Math-Net.Ru

Общероссийский математический портал

В. В. Головчанский, М. Н. Смотров, Явная формула
числа классов примитивных гиперболических элементов
группы $\Gamma_0(N)$, *Матем. сб.*, 2008, том 199, номер 7, 63–84

DOI: <https://doi.org/10.4213/sm3853>

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

Параметры загрузки:

IP: 3.91.87.62

26 апреля 2023 г., 15:42:09

УДК 511.342.2+512.817.2+514.774.8

В. В. Головчанский, М. Н. Смотров

Явная формула числа классов примитивных гиперболических элементов группы $\Gamma_0(N)$

Получена явная формула, выражающая число классов примитивных гиперболических элементов (число замкнутых геодезических) конгруэнц-подгруппы $\Gamma_0(N)$ через числа классов бинарных неопределенных квадратичных форм. Хорошо известные формулы чисел классов эллиптических и параболических элементов группы $\Gamma_0(N)$ являются частными случаями данной формулы.

Библиография: 11 названий.

§ 1. Введение

В модели Пуанкаре (верхняя полуплоскость) гиперболического пространства $\mathbb{H}^2$ группа движений с сохранением ориентации представляет собой группу дробно-линейных преобразований с вещественными коэффициентами, которая в свою очередь изоморфна группе $\mathrm{SL}_2(\mathbb{R})/\pm I$. Поэтому все элементы группы $\mathrm{SL}_2(\mathbb{R})$ (за исключением единичного) подразделяются на три вида: эллиптические, параболические и гиперболические, соответствующие типу преобразования, а именно вращению, переносу и растяжению. На группе $\mathrm{SL}_2(\mathbb{R})$ для гиперболического g задана спектральная норма $N(g) = (|\mathrm{tr}(g)| + \sqrt{\mathrm{tr}^2(g) - 4})^2/4$. Всякая дискретная подгруппа конечного объема $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$ униформизирует замкнутую риманову поверхность конечного рода. Числа классов примитивных эллиптических, параболических и гиперболических (с заданной нормой $N(g)$) элементов подгруппы Γ равны соответственно числу точек ветвления, числу каспидальных вершин и числу замкнутых геодезических длины $\ln N(g)$ соответствующей ей римановой поверхности и являются ее инвариантами. Замкнутые геодезические (периодические орбиты в классической механике) на римановых поверхностях с гиперболической метрикой как объект изучения естественным образом возникают в теории пространств Тейхмюллера, в теории чисел, в спектральной теории оператора Лапласа–Бельтрами, в теории квантового хаоса и в теории динамических систем. Хорошим введением в эту тему служит обзор [1].

В настоящей работе получена явная формула числа классов примитивных гиперболических элементов конгруэнц-подгруппы $\Gamma_0(N)$. Соответствующие формулы для эллиптических и параболических элементов хорошо известны (см. [2]) и являются частными вариантами этой формулы.

Напомним основные определения и введем необходимые обозначения. Гиперболический или параболический элемент g дискретной подгруппы Γ называется *примитивным*, если он не представим в виде $g = \pm g_0^k$, $k > 1$, $g_0 \in \Gamma$.

Эллиптический элемент называется *примитивным*, если он не является степенью элемента более высокого порядка, а в циклической подгруппе, им порожденной, осуществляет поворот на наименьший угол.

Отношение эквивалентности $g \sim \sigma^{-1}g\sigma$, $\sigma \in \Gamma$, разбивает подгруппу Γ на классы сопряженных элементов, при этом примитивные элементы образуют отдельные классы, а след является инвариантом при преобразовании подобия. Конгруэнц-подгруппа $\Gamma_0(N)$ определяется следующим образом:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv 0 \pmod{N} \right\}.$$

Так как $-I \in \Gamma_0(N)$, то числа классов примитивных сопряженных элементов со следами L и $-L$ для подгруппы $\Gamma_0(N)$ совпадают. Далее, для определенности будем считать $L \geq 0$.

Используем следующие обозначения.

$\nu(L, N)$ – число классов примитивных элементов подгруппы $\Gamma_0(N)$ со следом L .

D – фундаментальный дискриминант, который для $L \neq 2$ однозначно определяется из соотношения

$$L^2 - 4 = Q^2 D. \quad (1.1)$$

(T_1, U_1) – фундаментальное решение уравнения Пелля

$$t^2 - Du^2 = 4. \quad (1.2)$$

(T_k, U_k) – k -я степень фундаментального решения, а именно

$$\frac{T_k + U_k \sqrt{D}}{2} = \left(\frac{T_1 + U_1 \sqrt{D}}{2} \right)^k. \quad (1.3)$$

Целое $m \geq 1$ определяется из равенства

$$\frac{L + Q\sqrt{D}}{2} = \left(\frac{T_1 + U_1 \sqrt{D}}{2} \right)^m. \quad (1.4)$$

Запишем N и q в каноническом виде:

$$N = \prod_{i=1}^{\omega(N)} p_i^{s_i}, \quad q = q_0 \prod_{i=1}^{\omega(N)} p_i^{\alpha_i}, \quad (q_0, N) = 1.$$

В этих обозначениях справедлива

ТЕОРЕМА 1. Для $L \neq 2$ имеет место формула

$$\nu(L, N) = \sum_{\substack{q|Q \\ q \nmid U_k, k|m, k \neq m \\ x^2 \equiv q^2 D \pmod{4N}}} 2^{\omega(N/(q^2 D, N))} \prod_{i=1}^{\omega(N)} f(p_i, s_i, \alpha_i) h(q^2 D), \quad (1.5)$$

где $\omega(N)$ – число простых делителей N , $h(d)$ – число классов бинарных квадратичных форм дискриминанта d ,

$$f(p, s, \alpha) = p^{[\min(2\alpha, s)/2]} + \delta(p, s, \alpha)p^{[(\min(2\alpha, s)-1)/2]},$$

$$\delta(p, s, \alpha) = \begin{cases} 0, & \text{если выполняется одно из условий:} \\ & \alpha = 0; \\ & 2\alpha = s, \left(\frac{D}{p}\right) = -1 \text{ при } p \neq 2 \text{ и } D \equiv 5 \pmod{8} \text{ при } p = 2; \\ & 2\alpha = s - 1, p \mid D; \\ 2, & \text{если } 2\alpha = s, \left(\frac{D}{p}\right) = 1 \text{ при } p \neq 2 \text{ и } D \equiv 1 \pmod{8} \text{ при } p = 2; \\ 1 & \text{в остальных случаях.} \end{cases}$$

СЛЕДСТВИЕ 1. Пусть N бесквадратно; тогда

$$\nu(L, N) = \sum_{\substack{q \mid Q \\ q \nmid U_k, k \mid m, k \neq m \\ x^2 \equiv q^2 D \pmod{4N}}} d\left(\frac{N}{(qD, N)}\right) d(q, N) h(q^2 D),$$

где $d(N)$ – число делителей N .

СЛЕДСТВИЕ 2. Для модулярной группы

$$\nu(L, 1) = \sum_{\substack{q \mid Q \\ q \nmid U_k, k \mid m, k \neq m}} h(q^2 D). \quad (1.6)$$

Число всех классов гиперболических элементов $\nu_{\text{gen}}(L, N)$ подгруппы $\Gamma_0(N)$ со следом L весьма просто выражается через числа классов примитивных гиперболических элементов, а именно справедлива

ТЕОРЕМА 2. Пусть $L > 2$; тогда

$$\nu_{\text{gen}}(L, N) = \sum_{k \mid m} \nu(T_k, N).$$

ТЕОРЕМА 3. Для любого $\varepsilon > 0$

$$L^{1-\varepsilon} \ll \nu(L, 1) \ll L \log L,$$

$$\frac{\nu(L, N)}{\nu(L, 1)} \ll \sqrt{N} \log^2 \log N.$$

Оценка снизу для $\nu(L, 1)$ была получена Н. В. Кузнецовым (см. [3]). Здесь мы даем иное доказательство этой оценки.

Вкратце изложим содержание следующих параграфов. В § 2 устанавливается взаимно однозначное соответствие между классами примитивных элементов группы $\Gamma_0(N)$ и классами эквивалентных относительно подгруппы $\Gamma_0(N)$ бинарных квадратичных форм $[a, b, c]$ таких, что $N \mid a$ и форма $[a/N, b, c]$ примитивна. Для модулярной группы это соответствие фактически получено еще Дирихле (см. [4]), а именно, он исследовал группу автоморфизмов бинарной квадратичной формы $[a, b, c]$ и установил, что эта группа циклическая с образующей γ вида (2.1). П. Сарнак в работе [5] показал, что эта образующая

для неопределенной квадратичной формы $[a, b, c]$ является примитивным гиперболическим элементом и отображение $[a, b, c] \mapsto \gamma$ взаимно однозначно, при этом классы эквивалентных форм отображаются в классы сопряженных примитивных гиперболических элементов. Далее фиксируется след L и получается выражение для числа классов примитивных элементов с данным следом в виде суммы чисел классов $h_{N, N/n}((q/n)^2 D)$ примитивных квадратичных форм вида $[a, b, c] : (a, N) = N/n$ по подгруппе $\Gamma_0(N)$. Суммирование проводится по целым q и n , где q удовлетворяет условию из (1.5), а $n \mid (N, q)$.

В § 3 числа классов $h_{N, N/n}((q/n)^2 D)$ выражаются через классическую функцию чисел классов $h(q^2 D)$. Схема вычислений следующая: в каноническом разложении N по степеням простых выделяем сомножитель p^s и рассматриваем подмножества примитивных квадратичных форм

$$\mathcal{F}_{N, N/n} \left(\left(\frac{q}{n} \right)^2 D \right) \subset \mathcal{F}_{N_1, N_1/n_1} \left(\left(\frac{q}{n} \right)^2 D \right), \quad \text{где } N_1 = \frac{N}{p^s}, \quad n_1 = \frac{n}{p^s}.$$

Затем вычисляем число классов квадратичных форм вида $\mathcal{F}_{N, N/n}((q/n)^2 D)$, содержащихся в классе форм вида $\mathcal{F}_{N_1, N_1/n_1}((q/n)^2 D)$. Далее в N_1 вновь выделяем степень простого и повторяем тот же процесс; так поступаем до тех пор, пока не исчерпаем все простые, входящие в N . Таким образом, мы приходим к формам вида $\mathcal{F}_{1,1}((q/n)^2 D)$, которые представляют собой примитивные квадратичные формы с дискриминантом $(q/n)^2 D$, и, следовательно, получаем выражение $h_{N, N/n}((q/n)^2 D)$ через $h((q/n)^2 D)$.

В § 4 проводится суммирование по всем делителям n . В силу того, что уровень N – любое натуральное число, вычисления в § 3 и § 4 оказываются весьма громоздкими, однако конечная формула (1.5) вполне обозрима. Следует отметить, что формула для N бесквадратного значительно упрощается, и по ней судить о формуле для произвольного N вряд ли возможно.

