ДАЛЬНЕВОСТОЧНЫЙ МАТЕМАТИЧЕСКИЙ ЖУРНАЛ. 2009. Том 9. № 1–2. С. 48–73

УДК 512.817.2
MSC2000 11E57 11F72 11M36

© В.В. Головчанский, М.Н. Смотров*

Мультипликативные свойства функции числа классов примитивных гиперболических элементов конгруэнц-подгруппы $\Gamma_0(N)$ по уровню N

Посвящается Н.В. Кузнецову в связи с 70-летием

Получены арифметические представления формулы следа Сельберга и дзета-функции Сельберга для конгруэнц-подгруппы $\Gamma_0(N)$, явное выражение чисел классов примитивных гиперболических элементов конгруэнц-подгруппы уровня N через числа классов примитивных элементов конгруэнц-подгруппы уровня $N_1 = N/p^i, (N, N_1) = 1$ и точная оценка сверху чисел классов по уровню N.

Ключевые слова: *конгруэнц-подгруппа модулярной группы, классы примитивных гиперболических элементов, уравнение Пелля, формула следа Сельберга.*

1. Обозначения и формулировка результатов

Эта работа является непосредственным продолжением работы авторов [1]. В [1] вывод формулы числа классов примитивных гиперболических элементов с фиксированной нормой для конгруэнц-подгруппы $\Gamma_0(N)$ основан на переходе от уровня N к уровню $N_1 = N/p^\alpha, p \nmid N_1$, поэтому следует ожидать, что число классов для подгруппы $\Gamma_0(N)$ может быть выражено через числа классов для подгруппы $\Gamma_0(N_1)$. В настоящей работе эти соотношения установлены. Полученные формулы весьма сложны, однако в случае, когда все классы с фиксированной нормой примитивны, а именно такие нормы составляют подавляющее большинство норм, число классов для подгруппы уровня N выражается линейно через число классов с той же нормой для подгруппы уровня N_1. Одновременно с функцией числа классов мы рассматриваем арифметическую функцию, которая естественным образом возникает в формуле следа Сельберга и в формуле логарифмической производной дзета-функции Сельберга.

Для фуксовой группы Γ первого рода формула следа может быть записана в следующем

* Хабаровское отделение Института прикладной математики Дальневосточного Отделения РАН, 680000, Хабаровск, ул. Дзержинского, 54. Электронная почта: gsm@iam.khv.ru

виде:

$$\sum_{j=0}^{\infty} h(\varkappa_j) + \{\text{вклад непрерывного спектра}\} = \{\text{вклад негиперболических элементов}\}$$

$$+\sum_{\{P\}}\sum_{k=1}^{\infty}\frac{\log \mathbf{N}(P)}{\mathbf{N}(P)^{k/2}-\mathbf{N}(P)^{-k/2}}g(k\log \mathbf{N}(P)), \tag{1.1}$$

а логарифмическая производная дзета-функции Сельберга имеет вид

$$\frac{Z'}{Z}(s) = \sum_{\{P\}}\sum_{k=1}^{\infty}\frac{\log \mathbf{N}(P)}{\mathbf{N}(P)^{k/2}-\mathbf{N}(P)^{-k/2}}\mathbf{N}(P)^{-(s-1/2)k}, \tag{1.2}$$

