

# ЧЕБЫШЕВСКИЙ СБОРНИК

Том 14 Выпуск 2 (2013)

---

УДК 511.512

## О РАСПРЕДЕЛЕНИИ ПРИВЕДЕННЫХ НЕОПРЕДЕЛЕННЫХ БИНАРНЫХ КВАДРАТИЧНЫХ ФОРМ С УСЛОВИЕМ ДЕЛИМОСТИ ПЕРВЫХ КОЭФФИЦИЕНТОВ ПО КЛАССАМ ВЫЧЕТОВ

У. М. Пачев (г. Нальчик)

### Аннотация

Обобщены некоторые результаты Б.Ф. Скубенко и автора об асимптотическом распределении целочисленных приведенных неопределенных бинарных квадратичных форм, получаемые с помощью дискретного эргодического метода.

*Ключевые слова:* асимптотическое распределение, бинарная квадратичная форма, вектор-матрица второго порядка, дискретный эргодический метод.

## ON THE DISTRIBUTION OF REDUCED INDEFINITE BINARY QUADRATIC FORMS WITH THE CONDITION OF FIRST COEFFICIENTS DIVISIBILITY IN RESIDUE CLASSES

U. M. Pachev (Nalchik)

### Abstract

In this paper we generalize some B.F. Skubenko and autor results on the asymptotic distribution of integer indefinite binary quadratic forms obtained with the discrete ergodic method.

*Keywords:* asymptotic distribution of binary quadratic form, vector-matrix of the second order discrete ergodic method.

# 1. Введение. Формулировки результатов

В этой работе мы продолжаем исследование по асимптотическому подсчету числа приведенных бинарных квадратичных форм с условием делимости первых квадратичных коэффициентов, начатые Ю. В. Линником [1] в связи с приложениями разработанного им дискретного эргодического метода (далее ДЭМ) к аналитической арифметике неопределенных тернарных квадратичных форм. Исследования Ю. В. Линника были продолжены Б. Ф. Скубенко, А. В. Малышевым и автором в ряде работ (см. [2], [3]).

Обобщая результаты работ [2], [3] на случай распределения указанных форм по классам вычетов по заданному модулю, мы с помощью ДЭМ доказываем следующие предложения (обзор этого метода и результатов его применения см. [4], [5]), при этом результаты из [6] мы переносим на случай неопределенных бинарных квадратичных форм.

**ТЕОРЕМА 1.** . Пусть  $t < 0$  – целое число;  $\sqrt{-t} \notin Q$ ;  $q$  и  $g$  – нечетные числа, взаимно простые с  $t$ ;  $u$  – целое число, для которого

$$u^2 + t \equiv 0 \pmod{q} \quad (1)$$

Для произвольной примитивной матрицы  $Q$  второго порядка нормы  $q$  обозначим через  $r(t; g; Q, u)$  число приведенных собственно примитивных вектор-матриц  $L$  нормы  $t < 0$ , для которых

$$L \equiv L_0 \pmod{g}, \quad Q \setminus u + L$$

где  $L_0$  – целая вектор-матрица с условием  $N(L_0) \equiv t \pmod{g}$ .

Тогда при  $t \rightarrow -\infty$

$$r(t; g; Q, u) \sim \frac{T(t)}{\sigma_0(q)\rho(g, t)}, \quad (2)$$

где  $\sim$  – знак асимптотической эквивалентности;  $T(t)$  – число целочисленных приведенных неопределенных бинарных квадратичных форм определителя  $t$ ;  $\sigma_0(q)$  – число неассоциированных слева примитивных матриц нормы  $q$ ;  $\rho(g, t)$  – число решений сравнения

$$x_1x_3 - x_2^2 \equiv t \pmod{g}.$$

На теорему 1, имеющую самостоятельный интерес, опирается доказательство следующего результата.