В § 5 в качестве приложения формул (1.5) и (1.6) получена двусторонняя оценка числа классов гиперболических элементов модулярной группы $\nu(L, 1)$ и оценка сверху $\nu(L, N)$. Для модулярной группы по формуле (1.6) был вычислен остаточный член асимптотической формулы функции распределения числа классов примитивных гиперболических элементов. Главные члены этой формулы и формулы для числа простых чисел натурального ряда совпадают, поэтому проверялась гипотеза, что остаточный член есть величина порядка $O(T^{1/2+\varepsilon})$. Проведенные вычисления показывают хорошее согласие с этой гипотезой (см. [6]).

Статья посвящается памяти Николая Иосифовича Заворотного, с которым авторы обсуждали рассматриваемые здесь проблемы.

§ 2. Бинарные квадратичные формы над кольцом $\mathbb{Z}$ и примитивные элементы подгруппы $\Gamma_0(N)$

Используем следующие обозначения.

$[a, b, c] \equiv ax^2 + bxy + cy^2$ – квадратичная форма над кольцом целых чисел $\mathbb{Z}$;

$F_N = \{[a, b, c] : N \mid a, (a/N, b, c) = 1\}$;

G_N – множество примитивных элементов $\Gamma_0(N)$ с неотрицательным следом;

$\text{Aut}_N([a, b, c])$ – группа автоморфизмов формы $[a, b, c] \in F_N$ относительно действия $[a, b, c] \mapsto \gamma^t[a, b, c]\gamma$, $\gamma \in \Gamma_0(N)$.

Ниже мы будем часто использовать следующий технический результат.

ПРЕДЛОЖЕНИЕ 1. Пусть $[a, b, c] \in F_N$ и $n = (a, b, c)$ – наибольший общий делитель. Тогда:

- а) $n \mid N$ и $(a/N, n) = 1$;
- б) отображение $[a, b, c] \mapsto [a/n, b/n, c/n]$ задает биекцию $F_N \rightarrow F_1$.

ДОКАЗАТЕЛЬСТВО. Пункт а) легко следует из определения F_N . Докажем п. б). Пусть $[a_1, b_1, c_1] \neq [a_2, b_2, c_2]$ и для определенности $n_1 > n_2$. Допустим, что $[a_1/n_1, b_1/n_1, c_1/n_1] = [a_2/n_2, b_2/n_2, c_2/n_2]$. Тогда существует простое p , которое входит в разложение чисел N, n_1, n_2 с кратностями s, s_1, s_2 соответственно, при этом $s \geq s_1 > s_2 \geq 0$. Из нашего предположения и в силу того, что $p^{s-s_2} \mid (a_2/n_2)$, следует $p^{s+s_1-s_2} \mid a_1$. Отсюда заключаем, что p делит a_1/N , а поскольку p^{s_1} делит b_1 и c_1 , то форма $[a_1/N, b_1, c_1]$ непримитивна; пришли к противоречию. Обратно, пусть $[a, b, c] \in F_1$. Возьмем $n = N/(a, N)$. Тогда имеем $(na/N, nb, nc) = (a/(a, N), b, c) = 1$ и, следовательно, $[na, nb, nc] \in F_N$.

ПРЕДЛОЖЕНИЕ 2. Пусть $[a, b, c] \in F_N$. Тогда группа автоморфизмов $\text{Aut}_N([a, b, c])$ есть циклическая подгруппа проективной группы $\Gamma_0(N)/\pm I$ с образующей

$$\gamma = \pm \begin{pmatrix} \frac{t_1 - bu_1}{2} & -cu_1 \\ au_1 & \frac{t_1 + bu_1}{2} \end{pmatrix},$$

где пара (t_1, u_1) – фундаментальное решение уравнения Пелля $t^2 - du^2 = 4$, $d = b^2 - 4ac$; образующая γ примитивна в $\Gamma_0(N)$.

ДОКАЗАТЕЛЬСТВО. Как показано в [4; гл. 4, § 62], образующая группы автоморфизмов $\text{Aut}_1([a, b, c])$ равна

$$\gamma_0 = \pm \begin{pmatrix} \frac{t_1^* - (b/n)u_1^*}{2} & -\frac{c}{n}u_1^* \\ \frac{a}{n}u_1^* & \frac{t_1^* + (b/n)u_1^*}{2} \end{pmatrix},$$

где $n = (a, b, c)$ и (t_1^*, u_1^*) – фундаментальное решение уравнения $t^2 - d_1u^2 = 4$, $d_1 = d/n^2$. Так как (t_1, nu_1) является решением уравнения $t^2 - d_1u^2 = 4$, то (t_1, nu_1) – некоторая k -я степень фундаментального решения (t_1^*, u_1^*) . Тогда имеем

$$\gamma_0^k = \pm \begin{pmatrix} \frac{t_k^* - (b/n)u_k^*}{2} & -\frac{c}{n}u_k^* \\ \frac{a}{n}u_k^* & \frac{t_k^* + (b/n)u_k^*}{2} \end{pmatrix} = \pm \begin{pmatrix} \frac{t_1 - bu_1}{2} & -cu_1 \\ au_1 & \frac{t_1 + bu_1}{2} \end{pmatrix}.$$

Покажем, что элемент γ_0^k примитивен в $\Gamma_0(N)$ и, следовательно, является образующей группы $\text{Aut}_N([a, b, c])$. Пусть существует целое $l < k$ такое, что $\gamma_0^l \in \Gamma_0(N)$. Тогда N делит $(a/n)u_l^*$, что в силу п. а) предложения 1 влечет $n \mid u_l^*$. Поэтому пара $(t_l^*, u_l^*/n)$ есть решение уравнения $t^2 - du^2 = 4$, а поскольку (t_1, u_1) – фундаментальное решение этого уравнения, то существует такое $r \geq 1$, что

$$\left(\frac{t_1^* + \sqrt{d_1}u_1^*}{2} \right)^l = \frac{t_l^* + \sqrt{d_1}u_l^*}{2} = \left(\frac{t_1 + \sqrt{d}u_1}{2} \right)^r = \left(\frac{t_1^* + \sqrt{d_1}u_1^*}{2} \right)^{rk}.$$

Отсюда следует $l = rk$, что невозможно. Осталось показать, что эллиптический элемент γ_0^k осуществляет поворот на наименьший угол. Для эллиптических элементов $L = 0, 1$, и, соответственно, $(t_1, u_1) = (0, 1), (1, 1)$ и $d = -4, -3$. Тогда γ_0^k имеет вид

$$\pm \begin{pmatrix} -\frac{b}{2} & -c \\ a & \frac{b}{2} \end{pmatrix} \quad \text{при } d = -4, \quad \pm \begin{pmatrix} \frac{1-b}{2} & -c \\ a & \frac{1+b}{2} \end{pmatrix} \quad \text{при } d = -3.$$

Легко проверить, что γ_0^k имеет собственные значения $\exp(\pm\pi i/3)$ при $d = -3$ и $\exp(\pm\pi i/2)$ при $d = -4$; отсюда следует, что данные эллиптические примитивны.

Действие $[a, b, c] \mapsto \gamma^t[a, b, c]\gamma$, $\gamma \in \Gamma_0(N)$, задает отношение эквивалентности на множестве форм F_N . Справедливо следующее

ПРЕДЛОЖЕНИЕ 3. *Отображение $f: F_N \rightarrow G_N$, заданное формулой*

$$[a, b, c] \mapsto \begin{pmatrix} \frac{t_1 - bu_1}{2} & -cu_1 \\ au_1 & \frac{t_1 + bu_1}{2} \end{pmatrix}, \quad (2.1)$$

где пара (t_1, u_1) – фундаментальное решение уравнения $t^2 - du^2 = 4$, $d = b^2 - 4ac$, взаимно однозначно. Обратное отображение f^{-1} имеет вид

$$\begin{pmatrix} \alpha & \beta \\ N\gamma & \delta \end{pmatrix} \mapsto \left[\frac{N\gamma}{(\delta - \alpha, \gamma, \beta)}, \frac{\delta - \alpha}{(\delta - \alpha, \gamma, \beta)}, \frac{-\beta}{(\delta - \alpha, \gamma, \beta)} \right]. \quad (2.2)$$

При этом классы эквивалентных форм F_N взаимно однозначно отображаются в классы сопряженных элементов G_N .

ДОКАЗАТЕЛЬСТВО. Отображение задано корректно, так как согласно предложению 2 элемент в правой части (2.1) примитивен в $\Gamma_0(N)$. Пусть $[a, b, c] \neq [a', b', c'] \in F_N$ и $(t_1, u_1), (t'_1, u'_1)$ – соответствующие им фундаментальные решения уравнения Пелля. Если $t_1 \neq t'_1$, то из (2.1) сразу следует, что $f([a, b, c]) \neq f([a', b', c'])$. Предположим, что $t_1 = t'_1$ и $f([a, b, c]) = f([a', b', c'])$; тогда из (2.1) следует, что $[a, b, c] = [ka', kb', kc']$. Поскольку $(a/N, b, c) = 1$, то $k \mid N$, а так как $N \mid a'$, то $(a/N, b, c) > 1$; пришли к противоречию.

Проверим, что (2.2) задает отображение f^{-1} . Пусть

$$\sigma = \begin{pmatrix} \alpha & \beta \\ N\gamma & \delta \end{pmatrix} \in G_N.$$

Обозначим для краткости через $[a, b, c]$ квадратичную форму в правой части (2.2). Дискриминант этой формы

$$d = \frac{(\delta - \alpha)^2 + 4N\gamma\beta}{(\delta - \alpha, \gamma, \beta)^2} = \frac{(\delta + \alpha)^2 - 4}{(\delta - \alpha, \gamma, \beta)^2}, \quad (2.3)$$

а пара $(T, U) = (\delta + \alpha, (\delta - \alpha, \gamma, \beta))$ является решением уравнения Пелля $t^2 - du^2 = 4$. Пары (T, U) и квадратичной форме $[a, b, c]$ согласно предложению 2 соответствует элемент

$$\pm \begin{pmatrix} \frac{T - bU}{2} & -cU \\ aU & \frac{T + bU}{2} \end{pmatrix} \in \text{Aut}_N([a, b, c]),$$

который, как нетрудно проверить, равен $\pm\sigma$. Поскольку $\pm\sigma$ примитивен в $\Gamma_0(N)$, то он является образующей $\text{Aut}_N([a, b, c])$, а тогда (T, U) является фундаментальным решением и, значит, $f([a, b, c]) = \sigma$. И наконец, если $[a, b, c] = \sigma^*[a', b', c']\sigma$, то, очевидно,

$$\text{Aut}_N([a, b, c]) = \sigma^{-1} \text{Aut}_N([a', b', c'])\sigma,$$

что и требовалось доказать.

Построенное отображение позволяет выразить числа классов примитивных элементов группы $\Gamma_0(N)$ с данным следом $L \geq 0$ через числа классов эквивалентных по группе $\Gamma_0(N)$ квадратичных форм из F_N .

