



Math-Net.Ru

Общероссийский математический портал

Ю. Г. Тетерин, Асимптотическая формула для числа представлений вполне положительными тернарными квадратичными формами,
Изв. АН СССР. Сер. матем., 1985, том 49, выпуск 2, 393–426

<https://www.mathnet.ru/im1360>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<https://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 18.97.14.91

20 июня 2025 г., 23:21:15



УДК 511.512

ТЕТЕРИН Ю. Г.

**АСИМПТОТИЧЕСКАЯ ФОРМУЛА ДЛЯ ЧИСЛА ПРЕДСТАВЛЕНИЙ
ВПОЛНЕ ПОЛОЖИТЕЛЬНЫМИ ТЕРНАРНЫМИ
КВАДРАТИЧНЫМИ ФОРМАМИ**

Основной целью этой работы является доказательство асимптотической формулы для числа представлений чисел вполне положительными тернарными квадратичными формами над максимальными порядками вполне вещественных алгебраических числовых полей. Кроме того, будет рассмотрено распределение таких представлений по модулю идеала. Заметим, что если число переменных $k \geq 4$, то эта задача решается аналитическими методами: либо при помощи теории модулярных форм, либо круговым методом (см. [5, 11, 13, 14] и [8]). В так называемом «неопределенном» случае, т. е. когда либо числовое поле K не является вполне вещественным, либо форма не является вполне определенной, задача о представлении чисел формой также имеет вполне удовлетворительное решение (для $k \geq 4$ см. [17], $104 : 3$, для $k=3$ см. [12] и [17], $104 : 5$). Наконец, в случае $k=1$ эта задача тривиальна, а в случае $k=2$ (бинарные формы) получается существенно другая теория, в которой на первый план выходит понятие композиции бинарных форм. Таким образом, полное решение задачи для вполне положительных тернарных форм означало бы завершение в общих чертах теории представления чисел квадратичными формами. К сожалению, до сих пор полностью не решена даже простейшая задача о существовании представлений достаточно больших чисел положительной тернарной формой над кольцом целых чисел \mathbf{Z} (результаты этой статьи также не дают полного и безусловного решения этой задачи).

В основе этой работы лежит дискретный эргодический метод. История развития этого метода и его приложений до 1979 г. описана в обзоре А. В. Малышева (см. [7, с. 418–432]). Укажем лишь кратко, что основы метода были заложены Ю. В. Линником (см. [7, с. 84–122]); далее метод развивал А. В. Малышев сначала совместно с Ю. В. Линником, затем самостоятельно и со своими учениками (см., например, [8] и [1, 9]); говоря о методе, мы везде имеем в виду только приложения к положительным формам). Развитие дискретного эргодического метода шло по двум направлениям:

а) по линии уточнения результатов. Здесь техника метода совершенствовалась на простейшем случае форм, содержащихся в сумме трех квадратов. При этом были получены асимптотические формулы того же типа, что и в формулируемой далее теореме 1. В наиболее развитом виде эта техника изложена в статье [1] (см. также [9]). Эти результаты были перенесены Н. Н. Беловой еще на некоторые классы форм;

б) по линии получения возможно более общих результатов. Здесь

следует выделить монографию [8], в которой была получена оценка снизу для числа представлений положительной тернарной квадратичной формой нечетных взаимно простых инвариантов. Кроме того, в этой работе была построена развитая арифметика обобщенных кватернионов, отвечающих рациональным формам общего вида, которая явилась основой для последующих работ. Далее М. Петерс [18] соединил дискретный эргодический метод с теорией спинорных родов и получил теорему о существовании представлений рациональными формами общего вида. Идея такого соединения оказалась чрезвычайно плодотворной. К сожалению, статья [18] была написана весьма кратко и содержала ряд пробелов и неточностей. В частности, одна из этих неточностей лишала оснований почти всю часть статьи, касающуюся дискретного эргодического метода. В статье автора [10] эти пробелы были восполнены, а результаты статьи [18] усилены.

В основу предлагаемой статьи легли техника работы [1], средства из арифметики обобщенных кватернионов, содержащиеся в монографии [8], и простейшие результаты из теории спинорных родов. Кроме того, все результаты обобщены на случай алгебраического числового поля.

Статья состоит из семи параграфов. В § 1 будет сформулирован и обсужден основной результат статьи — теорема 1. В § 2 будет дано определение алгебры кватернионов и порядка целых кватернионов, отвечающих тернарной форме, и связанных с ними понятий. Эти объекты играют роль базиса для всех последующих рассуждений. В § 3 излагается техника дискретного эргодического метода, непосредственно обобщающая статью [1]. В § 4 на основе результатов предыдущего параграфа доказывается теорема 1. Ради удобства чтения мы вынесли доказательство так называемой «ключевой леммы» метода в § 5, а все вспомогательные леммы — в заключительные параграфы 6 и 7.

Другой подход к рассматриваемым здесь задачам принадлежит Е. П. Голубевой [6]. *

Приношу глубокую благодарность А. В. Малышеву за постановку задачи и внимание к работе.

§ 1. Основные результаты

Пусть K — вполне вещественное алгебраическое числовое поле, $[K : \mathbf{Q}] = n$. Мы отождествляем K с его образом при стандартном вложении в пространство \mathbf{R}^n (с покомпонентным сложением и умножением), которое переводит число $x \in K$ в вектор $(x^{(1)}, \dots, x^{(n)})$, где $x^{(1)}, \dots, x^{(n)}$ — образы x при всех вложениях K в \mathbf{R} . В пространстве \mathbf{R}^n определено отношение $<$: $(x_1, \dots, x_n) < (y_1, \dots, y_n)$, если $x_i < y_i$ для $i = 1, \dots, n$. Пусть \mathfrak{o} — кольцо целых элементов поля K , $n(\cdot)$ — норма чисел и идеалов в K . Везде в дальнейшем, если не оговорено противное, малые латинские буквы обозначают числа из \mathfrak{o} (или из \mathbf{Z} , что будет ясно из контекста), малые готические буквы — целые идеалы в \mathfrak{o} , отличные от нулевого; \mathfrak{p} — произвольный простой идеал. $v_{\mathfrak{p}}(\alpha)$ — показа-

* Недавно Е. П. Голубева усилила свои результаты.

тель, с которым \mathfrak{p} входит в идеал \mathfrak{a} ,

$$\tau(\mathfrak{a}) = \sum_{n|\mathfrak{a}} 1 = \prod_{\mathfrak{p}|\mathfrak{a}} (v_{\mathfrak{p}}(\mathfrak{a}) + 1)$$

— число делителей идеала \mathfrak{a} (или числа $a \in \mathfrak{o}$) относительно K ; $(\mathfrak{a}_1, \dots, \mathfrak{a}_k)$ — идеал, порожденный $\mathfrak{a}_1, \dots, \mathfrak{a}_k$.

Определим делитель вектора $\mathbf{x} \in \mathfrak{o}^k$ с координатами x_1, \dots, x_k : $\mathfrak{c}(\mathbf{x}) = (x_1, \dots, x_k)$. Очевидно, $\mathfrak{c}(\mathbf{x})^{-1} = \{a \in K \mid a\mathbf{x} \in \mathfrak{o}^k\}$.

Пусть $f(x_1, x_2, x_3) = f(\mathbf{x}) = \mathbf{x}F\mathbf{x}^t$ — вполне положительная тернарная квадратичная форма над K с матрицей F и определителем $d = \det F \neq 0$. Вполне положительность означает, что $0 < f(\mathbf{x})$, если $\mathbf{x} \neq \mathbf{0}$. Для $m \in K$, целых идеалов \mathfrak{a} , \mathfrak{c} и вектора $\mathbf{b} \in \mathfrak{o}^3$ обозначим через $r(f, m, \mathfrak{c}; \mathfrak{a}, \mathbf{b})$ число решений $\mathbf{x} \in \mathfrak{o}^3$ системы

$$f(\mathbf{x}) = m, \quad \mathfrak{c}(\mathbf{x}) = \mathfrak{c}, \quad \mathbf{x} \equiv \mathbf{b} \pmod{\mathfrak{a}}. \quad (1.1)$$

Наша основная цель — доказать асимптотическую формулу для этой величины. Без ограничения общности мы будем считать, что элементы матрицы F содержатся в \mathfrak{o} и, более того, $2 \mid d$. Поэтому везде в дальнейшем запись $(\mathfrak{g}, d) = \mathfrak{o}$ означает, в частности, что $(\mathfrak{g}, 2) = \mathfrak{o}$. При этих ограничениях для разрешимости системы (1.1) необходимо, чтобы $m \in \mathfrak{o}$, $\mathfrak{c}^2 \mid m$ и

$$f(\mathbf{b}) \equiv m \pmod{\mathfrak{a} \cdot (\mathfrak{a}, \mathfrak{c})}, \quad (\mathfrak{c}(\mathbf{b}), \mathfrak{a}) = (\mathfrak{c}, \mathfrak{a}). \quad (1.2)$$

Везде в дальнейшем мы считаем эти условия выполненными.

Введем следующие обозначения: $\#\mathcal{K}$ — число элементов конечного множества \mathcal{K} ; $\text{Cls } f$, $\text{Spn } f$ — класс и спинорный род формы f (см. [17]);

$$r(f, m, \mathfrak{c}) = r(f, m, \mathfrak{c}; \mathfrak{o}, \mathbf{0}),$$

$$\tilde{r}(\text{Spn } f, m, \mathfrak{c}) = \left\{ \sum_{\text{Cls } g \subset \text{Spn } f} \frac{1}{\#\mathcal{O}(g)} \right\}^{-1} \sum_{\text{Cls } g \subset \text{Spn } f} \frac{r(g, m, \mathfrak{c})}{\#\mathcal{O}(g)},$$

где $\mathcal{O}(g)$ — множество автоморфизмов формы g ;

$$\chi(\mathfrak{p}) = \chi(\mathfrak{p}; -dm, \mathfrak{c}) = \left(\frac{-dmc^{-2}}{\mathfrak{p}} \right), \quad \text{где } c \in \mathfrak{c}, \quad c \notin \mathfrak{c}\mathfrak{p};$$

здесь $\mathfrak{p} \nmid 2$, $\left(\frac{\cdot}{\mathfrak{p}} \right)$ — символ квадратичного вычета; $\left(\frac{a}{\mathfrak{p}} \right) = 0$, если $\mathfrak{p} \mid a$;

$$q(-dm, \mathfrak{c}) = \min \{n(\mathfrak{q}) \mid \mathfrak{q} \text{ — простой идеал, } \mathfrak{q} \nmid 2, \chi(\mathfrak{q}) = 1\};$$

$$L(-dm, \mathfrak{c}) = \prod_{\mathfrak{p} \nmid 2} (1 - \chi(\mathfrak{p}) n(\mathfrak{p})^{-1}),$$

произведение берется в порядке возрастания норм простых идеалов $\mathfrak{p} \nmid 2$;

$$\eta(m, \mathfrak{c}) = \frac{\log q(-dm, \mathfrak{c})}{\log n(mc^{-2})} \max \{-\log L(-dm, \mathfrak{c}), \log \log n(mc^{-2})\}.$$

Основным результатом этой работы является следующая теорема, доказательство которой будет дано в § 4.

ТЕОРЕМА 1. Если $(\mathfrak{a}, dmc^{-2}) = \mathfrak{o}$ и выполнено условие (1.2), то

$$r(f, m, \mathfrak{c}; \mathfrak{a}, \mathbf{b}) = \frac{\tilde{r}(\text{Spn } f, m, \mathfrak{c})}{n(\mathfrak{a}')^2 \prod_{\mathfrak{p}|\mathfrak{a}'} (1 + \chi(\mathfrak{p}) n(\mathfrak{p})^{-1})} (1 + O(\sqrt{\eta(m, \mathfrak{c}) \cdot |\log \eta(m, \mathfrak{c})|})), \quad (1.3)$$

где $a' = a \cdot (a, c)^{-1}$; постоянная в знаке O зависит только от K , рода f и идеала a' .

Формула (1.3) требует дополнительного анализа. Прежде всего, величина $\tilde{r}(\text{Spr } f, m, c)$, входящая в главный член, вычисляется, как правило, достаточно просто (см. [12], [15] и [10], предложения 2.7, 2.9). В частности, она совпадает со взвешенным числом представлений родом i , значит, вычисляется по формулам Зигеля [19], если $(m) \neq mn^2$, где $\mathfrak{m} | d$ (а также, конечно, если спинорный род f совпадает с родом f).

Остаточный член в (1.3) стремится к нулю, если $\eta(m, c) \rightarrow 0$. К сожалению, имеющиеся оценки для $q(-dm, c)$ и $L(-dm, c)$ не позволяют доказать без использования каких-либо не доказанных еще предположений, что это верно для всех m и c при $n(mc^{-2}) \rightarrow \infty$. Исторически принято при использовании дискретного эргодического метода выделять два случая, когда это удается доказать:

а) «Безусловный вариант». Из теоремы Зигеля — Брауэра (см. [16], гл. XVI, следствие теоремы 5), примененной к полю $K(\sqrt{-dm})$, следует, что $\log L(-dm, c) = o(\log n(mc^{-2}))$. Значит, остаточный член в (1.3) стремится к нулю при $n(mc^{-2}) \rightarrow \infty$, если ограничиться рассмотрением пар m, c с условием $q(-dm, c) \leq \kappa$, где κ — произвольная заранее выбранная постоянная. Довольно часто это условие почти не накладывает ограничений на m и c . Так, например, если для инвариантов рода f выполнены некоторые специальные условия, то вместо простого идеала \mathfrak{q} , входящего в определение $q(-dm, c)$, можно взять один из идеалов $\mathfrak{q}' | d$; формула (1.3) с бесконечно малым остаточным членом получается тогда для всех m и c , для которых $\mathfrak{q}' \nmid mc^{-2}$ (ср. [8], с. 178, 202–204). Аналогично, если задача (1.1) рассматривается при фиксированных a и b и $\left(\frac{-d \cdot f(b)}{\mathfrak{q}}\right) = 1$ для одного из простых идеалов $\mathfrak{q} | a$ (мы считаем для простоты, что $(a, c) = 0$), то для всех чисел m с условием (1.2) будет $q(-dm, c) \leq n(\mathfrak{q})$, и, значит, для всех допустимых m остаточный член в формуле (1.3) стремится к нулю при $n(mc^{-2}) \rightarrow \infty$.

б) «Условный вариант». Известно, что оценки для $q(-dm, c)$ и $L(-dm, c)$ тесно связаны. Поэтому хорошие оценки остаточного члена в формуле (1.3) можно вывести из предположений о поведении соответствующей L -функции в окрестности единицы. Докажем в качестве примера только простейший результат (ср. Е. П. Голубева [6]). Пусть $K = \mathbf{Q}$. Тогда задача (1.1) сводится к задаче о примитивных представлениях, и мы опускаем упоминание об идеале c , считая $c = \mathbf{Z}$. Известно, что если число m примитивно представимо родом f , то $-dm$ является дискриминантом некоторой примитивной бинарной квадратичной формы, так что символ Кронекера $\chi(k) = \left(\frac{-dm}{k}\right)$ определен и является характером по модулю dm .

ТЕОРЕМА 2. Пусть $K = \mathbf{Q}$, $c = \mathbf{Z}$, $a = a\mathbf{Z}$, $(a, dm) = 1$, выполнено условие (1.2) и функция $L(s) = \sum_{k=1}^{\infty} \left(\frac{-dm}{k}\right) k^{-s}$ не имеет нулей в прямоугольнике

$$1 - (\log dm)^{\varepsilon-1} < \text{Re } s < 1, \quad |\text{Im } s| < 1. \quad (1.4)$$

Тогда

$$r(f, m; a, \mathbf{b}) = \frac{\tilde{\tau}(\text{Spn } f, m)}{a^2 \prod_{p|a} \left(1 + \left(\frac{-dm}{p}\right) p^{-1}\right)} (1 + O((\log m)^{-\varepsilon/10})). \quad (1.5)$$

Постоянные в знаке O зависят только от d , a и $\varepsilon > 0$.

Доказательство. Согласно лемме 1 статьи [6] из условий теоремы следует, что при $z \geq \exp((\log dm)^{1-\varepsilon/2})$

$$\sum_{p \leq z} \left(\frac{-dm}{p}\right) \frac{1}{p} = \log L(1) + O(\log \log \log dm).$$

Учитывая, что $\sum_{p \leq z} \frac{1}{p} = \log \log z + O(1)$, получаем отсюда:

$$\begin{aligned} \log L(1) &\geq -\left(1 - \frac{\varepsilon}{2}\right) \log \log dm + O(\log \log \log dm), \\ &2 \cdot \sum_{p \leq \exp\left((\log dm)^{1-\frac{\varepsilon}{4}}\right), \left(\frac{-dm}{p}\right) = -1} \frac{1}{p} = \\ &= \log L(1) + \left(1 - \frac{\varepsilon}{4}\right) \log \log dm + O(\log \log \log dm) \geq \\ &\geq \frac{\varepsilon}{4} \log \log dm + O(\log \log \log dm), \end{aligned}$$

поэтому $\log q(-dm, \mathbf{c}) = O((\log m)^{1-\varepsilon/4})$. Так как $L(-dm, \mathbf{c})$ отличается от $L(1)$ только несущественным множителем, отсюда и из (1.3) следует (1.5). Теорема 2 доказана.

Заметим, что высоту области (1.4), по-видимому, можно уменьшить (ср. [8], § 5 гл. V).

Доказательство формулы (1.3) (с остаточным членом в форме (4.10), см. далее) вполне элементарно. Единственное неэлементарно доказываемое предложение, используемое при этом, — это теорема о представлении чисел кватернарными формами. В то же время для анализа формулы (1.3) приходится использовать такие средства, как понятие адель, теорию инвариантной меры на ортогональных группах, формулы Зигеля для числа представлений родом формы, теорему Зигеля — Брауэра, теорию L -функций.

Если нам известно, что представления чисел кватернарной формой $x_0^2 + d \cdot f(\mathbf{x})$ распределяются по соответствующей поверхности в K^4 асимптотически равномерно, то изложенные далее методы позволяют доказать такую равномерность и для представлений формой f . В частности, это справедливо для всех форм при $K = \mathbf{Q}$ (ср. [1]).

Если в формуле для числа представлений чисел формой $x_0^2 + d \cdot f(\mathbf{x})$ нам известна явная зависимость остаточного члена от модуля a (и от телесного угла λ соответствующей области, если мы интересуемся распределением представлений по поверхности), то мы можем получить явную зависимость от a (и λ) и для остаточного члена в формуле (1.3). В частности, в случае $K = \mathbf{Q}$ остаточный член в (1.3) имеет вид

$$O\left(\frac{a \log(a+1)}{\sqrt{\lambda}} \sqrt{\eta(m) \cdot |\log \eta(m)|}\right),$$

где постоянная в знаке O зависит только от d (ср. [9], [1]).

Несколько слов об условии $(a, dmc^{-2})=0$ в теореме 1. Если $(a, d) \neq 0$, то известны примеры, когда формула (1.3) перестает быть справедливой. Например, если $K=\mathbf{Q}$, $f(x, y, z)=x^2+y^2+yz+z^2$, $m=4n^2$, $c=\mathbf{Z}$, $a=3\mathbf{Z}$, то при $n \equiv 1 \pmod{3}$ все представления распределяются только по классам $b \pmod{3}$ с $b_1 \not\equiv 0 \pmod{3}$, а при $n \equiv 2 \pmod{3}$ — наоборот, только по классам с $b_1 \equiv 0 \pmod{3}$. В случае $(a, mc^{-2}) \neq 0$ нам не известны контрпримеры такого типа, однако ряд соображений говорит в пользу того, что это условие также существенно.