**ТЕОРЕМА 2.** . Пусть  $t < 0$  – целое число;  $\sqrt{-t} \notin Q$ ;  $q > 0$  и  $g$  – целые нечетные числа, взаимно простые с  $t$  и символ Лежандра  $\left(\frac{-t}{p}\right) = 1$  для всех простых  $p \mid q$ . Обозначим через  $T_1(t; g; q)$  число приведенных неопределенных

собственно примитивных бинарных квадратичных форм определителя  $m$ , коэффициенты которых лежат в заданном классе вычетов по модулю  $g$ , причем первые их коэффициенты делятся на  $q$ .

Тогда при  $m \rightarrow -\infty$

$$T_1(m; g; q) \sim \frac{2^{\nu(q)}}{\sigma_0(q)\rho(g, m)} T(m),$$

где  $\nu(q)$  – число различных простых делителей числа  $q$ .

Теорема 2 обобщает результаты [2], [3], относящиеся только к случаю  $g = 1$ .

## 2. Сведения из аналитической арифметики матриц второго порядка и ключевая лемма ДЭМ

При изучении с помощью ДЭМ вопроса о распределении целочисленных приведенных бинарных квадратичных форм (или что то же самое, соответствующих им целых точек на гиперблоидах) наиболее удобным вспомогательным аппаратом является аналитическая арифметика матриц второго порядка (см. [7]). Поэтому приведем необходимые для дальнейшего изложения определения и предложения из арифметики целых матриц второго порядка.

Наряду с этим будем рассматривать также целочисленную бинарную квадратичную форму

$$\varphi = \varphi(x, y) = ax^2 + 2bxy + cy^2 \quad (3)$$

с целыми коэффициентами  $a, b, c \in \mathbb{Z}$ ; при этом  $d = d(\varphi) = ac - b^2$  – ее определитель. Форму (3) будем коротко записывать в виде  $\varphi = (a, b, c)$ , учитывая при этом, что такая запись более соответствует тому, что в ДЭМ форме (3) сопоставляется точка  $(a, b, c) \in \mathbb{Z}^3$  на поверхности простейшего гиперблоида  $ac - b^2 = d$ .

Говорим, что форма  $\varphi$  является неопределенной, если ее определитель  $d(\varphi) < 0$ .

Неопределенную форму (3) определителя  $d$  называем приведенной, если для ее коэффициентов выполняются неравенства

$$0 < b < \sqrt{-d}, \quad \sqrt{-d} - b < |a| < \sqrt{-d} + b.$$

Две целочисленные формы  $\varphi$  и  $\varphi'$  называются эквивалентными, если каждая из них переходит в другую целочисленной линейной подстановкой переменных. Отношение эквивалентности разбивает формы заданного определителя на классы форм, число которых конечно.

В случае неопределенных форм имеется (см. [8], гл.IV) конечное число приведенных форм

$$\varphi_1, \varphi_2, \dots, \varphi_{2n}, \quad \varphi_i = \varphi_{i+2nk, k \in Z}, \quad (4)$$

эквивалентных какой-нибудь форме  $\varphi$ ; они образуют цикл (период) приведенных форм; при этом элементы цикла (4) упорядочены так, что  $\varphi_i$  и  $\varphi_{i+1}$  – соседние формы (см. [8], гл.IV).

Число этих циклов равно числу классов неопределенных бинарных квадратичных форм заданного определителя  $d < 0$ .

Приведем теперь необходимые сведения из арифметики матриц второго порядка, используемые в ДЭМ.

Мы рассматриваем квадратные целые матрицы второго порядка над кольцом целых чисел

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \quad a_{ij} \in Z \quad (i, j = 1, 2). \quad (5)$$

Нормой  $N(A)$  матрицы  $A$  называем  $\det A$ , т.е.  $N(A) = \det A$  (в тех случаях, когда  $N(A) < 0$ , в качестве нормы матрицы  $A$  в вопросах делимости матриц берут  $|N(A)|$ ).

Следом матрицы  $A$  называем число  $Sp(A) = a_{11} + a_{22}$ . Если  $Sp(A) = 0$ , то  $A$  называем вектор-матрицей.