где $\varkappa_j = \sqrt{\lambda_j - 1/4}$, λ_j — точка дискретного спектра оператора Лапласа —Бельтрами группы Γ, g — преобразование Фурье функции h, $\{P\}$ — класс примитивных гиперболических элементов группы Γ, $\mathbf{N}(P) \equiv ((|trP|+\sqrt{(trP)^2-4})/2)^2$ — норма гиперболического элемента P (и соответствующего ему класса). Отметим, что $\mathbf{N}^k(P) = \mathbf{N}(P^k)$, поэтому суммирование по классам примитивных элементов и натуральному ряду в (1.1) и (1.2) можно заменить суммированием по всем классам, при этом логарифм следует брать от нормы соответствующего примитивного класса. Введение нового объекта $\nu(\mathbf{N})$ — числа классов примитивных гиперболических элементов группы Γ с фиксированной нормой $\mathbf{N}$ — позволяет преобразовать двойные ряды в формулах (1.1) и (1.2) в ряды по нормам. Зафиксируем некоторую норму $\mathbf{N}$. Нормы пробегают дискретное множество значений, и каждая норма представима единственным образом в виде $\mathbf{N} = \mathbf{N}_0^m$, где m — наибольшее натуральное число и $\mathbf{N}_0$ — норма некоторого примитивного класса. Тогда $\mathbf{N} = (\mathbf{N}_0^k)^{m/k}$ для любого $k \mid m$, и других представлений нет. Всякий непримитивный класс является степенью некоторого примитивного, поэтому непримитивный класс $\{\gamma\}$ с нормой $\mathbf{N}$ есть степень $\{P\}^{m/k}$ примитивного класса с нормой $\mathbf{N}_0^k = \mathbf{N}^{k/m}$. Ясно, что число непримитивных классов с нормой $\mathbf{N}$, являющихся степенями с показателем m/k, равно $\nu(\mathbf{N}^{k/m})$, поэтому, принимая во внимание, что $\log \mathbf{N}^{k/m} = k/m \log \mathbf{N}$, получаем представление

$$\sum_{\{P\}}\sum_{k=1}^{\infty}\frac{\log \mathbf{N}(P)}{\mathbf{N}(P)^{k/2}-\mathbf{N}(P)^{-k/2}}g(k\log \mathbf{N}(P)) = 2\sum_{\mathbf{N}} B(\mathbf{N})g(\log \mathbf{N}) \text{ и } \frac{Z'}{Z}(s) = 2\sum_{\mathbf{N}}\frac{B(\mathbf{N})}{\mathbf{N}^{s-1/2}},$$

где

$$B(\mathbf{N}) = \frac{\log \mathbf{N}^{1/2}}{\mathbf{N}^{1/2}-\mathbf{N}^{-1/2}}\sum_{k|m}\frac{k}{m}\nu\left(\mathbf{N}^{\frac{k}{m}}\right)$$

и суммирование ведется по всем нормам гиперболических элементов группы.

Формула следа Сельберга в спектральной теории автоморфных форм дает явное выражение следа оператора Лапласа — Бельтрами через спектр соответствующей дискретной подгруппы Γ. Так как число классов эллиптических и параболических элементов подгруппы Γ конечно, то дискретный спектр оператора Лапласа — Бельтрами полностью определяется коэффициентами $B(\mathbf{N})$(устремляя $h(r)$ к функции $h(r_0)$ с носителем в точке r_0, получаем значение $h(r_0)$ как предел ряда $2\sum_{\mathbf{N}} B(\mathbf{N})g(\log \mathbf{N})$ при $h(r) \to h(r_0)$). Впервые $B(\mathbf{N})$ для случая модулярной группы, в которой эти коэффициенты определялись как вычеты специальных рядов Дирихле,изучались в работе Н.В. Кузнецова [2]. В связи с проблематикой квантового хаоса в [3] изучалась корреляционная функция $B(\mathbf{N}+l)B(\mathbf{N})$ для модулярной группы, в [4] вычислено среднее значение квадратов $B(\mathbf{N})$ для конгруэнц-подгрупп модулярной группы. Для любой фуксовой группы первого рода справедлива асимптотика

$$\sum_{\mathbf{N}\le X} B(\mathbf{N}) = \sqrt{X} + \sum_{0<\varkappa_j<1/2}\frac{X^{\varkappa_j}}{2\varkappa_j} + O(X^{1/4}). \tag{1.3}$$

Эта асимптотика получается частным суммированием из известной асимптотической формулы, полученной ещё Сельбергом:

$$\Psi(X) = X + \sum_{0<\varkappa_j<1/2} \frac{X^{1/2+\varkappa_j}}{1/2+\varkappa_j} + O(X^{3/4}), \tag{1.4}$$

где

$$\Psi(X) = \sum_{\{P\},\mathbf{N}(P)\le X} \ln(\mathbf{N}(P)) \equiv \sum_{\mathbf{N}\le X} \ln(\mathbf{N}) \sum_{k|m} \frac{k}{m}\nu\left(\mathbf{N}^{\frac{k}{m}}\right).$$