§ 2. Кватернионная алгебра, отвечающая форме f

В этом параграфе мы, следуя [8], гл. IV, построим кватернионную алгебру и порядок целых кватернионов, соответствующие форме f . Эти объекты играют важнейшую роль во всем доказательстве теоремы 1.

Пусть $\bar{F}=(\bar{f}_{ij})$ — взаимная F матрица. Рассмотрим алгебру \mathcal{A} ранга 4 над K с базисом $1, i_1, i_2, i_3$ и таблицей умножения:

$$\begin{aligned} 1 \cdot 1 &= 1, & 1 \cdot i_k &= i_k \cdot 1 = i_k, & k &= 1, 2, 3, \\ i_1 i_1 &= -df_{11}, & i_1 i_2 &= -df_{12} + \sum_{k=1}^3 \bar{f}_{3k} i_k, & i_1 i_3 &= -df_{13} - \sum_{k=1}^3 \bar{f}_{2k} i_k, \\ i_2 i_1 &= -df_{21} - \sum_{k=1}^3 \bar{f}_{3k} i_k, & i_2 i_2 &= -df_{22}, & i_2 i_3 &= -df_{23} + \sum_{k=1}^3 \bar{f}_{1k} i_k, \\ i_3 i_1 &= -df_{31} + \sum_{k=1}^3 \bar{f}_{2k} i_k, & i_3 i_2 &= -df_{32} - \sum_{k=1}^3 \bar{f}_{1k} i_k, & i_3 i_3 &= -df_{33}. \end{aligned}$$

Элементы этой алгебры $X = x_0 + x_1 i_1 + x_2 i_2 + x_3 i_3 = (x_0, \mathbf{x})$ называются кватернионами, $\text{Sc}(X) = x_0$ — скалярной частью X , $\bar{X} = (x_0, -\mathbf{x})$ — сопряженным X кватернионом, число поля K

$$N(X) = X\bar{X} = \bar{X}X = x_0^2 + d \cdot f(\mathbf{x}) \quad (2.1)$$

— нормой X . Если $\text{Sc}(X) = 0$, то X называется вектором.

Легко проверяются следующие свойства кватернионов:

- 1) $\bar{\bar{X}} = X$, $\overline{X+Y} = \bar{X} + \bar{Y}$, $\overline{XY} = \bar{Y}\bar{X}$,
- 2) если X — вектор, то $\bar{X} = -X$,
- 3) $N(\bar{X}) = N(X)$, $\text{Sc}(\bar{X}) = \text{Sc}(X)$,
- 4) $N(X) > 0$, если $X \neq 0$,
- 5) если $X \neq 0$, то $X^{-1} = N(X)^{-1}\bar{X}$,
- 6) $N(XY) = N(YX) = N(X)N(Y)$, $\text{Sc}(XY) = \text{Sc}(YX)$,
- 7) $N(X+Y) = N(X) + N(Y) + 2 \cdot \text{Sc}(X\bar{Y})$.

Кватернионы с координатами из \mathfrak{o} называются целыми. Целые кватернионы образуют кольцо \mathcal{O}_f . $\mathcal{O}_f = \mathfrak{o} \oplus \mathcal{V}_f$, где \mathcal{V}_f — множество целых векторов. Как и раньше, $c(X) = (x_0, c(\mathbf{x})) = (x_0, x_1, x_2, x_3)$. Очевидно, что $c(X) = c(\bar{X})$.

Обратимые элементы кольца \mathcal{O}_f называются единицами. Если E — единица, то $N(E)N(E^{-1}) = N(1) = 1$, значит, $N(E)$ — единица кольца \mathfrak{o} . Поскольку мы считаем, что $2 \mid d$ (см. § 1), то ввиду (2.1) в \mathcal{O}_f есть только две единицы нормы 1: $E = \pm 1$. Таким образом, ассоциированные кватернионы одинаковой нормы отличаются только знаком. Впрочем, это огра-

ничение несущественно и будет использовано нами только для упрощения рассуждений в § 3.

Мы говорим, что $Y \in \mathcal{O}_f$ делит справа X , и пишем X/Y , если $XY^{-1} \in \mathcal{O}_f$. Аналогична делимость слева: $Y \setminus X$, если $Y^{-1}X \in \mathcal{O}_f$. Простейшие свойства делимости см. в [8], с. 110. Запись $X \equiv Y \pmod{g}$ означает, что $g \mid c(X-Y)$.

Говорим, что целые кватернионы X и Y подобны \pmod{g} , если $X\bar{Y} \equiv 0 \pmod{c(X)c(Y)g}$. Из следствия 1 леммы 11 вытекает, что если $(g, d) = 0$, то отношение подобия \pmod{g} разбивает кватернионы $X \in \mathcal{O}_f$ с условием $N(X) \equiv 0 \pmod{c(X)^2g}$ на классы подобия \pmod{g} . Везде далее, говоря о подобии \pmod{g} , мы подразумеваем, что $(g, d) = 0$. Пусть \mathcal{G} — класс подобия \pmod{g} , \mathcal{H} — класс подобия \pmod{h} , $h \mid g$. Пишем \mathcal{G}/\mathcal{H} , если $\mathcal{G} \subset \mathcal{H}$. Если $A \in \mathcal{O}_f$, то запись \mathcal{G}/A означает, что \mathcal{G}/\mathcal{H} , где \mathcal{H} — класс подобия $\pmod{N(A)c(A)^{-2}}$, содержащий A . Легко проверить, что если \mathcal{G}/A , то кватернионы XA^{-1} при $X \in \mathcal{G}$, $c(A) \mid c(X)$ содержатся в одном классе подобия $\pmod{gN(A)^{-1}c(A)^2}$, обозначаемом $\mathcal{G}A^{-1}$. Иногда мы будем говорить о подобии X и $Y \pmod{g}$ слева, подразумевая под этим, что $\bar{X}Y \equiv 0 \pmod{c(X)c(Y)g}$, и о классах подобия \pmod{g} слева. Если X и Y подобны \pmod{g} , то \bar{X} и \bar{Y} подобны слева \pmod{g} . Поэтому все утверждения о подобных кватернионах переносятся и на подобие слева.

Пусть K_p — пополнение K относительно нормирования ν (архимедового или неархимедового), \mathfrak{o}_p — замыкание \mathfrak{o} в K_p . При расширении поля скаляров до K_p алгебра \mathcal{A} расширяется до K_p -алгебры \mathcal{A}_p , кольцо \mathcal{O}_f — до \mathfrak{o}_p -модуля \mathcal{O}_{fp} , также являющегося кольцом. Для них справедливо все сказанное выше, только свойства 4) и 5) ослабляются до свойства:

$$\text{если } N(X) \neq 0, \text{ то } X^{-1} = N(X)^{-1}\bar{X}.$$

Кроме того, кольцо \mathcal{O}_{fp} содержит бесконечно много единиц.

Если подстановка с матрицей (A) над K (или над K_p) переводит f в форму f' , то соответствие

$$\begin{pmatrix} i'_1 \\ i'_2 \\ i'_3 \end{pmatrix} = \det(A) \cdot (A) \begin{pmatrix} i_1 \\ i_2 \\ i_3 \end{pmatrix}$$

осуществляет изоморфизм алгебр \mathcal{A}' и \mathcal{A} (или соответственно \mathcal{A}'_p и \mathcal{A}_p). Поэтому мы будем отождествлять кватернионные алгебры, соответствующие K -эквивалентным формам. Поскольку замена формы f на \mathfrak{o} -эквивалентную или на \mathfrak{o}_p -эквивалентную сводится к замене базиса решеток векторов \mathcal{Y}_f или \mathcal{Y}_{fp} , то в § 6 мы часто будем заменять f на более удобные эквивалентные формы. В частности, при всех локальных рассмотрениях считаем без дальнейших оговорок, что при $\nu \nmid d$ для \mathcal{O}_{fp} (см. [17], § 92)

$$\bar{f}(x) = x\bar{F}x^t = u_1x_1^2 + u_2x_2^2 + u_3x_3^2, \quad \nu_p(u_k) = 0, \quad k = 1, 2, 3.$$

Далее, если не оговорено противное, мы рассматриваем только кватернионы из \mathcal{O}_f .

§ 3. Эргодические свойства разложений $l+L=VB$

Содержание этого параграфа и § 5 составляет существо дискретного эргодического метода в применении к задаче (1.1). Изложение близко [1], только вместо правых делителей нормы g везде рассматриваются классы подобия (mod g).

Везде далее κ_i — положительные постоянные, зависящие только от K , рода f и величин, указанных в скобках. β — постоянная из леммы 31. Положительное число ε считаем достаточно малым; для теоремы 1 это соответствует единственно нетривиальному случаю $|O\sqrt{\eta} \cdot |\log \eta|| < < n(\alpha')^3$. Напомним также, что в \mathcal{O}_f имеются только две единицы нормы 1: ± 1 , так что в силу следствия 2 леммы 11 если класс подобия делится справа на кватернион с заданными N и s , то этот делитель определен однозначно с точностью до знака.

ЛЕММА 1. Пусть $q \in \mathfrak{o}$, $(\alpha_1 \alpha_2 q, d) = \mathfrak{o}$, $(\alpha_1, q) = \mathfrak{o}$, $\alpha_2 | q$, $0 < q$, сравнение $x^2 \equiv q \pmod{8d}$ разрешимо, $1 \leq i_1 < \dots < i_s < k$ и для каждого $j = 1, \dots, s$ среди решений сравнения $N(X) \equiv q^{i_j} \pmod{\alpha_1}$ выделены совокупности \mathcal{B}_j из t классов (mod α_1), причем если $X \in \mathcal{B}_j$, то и $-X \in \mathcal{B}_j$; \mathcal{H}_1 — класс подобия (mod α_2) слева; \mathcal{H}_2 — класс подобия (mod α_2) (справа), причем если $A_1 \in \mathcal{H}_1$, $A_2 \in \mathcal{H}_2$, то $(c(A_2 A_1) c(A_1)^{-1} c(A_2)^{-1}, \alpha_2) = \mathfrak{o}$. Рассмотрим классы подобия \mathcal{G} со свойствами:

$$\mathcal{G}/A, \quad N(A) = q^{i_j}, \quad c(A) = \mathfrak{o}, \quad A \in \mathcal{B}_j, \quad A \in \mathcal{H}_1, \quad \mathcal{G}A^{-1} \in \mathcal{H}_2. \quad (3.1)$$

Тогда число классов подобия $\mathcal{G} \pmod{q^k}$, для которых

$$\# \{j = 1, \dots, s \mid \text{справедливо (3.1)}\} \cdot \frac{1}{\gamma^s} \notin (1 - \varepsilon, 1 + \varepsilon), \quad (3.2)$$

будет

$$< \kappa_1 \cdot n(q^k) \prod_{p|q} \left(1 + \frac{1}{n(p)}\right) \cdot s \exp\left(\left(-\frac{\gamma \varepsilon^2}{3(1-\gamma)} + \kappa_2(\alpha_1, \alpha_2) n(q)^{-\frac{1}{5}}\right) s\right).$$

Здесь

$$\gamma = \frac{\beta}{2} \frac{t}{n(\alpha_1)^3 \prod_{p|\alpha_1} (1 - n(p)^{-2}) \cdot n(\alpha_2)^2 \prod_{p|\alpha_2} (1 + n(p)^{-1})}.$$

Доказательство. Прежде всего, если разбить все кватернионы $A \in \mathcal{O}_f$ со свойствами

$$N(A) = q^i, \quad c(A) = \mathfrak{o}, \quad A \in \mathcal{B}_j, \quad A \in \mathcal{H}_1$$

на пары кватернионов, отличающихся знаком, то число классов подобия $\mathcal{G} \pmod{q^i \alpha_2}$ со свойством (3.1) для $i_j = i$ равно числу таких пар. Именно, каждый такой класс имеет вид $\mathcal{G} = \mathcal{G}_{\pm A} = \{XA \mid X \in \mathcal{H}_2\}$. Поэтому в силу лемм 31, 21 и 22

1) число классов подобия (mod $q^i \alpha_2$), для которых выполнено свойство (3.1) с $j=1$,

$$\leq \gamma \cdot n(q^i \alpha_2) \prod_{p|q} (1 + n(p)^{-1}) \cdot (1 + \delta),$$

а число остальных классов подобия (mod $q^i \alpha_2$)

$$\leq (1 - \gamma) n(q^i \alpha_2) \prod_{p|q} (1 + n(p)^{-1}) \cdot (1 + \delta);$$

2) если \mathcal{K} — класс подобия $(\text{mod } q^{i_j-1}a_2)$, $2 \leq j \leq s$, то число классов подобия $(\text{mod } q^{i_j}a_2)$, содержащихся в \mathcal{K} , для которых выполнено свойство (3.1), будет

$$\leq \gamma \cdot n(q^{i_j-1}a_2) \cdot (1 + \delta),$$

а число остальных классов подобия $(\text{mod } q^{i_j}a_2)$, содержащихся в \mathcal{K} , будет

$$\leq (1 - \gamma) n(q^{i_j-1}a_2) \cdot (1 + \delta).$$

Здесь $\delta \leq \kappa_3(a_1, a_2) n(qa_2^{-1})^{-1/5}$. Учитывая лемму 22, выводим отсюда, что для любого фиксированного набора чисел $1 \leq j_1 < \dots < j_v \leq s$ число классов подобия $(\text{mod } q^{i_j})$, для которых (3.1) выполнено для $j = j_1, \dots, j_v$, а для остальных j не выполнено, будет

$$\begin{aligned} &\leq \gamma^v \cdot (1 - \gamma)^{s-v} n(q^{i_1}a_2) n(q^{i_2-i_1}) \dots n(q^{i_s-i_{s-1}}) \times \\ &\quad \times n(q^{i_s}a_2^{-1}) \prod_{p|q} (1 + n(p)^{-1}) \cdot (1 + \delta)^{s \leq} \\ &\leq n(q^k) \prod_{p|q} (1 + n(p)^{-1}) \cdot \exp(\delta s) \cdot \gamma^v \cdot (1 - \gamma)^{s-v}. \end{aligned}$$

Поэтому число классов подобия со свойством (3.2) будет

$$\leq n(q^k) \prod_{p|q} (1 + n(p)^{-1}) \cdot \exp(\delta s) \cdot \sum_{\substack{1 \leq v \leq s, \\ \frac{v}{\gamma^s} \notin (1-\delta, 1+\delta)}} C_s^v \gamma^v (1 - \gamma)^{s-v}. \quad (3.3)$$

Согласно [9, с. 62—63, 76—77] сумма в (3.3)

$$\leq \kappa_4 \cdot s \cdot \exp\left(-\frac{\gamma \varepsilon^2}{3(1-\gamma)} s\right),$$

если только ε меньше некоторой абсолютной постоянной. Ввиду оценки для δ лемма 1 доказана.

Пусть теперь $m, l, q \in \mathfrak{o}$, $0 < q$, сравнение $x^2 \equiv q \pmod{8d}$ разрешимо, $c^2 | m$, $c | l$, $(dm c^{-2}, q) = \mathfrak{o}$, $q^k c^2 | (l^2 + dm)$, $n(q^k)^5 n(c)^2 \leq n(m)$; $(a_0 a_1, c) = a_0$, $a' = a_1 a_2 a_3$, $(a', d) = \mathfrak{o}$, $(a_1, m c^{-2} q) = \mathfrak{o}$, $a_2 | q$, $a_3 | m c^{-2}$; $L_0 \in \mathcal{V}_i$, $N(L_0) \equiv dm \pmod{a_0^2 a_1}$, $(c(L_0), a_0 a_1) = a_0$; \mathcal{H}_1 — класс подобия $(\text{mod } a_2)$ слева, \mathcal{H}_2 — класс подобия $(\text{mod } a_2)$ (справа), причем если $A_1 \in \mathcal{H}_1$, $A_2 \in \mathcal{H}_2$, то $(c(A_2 A_1) c(A_1)^{-1}, c(A_2)^{-1}, a_2) = \mathfrak{o}$; \mathcal{K} — класс подобия $(\text{mod } a_3)$.

ЛЕММА 2. Пусть $1 \leq i_1 < \dots < i_s < k$. Тогда число векторов L с условиями $N(L) = dm$, $c(L) = c$,

$$\begin{aligned} &\# \{j = 1, \dots, s | l + L = VB, N(B) = q^{i_j}, c(B) = \mathfrak{o}, (l + L)\bar{B} \equiv \\ &\quad \equiv 0 \pmod{cq^{i_j}}, BV \in \mathcal{H}_1, BV \in \mathcal{H}_2, L' \equiv L_0 \pmod{a_0 a_1}, \\ &\quad L' \in \mathcal{K}, \text{ где } L' = BLB^{-1} = BV - l\} \cdot \frac{1}{\gamma^s} \notin (1 - \varepsilon, 1 + \varepsilon) \end{aligned}$$

будет

$$\begin{aligned} &< \kappa_1(a') k^7 \tau(q)^7 \frac{V \overline{n(m)}}{n(c)} \left(\log \frac{n(m)}{n(c)^2}\right)^{\kappa_2} \times \\ &\quad \times \exp\left(\left(-\frac{\gamma \varepsilon^2}{6(1-\gamma)} + \kappa_3(a') n(q)^{-1/5}\right) s\right); \quad (3.4) \end{aligned}$$

здесь

$$\gamma = \frac{\beta}{2} \frac{1}{n(a_1 a_2)^2 \prod_{p|a_1 a_2} (1 + \chi(p) n(p)^{-1}) \cdot n(a_3) \prod_{p|a_3} (1 + n(p)^{-1})}.$$

Доказательство. Пусть искомое число векторов равно r . Поскольку общее число классов векторов $L \pmod{\mathfrak{c}(a_1 a_3)}$ с условием $\mathfrak{c}(L) = \mathfrak{c}$ не превосходит $n(a_1 a_3)^3$, то по крайней мере в одном классе $L^* \pmod{\mathfrak{c}(a_1 a_3)}$ содержится $r' \geq r \cdot n(a_1 a_3)^{-3}$ векторов рассматриваемого вида: $L_1, \dots, L_{r'}$. Пусть

$$\mathcal{B}_j = \{X \in \mathcal{O}_f \mid N(X) \equiv q^i \pmod{a_1 a_3}, XL^* \equiv L_0 X \pmod{a_0 a_1}, XL^* \bar{X} \in \mathcal{K}\}.$$

В силу лемм 23 и 24 \mathcal{B}_j состоит из

$$t = n(a_1) \prod_{p|a_1} (1 - \chi(p) n(p)^{-1}) \cdot n(a_3)^2 \prod_{p|a_3} (1 - n(p)^{-1})$$

классов $\pmod{a_1 a_3}$. Поэтому в силу леммы 1 число классов подобия $\pmod{q^k}$, содержащих кватернионы $l + L_i$, $i = 1, \dots, r'$, будет

$$\leq \kappa_4 \cdot n(q^k) \prod_{p|q} \left(1 + \frac{1}{n(p)}\right) \cdot s \cdot \exp\left(\left(-\frac{\gamma \varepsilon^2}{3(1-\gamma)} + \kappa_5(a') n(q)^{-1/5}\right) s\right).$$

С другой стороны, по лемме 6 (см. § 5) число тех же классов подобия будет

$$\begin{aligned} &\geq \kappa_6 \cdot n(q^k) \frac{r'^2}{\tau(q^k)^{13}} \frac{n(\mathfrak{c})^2}{n(m)} \left(\log \frac{n(m)}{n(\mathfrak{c})^2}\right)^{-\kappa_7} \geq \\ &\geq \kappa_6 \cdot n(q^k) \frac{r^2}{n(a_1 a_3)^6 \cdot k^{13} \tau(q)^{13}} \frac{n(\mathfrak{c})^2}{n(m)} \left(\log \frac{n(m)}{n(\mathfrak{c})^2}\right)^{-\kappa_7}. \end{aligned}$$

Сравнивая эти оценки, получаем (3.4).