Используем следующие обозначения:

$$G_N(L) = \{\sigma \in G_N : \text{tr}(\sigma) = L\};$$

$$F_{N,n} = \{[a, b, c] \in F_N : (a, b, c) = n\};$$

$$F_{N,n}(d) = \{[a, b, c] \in F_{N,n} : b^2 - 4ac = d\};$$

$$\tilde{h}_{N,n}(d) - \text{число классов эквивалентных относительно } \Gamma_0(N) \text{ форм } F_{N,n}(d).$$

Очевидно, семейство множеств $\{F_{N,n}\}$, когда n пробегает все делители N , образует разбиение F_N и $F_{N,n}$ является объединением классов эквивалентности его элементов по группе $\Gamma_0(N)$. В принятых обозначениях справедливо

ПРЕДЛОЖЕНИЕ 4.

$$\nu(L, N) = \begin{cases} \sum_{\substack{q|Q \\ q \nmid U_k, k|m, k \neq m}} \sum_{x^2 \equiv (q/n)^2 D \pmod{(4N/n)}} \tilde{h}_{N,n}(q^2 D), & \text{если } L \neq 2, \\ \sum_{n|N} \tilde{h}_{N,n}(0), & \text{если } L = 2, \end{cases} \quad (2.4)$$

где Q, D, U_k, m определены в (1.1)–(1.4).

ДОКАЗАТЕЛЬСТВО. Найдем $f^{-1}(G_N(L))$. Пусть

$$\sigma = \begin{pmatrix} \alpha & \beta \\ N\gamma & \delta \end{pmatrix} \in G_N(L).$$

В силу (2.3) дискриминант формы $[a, b, c] = f^{-1}(\sigma)$ равен

$$d = \frac{L^2 - 4}{(\delta - \alpha, \gamma, \beta)^2}.$$

1) $L \neq 2$. Имеем $L^2 - 4 = Q^2 D$. Поскольку D – фундаментальный дискриминант, то $d = q^2 D$, где $q = Q/(\delta - \alpha, \gamma, \beta)$, и, следовательно $[a, b, c] \in F_{N,n}(q^2 D)$, $q | Q$. Из (2.2) следует $n = (\delta - \alpha, N\gamma, \beta)/(\delta - \alpha, \gamma, \beta)$ и, значит, $n | q$. С другой стороны, $d = b^2 - 4ac$, из чего следует, что $(q/n)^2 D$ есть квадратичный вычет по модулю $4N/n$. Пусть $q | U_k$, $k | m$, $k \neq m$. Тогда фундаментальное решение уравнения $t^2 - q^2 D u^2 = 4$ есть пара $(T_{k'}, U_{k'}/q)$, где $k' | k$, поэтому $T_{k'} < L$ и, следовательно, $f([a, b, c]) \notin G_N(L)$. В противном случае фундаментальным решением уравнения Пелля будет пара $(L, Q/q)$ и, следовательно, $f([a, b, c]) \in G_N(L)$. Отсюда заключаем, что

$$f^{-1}(G_N(L)) = \bigcup_{\substack{q|Q \\ q \nmid U_k, k|m, k \neq m}} \bigcup_{x^2 \equiv (q/n)^2 D \pmod{(4N/n)}} F_{N,n}(q^2 D).$$

2) $L = 2$. Тогда $d = 0$ и, значит, имеем только одно условие $n \mid N$. Тогда получаем

$$f^{-1}(G_N(L)) = \bigcup_{n \mid N} F_{N,n}(0).$$

Поскольку $F_{N,n}(d)$ есть объединение классов эквивалентности, то отсюда следует (2.4).

Теперь переформулируем предложение 4 в терминах чисел классов примитивных квадратичных форм. Используем следующие обозначения:

$\mathcal{F}$ – множество примитивных квадратичных форм;

$\mathcal{F}_{N,k}(d) = \{[a, b, c] \in \mathcal{F} : (a, N) = k, b^2 - 4ac = d\}$;

$h_{N,k}(d)$ – число классов эквивалентных по группе $\Gamma_0(N)$ форм $\mathcal{F}_{N,k}(d)$.

Из предложения 1 следует, что отображение $F_{N,n}(d) \rightarrow \mathcal{F}_{N,N/n}(d/n^2)$, задаваемое формулой $[a, b, c] \mapsto [a/n, b/n, c/n]$, где $n = (a, b, c)$, взаимно однозначно, и классы отображаются в классы. Отсюда заключаем, что $\tilde{h}_{N,n}(q^2 D) = h_{N,N/n}((q/n)^2 D)$, и поэтому справедливо

СЛЕДСТВИЕ 3.

$$\nu(L, N) = \begin{cases} \sum_{q \mid Q} \sum_{q \nmid U_k, k \mid m, k \neq m} \sum_{x^2 \equiv (q/n)^2 D \pmod{4N/n}} h_{N,N/n}\left(\left(\frac{q}{n}\right)^2 D\right), & \text{если } L \neq 2, \\ \sum_{n \mid N} h_{N,N/n}(0), & \text{если } L = 2. \end{cases} \quad (2.5)$$

В § 3 правая часть (2.5) будет вычислена через классическую функцию числа классов.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 2. Пусть $\sigma = \sigma_0^k$, $\text{tr}(\sigma) = L$ и σ_0 примитивен. Из представления (2.1) примитивного элемента следует

$$\begin{pmatrix} \frac{t_1 - bu_1}{2} & -cu_1 \\ au_1 & \frac{t_1 + bu_1}{2} \end{pmatrix}^k = \begin{pmatrix} \frac{L - bu_k}{2} & -cu_k \\ au_k & \frac{L + bu_k}{2} \end{pmatrix}.$$

Так как (L, Q) есть решение уравнения $t^2 - Du^2 = 4$, то (t_1, u_1) – фундаментальное решение уравнения $t^2 - (q^2 D)u^2 = 4$ с некоторым $q \mid Q$ и $u_k = Q/q$. Обратно, если (t_1, u_1) – фундаментальное решение уравнения $t^2 - (q^2 D)u^2 = 4$, то для некоторого $k \geq 1$ справедливо

$$\left(\frac{t_1 + u_1 \sqrt{D}}{2}\right)^k = \frac{L + Q/q\sqrt{D}}{2}.$$

Тогда получаем

$$\nu_{\text{gen}}(L, N) = \sum_{q \mid Q} \sum_{x^2 \equiv (q/n)^2 D \pmod{4N/n}} h_{N,N/n}\left(\left(\frac{q}{n}\right)^2 D\right). \quad (2.6)$$

Множества $M_k = \{q \mid U_k : q \nmid U_{k'}, k' \mid k \text{ и } k' \neq k\}$, когда k пробегает все делители m , образуют разбиение множества всех положительных делителей Q .

Докажем это от противного. Пусть $q \in M_{k_1}, M_{k_2}$ и $k_1 \neq k_2$. Возьмем наименьшее k_3 такое, что $q \in M_{k_3}$. Тогда фундаментальное решение уравнения $t^2 - q^2 Du^2 = 4$ есть пара $(T_{k_3}, U_{k_3}/q)$. Поскольку $(T_{k_i}, U_{k_i}/q)$ при $i = 1, 2$ суть решения того же уравнения, то $k_3 \mid k_1$ и $k_3 \mid k_2$. Это возможно в силу определения множеств M_k только в случае $k_3 = k_1 = k_2$, что противоречит предположению $k_1 \neq k_2$. Из (2.6), (2.5) и только что доказанного свойства множеств M_k следует утверждение теоремы 2.

В заключение приведем алгоритм вычисления примитивного элемента x , степень которого x^n равна данному гиперболическому элементу $\sigma \in \Gamma_0(N)$.

Пусть

$$\sigma = \begin{pmatrix} \alpha & \beta \\ N\gamma & \delta \end{pmatrix}.$$

1. Полагаем $(\alpha + \delta)^2 - 4 = Q^2 D$, где D – фундаментальный дискриминант.
2. Находим фундаментальное решение (T_1, U_1) уравнения Пелля $t^2 - Du^2 = 4$.
3. Находим натуральное m из условия $(\alpha + \delta + Q\sqrt{D})/2 = ((T_1 + U_1\sqrt{D})/2)^m$.
4. Выписываем все делители m : $1 = k_1 < k_2 < \dots < k_{d(m)} = m$.
5. Полагаем $d = Q/(\delta - \alpha, \gamma, \beta)$.
6. $i := 0$.
7. $i := i + 1$.
8. Определяем U_{k_i} из условия $((T_1 + U_1\sqrt{D})/2)^{k_i} = (T_{k_i} + U_{k_i}\sqrt{D})/2$.
9. Если $d \nmid U_{k_i}$, то переходим к 7.

$$10. x = \begin{pmatrix} \frac{T_{k_i} - (\delta - \alpha) U_{k_i}/Q}{\frac{2}{\gamma N U_{k_i}}} & -\frac{\beta U_{k_i}}{\frac{Q}{2}} \\ \frac{T_{k_i} + (\delta - \alpha) U_{k_i}/Q}{2} & \end{pmatrix}, \quad n = \frac{m}{k_i}.$$

§ 3. Вычисление $h_{N, N/n}((q/n)^2 D)$

Запишем N , q и n в каноническом виде:

$$N = \prod_{i=1}^{\omega(N)} p_i^{s_i}, \quad q = q_0 \prod_{i=1}^{\omega(N)} p_i^{\alpha_i}, \quad (q_0, N) = 1, \quad n = \prod_{i=1}^{\omega(N)} p_i^{\beta_i}. \quad (3.1)$$

Для $\mathcal{F}_{N, N/n}((q/n)^2 D)$ определим рекуррентную последовательность вложенных множеств квадратичных форм следующим образом:

$$\mathcal{F}_{N_1, N_1/n_1} \left(\left(\frac{q}{n} \right)^2 D \right) \subset \dots \subset \mathcal{F}_{N_i, N_i/n_i} \left(\left(\frac{q}{n} \right)^2 D \right) \subset \dots \subset \mathcal{F}_{1,1} \left(\left(\frac{q}{n} \right)^2 D \right), \quad (3.2)$$

где

$$N_1 = N, \quad N_{i+1} = \frac{N_i}{p_i^{s_i}}, \quad n_1 = n, \quad n_{i+1} = \frac{n_i}{p_i^{\beta_i}}.$$

При этом

$$h_{1,1} \left(\left(\frac{q}{n} \right)^2 D \right) = h \left(\left(\frac{q}{n} \right)^2 D \right),$$

где $h(\cdot)$ – классическая функция числа классов примитивных квадратичных форм данного дискриминанта. Поэтому если мы найдем выражение для

$h_{N_i, N_i/n_i}((q/n)^2 D)$ через $h_{N_{i+1}, N_{i+1}/n_{i+1}}((q/n)^2 D)$, то получим формулу, выражающую $h_{N, N/n}((q/n)^2 D)$ через $h((q/n)^2 D)$. Реализацией этого подхода мы теперь и займемся.

