

О ПРЕДСТАВЛЕНИИ ЧИСЕЛ, ДЕЛЯЩИХСЯ НА БОЛЬШОЙ КВАДРАТ,
ПОЛОЖИТЕЛЬНОЙ ТЕРНАРНОЙ КВАДРАТИЧНОЙ ФОРМОЙ

§ I. Введение

Эта работа посвящена обобщению одной теоремы Ю.В.Линника [I] с теми уточнениями, которые были сделаны А.В.Малышевым [2,3]. Речь идет о перенесении указанных результатов на общие положительные тернарные квадратичные формы. Один результат в этом направлении был получен Петерсеном [8], лемма (3.7).

Структура статьи следующая. Далее в этом параграфе будут приведены необходимые определения и обозначения, а также сформулированы основные результаты: теоремы I.1 – I.4 и следствие I.5, являющееся обобщением цитированных результатов Линника и Малышева. В §§ 2 и 3 приводятся вспомогательные предложения из арифметики квадратичных форм и обобщенных кватернионов.

Результаты этих параграфов не являются оригинальными. В § 4 подробно рассматриваются условия \mathfrak{N} и Υ , встречающиеся в формулировках основных результатов. Здесь, в частности, приводится довольно общий вид форм, для которых эти условия не вносят дополнительных ограничений. § 5 содержит доказательство основных теорем (§ I).

ОБОЗНАЧЕНИЯ. Мы имеем дело с целой положительной тернарной квадратичной формой f , т.е. с однородным многочленом второй степени от трех переменных с целыми коэффициентами, положительным на всем \mathbb{R}^3 , кроме 0;

\bar{x} – вектор в \mathbb{R}^3 ; (\bar{x}, \bar{y}) – скалярное произведение $\bar{x}, \bar{y} \in \mathbb{R}^3$;
 $A = (a_{ij})_{i,j=1}^3$ – зигелева симметрическая целочисленная матрица формы f , т.е. $(\bar{x}, A\bar{x}) = 2f(\bar{x})$;

f – примитивная форма, если н.о.д. $(a_{ii}, 2a_{ij}) = 2$;
 $1 \leq i < j \leq 3$

$d = -\frac{1}{2} \det A$ – дискриминант формы f ;

ω – н.о.д. миноров второго порядка матрицы A ;

$\Omega = \begin{cases} \frac{\omega}{4} & \text{, если } f \text{ – собственно целая, т.е. } \frac{1}{2} A \\ & \text{– целая матрица,} \end{cases}$

ω в противном случае;

$B = \frac{\det A}{\omega} A^{-1}$ – примитивно взаимная к A

матрица; она целая, примитивная;

m, n – положительные целые числа;

$\Delta = \frac{2 \det A}{\omega^2}$ определяется для примитивной формы f ; в этом случае Δ целое число;

$\nu_p(a)$ - показатель, с которым простое число p входит в число a , $p^{\nu_p(a)} \parallel a$;

$\text{Gen } f$ - род формы f ;

$\text{Spr } f$ - спинорный род f ;

θ - спинорная норма (относительно этих определений см., например, [4]);

$\tau(f, m)$, $\tau(\text{Spr } f, m)$, $\tau(\text{Gen } f, m)$ - количество примитивных представлений числа m формой f , спинорным родом и родом f соответственно; известно (см. [4], гл. 9), что $\tau(\text{Gen } f, m) > 0$ тогда и только тогда, когда m примитивно представимо формой f над всеми \mathbb{Z}_p , $p \leq \infty$;

$\text{ind } f_p$ - количество изотропных компонент в разложении f на изотропную и анизотропную составляющие над \mathbb{Q}_p ; $\text{ind } f_p > 0$ означает, что уравнение $f(X) = 0$ нетривиально разрешимо в \mathbb{Z}_p ; если $\text{ind } f_p = 0$, то $p \mid 2d$;

$h(n)$ - число классов положительных примитивных бинарных квадратичных форм дискриминанта n ; форму $ax^2 + bxy + cy^2$ называем целой примитивной, если $a, b, c \in \mathbb{Z}$ и н.о.д. $(a, b, c) = 1$; $n = b^2 - 4ac$ - ее дискриминант; классы форм понимаются в смысле собственной эквивалентности - преобразуемости форм целой подстановкой определителя ± 1 .

\mathcal{O}_B - алгебра обобщенных кватернионов, отвечающая форме f и соответствующая матрице B ; относительно \mathcal{O} и всех связанных с нею понятий см. § 3.

В формулировках теорем I.1 и I.4 встречается следующее УСЛОВИЕ $\tilde{h}_f(m, s, c)$. Пусть \mathcal{O} - алгебра, отвечающая форме f и пусть t - целое число, взаимно простое с $2ds$, причем $p > c$ для всех простых $p \mid t$. Тогда для каждого примитивного вектора $L \in \mathcal{O}$ нормы $\Delta m t^2$ найдется целое число a , $1 \leq a \leq c$, и целый примитивный $(\text{mod } 2d3a)$ кватернион B с условиями

$$\begin{cases} as \equiv N(B) \pmod{8d\Delta^3 a^5 s^3}, \\ \text{делитель } (\text{mod } a^2 s) \bar{B} L B \text{ равен } a. \end{cases} \quad (\text{I})$$

ТЕОРЕМА I.1. Пусть f - целая положительная тернарная квадратичная форма дискриминанта d , $c > 0$ - произвольная постоянная. Тогда найдутся такие постоянные s_0 и $\mathcal{K} > 0$, зависящие только от f и c , что если

- 1) $s > s_0$,
- 2) s есть степень простого числа π ,
- 3) выполнено условие $\mathcal{H}_f(m, s, c)$,

то

$$z(f, ms^2) \geq \alpha \cdot z(\text{Sprn } f, m); \quad (2)$$

если сверх того $\pi \nmid 2d$, то

$$z(f, ms^2) \geq \alpha \cdot s \cdot z(\text{Sprn } f, m). \quad (3)$$

ТЕОРЕМА I.2. Для каждой целой положительной тернарной квадратичной формы f дискриминанта d найдутся такие постоянные s_0 и $\alpha > 0$, зависящие только от f , что если s есть степень простого числа π и $s > s_0$, то

1) если $\pi \nmid 2d$, то

$$z(f, ms^4) \geq \alpha \cdot s^2 \cdot z(\text{Sprn } f, m); \quad (4)$$

2) если $\pi \mid 2d$, $\text{ind } f_\pi > 0$, то найдется такое $e_f(\pi)$, равное 0 или 1, что если $s > s_0$, $s = \pi^{2k + e_f(\pi)}$ и $\pi^{2k + e_f(\pi)} \nmid m$, то

$$z(f, ms^2) \geq \alpha z(\text{Sprn } f, m); \quad (5)$$

3) если $\text{ind } f_\pi = 0$, то

$$z(f, ms^2) = 0. \quad (6)$$

ЗАМЕЧАНИЕ. Для $\pi \neq 2$

$$e_f(\pi) = \begin{cases} 0, & \text{если } \nu_\pi(\Omega) \equiv \nu_\pi(d) \equiv 0 \pmod{2}, \\ 1, & \text{в противном случае.} \end{cases} \quad (7)$$

В формулировках теорем I.3 и I.4 встречается следующее УСЛОВИЕ $\mathcal{Y}_f(m)$. Для всех простых чисел p

$$\theta(O^+(f_p)) \subseteq N_{K_p/\mathbb{Q}_p}(K_p^*); \quad (8)$$

здесь $O^+(f_p)$ - множество всех автоморфизмов формы f над Z_p , $K = \mathbb{Q}(\sqrt{dm})$, ρ - продолжение p в K , так что $K_\rho = \mathbb{Q}_p(\sqrt{dm})$, K_ρ^* мультипликативная группа поля, N норма расширения.

