.

Следуя [13], определим матрицу $\mathscr{E}_k = (E_L)^q E^{(r)}$, где $k \in \mathbb{Z}$, $k = 2nq + r$, $q$, $r \in \mathbb{Z}$, $0 \le r < 2n$.

Тогда

$$A_k L_k A_k^{-1} = L', \quad A_k = \mathscr{E}_k A \quad (k = 0, \pm 1, \pm 2, \ldots). \tag{18}$$

Среди матриц $A_k = \mathscr{E}_k A$, ассоциированных слева с матрицей $A$ и переводящих одну из вектор-матриц $L_k$ периода $\{L = L_1, L_2, \ldots, L_{2n}\}$ в вектор-матрицу $L'$ по формуле (18), можно подобрать матрицу (см. [1, 13]), играющую особую роль при применении ДЭМ к исследуемому вопросу (существование такой матрицы гарантирует следующее предложение).

**Предложение 3.** *Если $L$, $L'$ — приведенные неопределенные вектор-матрицы и $A$ — целая матрица с условием $ALA^{-1} = L'$, $N(A) > 0$, то найдется такая матрица $A' = EA = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}$, ассоциированная с $A$ слева, для которой $L'' = A'L(A')^{-1} = EL'E^{-1}$, эквивалентная $L'$, приведена, причем $\alpha'\beta'\gamma'\delta' \le 0$, где $E$ — целочисленная унимодулярная матрица.*

Доказательство этого предложения см. в [1].

Матрицу $A$ из предложения 3 будем называть, следуя [13], *полупримарной* (а по терминологии [3] — *удобной*).

Следующее предложение, относящееся к вопросу делимости целых матриц большой нормы, дает нужное нам уточнение соответствующего результата [4].

**Предложение 4.** *Пусть $q > 1$ — нечетное число, $t \ge 2$ — целое число. Пусть $Q_1$ и $Q_2$ — целые примитивные матрицы нормы $q$. Обозначим через $\sigma_0(q^t; Q_1, Q_2)$ число всех неассоциированных слева целых примитивных матриц $B$ с условием*

$$N(B) = q^t, \quad Q_1 \backslash B, \quad B / Q_2.$$

*Тогда при* $t \to \infty$

$$\sigma_0(q^t; Q_1, Q_2) = \frac{\sigma_0(q^t)}{\sigma_0(q^2)} + O((q^t)^{\frac{11}{12}+\varepsilon}), \tag{19}$$

*где постоянные, входящие в* $O$*, зависят только от* $q$ *и* $\varepsilon > 0$.

Доказательство непосредственно следует из предложения 4.2 в [9].

Следующее предложение дает нужное нам уточнение ключевой леммы ДЭМ из [14].

**Предложение 5** (ключевая лемма ДЭМ для вектор-матриц). *Пусть* $m \neq 0$ *— целое число. Рассмотрим* $r(m)$ *матричных равенств в кольце* $M_2(\mathbb{Z})$*:*

$$l + L_i = B_i U_i, \quad N(B_i) = b \quad (i = 1, \dots, r(m)), \tag{20}$$

*где* $B_i$ *— целая примитивная матрица;* $l$ *— целое число с условием*

$$l^2 + m \equiv 0 (\operatorname{mod} b), \tag{21}$$

*причем* $b = q^s$*, где* $q > 1$ *— нечетное число;* $s$ *— целое число, для которого*

$$c_2 \frac{\log|m|}{\log q} < s < c_1 \frac{\log|m|}{\log q}, \tag{22}$$

*здесь* $c_1 = \frac{1}{8}$, $c_2 > 0$ *— некоторая постоянная.*

*Пусть* $w$ *— число неассоциированных справа матриц* $B_i$*, которые встретятся в* $r'$ *произвольно выбранных равенствах* (20). *Тогда если*

$$r' \gg r(m) \cdot 2^{-\frac{c \log|m|}{\log\log|m|}}, \tag{23}$$

*где* $c > 0$ *— некоторая постоянная, то при* $|m| \to \infty$

$$w \gg b \cdot L(1, \chi) \cdot 2^{-\frac{c' \log|m|}{\log\log|m|}}, \tag{24}$$

*где* $c' = 4c + 2$*; постоянные, входящие в символ* $\gg$ *оценки* (24)*, зависят только от* $q$ *и* $c_2$.

Доказательство см. в [15].