ЛЕММА 3. Пусть $L_1, \dots, L_r \in \mathcal{Y}_f$, $N(L_i) = dm$, $\mathfrak{c}(L_i) = \mathfrak{c}$, $i = 1, \dots, r$. Тогда количество чисел $i = 1, \dots, k-1$ с условием

$$\begin{aligned} \# \{L = L_1, \dots, L_r \mid l + L = VB, N(B) = q^i, \mathfrak{c}(B) = \mathfrak{c}, (l + L)\bar{B} \equiv \\ \equiv 0 \pmod{cq^i}, BV \in \mathcal{H}_1, BV \in \mathcal{H}_2, L' \equiv L_0 \pmod{a_0 a_1}, L' \in \mathcal{K}, \end{aligned}$$

$$\text{где } L' = BLB^{-1} = BV - l\}. \frac{1}{\gamma r} \notin (1 - \varepsilon, 1 + \varepsilon),$$

где

$$\varepsilon = \kappa(a') \sqrt{\frac{1}{k} \max \left\{ \log \frac{\sqrt{n(m)}}{r \cdot n(\mathfrak{c})}, \log \log \frac{n(m)}{n(\mathfrak{c})^2}, \log \tau(q) \right\} + n(q)^{-1/5}},$$

будет $< k/3$. Здесь γ — та же, что и в лемме 2.

Доказательство. Предположим противное. Тогда найдется такая последовательность чисел $1 \leq i_1 < \dots < i_s < k$, что $s \geq k/6$ и либо

$$\# \{L = \dots\} \leq (1 - \varepsilon) \gamma r, \quad i = i_1, \dots, i_s, \quad (3.5)$$

либо

$$\# \{L = \dots\} \geq (1 + \varepsilon) \gamma r, \quad i = i_1, \dots, i_s, \quad (3.6)$$

Пусть имеет место (3.6) (случай (3.5) рассматривается аналогично —

ср. [1, с. 50]). Обозначим через r' число индексов $j=1, \dots, r$, для которых

$$\# \{i = i_1, \dots, i_s \mid l + L_j = VB, N(B) = q^i, c(B) = \mathfrak{o}, (l + L_j) \bar{B} \equiv 0 \pmod{cq^i}, BV \in \mathcal{H}_1, BV \in \mathcal{H}_2, L' \equiv L_0 \pmod{\mathfrak{a}_0 \mathfrak{a}_1}, L' \in \mathcal{H},$$

$$\text{где } L' = BLB^{-1} = BV - l\} \geq \left(1 + \frac{\varepsilon}{2}\right) \gamma s.$$

Тогда с учетом (3.6) получаем:

$$s \cdot (1 + \varepsilon) \gamma r \leq \left(1 + \frac{\varepsilon}{2}\right) \gamma s \cdot r + s \cdot r',$$

откуда

$$r' \geq \frac{\varepsilon \gamma}{2} r. \quad (3.7)$$

Однако, учитывая, что $n(q^k)^5 n(c)^2 \leq n(m)$, получаем $k \leq \log \frac{n(m)}{n(c)^2}$, по-

этому $\varepsilon \geq \kappa(\mathfrak{a}') \sqrt{\frac{\log k}{k}}$ и, следовательно, при подходящем выборе κ $\varepsilon \geq \exp\left(-\frac{\gamma \varepsilon^2}{6(1-\gamma)} \cdot \frac{k}{6}\right)$. Учитывая эти оценки, получим что (3.7) противоречит лемме 2.

§ 4. Доказательство теоремы 1

Доказательство проведем в два этапа: сначала докажем равномерную распределенность представлений формой по модулю, а затем выведем отсюда равномерную распределенность представлений спинорным родом по классам форм. Сведение второй задачи к первой представляет, на наш взгляд, и самостоятельный интерес, поскольку оно может быть применено к изучению задачи (1.1) и другими методами, отличными от дискретного эргодического.

Итак, пусть выполнены условия теоремы 1. Положим $L_0 = (0, \mathfrak{b}) \in \mathcal{V}_f$. Тогда, ввиду (2.1), представления (1.1) взаимно однозначно соответствуют векторам $L \in \mathcal{V}_f$ со свойствами $N(L) = dm$, $c(L) = c$, $L \equiv L_0 \pmod{\mathfrak{a}}$.

Обозначим

$$\eta(f, m, c) = \frac{\log q(-dm, c)}{\log n(mc^{-2})} \max \left\{ \log \frac{\sqrt{n(mc^{-2})}}{r(f, m, c)}, \log \log n(mc^{-2}) \right\},$$

$$\eta(\text{Spn } f, m, c) = \frac{\log q(-dm, c)}{\log n(mc^{-2})} \max \left\{ \log \frac{\sqrt{n(mc^{-2})}}{r(\text{Spn } f, m, c)}, \log \log n(mc^{-2}) \right\}.$$

ЛЕММА 4. Пусть выполнены условия теоремы 1, $\mathfrak{a}_3 \mid mc^{-2}$, $(\mathfrak{a}_3, d) = \mathfrak{o}$, \mathcal{H} — класс подобия $\pmod{\mathfrak{a}_3}$. Обозначим через $r(\mathcal{V}_f, dm, c; \mathfrak{a}, L_0; \mathcal{H})$ число векторов $L \in \mathcal{V}_f$ со свойствами:

$$N(L) = dm, c(L) = c, L \equiv L_0 \pmod{\mathfrak{a}}, L \in \mathcal{H}. \quad (4.1)$$

Тогда

$$r(\mathcal{V}_f, dm, c; \mathfrak{a}, L_0; \mathcal{H}) = \frac{r(f, m, c) \cdot (1 + O(\sqrt{V \eta(f, m, c) \cdot |\log \eta(f, m, c)|}))}{n(\mathfrak{a}')^2 \prod_{p \mid \mathfrak{a}'} (1 + \chi(p) n(p)^{-1}) \cdot n(\mathfrak{a}_3) \prod_{p \mid \mathfrak{a}_3} (1 + n(p)^{-1})}, \quad (4.2)$$

где $\alpha' = \alpha \cdot (\alpha, \mathfrak{c})^{-1}$; постоянная в знаке O зависит только от K , рода f и α'_3 .

Доказательство. Пусть $\mathfrak{q} = \mathfrak{q}(m, \mathfrak{c})$ — простой идеал минимальной нормы с условиями $\mathfrak{q} \nmid 2$, $\chi(\mathfrak{q}) = 1$. Тогда $\mathfrak{n}(\mathfrak{q}) = \mathfrak{q}(-dm, \mathfrak{c})$ в обозначениях § 1. Если h — число классов идеалов K , то $\mathfrak{q}^h = (q_1)$, $q_1 \in \mathfrak{o}$. Положим

$$q = q_1^{2s}, \quad s = [5 |\log \eta(f, m, \mathfrak{c})| / |\log |\mathfrak{n}(q_1)||] + \kappa_1(\alpha'), \quad (4.3)$$

где $\kappa_1 \geq 1$ выбрано так, что $(\alpha', q^2) | q$. Тогда

$$\mathfrak{n}(q)^{-1/2} \leq \eta(f, m, \mathfrak{c}), \quad (4.4)$$

$$\tau(q) = 2sh + 1 \leq \kappa_2 \cdot |\log \eta(f, m, \mathfrak{c})| + \kappa_1(\alpha') + 1. \quad (4.5)$$

Положим $k = [\log \mathfrak{n}(m\mathfrak{c}^{-2}) / (5 \log \mathfrak{n}(q))]$. Тогда в силу (4.3)

$$k \geq \log \mathfrak{n}(m\mathfrak{c}^{-2}) / 10(5 |\log \eta(f, m, \mathfrak{c})| + h \cdot \kappa_1 \cdot \log \mathfrak{n}(q)). \quad (4.6)$$

Поскольку $\chi(\mathfrak{q}) = 1$, найдется $l \in \mathfrak{c}$: $q^{kt^2} | (l^2 + dm)$. Таким образом, для чисел m, l, q и k выполнены все условия предыдущего параграфа.

Запишем $\alpha = \alpha_0'' \alpha_1 \alpha_2$, где $\alpha_0'' = (\alpha, \mathfrak{c})$, $\mathfrak{q} \nmid \alpha_0'' \alpha_1$, $\alpha_0'' \alpha_2 = \mathfrak{q}^t$. В силу (4.3) $\alpha_2 | q$. Пусть \mathcal{H}_1 и \mathcal{H}_2 — классы подобия соответственно слева и справа $(\text{mod } \alpha_2)$, содержащие $l + L_0$; поскольку

$$(l + L_0)^2 = 2l(l + L_0) - N(l + L_0) \not\equiv 0 \pmod{\alpha_0''^2 \alpha_2} \quad (4.7)$$

(если $\alpha_2 \neq \mathfrak{o}$, т. е. \mathcal{H}_1 и \mathcal{H}_2 не тривиальны), то \mathcal{H}_1 и \mathcal{H}_2 удовлетворяют условию § 3. Обозначим $\mathcal{V}_f(dm, \mathfrak{c}) = \{L \in \mathcal{V}_f | N(L) = dm, \mathfrak{c}(L) = \mathfrak{c}\}$. Как уже отмечалось, $\# \mathcal{V}_f(dm, \mathfrak{c}) = r(f, m, \mathfrak{c})$.

Если $L \in \mathcal{V}_f(dm, \mathfrak{c})$, то $L \equiv L_0 \pmod{\alpha'' \alpha_2}$ тогда и только тогда, когда $l + L \in \mathcal{H}_1 \cap \mathcal{H}_2$. Действительно, достаточность первого условия сразу следует из определения \mathcal{H}_1 и \mathcal{H}_2 . Пусть выполнено второе условие. Тогда с учетом равенства $L - L_0 = (l + L) - (l + L_0)$ получим: $(l + L_0) \times (L - L_0) \equiv (L - L_0)(l + L_0) \equiv 0 \pmod{\alpha_0''^2 \alpha_2}$. Отсюда и из (4.7) в силу леммы 16 следует, что $(L - L_0) \equiv 0 \pmod{\alpha_0'' \alpha_2}$.

Учитывая также (4.4) — (4.6), получаем по лемме 3, что по крайней мере для $\frac{2}{3}k$ чисел $i = 1, \dots, k-1$

$$\begin{aligned} \# \{L \in \mathcal{V}_f(dm, \mathfrak{c}) | l + L = VB, N(B) = q^t, \mathfrak{c}(B) = \mathfrak{o}, (l + L)\bar{B} \equiv \\ \equiv 0 \pmod{cq^t}, L' \equiv L_0 \pmod{\alpha}, L' \in \mathcal{K}, \text{ где } L' = BLB^{-1} = BV - l\} = \\ = \gamma \cdot r(f, m, \mathfrak{c}) \cdot (1 + O(\sqrt{|\eta(f, m, \mathfrak{c})| \log \eta(f, m, \mathfrak{c})})), \end{aligned} \quad (4.8)$$

где γ — та же, что и в лемме 2. Так как по следствию 2 леммы 11 при фиксированном i B определяется с точностью до знака, между векторами L и $L' = L'(i) \in \mathcal{V}_f(dm, \mathfrak{c})$ в (4.8) имеется взаимно однозначное соответствие. Поэтому из (4.8) получаем:

$$r(\mathcal{V}_f, dm, \mathfrak{c}; \alpha, L_0; \mathcal{K}) \geq \frac{\gamma}{2} r(f, m, \mathfrak{c}). \quad (4.9)$$

(Если остаток в (4.8) меньше $-1/2$, то формула (4.2) тривиальна.)

Применяя еще раз лемму 3 для сопряженных кватернионов и учитывая (4.9), получим, что по крайней мере для $\frac{2}{3}k$ чисел $i = 1, \dots, k-1$

$$\# \{L' \text{ с (4.1)} \mid l + L' = BV, N(B) = q^i, c(B) = \mathfrak{o}, \bar{B}(l + L) \equiv 0 \pmod{cq^i}\} = \\ = \frac{\beta}{2} r(\mathcal{V}_f, dm, c; \mathfrak{a}, L_0; \mathcal{K}) \cdot (1 + O(\sqrt{\eta(f, m, c)} \cdot |\log \eta(f, m, c)|)). \quad (4.10)$$

Поэтому по крайней мере для одного числа i имеет место как (4.8), так и (4.10). Но левые части (4.8) и (4.10) равны. Вспоминая определение γ (см. лемму 2), получаем отсюда (4.2).

Следствие. В условиях теоремы 1

$$r(f, m, c; \mathfrak{a}, \mathfrak{b}) = \\ = \frac{r(f, m, c)}{n(\mathfrak{a}')^2 \prod_{\mathfrak{p} \mid \mathfrak{a}'} (1 + \chi(\mathfrak{p})n(\mathfrak{p})^{-1})} (1 + O(\sqrt{\eta(f, m, c)} \cdot |\log \eta(f, m, c)|)).$$

ЛЕММА 5.

$$r(f, m, c) = \tilde{r}(\text{Spr } f, m, c) (1 + O(\psi)), \quad (4.11)$$

где $\psi = \sqrt{\eta(\text{Spr } f, m, c)} \cdot |\log \eta(\text{Spr } f, m, c)|$; постоянная в знаке O зависит только от K и рода f .

Доказательство. В первой половине нашего доказательства мы фактически повторим доказательство сильной теоремы об аппроксимации для поворотов (см. [17], 104:4 и § 57С), несколько уточнив результат. Детали легко уточнить по [17]. Итак, возьмем такой набор $\{f_1, \dots, f_k\}$ представителей классов из спинорного ряда f , что f переводится в f_i , $i=1, \dots, k$, подстановкой (A_i) с коэффициентами из K , $\det(A_i) = 1$. Как и в § 2, мы отождествим кватернионные алгебры, отвечающие f_i , с \mathcal{A} посредством изоморфизма

$$\begin{pmatrix} i'_1 \\ i'_2 \\ i'_3 \end{pmatrix} = (A_i) \begin{pmatrix} i_1 \\ i_2 \\ i_3 \end{pmatrix}.$$

Из вида изоморфизма и формулы (2.1) следует, что свободные \mathfrak{o} -решетки $\mathcal{V}_{f_1}, \dots, \mathcal{V}_{f_k}$ в подпространстве векторов алгебры \mathcal{A} с квадратичной функцией $d^{-1}N$ стандартным образом (см. [17], § 82В) отвечают формам f_1, \dots, f_k . Если обозначить через α_- автометрию этого пространства, меняющую знак у всех векторов, а через α_X — автометрию $L \rightarrow XLX^{-1}$, то любая симметрия τ_L запишется в виде $\tau_L = \alpha_- \alpha_L$. Поэтому α_X , $X \in \mathcal{A}$, исчерпывают все автометрии этого пространства, и для спинорной нормы θ справедливо равенство $\theta(\alpha_X) = N(X) (K^*)^2$. Точно так же все автометрии K_p -пополнения этого пространства исчерпываются α_X , $X \in \mathcal{A}_p$, и для спинорной нормы справедлива формула $\theta(\alpha_X) = N(X) (K_p^*)^2$. Положим $g = f_1$. Поскольку формы f_i принадлежат спинорному роду g , по определению спинорной родственности для любого i найдутся такие кватернионы $X(i) \in \mathcal{A}$ и $X_p(i) \in \mathcal{A}_p$, что $N(X_p(i)) \in (K_p^*)^2$ и $\mathcal{V}_{g,p} = \alpha_{X_p(i)} \alpha_{X(i)} \mathcal{V}_{f_i,p}$ для всех p . Так как для всякого $X \in \mathcal{A}$ α_X продолжается до автоморфизма всей алгебры \mathcal{A} $\alpha_X: Y \rightarrow XYX^{-1}$, то кольца $\mathcal{O}'_{f_i} = \alpha_{X(i)} \mathcal{O}_{f_i}$ с решетками векторов $\mathcal{V}'_{f_i} = \alpha_{X(i)} \mathcal{V}_{f_i}$ также соответствуют формам f_i и получаются просто при ином выборе подстановки, переводящей

f в f_i . Обозначим через P множество простых идеалов \mathfrak{p} , для которых $\mathcal{V}'_{i,\mathfrak{p}} \neq \mathcal{V}_{g,\mathfrak{p}}$ хотя бы для одного i . Множество P конечно (см. [17], 81 : 11). Так как умножение X на числа из K^* не меняет α_x , мы можем считать, что для всех i и $\mathfrak{p} \in P$ кватернионы $X_{\mathfrak{p}}(i)$ принадлежат $\mathcal{V}'_{i,\mathfrak{p}}$ и имеют одну и ту же норму $a^2 \in (\mathfrak{o})^2$.

Пусть \mathfrak{p}_0 — простой идеал наименьшей нормы со свойствами $\mathfrak{p}_0 \nmid d$, $\mathfrak{p}_0 \notin P$. Лемма 30 показывает, что если число t достаточно велико, $(s) = \mathfrak{p}_0^{ht}$, то для любого i найдется кватернион $Z(i)$ со свойствами:

$$\begin{cases} N(Z(i)) = a^2 s^2, & Z(i) \in \mathcal{O}'_{f_i} \text{ и в кольце } \mathcal{O}'_{f_i} \\ \mathfrak{p}_0 \nmid c(Z(i)), & Z(i) \equiv sX_{\mathfrak{p}}(i) \pmod{a^2} \text{ для } \mathfrak{p} \in P. \end{cases} \quad (4.12)$$

Тогда $\mathcal{O}''_{f_i} = \alpha_{Z(i)} \mathcal{O}'_{f_i}$ и $\mathcal{V}''_{f_i} = \alpha_{Z(i)} \mathcal{V}'_{f_i}$ снова отвечают формам f_i и

$$\mathcal{V}''_{f_i \mathfrak{p}_0} = Z(i) \mathcal{V}_{g, \mathfrak{p}_0} Z^{-1}(i), \quad \mathcal{V}''_{f_i, \mathfrak{p}} = \mathcal{V}_{g, \mathfrak{p}} \text{ для } \mathfrak{p} \neq \mathfrak{p}_0. \quad (4.13)$$

Действительно, первое равенство следует из определения \mathcal{V}''_{f_i} и того факта, что $\mathcal{V}'_{f_i, \mathfrak{p}_0} = \mathcal{V}_{g, \mathfrak{p}_0}$ в силу определения \mathfrak{p}_0 . Докажем второе равенство. Пусть $\mathfrak{p} \notin P$. Тогда $\mathcal{V}''_{f_i, \mathfrak{p}} = \mathcal{V}_{g, \mathfrak{p}}$, и (4.13) следует из (4.12), так как $Z(i) \in \mathcal{O}'_{f_i}$ и $\mathfrak{p} \nmid N(Z(i))$. Пусть $\mathfrak{p} \in P$. Тогда в силу (4.12) $Z(i)^{-1} X_{\mathfrak{p}}(i)$ и $X_{\mathfrak{p}}(i)^{-1} Z(i)$ принадлежат $\mathcal{O}'_{f_i, \mathfrak{p}}$, а значит, $\mathcal{V}''_{f_i, \mathfrak{p}} = \alpha_{Z(i)} \mathcal{V}'_{f_i, \mathfrak{p}} = \alpha_{X_{\mathfrak{p}}(i)} \mathcal{V}'_{f_i, \mathfrak{p}} = \mathcal{V}_{g, \mathfrak{p}}$. Заметим, что (4.13) почти эквивалентно сильной теореме об аппроксимации. Важное для нас усиление состоит в том, что степень \mathfrak{p}_0 , входящая в $N(Z(i))$, не зависит от i , и в силу условий (4.12), (4.13) и $\mathcal{O}'_{f_i, \mathfrak{p}_0} = \mathcal{O}_{g, \mathfrak{p}_0}$ как в $\mathcal{O}''_{f_i, \mathfrak{p}_0}$, так и в $\mathcal{O}_{g, \mathfrak{p}_0}$ $c(Z(i)) = c_{\mathfrak{p}_0}$.