Мы будем пользоваться тем, что любую матрицу  $A$  можно представить единственным образом в виде  $A = l + L$ , где  $l = \frac{1}{2}Sp(A)$  отождествляется со скалярной матрицей  $lE$ , а  $L$  – вектор-матрица. В используемом нами ДЭМ вектор-матрица

$$L = \begin{pmatrix} b - a \\ c - a \end{pmatrix}$$

взаимно однозначно сопоставляется с бинарной квадратичной формой  $\varphi = ax^2 + 2bxy + cy^2$ . В связи с этим можно говорить о положительной или неопределенной вектор-матрице, а также о приведенной вектор-матрице в понятном смысле.

Говорим, что матрица (5) примитивна, если  $\text{НОД}(a_{11}, a_{12}, a_{21}, a_{22}) = 1$ . Число  $t = t(A) = \text{НОД}(a_{11}, a_{12}, a_{21}, a_{22})$  называется числовым делителем матрицы  $A$ . Если  $t(A) = 1$  то матрица  $A$  называется примитивной. Если для некоторого целого числа  $g > 0$  делитель  $t(A)$  взаимно прост с  $g$ , то матрица  $A$  называется примитивной по модулю  $g$ .

В кольце  $M_2(Z)$  определяем ассоциированность матриц слева и справа. Матрицу  $A_1$  называем ассоциированной с матрицей  $A \in M_2(Z)$  слева, если найдется  $U \in M_2(Z)$  с нормой  $N(U) = \pm 1$ , что  $A_1 = UA$  (аналогично определяется ассоциированность матриц справа).

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

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

**ПРЕДЛОЖЕНИЕ 1.** . Пусть  $A$  – целая примитивная матрица из кольца  $M_2(Z)$  нормы  $N(A) = a \neq 0$  и пусть  $a = bc$ , где  $b, c$  – целые числа. Тогда найдутся такие матрицы  $B, C \in M_2(Z)$ , что  $A = BC$ ,  $N(B) = b$ ,  $N(C) = c$ . При этом, если  $A = B_1C_1$ , где  $B_1, C_1 \in M_2(Z)$ ,  $N(B_1) = b$ ,  $N(C_1) = c$ , то  $B_1$  ассоциирована справа с  $B$ .

Доказательство см. в [7], §2.

Предложение 1 используется в разложениях матриц и в преобразованиях подобия вектор-матриц.

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

Как и в [1], [9], введем в рассмотрение матрицы

$$E^{(0)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad E^{(i)} = \begin{pmatrix} k_1 & -1 \\ 1 & 0 \end{pmatrix}^{-1} \cdots \begin{pmatrix} k_i & -1 \\ 1 & 0 \end{pmatrix}^{-1},$$

$i = 1, \dots, 2n$ ,  $k_1, \dots, k_i$  – целые числа, так что

$$E^{(i)-1} L E^{(i)} = L_i,$$

где  $2n$  – длина цикла вектор-матрицы  $L$ .

Для целых вектор-матриц  $L$  и  $L'$  найдется (см. [7]) целая матрица  $A$  с условием  $A^{-1}LA = L'$  (такое свойство относится к теории поворотов вектор-матриц).

Обозначим  $E_L = t - uL$ , где  $t, u$  – наименьшее целое положительное решение уравнения Пелля

$$t^2 + mu^2 = 1, \quad m = N(L).$$

Следуя [9], определим матрицу  $\varepsilon_L(E_n)^q E^{(r)}$ , где  $k \in Z$ ,  $k = 2nq + r$ ,  $0 \leq r < 2n$ . Тогда

$$A_k^{-1} L_k A_k = L', \quad A_k = \mathcal{E}_k A \quad (k = 0, \pm 1, \pm 2, \dots). \quad (6)$$

где  $\mathcal{E}_k$  – целочисленная унимодулярная матрица второго порядка.

Среди матриц  $A_k = \mathcal{E}_k A$ , ассоциированных слева с матрицей  $A$  и переводящих одну из вектор-матриц  $L_k$  цикла  $\{L = L_1, L_2, \dots, L_{2n}\}$  в вектор-матрицу  $L'$  по формуле (6), можно подобрать матрицу, играющую особую роль при применении ДЭМ к неопределенным бинарным формам (существование такой матрицы гарантирует следующее предложение).