## 3. Доказательство теоремы 1

1°. Фиксируем число $\tau$ с условием $0 < \rho < \frac{1}{8}$ и рассмотрим целые числа

$$\delta(m) = \left[\frac{13 \log \eta(m)}{\log q}\right], \quad s_1 = \left[\frac{\rho \log|m|}{\delta(m) \log q}\right], \quad s = \delta(m) s_1, \tag{25}$$

где

$$\eta(m) = \frac{1}{l(m) + \frac{c' \log 2}{\log\log|m|}}. \tag{26}$$

В силу (4) можно подобрать целое число $l$ так, чтобы

$$l \equiv u (\operatorname{mod} q), \quad l^2 + m \equiv 0 (\operatorname{mod} q^s), \quad \text{НОД}\left(\frac{l^2+m}{q^s}, q\right) = 1. \tag{27}$$

Пусть $L_1, \dots, L_T$, $T = T(m)$, — полный набор приведенных собственно примитивных вектор-матриц нормы $m$.

В силу (27)

$$N(l+L_i) = l^2 + m \equiv 0 (\operatorname{mod} q^s) \quad (i=1,\dots,T).$$

Тогда по предложению 2 имеем матричные разложения

$$l+L_i = X_i B_i, \quad B_i = Q_{is}\cdot\ldots\cdot Q_{i1} \quad (i=1,\dots,T), \tag{28}$$

где $Q_{ij}$ — примитивные матрицы нормы $q$, $B_i$ — примитивные матрицы нормы $q^s$.

В случае неопределенных вектор-матриц, т. е. при $m<0$, следуя [1], в силу предложения 3 будем выбирать матрицы $T_{\alpha j} = Q_{\alpha j}\cdot\ldots\cdot Q_{\alpha 1}$ так, чтобы $T_{\alpha j}$ были полупримарными и $T_{\alpha j} L_\alpha T_{\alpha j}^{-1}$ приведенными вектор-матрицами нормы $m$. При этом сам выбор полупримарных матриц для поворота $T_{\alpha j} L_\alpha T_{\alpha j}^{-1}$ неоднозначен вследствие того, что число представителей в цикле класса соответствующих форм, вообще говоря, неодинаково для разных классов и в связи с этим имеется некоторый произвол в выборе матриц-операторов $T_{\alpha j}$. Будем считать, что в случае $m<0$ в матричных равенствах (28) уже произведен описанный выбор матриц $T_{\alpha j}$ для всех $\alpha$.

Из разложений (28), считая, что в них выполнены указанные выше требования, произвольным образом выберем $T'$ равенств

$$l+L_\beta = X_\beta B_\beta \quad (\beta=1,\dots,T'), \tag{29}$$

где $0<l<q^s$.

2°. Пусть $Q^{(1)}, \dots, Q^{(\sigma_0(q))}$ — некоторый набор всех примитивных неассоциированных слева матриц нормы $q$. Обозначим через $r_i(Q^{(i)},T')$ число матриц $T_{\beta i}$ в равенствах (29), которые делятся справа на $Q^{(i)}$, где $i\le i\le s$.

Тогда если

$$T' > T(m)\cdot|m|^{-\eta_0},$$

то для всех $i=1,\dots,s$, за возможным исключением $\eta(\eta_0)s$, справедливо асимптотическое соотношение

$$r_i(Q^{(i)},T') = \frac{T'}{\sigma_0(q)}\{1+O(\gamma(m))\}, \tag{30}$$

где $\eta(\eta_0)$ — некоторая положительная постоянная, зависящая от $\eta_0>0$.

Как и в [5] (см. также [16]), для доказательства (30) рассмотрим матрицу

$$\begin{pmatrix} Q_{11} & \dots & Q_{1s} \\ \dots & \dots & \dots \\ Q_{T'1} & \dots & Q_{T's} \end{pmatrix}, \tag{31}$$

составленную из матриц $Q_{ij}$.

Допустим, что соотношение (30) не имеет места. Тогда есть $\xi_0 s$ индексов $i$, для которых

$$r_i(Q^{(j)},T') > \frac{T'}{\sigma_0(q)}(1+c_0\gamma(m)) \tag{32}$$

или

$$r_i(Q^{(j)},T') < \frac{T'}{\sigma_0(q)}(1-c_0\gamma(m)),$$

где $c_0>0$ — некоторая постоянная.

Пусть эти неравенства выполняются для индексов $i_1, \dots, i_n$, где $\xi_0 s < n \le s$. Тогда найдется $s_1 = \frac{\xi_0 s}{2}$ индексов $i_1, \dots, i_{s_1}$ (считаем сделанной перенумерацию исходных индексов), для которых одновременно для всех $i_1, \dots, i_{s_1}$ будет выполнено одно из неравенств (32).

