РОССИЙСКАЯ АКАДЕМИЯ НАУК
ДАЛЬНЕВОСТОЧНОЕ ОТДЕЛЕНИЕ

ИНСТИТУТ ПРИКЛАДНОЙ МАТЕМАТИКИ

Препринт

В. В. ГОЛОВЧАНСКИЙ, М. Н. СМОТРОВ

ЯВНАЯ ФОРМУЛА ДЛЯ ЧИСЛА КЛАССОВ ПРИМИТИВНЫХ СОПРЯЖЕННЫХ ГИПЕРБОЛИЧЕСКИХ ЭЛЕМЕНТОВ ГРУППЫ $\Gamma_0(N)$

Хабаровск
1994

УДК 511.33

Головчанский В. В., Смотров М. Н. Явная формула для числа классов примитивных сопряженных гиперболических элементов группы $\Gamma_0(N)$. 1994.-36 с.-(Препринт/РАН, Дальневосточное отделение. Институт прикладной математики).

В настоящей работе получена явная формула выражающая число классов сопряженных примитивных гиперболических элементов с данным следом группы $\Gamma_0(N)$ через числа классов неопределенных бинарных квадратичных форм некоторых дискриминантов.

Печатается по решению секции ученого совета Хабаровского отделения Института прикладной математики ДВО РАН.

Ответственный редактор чл.-корр. РАН Н.В. Кузнецов.

РОССИЙСКАЯ АКАДЕМИЯ НАУК
ДАЛЬНЕВОСТОЧНОЕ ОТДЕЛЕНИЕ

ИНСТИТУТ ПРИКЛАДНОЙ МАТЕМАТИКИ

Препринт

В.В.ГОЛОВЧАНСКИЙ, М.Н.СМОТРОВ

ЯВНАЯ ФОРМУЛА ДЛЯ ЧИСЛА КЛАССОВ ПРИМИТИВНЫХ СОПРЯЖЕННЫХ ГИПЕРБОЛИЧЕСКИХ ЭЛЕМЕНТОВ ГРУППЫ $\Gamma_0(N)$

Хабаровск
1994

УДК 511.33

Головчанский В. В., Смотров М. М. Явная формула для числа классов примитивных сопряженных гиперболических элементов группы $\Gamma_0(N)$. 1994.-36 с.(Препринт/РАН, Дальневосточное отделение. Институт прикладной математики).

В настоящей работе получена явная формула выражающая число классов сопряженных примитивных гиперболических элементов с данным следом группы $\Gamma_0(N)$ через числа классов неопределенных бинарных квадратичных форм некоторых дискриминаитов.

Печатается по решению секции ученого совета Хабаровского отделения Института прикладной математики ДВО РАН.

Ответственный редактор чл.-корр. РАН Н.В. Кузнецов.

§1.Обозначения и формулировка результатов.

Чтобы сформулировать результаты работы сначала напомним основные определения и введем обозначения.

Как обычно $SL_2(Z)$-модулярная группа и $\Gamma_0(N)$ ее конгруэнц-подгруппа, а именно:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(Z) \mid c \equiv 0 (\mathrm{mod}\ N) \right\}.$$

В частности $\Gamma_0(1) = SL_2(Z)$. Элемент $g \in SL_2(Z)$ называется *гиперболическим*, если абсолютная величина его следа больше двух, т.е. $|\mathrm{tr}(g)| = |a+d| > 2$.

Элементы g_1 и $g_2 \in \Gamma_0(N)$ называются *сопряженными в* $\Gamma_0(N)$, если существует $\sigma \in \Gamma_0(N)$ такое, что $\sigma^{-1} g_1 \sigma = g_2$. Это соотношение эквивалентности разбивает группу $\Gamma_0(N)$ на классы сопряженных элементов. Число классов сопряженных элементов $\Gamma_0(N)$ с данным следом L конечно. Обозначим через $\nu^{-}(L,N)$ число этих классов.

Гиперболический элемент $g \in \Gamma_0(N)$ называется *примитивным* если он не является степенью никакого другого элемента группы $\Gamma_0(N)$. Класс, представителем которого является примитивный элемент, также называется примитивным. Число классов сопряженных примитивных элементов будем обозначать через $\nu(L,N)$.

Мы будем рассматривать невырожденные неопределенные бинарные квадратичные формы $ax^2+bxy+cy^2$ с дискриминантом $\Delta=b^2-4ac$, которые для краткости будем обозначать через $[a,b,c]$. Каждой форме соответствует *фундаментальный* дискриминант D, определяемый следующим образом: пусть $\Delta = q^2 d$, где d - бесквадратное, тогда положим

$$D = \begin{cases} d, & \text{если } d \equiv 1 (\mathrm{mod}\ 4) \\ 4d, & \text{если } d \not\equiv 1 (\mathrm{mod}\ 4). \end{cases} \tag{1.1}$$

Для любой невырожденной бинарной формы ее дискриминант представим в виде произведения некоторого квадрата на фундаментальный дискриминант. В частности, $L^2-4 = Q^2 D$, при $|L| \neq 2$.

Для всякого $L \geq 3$ через T_1 и U_1 обозначим фундаментальное решение уравнения Пелля

$$t^2 - Du^2 = 4$$

а через T_k и U_k обозначим решение этого уравнения, которое определяется из соотношения

$$\frac{T_k + U_k\sqrt{D}}{2} = \left(\frac{T_1 + U_1\sqrt{D}}{2} \right)^k. \tag{1.2}$$

Для каждого следа $L \geq 3$ определим число m из соотношения

$$\frac{L + Q\sqrt{D}}{2} = \left(\frac{T_1 + U_1\sqrt{D}}{2} \right)^m, \tag{1.3}$$

тогда $Q = U_m$, $L = T_m$.

Всюду, где не оговорено противное $(a_1,..,a_n) = \mathrm{НОД}(a_1,..,a_2)$.

Во введенных обозначениях сформулируем основные результаты :

ТЕОРЕМА 1. Пусть $L \geq 3$, $N \geq 1$ и каноническое разложение N имеет вид $N = \prod_{i=1}^{\omega(N)} p_i^{s_i}$,

тогда

$$\nu(L,N) = \sum_{\substack{q \mid Q \\ q \nmid U_k,\ k \mid m,\ k \neq m \\ x^2 \equiv q^2 D \pmod{4N}}} 2^{\omega\left(\frac{N}{(q^2D,N)}\right)} \times \prod_{i=1}^{\omega(N)} \left(p_i^{\left[\frac{\min(2\beta_i, s_i)}{2}\right]} + \delta(p_i, s_i, \beta_i)\, p_i^{\left[\frac{\min(2\beta_i, s_i)-1}{2}\right]} \right) \times h(q^2D),$$

где $\omega(N)$ - число простых делителей N, $q = q_1 \prod_{i=1}^{\omega(N)} p_i^{\beta_i}$ и $(q_1, N) = 1$, $[*]$-целая часть числа, $h(*)$ - классическая функция числа классов примитивных квадратичных форм данного дискриминанта,

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

$\left(\frac{*}{*}\right)$-символ Лежандра.

СЛЕДСТВИЕ 1. Пусть $L \geq 3$ и N-бесквадратное, тогда

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

где $d(*)$-функция числа делителей.

СЛЕДСТВИЕ 2. Пусть $L \geq 3$ и $N = 1$, тогда

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

ТЕОРЕМА 2. Пусть $L \leq -3$ и $m = 2^k m_1$, где $(m_1, 2) = 1$, тогда

$$\nu(L,N) = \sum_{i=0}^{k} \nu(T_{2^i m_1}, N).$$

ТЕОРЕМА 3. Пусть $|L| \geq 3$, тогда

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

Введем обозначение $\overline{\Gamma}_0(N) = \Gamma_0(N) \Big/ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Элемент $\overline{g} = \{\pm g\} \in \overline{\Gamma}_0(N)$ называется

гиперболическим если g - гиперболический. Норма элемента $\bar{g}$ задается следующей формулой:

$$N(\bar{g}) = \left(\frac{|L| + \sqrt{L^2 - 4}}{2} \right)^2, \qquad (1.4)$$

где L-след g.

Обозначим через $\bar{\nu}^-(L,N)$ число классов сопряженных гиперболических (соответственно через $\bar{\nu}(L,N)$ число классов сопряженных примитивных гиперболических) элементов $\bar{\Gamma}_0(N)$ с данной нормой $\left(\frac{L+\sqrt{L^2-4}}{2} \right)^2$, $L \geq 3$.

Легко заметить, что при $L \geq 3$ $\bar{\nu}^-(L,N) = \nu^-(L,N)$ и $\bar{\nu}(L,N) = \nu(L,N)$.

В §5 мы приводим результаты численных экспериментов с формулой из теоремы 1.

§2.Неопределенные квадратичные формы и примитивные гиперболические элементы.

Определим три множества:

$\mathcal{F}$-множество неопределенных примитивных квадратичных форм;

$F_N = \{ [a,b,c] : N \mid a, \left[\frac{a}{N}, b, c \right] \in \mathcal{F} \}$;

G_N - множество примитивных гиперболических элементов $\Gamma_0(N)$ с положительным следом.

ПРЕДЛОЖЕНИЕ 2.1. Если $[a,b,c] \in F_N$ и $n = (a,b,c)$, то

i) $n \mid N$ и $\left(\frac{a}{N}, n \right) = 1$;

ii) соответствие $[a,b,c] \longmapsto \left[\frac{a}{n}, \frac{b}{n}, \frac{c}{n} \right]$ задает биекцию $\phi: F_N \longrightarrow \mathcal{F}$.

ДОКАЗАТЕЛЬСТВО. i) легко следует из определения множества F_N.

Докажем ii). Инъективность. Пусть $[a_1,b_1,c_1] \neq [a_2,b_2,c_2]$, n_1, n_2 - наибольшие общие делители коэффициентов первой и второй форм соответственно. Предположим, что

$$\left[\frac{a_1}{n_1}, \frac{b_1}{n_1}, \frac{c_1}{n_1} \right] = \left[\frac{a_2}{n_2}, \frac{b_2}{n_2}, \frac{c_2}{n_2} \right].$$

Ясно, что $n_1 \neq n_2$. Для определенности положим $n_1 < n_2$. Тогда существует простое p, которое входит в n_1 с кратностью $s_1 \geq 0$ и в n_2 с кратностью $s_2 > 0$, причем $s_2 > s_1$. Так как $n_2 \mid N$, то p входит в разложение N с кратностью $s \geq s_2$. Из нашего предположения и очевидного факта: $p^{s-s_1} \mid \frac{a_1}{n_1}$ следует, что $p^{s-s_1} \mid \frac{a_2}{n_2}$. Значит $p^{s+s_2-s_1} \mid a_2$ и тогда $p^{s_2-s_1} \mid \frac{a_2}{N}$, с $s_2 - s_1 > 0$, а поскольку $p^{s_2} \mid b_2$ и $p^{s_2} \mid c_2$

получаем, что форма $\left[\frac{a_2}{N}, b_2, c_2\right]$ - непримитивная, противоречие.

Сюръективность. Пусть $[a,b,c] \in \mathcal{F}$. Возьмем $n = \frac{N}{(a,N)}$ и покажем, что квадратичная форма $[na,nb,nc] \in F_N$. Действительно $N \mid na$ и так как $(a,b,c) = 1$, то имеем

$$\left(\frac{na}{N}, nb, nc\right) = \left(\frac{a}{(a,N)}, \frac{Nb}{(a,N)}, \frac{Nc}{(a,N)}\right) = \left(\frac{a}{(a,N)}, \frac{N}{(a,N)}\right) = 1,$$

значит $[na,nb,nc] \in F_N$.■

Обозначим через $\mathrm{Aut}_N([a,b,c])$ группу автоморфизмов формы $[a,b,c]$ в $\Gamma_0(N)$ относительно действия $[a,b,c] \longmapsto \gamma^t[a,b,c]\gamma$, $\gamma \in \Gamma_0(N)$.

ПРЕДЛОЖЕНИЕ 2.2. Пусть $[a,b,c] \in F_N$. Тогда $\mathrm{Aut}_N([a,b,c])$ есть циклическая группа с образующей $\pm\begin{pmatrix} (t_1 - bu_1)/2 & -cu_1 \\ au_1 & (t_1 + bu_1)/2 \end{pmatrix}$, где пара (t_1,u_1) - фундаментальное решение уравнения $t^2 - du^2 = 4$ с $d = b^2 - 4ac$, и образующая примитивна в $\overline{\Gamma}_0(N)$

ДОКАЗАТЕЛЬСТВО. Вначале найдем $\mathrm{Aut}_1([a,b,c])$. Очевидно

$$[a,b,c] = \begin{pmatrix} \sqrt{n} & 0 \\ 0 & \sqrt{n} \end{pmatrix} \left[\frac{a}{n}, \frac{b}{n}, \frac{c}{n}\right] \begin{pmatrix} \sqrt{n} & 0 \\ 0 & \sqrt{n} \end{pmatrix}, \text{ где } n = (a,b,c).$$

Отсюда следует $\mathrm{Aut}_1([a,b,c]) = \mathrm{Aut}_1\left(\left[\frac{a}{n}, \frac{b}{n}, \frac{c}{n}\right]\right)$. Так как $\left[\frac{a}{n}, \frac{b}{n}, \frac{c}{n}\right]$ - примитивная форма, то как известно [3] $\mathrm{Aut}_1\left(\left[\frac{a}{n}, \frac{b}{n}, \frac{c}{n}\right]\right)$ - циклическая группа и ее образующая

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

примитивный элемент в $\overline{\Gamma}_0(1)$, где (t_1^*, u_1^*) - фундаментальное решение уравнения $t^2 - d_1u^2 = 4$ с $d_1 = d/n^2$.