**ПРЕДЛОЖЕНИЕ 2.** . Если  $L$  и  $L'$  – приведенные неопределенные вектор-матрицы и  $A$  – целая матрица с условием  $A^{-1}LA = L'$ ,  $N(A) > 0$ , то найдется такая матрица  $A' = \mathcal{E}A = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}$ , ассоциированная слева к  $A$ , для которой вектор-матрица  $L'' = (A')^{-1}LA' = \mathcal{E}^{-1}L'\mathcal{E}$  приведена, причем  $\alpha'\beta'\gamma'\delta' < 0$ , где  $\mathcal{E}$  – целочисленная унимодулярная матрица.

Доказательство этого предложения см. в [2] и [1], лемма 6.2.3.

Матрицу  $A$  из предложения 2 будем называть, следуя [9], полупримальной (а по терминологии [2] – удобной).

**ПРЕДЛОЖЕНИЕ 3.** (ключевая лемма ДЭМ для вектор-матриц). Пусть  $L_1, L_2, \dots, L_n, r = r(n)$  – все приведенные целые неопределенные вектор-матрицы второго порядка нормы  $m < 0$ . Пусть среди матричных равенств  $l + L_i = B_i U_i N(B_i)$  ( $i = 1, \dots, r$ ) произвольно выбрано  $r' \gg |m|^{\frac{1}{2}-\varepsilon}$  равенств (для любого  $\varepsilon > 0$ ), где  $l^2 + m \equiv 0 \pmod{q^s}$ ,  $s = \left\lceil \tau \frac{\log |m|}{\log q} \right\rceil$ ,  $0 < \tau < \frac{1}{8}$ ;  $B_i$  – целая примитивная матрица;  $U_i$  – целая матрица.

Тогда существует постоянная  $c > 0$ , зависящая от  $\varepsilon$ , такая, что количество  $w$  попарно неассоциированных справа матриц  $B_i$ , которые встречаются в этих  $r'$  равенствах, при  $m \rightarrow \infty$  удовлетворяет неравенству

$$w \geq c|m|^{\tau-\varepsilon}.$$

Доказательство этого предложения см. в [10], где изложение ведется сразу для обоих случаев: двуполостного и однополостного гиперблоидов.

Следующее предложение будет использовано в доказательстве теоремы 1.

**ПРЕДЛОЖЕНИЕ 4.** (о делимости матриц большой нормы). Пусть  $q > 1$  – нечетное число;  $g$  – нечетное число, взаимно простое с  $m$ ;  $t \geq 1$  – целое число;  $B$  – целая матрица с условием

$$N(B) \equiv q^t \pmod{g}.$$

Пусть  $A_1$  и  $A_2$  – примитивные матрицы нормы  $q$ . Через  $\sigma_0(q^t; g, B; A_1, A_2)$  обозначим число целых матриц  $M \in M_2(Z)$  нормы  $q^t$ , для которых  $M \equiv B \pmod{g}, A_1 \setminus M, M \setminus A_2$ .

Тогда при  $t \rightarrow -\infty$

$$\sigma_0(q^t; g, B; A_1, A_2) \sim \frac{\sigma_0(q^t)}{v(g, q^t)(\sigma_0(q))^2},$$

где  $v(g, q^t)$  – число различных по модулю  $g$ , примитивных по модулю  $g$  матриц  $B$ , удовлетворяющих сравнению

$$N(B) \equiv m \pmod{g}.$$

Доказательство см. в [7], где оно дается в более общем виде и с остаточным членом.

### 3. Доказательство теоремы 1

1°. Фиксируем число  $\tau$  из ключевой леммы,  $0 < \tau < \frac{1}{8}$ , и рассмотрим целые числа

$$s_1 = \left\lceil \frac{\tau \log m}{\log q} \right\rceil, \quad s = \delta s_1,$$

где  $\delta$  – некоторое целое число, выбираемое в дальнейшем.