Для конгруэнц-подгруппы $\Gamma_0(N)$ коэффициенты $B(\mathbf{N})$ можно представить в арифметической форме. В этом случае норма $\mathbf{N} = ((L+\sqrt{L^2-4}\,)/2)^2$, где $L \ge 3$ — целое ; $\nu\,(L,N)$ — число классов примитивных гиперболических элементов группы $\Gamma_0(N)$ с нормой $((L+\sqrt{L^2-4}\,)/2)^2$; D — фундаментальный дискриминант, который однозначно определяется из условия

$$L^2 - 4 = Q^2 D; \tag{1.5}$$

(T_1, U_1) — фундаментальное решение уравнения Пелля $t^2 - Du^2 = 4$, а пара (T_k, U_k) и натуральное m определяются из условий

$$\frac{T_k + \sqrt{D}\,U_k}{2} = \left(\frac{T_1+\sqrt{D}\,U_1}{2}\right)^k, \quad \frac{L+\sqrt{D}\,Q}{2} = \left(\frac{T_1+\sqrt{D}\,U_1}{2}\right)^m. \tag{1.6}$$

В этих обозначениях для конгруэнц-подгруппы $\Gamma_0(N)$

$$B(L,N) = \frac{\log((L+\sqrt{L^2-4})/2)}{\sqrt{L^2-4}} \sum_{k|m} \frac{k}{m}\nu(T_k, N). \tag{1.7}$$

В разделе 2 настоящей работы приведено арифметическое выражение (2.38) для $B(L,N)$. В работах [5], [6] также получено арифметическое представление логарифмической производной дзета-функции Сельберга для кватернионных подгрупп $SL_2(R)$ и конгруэнц-подгрупп модулярной группы соответственно, однако это представление существенно отличается от представленного в нашей работе.

Теперь перейдем к формулировке основных результатов работы. Далее всюду p обозначает простое число. Кроме того, зафиксируем следующие обозначения:

$$\begin{gathered} s \text{ – кратность, с которой } p \text{ входит в разложение } N;\\ \alpha \text{ – кратность, с которой } p \text{ входит в разложение } Q;\\ N_1 = N/p^s; \quad N = \prod_{i=1}^{\omega(N)} p_i^{s_i}; \quad Q = Q_1 \prod_{i=1}^{\omega(N)} p_i^{\alpha_i}, \text{ где } (Q_1, N) = 1 \text{ и} \end{gathered} \tag{1.8}$$

$\omega(N)$ — число простых, входящих в разложение числа N.

В разделе 2 получены формулы, выражающие $\nu(L,N)$ в виде линейной комбинации $\nu(T_{\frac{m}{k}}, N_1)$, а также формула, выражающая $B(L,N)$ через $B(L,N_1)$. Нам представляется, что последняя формула имеет самостоятельный интерес, и поэтому мы формулируем ее как теорему.

Теорема 1. *Для любого* $L \ge 3$

$$B(L,N) = \delta(p,s,\alpha)B(L,N_1),$$

и если (L,Q) фундаментальное решение уравнения Пелля $t^2 - Du^2 = 4$, то

$$\nu(L,N) = \delta(p,s,\alpha)\nu(L,N_1),$$

где

a) *если* $\left(\frac{D}{p}\right) = 1$ *при* $p \neq 2$ *и* $D \equiv 1 \pmod 8$ *при* $p = 2$, *то*

$$\delta(p,s,\alpha) = \begin{cases} 2p^{\alpha}, & \text{если } 2\alpha < s; \\ p^{[s/2]} + p^{[(s-1)/2]}, & \text{если } 2\alpha \geq s; \end{cases}$$

b) *если* $\left(\frac{D}{p}\right) = -1$ *при* $p \neq 2$ *и* $D \equiv 5 \pmod 8$ *при* $p = 2$, *то*

$$\delta(p,s,\alpha) = \begin{cases} 0, & \text{если } 2\alpha < s; \\ \left(p^{[s/2]} + p^{[(s-1)/2]}\right) \dfrac{p^{\alpha+1} + p^{\alpha} - \left(p^{[(s+1)/2]} + p^{[s/2]}\right)}{p^{\alpha+1} + p^{\alpha} - 2}, & \text{если } 2\alpha \geq s; \end{cases}$$

c) *если* $p \mid D$, *то*

$$\delta(p,s,\alpha) = \begin{cases} 0, & \text{если } 2\alpha < s-1; \\ \left(p^{[s/2]} + p^{[(s-1)/2]}\right) \dfrac{2p^{\alpha+1} - \left(p^{[(s+1)/2]} + p^{[s/2]}\right)}{2p^{\alpha+1} - 2}, & \text{если } 2\alpha \geq s-1. \end{cases}$$