Пусть (t_1,u_1) - фундаментальное решение уравнения $t^2 - du^2 = 4$, тогда пара (t_1, nu_1) есть решение уравнения $t^2 - d_1u^2 = 4$. Из этого следует существование $k \geq 1$ такого, что

$$\left(\frac{t_1^* + \sqrt{d_1}u_1^*}{2}\right)^k = \frac{t_k^* + \sqrt{d_1}u_k^*}{2} = \frac{t_1 + \sqrt{d_1}nu_1}{2}.$$

Из последнего следует,что

$$\gamma_0^k=\pm\begin{pmatrix}(t_k^*-\frac{b}{n}u_k^*)/2 & -\frac{c}{n}u_k^*\\ \frac{a}{n}u_k^* & (t_k^*+\frac{b}{n}u_k^*)/2\end{pmatrix}=\pm\begin{pmatrix}(t_1-bu_1)/2 & -cu_1\\ au_1 & (t_1+bu_1)/2\end{pmatrix}\in \mathrm{Aut}_N([a,b,c])$$

Покажем, что γ_0^k - образующая $\mathrm{Aut}_N([a,b,c])$. Допустим, что это не так. Тогда существует l такое, что $1\le l<k$ и $\gamma_0^l\in \mathrm{Aut}_N([a,b,c])$. Очевидно $\gamma_0^l\in \mathrm{Aut}_N([a,b,c])$ тогда и только тогда, когда $N\mid\left(\frac{a}{n}u_l^*\right)$. Из предложения 2.1 пункт i) видно, что условие $N\mid\left(\frac{a}{n}u_l^*\right)$ эквивалентно $n\mid u_l^*$ и поэтому пара чисел $(t_l^*,u_l^*/n)$ есть решение уравнения $t^2-du^2=4$. Поскольку (t_1,u_1)фундаментальное решение последнего уравнения, то тогда существует $r\ge 1$ и

$$\left(\frac{t_1^*+\sqrt{d}_1u_1^*}{2}\right)^l=\frac{t_l^*+\sqrt{d}_1u_l^*}{2}=\left(\frac{t_1+\sqrt{d}u_1}{2}\right)^r=\left(\frac{t_1^*+\sqrt{d}_1u_1^*}{2}\right)^{rk}.$$

Отсюда следует, что $l=rk$- чего не может быть. Из того факта, что γ_0^k образующая $\mathrm{Aut}_N([a,b,c])$ легко показать (методом от противного), что γ_0^k примитивен в $\Gamma_0(N)$.■

Формы $[a,b,c]$ и $[a',b',c']$ будем называть $\Gamma_0(N)$ эквивалентными и писать

$$[a,b,c]\overset{\Gamma_0(N)}{\sim}[a',b',c']$$

если существует $\gamma\in\Gamma_0(N)$ такой, что $[a',b',c']=\gamma^t[a,b,c]\gamma$. Заметим, что для любой формы $[a,b,c]\in F_N$ и любого $\gamma\in\Gamma_0(N)$ верно $\gamma^t[a,b,c]\gamma\in F_N$ и поэтому F_N распадается на классы эквивалентности по $\Gamma_0(N)$.

ПРЕДЛОЖЕНИЕ 2.3. Отображение $f: F_N\longrightarrow G_N$ заданное соответствием

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

где пара (t_1, u_1) - фундаментальное решение уравнения $t^2-du^2=4$ с $d=b^2-4ac$, биективно. Обратное к f отображение задается правилом

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

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

ДОКАЗАТЕЛЬСТВО. Отображение задано корректно, так как согласно предложению 2.2 элемент в правой части (2.1) примитивен в $\Gamma_0(N)$.

Инъективность. Пусть $[a_1,b_1,c_1]\ne[a_2,b_2,c_2]$, тогда согласно предложению 2.1 пункт ii) $\left[\frac{a_1}{n_1},\frac{b_1}{n_1},\frac{c_1}{n_1}\right]\ne\left[\frac{a_2}{n_2},\frac{b_2}{n_2},\frac{c_2}{n_2}\right]$, где $n_i=(a_i,b_i,c_i)$, $i=1,2$. Как показано в [3] образующие в $\mathrm{Aut}_1\left(\left[\frac{a_i}{n_i},\frac{b_i}{n_i},\frac{c_i}{n_i}\right]\right)$, $i=1,2$, неравны и примити-

вны в $\overline{\Gamma}_0(1)$. Поскольку $\mathrm{Aut}_1\left(\left[\frac{a_i}{n_i},\frac{b_i}{n_i},\frac{c_i}{n_i}\right]\right)=\mathrm{Aut}_1([a_i,b_i,c])$ и очевидно $\mathrm{Aut}_N([a_i,b_i,c_i])\subset \mathrm{Aut}_1([a_i,b_i,c_i])$, то образующие $\mathrm{Aut}_N([a_1,b_1,c_1])$ и $\mathrm{Aut}_N([a_2,b_2,c_2])$ неравны, что и требовалось доказать.

Сюръективность. Пусть $\sigma=\begin{pmatrix}\alpha & \beta\\ N\gamma & \delta\end{pmatrix}\in G_N$. Рассмотрим квадратичную форму

$$\left[\frac{N\gamma}{(\delta-\alpha,\gamma,\beta)},\frac{\delta-\alpha}{(\delta-\alpha,\gamma,\beta)},\frac{-\beta}{(\delta-\alpha,\gamma,\beta)}\right]\equiv[a,b,c].$$

Ясно, что $[a,b,c]\in F_N$. Непосредственно проверяется, что $\sigma^t[a,b,c]\sigma=[a,b,c]$, то есть $\sigma\in \mathrm{Aut}_N([a,b,c])$.Так как σ примитивна в $\Gamma_0(N)$, значит σ является образующей $\mathrm{Aut}_N([a,b,c])$ и образ формы $[a,b,c]$ равен σ, что и требовалось доказать.

Пусть $[a,b,c]\overset{\Gamma_0(N)}{\sim}[a',b',c']$. Очевидно существует $\sigma\in\Gamma_0(N)$ такое, что $\mathrm{Aut}_N([a,b,c])=\sigma^{-1}\mathrm{Aut}_N([a',b',c'])\sigma$. Отсюда и следует взаимнооднозначность отображения классов.■

Введем обозначення:

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

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

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

Очевидно, что $F_N=\bigcup_{n\mid N}F_{N,n}$ и $F_{N,i}\cap F_{N,j}=\emptyset$ ($i\neq j$) и $F_{N,n}$ является объединением классов эквивалентности его элементов по группе $\Gamma_0(N)$.

Обозначим через $\tilde{h}_{N,n}(d)$ число классов эквивалентных форм $F_{N,n}(d)$. В этих обозначениях имеем:

ПРЕДЛОЖЕНИЕ 2.4. Пусть $L\geq 3$. Тогда

$$\nu(L,N)=\sum_{\substack{q\mid Q\\ q\nmid U_k,\ k\mid m,\ k\neq m}}\ \sum_{n\mid(N,q)}\tilde{h}_{N,n}(q^2D).$$

ДОКАЗАТЕЛЬСТВО. Найдем $M\subset F_N$ такое, что $f(M)=G_N(L)$, где f -отображение определенное в (2.1).

Пусть $\begin{pmatrix}\alpha & \beta\\ N\gamma & \delta\end{pmatrix}\in G_N(L)$, его прообраз в F_N есть $\left[\frac{N\gamma}{(\delta-\alpha,\gamma,\beta)},\frac{\delta-\alpha}{(\delta-\alpha,\gamma,\beta)},\frac{-\beta}{(\delta-\alpha,\gamma,\beta)}\right]=[a,b,c]$ (предложение 2.3).

Непосредственно проверяется, что $b^2-4ac=\frac{L^2-4}{(\delta-\alpha,\gamma,\beta)^2}$. Тогда $[a,b,c]\in F_{N,n}(q^2D)$, где $n=\frac{(\delta-\alpha,N\gamma,\beta)}{(\delta-\alpha,\gamma,\beta)}$, $q=\frac{Q}{(\delta-\alpha,\gamma,\beta)}$. Отсюда $n\mid q$. Согласно предложению 2.1 i) $n\mid N$, значит $n\mid(N,q)$. Следовательно прообраз $G_N(L)$ содержится в

множестве $M' = \bigcup_{q \mid Q} \bigcup_{n \mid (N,q)} F_{N,n}(q^2 D)$.

Покажем, что если $[a,b,c] \in M'$, то $f([a,b,c]) \in G_N(L)$ тогда и только тогда, когда $q \nmid U_k$ для всех U_k, где $k \mid m$ и $k \neq m$.

Пусть q удовлетворяет этому условию. Тогда $(L, \frac{Q}{q})$ - фундаментальное решение уравнения $t^2 - q^2 D u^2 = 4$ и

$$f([a,b,c]) = \begin{pmatrix} (L - b\frac{Q}{q})/2 & -c\frac{Q}{q} \\ a\frac{Q}{q} & (L + b\frac{Q}{q})/2 \end{pmatrix} \in G_N(L).$$

Обратно, предположим $q \mid U_k$ для некоторых k и обозначим наименьшее из них k_0. Фундаментальное решение уравнения $t^2 - q^2 D u^2 = 4$ есть $\left(T_{k_0}, \frac{U_{k_0}}{q}\right)$ и $T_{k_0} < L$, значит $f([a,b,c]) \notin G_N(L)$.

Отсюда заключаем, что $M = \bigcup_{\substack{q \mid Q \\ q \mid U_k, k \mid m, k \neq m}} \bigcup_{n \mid (N,q)} F_{N,n}(q^2 D)$. Поскольку $F_{N,n}(d)$ есть объединение классов эквивалентности, то отсюда и следует требуемая формула.■

Положим

$$\mathcal{F}_{N,k}(d) = \{ [a,b,c] \in \mathcal{F} : (a,N) = k,\ b^2 - 4ac = d \}, \tag{2.2}$$

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

Из того, что отображение $F_{N,n}(q^2 D) \longrightarrow \mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$ задаваемое формулой $[a,b,c] \longmapsto \left[\frac{a}{n}, \frac{b}{n}, \frac{c}{n}\right]$, где $n = (a,b,c)$, биективно и классы отображаются в классы (это легко видно из предложения 2.1) следует $\tilde{h}_{N,n}(q^2 D) = h_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$. И поэтому верно

СЛЕДСТВИЕ. Пусть $L \geq 3$. Тогда

$$\nu(L,N) = \sum_{\substack{q \mid Q \\ q \nmid U_k,\ k \mid m,\ k \neq m}} \sum_{n \mid (N,q)} h_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right). \tag{2.3}$$

ПРЕДЛОЖЕНИЕ 2.5. Для $L \geq 3$

$$G_N(L) \neq \emptyset \Longleftrightarrow L^2 - 4 \text{ - квадратичный вычет по модулю } 4N.$$

ДОКАЗАТЕЛЬСТВО. Пусть $\sigma = \begin{pmatrix} \alpha & \beta \\ N\gamma & \delta \end{pmatrix} \in G_N(L)$. Положим $\delta - \alpha = x_0$, тогда $\alpha = (L - x_0)/2$, $\delta = (L + x_0)/2$. Поскольку $\det(\sigma) = 1$, то $L^2 - 4 = x_0^2 + 4N\gamma\beta$ и

сравнение $x^2 \equiv L^2 - 4 (\mathrm{mod}\ 4N)$ разрешимо.

Обратно, пусть сравнение $x^2 \equiv L^2 - 4 (\mathrm{mod}\ 4N)$ разрешимо и x_0 - некоторое решение. Тогда $L^2 - 4 = x_0^2 + 4Nk_0$ и поэтому $(L \pm x_0)/2$ целые числа и $\sigma = \begin{pmatrix} (L-x_0)/2 & k_0 \\ N & (L+x_0)/2 \end{pmatrix} \in \Gamma_0(N)$, $\mathrm{tr}(\sigma) = L$. Допустим, что σ – непримитивный элемент в $\Gamma_0(N)$. Тогда существует $k > 1$ и $\sigma = \sigma_1^k$, где σ_1 примитивен в $\Gamma_0(N)$. Тогда в силу предложения 2.3 $\sigma = \begin{pmatrix} (t_1 - bu_1)/2 & -cu_1 \\ au_1 & (t_1 + bu_1)/2 \end{pmatrix}^k$, где $[a,b,c] \in F_N$, так как $N \mid a$ и $u_k > 1$, то $au_k > N$ - противоречие.■

§3. Доказательство теорем 2 и 3.

ЛЕММА. Пусть $L \geq 3$. Тогда

$$\nu^-(L,N) = \sum_{q \mid Q} \sum_{n \mid (N,q)} \tilde{h}_{N,n}(q^2 D).$$

ДОКАЗАТЕЛЬСТВО. Обозначим через $G_N^-(L)$ множество гиперболических элементов $\Gamma_0(N)$ с положительным следом L. Покажем, что отображение

$$f^- : \bigcup_{q \mid Q} \bigcup_{n \mid (N,q)} F_{N,n}(q^2 D) \longrightarrow G_N^-(L) \qquad (3.1)$$

задаваемое формулой

$$[a,b,c] \longmapsto \begin{pmatrix} (L - b\frac{Q}{q})/2 & -c\frac{Q}{q} \\ a\frac{Q}{q} & (L + b\frac{Q}{q})/2 \end{pmatrix},$$

биективно и классы форм взаимнооднозначно отображаются в классы сопряженных гиперболических элементов.

Инъективность. Пусть $[a,b,c] \neq [a_1,b_1,c_1]$. Если $q = q_1$, то очевидно образы различны. Пусть $q \neq q_1$. Допустим, что

$$\begin{pmatrix} (L - b\frac{Q}{q})/2 & -c\frac{Q}{q} \\ a\frac{Q}{q} & (L + b\frac{Q}{q})/2 \end{pmatrix} = \begin{pmatrix} (L - b_1\frac{Q}{q_1})/2 & -c_1\frac{Q}{q_1} \\ a_1\frac{Q}{q_1} & (L + b_1\frac{Q}{q_1})/2 \end{pmatrix}.$$

Можно считать, что $(q,q_1) = 1$, в противном случае сократим q и q_1 на их общий делитель и равенство сохранится. Из равенства следует $\frac{a}{Nq} = \frac{a_1}{Nq_1}$, $\frac{b}{q} = \frac{b_1}{q_1}$, $\frac{c}{q} = \frac{c_1}{q_1}$. Так как q и q_1 взаимно просты, то $q \mid (\frac{a}{N}, b, c)$ и $q_1 \mid (\frac{a_1}{N}, b_1, c_1)$. Поскольку $q \neq q_1$, то по крайней мере одно из них отлично от единицы. Тогда либо $[a/N, b, c]$, либо $[a_1/N, b_1, c_1]$ непримитивна - противоречие.

Сюръективность. Пусть $\begin{pmatrix} \alpha & \beta \\ N\gamma & \delta \end{pmatrix} \in G_N^-(L)$. Возьмем форму

$$\left[\frac{N\gamma}{(\delta-\alpha,\gamma,\beta)},\frac{\delta-\alpha}{(\delta-\alpha,\gamma,\beta)},\frac{-\beta}{(\delta-\alpha,\gamma,\beta)}\right]\equiv[a,b,c]\in F_N.$$

Ее дискриминант равен q^2D, где $q=Q/(\delta-\alpha,\gamma,\beta)$. Поэтому

$$\begin{pmatrix}(L-b\frac{Q}{q})/2 & -c\frac{Q}{q}\\ a\frac{Q}{q} & (L+b\frac{Q}{q})/2\end{pmatrix}=\begin{pmatrix}\alpha & \beta\\ N\gamma & \delta\end{pmatrix}$$

и очевидно $(a,b,c)\,|\,(N,q)$.

Осталось показать, что эквивалентные формы отображаются в один класс сопряженных гиперболических элементов и обратно. Пусть

$$[a_1,b_1,c_1]^{\Gamma_0(N)}_{\sim}[a_2,b_2,c_2],$$

тогда $q_1=q_2=q$. Так как пара $(L,Q/q)$ есть решение уравнения Пелля $t^2-q^2Du^2=4$, то

$$\begin{pmatrix}(L-b_i\frac{Q}{q})/2 & -c_i\frac{Q}{q}\\ a_i\frac{Q}{q} & (L+b_i\frac{Q}{q})/2\end{pmatrix}=\begin{pmatrix}(t_1-b_iu_1)/2 & -c_iu_1\\ a_iu_1 & (t_1+b_iu_1)/2\end{pmatrix}^k,\ i=1,2,$$

где (t_1,u_1) – фундаментальное решение того же уравнения и $k\geq 1$. Отсюда следует, что $f([a_1,b_1,c_1])\sim f([a_2,b_2,c_2])$.