Подберем целое число  $l$  так, чтобы

$$l \equiv u \pmod{q}, \quad l^2 + m \equiv 0 \pmod{q^s}, \quad \text{НОД} \left( \frac{l^2 + m}{q^s}, q \right) = 1. \quad (7)$$

Возможность такого выбора следует из условия (1). В силу (7) для всех приведенных собственно примитивных неопределенных вектор-матриц

$$L_1, \dots, L_T, \quad T = T(m)$$

нормы  $m$  имеем

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

Но тогда, по предложению 1, имеем следующие матричные разложения

$$l + L_i = B_i X_i \quad (i = 1, \dots, T), \quad (8)$$

где  $B_i = Q_{i1} \cdot \dots \cdot Q_{is}$  – примитивные матрицы нормы  $q^s$ ;  $Q_{ij}$  – примитивные матрицы нормы  $q$ ;  $X_i$  – целые матрицы. Разложения (8) соответствуют рассмотрению делимости матриц слева и поворотов вида  $A^{-1}L_iA$ . Следуя [1], [2], в разложениях (8), в силу предложения 2, будем выбирать матрицы  $L_i$  так, чтобы  $T_{ij}$  были полупримарными и  $T_{ij}^{-1}L_iT_{ij}$  – приведенными вектор-матрицами нормы  $m < 0$ . Будем считать что в равенствах (8) уже произведен указанный выбор матриц  $T_{ij}$  для всех  $i = 1, \dots, T$ .

Из разложений (8), считая, что в них выполнены указанные требования произвольным образом выбираем  $T' > T(m) \cdot |m|^{-\eta}$  равенств

$$l + L_\alpha = B_\alpha X_\alpha \quad (i = 1, \dots, T'),$$

где  $B_\alpha = Q_{\alpha 1} \cdot \dots \cdot Q_{\alpha s}$ ;  $\eta$  – сколь угодно малое положительное число.

2°. Пусть  $L_0^{(1)}, \dots, L_0^{(\rho(g(m)))}$  – представители всех классов вычетов целых вектор-матриц  $(\text{mod } g)$  с условием

$$N \left( L_0^{(j)} \right) \equiv m \pmod{g} \quad (j = 1, \dots, \rho(g, m)).$$

Для данного целого положительного числа  $t$  сопоставим каждому классу вычетов  $L_0^{(j)} \pmod{g}$  совокупность  $\gamma_j = \gamma_{L_0^{(j)}}^{(t)}$  классов целых матриц  $S \pmod{g}$ , для которых

$$L_0^{(j)} S \equiv S L_0 \pmod{g}, \quad N(S) \equiv q^t \pmod{g}, \quad (9)$$

где  $L = \begin{pmatrix} b_2 & b_1 \\ b_3 & b_2 \end{pmatrix}$ .

В каждой совокупности  $L_{L_0^{(j)}}^{(t)}$  ( $j = 1, \dots, \rho(g, m)$ ) имеется одинаковое число классов вычетов  $S \pmod{g}$ , а именно

$$\#\gamma_{L_0^{(j)}}^{(t)} = g \prod_{p|g} \left( 1 - \frac{\left(\frac{-m}{p}\right)}{p} \right) \quad (10)$$

(см. [11], ч.2, гл.7).

Ввиду соотношений (9) и (10) приводимые рассуждения проходят и в случае НОД  $(q, g) \neq 1$ . Разобьем теперь множество  $T(m)$  всех собственно примитивных приведенных вектор-матриц  $L$  нормы  $m$  на  $\rho(g, m)$  множеств

$$Z_j = \{L_1^{(j)}, \dots, L_{r_j}^{(j)}\} \quad (j = 1, \dots, \rho(g, m)),$$

относя к  $Z_j$  все те  $L$ , для которых  $L \equiv L_0^{(j)} \pmod{g}$ . Ясно, что

$$\sum_{j=1}^{\rho(g, m)} r_j = T(m).$$

Соответственно, матричные равенства (8), отвечающие всем  $L_\alpha$  можно сгруппировать следующим образом

$$l + L_i^{(j)} = B_i^{(j)} X_i^{(j)} \quad (j = 1, \dots, \rho(g, m), i = 1, \dots, r_j), \quad (11)$$