Следуя теперь приему А. В. Малышева [16], будем в матрице (31) вести счет по столбцам с номерами $i_1, \dots, i_s$ и по строкам с номерами от 1 до $T'$, учитывая при этом неравенства (32). В случае неопределенных вектор-матриц, т. е. при $m < 0$, надо из матричных равенств (29), следуя рассуждениям [1], отбросить те, которые приводят к ассоциированным слева матрицам $T_{\beta i}$ при фиксированных $i$. Тогда в обоих случаях неравенств (32) получим $T_1 > \eta_1(\gamma(m))T'$ равенств (29) со следующим условием: произведения $B_\beta = Q_{\beta s} \cdot \ldots \cdot Q_{\beta 1}$ будут иметь больше, чем $\left(1 + \frac{c_0\gamma(m)}{2}\right)\frac{s_1}{\sigma_0(q)}$, или меньше, чем $\left(1 - \frac{c_0\gamma(m)}{2}\right)\frac{s_1}{\sigma_0(q)}$, матриц $Q_{\beta i}$, ассоциированных слева с $Q^{(j)}$ при $i = i_1, \dots, i_{s_1}$. При этом среди матриц $T_{\beta i}$ при фиксированном $i$ нет ассоциированных слева.

3°. Мы будем следовать рассуждениям [17], внося соответствующие изменения, связанные со случаем матриц вместо кватернионов. Среди индексов $i = 1, \dots, s$ отметим индексы с номерами

$$j_k = k\delta(m) \quad (k = 1, \dots, s_1). \tag{33}$$

Не нарушая общности, будем рассматривать только матрицы $B_\beta$, сомножители $Q_{\beta i}$ которых удовлетворяют условиям, что произведения $B_\beta = Q_{\beta s} \cdot \ldots \cdot Q_{\beta 1}$ будут иметь меньше, чем $\left(1 - \frac{c_0\gamma(m)}{2}\right)\frac{s_1}{\sigma_0(q)}$, матриц $Q_{\beta i}$, ассоциированных слева с $Q^{(i)}$ при $i = i_1, \dots, i_s$.

Тогда, следуя [17], можно показать, что среди $T'$ равенств (28) имеется

$$r' > \frac{\frac{c_0\gamma(m)}{2}}{1 - \frac{c_0\gamma(m)}{2}} T' \tag{34}$$

таких равенств (делая перенумерацию, считаем, что это первые $r'$ равенств (29))

$$l + L_\beta = X_\beta B_\beta, \quad B_\beta = Q_{\beta s} \cdot \ldots \cdot Q_{\beta 1} \quad (\beta = 1, \dots, r'), \tag{35}$$

что для каждого из них число индексов $k = 1, \dots, s_1$, для которых $Q_{ij_k}$ ассоциирована слева с $Q$, будет меньше, чем

$$\left(1 - \frac{c_0\gamma(m)}{2}\right)\frac{s_1}{\sigma_0(q)}. \tag{36}$$

4°. Пусть $w'$ — число неассоциированных слева примитивных матриц $B_\beta = Q_{\beta s} \cdot \ldots \cdot Q_{\beta 1}$ в равенствах (35). Оценим $w'$ сверху. Ясно, что

$$w' \le w_1, \tag{37}$$

где $w_1$ — число всех неассоциированных слева примитивных матриц вида

$$B^{(t)} = Q_s^{(t)} \cdot \ldots \cdot Q_1^{(t)} \quad (t = 1, \dots, w_1),$$

где $Q_1^{(t)}$ пробегает все различные матрицы из набора $\{Q_{11}, \dots, Q_{T'1}\}$; $Q_2^{(t)}$ — из набора $\{Q_{12}, \dots, Q_{T'2}\}$; $\dots$, $Q_s^{(t)}$ — из набора $\{Q_{1s}, \dots, Q_{T's}\}$, причем

$$\#\{k |\, Q_{ik}^{(t)} = EQ, N(E) = 1\} < \left(1 - \frac{c_0\gamma(m)}{2}\right)\frac{s_1}{\sigma_0(q)}. \tag{38}$$