Обратно, пусть τ_1 и τ_2 - сопряженные элементы из $G_N(L)$, значит существуют единственные примитивные σ_1 и σ_2 и $k\geq 1$ такие, что $\tau_i=\sigma_i^k$.

С другой стороны

$$\tau_i=\begin{pmatrix}(L-b_i\frac{Q}{q_i})/2 & -c_i\frac{Q}{q_i}\\ a_i\frac{Q}{q_i} & (L+b_i\frac{Q}{q_i})/2\end{pmatrix},\ i=1,2$$

и отсюда следует $q_1=q_2=q$. Тогда имеет место

$$\tau_i=\begin{pmatrix}(t_1-b_iu_1)/2 & -c_iu_1\\ a_iu_1 & (t_1+b_iu_1)/2\end{pmatrix}^k,$$

где (t_1,u_1) – фундаментальное решение уравнения $t^2-q^2Du^2=4$. Поскольку τ_1 и τ_2 сопряжены, то $\sqrt[k]{\tau_1}$ и $\sqrt[k]{\tau_2}$ сопряжены и примитивны, значит согласно предложению 2.3 $[a_1,b_1,c_1]^{\Gamma_0(N)}_{\sim}[a_2,b_2,c_2]$.■

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 3. Для каждого $k\,|\,m$ определим множество

$$M_k=\{q\,|\,U_k:\ q\nmid U_{k'},k'\,|\,k\ \text{и}\ k'\neq k\}. \tag{3.2}$$

$\bigcup_{k|m} M_k$ есть множество всех положительных делителей Q, поскольку $Q=U_m$. Покажем, что семейство $\{M_k\}_{k|m}$ образует разбиение. Допустим противное: пусть $q\in M_{k_1}$, $q\in M_{k_2}$ и $k_1\neq k_2$. Возьмем наименьшее k_3 такое, что $q\in M_{k_3}$ тогда фундаментальное решение уравнения $t^2-q^2Du^2=4$ есть $(T_{k_3},U_{k_3}/q)$. Поскольку $(T_{k_i},U_{k_i}/q)$ при $i=1,2$ есть решение того же уравнения, то $k_3\,|\,k_1$ и $k_3\,|\,k_2$. Это возможно, в силу определения множества M_k, только в случае $k_3=k_1$ и $k_3=k_2$, что противоречит

предположению $k_1 \neq k_2$.

Тогда в силу леммы, предложения 2.4 и только что доказанного свойства множеств M_k следует утверждение теоремы для $L \geq 3$. Так как соответствие $\sigma \longmapsto -\sigma$ задает биективное отображение гиперболических элементов с положительным следом в элементы с отрицательным следом и классы отображаются в классы, то утверждение теоремы верно при $|L| \geq 3$.■

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 2. Заметим, что всякий гиперболический элемент с отрицательным следом представим единственным образом в виде $-\sigma^k$, где $\sigma \in G_N$ и $k \geq 1$. Если $k = 2^n(2j+1)$, с $j \geq 1$, то очевидно $-\sigma^k$ imprimitiven. Докажем, что при $j = 0$ этот элемент примитивен. Допустим, что это не так, тогда $-\sigma^{2^n} = \sigma_1^r$ и $r > 1$. Из этого равенства заключаем, что $tr(\sigma_1) \leq -3$ и r – нечетно. Тогда имеем $\sigma^{2^n} = (-\sigma_1)^r = \sigma_2^{sr}$, где $\sigma_2 \in G_N$ и $s \geq 1$. Это может быть только в случае $\sigma = \sigma_2$ и $2^n = sr$, но ввиду нечетности r последнее равенство неверно, противоречие.

Значит определить число классов примитивных гиперболических элементов с отрицательным следом $-L$ это все равно, что определить число классов гиперболических элементов множества $\mathcal{K} = \{\tau \in G_N^-(L): \quad \tau = \sigma^{2^n}, \sigma \in G_N\}$. Для определения числа классов множества $\mathcal{K}$ достаточно показать, что

$$f^-\Big(\bigcup_{i=0}\ \bigcup_{q \in M_{2^i m_1}}\ \bigcup_{n \mid (N,q)} F_{N,n}(q^2 D)\Big) = \mathcal{K},$$

где f^- - биективное отображение определенное в (3.1) и M_r определено в (3.2).

Пусть $[a,b,c] \in \bigcup_{i=0}\ \bigcup_{q \in M_{2^i m_1}}\ \bigcup_{n \mid (N,q)} F_{N,n}(q^2 D)$, тогда в силу определения M_r и поскольку $(L, Q/q)$ – решение уравнения $t^2 - q^2 D u^2 = 4$ имеем

$$f^-([a,b,c]) = \begin{pmatrix} (L - b\frac{Q}{q})/2 & -c\frac{Q}{q} \\ a\frac{Q}{q} & (L + b\frac{Q}{q})/2 \end{pmatrix} = \left(\begin{pmatrix} (T_{2^i m_1} - b\frac{U_{2^i m_1}}{q})/2 & -c\frac{U_{2^i m_1}}{q} \\ a\frac{U_{2^i m_1}}{q} & (T_{2^i m_1} + b\frac{U_{2^i m_1}}{q})/2 \end{pmatrix} \right)^{\frac{m}{2^i m_1}} \equiv \sigma^{2^{k-i}} \in \mathcal{K}.$$

Пусть $[a,b,c] \in F_{N,n}(q^2 D)$, $q \mid Q$, но $q \notin M_{2^i m_1}$, тогда $q \in M_r$, где $m_1 \mid r$ и аналогично предыдущему получаем, что $f^-([a,b,c]) = \sigma^{\frac{m}{r}}$ и так как показатель $\frac{m}{r}$ не является степенью двойки, то $\sigma^{\frac{m}{r}} \notin \mathcal{K}$.

Отсюда и из предложения 2.4 следует утверждение теоремы.■

В заключение приведем алгоритм нахождения представления гиперболического элемента с положительным следом $\sigma \in \Gamma_0(N)$ в виде степени примитивного гиперболического элемента принадлежащего $\Gamma_0(N)$, то есть алгоритм решения уравнения $x^n = \sigma$.

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. Определяем целое m из условия

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

4. Возьмем все делители m по возрастанию: $1=k_1<k_2<\ldots<k_{d(m)}=m$.
5. Полагаем $d=\dfrac{Q}{(\delta-\alpha,\ \gamma,\ \beta)}$.
6. $i=0$
7. $i:=i+1$
8. Определяем U_{k_i} из условия $\left(\dfrac{T_1+U_1\sqrt{D}}{2}\right)^{k_i}=\dfrac{T_{k_i}+U_{k_i}\sqrt{D}}{2}$.
9. Если $d\nmid U_{k_i}$, то переходим к 7.
10. $x=\begin{pmatrix}\dfrac{T_{k_i}-(\delta-\alpha)U_{k_i}/Q}{2} & -\dfrac{\beta U_{k_i}}{Q}\\ \dfrac{N\gamma U_{k_i}}{Q} & \dfrac{T_{k_i}+(\delta-\alpha)U_{k_i}/Q}{2}\end{pmatrix}$, $n=\dfrac{m}{k_i}$. ■

§4. Доказательство теоремы 1.

Исходным пунктом доказательства будет служить равенство (2.3). В дальнейшем будем считать, что L^2-4 – квадратичный вычет по модулю 4N поскольку в силу предложения 2.5 только при этом условии в правой части равенства (2.3) имеются иенулевые слагаемые.

Прежде всего установим необходимые и достаточные условия существования форм $\mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$ определенных в (2.2).

Пусть N и q имеют разложение определенное в теореме 1. В множестве всех делителей (q,N) определим подмножество S(q,N) следующим образом: $n=\prod_{i=1}^{\omega(N)} p_i^{\alpha_i}\in S(q,N)$ если для всякого $p_i\neq 2$ α_i удовлетворяет хотя бы одному из условий:

$$\begin{aligned}&\alpha_i=0;\\ &1\leqslant\alpha_i\leqslant\min(2\beta_i-s_i,s_i)\ \text{ и }\ \alpha_i\equiv s_i(\mathrm{mod}\,2);\\ &\alpha_i=2\beta_i+1-s_i>0,\ p_i\mid D,\ \beta_i<s_i;\\ &\max(2\beta_i-s_i,0)<\alpha_i\leqslant\beta_i,\ \left(\frac{D}{p_i}\right)=1;\end{aligned}\qquad(4.1)$$

и для $p_i=2$ α_i удовлетворяет хотя бы одному из условий:

$$\begin{aligned}&\alpha_i=0;\\ &1\leqslant\alpha_i\leqslant\min(2\beta_i-2-s_i,s_i),\ \alpha_i\equiv s_i(\mathrm{mod}\,2);\\ &\alpha_i=2\beta_i-s_i>0,\ D\not\equiv 1(\mathrm{mod}\,8),\ \beta_i\leqslant s_i;\\ &\alpha_i=\beta_i=s_i,\ D\equiv 1(\mathrm{mod}\,8);\end{aligned}\qquad(4.2)$$

$\alpha_i = 2\beta_i + 1 - s_i > 0$, $D \equiv 0 \pmod 4$, $\beta_i < s_i$;

$\max(2\beta_i - s_i, 0) < \alpha_i \leq \beta_i$, $D \equiv 1 \pmod 8$.

Справедливо следующее

ПРЕДЛОЖЕНИЕ 4.1. $\mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right) \neq \emptyset$ тогда и только тогда, когда $n \in S(q,N)$ и q^2D - квадратичный вычет по модулю $4N$.

ДОКАЗАТЕЛЬСТВО. Необходимость. Пусть существует примитивная форма $[a,b,c]$ с дискриминантом $\left(\frac{q}{n}\right)^2 D$ и $(a,N) = \frac{N}{n}$. Значит $b^2 \equiv \left(\frac{q}{n}\right)^2 D \pmod{4\frac{N}{n}}$ и поэтому q^2D квадратичный вычет по модулю $4N$. Осталось показать, что $n \in S(q,N)$. Допустим, что это не так. Поскольку $n \mid (q,N)$, то имеем $n = \prod_{i=1}^{\omega(N)} p_i^{\alpha_i}$. Нетрудно заметить, что тогда справедливо утверждение: имеется $p_j \mid n$ такое, что выполняется одно из условий:

1) $1 \leq \alpha_j \leq \min(2\beta_j - s_j, s_j)$ и $\alpha_j \not\equiv s_j \pmod 2$;

2) $p_j = 2$, и $\alpha_j = 2\beta_j - s_j$, и $D \equiv 1 \pmod 8$, $\beta_j < s_j$.

Покажем, что в случае выполнения любого из этих условий форма $[a,b,c]$ непримитивна.

Пусть верно 1), тогда $2\beta_j - 2\alpha_j > s_j - \alpha_j$.

a) $p_j \neq 2$. Поскольку $b^2 = \left(\frac{q}{n}\right)^2 D + 4\frac{N}{n}\ell$, то b^2 делится по крайней мере на $p_j^{s_j - \alpha_j + 1}$. С другой стороны $b^2 - \left(\frac{q}{n}\right)^2 D = 4ac$ и поэтому $p_j^{s_j - \alpha_j + 1} \mid ac$. Так как $(a,N) = \frac{N}{n}$ и $\alpha_j > 0$, то $p_j^{s_j - \alpha_j + 1} \nmid a$, а тогда необходимо $p_j \mid c$ и значит форма $[a,b,c]$ непримитивна.

b) $p_j = 2$. Если $D \equiv 0 \pmod 4$ или ($D \equiv 1 \pmod 4$ и $2\beta_j - 2\alpha_j > s_j - \alpha_j + 1$), то аналогично пункту a) получаем, что $[a,b,c]$ непримитивна.

Осталось рассмотреть случай $2\beta_j - 2\alpha_j = s_j + 1 - \alpha_j$ и $D \equiv 1 \pmod 4$. В этом случае $b^2 / p_j^{s_j - \alpha_j + 1} \equiv 1 \pmod 8$ и $\left(\frac{q}{n}\right)^2 D / p_j^{s_j - \alpha_j + 1} \equiv 1 \pmod 4$. Отсюда следует, что $p_j^{s_j - \alpha_j + 3} \mid \left(b^2 - \left(\frac{q}{n}\right)^2 D\right)$ и значит $p_j \mid c$, то есть $[a,b,c]$ непримитивна.

Пусть верно 2), тогда $2\beta_j - 2\alpha_j = s_j - \alpha_j$ и мы имеем $b^2 / p_j^{s_j - \alpha_j} \equiv 1 \pmod 8$ и $\left(\frac{q}{n}\right)^2 D / p_j^{s_j - \alpha_j} \equiv 1 \pmod 8$. Значит $p_j^{s_j - \alpha_j + 3} \mid \left(b^2 - \left(\frac{q}{n}\right)^2 D\right)$ и значит $p_j \mid c$, то есть $[a,b,c]$ непримитивна.

Достаточность. Пусть q^2D - квадратичный вычет по модулю $4N$ и $n \in S(q,N)$.

Нетрудно проверить, что $n \mid (q,N)$ и $\left(\frac{q}{n}\right)^2 D$ - квадратичный вычет по модулю $4\frac{N}{n}$.

Доказательство проведем индукцией по числу простых входящих в каноническое разложение n.

База индукции: $n = p^{\alpha}$, p - простое и $\alpha > 0$.

$p \neq 2$.

Положим $a=(x_0^2-\left(\frac{q}{p^\alpha}\right)^2 D)/4$, $b=x_0$, $c=1$, где x_0- решение сравнения $x^2\equiv\left(\frac{q}{p^\alpha}\right)^2 D \pmod{4\frac{N}{p^\alpha}}$ такое, что $p^{s-\alpha+1}\nmid(x_0^2-\left(\frac{q}{p^\alpha}\right)^2 D)$. Тогда очевидно $[a,b,c]\in\mathcal{F}_{N,\frac{N}{p^\alpha}}\left(\left(\frac{q}{p^\alpha}\right)^2 D\right)$.

Покажем, что такое решение x_0 существует. Рассмотрим возможные случаи.

i) $1\leq\alpha\leq\min(2\beta-s,s)$ и $\alpha\equiv s\pmod 2$, в этом случае $2\beta-2\alpha\geq s-\alpha$ и сравнение $y^2\equiv\left(\frac{q}{p^{(\alpha+s)/2}}\right)^2 D \pmod{4\frac{N}{p^s}}$ имеет решение y_0 такое, что $p\nmid(y_0^2-\left(\frac{q}{p^{(\alpha+s)/2}}\right)^2 D)$. Тогда $x_0=p^{(s-\alpha)/2}y_0$ есть искомое решение.

ii) $\alpha=2\beta+1-s>0$, $p\mid D$, $\beta<s$, в этом случае $2\beta-2\alpha+1=s-\alpha=2s-2\beta-1$ и любое решение x_0 сравнения $x^2\equiv\left(\frac{q}{p^\alpha}\right)^2 D \pmod{4\frac{N}{p^\alpha}}$ делится на $p^{s-\beta}$, поэтому $p^{s-\alpha+1}\nmid(x_0^2-\left(\frac{q}{p^\alpha}\right)^2 D)$.

iii) $\max(2\beta-s,0)<\alpha\leq\beta$, $\left(\frac{D}{p}\right)=1$, в этом случае $2\beta-2\alpha<s-\alpha$ и сравнение $y^2\equiv\left(\frac{q}{p^\beta}\right)^2 D \pmod{4\frac{N}{p^{2\beta-\alpha}}}$ имеет решение поскольку $\left(\frac{D}{p}\right)=1$. Очевидно существует решение y_0 такое, что $p^{s+\alpha-2\beta+1}\nmid(y_0^2-\left(\frac{q}{p^\beta}\right)^2 D)$. Тогда $x_0=p^{\beta-\alpha}y_0$ есть искомое решение.