З а м е ч а н и е. Переход от группы $\Gamma_0(N)$ к группе $\Gamma_0(N_1)$ выражается в преобразовании $B(L,N) = \delta(p,s,\alpha)B(L,N_1)$, поэтому более детальное исследование $B(L,1)$ может помочь в решении проблемы исключительных собственных значений для конгруэнц-подгрупп (гипотеза Сельберга).

Следствие 1. *Пусть* $(N_1,N_2) = 1$, *тогда*

$$B(L,N_1N_2) = \frac{B(L,N_1)B(L,N_2)}{B(L,1)}.$$

Следствие 2. *Пусть N имеет каноническое разложение* (1.8), *тогда*

$$B(L,N) \leq A(N)B(L,1),$$

где

$$A(N) = \prod_{i=1}^{\omega(N)} (p_i^{[s_i/2]} + p_i^{[(s_i-1)/2]}). \tag{1.9}$$

В разделе 3 настоящей работы на основе результатов раздела 2 получена оценка отношения $\nu(L,N)/\nu(L,1)$.

Теорема 2. *Пусть N имеет каноническое разложение* (1.8), *тогда*

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

причем равенство достигается на бесконечном числе пар (L,N).

Хотя оценка теоремы 2 точна, в случае, когда N бесквадратно, можно получить лучшую оценку.

Теорема 3. *Пусть N бесквадратно, тогда*

$$\nu(L,N) \le 2^{\omega(N)}\nu(L,1).$$

В разделе 4 нами получено уточнение асимптотической формулы функции распределения величины $B(L,N)$ для конгруэнц-подгруппы $\Gamma_0(N)$ и приведены результаты численных экспериментов по проверке гипотетической функции распределения. Результаты вычислений подтверждают эту гипотезу.

Теорема 4. *Для конгруэнц-подгруппы $\Gamma_0(N)$ справедлива следующая асимптотическая формула для функции распределения величины $B(L,N)$:*

$$\sum_{L\le X} B(L,N) = X + \sum_{0<\varkappa_j<1/2} \frac{X^{2\varkappa_j}}{2\varkappa_j} + O(A(N)X^{2/5+\varepsilon}). \qquad (1.10)$$

2. Соотношения между числами классов групп $\Gamma_0(N)$ и $\Gamma_0(N_1)$. Мультипликативность $B(L,N)$ как функции N

Для краткости введем ряд обозначений:

$$f(q,N) = 2^{\omega\left(\frac{N}{(q^2D,N)}\right)} \prod_{i=1}^{\omega(N)} \left(p_i^{[\min(2\alpha_i,s_i)/2]} + \Delta(p_i,s_i,\alpha_i)p_i^{[(\min(2\alpha_i,s_i)-1)/2]}\right), \qquad (2.1)$$

где

$$q = q_1 \prod_{i=1}^{\omega(N)} p_i^{\alpha_i}, \quad (q_1,N)=1 \qquad (2.2)$$

и

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

$$M_k = \{q \mid U_k:\ q\nmid U_l,\ l\mid k,\ l\ne k\}, \quad M_{k,p} = \{q\in M_k:\ p\nmid q\}. \qquad (2.3)$$

В этих обозначениях

$$\nu(L,N) = \sum_{q\in M_m} f(q,N)h(q^2D), \qquad (2.4)$$

где m определяется из условия (1.6) и $h(d)$ обозначает число классов бинарных квадратичных форм дискриминанта d. Формула (2.4) отличается от приведенной в [1] отсутствием дополнительного условия $X^2 \equiv q^2 D \pmod{4N}$. Это условие неявным образом удовлетворяется доопределением величины $\Delta(p,s,\alpha)$. Кроме того, нам понадобится, как вспомогательный объект, следующая величина:

$$\nu_p(T_k, N) = \sum_{q \in M_{k,p}} f(q,N) h(q^2 D). \tag{2.5}$$

В дальнейшем мы используем следующее свойство множеств M_k.