Рассмотрим пару множеств квадратичных форм

$$\mathcal{F}_{N_i, N_i/n_i} \left(\left(\frac{q}{n} \right)^2 D \right) \subset \mathcal{F}_{N_{i+1}, N_{i+1}/n_{i+1}} \left(\left(\frac{q}{n} \right)^2 D \right).$$

Во избежание излишней громоздкости обозначим $p = p_i$, $N = N_i$, $N_1 = N_{i+1}$, $n = n_i$, $n_1 = n_{i+1}$, и пусть s, α, β обозначают показатели степеней, с которыми p входит в N, q, n соответственно. В этих обозначениях справедливо следующее

ПРЕДЛОЖЕНИЕ 5. Пусть $\mathcal{G}$ – класс форм из $\mathcal{F}_{N_1, N_1/n_1}((q/n)^2 D)$ и $h_{N, N/n}(\mathcal{G})$ есть число классов форм из $\mathcal{F}_{N, N/n}((q/n)^2 D)$, содержащихся в $\mathcal{G}$. Тогда справедлива формула

$$h_{N, N/n}(\mathcal{G}) = \frac{\#\{\sigma \in \mathcal{R}_{N, N_1} : \sigma^*[a, b, c]\sigma \in \mathcal{F}_{N, N/n}((q/n)^2 D)\}}{\ln((t_0 + q\sqrt{D}u_0)/2) / \ln((t_1 + (q/p^\alpha)\sqrt{D}u_1)/2)}, \quad (3.3)$$

где $[a, b, c] \in \mathcal{G}$, $\mathcal{R}_{N, N_1}$ – система представителей левых классов смежности $\Gamma_0(N_1)/\Gamma_0(N)$ и пары (t_0, u_0) , (t_1, u_1) – фундаментальные решения уравнений Пелля $t^2 - q^2 Du^2 = 4$ и $t^2 - (q/p^\alpha)^2 Du^2 = 4$ соответственно.

ДОКАЗАТЕЛЬСТВО. Из представления

$$\mathcal{G} = \bigcup_{\sigma \in \mathcal{R}_{N, N_1}} (\sigma \Gamma_0(N))^* [a, b, c] \sigma \Gamma_0(N), \quad [a, b, c] \in \mathcal{G},$$

следует, что число классов $h_{N, N/n}(\mathcal{G})$ равно числу неэквивалентных относительно $\Gamma_0(N)$ форм $\sigma^*[a, b, c]\sigma \in \mathcal{F}_{N, N/n}((q/n)^2 D)$, когда σ пробегает систему представителей $\mathcal{R}_{N, N_1}$. Если таких σ нет, то доказывать нечего. Пусть $\sigma_0^*[a, b, c]\sigma_0 = [a_0, b_0, c_0] \in \mathcal{F}_{N, N/n}((q/n)^2 D)$. Условие $\sigma^*[a_0, b_0, c_0]\sigma \sim [a_0, b_0, c_0]$ для $\sigma \in \mathcal{R}_{N, N_1}$ эквивалентно существованию элемента $\tau \in \text{Aut}_{N_1}([a_0, b_0, c_0])$ такого, что $\tau \in \sigma \Gamma_0(N)$. Пусть τ_0 – образующая $\text{Aut}_{N_1}([a_0, b_0, c_0])$. Тогда при некотором $k \geq 1$ элемент τ_0^k является образующей $\text{Aut}_N([a_0, b_0, c_0])$. Элементы $\tau_0, \dots, \tau_0^k$ лежат в разных классах смежности $\Gamma_0(N_1)/\Gamma_0(N)$ с некоторыми представителями $\sigma_1, \dots, \sigma_k$ из системы $\mathcal{R}_{N, N_1}$, и всякий $\tau \in \text{Aut}_{N_1}([a_0, b_0, c_0])$ сравним по модулю $\Gamma_0(N)$ с некоторым τ_0^i , $1 \leq i \leq k$. Тогда $(\sigma_0 \sigma_i)^*[a_0, b_0, c_0](\sigma_0 \sigma_i) \sim [a_0, b_0, c_0]$ при $1 \leq i \leq k$, и других элементов из $\mathcal{R}_{N, N_1}$ с этим свойством нет.

Осталось вычислить k . Поскольку $[a_0, b_0, c_0] \in \mathcal{F}_{N, N/n}((q/n)^2 D)$, то

$$[a_0 n, b_0 n, c_0 n] \in F_N(q^2 D), \quad [a_0 n_1, b_0 n_1, c_0 n_1] \in F_{N_1} \left(\left(\frac{q}{p^\alpha} \right)^2 D \right)$$

и, кроме того, $\text{Aut}_N([a_0, b_0, c_0]) = \text{Aut}_N([a_0 n, b_0 n, c_0 n])$ и $\text{Aut}_{N_1}([a_0, b_0, c_0]) = \text{Aut}_{N_1}([a_0 n_1, b_0 n_1, c_0 n_1])$. Согласно предложению 2 образующие τ_0 и τ_0^k групп автоморфизмов $\text{Aut}_{N_1}([a_0 n_1, b_0 n_1, c_0 n_1])$ и $\text{Aut}_N([a_0 n, b_0 n, c_0 n])$ имеют соответственно вид

$$\tau_0 = \begin{pmatrix} \frac{t_1 - b_0 n_1 u_1}{2} & -c_0 n_1 u_1 \\ a_0 n_1 u_1 & \frac{t_1 + b_0 n_1 u_1}{2} \end{pmatrix}, \quad \tau_0^k = \begin{pmatrix} \frac{t_0 - b_0 n u_0}{2} & -c_0 n u_0 \\ a_0 n u_0 & \frac{t_0 + b_0 n u_0}{2} \end{pmatrix}.$$

Тогда

$$k = \frac{\ln((t_0 + q\sqrt{D}u_0)/2)}{\ln((t_1 + (q/p^\alpha)\sqrt{D}u_1)/2)},$$

и, значит, (3.3) верно.

Чтобы вычислить числитель дроби (3.3), предварительно выпишем систему представителей левых классов смежности $\Gamma_0(N_1)/\Gamma_0(N)$.

ПРЕДЛОЖЕНИЕ 6. Совокупность матриц $\begin{pmatrix} 1 + N_1j & 1 \\ N_1j & 1 \end{pmatrix}$, где j пробегает полную систему вычетов по модулю p^s , и матриц $\begin{pmatrix} 1 + N_1j & j \\ N_1 & 1 \end{pmatrix}$, где $j = 1 + j_0 + j_1p$, $j_0N_1 \equiv -1 \pmod{p}$ и j_1 пробегает полную систему вычетов по модулю p^{s-1} , образует полную систему представителей $\mathcal{R}_{N,N_1}$ левых классов смежности $\Gamma_0(N_1)/\Gamma_0(N)$.

ДОКАЗАТЕЛЬСТВО. Пусть

$$\begin{pmatrix} a & b \\ N_1c & d \end{pmatrix} \in \Gamma_0(N_1).$$

Требуется показать, что существуют $\sigma \in \mathcal{R}_{N,N_1}$ и $\begin{pmatrix} \alpha & \beta \\ N\gamma & \delta \end{pmatrix} \in \Gamma_0(N)$ такие, что

$$\begin{pmatrix} a & b \\ N_1c & d \end{pmatrix} = \sigma \begin{pmatrix} \alpha & \beta \\ N\gamma & \delta \end{pmatrix}.$$

1) $N_1c - a \not\equiv 0 \pmod{p}$. Будем искать σ вида $\begin{pmatrix} 1 + N_1j & 1 \\ N_1j & 1 \end{pmatrix}$, где j – любое целое. Тогда

$$\begin{pmatrix} a & b \\ N_1c & d \end{pmatrix} = \begin{pmatrix} \alpha + N_1\alpha j + N\gamma & \beta + N_1\beta j + \delta \\ N_1\alpha j + N\gamma & N_1\beta j + \delta \end{pmatrix}. \quad (3.4)$$

Значит, $\beta = b - d$, $\alpha = a - N_1c$. Приравнявая левые нижние элементы матриц в (3.4), получаем $(a - N_1c)j + p^s\gamma = c$. Так как $p \nmid (a - N_1c)$, то существует решение (j, γ) этого уравнения в целых числах. Остается положить $\delta = d - N_1\beta j$, и равенство (3.4) выполняется.

2) $N_1c - a \equiv 0 \pmod{p}$. Будем искать σ вида $\begin{pmatrix} 1 + N_1j & j \\ N_1 & 1 \end{pmatrix}$, где $j = 1 + j_0 + j_1p$ и $j_0N_1 \equiv -1 \pmod{p}$. Тогда

$$\begin{pmatrix} a & b \\ N_1c & d \end{pmatrix} = \begin{pmatrix} \alpha + N_1\alpha j + N\gamma j & \beta + N_1\beta j + \delta j \\ N_1\alpha + N\gamma & N_1\beta + \delta \end{pmatrix}. \quad (3.5)$$

Приравнявая левые столбцы в (3.5), получаем $\alpha = c - p^s\gamma$ и $a = N_1cj + c - p^s\gamma$. Отсюда следует, что $(a - N_1c)/p + k_0 = N_1cj_1 - p^{s-1}\gamma$, где $k_0 = -c(1 + j_0N_1)/p$. Здесь $(N_1c, p) = 1$, так как в противном случае $p \mid c$, и поскольку $p \mid (N_1c - a)$, то $p \mid a$, что невозможно. Следовательно, уравнение имеет решение в целых числах (j_1, γ) . Положим $\beta = b - jd$, $\delta = d - N_1\beta$, и равенство (3.5) выполняется. Условие $\sigma_1^{-1}\sigma_2 \notin \Gamma_0(N)$ для любых $\sigma_1, \sigma_2 \in \mathcal{R}_{N,N_1}$ проверяется непосредственно.

ПРИМЕР. $\Gamma_0(4N)$ и $\Gamma_0(N)$, где N нечетное, $p = 2$, $s = 2$.

Для представителей вида $\begin{pmatrix} 1 + Nj & 1 \\ Nj & 1 \end{pmatrix}$ берем $j = 0, 1, 2, 3$ и получаем матрицы

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 + N & 1 \\ N & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 + 2N & 1 \\ 2N & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 + 3N & 1 \\ 3N & 1 \end{pmatrix}.$$

Для представителей вида $\begin{pmatrix} 1+Nj & j \\ N & 1 \end{pmatrix}$, где $j = 1 + j_0 + j_1 2$, берем $j_0 = 1$; тогда $j = 2, 4$, и получаем матрицы

$$\begin{pmatrix} 1+2N & 2 \\ N & 1 \end{pmatrix}, \quad \begin{pmatrix} 1+4N & 4 \\ N & 1 \end{pmatrix}.$$

Шесть этих матриц и образуют полную систему представителей левых классов смежности $\Gamma_0(N)/\Gamma_0(4N)$.

Для вычисления числителя дроби (3.3) нам понадобится

ЛЕММА. Пусть $[a, b, c] \in \mathcal{F}_{N_1, N_1/n_1}((q/n)^2 D)$. Тогда существует форма $[a', b', c'] \sim [a, b, c]$ относительно $\Gamma_0(N_1)$ такая, что $p \nmid (a' + b' + c')$.