где  $L_i^{(j)} \in Z_j$ ,  $B_i^{(j)}$ ,  $X_i^{(j)}$  – целые примитивные матрицы, причем

$$N(B_i^{(j)}) = q^s, \quad \text{НОД}\left(N(B_i^{(j)}), N(X_i^{(j)})\right) = 1, \quad B_i^{(j)} = Q_{i1}^{(j)}, \dots, Q_{is}^{(j)}.$$

**З°.** Дальнейшее доказательство базируется на следующем утверждении, равносильном теореме перемешивания в ДЭМ.

**ПРЕДЛОЖЕНИЕ 5. (R).** Пусть  $v_{j,t}$  ( $1 \leq t_0 \leq s-1$ ) – число индексов  $i$  ( $i = 1, \dots, r_j$ ) в равенствах (11) с условиями:

$$B_{it}^{(j)} = Q_{i1}^{(j)} \cdot \dots \cdot Q_{it}^{(j)} \in \gamma_j^{(t)}, \quad Q \setminus Q_{i,t+1}^{(j)},$$

где  $Q$  – любая матрица из полного набора неассоциированных слева матриц нормы  $q$ . Тогда найдется такой индекс  $t_0$ ,  $1 \leq t_0 \leq s-1$ , что

$$\tau_j < \frac{T(m)}{\log |m|} \quad (12)$$

или

$$\gamma_{j,t} \sim \frac{1}{\rho(g, m)} \cdot \frac{1}{\sigma_0(q)} r_j, \quad m \rightarrow -\infty, \quad (13)$$

где  $j = 1, \dots, \rho(g, m)$ . Постоянные, входящие в асимптотическую формулу (13), зависят только от  $q$ ,  $g$  и не зависят от  $m$ .

4°. Предложение (R) доказываем от противного. Обозначим для краткости  $\beta = \frac{1}{\rho(g,m)} \cdot \frac{1}{\sigma_0(q)}$ . Если (R) не имеет места, т.е. не выполняются (12) и (13), то для некоторого числа  $\gamma > 0$  найдется бесконечная последовательность чисел  $m$ , удовлетворяющих условиям теоремы 1, так что для каждого  $m$  имеется индекс  $j_0$ , для которого

$$r_{j_0} \geq \frac{T(m)}{\log |m|}; \quad |\gamma_{j_0,t} - \beta r_{j_0}| \geq \gamma \beta r_{j_0} \quad (t = 1, \dots, s-1). \quad (14)$$

Неравенства (14), в частности, справедливы для  $t = \delta, 2\delta, \dots, s_1\delta = s-1$ , причем для  $s_2 \geq \frac{1}{2}s_1$  индексов выполняются неравенства

$$\gamma_{j_0,t} \leq (1 - \gamma)\beta r_{j_0}$$

или

$$\gamma_{j_0,t} \geq (1 + \gamma)\beta r_{j_0}.$$

Из равенств (18) выбираем  $r' = r'_{j_0}$  равенств

$$l + L_i^{(j_0)} = B_i^{(j_0)} X_i^{(j_0)} \quad (i = 1, \dots, r'_{j_0}), \quad (15)$$

для которых

$$\#\left\{t_n \mid 1 \leq n \leq s_2, B_{it_n}^{(j_0)} \in \gamma_{j_0}^{(t_n)}, Q \setminus Q_{i,t_n+1}^{(j_0)}\right\} < \left(1 - \frac{\gamma}{2}\right) \beta s_2.$$

Как и в случае положительных вектор-матриц, доказывается, что

$$r' > \varkappa_\varepsilon |m|^{\frac{1}{2}-\varepsilon},$$

где постоянная  $\varkappa_\varepsilon > 0$  зависит только от  $q, g$  и  $\varepsilon$ .