Для каждого i рассмотрим множество $\mathcal{L}(i)$, состоящее из векторов $L \in \mathcal{A}$ со свойствами:

$$N(L) = dms^4, \quad c(L) = cs^2 \text{ в } \mathcal{O}''_{f_i}, \quad c(L) = c \text{ в } \mathcal{O}_g.$$

Рассмотрим $\mathcal{L}(i)$ относительно кольца \mathcal{O}''_{f_i} . Пусть $N(L) = dms^4$, $c(L) = cs^2$ в \mathcal{O}''_{f_i} . В силу (4.13) $c(L) = c$ в \mathcal{O}_g тогда и только тогда, когда $c(Z(i)LZ(i)^{-1}) = c$ в $\mathcal{O}''_{f_i, \mathfrak{p}_0}$, т. е. когда $Z(i)L\overline{Z(i)} \equiv 0 \pmod{\mathfrak{p}_0 c(L)}$. Если $\mathfrak{p}_0 \mid mc^{-2}$, то в силу следствия 3 леммы 11 $Z(i)L\overline{Z(i)} \equiv 0 \pmod{\mathfrak{p}_0 c(L)}$ тогда и только тогда, когда L принадлежит тому же классу подобия $(\text{mod } \mathfrak{p}_0)$, что и $Z(i)$. Учитывая это и лемму 25, получаем по лемме 4:

$$\# \mathcal{L}(i) = \frac{1 - \chi(\mathfrak{p}_0) n(\mathfrak{p}_0)^{-1}}{1 + n(\mathfrak{p}_0)^{-1}} r(f_i, m, c) (1 + O(\sqrt{\eta(f_i, m, c)} |\log \eta(f_i, m, c)|)), \quad (4.14)$$

поскольку, очевидно, $r(f_i, ms^4, cs^2) = r(f_i, m, c)$. Теперь рассмотрим $\mathcal{L}(i)$ относительно \mathcal{O}_g . Пусть $N(L) = dms^4$, $c(L) = c$ в \mathcal{O}_g . Снова учитывая (4.13), получаем, что $c(L) = cs^2$ в \mathcal{O}''_{f_i} тогда и только тогда, когда $c(Z(i)^{-1} LZ(i)) = cs^2$ в $\mathcal{O}_{g, \mathfrak{p}_0}$, т. е. когда $\overline{Z(i)} LZ(i) \equiv 0 \pmod{cs^4}$. По лемме 14 это эквивалентно тому, что L принадлежит тому же классу подо-

бия (mod s^2), что и $\overline{Z}(i)$. Поэтому по лемме 4

$$\# \mathcal{L}(i) = \frac{r(g, ms^4, c)}{n(s^2)(1+n(p_0)^{-1})} (1 + O(\sqrt{\eta(g, ms^4, c) \cdot |\log \eta(g, ms^4, c)|})). \quad (4.15)$$

Из определения $\tilde{r}(\text{Spr } f, m, c)$ следует, что по крайней мере для одной формы f_{i_0}

$$r(f_{i_0}, m, c) \geq \tilde{r}(\text{Spr } f, m, c).$$

Тогда остаточный член в (4.14) для $i=i_0$ будет $O(\psi) \geq -1/2$ (иначе (4.11) тривиальна), и, значит,

$$r(g, ms^4, c) \geq \# \mathcal{L}(i_0) \geq \frac{1}{8} \tilde{r}(\text{Spr } f, m, c).$$

Поэтому остаточный член в (4.15) также будет $O(\psi) \geq -1/2$, и, значит, для всех $i=1, \dots, k$

$$r(f_i, m, c) \geq \# \mathcal{L}(i) \geq \kappa_1(s) \cdot \tilde{r}(\text{Spr } f, m, c). \quad (4.16)$$

Поскольку система представителей $g=f_1, f_2, \dots, f_k$, а значит, и число s , фиксированы и зависят только от спинорного рода f , из (4.16) следует, что остаточные члены в (4.14) будут $O(\psi)$ для всех $i=1, \dots, k$. Сравнивая (4.14) и (4.15), выводим отсюда, что

$$r(f_i, m, c) = \kappa_2(\text{Spr } f, m, c) \cdot (1 + O(\psi)) \quad (4.17)$$

для всех $i=1, \dots, k$. Подставляя эти формулы в определение $\tilde{r}(\text{Spr } f, m, c)$, получим:

$$\kappa_2(\text{Spr } f, m, c) = \tilde{r}(\text{Spr } f, m, c) \cdot (1 + O(\psi)),$$

что вместе с (4.17) дает (4.11). Лемма 5 доказана.

Для завершения доказательства теоремы 1 заметим, что если $\tilde{r}(\text{Spr } f, m, c) = 0$, то, очевидно, и $r(f, m, c; a, b) = 0$, так что формула (1.3) тривиальна. Если же $\tilde{r}(\text{Spr } f, m, c) \neq 0$, то (1.3) следует из леммы 5, леммы 37 и следствия к лемме 4.

§ 5. «Ключевая лемма» метода

Этот раздел посвящен доказательству леммы 6, являющейся основой для всех построений § 3. Фактически лемма дает оценку сверху для числа решений одной задачи типа (1.1) для очень широкого интервала значений нормы модуля a . В предыдущих разделах было показано, как отсюда можно вывести асимптотическую формулу для числа решений (1.1) в случае модуля достаточно малой нормы.

Лемма 6 является обобщением на случай алгебраических числовых полей предложения 4.3 статьи [10], которое, в свою очередь, является обобщением лемм 1 и 2 гл. V монографии [8]. Представленное доказательство отличается от доказательства, изложенного в [10], в основном техническими деталями, связанными со спецификой алгебраического случая. Поскольку эти детали только затемняют идею доказательства, мы советуем первоначально обратиться к статье [10].

Оценка леммы 6 усилена по сравнению с предыдущими работами. Это усиление получается автоматически за счет применения лучших оценок сумм, содержащих τ -функцию (см. лемму 36) и никак не связано с

методом доказательства. Исключительно ради упрощения формулировки и доказательства мы предполагаем, что $(mc^{-2}, g) = 0$ и $n(g) \leq n(mc^{-2})^{1/5}$ (вместо $n(g) \leq n(mc^{-2})^{1/2-\epsilon}$).

ЛЕММА 6. Пусть $(g, d) = 0$, $\{L_1, \dots, L_r\} \subset \mathcal{V}_p^\circ$, $N(L_i) = dm$, $c(L_i) = c$, $i = 1, \dots, r$; $(mc^{-2}, g) = 0$, $n(g) \leq n(mc^{-2})^{1/5}$; $l \in c$, $g^2 \mid (l^2 + dm)$. Тогда кватернионы $l + L_i$, $i = 1, \dots, r$, лежат в

$$\geq \kappa_1 \cdot n(g) \frac{r^2}{n(mc^{-2})} \tau(g)^{-13} (\log n(mc^{-2}))^{-\kappa_2} \quad (5.1)$$

классах подобия $(\text{mod } g)$.

Доказательство. Мы будем отождествлять поле K с его образом при стандартном вложении $x \rightarrow (x^{(1)}, \dots, x^{(n)})$ K в \mathbf{R}^n с покомпонентным сложением и умножением. H — часть стандартной фундаментальной области поля K (см. [2], гл. V, § 1), лежащая в конусе $\mathbf{R}_+^n = \{x \in \mathbf{R}^n \mid x_i > 0, i = 1, \dots, n\}$. $H_2 = \{y = x^2 \mid x \in H\}$ — фундаментальная область для \mathbf{R}_+^n относительно группы квадратов единиц.

Заменяя все векторы L_i на sL_i , а l — на sl , $s \in K$, сведем лемму к случаю, когда $n(c) \leq \kappa_3$. Заменяя l по модулю cg , добьемся, чтобы

$$(l^2 + dm, dm) = c^2g. \quad (5.2)$$

Это можно сделать ввиду условия $(dmc^{-2}, g) = 0$. Такая замена не меняет классов подобия $(\text{mod } g)$, содержащих кватернионы $l + L_i$.

1°. Назовем два вектора L_1 и L_2 нормы dm и делителя c взаимными, если кватернионы $l + L_1$ и $l + L_2$ подобны $(\text{mod } g)$. Мы докажем далее, что число пар взаимных векторов в \mathcal{V}_f°

$$\leq \kappa_4 \cdot \frac{n(m)}{n(g)} \tau(g)^{13} (\log n(m))^{\kappa_5}. \quad (5.3)$$

Отсюда сразу будет следовать (5.1). Действительно, пусть $\mathcal{G}_1, \dots, \mathcal{G}_w$ — классы подобия $(\text{mod } g)$, содержащие все кватернионы $l + L_i$,

$i = 1, \dots, r$. Пусть $v_i = \#\{L = L_1, \dots, L_r \mid l + L \in \mathcal{G}_i\}$. Тогда $\sum_{i=1}^w v_i = r$.

С другой стороны, из векторов L_1, \dots, L_r можно составить $\sum_{i=1}^w v_i^2$ пар взаимных векторов. Оценка (5.1) следует из (5.3) и неравенства Коши

$$r^2 = \left(\sum_{i=1}^w v_i \right)^2 \leq w \cdot \sum_{i=1}^w v_i^2$$

(напомним, что $n(c) \leq \kappa_3$).

2°. Итак, доказываем (5.3). Пусть L_1 и L_2 взаимны, т. е.

$$\begin{cases} l + L_1 = V_1, & l + L_2 = V_2, & c(V_1) = c(V_2) = c, \\ N(V_1) = N(V_2) = l^2 + dm, & V_1 \bar{V}_2 \equiv 0 \pmod{c^2g}. \end{cases} \quad (5.4)$$

По лемме 26 найдется такой кватернион U , что

$$\begin{cases} L_1 U = -U L_2, & c(U) = c_1, & n(c_1) \leq \kappa_3, \\ N(U) = c_1^2 b u, & (u, dmN(V_2)) = 0, & b \mid 4d^4. \end{cases} \quad (5.5)$$

Положим $A' = UV_2$. В силу (5.2), (5.4), (5.5) и леммы 11

$$\begin{cases} c(A') = cc_1, & N(A') = a', & (a') = c^2c_1^2da'g, \\ (a', dm) = \mathfrak{o}; & A'\bar{V}_1 \equiv A'\bar{V}_2 \equiv 0 \pmod{c^2c_1g}, \end{cases} \quad (5.6)$$

$$L_1A' = -A'L_2. \quad (5.7)$$

Поэтому $\bar{A}'L_1A' = -a'L_2 \equiv 0 \pmod{c^3c_1^2a'}$, и в силу леммы 17

$$\bar{A}'(b' + L_1) \equiv 0 \pmod{c^2c_1a'}, \quad b' \in \mathfrak{c}. \quad (5.8)$$

Возьмем число $g \in \mathfrak{o}$ со свойствами:

$$(g) = \mathfrak{c}_1 b r g, \quad n(r) \leq \kappa_3.$$

Тогда из (5.6), (5.8) и леммы 11 следует, что

$$g \cdot (b' + L_1) = A'\bar{C}', \quad (5.9)$$

где

$$C' \in \mathcal{O}', \quad g|N(C') = c', \quad C'\bar{V}_1 \equiv C'\bar{V}_2 \equiv 0 \pmod{cg}. \quad (5.10)$$

Из (5.7) и (5.9) получаем:

$$g \cdot (b' - L_2) = A'^{-1}g(b' + L_1)A' = \bar{C}'A', \quad (5.11)$$

$$L_1C' = \left(\frac{1}{g}A'\bar{C}' - b'\right)C' = C' \left(\frac{1}{g}\bar{C}'A' - b'\right) = -C'L_2.$$

Ввиду (5.9) вполне положительная бинарная форма $\varphi'(x, y) = -N(A'x + C'y) = a'x^2 + 2gb'xy + c'y^2$ имеет определитель $N(gL_1) = g^2dm$. Кроме того, $g|(a', gb', c')$ и в силу (5.6) $n((a', gb', c')) \leq \kappa_6 \cdot n(g)$. По лемме 32 найдется невырожденная подстановка

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}, \quad \alpha_{ij} \in \mathfrak{o},$$

переводящая форму φ' в форму $\varphi(x, y) = ax^2 + 2bxy + cy^2$, для которой $|n(\det(\alpha_{ij}))| \leq \kappa_7$, $g^2dm \cdot (\det(\alpha_{ij}))^2 \in H_2$, и, значит, ввиду сказанного выше,

$$\begin{cases} g|(a, b, c), & n((a, b, c)) \leq \kappa_8 \cdot n(g), \\ \Delta = ac - b^2 = g_1m \in H_2, & g^2|g_1, \quad |n(g_1)| \leq \kappa_9 \cdot n(g^2), \end{cases} \quad (5.12)$$

а также

$$a \in H_2, \quad n(a) \leq \kappa_{10} \cdot n(g) \cdot n(m)^{1/2}, \quad b \in a \cdot \mathcal{P}, \quad (5.13)$$

где \mathcal{P} — фиксированный основной параллелепипед решетки \mathfrak{o} в \mathbf{R}^n . Для $c = a^{-1}(\Delta + b^2)$ получаем с учетом (5.12) и (5.13):

$$c \leq \kappa_{11} \cdot n(g^2ma^{-1})^{1/n}. \quad (5.14)$$

Положим

$$A = \alpha_{11}A' + \alpha_{21}C', \quad C = \alpha_{12}A' + \alpha_{22}C'. \quad (5.15)$$

Тогда с учетом (5.9) получим:

$$N(A) = a, \quad N(C) = c, \quad b + g \cdot \det(\alpha_{ij}) \cdot L_1 = A\bar{C}, \quad (5.16)$$

а в силу (5.6), (5.10), (5.7) и (5.11)

$$A\bar{V}_1 \equiv A\bar{V}_2 \equiv C\bar{V}_1 \equiv C\bar{V}_2 \equiv 0 \pmod{cg}, \quad (5.17)$$

$$L_1A = -AL_2, \quad L_1C = -CL_2. \quad (5.18)$$

Поэтому $V_1 A = lA + L_1 A = Al - AL_2 = A\bar{V}_2 \equiv 0 \pmod{\mathfrak{g}}$. Поскольку в силу (5.17) $V_1 \bar{A} \equiv 0 \pmod{\mathfrak{g}}$, получаем, что $V_1 \cdot 2Sc(A) \equiv 0 \pmod{\mathfrak{g}}$, и так как $\mathfrak{c}(V_1) = \mathfrak{c}$, то

$$Sc(A) \equiv 0 \pmod{\mathfrak{g}}.$$

Аналогично $Sc(C) \equiv 0 \pmod{\mathfrak{g}}$. Пусть

$$A = (a_0, a_1, a_2, a_3), \quad C = (c_0, c_1, c_2, c_3).$$

Тогда с учетом (2.1), (5.14) и (5.16) получим:

$$a_0, c_0 \in \mathfrak{g}, \quad a_0^2 \leq a, \quad c_0^2 \leq c \prec \kappa_{11} \cdot n (\mathfrak{g}^2 m a^{-1})^{1/n}. \quad (5.19)$$

Поскольку в силу (5.15) и определения формы φ'

$$\begin{aligned} \varphi(x, y) &= N(Ax + Cy) = \\ &= (a_0 x + c_0 y)^2 + d \cdot f(a_1 x + c_1 y, a_2 x + c_2 y, a_3 x + c_3 y), \end{aligned}$$

мы имеем представление

$$\begin{aligned} \psi(x, y) &= (a - a_0^2) x^2 + 2(b - a_0 c_0) xy + (c - c_0^2) y^2 = \\ &= d \cdot f(a_1 x + c_1 y, a_2 x + c_2 y, a_3 x + c_3 y) \end{aligned} \quad (5.20)$$

бинарной формы ψ тернарной формой $d \cdot f$. Поскольку в силу (5.16), (5.18) и (5.12) $A\bar{C} \equiv \bar{C}A \equiv 0 \pmod{\mathfrak{g}}$, по лемме 15

$$a_1 c_2 - a_2 c_1 \equiv a_1 c_3 - a_3 c_1 \equiv a_2 c_3 - a_3 c_2 \equiv 0 \pmod{\mathfrak{g}}. \quad (5.21)$$

3°. Определитель формы ψ равен нулю тогда и только тогда, когда

$$a_1 c_2 - a_2 c_1 = a_1 c_3 - a_3 c_1 = a_2 c_3 - a_3 c_2 = 0,$$

т. е. когда $A = a_0 + \alpha L$, $C = c_0 + \beta L$, $\alpha, \beta \in K$. Тогда в силу (5.16) и (5.18) $L_1 = \gamma L$, $L_2 = L_1$, т. е. пара L_1, L_2 тривиальна. Число r' таких пар равно числу векторов нормы dm и делителя \mathfrak{c} , т. е. $r' = r(f, m, \mathfrak{c})$. Используя формулу Зигеля для числа представлений родом f [19] и верхнюю оценку теоремы Зигеля — Брауэра ([16], гл. XVI, лемма 2), получаем:

$$r(f, m, \mathfrak{c}) \leq \kappa_{12} \cdot n(m)^{1/2} \cdot L(-dm, \mathfrak{c}) \leq \kappa_{13}(\varepsilon) \cdot n(m)^{1/2 + \varepsilon},$$

т. е. для r' справедлива оценка (5.3). Отметим, что это неравенство можно доказать и элементарно. Дадим набросок возможного доказательства. Пусть $L_1, \dots, L_{r'}$ — все векторы нормы dm и делителя \mathfrak{c} . Применяя результаты п. 2° для $\mathfrak{g} = \mathfrak{o}$, получим, что каждому вектору L_i соответствуют числа $a, b, c \in \mathfrak{o}$ с условиями:

$$\begin{cases} \Delta = ac - b^2 = g_1 m \in H_2, & |n(g_1)| \leq \kappa_9, \\ a \in H_2, & n(a) \leq \kappa_{10} \cdot n(m)^{1/2}, \quad b \in a \cdot \mathfrak{P} \end{cases} \quad (5.22)$$

и кватернионы $A, C \in \mathcal{O}_f$ с условиями:

$$N(A) = a, \quad N(C) = c, \quad b + tL_i = A\bar{C}, \quad |n(t)| \leq \kappa_{14}, \quad L_i A = -AL_i.$$

Можно показать и обратное, т. е. что каждому набору чисел a, b, c с условиями (5.22) соответствует $\leq \kappa_{15}$ векторов L_i (ср. [8], гл. IV, замечание 29). Если $(a, d) = \mathfrak{o}$, то это получается совсем просто: из леммы 11 следует, что имеется $\leq \kappa_{15}$ кватернионов A с условиями $A \setminus (b + tL_i)$, $N(A) = a$, и вектор L_i однозначно определяется по A в силу условия $L_i A = -AL_i$. Число наборов a, b, c с условием (5.22) оценивается так же, как в п. 6°. При этом получим:

$$r' \leq \kappa_{16} \cdot n(m)^{1/2} (\log n(m))^{\kappa_{17}}.$$

4°. Итак, осталось получить оценку (5.3) для числа нетривиальных пар взаимных векторов L_1, L_2 . Формулы (5.16) и (5.18) позволяют с точностью до знака восстановить пару L_1, L_2 по паре кватернионов A, C . Кроме того, нетривиальным парам соответствуют невырожденные формы ψ (см. п. 3°). Поэтому число нетривиальных пар взаимных векторов не превосходит удвоенного числа представлений (5.20) с условием (5.21), когда a, b, c, a_0 и c_0 пробегают все числа с условиями (5.12), (5.13), (5.19) и форма ψ невырождена.