Пусть $Q^{(1)} = Q, Q^{(2)}, \ldots, Q^{(\sigma_0(q))}$ — фиксированный набор всех неассоциированных слева примитивных матриц нормы $q$. Тогда, как и в [4], с учетом предложения 2 по матрице $B$ однозначно найдется ассоциированная ей слева примитивная матрица $B'$ так, что

$$B' = C_1 Q_1' C_2 Q_2' \cdot \ldots \cdot C_s Q_s', \tag{39}$$

где $C_1$ — некоторая матрица нормы $q^{\delta(m)-1}$,

$$Q_i' \in \{Q^{(1)}, Q^{(2)}, \ldots, Q^{(\sigma_0(q))}\} \quad (i = 1, \ldots, s_1).$$

Поэтому

$$w_1 \le w, \tag{40}$$

где $w$ — число всех матриц вида (39), когда $Q_{i-1}' C_i Q_i'$ пробегает все примитивные матрицы нормы $q^{\delta(m)+1}$ некоторой системы неассоциированных слева матриц, причем $Q_0' = E$ есть единичная матрица и в силу (37)

$$\#\{i |\, Q_i' = Q^{(1)} = Q\} < \left(1 - \frac{c_0 \gamma(m)}{2}\right) \frac{s_1}{\sigma_0(q)}.$$

Но по предложению 4, в котором возьмем $Q_2 = E$, при данных $j$ и $k$ число всех примитивных неассоциированных слева матриц $Q^{(j)} C Q^{(k)}$ нормы $q^{\delta(m)+1}$ при достаточно большом $\delta(m)$ оценивается так:

$$\#\{Q^{(j)} C Q^{(k)} | N(C) {=} q^{\delta(m)-1}, Q^{(j)} C Q^{(k)} \text{примитивные неассоциированные слева}\}$$
$$= \frac{1}{\sigma_0(q)} \cdot q^{j_1} \prod_{p|q} \left(1 + \frac{1}{p}\right) \left\{1 + O\left(q^{-\frac{j_1}{13}}\right)\right\};$$

аналогично

$$\#\{C Q^{(k)} \mid N(C) = q^{\delta(m)-1},\ C Q^{(k)} \text{ примитивные неассоциированные слева}\}$$
$$= q^{\delta(m)-1} \left\{1 + O\left(q^{-\frac{\delta(m)}{13}}\right)\right\}.$$

Поэтому число матриц $B'$ вида (39), у которых для $s_2$ индексов $i$ из набора $(i = 1, \ldots, s_1)$ имеет место равенство $Q_i' = Q^{(1)} = Q$, а для остальных $s_1 - s_2$ индексов имеет место равенство $Q_i' = Q^{(j)} \ne Q$ $(j = 2, \ldots, \sigma_0(q))$, равно

$$\left(\frac{1}{\sigma_0(q)}\right)^{s_2} \left(1 - \frac{1}{\sigma_0(q)}\right)^{s_1 - s_2} q^s \prod_{p|q} \left(1 + \frac{1}{p}\right) \prod_{k=1}^{s_1} \left(1 + O\left(q^{-\frac{\delta(m)}{13}}\right)\right).$$

Поэтому при $\delta(m) \to \infty$

$$w \le \left\{q^s \prod_{p|q} \left(1 + \frac{1}{p}\right)\right\} \left(1 + c' \cdot q^{-\frac{\delta(m)}{13}}\right)^{s_1}$$
$$\times \sum_{s_2 \le \left(1 - \frac{c_0 \gamma(m)}{2}\right) \frac{s_1}{\sigma_0(\eta)}} \frac{s_1!}{s_2!(s_1 - s_2)!} \left(\frac{1}{\sigma_0(q)}\right)^{s_2} \left(1 - \frac{1}{\sigma_0(q)}\right)^{s_1 - s_2}. \tag{41}$$

Рассуждая, как и в [4, с. 62, 63], т. е. произведя оценку сверху правой части неравенства (41), получим, что при некоторой постоянной $c'' = c''(c_0)$, зависящей от $c_0$, справедлива оценка

$$w \ll b |m|^{-\frac{c''}{\eta(m)}}, \tag{42}$$

где функция $\eta(m)$ определена равенством (27).

5°. С другой стороны, в силу ключевой леммы ДЭМ (предложение 5) имеем

$$w \gg b \cdot |m|^{-\frac{1}{\eta(m)}}. \tag{43}$$

Но при достаточно большом значении $c_0$, а следовательно, при достаточно большом значении $c'$ оценки (42) и (43) противоречат друг другу. Итак, мы привели к противоречию предположение п. 2°.