$p=2$.

i) $\alpha=\beta=s$, $D\equiv 1\pmod 8$. В силу того, что $\left(\frac{q}{p^\alpha}\right)^2 D\equiv 1\pmod 8$, сравнение $x^2\equiv\left(\frac{q}{p^\alpha}\right)^2 D \pmod{8\frac{N}{p^\alpha}}$ имеет решение. Возьмем такое решение x_0, что $16\nmid(x_0^2-\left(\frac{q}{p^\alpha}\right)^2 D)$. Тогда положим $a=(x_0^2-\left(\frac{q}{p^\alpha}\right)^2 D)/8$, $b=x_0$, $c=2$ и очевидно $[a,b,c]\in\mathcal{F}_{N,\frac{N}{p^\alpha}}\left(\left(\frac{q}{p^\alpha}\right)^2 D\right)$.

ii) $\alpha=2\beta+1-s>0$, $D\equiv 0\pmod 4$, $\beta<s$. Возьмем любое решение y_0 сравнения $y^2\equiv\left(\frac{q}{p^\beta}\right)^2\frac{D}{4} \pmod{2\frac{N}{p^s}}$. Если $8\mid D$, то $2\mid y_0$, если $8\nmid D$, то $\left(\frac{q}{p^\beta}\right)^2\frac{D}{4}\equiv 3\pmod 4$ и поэтому $4\nmid(y_0^2-\left(\frac{q}{p^\beta}\right)^2\frac{D}{4})$. Тогда $x_0=p^{(s-\alpha+1)/2}y_0$ есть искомое решение.

В остальных случаях существование x_0 доказывается аналогично 1.

Шаг индукции. Сформулируем индуктивное предположение следующим образом: если q^2D - квадратичный вычет по модулю $4N$, $n\in S(q,N)$ и n разлагается по степеням k простых, то существует такая форма $[a,b,c]\in\mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$, что $c=2$, если существует $1\leq j\leq\omega(N)$ для которого $p_j=2$, $\alpha_j=\beta_j=s_j$ и $D\equiv 1\pmod 8$, и $c=1$ в противном случае.

Теперь докажем, что найдется форма с такими же свойствами, для n имеющего в своем разложении $k+1$ простое.

Положим $n = n_1 p^{\alpha}$, $p \neq 2, \alpha > 0$, $p \nmid n_1$. Очевидно $n_1 \in S(q,N)$ и поскольку n_1 состоит из произведения k степеней простых, то согласно индуктивному предположению существует форма $[a,b,c] \in \mathcal{F}_{N,\frac{N}{n_1}}\left(\left(\frac{q}{n_1}\right)^2 D\right)$. Покажем, что существует форма $[a_1,b_1,c_1] \in \mathcal{F}_{N,\frac{N}{n_1}}\left(\left(\frac{q}{n_1}\right)^2 D\right)$ такая, что $p^{s+\alpha} \mid a_1$ и $p^{s+\alpha+1} \nmid a_1$. Будем искать $[a_1,b_1,c_1]$ в виде:

$$b_1 = b + 4\frac{N}{p^s}x, \quad a_1 = (b_1^2 - \left(\frac{q}{n_1}\right)^2 D)/4c, \quad c_1 = c, \tag{4.3}$$

тогда

$$a_1 = \frac{N}{n_1 p^s}\left(\frac{a p^s}{N/n_1} + \frac{2}{c} b n_1 x + \frac{4N n_1}{c p^s} x^2\right). \tag{4.4}$$

Если $c = 2$, то по индуктивному предположению $2^{\alpha} \mid n_1$, $\alpha = \beta = s$. Так как $(a,N) = \frac{N}{n}$, то a нечетное и тогда в силу (4.4) a_1 нечетно. Значит форма $[a_1,b_1,c_1]$ примитивна.

Так как $(a,N) = \frac{N}{n}$, то $\left(\frac{a p^s}{N/n_1}, n_1\right) = 1$, а тогда в силу (4.4) $\left(a_1, \frac{N}{p^s}\right) = \frac{N}{n_1 p^s}$.

Теперь выберем x_0 таким, чтобы $p^{s+\alpha} \mid a_1$ и $p^{s+\alpha+1} \nmid a_1$, тогда $[a_1,b_1,c_1] \in \mathcal{F}_{N,\frac{N}{n_1}}\left(\left(\frac{q}{n_1}\right)^2 D\right)$.

Рассмотрим возможные случаи:

1. $1 \leq \alpha \leq \min(2\beta - s, s)$ и $\alpha \equiv s \pmod 2$.

Если $p \nmid D$ и $2\beta - s = \alpha$, то p входит в разложение $\left(\frac{q}{n_1}\right)^2 D$ с показателем $s+\alpha$. Тогда определяем x_0 из уравнения $b + 4\frac{N}{p^s}x = p^{(s+\alpha)/2+1} y$.

В противном случае p входит в разложение $\left(\frac{q}{n_1}\right)^2 D$ с показателем большим $s+\alpha$ и тогда определяем x_0 из уравнения $b + 4\frac{N}{p^s}x = p^{(s+\alpha)/2} + p^{(s+\alpha)/2+1} y$.

При таком выборе x_0 (в силу (4.3)) p входит в a_1 с показателем $s+\alpha$.

2. $\alpha = 2\beta + 1 - s > 0$, $p \mid D$, $\beta < s$

Тогда p входит в разложение $\left(\frac{q}{n_1}\right)^2 D$ с показателем $s+\alpha$ и тогда определяем x_0 из уравнения $b + 4\frac{N}{p^s}x = p^{(s+\alpha+1)/2} y$. При таком выборе x_0 (в силу (4.3)) p входит в a_1 с показателем $s+\alpha$.

3. $\max(2\beta - s, 0) < \alpha \leq \beta$, $\left(\frac{D}{p}\right) = 1$

Тогда $2\beta < s+\alpha$ и так как $\left(\frac{D}{p}\right) = 1$, то сравнение $w^2 \equiv \left(\frac{q}{n_1 p^{\beta}}\right)^2 D \pmod{p^{s+\alpha-2\beta}}$ разрешимо. Возьмем решение w_0 такое, что $w_0^2 - \left(\frac{q}{n_1 p^{\beta}}\right)^2 D$ не делится на $p^{s+\alpha-2\beta+1}$.

Определяем x_0 из уравнения $b + 4\frac{N}{p^s}x = p^{\beta}w_0 + p^{s+\alpha-\beta+1}y$. При таком выборе x_0 (в силу (4.3)) p входит в a_1 с показателем $s+\alpha$.

Теперь положим $a_2 = a_1/p^{2\alpha}$, $b_2 = b_1/p^{\alpha}$, $c_2 = c_1$ и форма $[a_2,b_2,c_2] \in \mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$, что и требовалось показать.■

Из формулы (2.3) и предложения 4.1 иепосредственио получаем

СЛЕДСТВИЕ.

$$\nu(L,N) = \sum_{\substack{q \mid Q \\ q \nmid U_k,\ k \mid m,\ k \neq m \\ x^2 \equiv q^2 D \pmod{4N}}} \sum_{n \in S(q,N)} h_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right) \tag{4.5}$$

и все слагаемые в правой части отличны от нуля.

Прежде чем перейти к вычислению $h_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$, докажем два вспомогательных утверждения.

ПРЕДЛОЖЕНИЕ 4.2. Пусть $\mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right) \neq \emptyset$ и p - простое. Тогда в каждом классе форм множества $\mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$ относительно группы $\Gamma_0(N)$ существует форма $[a_0,b_0,c_0]$ такая, что $p \nmid (a_0+b_0+c_0)$ за исключением случая: $p = 2$, $\alpha = \beta = s$ (α, β, s - показатели, с которыми p входит в n, q, N соответственно) и $D \equiv 1 \pmod 8$. В этом случае для любой формы $[a,b,c] \in \mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$ $p \mid (a+b+c)$.

ДОКАЗАТЕЛЬСТВО. Возьмем $\sigma = \begin{pmatrix} N+1 & 1 \\ N & 1 \end{pmatrix}$ и положим $[a_0,b_0,c_0] = \sigma^t [a,b,c]\,\sigma$, где $[a,b,c] \in \mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$. Отметим, что $c_0 = a+b+c$. Рассмотрим возможные случаи:

i) $s - \alpha > 0$

Пусть $p \mid (a+b+c)$. Тогда $p \mid c_0$ и поскольку $s - \alpha > 0$, то $p \mid a_0$ и значит $p \nmid (a_0+b_0+c_0)$.

ii) $2\beta - 2\alpha > s - \alpha = 0$

Пусть $p \mid (a+b+c)$. Тогда $p \mid c_0$ и поскольку $2\beta - 2\alpha > 0$, то $p \mid b_0$ и значит $p \nmid (a_0+b_0+c_0)$.

iii) $2\beta - 2\alpha = s - \alpha = 0$

а) $p \neq 2$ и $\left(\frac{D}{p}\right) = -1$ или $p = 2$ и $D \equiv 5 \pmod 8$

Пусть $p \mid (a+b+c)$. Тогда $p \mid c_0$ и поэтому $b_0^2 \equiv \left(\frac{q}{n}\right)^2 D \pmod p$ для $p \neq 2$ и $b_0^2 \equiv \left(\frac{q}{n}\right)^2 D \pmod 8$ для $p = 2$. С другой стороны, поскольку $\beta = \alpha$ и из условия а) следует, что соответствующие сравнения $x^2 \equiv \left(\frac{q}{n}\right)^2 D \pmod p$ и $x^2 \equiv \left(\frac{q}{n}\right)^2 D \pmod 8$ не

имеют решения - противоречие.

b) $p \mid D$

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

c) $\left(\frac{D}{p}\right) = 1$

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 возьмем $\sigma_p = \begin{pmatrix} pN+1 & 1 \\ pN & 1 \end{pmatrix}$ и рассмотрим форму $[a_1,b_1,c_1] = \sigma_p^t [a_0,b_0,c_0] \sigma_p$. Легко проверить, что $a_1+b_1+c_1 \equiv 3a_0+b_0 \pmod p$. Так как $p \mid c_0$, то $p \mid (a_0+b_0)$ и так как $p \nmid b_0$, то $p \nmid a_0$ и значит $p \nmid (3a_0+b_0)$. Следовательно $p \nmid (a_1+b_1+c_1)$, что и требовалось доказать.

d) $p = 2$, $D \equiv 1 \pmod 8$

В этом случае $8 \mid \left(b^2 - \left(\frac{q}{n}\right)^2 D\right)$ и значит $2 \mid c$, а отсюда $2 \mid (a+b+c)$.■

Введем обозначение

$$N_1 = \frac{N}{p^s}, \quad n_1 = \frac{n}{p^\alpha}, \quad q_1 = \frac{q}{p^\beta} \tag{4.6}$$

где $(N_1,p) = 1$, $(n_1,p) = 1$, $(q_1,p) = 1$, $s \geq 1$, $\alpha \geq 0$, $\beta \geq 0$.

Справедливо следующее

ПРЕДЛОЖЕНИЕ 4.3. Пусть $\mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right) \neq \emptyset$, тогда в каждом сопряженном классе форм $\mathcal{F}_{N_1,\frac{N_1}{n_1}}\left(\left(\frac{q}{n}\right)^2 D\right)$ относительно $\Gamma_0(N_1)$ существует форма $[a_0,b_0,c_0] \in \mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$.

ДОКАЗАТЕЛЬСТВО. Очевидно $\mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right) \subset \mathcal{F}_{N_1,\frac{N_1}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$ и значит $\mathcal{F}_{N_1,\frac{N_1}{n_1}}\left(\left(\frac{q}{n}\right)^2 D\right) \neq \emptyset$. Рассмотрим семейство матриц $\sigma_j = \begin{pmatrix} jN_1+1 & 1 \\ jN_1 & 1 \end{pmatrix}$, где j - целое. Покажем, что для любой формы $[a,b,c] \in \mathcal{F}_{N_1,\frac{N}{n_1}}\left(\left(\frac{q}{n}\right)^2 D\right)$ существует j такое, что $[a_0,b_0,c_0] = \sigma_j^t [a,b,c] \sigma_j \in \mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$. Так как $a_0 = a + N_1 j(2a+b+N_1 j(a+b+c))$, то последнее выполняется тогда и только тогда, когда при $\gamma = s-\alpha$ сравнение

$$N_1^2 j^2 (a+b+c) + N_1 j (2a+b) + a \equiv 0 \pmod{p^\gamma} \tag{4.7}$$

разрешимо и если $\alpha > 0$, то существует решение j_0 сравнения (4.7) при $\gamma = s-\alpha$, которое не является решением сравнения (4.7) при $\gamma = s-\alpha+1$.

Рассмотрим два случая:

1) $p > 2$

В силу предложения 4.2 можно считать, что $p \nmid (a+b+c)$. Из этого следует, что умножая (4.7) на $4(a+b+c)$ получаем следующую эквивалентную систему

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

Поскольку $\mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right) \neq \emptyset$, то сравнение при $\gamma = s - \alpha$ разрешимо. Более того, в силу предложения 4.1 $n \in S(q,N)$ и поэтому, как показано в доказательстве предложеиия 4.1 мы можем выбрать при $\alpha > 0$ такое решение x_0, что $p^{s-\alpha+1} \nmid (x_0^2 - \left(\frac{q}{n}\right)^2 D)$.

Далее, решаем уравнение

$$x_0 + kp^{s-\alpha+1} = 2N_1(a + b + c)j + 2a + b$$

в целых числах относительно k, j. Решение существует, так как $p \nmid 2N_1(a + b + c)$. Тогда при таком выборе j верно $(a_0, p^s) = p^{s-\alpha}$ и значит $(a_0, N) = \frac{N}{n}$, отсюда $[a_0,b_0,c_0] \in \mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$.