5°. Покажем, что число таких представлений при фиксированных a, b, c

$$\leq \kappa_{18} \cdot n(ma^{-1})^{1/2} \cdot \max \left\{ \frac{n(a)^{1/2}}{n(g)}, 1 \right\} \tau(a)^4 \tau(g^8) (\log n(m))^{\kappa_{19}}. \quad (5.23)$$

Действительно, определитель формы ψ равен $\Delta' = \Delta - (ac_0^2 - 2bc_0a_0 + ca_0^2)$. В силу (5.12) $(\Delta) = g^2 \cdot (m)c^{-2}\tau_2$, где $n(\tau_2) \leq \kappa_{20}$. Мы можем считать, что для всех $\mathfrak{p} | g$ будет $n(\mathfrak{p}^{vp(g)}) > \kappa_{20}$. (Если это не так, то g можно представить в виде $g = g_1 g_2$, где для g_1 требуемое свойство выполнено, а $n(g_2) \leq \kappa_{21}$. Тогда получим (5.1) для g_1 вместо g и воспользуемся леммой 22.) Поскольку $a, b, c, a_0, c_0 \in \mathfrak{g}$ и $(g, m\tau^{-2}) = 0$, отсюда следует, что $(\Delta' g^{-2}, g) | \tau_2$. Если $a - a_0^2 \equiv b - a_0 c_0 \equiv c - c_0^2 \equiv 0 \pmod{g a^2}$, то $\Delta = ac - b^2 \equiv 0 \pmod{g^2 a^2}$. Поэтому в силу леммы 33 искомое число представлений будет

$$\leq \kappa_{21} \sum_{a | \Delta g^{-2}} n(a) \sum_{\substack{a_0, c_0 \in \mathfrak{g}, a_0^2 < a, c_0^2 < \kappa_{11} \cdot n(g^2 m a^{-1})^{1/n}, \\ \Delta' \neq 0, a - a_0^2 \equiv b - a_0 c_0 \equiv c - c_0^2 \equiv 0 \pmod{g a^2}}} \tau(\Delta')^4 \quad (5.24)$$

(поскольку если $a_0^2 = a$, то $\Delta' = 0$).

Ввиду (5.12) система сравнений

$$a_0 \equiv c_0 \equiv 0 \pmod{g}, \quad a - a_0^2 \equiv b - a_0 c_0 \equiv c - c_0^2 \equiv 0 \pmod{g a^2}$$

имеет $\leq \kappa_8 \cdot \tau(a^2)$ решений $\pmod{g a^2}$. Кроме того, в силу (5.12) — (5.14) в области суммирования $n(\Delta') \leq \kappa_{22} \cdot n(g^2 m) \leq \kappa_{22} \cdot n(m)^2$, так что при $n(a) \leq \kappa_{23} \cdot n(m)^{1/40}$ для суммы по c_0 выполнены условия леммы 36 с $g' = ga^2$, $N = \kappa_{24} \cdot n(g^2 m a^{-1})^{1/2}$ и $\alpha = 30$. Поскольку $(a, 2ba_0, \Delta - ca_0^2) | a$, применение леммы 36 и оценок лемм 34, 35 дает:

$$\begin{aligned} & \sum_{n(a) \leq \kappa_{23} \cdot n(m)^{1/40}} n(a) \cdot \sum \tau(\Delta')^4 \leq \\ & \leq \sum_{n(a) \leq \kappa_{23} \cdot n(m)^{1/40}} n(a) \cdot \kappa_8 \tau(a^2) \cdot \kappa_{25} \max \left\{ \frac{n(a)^{1/2}}{n(g)}, 1 \right\} \times \\ & \quad \times \frac{n(g^2 m a^{-1})^{1/2}}{n(g a^2)} \tau(a)^4 \tau(g a^2)^8 \left(\log \frac{n(g^2 m a^{-1})^{1/2}}{n(g a^2)} \right)^{\kappa_{26}} \leq \\ & \leq \kappa_{27} \cdot n(m a^{-1})^{1/2} \max \left\{ \frac{n(a)^{1/2}}{n(g)}, 1 \right\} \tau(a)^4 \tau(g)^8 (\log n(m))^{\kappa_{28}}. \quad (5.25) \end{aligned}$$

Из условий $g a^2 | (a - a_0^2)$, $a_0^2 < a$ следует, что $n(g a^2) \leq n(a - a_0^2) \leq n(a) \leq \kappa_{10} \cdot n(g) n(m)^{1/2}$, т. е. $n(a) \leq \kappa_{29} \cdot n(m)^{1/4}$. В силу (5.13) $n(a m^{-1}) \leq \kappa_{30} \cdot$

$\cdot n(g^2 a^{-1})$. Учитывая эти оценки, условия (5.12) и $n(g) \leq n(m)^{1/5}$ и применяя лемму 34 и оценку $\tau(m) \leq \kappa(\varepsilon) n(m)^\varepsilon$, получим:

$$\begin{aligned} & \sum_{a \mid \Delta g^{-2}, n(a) \geq \kappa_{23} \cdot n(m)^{1/40}} n(a) \sum \tau(\Delta')^4 \leq \\ & \leq \sum_{\substack{a \mid \Delta g^{-2}, \\ \kappa_{23} \cdot n(m)^{1/40} \leq n(a) \leq \kappa_{20} \cdot n(m)^{1/4}}} n(a) \cdot \kappa_8 \tau(a^2) \cdot \kappa_{31} \cdot \left(\frac{1}{n(ga^2)} + \frac{1}{n(a)^{1/2}} \right) n(a)^{1/2} \times \\ & \quad \times \kappa_{31} \cdot \left(\frac{1}{n(ga^2)} + \frac{1}{n(g^2 ma^{-1})^{1/2}} \right) n(g^2 ma^{-1})^{1/2} \cdot \kappa_{32} \cdot n(m)^{1/50} \leq \\ & \leq \kappa_{33} \cdot n(mg^{-2})^{1/2} \cdot \left(n(m)^{-1/21} + \tau(m) n(m)^{-1/41} \frac{n(g)}{n(a)^{1/2}} + \right. \\ & \quad \left. + \tau(m) n(m)^{\frac{1}{4} + \frac{1}{40}} \frac{n(g)}{n(m)^{1/2}} \right) n(m)^{1/50} \leq \kappa_{34} \cdot n(ma^{-1})^{1/2} \max \left\{ \frac{n(a)^{1/2}}{n(g)}, 1 \right\}. \end{aligned} \quad (5.26)$$

Из (5.24) — (5.26) следует (5.23).

6°. Количество чисел Δ с условием (5.12) будет $\leq \kappa_{35}$. Для фиксированных $\Delta \in g^2$ и $a \in g$ количество чисел $b, c \in g$ с условиями $\Delta = ac - b^2$, $b \in a \cdot \mathcal{P}$ не превосходит числа решений $b \pmod{a}$ сравнения $b^2 \equiv -\Delta \pmod{ag}$, т. е.

$$\leq \kappa_{36} \cdot \tau(ag^{-1}) \prod_{p \mid (ag^{-1}, \Delta g^{-2})} n(p)^{\lceil v_p((ag^{-1}, \Delta g^{-2})/2) \rceil}.$$

Поэтому в силу п. 4° и (5.23) число нетривиальных пар взаимных векторов

$$\begin{aligned} & \leq \kappa_{37} \cdot \tau(g)^8 n(m)^{1/2} (\log n(m))^{\kappa_{19}} \times \\ & \times \sum_{m^2 \mid m} n(m) \cdot \sum_{\substack{a \in H_2, gm^2 \mid a, \\ n(a) \leq \kappa_{10} \cdot n(g)n(m)^{1/2}}} \tau(a)^5 \max \{n(g)^{-1}, n(a)^{-1/2}\}. \end{aligned}$$

Поскольку H_2 покрывается $\leq \kappa_{38}$ областями $e_i H$, где e_i — единицы K , то

$$\begin{aligned} & \sum_{\substack{a \in H_2, gm^2 \mid a, \\ n(a) \leq \kappa_{10} \cdot n(g)n(m)^{1/2}}} \tau(a)^5 \max \{n(g)^{-1}, n(a)^{-1/2}\} \leq \\ & \leq \kappa_{38} \cdot \sum_{\substack{gm^3 \mid a \\ n(a) \leq \kappa_{10} \cdot n(g)n(m)^{1/2}}} \tau(a)^5 \max \{n(g)^{-1}, n(a)^{-1/2}\}. \end{aligned}$$

Применяя лемму 35, получим:

$$\begin{aligned} & \sum_{m^2 \mid m} n(m) \cdot \sum_{\substack{gm^2 \mid a, \\ n(a) \leq n(g)^2}} \tau(a)^5 n(a)^{-1/2} \leq \tau(g)^5 n(g)^{-1/2} \times \\ & \times \sum_m \tau(m)^{10} \sum_{n(b) \leq n(g)n(m)^{-2}} \tau(b)^5 n(b)^{-1/2} \leq \kappa_{39} \cdot \tau(g)^5 n(g)^{-1/2} \times \\ & \times \sum_m \tau(m)^{10} n(g) n(m)^{-2} \leq \kappa_{40} \cdot \tau(g)^5 n(g)^{1/2} \leq \kappa_{41} \tau(g)^5 n(m)^{1/2} n(g)^{-1}. \end{aligned}$$

$$\begin{aligned}
& \sum_{m^2 | m} n(m) \sum_{\substack{gm^2 | a, \\ n(a) \leq \kappa_{10} \cdot n(g)n(m)^{1/2}}} \tau(a)^5 n(g)^{-1} \leq \\
& \leq \tau(g)^5 n(g)^{-1} \sum_{n(m) \leq n(m)} n(m) \tau(m)^{10} \sum_{n(b) \leq \kappa_{10} \cdot n(m)^{1/2} n(m)^{-2}} \tau(b)^5 \leq \\
& \leq \kappa_{42} \cdot \tau(g)^5 n(g)^{-1} \sum_{n(m) \leq n(m)} \tau(m)^{10} n(m)^{1/2} n(m)^{-1} (\log n(m))^{\kappa_{43}} \leq \\
& \leq \kappa_{44} \cdot \tau(g)^5 n(m)^{1/2} n(g)^{-1} (\log n(m))^{\kappa_{45}}.
\end{aligned}$$

Из приведенных оценок следует оценка (5.3) для числа нетривиальных пар взаимных векторов. Это заканчивает доказательство леммы 6.

§ 6. Арифметика кольца целых кватернионов \mathcal{O}_f

В этом параграфе будут доказаны свойства кольца целых кватернионов \mathcal{O}_f , использованные нами в предыдущих параграфах. Мы старались по возможности следовать изложению гл. IV монографии [8]. Отличия сводятся в основном к тому, что вместо сравнений по модулю числа рассматриваются сравнения по модулю идеала, а вместо примитивных кватернионов приходится рассматривать кватернионы с фиксированным делителем. Все локальные рассмотрения вообще не требуют изменений. Поэтому мы будем отмечать только те моменты доказательств, которые требуют наибольших изменений по сравнению с [8], гл. IV. Все кватернионы, рассматриваемые в этом разделе, — целые.

ЛЕММА 7. Пусть $\mathfrak{g}_1, \dots, \mathfrak{g}_k$ — попарно взаимно простые идеалы, $A_1, \dots, A_k \in \mathcal{O}_f$. Тогда найдется $X \in \mathcal{O}_f$, для которого

$$X \equiv A_i \pmod{\mathfrak{g}_i}, \quad i=1, \dots, k.$$

Доказательство. Следует из китайской теоремы об остатках (см. [16], § 4 гл. I).

ЛЕММА 8. $M=AM'V$ тогда и только тогда, когда $\overline{AM\overline{B}} \equiv 0 \pmod{N(A)N(B)}$.

ЛЕММА 9. Пусть $A, B \in \mathcal{O}_f$, $(g, N(A)) = 0$, $AB \equiv 0 \pmod{g}$. Тогда $B \equiv 0 \pmod{g}$.

ЛЕММА 10. Пусть $(g, d) = 0$, $A, B \in \mathcal{O}_f$, $g | N(B)$, $\mathfrak{c}(A\overline{B}) | u$. Тогда найдется $X \in \mathcal{O}_f$, для которого $N(A+XB) \equiv N(A) + u \pmod{g}$.

Доказательство. См. [8], замечание 6.

Следствие 1. В условиях леммы 10 найдется $X \in \mathcal{O}_f$, для которого $(N(A+XB), g) | (\mathfrak{c}(A\overline{B}), g)$.

Следствие 2. Пусть $(g, d) = 0$. Тогда для любого кватерниона A найдутся такие кватернионы $A' \equiv A \pmod{g}$ и $A'' \equiv A \pmod{\mathfrak{c}(A)g}$, что $(N(A'), g^2) | g \cdot (g, \mathfrak{c}(A))$ и $(N(A''), \mathfrak{c}(A)^2 g^2) | \mathfrak{c}(A)^2 g$.

Доказательство. Возьмем число $g \equiv 0$ со свойством $(g, g^2) = g$, применим следствие 1 с $B = g$ и g^2 вместо g и положим $A' = A + gX$. Возьмем $c \equiv 0$ со свойством $(c, \mathfrak{c}(A)g) = \mathfrak{c}(A)$, применим полученный результат к кватерниону $A_1 \equiv c^{-1}A \pmod{g}$ и положим $A'' = cA_1'$.

ЛЕММА 11. Пусть $(g, d) = 0$, $A\overline{B} \equiv 0 \pmod{\mathfrak{c}(A)\mathfrak{c}(B)g}$, $A\overline{C} \equiv 0 \pmod{\mathfrak{c}(A)\mathfrak{c}(C)g}$. Тогда $B\overline{C} \equiv 0 \pmod{\mathfrak{c}(B)\mathfrak{c}(C)g}$.

Доказательство. Пусть A'' — кватернион из следствия 2 леммы 10. Тогда $N(A'')B\bar{C} = \overline{(A''B)}(A''\bar{C}) \equiv 0 \pmod{\mathfrak{c}(B)\mathfrak{c}(C)g^2 \cdot \mathfrak{c}(A)^2}$ и, значит, $B\bar{C} \equiv 0 \pmod{\mathfrak{c}(B)\mathfrak{c}(C)g}$ в силу условий на A'' .

Следствие 1. *Отношение подобия $(\text{mod } g)$ есть отношение эквивалентности на множестве кватернионов A с условием $g | N(A)\mathfrak{c}(A)^{-2}$.*

Следствие 2. *Пусть \mathcal{G} — класс подобия $(\text{mod } g)$, $\mathcal{G}/A, \mathcal{G}/B, N(A) = N(B) = N, \mathfrak{c}(A) = \mathfrak{c}(B) = \mathfrak{c}$. Тогда $A = EB$, где E — единица кольца \mathcal{O}_f , $N(E) = 1$.*

Доказательство. В силу леммы 11 $A\bar{B} \equiv B\bar{A} \equiv 0 \pmod{\mathfrak{c}^2 \cdot N\mathfrak{c}^{-2}}$. Поэтому $E = AB^{-1} \in \mathcal{O}_f$, $E^{-1} = BA^{-1} \in \mathcal{O}_f$.

Следствие 3. *Пусть \mathcal{G} — класс подобия $(\text{mod } g)$, $AB \in \mathcal{G}$, $g | N(B)\mathfrak{c}(B)^{-2}$. Тогда $B \in \mathcal{G}$.*

Доказательство. Пусть $C \in \mathcal{G}$. Заменяя в лемме 11 A на AB , получаем требуемое соотношение.

ЛЕММА 12. *Каждый класс подобия $(\text{mod } g)$ содержит кватернион A со свойствами $(\mathfrak{c}(A), g) = \mathfrak{o}$, $(N(A), g^2) = g$.*

Доказательство. Пусть B принадлежит данному классу. Возьмем число $c \in \mathfrak{o}$ со свойством $(c, \mathfrak{c}(B)g) = \mathfrak{c}(B)$ и положим $A' \equiv c^{-1}B \pmod{g}$. Тогда A' принадлежит тому же классу подобия и $(\mathfrak{c}(A'), g) = \mathfrak{o}$. Теперь применим следствие 2 леммы 10.

ЛЕММА 13. *Пусть $(g_1, g_2, d) = \mathfrak{o}$, $g_1g_2 | N(M)\mathfrak{c}(M)^{-2}$, $AM \equiv 0 \pmod{\mathfrak{c}(A)\mathfrak{c}(M)g_1}$, $MB \equiv 0 \pmod{\mathfrak{c}(M)\mathfrak{c}(B)g_2}$. Тогда $AMB \equiv 0 \pmod{\mathfrak{c}(A)\mathfrak{c}(M)\mathfrak{c}(B)g_1g_2}$.*

Доказательство. Запишем $g_2 = g_2'g_2''$, где $(g_2', g_2'') = (g_1, g_2') = (d, g_2'') = \mathfrak{o}$. Тогда

$$AMB \equiv 0 \pmod{\mathfrak{c}(A)\mathfrak{c}(M)\mathfrak{c}(B)g_1g_2'}. \quad (6.1)$$

Далее, из условий леммы следует, что $M\overline{AM} \equiv 0 \pmod{\mathfrak{c}(A)\mathfrak{c}(M)^2g_1g_2''}$, $MB \equiv 0 \pmod{\mathfrak{c}(M)\mathfrak{c}(B)g_2''}$, $g_1\mathfrak{c}(A)\mathfrak{c}(M) | \mathfrak{c}(AM)$. Поэтому, применяя лемму 11, получим $AMB \equiv 0 \pmod{\mathfrak{c}(A)\mathfrak{c}(M)\mathfrak{c}(B)g_1g_2''}$. Ввиду (6.1) это доказывает лемму 13.

ЛЕММА 14. *Если $(g, d) = \mathfrak{o}$, $L \in \mathcal{V}_f$ и $g^2 | N(L)\mathfrak{c}(L)^{-2}$, то $\bar{Z}LZ \equiv 0 \pmod{\mathfrak{c}(L)\mathfrak{c}(Z)^2g^2}$ тогда и только тогда, когда $LZ \equiv 0 \pmod{\mathfrak{c}(L)\mathfrak{c}(Z)g}$.*

Доказательство. Так как $L \in \mathcal{V}_f$, то $LZ \equiv 0 \pmod{\mathfrak{c}(L)\mathfrak{c}(Z)g}$ тогда и только тогда, когда $\bar{Z}L \equiv 0 \pmod{\mathfrak{c}(L)\mathfrak{c}(Z)g}$. Поэтому необходимость первого условия следует из леммы 13, а достаточность — из следствия 3 леммы 11.