ТЕОРЕМА I.3. Для каждой целой положительной тернарной квадратичной формы f найдутся такие постоянные $\alpha_1, \alpha_2 > 0$ и s_0 , зависящие только от f , что если

- 1) $n = m s^4$, $s > s_0$,
- 2) $\nu(\text{Gen } f, n) > 0$,
- 3) условие $\Upsilon_f(n)$ не имеет места, то

$$\alpha_1 h(dn) < \nu(f, n) < \alpha_2 h(dn). \quad (9)$$

ТЕОРЕМА I.4. В условиях теоремы I.1 при той же постоянной δ_0 найдется такая постоянная $\alpha > 0$, зависящая только от f и C , что если для числа $n = m s^4$ выполнены условия 1), 2), 3) теоремы I.1, а также условия

- 4) 3 взаимно просто с $2d$,
- 5) $\nu(\text{Gen } f, n) > 0$,
- 6) условие $\Upsilon_f(n)$ не имеет места, то

$$\nu(f, n) > \alpha \cdot h(dn). \quad (10)$$

Пусть форма f примитивна. Введем новые обозначения:

$$P = \left\{ p > 2 - \text{простое число, } p \mid n. \text{ о. д. } (\Omega, \Delta) \right\}.$$

В P выделим подмножества:

P_ν - набор тех чисел $p \in P$, для которых форма f эквивалентна над \mathbb{Z}_p форме $f' = p^{k_1} u_1 x_1^2 + p^{k_2} u_2 x_2^2 + p^{k_3} u_3 x_3^2$, причем $\left(\frac{u_1 u_2}{p}\right) = -1$ и $k_1 = k_2 \pmod{2}$;

P_H - множество чисел p из $P \setminus P_\nu$, для которых f эквивалентна над \mathbb{Z}_p форме f' того же вида с $\left(\frac{u_1 u_2}{p}\right) = -1$, так что $k_1 \neq k_2 \pmod{2}$.

Отношение $<$ на некотором множестве нечетных простых чисел будем называть отношением правильного порядка, если оно задает полный порядок и $\left(\frac{p}{q}\right) = 1$ если $q < p$. Пустое и одноэлементное множество считаем правильно упорядоченными.

СЛЕДСТВИЕ I.5. Пусть для примитивной собственно целой положительной тернарной квадратичной формы f выполнены следующие три условия:

- 1) либо а) $\nu_2(\Omega) \leq 1$, $\nu_2(\Delta) \leq 1$, причем если $\nu_2(\Omega) = 1$, $\nu_2(\Delta) = 0$ и форма Δf эквивалентна над \mathbb{Z}_2 форме $u x_1^2 + 4(b_1 x_2^2 + b_2 x_2 x_3 + b_3 x_3^2)$ с $u \equiv b_2 \equiv 1 \pmod{2}$, то $u \equiv 3 \pmod{4}$, либо б) $\nu_2(\Omega) \geq 2$, $\nu_2(\Delta) = 0$ и форма Δf эквивалентна над \mathbb{Z}_2 форме $u x_1^2 + 2^{\nu_2(\Omega)+1}(b_1 x_2^2 + b_2 x_2 x_3 + b_3 x_3^2)$, $u \equiv 3 \pmod{4}$, $b_2 \equiv 1 \pmod{2}$;

$$2) P = P_\nu \cup P_H;$$

3) P_n допускает правильное упорядочение. Тогда найдутся такие постоянные β_0 и $\alpha_1, \alpha_2 > 0$, зависящие только от f , что если число n примитивно представимо родом f и делится на квадрат, больший β_0 , то

$$\alpha_1 h(dn) < z(f, n) < \alpha_2 h(dn). \quad (II)$$

Случай Линника - Малышева ([3], теорема I гл.5) непосредственно следует отсюда, так как он соответствует $\chi_2(\Omega) = \chi_2(\Delta) = 0$, $\rho = \emptyset$, т.е. условия 2) и 3) выполняются тривиально.

Предложения I.I-I.5 имеют пересечения с результатами, полученными с помощью дискретного эргодического метода (см. [3], гл.V; [8]).

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

§ 2. Вспомогательные предложения из арифметики квадратичных форм

Определим понятие меры (или веса) представимости. Пусть M - совокупность классов форм с представителями f_1, \dots, f_n , $M \subseteq \text{Gen } f$, $|O(f_i)|$ - количество автоморфизмов формы f_i . Тогда мера примитивной представимости числа m совокупностью M есть по определению

$$\tilde{z}(M, m) \stackrel{\text{def}}{=} \sum_{i=1}^n \frac{z(f_i, m)}{|O(f_i)|}, \quad (I2)$$

аналогично мера представимости:

$$\tilde{R}(M, m) \stackrel{\text{def}}{=} \sum_{i=1}^n \frac{R(f_i, m)}{|O(f_i)|}, \quad (I3)$$

где $R(f_i, m)$ есть количество представлений числа m формой f_i .

ПРЕДЛОЖЕНИЕ 2.I. Для каждой целой положительной тернарной квадратичной формы f дискриминанта d найдутся такие постоянные $\alpha_1, \alpha_2 > 0$, зависящие только от f , что если $z(\text{Gen } f, m) \neq 0$, то

$$\alpha_1 h(dm) < \tilde{z}(\text{Gen } f, m) < \alpha_2 h(dm). \quad (I4)$$

ДОКАЗАТЕЛЬСТВО. набросок возможного доказательства приведен в [8], предложение (3.1). Результат может быть получен также прямым применением формул работы [9].

ПРЕДЛОЖЕНИЕ 2.2. Пусть f — целая тернарная квадратичная форма дискриминанта d . Тогда: 1) а) если условие $\Upsilon_f(m)$ не выполнено, то $\tilde{\epsilon}(\text{Spr } f_i, m)$ одинакова для всех f_i из рода f ; б) если $\Upsilon_f(m)$ выполнено, то множество всех спинорных родов из рода f распадается на два подмножества, состоящих из одинакового числа спинорных родов, и $\tilde{\epsilon}(\text{Spr } f_i, m)$ постоянна, когда f_i пробегает любое из этих двух подмножеств.

2) То же верно для $\tilde{R}(\text{Spr } f_i, m)$.

ДОКАЗАТЕЛЬСТВО ведется так же, как в работе [6], если учесть результаты [5], где проводятся все необходимые вычисления для общего случая тернарной формы над A -полем. Формулировка теоремы заимствована из [8].

ПРЕДЛОЖЕНИЕ 2.3. Если $f' \in \text{Spr } f$, число переменных f и $f' \geq 3$, $\text{ind } f_p > 0$, то f' эквивалентна f над $\mathbb{Z}[\frac{1}{p}]$ -кольцом рациональных чисел вида $\frac{m}{p^k}$, где $k, m \in \mathbb{Z}$, p — простое число.

ДОКАЗАТЕЛЬСТВО. См. [4], гл. II, теорема 8.3.

ПРЕДЛОЖЕНИЕ 2.4. Пусть сравнение $f(\bar{x}) \equiv m \pmod{p^k}$ примитивно разрешимо при $k \geq \nu_p(\omega \Delta) + 2$. Тогда уравнение $f(\bar{y}) = m$ разрешимо в \mathbb{Z}_p с дополнительным условием $\bar{y} \equiv \bar{x} \pmod{p^{k - \nu_p(\omega \Delta)}}$.