2) $p = 2$

а) $\alpha = \beta = s$ и $D \equiv 1 \pmod 8$

Пусть $[a,b,c] \in \mathcal{F}_{N_1,\frac{N_1}{n_1}}\left(\left(\frac{q}{n}\right)^2 D\right)$, тогда $2 \nmid b$. Если $2 \nmid a$, то $(a,N) = \frac{N}{n}$ и $[a,b,c] \in \mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$. Поэтому пусть $2 \mid a$. Согласно предложению 4.2 $2 \mid (a+b+c)$, поэтому $2 \nmid c$. Возьмем $[a_0,b_0,c_0] = \sigma_1^t[a,b,c]\sigma_1$ и тогда $2 \nmid a_0$.

b) В остальных случаях согласно предложению 4.2 в каждом сопряженном классе множества $\mathcal{F}_{N_1,\frac{N_1}{n_1}}\left(\left(\frac{q}{n}\right)^2 D\right)$ относительио $\Gamma_0(N_1)$ существует форма $[a,b,c]$ такая, что $2 \nmid (a + b + c)$. Домножая (4.7) на $4(a + b + c)$ получаем систему

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

Из соображений аналогичных приведенных в 1) следует, что существует такое решение x_0, что $2^{s-\alpha+3} \nmid (x_0^2 - \left(\frac{q}{n}\right)^2 D)$ при $\alpha > 0$. Уравнение

$$x_0 + k2^{s-\alpha+3} = 2N_1(a + b + c)j + 2a + b$$

относительно k, j имеет целочисленное решение, поскольку $b - x_0$ делится иа 2 и $2 \nmid N_1(a + b + c)$. При таком выборе j $(a_0, N) = \frac{N}{n}$, отсюда $[a_0,b_0,c_0] \in \mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$, что и требовалось доказать.■

Для всякого $\mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right) \neq \emptyset$ определим рекуррентную последовательность вложенных множеств квадратичных форм следующим образом:

$$\mathcal{F}_{N_1,\frac{N_1}{n_1}}\left(\left(\frac{q}{n}\right)^2 D\right) \subset \ldots \subset \mathcal{F}_{N_i,\frac{N_i}{n_i}}\left(\left(\frac{q}{n}\right)^2 D\right) \subset \mathcal{F}_{N_{i+1},\frac{N_{i+1}}{n_{i+1}}}\left(\left(\frac{q}{n}\right)^2 D\right) \subset \ldots \subset \mathcal{F}_{1,1}\left(\left(\frac{q}{n}\right)^2 D\right),$$

где

$$N_1 = N,\ N_{i+1} = \frac{N_i}{p_i^{s_i}} \text{ и } n_1 = n,\ n_{i+1} = \frac{n_i}{p_i^{\alpha_i}}. \tag{4.8}$$

Заметим, что $h_{1,1}\left(\left(\frac{q}{n}\right)^2 D\right) = h\left(\left(\frac{q}{n}\right)^2 D\right)$, где $h(*)$ - классическая функция числа классов примитивных квадратичных форм данного дискриминанта.

Теперь, если мы выразим $h_{N_i,\frac{N_i}{n_i}}\left(\left(\frac{q}{n}\right)^2 D\right)$ через $h_{N_{i+1},\frac{N_{i+1}}{n_{i+1}}}\left(\left(\frac{q}{n}\right)^2 D\right)$ для любого $1 \le i \le \omega(N)$, то тогда получим формулу, выражающую $h_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$ через $h\left(\left(\frac{q}{n}\right)^2 D\right)$. Реализацией этого подхода мы теперь и займемся.

ПРЕДЛОЖЕНИЕ 4.4. Пусть $\mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right) \neq \emptyset$, $\mathcal{G}$ - класс форм $\mathcal{F}_{N_1,\frac{N_1}{n_1}}\left(\left(\frac{q}{n}\right)^2 D\right)$ относительно $\Gamma_0(N_1)$, $h(\mathcal{G})$ - число классов форм $\mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$ относительно $\Gamma_0(N)$ содержащихся в $\mathcal{G}$ и N_1, n_1 определены в 4.5. Тогда

$$h(\mathcal{G}) = \frac{\#\left\{ \sigma \in \mathcal{R}_{N,N_1} : \sigma^t [a,b,c]\sigma \in \mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)\right\}}{\left[\operatorname{Aut}_{\frac{N}{p^\alpha}}([a,b,c]) : \operatorname{Aut}_N([a,b,c]) \right]}, \tag{4.9}$$

где $[a,b,c] \in \mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right) \cap \mathcal{G}$, $\mathcal{R}_{N,N_1}$-система представителей левых классов смежности $\Gamma_0(N)\backslash\Gamma_0(N_1)$, $\operatorname{Aut}_N([a,b,c])$ определена в § 2.

ДОКАЗАТЕЛЬСТВО. Согласно предложению 4.3 существует форма $[a,b,c] \in \mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right) \cap \mathcal{G}$. Имеем представление $\mathcal{G} = \bigcup_{\sigma \in \mathcal{R}_{N,N_1}} \mathcal{H}_\sigma[a,b,c]$, где $\mathcal{H}_\sigma[a,b,c] = \bigcup_{\tau \in \Gamma_0(N)} \tau^t \sigma^t [a,b,c]\sigma\tau$. Из этого представления следует

$$h(\mathcal{G}) = \#\{\mathcal{H}_\sigma[a,b,c] \subset \mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right) : \sigma \in \mathcal{R}_{N,N_1}\}.$$

Очевидно, что $\mathcal{H}_{\sigma_1}[a,b,c] = \mathcal{H}_{\sigma_2}[a,b,c]$ тогда и только тогда, когда $\sigma_1^t[a,b,c]\sigma_1 \overset{\Gamma_0(N)}{\sim} \sigma_2^t[a,b,c]\sigma_2$. Поэтому вопрос о числе классов сводится к вопросу о числе форм $\sigma^t[a,b,c]\sigma$, где $\sigma \in \mathcal{R}_{N,N_1}$, эквивалентных данной форме $\sigma_0^t[a,b,c]\sigma_0 \in \mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$, $\sigma_0 \in \mathcal{R}_{N,N_1}$.

Рассмотрим сначала случай $\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Поскольку $[a,b,c] \in \mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$, то

$\sigma^t[a,b,c]\,\sigma \overset{\Gamma_0(N)}{\sim} [a,b,c]$ тогда и только тогда, когда существует $\tau \in \mathrm{Aut}_{\underline{N}}{}_{p^\alpha}[a,b,c]$ такое, что $\tau \in \sigma\Gamma_0(N)$. Пусть τ_0 - образующая $\mathrm{Aut}_{\underline{N}}{}_{p^\alpha}[a,b,c]$. Тогда при

$$k = [\mathrm{Aut}_{\underline{N}}{}_{p^\alpha}([a,b,c]) : \mathrm{Aut}_N([a,b,c])]$$

(4.8)

τ_0^k является образующий $\mathrm{Aut}_N([a,b,c])$. Элементы $\tau_0,\ldots,\tau_0^k$ лежат в разных классах смежности $\Gamma_0(N)\backslash\Gamma_0(N_1)$ с некоторыми представителями $\sigma_1,\ldots\sigma_k$ из системы $\mathcal{R}_{N,N_1}$ и всякий $\tau \in \mathrm{Aut}_{\underline{N}}{}_{p^\alpha}([a,b,c])$ сравним по модулю $\Gamma_0(N)$ с некоторым τ_0^i, $1 \leqslant i \leqslant k$. Тогда $\sigma_i^t[a,b,c]\,\sigma_i \overset{\Gamma_0(N)}{\sim} [a,b,c]$ при $1 \leqslant i \leqslant k$ и других элементов из $\mathcal{R}_{N,N_1}$ с этим свойством нет. Значит $\#\{\sigma \in \mathcal{R}_{N,N_1} : \sigma^t[a,b,c]\,\sigma \overset{\Gamma_0(N)}{\sim} [a,b,c]\} = k$.

Теперь покажем, что общий случай сводится к только что рассмотренному. Условие

$$\sigma^t[a,b,c]\,\sigma \overset{\Gamma_0(N)}{\sim} \sigma_0^t[a,b,c]\,\sigma_0$$

эквивалеитио условию

$$(\sigma_0^{-1}\sigma)^t[a_1,b_1,c_1](\sigma_0^{-1}\sigma) \overset{\Gamma_0(N)}{\sim} [a_1,b_1,c_1],$$

где $[a_1,b_1,c_1] = \sigma_0^t[a,b,c]\,\sigma_0 \in \mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$. Элементы $\sigma_0^{-1}\sigma$ образуют систему представителей, когда σ пробегает $\mathcal{R}_{N,N_1}$. Образующей $\mathrm{Aut}_{\underline{N}}{}_{p^\alpha}([a,b,c])$ будет $\sigma_0^{-1}\tau_0\,\sigma_0$ и образующей $\mathrm{Aut}_N([a,b,c])$ будет $\sigma_0^{-1}\tau_0^k\,\sigma_0$. Значит

$$\#\{\sigma \in \mathcal{R}_{N,N_1} : \sigma^t[a,b,c]\,\sigma \overset{\Gamma_0(N)}{\sim} \sigma_0^t[a,b,c]\,\sigma_0\} = k,$$

что и завершает доказательство.■

В следующем предложении мы вычисляем знаменатель дроби (4.9).

ПРЕДЛОЖЕНИЕ 4.5. Пусть $[a,b,c] \in \mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$, тогда

$$[\mathrm{Aut}_{\underline{N}}{}_{p^\alpha}([a,b,c]) : \mathrm{Aut}_N([a,b,c])] = \frac{\ln((t_0 + q\sqrt{D}\,u_0)/2)}{\ln((t_1 + \frac{q}{p^\alpha}\sqrt{D}\,u_1)/2)},$$

где (t_0,u_0) и (t_1,u_1) - фундаментальные решения уравиеиий $t^2 - q^2Du^2 = 4$ и $t^2 - \left(\frac{q}{p^\alpha}\right)^2 Du^2 = 4$ соответственно.

ДОКАЗАТЕЛЬСТВО. Поскольку $[a,b,c] \in \mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$, то $[an,bn,cn] \in F_N(q^2D)$ и очевидно $\mathrm{Aut}_N([a,b,c]) = \mathrm{Aut}_N([an,bn,cn])$. Согласно предложению 2.2 $\mathrm{Aut}_N([an,bn,cn])$ имеет образующую

$$\tau = \begin{pmatrix} (t_0 - bnu_0)/2 & -cu_0 \\ au_0 & (t_0 + bnu_0)/2 \end{pmatrix}.$$

Аналогичным образом $\mathrm{Aut}_{\underline{N}}{}_{p^\alpha}([a,b,c])$ имеет образующую

$$\vartheta = \begin{pmatrix} (t_1 - b\frac{n}{p}\alpha u_1)/2 & -c\frac{n}{p}\alpha u_1 \\ a\frac{n}{p}\alpha u_1 & (t_1 + b\frac{n}{p}\alpha u_1)/2 \end{pmatrix}.$$

Поскольку $\tau = \vartheta^k$ для иекоторого $k \geq 1$, то $\frac{t_0 + q\sqrt{Du_0}}{2} = \left(\frac{t_1 + \frac{n}{p}\alpha\sqrt{Du_1}}{2}\right)^k$, что и требовалось доказать.■

Для того, чтобы вычислить числитель дроби в правой части (4.9) предварительио выпишем систему представителей левых классов смежиости $\Gamma_0(N)\backslash\Gamma_0(N_1)$.

ПРЕДЛОЖЕНИЕ 4.6. Пусть $N = N_1 p^S$ и $(N_1, p) = 1$, тогда множество $\mathcal{R}_{N,N_1}$ состоящее из матриц вида $\begin{pmatrix} 1+N_1 j & 1 \\ N_1 j & 1 \end{pmatrix}$, где j пробегает полиую систему вычетов по модулю p^S и матриц вида $\begin{pmatrix} 1+N_1 j & j \\ N_1 & 1 \end{pmatrix}$, где $j = 1 + j_0 + j_1 p$, j_1 пробегает полиую систему вычетов по модулю p^{S-1} и j_0 - фиксированное решение сравнения $j_0 N_1 \equiv -1 (\mathrm{mod}\, p)$, образует систему представителей левых классов смежности $\Gamma_0(N)\backslash\Gamma_0(N_1)$.

ДОКАЗАТЕЛЬСТВО. Покажем, что $\Gamma_0(N_1) = \bigcup_{\sigma \in \mathcal{R}_{N,N_1}} \sigma\Gamma_0(N)$. Пусть $\begin{pmatrix} a & b \\ N_1 c & d \end{pmatrix} \in \Gamma_0(N_1)$. Требуется показать, что существуют $\sigma \in \mathcal{R}_{N,N_1}$ и $\begin{pmatrix} \alpha & \beta \\ N\gamma & \delta \end{pmatrix} \in \Gamma_0(N)$, что

$$\begin{pmatrix} a & b \\ N_1 c & d \end{pmatrix} = \sigma \begin{pmatrix} \alpha & \beta \\ N\gamma & \delta \end{pmatrix}.$$

1. $N_1 c - a \not\equiv 0 (\mathrm{mod}\, p)$.

Будем искать σ вида $\begin{pmatrix} 1+N_1 j & 1 \\ N_1 j & 1 \end{pmatrix}$, j - **любое целое. Тогда**

$$\begin{pmatrix} a & b \\ N_1 c & d \end{pmatrix} = \begin{pmatrix} \alpha + N_1 j\alpha + N\gamma & \beta + N_1 j\beta + \delta \\ N_1 j\alpha + N\gamma & N_1 j\beta + \delta \end{pmatrix}. \tag{4.10}$$

Значит $\beta = b - d$, $\alpha = a - N_1 c$. Приравнивая **левые нижние элементы** матриц в (4.10) получаем $j(a - N_1 c) + p^S \gamma = c$. Так как $p \nmid (a - N_1 c)$, **то существует** решение j_0, γ_0 этого уравнения в целых числах. **Остается положить** $\delta = d - N_1 j_0 \beta$ и равенство (4.10) выполняется.

2. $N_1 c - a \equiv 0 (\mathrm{mod}\, p)$.

Будем искать σ вида $\begin{pmatrix} 1+N_1 j & j \\ N_1 & 1 \end{pmatrix}$, где $j = 1+j_0+j_1 p$ и $j_0 N_1 \equiv -1 (\mathrm{mod}\, p)$, тогда

$$\begin{pmatrix} a & b \\ N_1 c & d \end{pmatrix} = \begin{pmatrix} \alpha+N_1 j\alpha+N j\gamma & \beta+N_1 j\beta+\delta j \\ N_1\alpha + N\gamma & N_1\beta + \delta \end{pmatrix}. \tag{4.11}$$

Приравнивая левые столбцы в матрицах в (4.11) получаем $\alpha = c - p^s\gamma$ и $a = N_1 jc + c - p^s\gamma$. Отсюда следует, что

$$(a - N_1 c)/p + k_0 = j_1 N_1 c - p^{s-1}\gamma, \tag{4.12}$$

где $k_0 = -c(1 + j_0 N_1)/p$. $(N_1 c, p) = 1$ так как в противном случае $p \mid c$ и поскольку $p \mid (N_1 c - a)$, то $p \mid a$ что невозможно. Следовательно уравнение (4.12) имеет решение в целых числах j_1, γ. Положим $\beta = b - jd$, $\delta = d - N_1\beta$ и равенство (4.11) выполняется.