ЛЕММА 15. *Пусть $(g, d) = \mathfrak{o}$, $A\bar{B} \equiv B\bar{A} \equiv 0 \pmod{g}$. Тогда $aA + bB \equiv 0 \pmod{g}$, где $(a, g) = (\mathfrak{c}(B), g)$ и $(b, g) = (\mathfrak{c}(A), g)$.*

Доказательство. См. [8], доказательство замечания 10.

ЛЕММА 16. *Пусть $(g, d) = \mathfrak{o}$, $(\mathfrak{c}(A_1A_2)\mathfrak{c}(A_1)^{-1}\mathfrak{c}(A_2)^{-1}, g) = \mathfrak{o}$, $L \in \mathcal{V}_f$, $\mathfrak{c} | \mathfrak{c}(L)$, $A_1L \equiv 0 \pmod{\mathfrak{c} \cdot \mathfrak{c}(A_1)g}$, $LA_2 \equiv 0 \pmod{\mathfrak{c} \cdot \mathfrak{c}(A_2)g}$. Тогда $L \equiv 0 \pmod{g}$.*

Доказательство. Предположим противное. Тогда найдется такой простой идеал $\mathfrak{p} \nmid d$, что $\mathfrak{p}^k | \mathfrak{c}g$, $\mathfrak{p}^k \nmid \mathfrak{c}(L)$. Возьмем числа c_1 и c_2 с условиями $(c_1, \mathfrak{c}(A_1)\mathfrak{p}) = \mathfrak{c}(A_1)$, $(c_2, \mathfrak{c}(A_2)\mathfrak{p}) = \mathfrak{c}(A_2)$ и рассмотрим кватернионы $A_1' \equiv c_1^{-1}A_1 \pmod{\mathfrak{p}^k}$, $A_2' \equiv c_2^{-1}A_2 \pmod{\mathfrak{p}^k}$. Тогда из условий леммы следует, что $\mathfrak{p} \nmid \mathfrak{c}(A_1'A_2')$, $A_1'L \equiv LA_2' \equiv 0 \pmod{\mathfrak{p}^k}$. Так как $\mathfrak{p}^k \nmid \mathfrak{c}(L)$, отсюда следует, что $N(A_2') \equiv 0 \pmod{\mathfrak{p}}$. Поэтому в силу следствия 1 леммы 10

найдется такой кватернион X , что $\mathfrak{p} \nmid N(A_1' + X\bar{A}_2')$. Учитывая, что $L \in \mathcal{V}_{\mathfrak{f}}$, получим $(A_1' + X\bar{A}_2')L = A_1'L - X \cdot \bar{L}A_2' \equiv 0 \pmod{\mathfrak{p}^k}$, и в силу леммы 9 $L \equiv 0 \pmod{\mathfrak{p}^k}$, что противоречит первоначальному предположению.

ЛЕММА 17. Если $(g, d) = 0$ и $g \mid N(A)c(B)$, то $\bar{A}BA \equiv 0 \pmod{g}$ тогда и только тогда, когда $(u+B)A \equiv 0 \pmod{g \cdot c(A)^{-1}}$ для некоторого $u \in c(B)$.

Доказательство. Необходимость первого условия проверяется непосредственно. Докажем его достаточность. Пусть $\bar{A}BA \equiv 0 \pmod{g}$. Поскольку $(BA)\bar{A} = B \cdot N(A) \equiv 0 \pmod{g}$, из леммы 15 следует, что $u_1A + u_2BA \equiv 0 \pmod{g}$, $(u_1, g) \subset (c(A)c(B), g)$, $(u_2, g) = (c(A), g)$. Поэтому найдется число u со свойствами $u \equiv u_1u_2^{-1} \pmod{gc(A)^{-1}}$, $u \in c(B)$, которое и будет искомым.

ЛЕММА 18. Пусть $(g, d) = 0$, $A, B \in \mathcal{O}_{\mathfrak{f}}$, $\alpha: \mathcal{O}_{\mathfrak{f}} \rightarrow \mathcal{O}_{\mathfrak{f}}$ задается равенством $\alpha(X) = AXB$. Тогда найдутся такие два базиса X_1, \dots, X_4 и Y_1, \dots, Y_4 \mathfrak{o} -модуля $\mathcal{O}_{\mathfrak{f}}$, что $\alpha(X_i) \equiv c_i Y_i \pmod{g}$, где $(c_1, g) = (c_1c_2, g)$, $(c_2, g) = (c_1c_2 \cdot (n_1, n_2), g)$, $(c_3, g) = (c_1c_2n_1n_2 \cdot (n_1, n_2)^{-1}, g)$, $(c_4, g) = (c_1c_2n_1n_2, g)$; здесь $c_1 = c(A)$, $c_2 = c(B)$, $n_1 = N(A)c_1^{-2}$, $n_2 = N(B)c_2^{-2}$.

Доказательство. Непосредственно вычисляем н.о.д. миноров i -го порядка матрицы α по модулю g для $i=1, \dots, 4$ (см. [8, с. 123]) и применяем теорему об элементарных делителях.

ЛЕММА 19. Пусть \mathcal{G} — класс подобия \pmod{g} , $g \mid N(A)c(A)^{-2}$; $u \in \mathfrak{o}$, $(u, g) = 0$. Тогда найдется такой кватернион X , что $AX \in \mathcal{G}$, $N(X) \equiv u \pmod{g}$.

Доказательство. По лемме 12 найдется кватернион $G \in \mathcal{G}$ со свойствами $(c(G), g) = 0$, $(N(G), g^2) = g$. Возьмем такое $c \in \mathfrak{o}$, что $(c, c(A)g) = c(A)$, и $A' \equiv c^{-1}A \pmod{g}$. Тогда по лемме 18 найдется такой кватернион U , что $(c(\bar{A}'UG), g) = 0$. Поэтому по следствию 1 леммы 10 найдется такой кватернион $X = \bar{A}'U + ZG$, что $N(X) \equiv u \pmod{g}$. Тогда $AX\bar{G} \equiv 0 \pmod{c(A)g}$, а поскольку $(u, g) = 0$, то $(c(AX), g) = (c(A), g)$. Поэтому X будет искомым.

ЛЕММА 20. Пусть \mathcal{G}_1 — класс подобия $\pmod{g_1}$ слева, \mathcal{G}_2 — класс подобия $\pmod{g_2}$. Тогда число классов кватернионов $A \pmod{g_1g_2}$ с условиями $(c(A), g_1g_2) = 0$, $A \in \mathcal{G}_1$, $A \in \mathcal{G}_2$ равно

$$n(g_1g_2)^2 \prod_{\substack{\mathfrak{p} \mid g_1g_2 \\ \mathfrak{p} \nmid (g_1, g_2)}} (1 - n(\mathfrak{p})^{-2}) \cdot \prod_{\mathfrak{p} \mid (g_1, g_2)} (1 - n(\mathfrak{p})^{-1}).$$

Доказательство. В силу леммы 12 найдутся кватернионы $G_1 \in \mathcal{G}_1$ и $G_2 \in \mathcal{G}_2$ со свойствами $(c(G_1), g_1) = (c(G_2), g_2) = 0$, $(N(G_1), g_1^2) = g_1$, $(N(G_2), g_2^2) = g_2$. Тогда из леммы 13 следует, что если $(c(A), g_1g_2) = 0$, то условия $A \in \mathcal{G}_1$, $A \in \mathcal{G}_2$ равносильны сравнению $\bar{G}_1A\bar{G}_2 \equiv 0 \pmod{g_1g_2}$. Поэтому заключение леммы прямо следует из леммы 18.

ЛЕММА 21. Число классов подобия \pmod{g} равно $n(g) \prod_{\mathfrak{p} \mid g} (1 + n(\mathfrak{p})^{-1})$.

Доказательство. Каждый кватернион A с условиями $(c(A), g) = 0$, $g \mid N(A)$ содержится ровно в одном классе подобия \pmod{g} . Число классов $A \pmod{g}$ с указанным свойством будет $n(g)^3 \prod_{\mathfrak{p} \mid g} (1 - n(\mathfrak{p})^{-2}) \times$

$\times (1 + n(p)^{-1})$ (см. [19, лемма 57]). Учитывая лемму 20, получаем заключение леммы.

ЛЕММА 22. Пусть $(h, d) = 0$, $g|h$, \mathcal{G} — класс подобия $(\text{mod } g)$. Тогда число классов подобия $(\text{mod } h)$, содержащихся в \mathcal{G} , равно

$$\frac{n(h)}{n(g)} \prod_{p|h, p \nmid g} \left(1 + \frac{1}{n(p)}\right). \quad (6.2)$$

Доказательство. Сначала докажем (6.2) для случая, когда h — степень простого идеала. Пусть $h = p^i$, $g = p^k$. Применим индукцию по величине $i - k$. Для $i - k = 0$ (6.2) тривиальна. Пусть $i > k$. Возьмем (лемма 12) кватернион $G \in \mathcal{G}$ со свойствами $(N(G), h) = g$, $(c(G), h) = 0$. Тогда отображение $A \rightarrow A' \equiv AG^{-1} (\text{mod } p^{i-k})$ осуществляет взаимно однозначное соответствие между классами подобия $(\text{mod } h)$, содержащимися в \mathcal{G} , и классами подобия $(\text{mod } p^{i-k})$, которые не содержатся в том же классе подобия $(\text{mod } p)$, что и \bar{G} . В силу леммы 21 и индукционного предположения число таких классов будет

$$n(p^{i-k}) (1 + n(p)^{-1}) - n(p^{i-k}) n(p)^{-1} = n(p^{i-k})$$

(в случае $k = 0$ формула (6.2) совпадает с леммой 21). Для произвольного идеала h (6.2) выводится отсюда при помощи того простого замечания, что если $(g_1, g_2) = 0$, то каждый класс подобия $\mathcal{G} (\text{mod } g_1 g_2)$ является пересечением классов $(\text{mod } g_1)$ и $(\text{mod } g_2)$, содержащих \mathcal{G} , а в силу леммы 7 каждое такое пересечение не пусто.

ЛЕММА 23. Пусть $(a_1, dmc^{-2}) = 0$, $L_1, L_2 \in \mathcal{V}_f$, $(c(L_1), a_0 a_1) = (c(L_2), a_0 a_1) = (c, a_0 a_1) = a_0$, $N(L_1) \equiv N(L_2) \equiv dm (\text{mod } a_0^2 a_1)$, $s \equiv 0$, $(s, a_1) = 0$. Тогда

$$\begin{aligned} \# \{X (\text{mod } a_1) | N(X) \equiv s (\text{mod } a_1), XL_1 \equiv L_2 X (\text{mod } a_0 a_1)\} = \\ = n(a_1) \prod_{p|a_1} (1 - \chi(p) n(p)^{-1}), \end{aligned} \quad (6.3)$$

где $\chi(p)$ определено в § 1.

Доказательство. Повторяя рассуждения [10, лемма 3.16], покажем, что левая часть (6.3) равна числу решений сравнения $x^2 + dmc^{-2}y^2 \equiv us (\text{mod } a_1)$, где $(c, a_1) = c$, $(u, a_1) = 0$. В силу [19, лемма 56] это число равно правой части (6.3).

ЛЕММА 24. Пусть $(g, d) = 0$, $g|N(L)c(L)^{-2}$, $s \equiv 0$, $(s, g) = 0$, \mathcal{K} — класс подобия $(\text{mod } g)$. Тогда

$$\# \{X (\text{mod } g) | N(X) \equiv s (\text{mod } g), XL\bar{X} \in \mathcal{K}\} = n(g)^2 \prod_{p|g} (1 - n(p)^{-1}). \quad (6.4)$$

Доказательство. Покажем, что левая часть (6.4) не зависит от класса \mathcal{K} . Действительно, пусть \mathcal{K}_1 и \mathcal{K}_2 — два таких класса. В силу леммы 19 найдется кватернион A со свойствами $N(A) \equiv 1 (\text{mod } g)$, $\mathcal{K}_1 A = \mathcal{K}_2$. Тогда отображение $X \rightarrow AX$ осуществляет взаимно однозначное соответствие между множествами в левой части (6.4), отвечающими \mathcal{K}_1 и \mathcal{K}_2 . Поэтому (6.4) получается из формулы

$$\# \{X (\text{mod } g) | N(X) \equiv s (\text{mod } g)\} = n(g)^3 \prod_{p|g} (1 - n(p)^{-2})$$

(см. [19, лемма 56]) и леммы 21.

ЛЕММА 25. Пусть $g = \mathfrak{p}^k$, $(g, dmc^{-2}) = 0$, $(c(A), g) = 0$, $g | N(A)$. Тогда число классов векторов $L \pmod{cg}$ с условиями $(c(L), cg) = c$, $N(L) \equiv dm \pmod{c^2g}$, $AL\bar{A} \equiv 0 \pmod{cg}$ равно $n(g)(1 + \chi(\mathfrak{p}))$.

Доказательство. Ввиду леммы 17 $AL\bar{A} \equiv 0 \pmod{cg}$ тогда и только тогда, когда $A(l+L) \equiv 0 \pmod{cg}$ для некоторого $l \in c$. Отсюда следует, что $l^2 + dm \equiv 0 \pmod{c^2g}$ и число таких $l \pmod{cg}$ равно $1 + \chi(\mathfrak{p})$. Зафиксируем одно из таких l (если оно существует) и покажем, что

$$\# \{L \pmod{cg} \mid (c(L), cg) = c, N(L) \equiv dm \pmod{c^2g}, AL\bar{A} \equiv 0 \pmod{cg}\} \quad (6.5)$$

не зависит от A . Действительно, пусть A_1 и A_2 удовлетворяют условиям леммы. В силу леммы 19 найдется кватернион X со свойствами $N(X) \equiv 1 \pmod{g}$, $A_2 X \bar{A}_1 \equiv 0 \pmod{g}$. Тогда отображение $L \rightarrow XL\bar{X}$ осуществляет взаимно однозначное соответствие между множествами в (6.5), отвечающими A_1 и A_2 . Так как это множество однозначно соответствует классу подобия $(\text{mod } g)$, содержащему A , и

$$\# \{L \pmod{cg} \mid (c(L), cg) = c, N(L) \equiv dm \pmod{c^2g}\} = n(g)^2(1 + \chi(\mathfrak{p})n(\mathfrak{p})^{-1})$$

(см. [19, лемма 56]), то (6.5) равно $n(g)$ (так как $\chi(\mathfrak{p}) = 1$, если l существует). Отсюда следует заключение леммы, поскольку разным $l \pmod{cg}$ соответствуют разные $L \pmod{cg}$ в (6.5).

ЛЕММА 26. Пусть $L_1, L_2 \in \mathcal{Y}_j^0$, $c(L_1) = c(L_2) = c$, $N(L_1) = N(L_2)$, g — произвольный идеал. Тогда найдется такой кватернион U , что $(N(U)) = c(U)^2 \mathfrak{d}u$, $n(c(U)) \leq \kappa$, $\mathfrak{d} | 4d^4$, $(u, dg) = 0$ и $L_1 U = U L_2$.

Доказательство. Домножая, если нужно, L_1 и L_2 на $a \in K$, мы можем считать, что $(c, dg) = 0$. Повторяя рассуждения леммы 3.15 статьи [10], получим, что найдется такой кватернион $U' = L_1 Z + Z L_2$, что $(N(U')) = \mathfrak{d}u'$, где $\mathfrak{d} | 4d^4$, $(u', dg) = 0$ и $L_1 U' = U' L_2$. Теперь возьмем такое число $c \in K$, что $(c) = c(U')c_1^{-1}$, $n(c_1) \leq \kappa$, и положим $U = c^{-1}U'$.

ЛЕММА 27. Каждый класс подобия $(\text{mod } g)$ содержит такой кватернион X , что $(N(X)) = g\mathfrak{h}c^2$, $c = c(X)$, $n(\mathfrak{h}) \leq \kappa(q)$, $(\mathfrak{h}, q) = 0$ (q — заранее выбранный произвольный идеал).

Доказательство. В доказательстве мы будем использовать понятия и результаты [17], часть 4. Из теоремы конечности ([17], 103:4) следует, что существует такая конечная система чисел $a_1, \dots, a_k \in \mathfrak{O}$, $(a_i, qd) = 0$, $i = 1, \dots, k(q)$, что если решетка в 4-мерном K -пространстве с квадратичной функцией имеет целую «норму» \mathfrak{n} , взаимно простую с qd , и «объем» $(ad)^4$, где $n(a) \leq \kappa_1(q)$ (κ_1 будет определено позднее), то эта решетка представляет одно из чисел a_1, \dots, a_k . Положим $g' = (a_1 \cdot \dots \cdot a_k)g$. Тогда $n(g') \leq \kappa_2(q)n(g)$. Возьмем такой вектор X из рассматриваемого класса подобия $(\text{mod } g)$, что $g' | N(X)c(X)^{-2}$. Тогда ввиду леммы 18 кватернионы A с условием $A\bar{X} \equiv 0 \pmod{c(X)g'}$ образуют в векторном K -пространстве \mathcal{A} с квадратичной функцией N решетку \mathcal{M} «объема» $(g'd)^4$. Возьмем такое число $g \in K$, что $(g) = ag'^{-1}$, $(a, qd) = 0$, $n(a) \leq \kappa_1(q)$. Так как $g' | N(A)$ для всех $A \in \mathcal{M}$, то решетка \mathcal{M} имеет в пространстве \mathcal{A} с квадратичной функцией gN целую «норму» a и «объем» $(ad)^4$. В силу выбора системы чисел a_1, \dots, a_k найдется число $a \in \{a_1, \dots, a_k\}$ и кватернион $A \in \mathcal{M}$ с условием $gN(A) = a$, т. е. $N(A) = ag^{-1} | ag'$. Так как $A\bar{X} \equiv 0 \pmod{c(X)g'}$, то $N(A)\bar{X} \equiv 0 \pmod{c(A)c(X)g'}$,

так что $\mathfrak{c}(A) \mid a$. Поэтому $A\bar{X} \equiv 0 \pmod{\mathfrak{c}(A)\mathfrak{c}(X)\mathfrak{g}}$, т. е. A обладает требуемыми свойствами.

ЛЕММА 28. Если $0 < s$, то

$$\begin{aligned} & \# \{X \in \mathcal{O}_f \mid N(X) = s, X \equiv X_0 \pmod{\mathfrak{a}}\} = \\ & = R_\infty(\mathcal{O}_f, s) \cdot \prod_p R_p(\mathcal{O}_f, s; \mathfrak{a}, X_0) + O(n(s)^{\frac{3}{4} + \delta}), \end{aligned} \quad (6.6)$$

где

$$R_\infty(\mathcal{O}_f, s) = \frac{\pi^{2n}}{|D|^{3/2} n(d)^2} n(s)$$

(D — дискриминант поля K),

$$R_p(\mathcal{O}_f, s; \mathfrak{a}, X_0) = \lim_{k \rightarrow \infty} \frac{R_p^k(\mathcal{O}_f, s; \mathfrak{a}, X_0)}{n(p)^{3k}}$$

и $R_p^k(\mathcal{O}_f, s; \mathfrak{a}, X_0)$ — число решений системы сравнений $N(X) \equiv s \pmod{\mathfrak{p}^k}$, $X \equiv X_0 \pmod{(\mathfrak{p}^k, \mathfrak{a})}$. Постоянная в знаке O зависит только от K , рода f , идеала \mathfrak{a} и числа $\varepsilon > 0$.