ДОКАЗАТЕЛЬСТВО. Пусть p нечетно, f эквивалентна над \mathbb{Z}_p форме $p^{k_1} u_1 x_1^2 + p^{k_2} u_2 x_2^2 + p^{k_3} u_3 x_3^2$. Пусть в \bar{x} , например, $x_1 \not\equiv 0 \pmod{p}$. Тогда уравнение

$$p^{k_1} u_1 x_1^2 = m - p^{k_2} u_2 x_2^2 - p^{k_3} u_3 x_3^2 \quad (15)$$

разрешимо относительно x_1 по модулю p^k , а значит и в \mathbb{Z}_p , так как $k > k_1$, причем это решение x_1 удовлетворяет сравнению $x_1' \equiv x_1 \pmod{p^{k - k_1}}$. Поскольку $k_1 \leq \nu_p(\omega \Delta)$, то $\bar{y} = (x_1', x_2, x_3)$ будет искомым решением. Случай $p = 2$ разбирается аналогично.

§ 3. Вспомогательные предложения из арифметики кватернионов

Почти все результаты этого параграфа заимствованы из [3], гл. IV. Там в § I гл. IV показано, как по симметричной положительной матрице B размера 3×3 строится алгебра $\mathcal{A} = \mathcal{A}_B$ обобщенных кватернионов вида $X = (x_0, x_1, x_2, x_3) = (x_0, \bar{x}_1)$, для которых определяется скалярная часть $Sc(X) = x_0$, сопряженный кватернион

$\bar{X} = (x_0, -\bar{x})$ и норма $N(X) = X\bar{X} = \bar{X}X = x_0^2 + N((0, \bar{x}))$.

Особенно важна формула для нормы

$$N((x_0, \bar{x})) = x_0^2 + (\bar{x}, \bar{B}\bar{x}), \quad (16)$$

где $\bar{B} = (\det B) B^{-1}$ - взаимная к B матрица. В нашем случае, когда B является примитивно взаимной матрицей для формы f , эта формула переписывается в виде

$$N((x_0, \bar{x})) = x_0^2 + \Delta f(\bar{x}). \quad (17)$$

Если $Sc(X) = 0$, то X называется вектором.

Кватернионы с целыми координатами называются целыми. Запись $X \equiv Y \pmod{\mathbb{Z}}$ справа означает, что $X - Y = VZ$ для некоторого целого кватерниона V , т.е. кватернион $\frac{1}{N(\mathbb{Z})}(X - Y)Z$ целый. Число q называется критическим для алгебры \mathcal{O}_B , если $\text{н.о.д.}(q, 2 \det B) > 1$. Целый кватернион X называется примитивным, если $\text{н.о.д.}(x_0, x_1, x_2, x_3) = 1$; примитивным \pmod{n} , если $\text{н.о.д.}(n, x_0, x_1, x_2, x_3) = 1$.

ПРЕДЛОЖЕНИЕ 3.1. Пусть $m_1, \dots, m_n \in \mathbb{Z}$ попарно взаимно просты, A_1, \dots, A_n - целые кватернионы. Тогда найдется целый кватернион X , для которого

$$X \equiv A_i \pmod{m_i}, \quad i = 1, \dots, n. \quad (18)$$

ДОКАЗАТЕЛЬСТВО. См. [3], гл. IV, замечание 2.

ПРЕДЛОЖЕНИЕ 3.2. Пусть $\varphi(x_0, \bar{x}) = x_0 + \Delta f(\bar{x})$ - норменная форма с дискриминантом $d\Delta^3$, m и q - целые положительные числа, кватернион B примитивен \pmod{q} ,

$$N(B) \equiv m \pmod{8d\Delta^3 m_1 q}, \quad (19)$$

где $m = m_1 m_2$ и $\text{н.о.д.}(m_2, 2dq) = 1$, и $q^{50} < cm$. Тогда для числа $\tau_{q,B}(m)$ примитивных кватернионов M нормы m с условием $M \equiv B \pmod{q}$ верна формула

$$\tau_{q,B}(m) = \frac{4\pi^2 m}{\omega \Delta^2} G_{q,B}(\varphi, m) + O(q^{13} m^{1-\frac{1}{40}+\epsilon}), \quad (20)$$

где $G_{q,B}(\varphi, m)$ - примитивный особый ряд (см. [3], гл. III, (159)); постоянные, входящие в знак O , зависят только от d и ϵ ; остаточный член бесконечно мал по сравнению с главным.

ДОКАЗАТЕЛЬСТВО. Предложение есть частный случай замечания 15 гл. IV монографии [3].

ПРЕДЛОЖЕНИЕ 3.3. В условиях предложения 3.2

$$G_{g, B}(f, m) \geq \varkappa \cdot g^{-6} \prod_{p|m} \left(1 - \frac{1}{p}\right), \quad (21)$$

где постоянная $\varkappa > 0$ зависит только от f .

ДОКАЗАТЕЛЬСТВО получается из [3], гл. III, формулы (I60) и (I73).

ПРЕДЛОЖЕНИЕ 3.4. Пусть $g = g_1 g_2$, $g_1 \leq \varkappa_1$, g_2 - некритическое число \mathcal{A} , A - целый кватернион с числовым делителем t , н.о.д. $(t, g_2) \leq \varkappa_2$. Тогда число кватернионов \mathcal{A} нормы g с условием $A \equiv 0 \pmod{\mathcal{A}}$ справа ограничено постоянной, зависящей только от \varkappa_1, \varkappa_2 и f .

ДОКАЗАТЕЛЬСТВО. См. [3], гл. IV, замечание 8.

ПРЕДЛОЖЕНИЕ 3.5. Пусть g - целое некритическое число алгебры \mathcal{A} , A - целый кватернион с числовым делителем t . Тогда количество примитивных кватернионов \mathcal{A} нормы g с условием $A \equiv 0 \pmod{\mathcal{A}}$ справа будет не больше, чем

$$8 \cdot \text{н.о.д.}(t, g) \prod_{p|g, p \nmid \frac{g}{\text{н.о.д.}(t, g)}} \left(1 + \frac{1}{p}\right). \quad (22)$$

ДОКАЗАТЕЛЬСТВО. См. [3], гл. IV, замечание 22.

ПРЕДЛОЖЕНИЕ 3.6. Пусть t - некритическое число алгебры \mathcal{A} , L - примитивный $(\text{mod } t)$ вектор, T - целый кватернион нормы t , $N(L) \equiv 0 \pmod{t^2}$, $L \equiv 0 \pmod{T}$ справа. Тогда $L = \overline{T} L_0 T$ для некоторого целого вектора L_0 .

ДОКАЗАТЕЛЬСТВО. См. [3], гл. IV, следствие 3 к замечанию 9.

ПРЕДЛОЖЕНИЕ 3.7. Пусть t - некритическое число алгебры \mathcal{A} , целые кватернионы T и M примитивны $(\text{mod } t)$, $N(T) = t$, $N(M) \equiv 0 \pmod{t}$, k и n - целые числа. Тогда для некоторого целого кватерниона X имеем

$$\begin{cases} N(X) \equiv n \pmod{t^k} \\ MX \equiv 0 \pmod{T \text{ справа}} \end{cases} \quad (23)$$

ДОКАЗАТЕЛЬСТВО. В [3], гл. IV, следствие к замечанию 13 это утверждение доказывается для случая $k = 1$. Учитывая, что t - некритическое число, это решение нетрудно поднять до решения по модулю t^k .