ДОКАЗАТЕЛЬСТВО. Положим

$$\sigma_j = \begin{pmatrix} jN_1 + 1 & 1 \\ jN_1 & 1 \end{pmatrix}, \quad [a_j, b_j, c_j] = \sigma_j^* [a, b, c] \sigma_j.$$

Отметим, что $c_j = a + b + c$. Рассмотрим возможные случаи.

1) $\alpha > \beta$. Пусть $p \mid (a + b + c)$. Тогда $p \mid c_0$, и поскольку $\alpha > \beta$, то $p \mid b_0$; значит, $p \nmid (a_0 + b_0 + c_0)$.

2) $\alpha = \beta$.

а) $\left(\frac{D}{p}\right) = -1$ при $p \neq 2$ и $D \equiv 5 \pmod{8}$ при $p = 2$. Пусть $p \mid (a + b + c)$. Тогда $p \mid c_0$, и поэтому $b_0^2 \equiv (q/n)^2 D \pmod{p}$ для $p \neq 2$ и $b_0^2 \equiv (q/n)^2 D \pmod{8}$ для $p = 2$. С другой стороны, в силу того, что $\alpha = \beta$, и условия а) получаем, что эти сравнения не имеют решения – противоречие.

б) $p \mid D$. Пусть $p \mid (a + b + c)$. Тогда $p \mid c_0$, и поскольку $p \mid D$, то $p \mid b_0$; следовательно, $p \nmid (a_0 + b_0 + c_0)$.

с) $p \neq 2$, $\left(\frac{D}{p}\right) = 1$. Пусть $p \mid (a + b + c)$. Тогда $p \mid c_0$ и $p \nmid b_0$. Если $p \mid (a_0 + b_0 + c_0)$, то рассмотрим форму $[a^{(p)}, b^{(p)}, c^{(p)}] = \sigma_p^* [a_0, b_0, c_0] \sigma_p$. Нетрудно убедиться, что

$$a^{(p)} + b^{(p)} + c^{(p)} \equiv 3a_0 + b_0 \pmod{p}.$$

Так как $p \mid c_0$, то $p \mid (a_0 + b_0)$, и так как $p \nmid b_0$, то $p \nmid a_0$; значит, $p \nmid (3a_0 + b_0)$. Следовательно, $p \nmid (a^{(p)} + b^{(p)} + c^{(p)})$, что и требовалось доказать.

д) $p = 2$, $D \equiv 1 \pmod{8}$. В этом случае $2 \nmid b$. Пусть $2 \mid (a + b + c)$; тогда $2 \mid c_0$, $2 \nmid b_0$. Если a_0 четно, то форма $[a_0, b_0, c_0]$ искомая, в противном случае возьмем форму $[a^{(1)}, b^{(1)}, c^{(1)}] = \sigma_1^* [a_0, b_0, c_0] \sigma_1$. Поскольку $a^{(1)} \equiv a_0 + N_1 a_0 \pmod{2}$, то $a^{(1)}$ четно и $2 \nmid (a^{(1)} + b^{(1)} + c^{(1)})$.

Лемма доказана.

Теперь опишем множество всех делителей n в (2.5) в терминах его канонического разложения. Сравнение $x^2 \equiv (q/n)^2 D \pmod{4N/n}$ разрешимо в том и только том случае, если для любого p_i , входящего в разложение (3.1), показатель степени β_i удовлетворяет одному из следующих взаимоисключающих условий:

$$\begin{aligned} 2\alpha_i - 2\beta_i &\geq s_i - \beta_i; \\ 2\alpha_i - 2\beta_i &= s_i - \beta_i - 1, \quad p_i \mid D; \\ 2\alpha_i - 2\beta_i &< s_i - \beta_i, \quad \left(\frac{D}{p_i}\right) = 1 \quad \text{при } p_i \neq 2, \quad D \equiv 1 \pmod{8} \quad \text{при } p_i = 2. \end{aligned} \tag{3.6}$$

Обозначим множество всех делителей n , удовлетворяющих условию (3.6), через $S(N, q)$. Тогда (2.5) можно переписать в следующем виде:

$$\nu(L, N) = \sum_{\substack{q|Q \\ q \nmid U_k, k|m, k \neq m}} \sum_{n \in S(N, q)} h_{N, N/n} \left(\left(\frac{q}{n} \right)^2 D \right). \quad (3.7)$$

ПРЕДЛОЖЕНИЕ 7. Пусть $[a, b, c] \in \mathcal{F}_{N_1, N_1/n_1}((q/n)^2 D)$. Тогда

$$\begin{aligned} \# \left\{ \sigma \in \mathcal{R}_{N, N_1} : \sigma^*[a, b, c] \sigma \in \mathcal{F}_{N, N/n} \left(\left(\frac{q}{n} \right)^2 D \right) \right\} \\ = \varepsilon(p, s, \alpha, \beta) p^{\lfloor \min(2\alpha, s+\beta)/2 \rfloor} \left(1 - \frac{\eta(p, s, \alpha, \beta)}{p} \right), \end{aligned} \quad (3.8)$$

где

$$\eta(p, s, \alpha, \beta) = \begin{cases} -1, & \text{если } 2\alpha - 2\beta = s - \beta = 0, \\ & \left(\frac{D}{p} \right) = -1 \text{ при } p \neq 2, \quad D \equiv 5 \pmod{8} \text{ при } p = 2; \\ 1, & \text{если } \beta > 0 \text{ и выполняется хотя бы одно из условий:} \\ & 2\alpha - 2\beta > s - \beta > 0, \quad s \equiv \beta \pmod{2}; \\ & 2\alpha - 2\beta = s - \beta > 0, \quad p \mid D; \\ & 2\alpha - 2\beta = s - \beta = 0, \\ & \left(\frac{D}{p} \right) = 1 \text{ при } p \neq 2, \quad D \equiv 1 \pmod{8} \text{ при } p = 2; \\ & 2\alpha - 2\beta < s - \beta, \\ & \left(\frac{D}{p} \right) = 1 \text{ при } p \neq 2, \quad D \equiv 1 \pmod{8} \text{ при } p = 2; \\ 2, & \text{если } \beta > 0 \text{ и выполняется условие} \\ & 2\alpha - 2\beta = s - \beta > 0, \\ & \left(\frac{D}{p} \right) = 1 \text{ при } p \neq 2, \quad D \equiv 1 \pmod{8} \text{ при } p = 2; \\ p, & \text{если } \beta > 0, \quad 2\alpha - 2\beta > s - \beta > 0, \quad s \not\equiv \beta \pmod{2}; \\ 0 & \text{в остальных случаях,} \end{cases}$$

$$\varepsilon(p, s, \alpha, \beta) = \begin{cases} 2, & \text{если } 2\alpha < s + \beta, \\ & \left(\frac{D}{p} \right) = 1 \text{ при } p \neq 2, \quad D \equiv 1 \pmod{8} \text{ при } p = 2; \\ 1 & \text{в противном случае.} \end{cases}$$

ДОКАЗАТЕЛЬСТВО. Согласно лемме возьмем квадратичную форму $[a, b, c]$, удовлетворяющую условию $p \nmid (a + b + c)$, и систему представителей $\mathcal{R}_{N, N_1}$, полученную в предложении 6. Вначале рассмотрим элементы $\mathcal{R}_{N, N_1}$ вида $\sigma_j = \begin{pmatrix} 1 + N_1 j & j \\ N_1 & 1 \end{pmatrix}$, где $j = 1 + j_0 + j_1 p$, а j_1 пробегает полную систему вычетов по модулю p^{s-1} и $N_1 j_0 \equiv -1 \pmod{p}$. Нетрудно проверить, что для формы $[a_j, b_j, c_j] = \sigma_j^*[a, b, c] \sigma_j$ справедливо сравнение $a_j \equiv N_1^2(a + b + c) \pmod{p}$. Условие $[a_j, b_j, c_j] \in \mathcal{F}_{N, N/n}((q/n)^2 D)$ эквивалентно выполнению равенства $(a_j, p^s) = p^{s-\beta}$. Отсюда заключаем, что при $s > \beta$ справедливо

$$[a_j, b_j, c_j] \notin \mathcal{F}_{N, N/n} \left(\left(\frac{q}{n} \right)^2 D \right),$$

а при $s = \beta$ все p^{s-1} элементов $\mathcal{R}_{N,N_1}$ данного вида переводят форму $[a, b, c]$ в $\mathcal{F}_{N,N/n}((q/n)^2 D)$. Запишем это в удобном для нас виде:

$$\#\{\sigma_j : (a_j, p^s) = p^{s-\beta}\} = \begin{cases} 0, & \text{если } s - \beta > 0, \\ p^{(s+\beta)/2} \frac{1}{p}, & \text{если } s - \beta = 0. \end{cases}$$

Теперь рассмотрим оставшуюся часть $\mathcal{R}_{N,N_1}$, т.е. элементы вида

$$\sigma_j = \begin{pmatrix} 1 + jN_1 & 1 \\ jN_1 & 1 \end{pmatrix},$$

где j пробегает полную систему вычетов по модулю p^s . Для формы $[a_j, b_j, c_j] = \sigma_j^*[a, b, c]\sigma_j$ имеем $a_j = a + jN_1(2a + b + jN_1(a + b + c))$. Поэтому условие $(a_j, p^s) = p^{s-\beta}$ выполняется тогда и только тогда, когда j является решением сравнения

$$j^2 N_1^2 (a + b + c) + jN_1(2a + b) + a \equiv 0 \pmod{p^\gamma} \quad (3.9)$$

при $\gamma = s - \beta$, и если $\beta > 0$, то j не является решением сравнения (3.9) при $\gamma = s - \beta + 1$. Домножая (3.9) на $4(a + b + c)$ и выделяя полный квадрат, получаем при $p \neq 2$ эквивалентную систему

$$\begin{cases} x^2 \equiv \left(\frac{a}{n}\right)^2 D \pmod{p^\gamma}, \\ x = 2N_1(a + b + c)j + 2a + b. \end{cases} \quad (3.10)$$

В случае $p = 2$ в (3.10) γ следует заменить на $\gamma + 2$. Мы найдем число различных $j \pmod{p^s}$, удовлетворяющих требуемому условию $(a_j, p^s) = p^{s-\beta}$, если подсчитаем число решений (x, j) системы (3.10) при $\gamma = s - \beta$ с различными $j \pmod{p^s}$ и в случае $\beta > 0$ вычтем из него число решений (x, j) системы (3.10) при $\gamma = s - \beta + 1$ с различными $j \pmod{p^s}$.

Рассмотрим вначале случай $p \neq 2$. Прежде всего, отметим, что тогда уравнение в (3.10) всегда разрешимо, поскольку $p \nmid (a + b + c)$, а решение сравнения образует одну или две арифметические прогрессии с шагом, равным степени p . При $2\alpha - 2\beta \geq \gamma$ и при $2\alpha - 2\beta = \gamma - 1, p \mid D$ решение сравнения имеет вид

$$x = p^{[(\gamma+1)/2]} k,$$

где k любое целое. Тогда получаем $p^{s-[(\gamma+1)/2]}$ решений уравнения с различными $j \pmod{p^s}$. При $2\alpha - 2\beta < \gamma$ и $\left(\frac{D}{p}\right) = 1$ решение сравнения имеет вид

$$x = \pm p^{\alpha-\beta} x_0 + p^{\gamma-(\alpha-\beta)} k, \quad p \nmid x_0.$$

Так как $\gamma - (\alpha - \beta) > \alpha - \beta$ и $p^s \nmid 2p^{\alpha-\beta} x_0$, то получаем $2p^{s-\gamma+(\alpha-\beta)}$ решений уравнения с различными $j \pmod{p^s}$. В остальных случаях сравнение решений не имеет. Приводим окончательный результат, следуя условиям (3.6).