Доказательство. Лемма прямо следует из асимптотической формулы для числа представлений чисел квадратичными формами от четырех переменных. Эта формула известна по крайней мере со времен появления фундаментальных работ Клостермана [13], [14], в которых он, используя теорию модулярных форм, выделил главный и остаточный член формулы и привел метод вычисления главного члена, и статьи [11], в которой дана оценка остаточного члена. Более подробно метод вычисления главного члена рассмотрен в работе [5]. Правда, там рассматривается случай форм от пяти и более переменных, однако в случае кватернарных форм рассуждения остаются такими же, только для обеспечения сходимости появляющихся рядов следует использовать стандартный метод аналитического продолжения рядов — см. [13], [14]. Во всех указанных работах рассматриваются только модули \mathfrak{a} специального вида: $\mathfrak{a} = (\lambda)\mathfrak{b}^{-1}$, где \mathfrak{b} — дифферента поля K , $\lambda > 0$. Однако это ограничение несущественно, поскольку всегда можно по заданному модулю \mathfrak{a} подобрать такой идеал \mathfrak{a}' , что $n(\mathfrak{a}') \leq \kappa$, $\mathfrak{a}\mathfrak{a}'\mathfrak{b} = (\lambda)$, получить формулы (6.6) для $\mathfrak{a}\mathfrak{a}'$ вместо \mathfrak{a} и просуммировать их по всем классам кватернионов $X_0' \pmod{\mathfrak{a}\mathfrak{a}'}$ с условием $X_0' \equiv X_0 \pmod{\mathfrak{a}}$.

ЛЕММА 29. Если $0 < s$, $\mathfrak{c}^2 \mid s$, то

$$\begin{aligned} & \# \{X \in \mathcal{O}_f \mid N(X) = s, \mathfrak{c}(X) = \mathfrak{c}, X \equiv X_0 \pmod{\mathfrak{a}}\} = \\ & = \frac{\pi^{2n}}{|D|^{3/2} n(d)^2} n(s) \prod_p r_p(\mathcal{O}_f, s, \mathfrak{c}; \mathfrak{a}, X_0) + O(n(s\mathfrak{c}^{-2})^{\frac{3}{4} + \delta}). \end{aligned} \quad (6.7)$$

где

$$r_p(\mathcal{O}_f, s, \mathfrak{c}; \mathfrak{a}, X_0) = \lim_{k \rightarrow \infty} \frac{r_p^k(\mathcal{O}_f, s, \mathfrak{c}; \mathfrak{a}, X_0)}{n(p)^{3k}},$$

а $r_p^k(\mathcal{O}_f, s, \mathfrak{c}; \mathfrak{a}, X_0)$ — число решений $X \pmod{\mathfrak{p}^k}$ системы $N(X) \equiv s \pmod{\mathfrak{p}^k}$, $(\mathfrak{c}(X), \mathfrak{p}^k) = (\mathfrak{c}, \mathfrak{p}^k)$, $X \equiv X_0 \pmod{(\mathfrak{p}^k, \mathfrak{a})}$.

Доказательство. Покажем, что если $s^2 | s$, то

$$R(\mathcal{O}_f, s, \mathfrak{s}; \mathfrak{a}, X_0) = \# \{X \in \mathcal{O}_f \mid N(X) = s, X \equiv 0 \pmod{\mathfrak{s}}, X \equiv X_0 \pmod{\mathfrak{a}}\} = \\ = \frac{\pi^{2n}}{|D|^{3/2} n(d)^2} n(s) \prod_p R_p(\mathcal{O}_f, s, \mathfrak{s}; \mathfrak{a}, X_0) + O(n(s\mathfrak{s}^{-2})^{\frac{3}{4} + \delta}). \quad (6.8)$$

Здесь

$$R_p(\mathcal{O}_f, s, \mathfrak{s}; \mathfrak{a}, X_0) = \lim_{k \rightarrow \infty} \frac{R_p^k(\mathcal{O}_f, s, \mathfrak{s}; \mathfrak{a}, X_0)}{n(p)^{3k}},$$

$R_p^k(\mathcal{O}_f, s, \mathfrak{s}; \mathfrak{a}, X_0)$ — число решений системы $N(X) \equiv s \pmod{p^k}$, $X \equiv 0 \pmod{p^k \mathfrak{s}}$, $X \equiv X_0 \pmod{p^k \mathfrak{a}}$. Действительно, возьмем такой идеал \mathfrak{s}' , что $n(\mathfrak{s}') \leq \kappa$, $\mathfrak{s}'\mathfrak{s}^{-1} = (t)$, и положим $\mathfrak{s}' = t^2\mathfrak{s}$, $X_0' = tX_0$, $\mathfrak{a}' = \mathfrak{a}\mathfrak{s}' \cdot (\mathfrak{a}\mathfrak{s}', \mathfrak{s})^{-1}$. (Мы считаем, что $X_0 \equiv 0 \pmod{(\mathfrak{a}, \mathfrak{s})}$, иначе в (6.8) левая часть и главный член правой части равны нулю.) Тогда легко проверяется, что $R(\mathcal{O}_f, s, \mathfrak{s}; \mathfrak{a}, X_0) = R(\mathcal{O}_f, \mathfrak{s}', \mathfrak{s}'; \mathfrak{a}', X_0')$, $R_p(\mathcal{O}_f, s, \mathfrak{s}; \mathfrak{a}, X_0) = n(p)^{v_p(\mathfrak{s}\mathfrak{s}'^{-1})} R_p(\mathcal{O}_f, \mathfrak{s}', \mathfrak{s}'; \mathfrak{a}', X_0')$.

Таким образом, мы свели доказательство (6.8) к случаю, когда $n(\mathfrak{s}) \leq \kappa$. Для доказательства (6.8) в этом случае следует просто применить (6.6), заменив \mathfrak{a} на $\mathfrak{a}\mathfrak{s} \cdot (\mathfrak{a}, \mathfrak{s})^{-1}$, а X_0 — на X_0'' с условием $X_0'' \equiv X_0 \pmod{\mathfrak{a}}$, $X_0'' \equiv 0 \pmod{\mathfrak{s}}$.

Определим функцию Мёбиуса $\mu(\mathfrak{s}) : \mu(\mathfrak{s}) = (-1)^k$, если \mathfrak{s} есть произведение k различных простых идеалов, и $\mu(\mathfrak{s}) = 0$, если \mathfrak{s} содержит квадрат. Учитывая (6.8) (и последнюю оценку леммы 35), получим, что левая часть (6.7) равна

$$\sum_{c^2 \mathfrak{s}^2 | s} \mu(\mathfrak{s}) R(\mathcal{O}_f, s, c\mathfrak{s}; \mathfrak{a}, X_0) = \\ = \sum_{c^2 \mathfrak{s}^2 | s} \frac{\pi^{2n} n(s)}{|D|^{3/2} n(d)^2} \mu(\mathfrak{s}) \prod_p R_p(\mathcal{O}_f, s, c\mathfrak{s}; \mathfrak{a}, X_0) + O(n(sc^{-2})^{\frac{3}{4} + \delta}) = \\ = \frac{\pi^{2n} n(s)}{|D|^{3/2} n(d)^2} \prod_p (R_p(\mathcal{O}_f, s, c; \mathfrak{a}, X_0) - R_p(\mathcal{O}_f, s, c\mathfrak{p}; \mathfrak{a}, X_0)) + O(n(sc^{-2})^{3/4 + \delta}),$$

то есть совпадает с правой частью (6.7).

ЛЕММА 30. Пусть $\mathfrak{a} = \mathfrak{a}_0 \mathfrak{a}_1$, все простые делители \mathfrak{a}_0 входят в \mathfrak{d} , $(\mathfrak{a}_1, \mathfrak{d}) = 0$, $0 < s$, $c^2 | s$, $(s, \mathfrak{d}) = 0$ и $N(X_0) \equiv s \pmod{\mathfrak{a}_1 \cdot (\mathfrak{a}_1, \mathfrak{c})}$, $(\mathfrak{c}(X_0), \mathfrak{a}_1) = (\mathfrak{c}, \mathfrak{a}_1)$. Тогда

$$\# \{X \in \mathcal{O}_f \mid N(X) = s, \mathfrak{c}(X) = \mathfrak{c}, X \equiv X_0 \pmod{\mathfrak{a}}\} = \\ = \frac{\alpha \prod_{p | \mathfrak{d}} r_p(\mathcal{O}_f, s, 0; \mathfrak{a}_0, X_0)}{n(\mathfrak{a}_1')^3 \prod_{p | \mathfrak{a}_1'} (1 - n(p)^{-2}) \cdot \prod_{p | (s, \mathfrak{a}_1')} (1 + n(p)^{-1})} n(sc^{-2}) \times \\ \times \prod_{p | sc^{-2}} \left(1 + \frac{1}{n(p)}\right) + O(n(sc^{-2})^{\frac{3}{4} + \delta}),$$

где $\mathfrak{a}_1' = \mathfrak{a}_1 \cdot (\mathfrak{a}_1, \mathfrak{c})^{-1}$, постоянная $\alpha > 0$ зависит только от K и рода f .

Доказательство. Подставляем в (6.7) формулы для числа решений квадратичных сравнений (см., например, [19, §§ 7, 10]).

ЛЕММА 31. Пусть $0 < s$, $(s, d) = 0$, сравнение $x^2 \equiv s \pmod{8d}$ разрешимо; $(a, ds) = 0$, $N(X_0) \equiv s \pmod{a}$, $(\epsilon(X_0), a) = 0$; $a_1 a_2 | s$, \mathcal{H}_1 — класс подобия $\pmod{a_1}$ слева, \mathcal{H}_2 — класс подобия $\pmod{a_2}$. Тогда

$$\begin{aligned} \# \{X \in \mathcal{O}_f | N(X) = s, \epsilon(X) = 0, X \equiv X_0 \pmod{a}, X \in \mathcal{H}_1, X \in \mathcal{H}_2\} = \\ = \beta \frac{1}{n(a)^3 \prod_{p|a} (1 - n(p)^{-2}) \cdot n(a_1) \prod_{p|a_1} (1 + n(p)^{-1}) \cdot n(a_2) \prod_{p|a_2} (1 + n(p)^{-1})} \times \\ \times n(s) \prod_{p|s} \left(1 + \frac{1}{n(p)}\right) + O(n(sa_2^{-1})^{\frac{3}{4} + \epsilon}), \end{aligned} \quad (6.9)$$

где $\beta > 0$ зависит только от K и рода f , а постоянная в знаке O зависит только от K , рода f , идеала aa_1 и числа $\epsilon > 0$ (и не зависит от a_2).

Доказательство. Заметим, что (6.9) с постоянной в знаке O , зависящей от a_2 , прямо следует из лемм 20 и 30 (ср. [8], замечание 17 гл. IV). Поэтому основная наша цель — исключить эту зависимость. Заметим также, что при доказательстве теоремы 1 эта лемма фактически применяется только в случае, когда a_1 , a_2 и s делятся только на один простой идеал \mathfrak{q} (см. доказательство леммы 1 и определение q в начале доказательства леммы 4). Для простоты мы ограничимся только этим случаем. Пусть (см. лемму 27) $H \in \mathcal{H}_2$, $N(H) = h$, $(h) = a_2 \mathfrak{h}^2$, $\epsilon = \epsilon(H)$, $(\mathfrak{h}, qd) = 0$, $n(\mathfrak{h}) \leq \kappa_1$ (из доказательства леммы 27 видно, что κ_1 можно считать не зависящей от q). Положим $(g) = g\mathfrak{h}$, где $(g, d) = 0$. Тогда легко проверяется, что кватернион X обладает свойствами (6.9) тогда и только тогда, когда $Y = gXH^{-1}$ обладает свойствами:

$$\begin{aligned} N(Y) = g^2 h^{-1} s, \quad \epsilon(Y) = g, \quad \epsilon(YH) = (g), \quad Y \in \mathcal{H}_1, \\ Y \equiv B \equiv gh^{-1} X_0 \bar{H} \pmod{ga}. \end{aligned}$$

Условие $\epsilon(YH) = (g)$ равносильно тому, что $Y \in \mathcal{H}$, где \mathcal{H} — класс подобия $\pmod{\mathfrak{h}}$, содержащий \bar{H} , и при этом $YH \not\equiv 0 \pmod{gq}$. Поэтому, применяя леммы 20 и 30, получаем, что левая часть (6.9) равна

$$\alpha_0 = \gamma \cdot n(sa_2^{-1}) \left(1 + \frac{1}{n(q)}\right) - \alpha_1 + O(n(sa_2^{-1})^{\frac{3}{4} + \epsilon}),$$

где

$$\gamma = \frac{\beta}{n(a)^3 \prod_{p|a} (1 - n(p)^{-2}) \cdot n(a_1) \prod_{p|a_1} (1 + n(p)^{-1})},$$

$$\begin{aligned} \alpha_1 = \# \{Y \in \mathcal{O}_f | N(Y) = g^2 h^{-1} s, \epsilon(Y) = g, \\ YH \equiv 0 \pmod{gq}, Y \in \mathcal{H}_1, Y \equiv B \pmod{ga}\}. \end{aligned}$$

Аналогично найдем в классе подобия \pmod{q} , содержащем \bar{H} , кватернион H_1 со свойствами: $N(H_1) = h_1$, $(h_1) = q\mathfrak{h}_1 c_1^2$, $c_1 = \epsilon(H_1)$, $(\mathfrak{h}_1, dq\mathfrak{h}) = 0$, $n(\mathfrak{h}_1) \leq \kappa_2$ и положим $(g_1) = g_1 \mathfrak{h}_1 c_1$, где $(g_1, d) = 0$, $Y_1 = g_1 Y H^{-1}$. Тогда получим:

$$\begin{aligned} \alpha_1 = \# \{Y_1 \in \mathcal{O}_f | N(Y_1) = g^2 g_1^2 h^{-1} h_1^{-1} s, \epsilon(Y_1) = gg_1, \\ \epsilon(Y_1 H_1) = g g_1, Y_1 H_1 \in \mathcal{H}, Y_1 \in \mathcal{H}_1, Y_1 \equiv B_1 \equiv g_1 h_1^{-1} B \bar{H}_1 \pmod{gg_1 a}\}; \end{aligned}$$

применение лемм 20 и 30 даст снова

$$\alpha_1 = \gamma \cdot n (sa_2^{-1}q^{-1}) \left(1 + \frac{1}{n(q)}\right) - \alpha_2 + O(n (sa_2^{-1})^{\frac{3}{4} + \varepsilon}),$$

$$\alpha_2 = \# \{Y_1 \in \mathcal{O}_f | N(Y_1) = g^2 g_1^2 h^{-1} h_1^{-1} s, c(Y_1) = gg_1,$$

$$Y_1 H_1 \equiv 0 \pmod{gg_1 c_1 h_1 q}, Y_1 H_1 \in \mathcal{H}, Y_1 \in \mathcal{H}_1, Y_1 \equiv B_1 \pmod{gg_1 a}\}.$$

Далее точно так же делим на \bar{H}_1 , затем на H_1 , затем снова на \bar{H}_1 и т. д. При этом получим последовательность равенств

$$\alpha_i = \gamma \cdot n (sa_2^{-1}q^{-i}) \left(1 + \frac{1}{n(q)}\right) - \alpha_{i-1} + O(n (sa_2^{-1})^{\frac{3}{4} + \varepsilon})$$

для $i=0, \dots, k$ и, наконец,

$$\alpha_{k+1} = O(n (sa_2^{-1})^{\frac{3}{4} + \varepsilon}).$$

Поскольку $k = O(\log n (sa_2^{-1}))$, то, подставляя последовательно значения α_i для $i=k+1, k, \dots, 1$, получим, что $\alpha_0 = \gamma \cdot n (sa_2^{-1}) + O(n (sa_2^{-1})^{\frac{3}{4} + \varepsilon})$; это равносильно (6.9).

§ 7. Разные леммы

ЛЕММА 32. Пусть $\varphi(x, y) = ax^2 + 2bxy + cy^2$ — вполне положительная форма, $\Delta = ac - b^2$. Тогда найдется такая невырожденная подстановка $(\alpha_{ij})_{i=1,2, j=1,2}$, переводящая φ в форму $\varphi'(x, y) = a'x^2 + 2b'xy + c'y^2$, что $\alpha_{ij} \in \mathfrak{o}$,

$|n(\det(\alpha_{ij}))| \leq \kappa$, $\Delta' = a'c' - b'^2 \in H_2$, $a' \in H_2$, $n(a') \leq |D| \left(\frac{4}{\pi}\right)^n \sqrt{n(\Delta)}$, $b' \in a' \cdot \mathcal{P}$, где (см. начало доказательства леммы 6) H_2 — фундаментальная область вполне положительных чисел относительно группы квадратов единиц, \mathcal{P} — основной параллелепипед решетки \mathfrak{o} .

Доказательство. Рассмотрим в пространстве \mathbf{R}^{2n} решетку \mathfrak{o}^2 и область $\mathcal{M} = \{(x, y) = (x_1, \dots, x_n, y_1, \dots, y_n) \in \mathbf{R}^{2n} | n(\varphi(x, y)) = \prod_{i=1}^n \varphi^{(i)}(x_i, y_i) = \prod_{i=1}^n (a^{(i)}x_i^2 + 2b^{(i)}x_i y_i + c^{(i)}y_i^2) \leq |D| \left(\frac{4}{\pi}\right)^n \sqrt{n(\Delta)}\}$. Так как \mathcal{M} содержит замкнутое выпуклое симметричное тело

$$\mathcal{M}_1 = \left\{ (x, y) \in \mathbf{R}^{2n} | \varphi^{(i)}(x_i, y_i) \leq |D|^{1/n} \frac{4}{\pi} n(\Delta)^{1/2n}, i = 1, \dots, n \right\}$$

объема

$$\prod_{i=1}^n \frac{\pi \cdot |D|^{1/n} \frac{4}{\pi} n(\Delta)^{1/2n}}{\sqrt{\Delta^{(i)}}} = |D| 2^{2n},$$

а определитель решетки \mathfrak{o}^2 равен $|D|$, то из теоремы Минковского о выпуклом теле (см. [2, гл. II, § 4, теорема 3]) следует, что найдется такая пара $x, y \in \mathfrak{o}$, что $0 < n(\varphi(x, y)) < |D| \left(\frac{4}{\pi}\right)^n \sqrt{n(\Delta)}$. Возьмем такое число $s \in K$, что $(s) = \mathfrak{s} \cdot (x, y)^{-1}$, $n(\mathfrak{s}) \leq \kappa_1$, $n(\mathfrak{s}) \leq n((x, y))$, $s^2 \varphi(x, y) \in H_2$. Тог-

да $\alpha_{11} = sx \in \mathfrak{o}$, $\alpha_{21} = sy \in \mathfrak{o}$, $a' = \varphi(\alpha_{11}, \alpha_{21}) \in H_2$, $n(a') \leq |D| \left(\frac{4}{\pi}\right)^n \cdot \sqrt{n(\Delta)}$, $(\alpha_{11}, \alpha_{21}) = \mathfrak{s}$. Поэтому найдутся такие числа $\alpha'_{12}, \alpha'_{22} \in \mathfrak{o}$, что $0 < |n(\alpha_{11}\alpha'_{22} - \alpha_{21}\alpha'_{12})| \leq \kappa_2 \cdot n(\mathfrak{s}) \leq \kappa$, $(\alpha_{11}\alpha'_{22} - \alpha_{21}\alpha'_{12})^2 \Delta \in H_2$. Тогда подстановка (α_{ij}) с $\alpha_{12} = \alpha'_{12} + \nu\alpha_{11}$, $\alpha_{22} = \alpha'_{22} + \nu\alpha_{21}$ будет искомой. Число $\nu \in \mathfrak{o}$ определяется условием $b' \in a' \cdot \mathfrak{P}$.