ПРЕДЛОЖЕНИЕ 3.8. Пусть g - некритическое число алгебры \mathcal{A} , целый кватернион A и вектор L примитивны $(\text{mod } g)$.

$N(A) \equiv 0 \pmod{q}$ В этом случае

$$\bar{A} L A \equiv 0 \pmod{q} \quad (24)$$

тогда и только тогда, когда для некоторого целого числа l будет

$$(l + L) A \equiv 0 \pmod{q}. \quad (25)$$

ДОКАЗАТЕЛЬСТВО. Предложение совпадает с [3], замечание 27 гл. IV, если в (25) перейти к сопряженным кватернионам.

ПРЕДЛОЖЕНИЕ 3.9. Пусть вектор L примитивен, Q - кватернион нормы q , t - числовой делитель вектора $\bar{Q} L Q$. Тогда $t | q^2$.

ДОКАЗАТЕЛЬСТВО. Если $\bar{Q} L Q = tV$, где V - целый вектор, то $q^2 L = t Q V \bar{Q}$, и $t \nmid q^2$ в силу примитивности L .

§ 4. Об условиях $\mathfrak{N}_f(m, s, c)$ и $\Upsilon_f(m)$.

В этом параграфе будут приведены некоторые достаточные условия справедливости \mathfrak{N} и Υ , при помощи которых, в частности, из теорем I.3 и I.4 будет выведено следствие I.5.

Займемся сначала условием \mathfrak{N} . Прежде всего укажем, как удобно выяснить, допускает ли множество P_H правильное упорядочение. Из квадратичного закона взаимности следует, что если P_H правильно упорядочено, то

а) для любого $p \in P_H$, $p \equiv 1 \pmod{4}$ должно быть $\left(\frac{q}{p}\right) = 1$ для всех $q \in P_H$, $q \neq p$;

б) если $P_H^{3(4)} = \{p \in P_H \mid p \equiv 3 \pmod{4}\}$, то $P_H^{3(4)}$ также правильно упорядочено.

Обратно, если условия а) и б) выполнены, то можно просто приписать все простые числа $p \equiv 1 \pmod{4}$ из P_H позади $P_H^{3(4)}$, и это не нарушит правильного порядка. На множестве $P_H^{3(4)}$ отношение $<$, определяемое условием $p < q$, если $\left(\frac{q}{p}\right) = 1$, обладает всеми свойствами линейного порядка, кроме транзитивности. Для проверки транзитивности индуктивно строим соответствующую упорядоченную цепочку: если $p_1 < p_2 < \dots < p_k$, то на следующем шаге следует взять любой элемент p из оставшихся в $P_H^{3(4)}$, и если найдется такой номер i , $0 < i < k$, что

$$p_j < p < p_i, \quad p < p_i, \quad i+1 \leq j \leq k, \quad (26)$$

то мы помещаем p между p_i и p_{i+1} , а если такого i нет, то $P_H^{3(4)}$ не может быть правильно упорядочено. Если же нам удаст-

ся включить таким образом в цепочку все элементы $\rho_H^{3(4)}$, то мы тем самым явно зададим правильный порядок на $\rho_H^{3(4)}$.

Займемся теперь непосредственно условием $\tilde{\mathcal{N}}$. В силу предложения 3.1 для выполнения сравнений (I), входящих в условие $\tilde{\mathcal{N}}$, достаточно выполнения для некоторого $a \leq c$ и B_{p_1}, \dots, B_{p_k} условий

$$\begin{cases} a\zeta \equiv N(B_p) \pmod{\rho^{\nu_p}(8d\Delta^3 a^5 \zeta^3)} \\ B_p \text{ примитивен } \pmod{\rho} \\ \rho^{\nu_p(a)} \parallel \bar{B}_p \perp B_p \end{cases} \quad (27)$$

для всех простых чисел $p \mid 2da\zeta$, причем третье условие в (27) выполняется автоматически, если $p \nmid a\zeta$, в силу предложения 3.9.

ПРЕДЛОЖЕНИЕ 4.1. Пусть для простого числа $p \neq 2$ выполнено одно из следующих условий:

- 1) $p \mid \Omega$, $p \nmid \Delta\zeta a$,
- 2) $p \mid \Delta$, $p \nmid \Omega\zeta$, $\nu_p(a) = \nu_p(\Delta)$,
- 3) $p \mid \zeta$, $p \nmid ad$,
- 4) $p \mid a$, $p \nmid \zeta$, $\left(\frac{-\Delta m}{p}\right) = 1$.

Тогда система (27) разрешима относительно B_p .

ДОКАЗАТЕЛЬСТВО. Для случаев 1), 2), 3) доказательство вполне аналогично [3], гл.5, § 2 теорема I, п.5^o.

Для случая 4) заметим прежде всего, что если $N(L) = \Delta m t^2$ и все простые делители t больше c , то ввиду $p \mid a$, $a \leq c$ имеем $p \nmid t$. Из условия $\left(\frac{-\Delta m}{p}\right) = 1$ следует, что уравнение

$$x^2 + \Delta m t^2 = a\zeta \quad (28)$$

разрешимо в \mathbb{Z}_p , а значит и соответствующее сравнение по любой степени p . Положив $B_p = B = x + Lt$, будем иметь, во-первых, $N(B) \equiv a\zeta \pmod{p^k}$; во-вторых, B примитивен в силу примитивности L ; в третьих, $\bar{B} \perp B = N(B)L \equiv a\zeta L \pmod{p^k}$, и $\rho^{\nu_p(a)} \parallel \bar{B} \perp B$ в силу примитивности L и условия $p \nmid \zeta$.

Предложение 4.1 доказано.

ПРЕДЛОЖЕНИЕ 4.2. Пусть $a \equiv \zeta \equiv 1 \pmod{2}$ и для примитивной собственной целой формы f выполнено одно из следующих условий:

- 1) $\nu_2(\Omega) \leq 1$ и $\nu_2(\Delta) \leq 1$, причем если $\nu_2(\Omega) = 1$, $\nu_2(\Delta) = 0$ и форма Δf эквивалентна над \mathbb{Z}_2

форме $u x_1^2 + 4(b_1 x_2^2 + b_2 x_2 x_3 + b_3 x_3^2)$ с $u \equiv b_2 \equiv 1(2)$,
то $u \equiv 3(4)$;

2) $\nu_2(\Omega) \geq 2$ и $\nu_2(\Delta) = 0$, форма Δf эквивалентна над \mathbb{Z}_2 форме $u x_1^2 + \varphi(x_2, x_3)$ с $u \equiv 3(4)$.

Тогда система (27) разрешима для $p = 2$.

ДОКАЗАТЕЛЬСТВО. В силу условия $a \equiv 3 \equiv 1(2)$ достаточно решить только первое сравнение системы (27), что нетрудно проделать для данных случаев.

Предложение 4.2 доказано.

ПРЕДЛОЖЕНИЕ 4.3. Пусть примитивная собственно целая форма f

1) удовлетворяет условиям предложения 4.2;

2) все нечетные простые делители н.о.д. (Ω, Δ) входят либо в P_τ , либо в P_H ;

3) множество P_H может быть правильно упорядочено.

Тогда условие $\tilde{h}_f(m, s, c)$ выполняется для любого m, s взаимно простого с $2d$ и $c \geq \Omega \Delta^2$.