5°. Пусть  $w'$  – число неассоциированных справа примитивных матриц  $B_i^{(j_0)}$  нормы  $q^s$  в равенствах (15), и значит

$$w' \leq w, \quad (16)$$

где  $w$  – общее число неассоциированных справа примитивных матриц  $B^{(i)} = Q_1^{(i)} \cdot \dots \cdot Q_s^{(i)}$  нормы  $q^s$ , ( $i = 1, \dots, w$ );  $Q_j^{(i)}$ , ( $j = 1, \dots, s$ ) – примитивные матрицы нормы  $q$ , причем для каждого фиксированного индекса  $i = 1, \dots, w$

$$\#\left\{t_n \mid 1 \leq n \leq s_2, B_{t_n}^{(i)} \in \gamma_{j_0}^{(t_n)}, Q \setminus Q_{t_n+1}^{(i)}\right\} < \left(1 - \frac{\gamma}{2}\right) \beta s_2, \quad (17)$$

здесь  $B_{t_n}^{(i)} = Q_1^{(i)} \cdot \dots \cdot Q_{t_n}^{(i)}$ .

В силу предложения 4 и неравенства (17) получаем

$$w \leq \sigma_0(q^s)(1 + \varepsilon)^{s_2} \sum_{v \leq \left(1 - \frac{\gamma}{2}\right) \beta s_2} \frac{s_2!}{v!(s_2 - v)!} \beta^v (1 - \beta)^{s_2 - v}.$$

Рассуждая как и в [3], т.е. произведя оценку сверху правой части неравенства (27), получим, что

$$w \ll |m|^{\tau-\theta}, \quad (18)$$

где  $\theta = \theta(q) > 0$  – некоторая постоянная, зависящая только от  $q$ .

С другой стороны, в силу ключевой леммы, для любого  $\varepsilon > 0$

$$w \gg |m|^{\tau-\varepsilon}. \quad (19)$$

Полагая  $\varepsilon = \frac{\theta}{2}$ , получаем, что ввиду (9) при достаточно больших  $|m|$  оценки (18) и (19) противоречат друг другу, что и доказывает предложение (R).

Применяя теперь предложение (R) к области приведения  $\Delta_m$  найдем постоянную  $\varkappa > 0$  (зависящую от только от  $q, g$ ) и  $t_0$  ( $1 \leq t_0 \leq s$ ) такие, что при достаточно больших  $|m|$  для любого  $1 \leq j \leq \rho(g, m)$  выполняются неравенства:

$$r_j < \frac{T(m)}{\log |m|}$$

или

$$\gamma_{j,t_0} < (1 + \varkappa_1) \frac{1}{\rho(g, m)} \cdot \frac{1}{\sigma_0(q)} r_j.$$

Тогда

$$\begin{aligned} r(m; g; Q, u) &\leq \sum_{j=1}^{\rho(g, m)} r_{j,t_0} < \sum_{j=1}^{\rho(g, m)} \left\{ (1 + \varkappa_1) \frac{1}{\rho(g, m) \sigma_0(q)} r_j + \frac{T(m)}{\log |m|} \right\} < \\ &< (1 + \varkappa^+) \frac{1}{\rho(g, m)} \cdot \frac{1}{\sigma_0(q)} T(m) \end{aligned}$$

при некоторой постоянной  $\varkappa^+ > 0$ , зависящей от  $\varkappa_1$ .

Аналогично устанавливается, что

$$r(m; g; Q, u) > (1 - \varkappa^-) \frac{1}{\rho(g, m)} \cdot \frac{1}{\sigma_0(q)} T(m).$$

Обе эти оценки при  $|m| \rightarrow \infty$  равносильны асимптотической формуле (2) и теорема 1 доказана.

## 4. Доказательство теоремы 2

Пусть  $\Phi(m) = \{\varphi_1, \dots, \varphi_{T(m)}\}$  – множество всех приведенных собственно примитивных неопределенных бинарных квадратичных форм определителя  $m < 0$ , так что для

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

имеем

$$a, b, c \in Z, \quad \text{НОД}(a, 2b, c) = 1,$$

и выполняются условия приведенности

$$0 \leq b \leq \sqrt{-m}, \quad \sqrt{-m} - b < |a| < \sqrt{-m} + b.$$

Обозначим через  $\Phi_g(m, q)$  совокупность форм  $\varphi(a, b, c) \in \Phi(m)$ , для которых

$$a \equiv 0 \pmod{q} \tag{20}$$

и

$$(a, b, c) \equiv (a_0, b_0, c_0) \pmod{q}, \tag{21}$$

где  $a_0, b_0, c_0$  – некоторые фиксированные целые числа;  $\text{НОД}(g, 2qm) = 1$ .