1. Если $2\alpha - 2\beta > s - \beta$, то

$$\#\{\sigma_j : (a_j, p^s) = p^{s-\beta}\} = \begin{cases} p^{[(s+\beta)/2]}, & \text{если } \beta = 0, \\ p^{[(s+\beta)/2]} \left(1 - \frac{1}{p}\right), & \text{если } \beta \equiv s \pmod{2}, \\ 0, & \text{если } \beta \not\equiv s \pmod{2}. \end{cases}$$

2. Если $2\alpha - 2\beta = s - \beta$, то

$$\#\{\sigma_j : (a_j, p^s) = p^{s-\beta}\} = \begin{cases} p^{[(s+\beta)/2]}, & \text{если } \left(\frac{D}{p}\right) = -1 \text{ или } \beta = 0, \\ p^{[(s+\beta)/2]} \left(1 - \frac{1}{p}\right), & \text{если } p \mid D, \\ p^{[(s+\beta)/2]} \left(1 - \frac{2}{p}\right), & \text{если } \left(\frac{D}{p}\right) = 1. \end{cases}$$

3. Если $2\alpha - 2\beta = s - \beta - 1$ и $p \mid D$, то

$$\#\{\sigma_j : (a_j, p^s) = p^{s-\beta}\} = p^{[(s+\beta)/2]}.$$

4. Если $2\alpha - 2\beta < s - \beta$ и $(\frac{D}{p}) = 1$, то

$$\#\{\sigma_j : (a_j, p^s) = p^{s-\beta}\} = \begin{cases} 2p^\alpha, & \text{если } \beta = 0, \\ 2p^\alpha(1 - \frac{1}{p}), & \text{если } \beta > 0. \end{cases}$$

При $p = 2$ все решения сравнения в (3.10) образуют не более четырех арифметических прогрессий. Так как $\gamma + 2 \geq 2$, то шаг прогрессии есть степень двойки, и поэтому уравнение в (3.10) разрешимо только в том случае, если свободный член в уравнении есть четное число. Если $(q/n)^2 D$ четно, то b и x четны, в противном случае b и x нечетны, поэтому уравнение всегда имеет решение, если сравнение имеет решение. Покажем, что формулы для числа решений системы при $p = 2$ и $\gamma + 2$ в точности совпадают с формулами для $p \neq 2$ и γ .

Пусть $p \neq 2$ и решение сравнения при γ имеет вид $x = p^{[(\gamma+1)/2]}k$. Тогда при $p = 2$ и $\gamma + 2$ решение сравнения существует и имеет вид $x = 2^{[(\gamma+1)/2]+1}k$ или $x = 2^{[(\gamma+1)/2]} + 2^{[(\gamma+1)/2]+1}k$. Подставляя решение сравнения в уравнение и сокращая его на общий множитель, равный 2, получаем решение $j = j_0 + 2^{[(\gamma+1)/2]}k$. Тогда число решений системы (3.10) будет равно $2^{s-[(\gamma+1)/2]}$.

Пусть при $p \neq 2$ решение сравнения имеет вид $x = \pm p^{\alpha-\beta}x_0 + p^{\gamma-(\alpha-\beta)}k$, $p \nmid x_0$, $2\alpha - 2\beta < s - \beta$. Тогда при $p = 2$ имеем четыре решения сравнения: $\pm 2^{\alpha-\beta}x_1 + 2^{\gamma-(\alpha-\beta)+2}k$ и $\pm 2^{\alpha-\beta}x_2 + 2^{\gamma-(\alpha-\beta)+2}k$, где $x_1 \equiv 1 \pmod{8}$ и $x_2 \equiv 3 \pmod{8}$. Тогда каждому решению сравнения соответствует решение уравнения вида $j = j_0 + 2^{\gamma-(\alpha-\beta)+1}k$, что дает $2^{\max(0, s-\gamma+(\alpha-\beta)-1)}$ решений системы. Возьмем решения уравнения j_1 и j_2 , соответствующие различным решениям сравнения, и составим их разность; тогда получим

$$(a + b + c)(j_1 - j_2) = 2^{\alpha-\beta-1}(x_1 \pm x_2) + 2^{\gamma-(\alpha-\beta)+1}(k_1 \pm k_2),$$

где $x_1 + x_2 \equiv 4 \pmod{8}$ и $x_1 - x_2 \equiv 2 \pmod{8}$. Тогда первое слагаемое в правой части делится не более чем на $2^{\alpha-\beta+1}$, а поскольку $\gamma > 2\alpha - 2\beta$, то и левая часть делится не более чем на $2^{\alpha-\beta+1}$. Легко видеть, что $s = \alpha - \beta + 1$ только при $\alpha = \beta = 0$, и в этом случае число решений будет равно

$$2 \cdot 2^{\max(0, s-\gamma+(\alpha-\beta)-1)} = 2 \cdot 2^{s-\gamma+(\alpha-\beta)}.$$

В остальных случаях $s > \alpha - \beta + 1$, и, следовательно, все четыре решения сравнения несравнимы по модулю p^s , и число решений системы будет равно

$$4 \cdot 2^{\max(0, s-\gamma+(\alpha-\beta)-1)} = 2 \cdot 2^{s-\gamma+(\alpha-\beta)}.$$

Теперь, объединяя полученные выражения для числа представителей $\sigma \in \mathcal{R}_{N, N_1}$, для которых верно $(a_1, p^s) = p^{s-\beta}$, получаем требуемую формулу.

СЛЕДСТВИЕ 4. Пусть $n \in S(N, q)$. Тогда

$$\begin{aligned} h_{N, N/n} \left(\left(\frac{q}{n} \right)^2 D \right) \\ = \frac{\varepsilon(p, s, \alpha, \beta) p^{[\min(2\alpha, s+\beta)/2]} (1 - \eta(p, s, \alpha, \beta)/p)}{\ln((t_0 + q\sqrt{D}u_0)/2) / \ln((t_1 + (q/p^\alpha)\sqrt{D}u_1)/2)} h_{N_1, N_1/n_1} \left(\left(\frac{q}{n} \right)^2 D \right). \end{aligned} \quad (3.11)$$

Действительно, правая часть (3.3) согласно предложению 7 не зависит от класса $\mathcal{G}$ форм $\mathcal{F}_{N_1, N_1/n_1}((q/n)^2 D)$.

Теперь все готово, чтобы получить формулу, выражающую число классов квадратичных форм $\mathcal{F}_{N, N/n}((q/n)^2 D)$ через классическую функцию числа классов $h(q^2 D)$.

ПРЕДЛОЖЕНИЕ 8. Пусть $n \in S(N, q)$. Тогда

$$h_{N, N/n} \left(\left(\frac{q}{n} \right)^2 D \right) = \prod_{i=1}^{\omega(N)} f(p_i, s_i, \alpha_i, \beta_i) \cdot h(q^2 D),$$

где

$$f(p, s, \alpha, \beta) = \varepsilon(p, s, \alpha, \beta) p^{\lfloor \min(2\alpha-2\beta, s-\beta)/2 \rfloor} \left(1 - \frac{\bar{\eta}(p, s, \alpha, \beta)}{p} \right),$$

$$\bar{\eta}(p, s, \alpha, \beta) = \begin{cases} 1, & \text{если } \beta > 0 \text{ и выполняется хотя бы одно из условий:} \\ & 2\alpha - 2\beta > s - \beta > 0, \quad s \equiv \beta \pmod{2}; \\ & 2\alpha - 2\beta = s - \beta > 0, \quad p \mid D; \\ & 0 < 2\alpha - 2\beta < s - \beta, \\ & \quad \left(\frac{D}{p} \right) = 1 \text{ при } p \neq 2, \quad D \equiv 1 \pmod{8} \text{ при } p = 2; \\ 2, & \text{если } \beta > 0 \text{ и выполняется условие} \\ & 2\alpha - 2\beta = s - \beta > 0, \\ & \quad \left(\frac{D}{p} \right) = 1 \text{ при } p \neq 2, \quad D \equiv 1 \pmod{8} \text{ при } p = 2; \\ p, & \text{если } \beta > 0, \quad 2\alpha - 2\beta > s - \beta > 0, \quad s \not\equiv \beta \pmod{2}; \\ 0 & \text{в остальных случаях,} \end{cases} \quad (3.12)$$

а $\varepsilon(p, s, \alpha, \beta)$ определена в (3.9).

ДОКАЗАТЕЛЬСТВО. Так как $n \in S(N, q)$, то для любой пары множеств

$$\mathcal{F}_{N_i, N_i/n_i} \left(\left(\frac{q}{n} \right)^2 D \right), \quad \mathcal{F}_{N_{i+1}, N_{i+1}/n_{i+1}} \left(\left(\frac{q}{n} \right)^2 D \right)$$

верно (3.11). Применим (3.11) к последовательности (3.2), начиная с $N_1 = N$ и заканчивая $N_{\omega(N)} = 1$, а затем выразим $h((q/n)^2 D)$ через $h(q^2 D)$, для чего воспользуемся хорошо известной формулой

$$h(s^2 d) = s \prod_{p \mid s} \left(1 - j(d, p) \frac{1}{p} \right) \frac{\ln((t_1 + \sqrt{d} u_1)/2)}{\ln((t_0 + s\sqrt{d} u_0)/2)} h(d), \quad (3.13)$$

где $(t_0, u_0), (t_1, u_1)$ – фундаментальные решения уравнений Пелля $t^2 - s^2 du^2 = 4$ и $t^2 - du^2 = 4$ соответственно и

$$j(d, p) = \begin{cases} \left(\frac{d}{p} \right), & \text{если } p \neq 2, \\ \chi_8(d), & \text{если } p = 2, \end{cases}$$

$$\chi_8(d) = \begin{cases} 0, & \text{если } d \equiv 0 \pmod{2}, \\ 1, & \text{если } d \equiv 1, 7 \pmod{8}, \\ -1, & \text{если } d \equiv 3, 5 \pmod{8}. \end{cases} \quad (3.14)$$

Тогда из (3.11) и (3.13) следует

$$\frac{h_{N,N/n}((q/n)^2 D)}{h(q^2 D)} = \prod_{i=1}^{\omega(N)} \varepsilon(p_i, s_i, \alpha_i, \beta_i) \frac{p_i^{\lfloor \min(2\alpha_i - 2\beta_i, s_i - \beta_i)/2 \rfloor} (1 - \eta(p_i, s_i, \alpha_i, \beta_i)/p_i)}{1 - j(p_i^{2\alpha_i - 2\beta_i} D, p_i)/p_i}.$$

Знаменатель дроби отличен от 1 только при $\alpha_i = \beta_i$ и $p_i \nmid D$. Здесь возможны два случая.