Следуя [5], с учетом асимптотического соотношения (30) получаем

$$r(m;Q,u) = r_1(Q^{(j)},T(m)) = \frac{T(m)}{\sigma_0(q)} \cdot \{1 + O(\gamma(m))\},$$

где

$$r_1(Q^{(j)},T') = \#\{T_{\beta 1} |\, 1 \le \beta \le T',\ T'_{\beta 1}/Q^{(j)}\}$$

(здесь # — знак мощности множества). Теорема 1 доказана.

## 4. Доказательство теоремы 2

Пусть $\Phi(m) = \{\varphi_1, \ldots, \varphi_{T(m)}\}$ — полная система целочисленных собственно примитивных бинарных квадратичных форм определителя $m$, так что

$$\varphi = (a,b,c) = ax^2 + 2bxy + cy^2 \in \Phi(m),$$

если $a$, $b$, $c \in \mathbb{Z}$, НОД$(a,2b,c) = 1$, $ac - b^2 = m$ и выполнены условия приведения (12) или (13).

Как и в [5], пусть $\Phi(m,q) \subset \Phi(m)$ — совокупность тех форм $\varphi = (a,b,c) \in \Phi(m)$, первые коэффициенты которых делятся на $q$, т. е.

$$a \equiv 0 \,(\operatorname{mod} q). \tag{44}$$

Из (44) следует, что

$$b^2 + m \equiv 0 \,(\operatorname{mod} q). \tag{45}$$

Поэтому если $u_1, \ldots, u_{2^\nu}$ — полная система решений $(\operatorname{mod} q)$ сравнения

$$x^2 + m \equiv 0 (\operatorname{mod} q),$$

где $\nu = \nu(q)$ — число различных простых делителей числа $q$ и $(a,b,c) \in \Phi(m,q)$, то в силу (45) имеем $b = u_{i_0} (\operatorname{mod} q)$ для некоторого $i_0$, $1 \le i_0 \le 2^\nu$. Тем самым множество $\Phi(m,q)$ разбивается на $2^\nu$ попарно не пересекающихся множеств $\Phi(m,q,u_i)$, где $\Phi(m,q,u_i)$ — множество тех $\varphi = (a,b,c) \in \Phi(m,q)$, для которых

$$b \equiv u_i \,(\operatorname{mod} q) \quad (i = 1, \ldots, 2^\nu). \tag{46}$$

Повторяя матричные рассуждения, связанные с теоремой 1, получаем, что

$$u_i + L_\alpha / Q, \tag{47}$$

где

$$Q = \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}, \quad L_\alpha = \begin{pmatrix} b_\alpha & a_\alpha \\ c_\alpha & -b_\alpha \end{pmatrix}$$

— вектор-матрица, соответствующая квадратичной форме $\varphi_\alpha = (a_\alpha, b_\alpha, c_\alpha) \in \Phi(m,q,u_i)$. Обратно, если имеет место (47), то выполняются условия (44) и (46), так что

$$\varphi_\alpha = (a_\alpha, b_\alpha, c_\alpha) \in \Phi(m,q,u_i).$$

Поэтому

$$\#\Phi(m,q,u_i) = r(m;Q,u_i) \quad (i = 1,\dots,2^\nu). \tag{48}$$

Наконец, из (48) в силу теоремы 1 и предложения 1 получаем

$$T_1(m,q) = \#\Phi(m,q) = \sum_{i=1}^{2^\nu} \#\Phi(m,q,u_i)$$
$$= \sum_{i=1}^{2^\nu} r(m;Q,u_i) = \frac{2^{\nu(q)}}{q\prod\limits_{p|q}\left(1+\frac{1}{p}\right)} T(m)\{1+O(\gamma(m))\}.$$

Теорема 2 доказана.

## 5. Асимптотические формулы для $T_1(m,q)$ на основе гипотез $(\mathfrak{K})$ и $(\mathscr{G})$

Для получения с помощью ДЭМ асимптотических формул для $T_1(m,q)$ с остаточными членами, зависящими от элементарных функций, придется использовать гипотезы $(\mathfrak{K})$ и $(\mathscr{G})$ о поведении $L$-функции Дирихле.

Пусть в условиях теоремы 2 выполнена гипотеза $(\mathfrak{K})$. Тогда теорема 3 следует из теоремы 2 и ключевой леммы (предложение 5), если возьмем $\eta(m) \ll \log\log|m|$, откуда

$$\gamma(m) = \sqrt{\frac{\log \eta(m)}{\eta(m)}} \ll \sqrt{\frac{\log\log\log|m|}{\log\log|m|}}.$$

Если же в условиях теоремы 2 выполнена гипотеза $(\mathscr{G})$, то, положив $\eta(m) = \sqrt{\log|m|}\log\log|m|$, имеем $\gamma(m) \ll \frac{1}{(\log|m|)^{\frac{1}{4}}}$, т. е. в этом случае мы получаем теорему 4.