ЛЕММА 33. Пусть $\varphi(x, y) = ax^2 + 2bxy + cy^2$, $(a, b, c) = \mathfrak{a}$, $ac - b^2 = \Delta \neq 0$, \mathfrak{g} — целый идеал. Тогда число представлений

$$\varphi(x, y) = f(u_1x + v_1y, u_2x + v_2y, u_3x + v_3y)$$

с условием

$$\mathfrak{g} | \mathfrak{h} = (u_1v_2 - u_2v_1, u_1v_3 - u_3v_1, u_2v_3 - u_3v_2) \quad (7.1)$$

будет

$$\leq \kappa \cdot \tau(\mathfrak{a}) \tau(\Delta)^3 \prod_{\mathfrak{p} | (\Delta \mathfrak{g}^{-2}, \mathfrak{a})} n(\mathfrak{p})^{[v_{\mathfrak{p}}((\Delta \mathfrak{g}^{-2}, \mathfrak{a}))^2]} \quad (7.2)$$

Доказательство. Дадим полностью элементарное доказательство, прямо следуя [8, с. 144—145]. Мы можем считать, что $(a, \Delta) = \mathfrak{a}$ (иначе заменим φ на эквивалентную форму). Если представления с условием (7.1) существуют, то положим $\mathfrak{q} = (u_1, u_2, u_3)$, $\mathfrak{h} = \mathfrak{q}\mathfrak{r}$. В силу (7.1) $\mathfrak{g} | \mathfrak{q}\mathfrak{r}$. Поскольку $\mathfrak{h}^2 | \Delta$, число пар $\mathfrak{q}, \mathfrak{r}$ будет $\leq \tau(\Delta)^2$. Возьмем такие идеалы $\mathfrak{q}_1, \mathfrak{r}_1$, что $n(\mathfrak{q}_1), n(\mathfrak{r}_1) \leq \kappa_1$, $\mathfrak{q}\mathfrak{q}_1^{-1} = (\mathfrak{q})$, $\mathfrak{r}\mathfrak{r}_1^{-1} = (\mathfrak{r})$, $\mathfrak{q}, \mathfrak{r} \in K$. Повторяя рассуждения [3, с. 141—142], получим, что число представлений с фиксированными $\mathfrak{q}, \mathfrak{r}$ не превосходит общего числа представлений форм вида

$$\varphi'(x, y) = \varphi\left(\frac{1}{\mathfrak{q}}x - \frac{\mathfrak{s}}{\mathfrak{q}\mathfrak{r}}y, \frac{1}{\mathfrak{r}}y\right) \quad \text{формой } f \text{ с условиями} \\ (u_1v_2 - u_2v_1, u_1v_3 - u_3v_1, u_2v_3 - u_3v_2) = \mathfrak{g}_1\mathfrak{r}_1, \quad (7.3)$$

когда \mathfrak{s} пробегает все различные $(\text{mod } \mathfrak{r})$ числа из идеала \mathfrak{q}_1^{-1} , для которых форма φ' целая.

Оценим число таких \mathfrak{s} . Из условия, что форма φ' целая, следует:

$$-as + bq = q^2rt, \quad t \in \mathfrak{o}, \quad (7.4)$$

$$q^{-2}r^{-2}(-as + bq)^2 + \Delta r^{-2} \equiv 0 \pmod{\mathfrak{a}}$$

и, значит,

$$t^2 \equiv \frac{\Delta}{(\mathfrak{q}\mathfrak{r})^2} \pmod{\mathfrak{a}\mathfrak{q}^{-2}}.$$

Это сравнение имеет

$$\leq \tau(\mathfrak{a}) \cdot \prod_{\mathfrak{p} | (\Delta \mathfrak{q}^{-2} r^{-2}, \mathfrak{a}\mathfrak{q}_1^2)} n(\mathfrak{p})^{[v_{\mathfrak{p}}((\Delta \mathfrak{q}^{-2} r^{-2}, \mathfrak{a}\mathfrak{q}_1^2))/2]} \leq \\ \leq \kappa_1^2 \cdot \tau(\mathfrak{a}) \cdot \prod_{\mathfrak{p} | (\Delta \mathfrak{g}^{-2}, \mathfrak{a})} n(\mathfrak{p})^{[v_{\mathfrak{p}}((\Delta \mathfrak{g}^{-2}, \mathfrak{a}))^2]}$$

решений. Поскольку $\mathfrak{r} | \Delta$, $(a, \Delta) = \mathfrak{a}$, то в силу (7.4) каждому такому решению отвечает $\leq n(\mathfrak{q}_1\mathfrak{r}_1) \leq \kappa_1^2$ различных $(\text{mod } \mathfrak{r})$ чисел \mathfrak{s} .

Пусть теперь $\varphi'(x, y) = a'x^2 + 2b'xy + c'y^2$ фиксирована, $a'c' - b'^2 = \Delta'$. Поскольку $n(\mathfrak{q}_1\mathfrak{r}_1) \leq \kappa_1^2$, найдется такое число $\mathfrak{p} \in \mathfrak{o} \cap H$, что $\mathfrak{q}_1\mathfrak{r}_1 | \mathfrak{p}$, $|n(\mathfrak{p})| \leq \kappa_2$. Следуя рассуждениям [3, с. 138—140], получим, что число представлений формы φ' формой f с условием (7.3) не превосходит общего

$$\begin{pmatrix} u_1 & v_1 & w_1 \\ u_2 & v_2 & w_2 \\ u_3 & v_3 & w_3 \end{pmatrix}$$

определителя p , переводящих f в форму g с матрицей $d^{-1}p^{-2}\bar{S}$, где \bar{S} — матрица, взаимная

$$S = \begin{pmatrix} P & Q & M \\ Q & R & N \\ M & N & -\Delta' \end{pmatrix},$$

когда M, N пробегает набор представителей решений системы

$$N^2 \equiv -dp^2a', \quad MN \equiv dp^2b', \quad M^2 \equiv -dp^2c' \pmod{\Delta'}, \quad (7.5)$$

а P, Q и R определяются из условий

$$R\Delta' - N^2 = dp^2a', \quad MN - Q\Delta' = dp^2b', \quad P\Delta' - M^2 = dp^2c'.$$

Поскольку $(M, N, \Delta') \mid \det S = d^2p^4$, число решений системы (7.5) не превосходит $\kappa_3 \cdot \tau(\Delta') \leq \kappa_4 \cdot \tau(\Delta)$. Кроме того, если M и N , а значит, и форма g , фиксированы, то число целых подстановок определителя p , переводящих f в g , будет $\leq \kappa_5$, поскольку $|n(p)| \leq \kappa_2$, $p \in H$, а форма f вполне положительная. Учитывая предыдущие оценки, получаем (7.2).

ЛЕММА 34. Пусть $a \in \mathbf{R}^n$, $n(a) = a_1 \cdot \dots \cdot a_n$, \mathfrak{g} — целый идеал. Тогда

$$\sum_{x \in \mathfrak{g}, x^2 < a} 1 \leq \kappa \cdot \max \left\{ \frac{n(a)^{1/2}}{n(\mathfrak{g})}, 1 \right\}. \quad (7.6)$$

Доказательство. Возьмем такое число $g \in K$, что $(g) = \mathfrak{g}a^{-1}$, $n(a) \leq \kappa_1$, $g^{-1}a^{1/2} \in H$, где H — стандартная фундаментальная область. Тогда

$$\sum_{x \in \mathfrak{g}, x^2 < a} 1 \leq \sum_{\substack{x=gy, y \in \mathcal{M} \\ |x^{(i)}| < a_i^{1/2}}} 1 \leq \sum_{y \in \mathcal{M}} 1,$$

где $\mathcal{M} = \{y \in \mathbf{R}^n \mid |y_i| \leq a_i^{1/2} / |g^{(i)}|\}$. Отсюда следует (7.6), поскольку объем тела \mathcal{M} равен $n(a)^{1/2} / n(g) \leq \kappa_1 \cdot n(a)^{1/2} / n(g)$, а площадь поверхности \mathcal{M} будет

$$O \left(\left(\frac{n(a)^{1/2}}{n(g)} \right)^{1 - \frac{1}{n}} \right).$$

ЛЕММА 35. При $k \geq 0$

$$\begin{aligned} \sum_{n(\mathfrak{m}) \leq N} \frac{\tau(\mathfrak{m})^k}{n(\mathfrak{m})} &\leq \kappa_1(k) (\log N)^{2k}, \\ \sum_{n(\mathfrak{m}) \leq N} \tau(\mathfrak{m})^k &\leq \kappa_2(k) \cdot N \cdot (\log N)^{2k-1}, \\ \tau(\mathfrak{m}) &\leq \tau_Z(n(\mathfrak{m}))^n \leq \kappa_3(\varepsilon) n(\mathfrak{m})^\varepsilon. \end{aligned}$$

Доказательство. Пусть $k=0$, H — стандартная фундаментальная область, a_1, \dots, a_n — набор представителей классов идеалов поля K .

Тогда

$$\begin{aligned} \sum_{n(m) \leq N} n(m)^{-1} &= \sum_{i=1}^h n(a_i) \sum_{\substack{m \in a_i, m \in H, \\ n(m) \leq N \cdot n(a_i)}} n(m)^{-1} \leq \\ &\leq \kappa_4 \cdot \int_{\substack{x=(x_1, \dots, x_n) \in H, \\ 1 \leq x_1 \dots x_n \leq \kappa_6 \cdot N}} \frac{dx_1 \dots dx_n}{x_1 \dots x_n} \leq \kappa_6 \cdot \log N. \end{aligned}$$

Аналогично получается вторая оценка при $k=0$. Далее применяем индукцию по k :

$$\begin{aligned} \sum_{n(m) \leq N} \frac{\tau(m)^{k+1}}{n(m)} &= \sum_{n(m) \leq N} \frac{\tau(m)^k}{n(m)} \sum_{n|m} 1 \leq \sum_{n(n) \leq N} \frac{\tau(n)^k}{n(n)} \times \\ &\times \sum_{n(m) \leq N \cdot n(n)^{-1}} \frac{\tau(m)^k}{n(m)} \leq \kappa_1(k)^2 ((\log N)^{2k})^2 = \kappa_1(k+1) (\log N)^{2k+1}, \\ \sum_{\bar{n}(m) \leq N} \tau(m)^{k+1} &\leq \sum_{n(n) \leq N} \tau(n)^k \sum_{n(m) \leq N \cdot n(n)^{-1}} \tau(m)^k \leq \\ &\leq \kappa_2(k) \sum_{n(n) \leq N} \frac{\tau(n)^k}{n(n)} N \cdot (\log N)^{2k-1} \leq \kappa_2(k+1) N \cdot (\log N)^{2k+1-1}. \end{aligned}$$

Наконец, из определения $\tau(m)$ получаем:

$$\tau(m) = \prod_{p|m} (v_p(m) + 1) \leq \prod_{p|n(m)} (v_p(n(m)) + 1)^n = \tau_Z(n(m))^n.$$

ЛЕММА 36. Пусть $g(x) = ax^2 + bx + c$, $a, b, c, x_0 \in \mathfrak{o}$, \mathfrak{g} — целый идеал, $\mathcal{M} = \{x \in K \mid u_i < x^{(i)} < v_i, i = 1, \dots, n\}$, $N = \prod_{i=1}^n (v_i - u_i)$, $|n(g(x))| \leq \leq (N/n(g))^\alpha$ при $x \in \mathcal{M}$. Тогда *

$$\sum_{\substack{x \in \mathcal{M}, g(x) \neq 0, \\ x \equiv x_0 \pmod{\mathfrak{g}}}} \tau(g(x))^k \leq \kappa_1(k, \alpha) \tau((a, b, c))^k \tau(\mathfrak{g})^{2k} \frac{N}{n(\mathfrak{g})} \left(\log \frac{N}{n(\mathfrak{g})} \right)^{\kappa_2(k, \alpha)}. \quad (7.7)$$

Доказательство. Для $K = \mathbf{Q}$ такие суммы оценивались А. И. Виноградовым [4]. Будем действовать аналогичными методами. Заменяя g на ωg , $\omega \in K$, сводим задачу к случаю, когда $n((a, b, c)) \leq \kappa_3$. Рассмотрим сначала случай $\mathfrak{g} = \mathfrak{o}$. Пусть $D = b^2 - 4ac$. Для каждого $x \in \mathcal{M}$, $g(x) \neq \neq 0$, запишем $(g(x)) = m_1 n_1^2 \dots m_s n_s^2 \mathfrak{r}$, где \mathfrak{r} содержит только простые идеалы нормы $\geq N^{1/4}$ (так что $\tau(\mathfrak{r})^k \leq \kappa_4(k, \alpha)$), m_i бесквадратно, $n(m_i)$, $n(n_i)^2 \leq N^{1/2}$ для $i = 1, \dots, s$ и $s \leq 4\alpha$. Тогда с учетом леммы 35 (ср. также лемму 34) получаем:

$$\begin{aligned} \sum_{x \in \mathcal{M}, g(x) \neq 0} \tau(g(x))^k &\leq \kappa_4(k, \alpha) \sum_{x \in \mathcal{M}, g(x) \neq 0} \max_{i \leq s} \tau(m_i)^{ks} \cdot \max_{i \leq s} \tau(n_i^2)^{ks} \leq \\ &\leq \kappa_4(k, \alpha) \sqrt{\sum_{\substack{x \in \mathcal{M}, \\ g(x) \neq 0}} \max_{i \leq s} \tau(m_i)^{2ks}} \cdot \sqrt{\sum_{\substack{x \in \mathcal{M}, \\ g(x) \neq 0}} \max_{i \leq s} \tau(n_i)^{4ks}} \leq \end{aligned}$$

* Несколько усложняя доказательство, можно исключить зависимость κ_2 от α .

$$\begin{aligned} &\leq \kappa_4(k, \alpha) \sqrt{\sum_{n(m) \leq N^{1/2}} \tau(m)^{2ks} \sum_{\substack{x \in \mathcal{M} \\ m|g(x)}} 1} \cdot \sqrt{\sum_{n(n) \leq N^{1/4}} \tau(n)^{4ks} \sum_{\substack{x \in \mathcal{M} \\ n^2|g(x)}} 1} \leq \\ &\leq \kappa_5(k, \alpha) \sqrt{\sum_{n(m) \leq N^{1/2}} \tau(m)^{2ks} \cdot \tau(m) \frac{N}{n(m)}} \times \\ &\times \sqrt{\sum_{\substack{n(n) \leq N^{1/4}}} \tau(n)^{4ks} \cdot \tau(n)^2 \cdot n((n, D)) \frac{N}{n(n)^2}} \leq \kappa_6(k, \alpha) \cdot N \cdot (\log N)^{\kappa_7(k, \alpha)}. \end{aligned}$$

Пусть теперь $g \neq 0$. Положим $(q) = gn^{-1}$, $(m) = mn$, $|n(m)| \leq \kappa_8$. Тогда сумма (7.7)

$$\leq \sum_{\substack{x \in \mathcal{M}, g(x) \neq 0, \\ x = x_0 + qy, y \in \mathcal{O}}} \tau(m^2 g(x))^k = \sum_{y \in \mathcal{M}', g'(y) \neq 0} \tau(g'(y))^k,$$

где $g'(y) = m^2 g(x_0 + qy) = am^2 q^2 y^2 + (2ax_0 + b)m^2 qy + (ax_0^2 + bx_0 + c)m^2$, $\mathcal{M}' = q^{-1}(\mathcal{M} - x_0) = \{y \in K \mid u_i - x_0^{(i)} < q^{(i)} y^{(i)} < v_i - x_0^{(i)}, i = 1, \dots, n\}$. Таким образом, (7.7) сводится к рассмотренному случаю $g = 0$, поскольку $N_{\mathcal{M}'} = N/|n(q)| \leq \kappa_8 \cdot N/n(q)$,

$$(am^2 q^2, (2ax_0 + b)m^2 q, (ax_0^2 + bx_0 + c)m^2) \mid (a, b, c) \cdot g^2 \cdot m^2.$$

ЛЕММА 37. Если $\tilde{r}(\text{Spn } f, m, c) \neq 0$, то

$$\kappa_1 \cdot n(m c^{-2})^{1/2} L(-dm, c) < \tilde{r}(\text{Spn } f, m, c) < \kappa_2 \cdot n(m c^{-2})^{1/2} L(-dm, c). \quad (7.8)$$

Доказательство. Доказательство леммы получается точно так же из [12] и [15], как это сделано в § 2 статьи [10] для случая $K = \mathbb{Q}$. Мы не останавливаемся на этом подробнее, так как оценка (7.8) не используется нами в доказательстве, а нужна только для преобразования остаточного члена в форме (4.10) к виду (1.3).

Литература

1. Белова Н. Н., Мальшев А. В. Эргодические свойства целых точек на эллипсоидах рода $\mathcal{O}[\Omega, 1]$.— Зап. науч. семинаров ЛОМИ, 1981, т. 106, с. 17—51.
2. Боревич З. И., Шафаревич И. Р. Теория чисел. М.: Наука, 1972.
3. Венков Б. А. Элементарная теория чисел. М.—Л.: ОНТИ, 1937.
4. Виноградов А. И. Об одной оценке квадратичных форм, используемой в арифметике.— Вестник ЛГУ, 1959, № 19, с. 60—63.
5. Головизин В. В. О представлении целых чисел положительно определенными квадратичными формами в вполне вещественных полях алгебраических чисел.— Зап. науч. семинаров ЛОМИ, 1983, т. 121, с. 32—46.
6. Голубева Е. П. Асимптотика числа целых точек на некоторых эллипсоидах.— Матем. заметки, 1972, т. 11, № 6, с. 625—634.
7. Линник Ю. В. Избранные труды. Теория чисел. Эргодический метод и L -функции. Л.: Наука, 1979.
8. Мальшев А. В. О представлении целых чисел положительными квадратичными формами. Труды Мат. ин-та им. В. А. Стеклова АН СССР, т. 65, 1962, 212 с.
9. Мальшев 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.
10. Тетерин Ю. Г. О представлении целых чисел положительными тернарными квадратичными формами.— Зап. науч. семинаров ЛОМИ, 1983, т. 121, с. 117—156.
11. Gundlach K.-B. Über die Darstellung der ganzen Spitzenformen zu den Idealstufen der Hilbertschen Modulgruppe und die Abschätzung ihrer Fourierkoeffizienten.— Acta math., 1954, Bd. 92, s. 309—345.
12. Hsia J. S. Representations by spinor genera.— Pacific J. Math., 1976, v. 63, № 1, p. 147—152.

13. *Kloosterman H. D.* Theorie der Eisensteinschen Reihen von mehreren Veränderlichen.— Abh. Math. Seminar Hamburg. Univ., 1928, Bd. 6, Hf. 3/4, s. 163—188.
14. *Kloosterman H. D.* Thetareihen in total-reellen algebraischen Zahlkörpern.— Math. Ann., 1930, Bd. 103, s. 279—299.
15. *Kneser M.* Darstellungsmasse indefiniter quadratischer Formen.— Math. Z., 1961, Bd. 77, № 2, s. 188—194.
16. *Lang S.* Algebraic number theory. Reading: Addison-Wesley, 1970.
17. *O'Meara O. T.* Introduction to quadratic forms. Berlin: Springer, 1963.
18. *Peters M.* Darstellungen durch definite ternäre quadratische Formen.— Acta arithm., 1977, Bd. 34, № 1, s. 57—80.
19. *Siegel C. L.* Über die analytische Theorie der quadratischen Formen. III.— Ann. Math., 1937, Bd. 38, s. 212—291.

Поступила в редакцию
9.VI.1983