Из (20) следует, что

$$b^2 + m \equiv 0 \pmod{q}. \tag{22}$$

Тогда сравнение  $x^2 + m \equiv 0 \pmod{q}$  имеет  $2^\nu$  решений, где  $\nu = \nu(q)$  – число различных простых делителей числа  $q$ . Поэтому, если  $u_1, \dots, u_{2^\nu}$  – полная система решений  $\pmod{q}$  этого сравнения и верно (21), то в силу (22) имеем, что

$$b \equiv -u_{i_0} \pmod{q} \tag{23}$$

либо

$$b \equiv u_{i_0} \pmod{q},$$

где  $1 \leq i_0 \leq 2^\nu$ .

Тем самым, множество  $\Phi_g(m, q)$  разбивается на попарно непересекающиеся множества  $\Phi_g(m, q, u_i)$ , где каждое  $\Phi_g(m, q, u_i)$  есть множество тех  $\varphi = (a, b, c) \in \Phi(m)$ , которые удовлетворяют (23).

Берем теперь в теореме 1 примитивную матрицу вида  $\begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}$ . Тогда, в силу (19) и (33), имеем

$$Q \setminus (u_i + L). \tag{24}$$

Обратно, если имеет место (24), то выполняются (20), (21) и (22). Поэтому

$$\#\Phi_g(m, q, u_i) = r(m; g; Q, u_i). \tag{25}$$

Тогда, учитывая, что  $T_1(m; g; q) = \#\Phi_g(m; q)$ , в силу теоремы 1 и равенства (25) получаем

$$T_1(m; g; q) = \sum_{i=1}^{2^\nu} \#\Phi_g(m; q, u_i) = \sum_{i=1}^{2^\nu} r(m; g; q, u_i) \sim \frac{2^\nu}{\sigma_0(q)} \cdot \frac{1}{\rho(g, m)} T(m).$$

Теорема 2 доказана.

**СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ**

1. Линник Ю. В. Эргодические свойства алгебраических полей. Л.: Изд-во Ленингр. ун-та, 1967.
2. Скубенко Б. Ф. Асимптотическое распределение целых точек на однополостных гиперблоидах и эргодические теоремы // Известия АН СССР. Сер. Математика. 1962. Т. 26, № 5. С. 721—752.
3. Пачев У. М. О числе приведенных целочисленных неопределенных бинарных квадратичных форм с условием делимости первых коэффициентов // Чебышевский сборник. 2003. Т. 4, № 3(7). С. 92—105.
4. Линник Ю. В. Избранные труды. Теория чисел. Эргодический метод и L-функции. Л.: Наука, 1979.
5. Пачев У. М. Обзор исследований по дискретному эргодическому методу в теории чисел // Чебышевский сборник. 2010. Т. 11, № 1(33). С. 217—233.
6. Пачев У. М. О распределении приведенных положительных бинарных квадратичных форм с условием делимости первых коэффициентов по классам вычетов // Ученые зап. Орловского гос. ун-та. 2012. № 6(50). С. 177—182.
7. Малышев А. В., Пачев У. М. Об арифметике матриц второго порядка // Зап. науч. сем. ЛОМИ. 1980. Т. 93. С. 43—86.
8. Венков Б. А. Элементарная теория чисел. М. ; Л.: ОНТИ, 1937.
9. Малышев А. В., Нгуен Нгор Гой. О распределении целых точек на некоторых однополостных гиперблоидах // Зап. науч. сем. ЛОМИ. 1983. Т. 121. С. 83—93.
10. Малышев А. В., Широков Б. М. Новое доказательство ключевой леммы дискретного эргодического метода для вектор-матриц второго порядка // Вестн. Ленинград. ун-та. 1991. Серия 1, вып. 2. С. 34—40.
11. Bachman P. Die Arithmetik der quadratischen Formen. Leipzig: Teubner, 1898.

Кабардино-Балкарский государственный университет им. Х. М. Бербекова  
Поступило 29.05.2013