Условие $\sigma_1^{-1}\sigma_2 \notin \Gamma_0(N)$ для любых $\sigma_1, \sigma_2 \in \mathcal{R}_{N,N_1}$ и $\sigma_1 \neq \sigma_2$ проверяется непосредственно.■

ПРЕДЛОЖЕНИЕ 4.7. Пусть $[a,b,c] \in \mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$, тогда

$$\#\left\{ \sigma \in \mathcal{R}_{N,N_1} : \sigma^t [a,b,c]\, \sigma \in \mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right) \right\} =$$

$$\varepsilon(p,q,n)\left(p^{\left[\frac{\min(2\beta, s+\alpha)}{2}\right]} + \eta(p,q,n)\, p^{\left[\frac{\min(2\beta, s+\alpha}{2}\right]-1} \right),$$

где $N_1, \alpha, \beta, s,$ определены в 4.5,

$$\varepsilon(p,q,n) = \begin{cases} 1, & \text{если } 2\beta \geq s+\alpha \\ 2, & \text{если } 2\beta < s+\alpha \end{cases}, \tag{4.13}$$

$$\eta(p,q,n) =$$

$$\begin{cases} -1, \text{ если } s = \beta = \alpha \text{ и } \left(\left(\frac{D}{p}\right) = -1 \text{ и } p > 2 \text{ или } D \equiv 5 (\mathrm{mod}\ 8) \text{ и } p = 2\right); \\ 1, \text{ если } \alpha > 0 \text{ и выполняется хотя бы одно из условий:} \\ \quad 2\beta - 2\alpha > s - \alpha > 0; \\ \quad 2\beta - 2\alpha = s - \alpha > 0 \text{ и } p \mid D; \\ \quad \beta = \alpha = s \text{ и } \left(\left(\frac{D}{p}\right) = 1 \text{ и } p > 2 \text{ или } D \equiv 1 (\mathrm{mod}\ 8) \text{ и } p = 2\right); \\ \quad 2\beta < s + \alpha \text{ и } \left(\left(\frac{D}{p}\right) = 1 \text{ и } p > 2 \text{ или } D \equiv 1 (\mathrm{mod}\ 8) \text{ и } p = 2\right); \\ 2, \text{ если } \alpha > 0 \text{ и } 2\beta - 2\alpha > s - \alpha > 0 \text{ и } \left(\frac{D}{p}\right) = 1; \\ 0, \text{ в остальных случаях.} \end{cases} \tag{4.14}$$

ДОКАЗАТЕЛЬСТВО. Рассмотрим систему представителей $\mathcal{R}_{N,N_1}$ определенную в предложении 4.6. Элементы $\begin{pmatrix} 1+N_1 j & 1 \\ N_1 j & 1 \end{pmatrix}$, где $j \pmod{p^s}$, будем называть представителями первого типа, а остальные второго типа.

Положим $[a_1,b_1,c_1] = \sigma^t[a,b,c]\sigma$. Для представителей второго типа, принимая во внимание, что $j = 1+j_0+j_1p$ и $j_0N_1 \equiv -1 \pmod p$, легко получить

$$a_1 \equiv N_1^2(a+b+c) \pmod p. \tag{4.15}$$

Для представителей первого типа рассмотрим вначале случай $p \neq 2$.

Согласно предложению 4.2 в каждом классе форм из $\mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$ существует форма $[a,b,c]$ такая, что $p \nmid (a+b+c)$. Возьмем такую форму. Пусть σ-представитель первого типа. Тогда, как показано в предложении 4.3, условие $p^\gamma \mid a_1$ эквивалентно существованию решения x, j системы

$$\begin{cases} x^2 \equiv \left(\frac{q}{n}\right)^2 D \pmod{p^\gamma} \\ x = 2N_1(a+b+c)j + 2a + b \end{cases} \tag{4.16}$$

1.$s-\alpha > 0$.

Так как $p \nmid (a+b+c)$, то согласно (4.15) $p \nmid a_1$ при любом σ второго типа.

а) $2\beta-2\alpha > s-\alpha$

Решаем систему (4.16) при $\gamma = s-\alpha$. Так как $2\beta-2\alpha > s-\alpha$, то $\left(\frac{q}{n}\right)^2 D \equiv 0 \pmod{p^{s-\alpha}}$ и тогда $x \equiv 0 \pmod{p^{[(s-\alpha+1)/2]}}$, $2a+b \equiv 0 \pmod{p^{[(s-\alpha+1)/2]}}$ значит $j \equiv 0 \pmod{p^{[(s-\alpha+1)/2]}}$.

Если $\alpha > 0$, то решаем систему (4.16) при $\gamma = s-\alpha+1$ $x \equiv 0 \pmod{p^{[(s-\alpha+2)/2]}}$, значит $j \equiv j_0 \pmod{p^{[(s-\alpha+2)/2]}}$. Тогда имеем $p^{[(s+\alpha)/2]-1}$ различных j по модулю p^s.

Таким образом имеем $p^{[s/2]}$ при $\alpha = 0$ и $p^{[(s+\alpha)/2]} - p^{[(s+\alpha)/2]-1}$ при $\alpha > 0$ представителей $\sigma \in \mathcal{R}_{N,N_1}$ таких, что $\sigma^t[a,b,c]\sigma \in \mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$.

б) $2\beta-2\alpha = s-\alpha$

Число решений системы (4.16) при $\gamma = s-\alpha$ равно $p^{[(s+\alpha)/2]}$. Пусть $\alpha > 0$. Решаем систему (4.16) при $\gamma = s-\alpha+1$. Если $\left(\frac{D}{p}\right) = -1$, то сравнение $x^2 \equiv \left(\frac{q}{n}\right)^2 D \pmod{p^{s-\alpha+1}}$ решений не имеет. Если $p \mid D$, то имеется $p^{[(s+\alpha)/2]-1}$ решение. Если $\left(\frac{D}{p}\right) = 1$, то сравнение $x^2 \equiv \left(\frac{q}{n}\right)^2 D \pmod{p^{s-\alpha+1}}$ имеет два решения $\pm x_0$ по модулю $p^{(s-\alpha+2)/2}$, а тогда получаем $2p^{(s+\alpha)/2-1}$ различных j по модулю p^s.

Таким образом, если $\alpha = 0$,то имеем $p^{[s/2]}$, если $\alpha > 0$, то если $\left(\frac{D}{p}\right) = -1$, то $p^{[(s+\alpha)/2]}$, если $p \mid D$, то $p^{[(s+\alpha)/2]} - p^{[(s+\alpha)/2]-1}$ и если $\left(\frac{D}{p}\right) = 1$, то $p^{[(s+\alpha)/2]} - 2p^{[(s+\alpha)/2]-1}$ представителей $\sigma \in \mathcal{R}_{N,N_1}$ таких, что $\sigma^t[a,b,c]\sigma \in \mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$.

в) $2\beta - 2\alpha + 1 = s - \alpha$ и $p \mid D$

Решаем систему (4.16) при $\gamma = s - \alpha$. Имеем $x \equiv 0 (\mathrm{mod}\, p^{(s-\alpha+1)/2})$. Тогда получаем $p^{[(s+\alpha)/2]}$ различных j по модулю p^s. Система (4.16) при $\gamma = s - \alpha + 1$ не имеет решения, значит получаем $p^{[(s+\alpha)/2]}$ представителей $\sigma \in \mathcal{R}_{N,N_1}$ таких, что $\sigma^t[a,b,c]\sigma \in \mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$.

г) $2\beta - 2\alpha < s - \alpha$ и $\left(\frac{D}{p}\right) = 1$

Имеет $p^{\beta-\alpha} \mid b$ и $p^{\beta-\alpha+1} \nmid b$. Решаем систему (4.16) при $\gamma = s - \alpha$. Сравнение $x^2 \equiv \left(\frac{q}{n}\right)^2 D (\mathrm{mod}\, p^{s-\alpha+1})$ имеет два решения $x_1 \equiv b (\mathrm{mod}\, p^{s-\beta})$ и $x_2 \equiv -b (\mathrm{mod}\, p^{s-\beta})$. Тогда j определяются из решений сравнений $N_1(a+b+c)j \equiv 0 (\mathrm{mod}\, p^{s-\beta})$ и $N_1(a+b+c)j \equiv -b (\mathrm{mod}\, p^{s-\beta})$ и решения этих сравнений различны по модулю p^s так как $b \not\equiv 0 (\mathrm{mod}\, p^{s-\beta})$. Значит имеем $2p^\beta$ различных j по модулю p^s.

Решаем систему (4.16) при $\gamma = s - \alpha + 1$. Сравнение $x^2 \equiv \left(\frac{q}{n}\right)^2 D (\mathrm{mod}\, p^{s-\alpha+1})$ имеет два решения $\pm(b + x_0)$ по модулю $p^{s-\beta+1}$, где x_0 есть решение сравнения $bx \equiv -2ac (\mathrm{mod}\, p^{s-\alpha+1})$. Тогда j определяется из решений сравнений $2N_1(a+b+c)j \equiv x_0 (\mathrm{mod}\, p^{s-\beta+1})$ и $2N_1(a+b+c)j \equiv -2b - x_0 (\mathrm{mod}\, p^{s-\beta+1})$, при этом $b + x_0 \not\equiv 0 (\mathrm{mod}\, p^{s-\beta+1})$ поскольку $p^{\beta-\alpha+1} \nmid b$, $p^{s-\beta} \mid x_0$ и $s - \beta > \beta - \alpha$. Значит решения этих сравнений различны по модулю p^s и имеем $2p^{\beta-1}$ различных j по модулю p^s.

Таким образом имеем при $\alpha = 0$ $2p^\beta$ и при $\alpha > 0$ $2(p^\beta - p^{\beta-1})$ представлений $\sigma \in \mathcal{R}_{N,N_1}$ таких, что $\sigma^t[a,b,c]\sigma \in \mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$.

2. $s - \alpha = 0$.

Поскольку $p \nmid (a+b+c)$ и в силу (4.16) $\sigma^t[a,b,c]\sigma \in \mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$ для любого σ второго типа, следовательно имеем p^{s-1} представителей второго типа.

Подсчет представителей первого типа проводится аналогично пункту 1. Тогда мы получаем: если $2\beta - 2\alpha > s - \alpha$, то имеем: если $\left(\frac{D}{p}\right) = -1$, то $p^s + p^{s-1}$, если $p \mid D$, то p^s, если $\left(\frac{D}{p}\right) = 1$, то $p^s - p^{s-1}$ представителей $\sigma \in \mathcal{R}_{N,N_1}$ таких, что $\sigma^t[a,b,c]\sigma \in \mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$.

2. $p = 2$.

Исключительный случай: $\alpha=\beta=s$ и $D\equiv 1(\mathrm{mod}\,8)$. Имеем $2\nmid b$ и $2\mid(a+b+c)$ для любой формы $[a,b,c]\in\mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$.

Для представителей первого типа $a_1=a+N_1j(2a+b+N_1j(a+b+c))$. Так как $2\mid(a+b+c)$ и $2\nmid(2a+b)$, то $2\nmid a_1$ в том и только в том случае, когда $j\equiv 0(\mathrm{mod}\,2)$ и значит имеем 2^S-2^{S-1} различных j по модулю 2^S.

Для представителей второго типа в силу (4.15) и так как $2\mid(a+b+c)$ верно $2\mid a_1$.Значит имеем 2^S-2^{S-1} представителей $\sigma\in\mathcal{R}_{N,N_1}$ таких, что $\sigma^t[a,b,c]\,\sigma\in\mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$.

В остальных случаях, согласно предложению 3.2, в каждом классе форм $\mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$ существует форма $[a,b,c]$ такая, что $2\nmid(a+b+c)$. Возьмем такую форму. Тогда для представителей первого типа условие $2^\gamma\mid a_1$ эквивалентно существованию решения системы

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

с неизвестными x, j.

Подсчет числа представителей проводится аналогично пункту 1. Формулы для числа представителей получаются теже самые, что и для $p>2$, только условия на дискриминант D: $\left(\frac{D}{p}\right)=-1$, $p\mid D$, $\left(\frac{D}{p}\right)=1$следует заменить соответственно на $D\equiv 5(\mathrm{mod}\,8)$, $D\equiv 0(\mathrm{mod}\,4)$, $D\equiv 1(\mathrm{mod}\,8)$.

Теперь, объединяя полученные выражения для числа представителей $\sigma\in\mathcal{R}_{N,N_1}$ таких, что $\sigma^t[a,b,c]\,\sigma\in\mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$ в единую формулу, мы получаем предложение 4.7.■

ПРЕДЛОЖЕНИЕ 4.8. Пусть $\mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)\neq\emptyset$ и p,N_1,n_1,α,β,s - целые числа, определенные в 4.5. Тогда

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

$$\frac{\varepsilon(p,q,n)\left(p^{[\min(2\beta,\,s+\alpha)/2]}-\eta(p,q,n)p^{[\min(2\beta,\,s+\alpha)/2]-1}\right)}{\ln\left((t_0+q\sqrt{Du_0})/2\right)\,/\,\ln\left((t_1+\frac{q}{p^\alpha}\sqrt{Du_1})/2\right)} \qquad (4.17)$$

$$\times h_{N_1,\frac{N_1}{n_1}}\left(\left(\frac{q}{n}\right)^2 D\right),$$

где $\varepsilon(p,q,n)$ и $\eta(p,q,n)$ определены в (4.13) и (4.14) соответственно, и (t_0,u_0), (t_1,u_1) - фундаментальные решения уравнений $t^2+q^2Du^2=4$ и $t^2+\left(\frac{q}{p^\alpha}\right)^2 Du^2=4$ соответственно.

ДОКАЗАТЕЛЬСТВО. Так как $\mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right) \subset \mathcal{F}_{N_1,\frac{N}{n_1}}\left(\left(\frac{q}{n}\right)^2 D\right)$, то в силу предложений 4.4, 4.5 и 4.7 получаем

$$h(\mathcal{G}) = \frac{\varepsilon(p,q,n)(p^{[\min(2\beta,\, s+\alpha)/2]} - \eta(p,q,n)p^{[\min(2\beta,\, s+\alpha)/2]-1})}{\ln((t_0 + q\sqrt{Du_0})/2) \;/\; \ln((t_1 + \frac{q}{p^{\alpha}}\sqrt{Du_1})/2)},$$

где $h(\mathcal{G})$-число классов форм из $\mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$ по $\Gamma_0(N)$ содержащихся в классе $\mathcal{G} \subset \mathcal{F}_{N_1,\frac{N}{n_1}}\left(\left(\frac{q}{n}\right)^2 D\right)$ по $\Gamma_0(N_1)$. Из этой формулы следует, что $h(\mathcal{G})$ не зависит от класса $\mathcal{G}$ и следовательно верно 4.17.■

Теперь мы легко получаем следующее важное утверждение.

ПРЕДЛОЖЕНИЕ 4.9. Пусть $\mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right) \neq \emptyset$. Тогда

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

$$= \frac{\prod_{i=1}^{\omega(N)} \varepsilon(p_i,q,n)(p_i^{[\min(2\beta_i,\, s_i+\alpha_i)/2]} - \eta(p_i,q,n)p_i^{[\min(2\beta_i,\, s_i+\alpha_i)/2]-1})}{\ln((t_0 + q\sqrt{Du_0})/2) \;/\; \ln((t_1 + \frac{q}{n}\sqrt{Du_1})/2)} \qquad (4.18)$$

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

где p_i, β_i, s_i определены в теореме 1 и α_i - показатель p_i в каноническом разложении числа n.