ДОКАЗАТЕЛЬСТВО. Прежде всего построим число a , требуемое в условии \tilde{h} . Все простые делители a будут браться из $\Omega \Delta$. Положим для нечетного простого числа p

$$\nu_p(a) = 0, \text{ если } p \nmid \Omega, p \nmid \Delta,$$

$$\nu_p(a) = \nu_p(\Delta), \text{ если } p \nmid \Delta, p \nmid \Omega.$$

По определению P_τ для $p \in P_\tau$ форма Δf эквивалентна над \mathbb{Z}_p форме вида $p^{k_1} b_1 x_1^2 + p^{k_2} b_2 x_2^2 + p^{k_3} b_3 x_3^2$ с $\left(\frac{b_1 b_2}{p}\right) = -1$ и $k_1 \equiv k_2 \pmod{2}$. Положим предварительно $\nu_p(a) = k_1$.

Займемся теперь множеством P_H . По предположению $P_H = \{p_1, \dots, p_n\}$ и $\left(\frac{p_i}{p_j}\right) = 1$ при $j < i$. Последовательно рассматриваем p_i . По определению для каждого p_i форма Δf эквивалентна над \mathbb{Z}_{p_i} форме $p_i^{k_1^{(i)}} b_1^{(i)} x_1^2 + p_i^{k_2^{(i)}} b_2^{(i)} x_2^2 + p_i^{k_3^{(i)}} b_3^{(i)} x_3^2$, $\left(\frac{b_1^{(i)} b_2^{(i)}}{p_i}\right) = -1$. Пусть a_i есть произведение $p_i^{\nu_p(a)}$ по всем p , для которых $\nu_p(a)$ уже определено, т.е. $p \nmid \Omega \Delta$, $p \nmid 2$ н.о.д. (Ω, Δ) , или $p \in P_\tau$, или $p = p_j \in P_H$, $j < i$. Положим $\nu_{p_i}(a) = k_j^{(i)}$, где индекс $j = 1, 2$ определяется из того условия, что $a_i \cdot 3 \cdot b_j^{(i)}$ есть квадрат в \mathbb{Z}_{p_i} .

После этого мы окончательно определим $\nu_p(a)$ для $p \in P_\tau$, задавая $\nu_p(a)$ тем же условием, что и в случае $p \in P_H$. Поскольку при этом $k_1 \equiv k_2 \pmod{2}$, то a меняется лишь на

квадрат. Наконец, положим: $\forall_p(a) = 0$.

Для построенного таким способом $a = \prod_{p \nmid 2\Omega\Delta} p^{\forall_p(a)}$ система (27) будет примитивно разрешима для всех p . Действительно, разрешимость системы при $p=2$, или $p \nmid \text{н.о.д.}(\Omega, \Delta)$ следует из предложений 4.2 и 4.1. Далее, заметим, что замена формы на эквивалентную сводится в алгебре \mathcal{O} к замене базиса в решетке целых кватернионов, что не меняет рассматриваемые нами отношения и величины. Поэтому достаточно взять $B_p = u \cdot i_j$, где $i_j, j=1, 2$ - подходящий орт базиса, соответствующего каноническому виду формы над \mathbb{Z}_p , $p \nmid u$. Такое u всегда можно подобрать в силу определения $\forall_p(a)$ и того факта, что порядок в P_H правильный, а при уточнении $\forall_p(a)$ для $p \in P_2$ число a меняется только на квадрат. Легко проверить также, что при таком выборе B_p третье условие системы (27) также выполняется.

Заметим, наконец, что по построению $\forall_p(a) \leq \forall_p(\Omega \Delta^2) = \max_{j=1,2,3} k_j$, где k_j - соответствующие показатели в каноническом виде формы.

Предложение 4.3 доказано.

Покажем, как можно использовать случай 4) предложения 4.1, если предложение 4.3 неприменимо. Если построить правильный порядок на всем P_H невозможно, построим его на возможно большем подмножестве $P'_H \subseteq P_H$. Объединим во множество P' все простые сомножители из н.о.д. (Ω, Δ) , не входящие в P_2 или P_H и число 2, если не выполнено условие предложения 4.2. Найдем такие простые числа $p^{(1)}, \dots, p^{(n)}$, что если $q = \prod_{p \in P'} p$, н.о.д. $(3, q) = 1$, то для некоторого числа x и индекса $i \in \{1, \dots, n\}$

$$p^{(i)} z \equiv x^2 \pmod{q} \quad (29)$$

и, кроме того, $p^{(j)} \equiv 1 \pmod{p^{(r)}}$ для всякого $p \notin P'$, $p \nmid 2\Omega\Delta$; $r=3$ для $p=2$ и $r=1$ для $p>2$; $1 \leq j \leq n$. Пусть

a - число, построенное в предложении 4.3, z взаимно просто с $2d$. Решим уравнение $p^{(j)} a z \equiv x^2 \pmod{q}$. Тогда система (27) останется разрешимой при $a' = p^{(j)} a$ для $p \notin P'$ по тем же соображениям, что и в предложении 4.3; для $p \in P'$ решением будет просто $B_p = x$, а для $p = p^{(j)}$ она будет разрешима согласно предложению 4.1, случай 4) тогда, когда $\left(\frac{-\Delta m}{p^{(j)}}\right) = 1$.

Таким образом, условие $\mathfrak{h}_f(m, s, c)$ будет выполнено для всех m с условием $\left(\frac{-\Delta m}{p^{(j)}}\right) = 1$ и для $c > p^{(j)} \Omega \Delta^2$. Увеличивая c , а вместе с ним и набор $p^{(i)}$, мы будем получать справедливость условия \mathfrak{h} для все более широкого набора значений m .

Завершим изучение условия \tilde{h} почти тривиальным свойством.

ПРЕДЛОЖЕНИЕ 4.4. Условие $\tilde{h}_f(m, \mathfrak{z}^2, c)$ выполнено для любого m и \mathfrak{z} , взаимно простого с $2d$, $c \geq 1$.

ДОКАЗАТЕЛЬСТВО. Достаточно взять $a = 1$. Тогда система (27) разрешима при $p \nmid \mathfrak{z}$ по предложению 4.1, 3), а для $p \mid 2d$ достаточно взять $\mathfrak{B}_p = \mathfrak{z}$.

Предложение 4.4 доказано.

Перейдем теперь к рассмотрению условия $\gamma_f(m)$.

ПРЕДЛОЖЕНИЕ 4.5. Пусть выполнено условие $\gamma_f(m)$; пусть $p > 2$ - простое число, причем $p \nmid \text{н.о.д.}(\Omega, \Delta)$ или $p \in P_z$. Тогда $\mathfrak{v}_p(m) \equiv \mathfrak{v}_p(d) \pmod{2}$.

ДОКАЗАТЕЛЬСТВО. Для описанного p имеем $\theta(O^+(f_p)) \geq U_p$, где U_p - множество обратимых элементов Z_p (для $p \nmid \text{н.о.д.}(\Omega, \Delta)$ см. [4], гл. II, лемма 3.7; для $p \in P_z$ доказательство аналогично). С другой стороны, для циклических, и в частности, для квадратичных расширений известна (см., например, [7]) формула

$$(U_p : N_{K_p/\mathbb{Q}_p}(U_p)) = e_p \quad (30)$$

где e_p - индекс ветвления. Выполнение условия $\gamma_f(m)$ влечет поэтому $e_p = 1$. Поскольку $K_p = \mathbb{Q}_p(\sqrt{dm})$, условие $e_p = 1$ означает, что $\mathfrak{v}_p(dm) \equiv 0 \pmod{2}$.

Предложение 4.5 доказано.