1. $\left(\frac{D}{p_i}\right) = -1$ при $p_i \neq 2$ и $D \equiv 5 \pmod{8}$ при $p_i = 2$. Тогда в силу условий (3.6) $2\alpha_i - 2\beta_i \geq s_i - \beta_i$, и, значит, $s_i = \beta_i$. Согласно (3.8) в этом случае $\eta(p_i, s_i, \alpha_i, \beta_i) = -1$, поэтому следует положить $\bar{\eta}(p_i, s_i, \alpha_i, \beta_i) = 0$.

2. $\left(\frac{D}{p_i}\right) = 1$ при $p_i \neq 2$ и $D \equiv 1 \pmod{8}$ при $p_i = 2$. Тогда $\eta(p_i, s_i, \alpha_i, \beta_i) = 1$, и вновь следует положить $\bar{\eta}(p_i, s_i, \alpha_i, \beta_i) = 0$. Доказательство полностью закончено.

§ 4. Доказательство теоремы 1

Теперь формулу (3.4) мы можем переписать в следующем виде:

$$\nu(L, N) = \sum_{\substack{q|Q \\ q \nmid U_k, k|m, k \neq m}} \sum_{n \in S(N, q)} \prod_{i=1}^{\omega(N)} f(p_i, s_i, \alpha_i, \beta_i) h(q^2 D).$$

Легко заметить, что множество делителей $S(N, q)$ есть прямое произведение множеств $S(p_i^{s_i}, p_i^{\alpha_i})$, где $i = 1, \dots, \omega(N)$. Поэтому справедливо равенство

$$\sum_{n \in S(N, q)} \prod_{i=1}^{\omega(N)} f(p_i, s_i, \alpha_i, \beta_i) = \prod_{i=1}^{\omega(N)} \sum_{p_i^{\beta_i} \in S(p_i^{s_i}, p_i^{\alpha_i})} f(p_i, s_i, \alpha_i, \beta_i).$$

Покажем, что

$$\sum_{p^\beta \in S(p^s, p^\alpha)} f(p, s, \alpha, \beta) = \varepsilon_1(p, s, \alpha) (p^{\lfloor \min(2\alpha, s)/2 \rfloor} + \delta(p, s, \alpha) p^{\lfloor (\min(2\alpha, s) - 1)/2 \rfloor}),$$

где

$$\varepsilon_1(p, s, \alpha) = \begin{cases} 2, & \text{если } 2\alpha < s, \left(\frac{D}{p}\right) = 1 \text{ при } p \neq 2, D \equiv 1 \pmod{8} \text{ при } p = 2, \\ 1 & \text{в противном случае,} \end{cases}$$

а $\delta(p, s, \alpha)$ определено в (1.5).

Рассмотрим последовательно ряд возможных случаев.

1. $\alpha \geq s$. Тогда $\varepsilon(p, s, \alpha, \beta) = 1$ и $2\alpha - 2\beta \geq s - \beta$. Согласно (3.6) $\beta = s - k$, $k = 0, \dots, s$. В силу (3.12) $f(p, s, \alpha, \beta) = 0$ при k нечетном и не равном s , $\bar{\eta}(p, s, \alpha, \beta) = 0$ при $k = 0, s$ и $\bar{\eta}(p, s, \alpha, \beta) = 1$ для остальных k . Тогда получаем

$$\sum_{p^\beta \in S(p^s, p^\alpha)} f(p, s, \alpha, \beta) = 1 + \sum_{i=1}^{\lfloor (s-1)/2 \rfloor} (p^i - p^{i-1}) + p^{\lfloor s/2 \rfloor} = p^{\lfloor s/2 \rfloor} + p^{\lfloor (s-1)/2 \rfloor}.$$

2. $[s/2] < \alpha < s$.

а) $(\frac{D}{p}) = -1$ при $p \neq 2$ и $D \equiv 5 \pmod{8}$ при $p = 2$. При этом условия из (3.6) следует $2\alpha - 2\beta \geq s - \beta$. Тогда $\beta = 2\alpha - s - k$, $k = 0, \dots, 2\alpha - s$, и $\varepsilon(p, s, \alpha, \beta) = 1$. Из (3.12) следует $\bar{\eta}(p, s, \alpha, \beta) = 0$ при $\beta = 0$ и $\beta = 2\alpha - s$. Для остальных β $f(p, s, \alpha, \beta)$ принимает те же значения, что и в п. 1. Тогда получаем

$$\sum_{p^\beta \in S(p^s, p^\alpha)} f(p, s, \alpha, \beta) = p^{s-\alpha} + \sum_{i=1}^{\alpha - [(s+2)/2]} (p^{s-\alpha+i} - p^{s-\alpha+i-1}) + p^{[s/2]} = p^{[s/2]} + p^{[(s-1)/2]}.$$

б) $p \mid D$. В этом случае согласно (3.6) в сумме появляется дополнительное слагаемое $\beta = 2\alpha - s + 1$, однако при этом в силу (3.12) $\bar{\eta}(p, s, \alpha, 2\alpha - s) = 1$, $\bar{\eta}(p, s, \alpha, 2\alpha - s + 1) = 0$, и, следовательно, сумма вновь равна $p^{[s/2]} + p^{[(s-1)/2]}$.

с) $(\frac{D}{p}) = 1$ при $p \neq 2$ и $D \equiv 1 \pmod{8}$ при $p = 2$. В этом случае согласно (3.6) и (3.12) при $\beta = 0$ и $\beta = 2\alpha - s - 2i$, $i = 0, \dots, \alpha - [(s+2)/2]$, имеем $\varepsilon(p, s, \alpha, \beta) = 1$, а при $\beta = 2\alpha - s + i$, $i = 1, \dots, s - \alpha$, имеем $\varepsilon(p, s, \alpha, \beta) = 2$. При этом $\bar{\eta}(p, s, \alpha, 2\alpha - s) = 2$, $\bar{\eta}(p, s, \alpha, 0) = \bar{\eta}(p, s, \alpha, \alpha) = 0$ и $\bar{\eta}(p, s, \alpha, \beta) = 1$ для остальных β . Тогда получаем

$$\begin{aligned} \sum_{p^\beta \in S(p^s, p^\alpha)} f(p, s, \alpha, \beta) &= p^{s-\alpha} - 2p^{s-\alpha-1} + \sum_{i=1}^{\alpha - [(s+2)/2]} (p^{s-\alpha+i} - p^{s-\alpha+i-1}) + p^{[s/2]} \\ &\quad + 2 \sum_{i=1}^{s-\alpha-1} (p^{s-\alpha-i} - p^{s-\alpha-i-1}) + 2 = p^{[s/2]} + p^{[(s-1)/2]}. \end{aligned}$$

3. $2\alpha = s$.

а) $(\frac{D}{p}) = -1$ при $p \neq 2$ и $D \equiv 5 \pmod{8}$ при $p = 2$. При этих условиях согласно (3.6) и (3.12) $S(p^s, p^\alpha) = \{1\}$ и $f(p, s, \alpha, 0) = p^\alpha = p^{[2\alpha/2]}$.

б) $p \mid D$. Тогда из (3.6) и (3.12) следует $S(p^s, p^\alpha) = \{1, p\}$ и $f(p, s, \alpha, 0) + f(p, s, \alpha, 1) = p^{[2\alpha/2]} + p^{[(2\alpha-1)/2]}$.

с) $(\frac{D}{p}) = 1$ при $p \neq 2$ и $D \equiv 1 \pmod{8}$ при $p = 2$. В этом случае $\varepsilon(p, s, \alpha, 0) = 1$ и $\varepsilon(p, s, \alpha, 0) = 2$ при $\beta = 1, \dots, \alpha$, $\bar{\eta}(p, s, \alpha, 0) = \bar{\eta}(p, s, \alpha, \alpha) = 0$ и $\bar{\eta}(p, s, \alpha, \beta) = 1$ при $\beta = 1, \dots, \alpha - 1$. Тогда имеем

$$\sum_{p^\beta \in S(p^s, p^\alpha)} f(p, s, \alpha, \beta) = p^\alpha + 2 \sum_{i=1}^{\alpha-1} (p^{\alpha-i} - p^{\alpha-i-1}) + 2 = p^{[2\alpha/2]} + 2p^{[(2\alpha-1)/2]}.$$

4. $2\alpha < s$.

а) $p \mid D$. Из (3.6) и (3.12) следует $S(p^s, p^\alpha) = \{1\}$ и $f(p, s, \alpha, 0) = p^{[2\alpha/2]}$.

б) $(\frac{D}{p}) = 1$ при $p \neq 2$ и $D \equiv 1 \pmod{8}$ при $p = 2$. В этом случае $\varepsilon(p, s, \alpha, \beta) = 2$, $\beta = 0, \dots, \alpha$, $\bar{\eta}(p, s, \alpha, 0) = \bar{\eta}(p, s, \alpha, \alpha) = 0$ и $\bar{\eta}(p, s, \alpha, \beta) = 1$ при $\beta = 1, \dots, \alpha - 1$. Тогда имеем

$$\sum_{p^\beta \in S(p^s, p^\alpha)} f(p, s, \alpha, \beta) = 2p^\alpha + 2 \sum_{i=1}^{\alpha-1} (p^{\alpha-i} - p^{\alpha-i-1}) + 2 = 2(p^{[2\alpha/2]} + p^{[(2\alpha-1)/2]}).$$

Теперь, принимая во внимание, что

$$\prod_{i=1}^{\omega(N)} \varepsilon_1(p_i, s_i, \alpha_i) = 2^{\omega(N/(q^2 D, N))},$$

получаем утверждение теоремы 1.

В заключение этого параграфа получим хорошо известные (см. [2]) формулы для числа неэквивалентных параболических и эллиптических неподвижных точек группы $\Gamma_0(N)$.

1) *Эллиптический случай.* При $L = 0, 1$ дискриминант $L^2 - 4$ принимает значения $-4, -3$ соответственно, которые являются фундаментальными дискриминантами, значит, $q = n = 1$. Поскольку $h(-3) = h(-4) = 1$, то из (1.5) следует

$$\begin{aligned} \nu(1, N) &= \begin{cases} 2^{\omega(N/(3, N))}, & \text{если } x^2 \equiv -3 \pmod{N}, \\ 0 & \text{в противном случае,} \end{cases} \\ \nu(0, N) &= \begin{cases} 2^{\omega(N/(4, N))}, & \text{если } x^2 \equiv -1 \pmod{N}, \\ 0 & \text{в противном случае.} \end{cases} \end{aligned}$$

2) *Параболический случай.* Дискриминант $d = 0$ не представим в форме Q^2D , и поэтому условия (3.6) не распространяются на параболический случай. В системе (3.10) при $d = 0$ сравнение имеет вид $x^2 \equiv 0 \pmod{p^\gamma}$, и решение есть $x = p^{[(\gamma+1)/2]}k$ для любого γ . В (3.6) это соответствует условию $2\alpha - 2\beta > s - \beta$ для любого $\beta \leq s$. Тогда условие $2\alpha > s$ в (1.5) соответствует параболическому случаю, и, принимая во внимание, что $h(0) = 1$, из (1.5) немедленно следует формула для числа неэквивалентных параболических вершин

$$\nu(2, N) = \prod_{i=1}^{\omega(N)} (p_i^{[s_i/2]} + p_i^{[(s_i-1)/2]}).$$

§ 5. Двусторонняя оценка $\nu(L, 1)$

Отправным пунктом для получения оценок будут служить формулы (1.5) и (1.6).