ДОКАЗАТЕЛЬСТВО. Рассмотрим пары (N_i,n_i), (N_{i+1},n_{i+1}) из рекуррентной последовательности (4.8). Тогда $\mathcal{F}_{N_i,\frac{N_i}{n_i}}\left(\left(\frac{q}{n}\right)^2 D\right) \subset \mathcal{F}_{N_{i+1},\frac{N_{i+1}}{n_{i+1}}}\left(\left(\frac{q}{n}\right)^2 D\right)$ и так как $\mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right) \neq \emptyset$, то $\mathcal{F}_{N_i,\frac{N_i}{n_i}}\left(\left(\frac{q}{n}\right)^2 D\right) = \emptyset$. Поскольку $\frac{q}{n} = \frac{\frac{qn_i}{n}}{n_i} = \frac{q_i}{n_i}$ и p_i, N_{i+1}, α_i, β_i, s_i - удовлетворяют условиям (4.6), то к $\mathcal{F}_{N_i,\frac{N_i}{n_i}}\left(\left(\frac{q}{n}\right)^2 D\right)$ применимо предложение 4.8. Последовательно применяя формулу (4.17) мы получаем (4.18).■

Теперь подставляя (4.18) в формулу (4.5), мы получаем формулу, выражающую $\nu(L,N)$ через линейную комбинацию $h\left(\left(\frac{q}{n}\right)^2 D\right)$. Эту формулу можно значительно упростить, выразив $h\left(\left(\frac{q}{n}\right)^2 D\right)$ через $h(q^2D)$ и затем вычислив внутреннюю сумму по делителям $n \in S(q,N)$.

ПРЕДЛОЖЕНИЕ 4.10. Пусть $\mathcal{F}_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right) \neq \emptyset$. Тогда

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

$$= \prod_{i=1}^{\omega(N)} \varepsilon(p_i,q,n)\left(p_i^{[\min(2\beta_i-2\alpha_i,s_i-\alpha_i)/2]} - \bar{\eta}(p_i,q,n)p_i^{[\min(2\beta_i-2\alpha_i,s_i-\alpha_i)/2]-1}\right)$$

$$\times h(q^2D)$$

$$\bar{\eta}(p,q,n) = \begin{cases} 1, \text{ если } \alpha > 0 \text{ и выполняется хотя бы одно из условий:} \\ \quad 2\beta - 2\alpha > s - \alpha > 0; \\ \quad 2\beta - 2\alpha = s - \alpha > 0 \text{ и } p \mid D; \\ \quad 2\beta - 2\alpha < s - \alpha < 0 \text{ и } \left(\left(\frac{D}{p}\right) = 1 \text{ и } p > 2 \text{ или } D \equiv 1 \pmod 8 \text{ и } p = 2\right); \\ 2, \text{ если } \alpha > 0 \text{ и } 2\beta - 2\alpha = s - \alpha > 0 \text{ и } \left(\frac{D}{p}\right) = 1; \\ 0, \text{ в остальных случаях.} \end{cases}$$

ДОКАЗАТЕЛЬСТВО. Воспользуемся хорошо известной формулой

$$h(s^2d) = h(d)\frac{\ln((t_1+u_1\sqrt{d})/2)}{\ln((t_0+u_0\sqrt{d})/2)} s \prod_{p \mid s}(1-j(d,p)\frac{1}{p}), \qquad (4.19)$$

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

$$j(d,p) = \begin{cases} \left(\frac{d}{p}\right), \text{ если } p \neq 2 \\ \chi_8(d), \text{ если } p = 2 \end{cases}, \qquad \chi_8(d) = \begin{cases} 0, \text{ если } d \equiv 0 \pmod 2 \\ 1, \text{ если } d \equiv 1, 7 \pmod 8. \\ -1, \text{ если } d \equiv 3, 5 \pmod 8 \end{cases}$$

Выражая $h\left(\left(\frac{q}{n}\right)^2 D\right)$ через $h(q^2D)$ по формуле (4.19) и подставляя в (4.18) получаем:

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

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

$$\times h(q^2D).$$

Знаменатель дроби отличен от единицы только в случае $\beta_i = \alpha_i$ и $p_i \nmid D$.

Рассмотрим отдельно два случая:

1. $\left(\frac{D}{p_i}\right) = -1$ и $p_i > 2$ или $D \equiv 5 \pmod 8$ и $p_i = 2$.

Тогда $2\beta_i - 2\alpha_i \geq s_i - \alpha_i$ и значит $s_i = \alpha_i$ и по определению в этом случае $\eta(p_i,q,n) = -1$ и поэтому дробь равна единице и значит $\bar{\eta}(p_i,q,n) = 0$.

2. $\left(\frac{D}{p_i}\right) = 1$ и $p_i > 2$ или $D \equiv 1 \pmod 8$ и $p_i = 2$.

Тогда по определению $\eta(p_i,q,n) = 1$ и поэтому дробь равна единице и значит $\bar{\eta}(p_i,q,n) = 0$.■

Подставляя выражение для $h_{N,\frac{N}{n}}\left(\left(\frac{q}{n}\right)^2 D\right)$ полученное в предложении 4.10 в формулу (4.5) получаем

$$\nu(L,N) = \sum_{\substack{q \mid Q \\ q \nmid U_k,\ k \mid m,\ k \neq m \\ x^2 \equiv q^2 D \pmod{4N}}} \left(\sum_{n \in S(q,N)} \prod_{i=1}^{\omega(N)} \varepsilon(p_i,q,n) \right.$$

$$\left. \times \left(p_i^{[\min(2\beta_i - 2\alpha_i, s_i - \alpha_i)/2]} - \overline{\eta}(p_i,q,n) p_i^{[\min(2\beta_i - 2\alpha_i, s_i - \alpha_i)/2]-1} \right) \right) \times h(q^2 D).$$

Осталось провести суммирование по делителям n.

Доказательство теоремы 1.

Для краткости введем обозначение

$$f(p,q,n) = \varepsilon(p,q,n)\left(p^{[\min(2\beta - 2\alpha, s-\alpha)/2]} - \overline{\eta}(p,q,n) p^{[\min(2\beta - 2\alpha, s-\alpha)/2]-1}\right).$$

ЛЕММА 1.

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

ДОКАЗАТЕЛЬСТВО. Доказательство проведем индукцией по числу простых, входящих в каноническое разложение N.

База индукции $N = p^S$. Из определения S(q,N) (смотри (4.1), (4.2)) следует, что $S(q,p^S) = S(p^\beta,p^S)$. Очевидно $f(p,q,n) = f(p,p^\beta,n)$ и значит формула верна.

Шаг индукции $N = \prod_{i=1}^{r} p_i^{s_i}$, где $r = \omega(N) \geq 2$. Положим $N = N_1 p_r^{s_r}$, $q = q_1 p_r^{\beta_r}$.

Из определения S(q,N) следует, что всякое $n \in S(q,N)$ единственным образом представимо в виде $n = n' n_r$, где $n' \in S(q_1,N_1)$ и $n_r \in S(p_r^{\beta_r},p_r^{s_r})$. Тогда имеем

$$\sum_{n \in S(q,N)} \prod_{i=1}^{r} f(p_i,q,n) = \sum_{n' \in S(q_1,N_1)} \sum_{n_r \in S(p_r^{\beta_r},p_r^{s_r})} f(p_r,q,n'n_r) \prod_{i=1}^{r-1} f(p_i,q,n'n_r) =$$

$$\sum_{n_r \in S(p_r^{\beta_r},N)} f(p_r,p_r^{\beta_r},n_r) \sum_{n' \in S(q_1,N_1)} \prod_{i=1}^{r-1} f(p_i,q_1,n').$$

По индуктивному предположению

$$\sum_{n' \in S(q_1,N_1)} \prod_{i=1}^{r-1} f(p_i,q_1,n') = \prod_{i=1}^{r-1} \sum_{n_i \in S(p_i^{\beta_i},N)} f(p_i,p_i^{\beta_i},n_i)$$

и поэтому наша сумма равна

$$\prod_{i=1}^{r} \sum_{n_i \in S(p_i^{\beta_i},N)} f(p_i,p_i^{\beta_i},n_i),$$

что и требовалось доказать.■

ЛЕММА 2.

$$\sum_{n\in S(p^{\beta},N)} f(p,p^{\beta},n) = \varepsilon_1(p,\beta,s)\,(p^{[\min(2\beta,s)/2]} + \delta(p,\beta,s)p^{[\min(2\beta,s)-1)/2]}),$$

где

$$\varepsilon_1(p,\beta,s) = \begin{cases} 2 \text{ если } 2\beta < s \text{ и } \left(\left(\frac{D}{p_i}\right) = 1 \text{ и } p_i > 2 \text{ или } D \equiv 1 (\mathrm{mod}\ 8) \text{ и } p_i = 2\right), \\ 1 \text{ в противном случае} \end{cases}$$

$\delta(p,\beta,s)$-определено в теореме 1.

ДОКАЗАТЕЛЬСТВО. Введем обозначение: $\bar{s} = [(s-1)/2]$ и рассмотрим отдельно несколько случаев.

1. $\beta \geq s$.

В силу (4.13) $\varepsilon(p,p^{\beta},n) = 1$ и так как $\min(2\beta-2\alpha,\ s-\alpha) = s-\alpha$, то

$$\sum_{n\in S(p^{\beta},N)} f(p,p^{\beta},n) = \sum_{n\in S(p^{\beta},N)} (p^{[(s-\alpha)/2]} - \bar{\eta}(p,p^{\beta},n)\,p^{[(s-\alpha)/2]-1}) =$$

$$= p^{[s/2]} + \sum_{k=0}^{\bar{s}} (p^{\bar{s}-k} - \bar{\eta}(p,p^{\beta},p^{s-2\bar{s}+2k})\,p^{\bar{s}-k-1}) = p^{[s/2]} + p^{\bar{s}}.$$

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

В этом случае $\min(2\beta-s,s) = 2\beta-s$.

а). $\left(\frac{D}{p}\right) = -1$ и $p > 2$ или $D \equiv 5(\mathrm{mod}\ 8)$ и $p = 2$.

Тогда

$$\sum_{n\in S(p^{\beta},N)} f(p,p^{\beta},n) = p^{[s/2]} + \sum_{k=0}^{\beta-s+\bar{s}} (p^{\bar{s}-k} - \bar{\eta}(p,p^{\beta},p^{s-2\bar{s}+2k})\,p^{\bar{s}-k-1} = p^{[s/2]} + p^{\bar{s}}.$$

б). $p \mid D$.

$$\sum_{n\in S(p^{\beta},N)} f(p,p^{\beta},n) =$$

$$p^{[s/2]} + \sum_{k=0}^{\beta-s+\bar{s}} (p^{\bar{s}-k} - \bar{\eta}(p,p^{\beta},p^{s-2\bar{s}+2k})\,p^{\bar{s}-k-1} + p^{s-k-1} - \bar{\eta}(p,p^{\beta},p^{2\beta-s+1})\,p^{s-\beta-2} = p^{[s/2]} + p^{\bar{s}}.$$

в). $\left(\frac{D}{p}\right) = 1$ и $p > 2$ или $D \equiv 1(\mathrm{mod}\ 8)$ и $p = 2$.

В этом случае $2^{2\beta-s} \notin S(2^{\beta},N)$. Положим формально $\bar{\eta}(2,2^{\beta},2^{2\beta-s}) = 2$ и тогда $2^{s-\beta} - \bar{\eta}(2,2^{\beta},2^{2\beta-s})\,2^{s-\beta-1} = 0$.

Поэтому имеем

$$\sum_{n\in S(p^{\beta},N)} f(p,p^{\beta},n) =$$

$$p^{[s/2]}+\sum_{k=0}^{\beta-s+\bar{s}}(p^{\bar{s}-k}-\bar{\eta}(p,p^{\beta},p^{s-2\bar{s}+2k})\,p^{\bar{s}-k-1}+p^{s-k-1}-\bar{\eta}(p,p^{\beta},p^{2\beta-s+1})\,p^{s-\beta-2}=p^{[s/2]}+p^{\bar{s}}.$$

3. $2\beta = s$

а) $\left(\frac{D}{p}\right) = -1$ и $p \neq 2$ или $D \equiv 5 \pmod 8$ и $p = 2$. Тогда $S(p^{\beta},N) = \{1\}$ и

$$f(p,p^{\beta},1) = p^{\beta}.$$

б) $p \mid D$

Тогда $S(p^{\beta},N) = \{1\}$ и

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

в) $\left(\frac{D}{p}\right) = 1$ и $p \neq 2$ или $D \equiv 1 \pmod 8$ и $p = 2$.

$$\sum_{n\in S(p^{\beta},N)} f(p,p^{\beta},n) = p^{\beta}+2\sum_{k=1}^{\beta}(p^{\beta-k}-\bar{\eta}(p,p^{\beta},p^{k})\,p^{\beta-k-1}) = p^{\beta}+2p^{\beta-1} = p^{[2\beta/2]}+p^{[(2\beta-1)/2]}.$$

4. $2\beta < s$

а) $p \mid D$

Тогда $S(p^{\beta}) = \{1\}$ и $f(p,p^{\beta},1) = p^{[2\beta/2]}$.

б) $\left(\frac{D}{p}\right) = 1$ и $p \neq 2$ или $D \equiv 1 \pmod 8$ и $p = 2$.

$$\sum_{n\in S(p^{\beta},N)} f(p,p^{\beta},n) = 2p^{\beta}+2\sum_{k=1}^{\beta}(p^{\beta-k}-\bar{\eta}(p,p^{\beta},p^{k})\,p^{\beta-k-1}) = 2(p^{[2\beta/2]}+p^{[(2\beta-1)/2]}).$$

Тогда в силу лемм 1 и 2 и учитывая, что

$$\prod_{i=1}^{\omega(N)}\varepsilon_i(p_i,\beta_i,s_i) = 2^{\omega\left(\frac{N}{(q^2D,N)}\right)},$$

получаем утверждение теоремы 1.■

§5 Результаты вычислений.

На основе формулы из теоремы 1 нами была написана программа для IBM PC и **вычислены** зиачения функции $\nu(L,N)$ для $3 \leq L \leq 10000$ и $1 \leq N \leq 12$. В ниже

напечатанной таблице приведена часть этих результатов: $3 \leq L \leq 102$ и $1 \leq N \leq 10$.

Из таблицы видно, что для простого N

$$\nu(L,N) < 3\,\nu(L,1). \tag{5.1}$$

В следующей работе мы докажем неравенства типа (5.1) для любого N.