ПРЕДЛОЖЕНИЕ 4.6. Пусть форма f удовлетворяет следующим условиям:

1) f эквивалентна над Z_2 одной из форм вида

$$(i) \quad 2^{k_1} (b_1 x_1^2 + b_2 x_1 x_2 + b_3 x_2^2) + 2^{k_2} x_3^2, \quad b_2 \equiv 1 \pmod{2},$$

$$(ii) \quad b_1 x_1^2 + b_2 x_2^2 + b_3 x_3^2, \quad \mathfrak{v}_2(b_1) - \mathfrak{v}_2(b_2) = 0 \text{ или } 1,$$

$$\text{и} \quad \mathfrak{v}_2(b_2) - \mathfrak{v}_2(b_3) = 0 \text{ или } 1;$$

2) все нечетные простые числа из н.о.д. (Ω, Δ) входят в P_z или P_H ;

3) P_H допускает правильное упорядочение.

Тогда в роде формы f содержится один спинорный род.

ДОКАЗАТЕЛЬСТВО. По лемме 3.8 гл. II книги [4] из условия 1) следует, что $U_2 \subseteq \theta(O^+(f_2))$. Из условия 2) следует, что

$U_p \subseteq \theta(O^+(f_p))$ для всех $p \notin P_H$, $p \neq 2$ (ср. доказательств-

во предложения 4.5). Учитывая это, условие 3) и вычисляя согласно лемме 3.6, [4], гл. II группу G , порядок которой равен числу спинорных родов в роде f , получаем утверждение.

Предложение 4.6 доказано.

ПРЕДЛОЖЕНИЕ 4.7. Если в роде формы f содержится один спинорный род, то множество чисел m , для которых выполняется условие $\gamma_f(m)$, пусто.

ДОКАЗАТЕЛЬСТВО. Из результатов работы [5] следует, что если для какого-то m условие $\gamma_f(m)$ выполнено, то множество спинорных родов в роде f распадается на два подмножества из одинакового количества спинорных родов.

Предложение 4.7 доказано.

Предложения 4.3, 4.6, 4.7 показывают, что следствие I.5 действительно прямо вытекает из теорем I.3 и I.4, если учесть лемму 5.1.

§ 5. Доказательство основных результатов

На протяжении всего этого параграфа все постоянные $\mathfrak{X}_i > 0$ зависят только от f , а при доказательстве теорем I.1 и I.4 также от C . В дальнейшем мы не будем специально отмечать это. Кроме того, считаем без ограничения общности форму f примитивной.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ I.1. I^o. Мы будем различать в доказательстве следующие случаи (считаем $C > |2d|$)

а) $\mathfrak{N} \mid 2d$

б) $\mathfrak{N} \nmid 2d, \mathfrak{N} \leq \mathfrak{X}_1$

в) $\mathfrak{N} > \mathfrak{X}_1$ и либо $\mathfrak{Z} = \mathfrak{N}$, либо $\mathfrak{Z} = \mathfrak{N}^{2k}$, $k \geq 1$.

Постоянная $\mathfrak{X}_1 > C$ будет выбрана в п. 5^o а). Общий случай $\mathfrak{N} > \mathfrak{X}_1$ сведется к случаю в). Действительно, если $\mathfrak{Z} = \mathfrak{N}^{2k+1}$, то условие $\mathfrak{N}_f(m, \mathfrak{N}^{2k}, C)$ выполнено по предложению 4.4, а из справедливости $\mathfrak{N}_f(m, \mathfrak{N}^{2k+1}, C)$ следует справедливость $\mathfrak{N}_f(m, \mathfrak{N}, C)$ в силу предложения 4.1, пункт 3) ввиду $\mathfrak{N} > \mathfrak{X}_1 > C$ и довольно тривиальных соображений относительно разрешимости системы (27) при $\rho \neq \mathfrak{N}$. Дважды применяя теорему (к \mathfrak{N} и \mathfrak{N}^{2k}), мы получим утверждение теоремы для \mathfrak{Z} .

2^o. Существует бесконечно много простых чисел ρ с условием $\rho \equiv 1 \pmod{8d\Delta^3}$. Для таких ρ сравнение

$$x_0^2 + \Delta f(\bar{x}) \equiv \rho^n \pmod{8d\Delta^3} \quad (31)$$

разрешимо: $X_0 = 1, \bar{X} = 0$. Тогда по предложению 4.2 при $\rho > \alpha_2 > C$ для любого $n > 0$ найдется примитивный кватернион нормы ρ^n . Зафиксируем наименьшее из таких ρ с условиями $\rho > \alpha_2, \rho \neq \pi$. Этот выбор, конечно, не отразится в дальнейшем на независимости всех постоянных от π . Так как $\rho \equiv 1 \pmod{8d\Delta^3}$, т.е. $\rho \nmid 2d$, то $\text{ind } f_\rho > 0$.

3°. Пусть $\alpha_3 > 0$ - число классов в спинорном роде f . Тогда по крайней мере для одной из форм $f' \in \text{Spn } f$ будем иметь

$$\tau(f', m) \geq \frac{1}{\alpha_3} \cdot \tau(\text{Spn } f, m). \quad (32)$$

Поскольку $\text{ind } f_\rho > 0$, по предложению 2.3 найдется рациональная подстановка определителя I с общим знаменателем $\rho^n, n \geq 0$, переводящая f в f' . Подействовав ею на все примитивные представления числа m формой f' и домножив их на нужную степень $\rho^j, 0 \leq j \leq n$, получим примитивные представления чисел $m \cdot \rho^{2j}$ формой f , общим количеством $\tau(f', m)$. Тогда по крайней мере для одного из $n+1$ значений j имеем в силу (32)

$$\tau(f, m \rho^{2j}) \geq \frac{1}{n+1} \tau(f', m) \geq \alpha_4 \cdot \tau(\text{Spn } f, m). \quad (33)$$

Обозначим $t = \rho^j$. Таким образом, в алгебре \mathcal{O} найдется не менее $\alpha_4 \cdot \tau(\text{Spn } f, m)$ примитивных векторов L_i нормы $\Delta m t^2$.

Кроме того, согласно пункту 2° в \mathcal{O} имеется примитивный кватернион T нормы t (если $j=0$, т.е. $t=1$, то очевидно, $T=1$ и в дальнейшем доказательстве t и T можно вообще опустить).

4°. Пусть $L \in \mathcal{O}$ примитивный вектор нормы $\Delta m t^2$, a - целое число, существование которого утверждается в условии $\mathcal{H}_f(m, s, c)$ в случае $\pi > \alpha_1, s = \pi^{2k}$ (пункт I°, в)) $a=1$ по предложению 4.4. Найдется примитивный $(\text{mod } 2dast)$ кватернион B со свойствами

$$\begin{cases} N(B) \equiv as \pmod{8d\Delta^3 \cdot as \cdot a^4 \pi^{2k}}, \\ LB \equiv 0 \pmod{T \text{ справа}}, \\ \text{делитель } (\text{mod } a^2s) \bar{B}LB \text{ равен } a. \end{cases} \quad (34)$$

Действительно, из условия \mathcal{H} следует существование примитивного $(\text{mod } 2dsa)$ кватерниона B_1 со свойствами

$$\begin{cases} N(B_1) \equiv as \pmod{8d\Delta^3 a^5 s^3} \\ \text{делитель } \pmod{a^2 s} \bar{B}_1 L B_1 \text{ равен } a. \end{cases} \quad (35)$$

Согласно предложению 3.7 найдется кватернион B_2 со свойствами

$$\begin{cases} N(B_2) \equiv as \pmod{t^2} \\ L B_2 \equiv 0 \pmod{T \text{ справа}} \end{cases} \quad (36)$$

Учитывая, что $t = p^j$, $p \neq \pi$, а также $p > c$ и $2d, a \leq c$, и значит t взаимно просто с $2d s a$, строим кватернион B со свойствами (34) по предложению 3.1 и 3.9.