ПРЕДЛОЖЕНИЕ 9.

$$\nu(L, 1) \ll L \log L \quad u \quad \frac{\nu(L, N)}{\nu(L, 1)} \ll \sqrt{N} \log^2 \log N.$$

ДОКАЗАТЕЛЬСТВО. Для всякого $q \mid U_m$ и $q \nmid U_k$, где $k \mid m$ и $k \neq m$, верно равенство

$$h(q^2D) = q \frac{\log((T_1 + \sqrt{D}U_1)/2)}{\log((L + \sqrt{D}Q)/2)} \prod_{p|q} \left(1 - j(D, p) \frac{1}{p}\right) h(D). \quad (5.1)$$

Из формулы Дирихле для фундаментального дискриминанта получаем

$$h(D) = \frac{D^{1/2}}{\log((T_1 + \sqrt{D}U_1)/2)} L(1, \chi_D), \quad (5.2)$$

где $L(1, \chi_D)$ — L -ряд Дирихле с примитивным вещественным характером χ_D .

Тогда из (1.6), (3.14), (5.1) и (5.2) следует

$$\nu(L, 1) \leq \frac{\sqrt{L^2 - 4} L(1, \chi_D)}{\log((L + \sqrt{L^2 - 4})/2) Q} \sum_{q|Q} q \prod_{p|q} \left(1 + \frac{1}{p}\right). \quad (5.3)$$

Для вещественного примитивного характера χ_D справедлива оценка $L(1, \chi_D) \ll \log D$ (см. [7]). Покажем, что верна оценка

$$\sum_{q|Q} q \prod_{p|q} \left(1 + \frac{1}{p}\right) \ll Q \log Q. \quad (5.4)$$

Справедлива следующая цепочка неравенств:

$$\sum_{q|Q} q \prod_{p|q} \left(1 + \frac{1}{p}\right) \leq \sum_{q|Q^*} q \leq Q^* \sum_{q \leq d(Q^*)} \frac{1}{q} \ll Q^* \frac{\log Q^*}{\log \log Q^*}, \quad (5.5)$$

где $Q^* = Q \prod_{p|Q} (1 + 1/p)$. Последняя оценка в (5.5) верна в силу неравенства $d(n) \leq \exp(c \log n / \log \log n)$ (см. [8; гл. 1, § 5]). Для числа простых делителей $\omega(n)$, очевидно, верна оценка $\omega(n) \ll \log n$. Поэтому имеем

$$\prod_{p|Q} \left(1 + \frac{1}{p}\right) \ll \log \log Q, \quad Q^* \ll Q \log \log Q.$$

Теперь из оценки Q^* и (5.5) получаем (5.4). Оценка $\nu(L, 1)$ следует из (5.3), оценки для L -ряда и (5.4).

Чтобы оценить $\nu(L, N)$, воспользуемся формулой (1.5). Во-первых, отметим, что, отбросив условие $x^2 \equiv q^2 D \pmod{4N}$, сумму правой части (1.5) мы не уменьшим. Во-вторых, наибольшее значение по N достигается, когда $N \mid Q^2$ и N – полный квадрат. Последнее требование выполняется, если положить $d = ND$, где D – некоторый фундаментальный дискриминант, найти решение (T, Q) уравнения Пелля $x^2 - dy^2 = 4$ и положить $L = T$. Тогда получаем

$$\frac{\nu(L, N)}{\nu(L, 1)} \leq \sqrt{N} \prod_{p|N} \left(1 + \frac{2}{p}\right) \ll \sqrt{N} \log^2 \log N.$$

Более тщательный анализ показывает, что справедлива точная оценка

$$\frac{\nu(L, N)}{\nu(L, 1)} \leq \prod_{i=1}^{\omega(N)} (p_i^{[s_i/2]} + p_i^{[(s_i-1)/2]} + 2),$$

однако мы не приводим доказательство, поскольку это заняло бы много места.

ПРЕДЛОЖЕНИЕ 10.

$$\nu(L, 1) \gg L^{1-\varepsilon}$$

для любого $\varepsilon > 0$.

ДОКАЗАТЕЛЬСТВО. Из (2.6) и теоремы 2 следует

$$\nu(L, 1) = \sum_{q|Q} h(q^2 D) - \sum_{k|m, k>1} \nu(T_k, 1). \quad (5.6)$$

Принимая во внимание формулы (5.1)–(5.3), получаем

$$\sum_{q|Q} h(q^2 D) \geq \frac{\sqrt{L^2 - 4} L(1, \chi_D)}{\log((L + \sqrt{L^2 - 4})/2) Q} \sum_{q|Q} \varphi(q),$$

где $\varphi(\cdot)$ – функция Эйлера. По теореме Зигеля (см. [9]) $L(1, \chi_D) \gg D^{-\varepsilon}$. Поэтому, принимая во внимание, что $\sum_{q|Q} \varphi(q) = Q$, получаем

$$\sum_{q|Q} h(q^2 D) \gg \frac{L}{\log L} D^{-\varepsilon}. \quad (5.7)$$

В силу предложения 9 имеем $\nu(T_k, 1) \ll T_k \log(T_k)$, а для T_k , очевидно, верна оценка $T_k \ll L^{1/k}$. Тогда получаем

$$\sum_{k|m, k>1} \nu(T_k, 1) \ll L^{1/2} \log L. \quad (5.8)$$

Теперь из формул (5.6)–(5.8) следует оценка для $\nu(L, 1)$.

В работе [3] была получена асимптотическая формула функции распределения $\pi_{\Gamma(1)}(T)$ норм примитивных гиперболических классов модулярной группы

$$\pi_{\Gamma(1)}(T) = \int_2^T \frac{dx}{\ln x} + O\left(\frac{T^{3/4}}{\sqrt{\ln T}}\right), \quad (5.9)$$

которая впоследствии была доказана для общего случая фуксовой группы первого рода (см. [10]) и получила название *теорема о простых геодезических* в силу того, что главные члены (5.9) и функции распределения простых чисел совпадают. Поэтому естественно предположить, что остаточный член в (5.9) есть величина $O(T^{1/2+\varepsilon})$. Для конгруэнц-подгрупп в работе [11] было получено степенное понижение $O(T^{7/10+\varepsilon})$. Авторами по формуле (1.6) был вычислен нормированный остаточный член (5.9) для модулярной группы

$$\theta(T) = \frac{\pi_{\Gamma(1)}(T) - \int_2^T \frac{dx}{\ln x}}{\sqrt{T}}$$

при $3 \leq T \leq 16000$. Результаты вычислений показывают, что $-0.43 \leq \theta(T) \leq 0.16$, минимум достигается при $T = 717$, а максимум при $T = 7778$. Более подробные результаты вычислений приведены в работе [5].

§ 6. Заключение

В статистической физике в связи с проблемой квантового хаоса ведутся активные вычисления чисел классов примитивных гиперболических элементов (количество замкнутых геодезических на римановой поверхности) для треугольных групп Гекке. Эти вычисления основаны на оптимальном переборе и требуют большого объема памяти. Полученная авторами настоящей статьи формула позволяет вычислять числа классов без перебора.

Используемый в настоящей работе прием перехода от уровня N к меньшему уровню N_1 может быть применен для получения явных формул, выражающих $\nu(L, N)$ через $\nu(L, N_1)$, а также арифметических величин, являющихся линейными комбинациями $\nu(L_k, N)$, которые возникают в формуле следа Сельберга и дзета-функции Сельберга. Авторами статьи получены некоторые результаты в этом направлении.

Список литературы

- [1] P. S. Schaller, “Geometry of Riemann surfaces based on closed geodesics”, *Bull. Amer. Math. Soc.*, **35**:3 (1998), 193–214.
- [2] Г. Шимура, *Введение в арифметическую теорию автоморфных функций*, Мир, М., 1973; пер. с англ.: G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publ. Math. Soc. Japan., **11**, Iwanami Shoten, Tokyo; Princeton Univ. Press, Princeton, NJ, 1971.
- [3] Н. В. Кузнецов, “Распределение норм примитивных гиперболических классов модулярной группы и асимптотические формулы для собственных значений оператора Лапласа–Бельтрами на фундаментальной области модулярной группы”, *Докл. АН СССР*, **242**:1 (1978), 40–43; англ. пер.: N. V. Kuznetsov, “The distribution of norms of primitive hyperbolic classes of the modular group and asymptotic formulas for the eigenvalues of the Laplace–Beltrami operator on a fundamental region of the modular group”, *Soviet Math. Dokl.*, **19** (1978), 1053–1056.
- [4] П. Г. Л. Дирихле, *Лекции по теории чисел*, ОНТИ, М.–Л., 1936; пер. с нем.: P. G. L. Dirichlet, *Vorlesungen über Zahlentheorie*, Vieweg, Braunschweig, 1894.
- [5] P. Sarnak, “Class numbers of indefinite binary quadratic forms”, *J. Number Theory*, **15**:2 (1982), 229–247.
- [6] В. В. Головчанский, М. Н. Смотров, *Явная формула для числа классов примитивных сопряженных гиперболических элементов группы $\Gamma_0(N)$* , Препринт, ХО ИПМ, Хабаровск, 1994.
- [7] Н. Г. Чудаков, *Введение в теорию L-функций Дирихле*, ОГИЗ, М.–Л., 1947.
- [8] К. Прахар, *Распределение простых чисел*, Мир, М., 1967; пер. с нем.: K. Prachar, *Primzahlverteilung*, Springer-Verlag, Berlin–Göttingen–Heidelberg, 1957.
- [9] Г. Дэвенпорт, *Мультипликативная теория чисел*, Наука, М., 1971; пер. с англ.: H. Davenport, *Multiplicative number theory*, Markham, Chicago, IL, 1967.
- [10] P. Sarnak, *Prime geodesic theorems*, Thesis Ph. D., Stanford University, 1980.
- [11] W. Luo, Z. Rudnick, P. Sarnak, “On Selberg’s eigenvalue conjecture”, *Geom. Funct. Anal.*, **5**:2 (1995), 387–401.

В. В. Головчанский (V. V. Golovchanskii)
Хабаровское отделение
Института прикладной математики ДВО РАН
E-mail: gsm@iam.khv.ru

Поступила в редакцию
15.03.2007 и 17.03.2007

М. Н. Смотров (M. N. Smotrov)
Хабаровское отделение
Института прикладной математики ДВО РАН
E-mail: gsm@iam.khv.ru