Кроме того нами были проведены вычисления связанные с функцией распределения

$$\pi_{\Gamma(1)}(T) = \#\{\,\{\bar{g}\} - \text{примитивный класс},\ N(\bar{g}) \leq T\,\}.$$

Ниже мы приводим график функции

$$M(x) = (\pi_{\Gamma(1)}(T) - \mathrm{li}(T))/T^{1/2},$$

где $T = ((x + \sqrt{x^2-4})/2)^2$, $3 \leq x \leq 10000$. График разбит на 17 фрагментов. Абцисса каждого фрагмента, кроме первого и последнего, содержит по 600 точек соответствующих целым значениям x. По оси ординат отмечены две точки $+0.1$ и -0.1.

Отметим, что

$$\max_{600 \leq x \leq 10000} M(x) \approx 0.16 \quad \text{при } x = 7778,$$

$$\min_{600 \leq x \leq 10000} M(x) \approx -0.43 \quad \text{при } x = 717,$$

$$\min_{1200 \leq x \leq 10000} M(x) \approx -0.42 \quad \text{при } x = 1869,$$

$$\min_{2400 \leq x \leq 10000} M(x) \approx -0.41 \quad \text{при } x = 7161,$$

$$\min_{7200 \leq x \leq 10000} M(x) \approx -0.39 \quad \text{при } x = 9001,$$

$$\max_{7800 \leq x \leq 10000} M(x) \approx 0.15 \quad \text{при } x = 8842.$$

Мы благодарим Н.В. Кузнецова и В.А. Быковского за стимулирующий интерес к нашей работе, а так же М.М. Смотрова за помощь в общении с компьютером и написании программ.

Литература.

1. Дирихле П.Г. Лекции по теории чисел.-М.,Л., 1936.-403с.

2. Кузнецов Н.В. Арифметическая форма формулы следа Сельберга и распределение норм примитивных гиперболических классов модулярной группы.-Хабаровск,1978.-44с.-(Препринт/АН СССР, Дальневост. науч. центр, ХабКНИИ).

3. Sarnak P. Class Numbers of Indefinite Binary Quadratic Forms.//J.number theory.-1982.-V.15.-p.229-247.

Таблица чисел $\nu(L,N)$ **классов сопряженных примитивных гиперболических элементов группы** $\Gamma_0(N)$ **со следом** L.

L\N	1	2	3	4	5	6	7	8	9	10
3	1	0	0	0	1	0	0	0	0	0
4	2	2	2	0	0	2	0	0	0	0
5	2	0	2	0	4	0	2	0	0	0
6	3	5	0	6	0	0	6	4	0	0
7	2	0	4	0	2	0	0	0	6	0
8	4	4	4	0	4	4	8	0	0	4
9	2	0	0	0	0	0	2	0	0	0
10	6	10	6	12	12	10	0	8	0	20
11	3	0	6	0	0	0	0	0	12	0
12	4	4	0	0	4	0	4	0	0	4
13	4	0	4	0	4	0	8	0	0	0
14	6	12	6	18	0	12	0	20	0	0
15	4	0	0	0	8	0	8	0	0	0
16	6	6	12	0	0	12	6	0	24	0
17	4	0	4	0	4	0	0	0	0	0
18	7	14	0	20	7	0	0	24	0	14
19	4	0	4	0	0	0	4	0	0	0
20	10	10	16	0	20	16	20	0	24	20
21	2	0	0	0	0	0	0	0	0	0
22	12	20	12	24	12	20	24	16	0	20
23	4	0	4	0	8	0	4	0	0	0
24	4	4	0	0	0	0	0	0	0	0
25	8	0	14	0	16	0	0	0	24	0
26	12	20	12	24	0	20	12	16	0	0
27	5	0	0	0	10	0	10	0	0	0
28	8	8	8	0	8	8	0	0	0	8
29	8	0	14	0	0	0	16	0	24	0
30	14	26	0	36	28	0	14	40	0	52
31	4	0	4	0	0	0	0	0	0	0
32	8	8	8	0	8	8	0	0	0	8
33	4	0	0	0	4	0	4	0	0	0
34	16	30	28	42	0	52	32	48	42	0
35	8	0	8	0	16	0	0	0	0	0
36	8	8	0	0	0	0	16	0	0	0
37	8	0	8	0	8	0	8	0	0	0
38	18	30	36	36	18	60	0	24	72	30
39	4	0	0	0	0	0	0	0	0	0
40	16	16	16	0	32	16	16	0	0	32
41	8	0	8	0	0	0	16	0	0	0
42	12	20	0	24	12	0	0	16	0	20
43	12	0	24	0	12	0	24	0	48	0
44	8	8	8	0	0	8	8	0	0	0
45	6	0	0	0	12	0	0	0	0	0
46	16	32	16	48	0	32	0	64	0	0
47	10	0	16	0	10	0	20	0	24	0
48	14	14	0	0	24	0	28	0	0	24
49	4	0	4	0	0	0	0	0	0	0
50	28	52	28	72	56	52	56	80	0	104
51	7	0	0	0	0	0	14	0	0	0
52	18	18	32	0	32	32	0	0	56	32

L\N	1	2	3	4	5	6	7	8	9	10
53	8	0	8	0	8	0	0	0	0	0
54	12	20	0	24	0	0	12	16	0	0
55	12	0	12	0	24	0	24	0	0	0
56	16	16	28	0	0	28	0	0	48	0
57	8	0	0	0	8	0	16	0	0	0
58	24	40	24	48	24	40	24	32	0	40
59	8	0	8	0	0	0	0	0	0	0
60	12	12	0	0	24	0	0	0	0	24
61	10	0	16	0	0	0	10	0	24	0
62	28	56	28	84	28	56	56	104	0	56
63	8	0	0	0	8	0	0	0	0	0
64	16	16	16	0	0	16	32	0	0	0
65	18	0	36	0	36	0	18	0	72	0
66	16	32	0	48	0	0	0	64	0	0
67	8	0	8	0	8	0	0	0	0	0
68	16	16	16	0	16	16	16	0	0	16
69	10	0	0	0	0	0	20	0	0	0
70	36	60	72	72	72	120	0	48	144	120
71	8	0	8	0	0	0	16	0	0	0
72	8	8	0	0	8	0	8	0	0	8
73	14	0	14	0	24	0	0	0	0	0
74	30	50	48	60	0	80	0	40	72	0
75	12	0	0	0	24	0	12	0	0	0
76	16	16	16	0	0	16	32	0	0	0
77	14	0	14	0	24	0	0	0	0	0
78	28	52	0	72	28	0	56	80	0	52
79	16	0	32	0	0	0	16	0	60	0
80	24	24	24	0	48	24	0	0	0	48
81	6	0	0	0	0	0	0	0	0	0
82	32	64	32	96	32	64	32	128	0	64
83	18	0	36	0	18	0	36	0	72	0
84	8	8	0	0	0	0	0	0	0	0
85	20	0	20	0	40	0	40	0	0	0
86	24	40	24	48	0	40	24	32	0	0
87	8	0	0	0	8	0	0	0	0	0
88	20	20	32	0	20	32	0	0	48	20
89	8	0	8	0	0	0	8	0	0	0
90	36	60	0	72	72	0	72	48	0	120
91	12	0	12	0	0	0	0	0	0	0
92	36	36	72	0	36	72	72	0	144	36
93	8	0	0	0	8	0	8	0	0	0
94	28	52	28	72	0	52	0	80	0	0
95	16	0	16	0	32	0	0	0	0	0
96	18	18	0	0	0	0	32	0	0	0
97	24	0	48	0	24	0	48	0	96	0
98	32	60	32	84	64	60	0	96	0	120
99	8	0	0	0	0	0	16	0	0	0
100	28	28	28	0	56	28	56	0	0	56
101	10	0	16	0	0	0	0	0	24	0
102	30	50	0	60	60	0	0	40	0	100

График функции M(x).

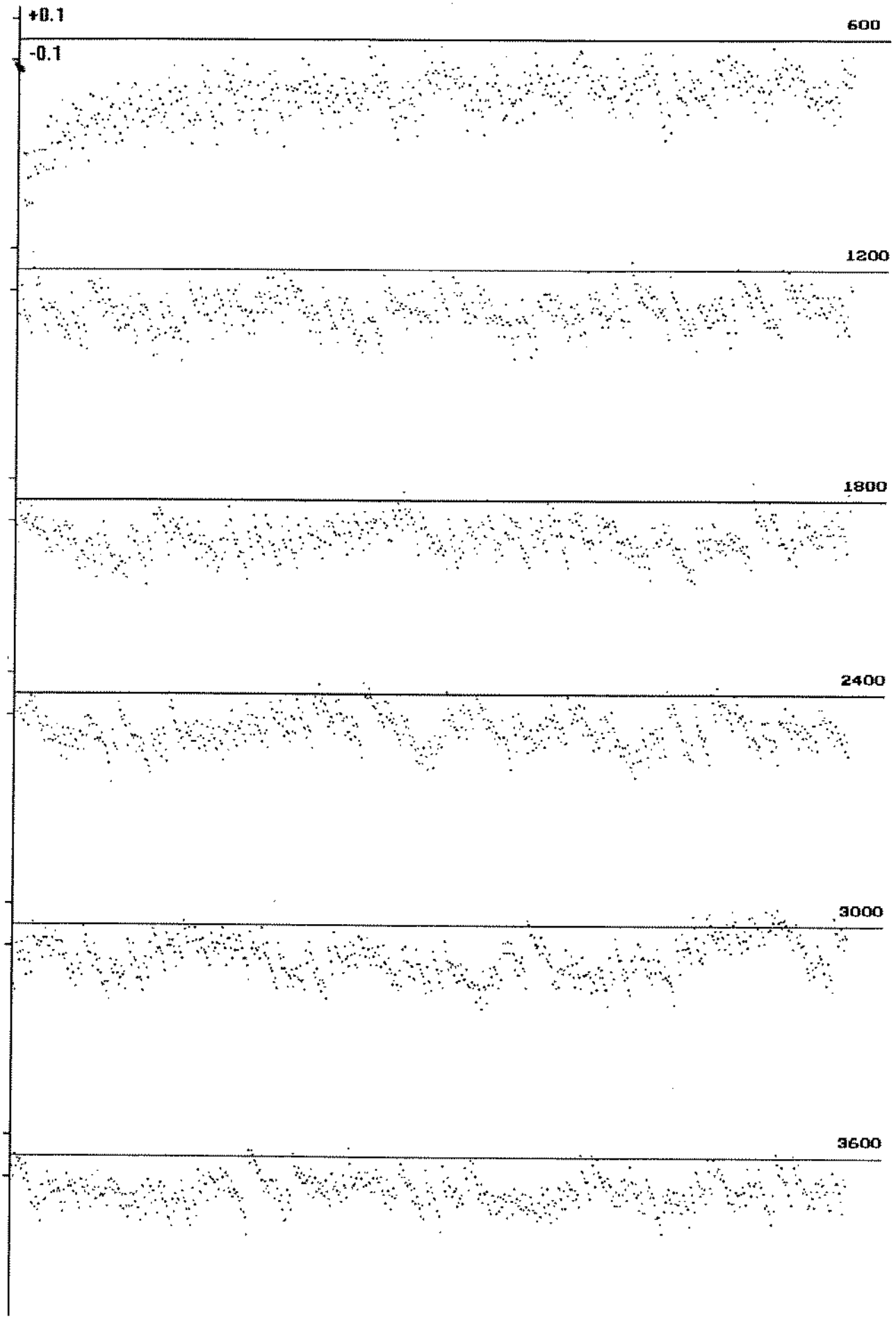

График функции M(x) (продолжение).

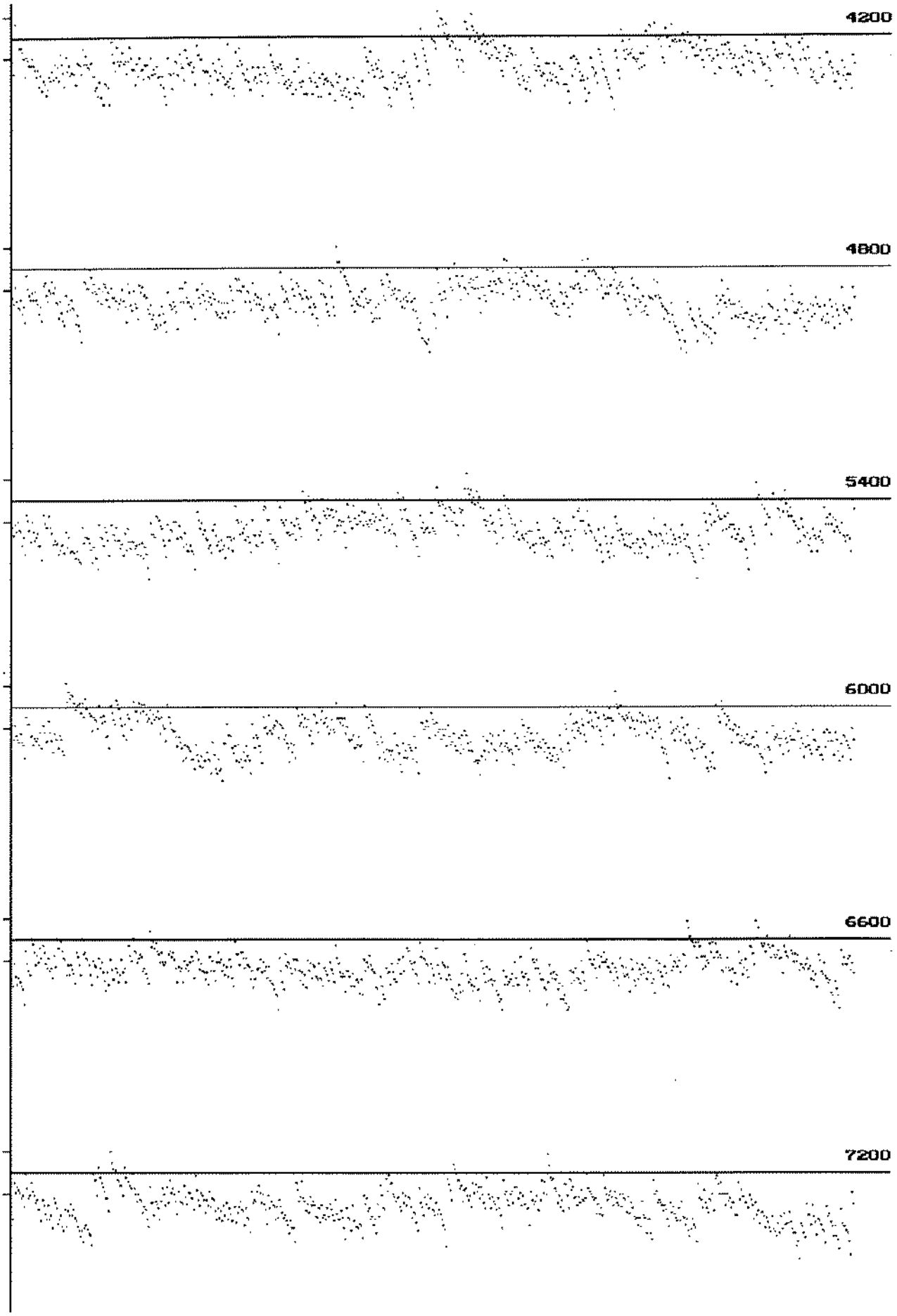

График функции M(x) (окончание).