5°. Докажем, что при достаточно большом s , для каждого примитивного вектора L нормы $\Delta m t^2$ найдется не менее $\alpha_5 s$ примитивных кватернионов Q нормы as , для которых $\frac{1}{a} \bar{Q} L Q$ есть целый примитивный вектор нормы $\Delta m s^2 t^2, \equiv 0 \pmod{T}$ (справа). Рассмотрим два случая:

а) $\pi > \alpha_1$. По предложениям 3.2 и 3.3 если α_1 достаточно велико, то найдется не менее $\alpha_6 s \cdot G_{a^2 t, B}(\varphi, as) > \alpha_7 s$ примитивных кватернионов Q ,

$$N(Q) = as, \quad Q \equiv B \pmod{a^2 t} \quad (37)$$

Из (34) и (37) следует, что $\frac{1}{a} \bar{Q} L Q$ есть целый вектор нормы $\Delta m s^2 t^2, \equiv 0 \pmod{T}$ (справа) и примитивный \pmod{a} . Не менее, чем $\alpha_8 s$ из них будут примитивны и \pmod{s} , то есть по предложению 3.9 вообще примитивны. Действительно, если $\bar{Q} L Q \equiv 0 \pmod{\pi}$, то по предложению 3.8 найдется такое целое число l , что $(l+L)Q \equiv 0 \pmod{\pi}$. Домножая последнее сравнение на $(l-L)$ слева, получаем в силу примитивности Q , что $l^2 \equiv -N(L) \pmod{\pi}$, то есть l может принимать не более двух значений $\pmod{\pi}$. С другой стороны, домножая то же сравнение на \bar{Q} справа и учитывая, что $N(Q) = as$, получим

$$a(l+L) \equiv 0 \pmod{\bar{Q} \text{ справа}}, \text{ если } s = \pi \quad (38)$$

$$\pi^{2k-1} (l+L) \equiv 0 \pmod{\bar{Q} \text{ справа}}, \text{ если } s = \pi^{2k}, \quad (39)$$

так как в последнем случае $a = 1$. Применяя предложения 3.4 и 3.5, получим в обоих случаях, что количество таких Q не превосходит $\frac{1}{\pi} \alpha_9 s < \frac{1}{\alpha_1} \alpha_9 s$. Таким образом, при достаточно большом α_1 у нас остается не менее $\alpha_8 s$ кватернионов Q

с нужными свойствами.

б) $\pi \leq x_1$. В этом случае найдем при помощи предложений 3.2 и 3.3 не менее $x_{10} \cdot s \cdot G_{a^2 t \pi, B}(\varphi, as) > x_{11} \cdot s$ примитивных кватернионов Q со свойствами

$$N(Q) = as, \quad Q \equiv B \pmod{a^2 t \pi}, \quad (40)$$

если $s \geq s_0$ достаточно велико. Из (34) и (40) следует, что вектор $\frac{1}{a} \bar{a} L Q$ обладает требуемыми свойствами.

6°. Итак, мы построили не менее $x_{12} \cdot s \cdot z(\text{Spr } f, m)$ примитивных векторов вида $\frac{1}{a} \bar{a} L Q$ нормы $\Delta m s^2 t^2$. Покажем, что среди них имеется по крайней мере $x_{13} \cdot s \cdot z(\text{Spr } f, m)$ различных в случае $\pi \nmid 2d$ и по крайней мере $x_{13} \cdot z(\text{Spr } f, m)$ различных в случае $\pi \mid 2d$.

Нам достаточно оценить количество равенств

$$a \bar{a}_1 L_1 Q_1 = a_1 \bar{a} L Q \quad (41)$$

при фиксированных L и Q . Так как при этом $a_1 \bar{a} L Q \equiv 0 \pmod{Q_1}$ (справа), и числовой делитель вектора $a_1 \bar{a} L Q$ равен $aa_1 \leq c^2$, то по предложению 3.4 в случае $\pi \nmid 2d$ получаем, что количество таких равенств не превосходит x_{14} , откуда получается наше утверждение.

В случае $\pi \mid 2d$ количество таких равенств не превосходит количества примитивных кватернионов нормы $a_1 s$, и значит в силу предложения 3.2 и рассмотрений пункта 5°, б) количество различных векторов вида $\frac{1}{a} \bar{a} L Q$ будет не меньше, чем $x_{13} \cdot z(\text{Spr } f, m)$, где

$$0 < x_{13} \leq \frac{x_{10} \cdot s \cdot \min_{B_a, asc} G_{a^2 t \pi, B_a}(\varphi, as)}{x_{15} \cdot s \cdot \max_{a_1 \leq c} G_{1,0}(\varphi, a_1 s)} = \quad (42)$$

$$= x_{16} \cdot \min_{B_a; a, a_1 \leq c} \left\{ \prod_{\substack{q \text{ — простое} \\ q \leq c \text{ или} \\ q = p, \pi}} \frac{\Psi_{a^2 t \pi, B_a}(q, \varphi, as)}{\Psi_{1,0}(q, \varphi, a_1 s)} \right\}$$

и α_{13} не зависит от π , если применить обозначения и замечания [3], гл. III, § 5.

7°. Поскольку $LQ \equiv 0 \pmod{\pi}$ справа, по предложению 3.6 каждому вектору $\frac{1}{a} \bar{Q} L Q$ взаимно однозначно соответствует примитивный вектор L' нормы $\Delta m s^2$ с условием

$$\frac{1}{a} \bar{Q} L Q = \bar{\pi} L' \pi. \quad (43)$$

Каждому такому вектору соответствует примитивное представление числа $m s^2$ формой f

Теорема I.1 доказана.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ I.2. Утверждение I) прямо следует из теоремы I.1 и предложения 4.4.

Пусть $f(\bar{X}) = m \pi^k$ есть примитивное представление числа $m \pi^k$ формой f , $k > \nu_{\pi}(\omega \Delta) + 1$, в частности, $f(\bar{X}) \equiv 0 \pmod{\pi^k}$. По предложению 2.4 это сравнение может быть продолжено до нетривиального решения уравнения $f(\bar{X}) = 0$ в \mathbb{Z}_{π} . Поэтому $\text{ind } f_{\pi} > 0$, откуда следует утверждение 3).

Покажем теперь, что в случае 2) условие $\bar{\pi}_f(m, s, c)$ выполнено при $c = 4 \Omega \Delta^2$. Действительно, пусть $\pi \neq 2$. Как всегда, считаем форму f примитивной. Пусть форма Δf эквивалентна над \mathbb{Z}_{π} форме

$$\pi^i (u_1 X_1^2 + \pi^k u_2 X_2^2 + \pi^{i+k} u_3 X_3^2), \quad (44)$$

где $i = \nu_{\pi}(\Delta)$, $k = \nu_{\pi}(\Omega)$, $u_j \not\equiv 0 \pmod{\pi}$ $j=1, 2, 3$.