В заключение отметим, что безусловные оценки остаточных членов (если не считать оценки (8), где $\gamma(m)$ удовлетворяет (7)), до сих пор не установлены, хотя в работе Дьюка [18] получена безусловная оценка остаточного члена в асимптотической формуле для распределения приведенных бинарных квадратичных форм по областям на соответствующих гиперболоидах.

## *ЛИТЕРАТУРА*

1. *Линник Ю. В.* Эргодические свойства алгебраических полей. Л.: Изд-во Ленингр. ун-та, 1967.
2. *Malyschev A. V.* Yu. V. Linnik's ergodic method in number theory // Acta Arithm. 1975. Bd 27. S. 555–598.
3. *Скубенко Б. Ф.* Асимптотическое распределение целых точек на однополостном гиперболоиде и эргодические теоремы // Изв. АН СССР. Сер. мат. 1962. Т. 26, № 5. С. 721–752.
4. *Малышев А. В., Пачев У. М.* О числе классов целочисленных положительных бинарных квадратичных форм, арифметический минимум которых делится на заданное число // Алгебра и теория чисел. Нальчик, 1979. № 4. С. 53–67.
5. *Пачев У. М.* О числе приведенных целочисленных неопределенных бинарных квадратичных форм с условием делимости первых коэффициентов // Чебышевский сб. Тула, 2003. Т. 4. № 3. С. 92–105.
6. *Прахар К.* Распределение простых чисел. М.: Мир, 1967.
7. *Siegel C. L.* Über die Classenzahl quadratischer Zahlkorper // Acta Arithm. 1935. Bd 1, H. 1. S. 83–86.
8. *Landau E.* Über die Klassenzahl imaginarquadratischer Zahlkorper // Nach. Gesellsch. Wissensch. Gottingen. Math.-Phys. Ki. 1918. S. 285–296.

**9.** *Малышев А. В., Пачев У. М.* Об арифметике матриц второго порядка // Зап. науч. семинаров ЛОМИ. 1980. Т. 93. С. 41–86.

**10.** *Венков Б. А.* Элементарная теория чисел. М.; Л.: ОНТИ, 1937.

**11.** *Пачев У. М.* Об асимптотике с остаточным членом для числа бинарных квадратичных форм с условием делимости первых коэффициентов // Тез. докл. VI Междунар. конф. «Алгебра и теория чисел: современные проблемы и приложения», посвященной 100-летию Н. Г. Чудакова. Саратов, 13–17 сентября 2004 г. С. 90–91.

**12.** *Newman M.* Integral matrices. New York; London: Acad. Press, 1972.

**13.** *Малышев А. В., Нгуен Нгор Гой.* О распределении целых точек на некоторых однополостных гиперболоидах // Зап. науч. семинаров ЛОМИ. 1983. Т. 121. С. 83–93.

**14.** *Малышев А. В., Широков Б. М.* Новое доказательство ключевой леммы дискретного эргодического метода для вектор-матриц второго порядка // Вестн. Ленингр. ун-та. 1991. Т. 2, № 8. С. 34–40.

**15.** *Пачев У. М.* Об уточнении ключевой леммы дискретного эргодического метода для вектор-матриц второго порядка // Чебышевский сб. Тула, 2004. Т. 5, № 2. С. 89–97.

**16.** *Малышев А. В.* Асимптотический закон для представления чисел некоторыми положительными тернарными квадратичными формами // Докл. АН СССР. 1953. Т. 93, № 5. С. 771–774.

**17.** *Малышев А. В., Пачев У. М.* О представлении целых чисел положительными тернарными квадратичными формами (новый вариант дискретного эргодического метода) // Зап. науч. семинаров ЛОМИ. 1979. Т. 82. С. 33–87.

**18.** *Duke W.* Hyperbolic distribution problems and half-integral weight Maas forms // Invent. Math. 1988. V. 92. P. 78–90.


*Статья поступила 20 сентября 2005 г.*

*Пачев Урусби Мухамедович*
*Кабардино-Балкарский гос. университет, математический факультет,*
*кафедра геометрии и высшей алгебры,*
*ул. Чернышевского, 173, Нальчик 360004*
urusbi@rambler.ru