Пусть L - примитивный $\pmod{\pi}$ вектор нормы $\Delta m t^2$, $L = (0, l_1, l_2, l_3)$. Пусть, например, $l_3 \not\equiv 0 \pmod{\pi}$. По условию $\nu_{\pi}(m) > k + i + 1$. Мы можем считать также $\nu_{\pi}(s) > 2i + k + 1$. Поэтому мы можем по предложению 2.4 найти вектор $B_1 = (0, l_1, l_2, l_3)$, где $l_3' \equiv l_3 \pmod{\pi}$, нормы $N(B_1) \equiv \pi^{2i+k} s \pmod{\pi^{\infty}}$, причем в этом случае скалярная часть $B_1 L$ есть

$$Sc(B_1 L) = -\pi^i (u_1 l_1^2 + \pi^k u_2 l_2^2 + \pi^{i+k} u_3 l_3 l_3') \equiv 0 \pmod{\pi^{2i+k+1}}.$$

Поэтому если мы положим $B = (0, l_1, l_2, -l_3')$, то будем иметь

$$N(B) = N(B_1) \equiv \pi^{2i+k} s \pmod{\pi^{\infty}} \quad (45)$$

$$Sc(BL) \equiv 2 \cdot \pi^{2i+k} u_3 l_3' l_3 \pmod{\pi^{2i+k+1}} \quad (46)$$

Кроме того, поскольку B и L - векторы, та

$$BL + LB = BL + \overline{BL} = 2 Sc(BL) \quad (47)$$

$$\begin{aligned} \overline{BL}B &= \overline{2 Sc(BL) - BL} = -N(B)L - 2 Sc(BL) \cdot B \equiv \\ &\equiv \pi^{2i+k} u_4 \pmod{\pi^{2i+k+1}} \end{aligned} \quad (48)$$

в силу (45), (46) и условия $\pi \mid \delta$. Поэтому система (27) разрешима для $\rho = \pi$ при $a = \pi^{2i+k}$. Если $e_f(\pi) \equiv k \pmod{2}$, то система разрешима и для остальных ρ , если взять $B_\rho = \pi^{i + \frac{1}{2}(k + \chi(\rho))}$. Аналогично если $l_2 \not\equiv 0 \pmod{\pi}$, $l_3 \equiv 0 \pmod{\pi}$, то следует взять $a = \pi^{i+k}$, $e_f(\pi) \equiv i+k \pmod{2}$. Из условия $m \equiv 0 \pmod{\pi}$ и примитивности L следует, что других случаев нет. Несложно проверить также, что $e_f(\pi)$ описывается формулой (7) замечания и не зависит от L . Поэтому условие $\mathcal{N}_f(m, \delta, c)$ выполнено, если $c \geq \Omega \Delta^2$.

Для случая $\pi = 2$ рассуждения вполне аналогичны, но здесь, как всегда, значительно больше случаев. В этом случае также можно добиться, чтобы $e_f(2)$ не зависело от L , но теперь оно будет зависеть не только от Ω и Δ , но и от вида приведенной над \mathbb{Z}_2 формы. Таким образом, установим справедливость условия \mathcal{N} и в этом случае. Утверждение 2) следует теперь из теоремы I.1.

Теорема I.2 доказана.

ЛЕММА 5.1. Пусть целое число δ больше δ_0 . Тогда δ делится на степень простого числа, большую δ_0 .

ДОКАЗАТЕЛЬСТВО. Пусть $\delta = \prod_{1 \leq i \leq N} p_i^{k_i}$, где p_i - различные простые числа, $k_i \geq 1$. Если $N \geq \delta_0$, то по крайней мере для одного i будет $p_i > N \geq \delta_0$. Если же $N < \delta_0$, то по крайней мере один из сомножителей больше δ_0 .

Лемма 5.1 доказана.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ I.3. Учитывая лемму 5.1, мы можем считать δ степенью простого числа, $\delta = \pi^k$. Поскольку условие \mathcal{Y}_f описывает квадратичные классы, условие $\mathcal{Y}_f(m)$ не выполняется вместе с $\mathcal{Y}_f(n)$. Так как $\tau(\text{Gen } f, n) > 0$, то уравнение $f(\overline{x}) = m\pi^{4k}$ примитивно разрешимо во всех \mathbb{Z}_p , значит уравнения $f(\overline{x}) = m\pi^{2t}$ примитивно разрешимы во всех \mathbb{Z}_p , $p \neq \pi$ для любого t . Если $\pi \nmid 2d$, то оно разрешимо и в \mathbb{Z}_π . Если же $\pi \mid 2d$, то мы можем считать $k \geq \nu_\pi(d) + 1$, и значит сравнение $f(\overline{x}) \equiv 0 \pmod{\pi^{\nu_\pi(d)+2}}$ примитивно разре-

шимо. Поэтому согласно предложению 2.4 $\text{ind } f_{\pi} > 0$, уравнение $f(\bar{x}) = m\pi^{2t}$ примитивно разрешимо в \mathbb{Z}_{π} при $t \geq \nu_{\pi}(d) + 1$, и для всех таких t имеем $r(\text{Gen } f, m\pi^{2t}) > 0$. Увеличив, если нужно, s_0 , мы можем считать просто, что $\nu_{\pi}(m) \geq \nu_{\pi}(d) + 2$ для $\pi \nmid 2d$ и значит $r(\text{Gen } f, m) > 0$. Из предложений 2.1 и 2.2 следует, что

$$r(\text{Spn}, m) > \alpha_1 h(dm). \quad (49)$$

Поэтому в случае $\pi \nmid 2d$ согласно теореме I.2, 1)

$$r(f, n) \geq \alpha_2 \cdot s^2 \alpha_1 h(dm) > \alpha_3 h(dm s^4) = \alpha_3 h(dn). \quad (50)$$

В случае $\pi \mid 2d$ выделим из s^2 наименьшую степень π^k , которая будет удовлетворять условиям теоремы I.2, 2). Тогда

$$r(f, n) \geq \alpha_4 h(dm) = \alpha_4 h(dn \cdot \pi^{-2k}) > \alpha_5 h(dn),$$

так как π и k принимают только конечное количество значений.

Оценка сверху следует из предложения 2.1.

Теорема I.3 доказана.

Теорема I.4 выводится из теоремы I.1 вполне аналогично.

Следствие I.5 получается из теорем I.3 и I.4, если учесть предложения 4.3, 4.6 и 4.7 и лемму 5.1.

Литература

1. Л и н н и к Ю.В. Одна общая теорема о представлении чисел отдельными тернарными квадратичными формами. - Изв.АН СССР. Сер.мат., 1939, т.3, с.87-108.
2. М а л ы ш е в А.В. К теории тернарных квадратичных форм, II. Об одной теореме Линника. - Вестн.Ленингр.ун-та, 1959, № 13, с.63-70.
3. М а л ы ш е в А.В. О представлении целых чисел положительными квадратичными формами. - Труды Мат.ин-та АН СССР, 1962, т.65, 212 с.
4. С а s s e l s J.W.S. Rational quadratic forms. London, 1978, xvi, 413 p.
5. Н s i a J.S. Representations by spinor genera. - Pacific J. Math., 1976, vol.63, N 1, p.147-152.
6. К n e s e r M. Darstellungsgabe indefiniter quadratischer Formen. - Math.Z., 1961, Bd.77, N 2, S.188-194.

7. L a n g S. Algebraic number theory. Reading (Mass.) a.o., xi, 354 p.
8. P e t e r s M. Darstellungen durch definite ternäre quadratische Formen. - Acta arithm., 1977, Bd.34, N 1, S.57-80.
9. S i e g e l C.L. Über die analutische Theorie der quadratischen Formen. - Ann.Math., 1935, Bd.36, S.527-606.