Предложение 2.1. *Пусть $q \in M_k$. Тогда $q \mid U_l \Leftrightarrow k \mid l$.*

Д о к а з а т е л ь с т в о. Очевидно, что если $k \mid l$, то $q \mid U_l$. Наоборот, пусть $q \mid U_l$ и $k \nmid l$. Выберем наименьшее l с таким свойством. В работе [1] (§2, доказательство теоремы 2) показано, что множество всех делителей числа U_{kl} разбивается на множества M_i, где i пробегает все делители числа kl. По условию $q \in M_k$, а — в силу минимальности l — $q \in M_l$. Тогда необходимо $k = l$, но это невозможно, так как $k \nmid l$. ∎

Вкратце содержание этого раздела состоит в следующем. Прежде всего получаем разбиение множества M_m в виде объединения множеств $p^i M_k$ и $p^i M_{k,p}$, где $k \mid m$. На втором шаге, используя это разбиение, получаем выражение для $\nu(L,N)$ в виде линейной комбинации $\nu(T_k, N_1)$ и $\nu_p(T_{k'}, N_1)$, где k и k' пробегают некоторые делители m. На третьем шаге вновь используем разбиение M_m и получаем рекуррентные соотношения, в которые входят линейным образом $\nu(T_k, N_1)$ и $\nu_p(T_{k'}, N_1)$. Из этих соотношений получаем $\nu_p(T_{k'}, N_1)$ в виде линейной комбинации $\nu(T_k, N_1)$. И наконец, подставляя выражения для $\nu_p(T_{k'}, N_1)$ в формулу для $\nu(L,N)$, получаем $\nu(L,N)$ в виде линейной комбинации $\nu(T_k, N_1)$, где $k \mid m$. Параллельно получаем формулу для $B(L,N)$, из которой непосредственно следует мультипликативность $B(L,N)$ по N.

Введем два параметра, характеризующие фундаментальный дискриминант D:

$$\begin{aligned} &m_0 \text{ — наименьшее целое такое, что } p \mid U_{m_0};\\ &\alpha_0 \text{ — кратность, с которой } p \text{ входит в } U_{m_0}. \end{aligned} \tag{2.6}$$

Следует отметить, что — из свойств решений уравнения Пелля — такое m_0 всегда существует. Введение этих параметров позволяет полностью описать структуру показателя степени m фундаментального решения уравнения Пелля.

Предложение 2.2.

1. *Пусть $p \nmid D$, тогда*
   если $p = 2$ и $D \equiv 1 \pmod 8$, то $m_0 = 1$;
   если $p = 2$ и $D \equiv 5 \pmod 8$, то $m_0 = 1, 3$;
   если $m_0 \mid m$, то $m = p^{\alpha - \alpha_0} m_0 m_1$ и $p \nmid m_0 m_1$.
2. *Пусть $p \mid D$, тогда*
   $m_0 = 1, p$;
   если $m_0 \mid m$, то $m = p^{\alpha - \alpha_0} m_0 m_1$ и $p \nmid m_1$.

Д о к а з а т е л ь с т в о. Для $U_{k_1 k_2}$ в силу (1.6) получаем

$$2^{k_2 - 1} U_{k_1 k_2} = \sum_{i \equiv 1 \pmod 2}^{k_2} C_{k_2}^i T_{k_1}^{k_2 - i} U_{k_1}^i D^{(i-1)/2}. \tag{2.7}$$

Рассмотрим первый случай: $p \nmid D$.
Пусть $p = 2$ и $D \equiv 1 \pmod 8$. Тогда, если пара (T_1, U_1) нечетна, то $T_1^2 - DU_1^2 \equiv 0 \pmod 8$, значит, пара (T_1, U_1) необходимо четна и $m_0 = 1$. Пусть $p = 2$, $D \equiv 5 \pmod 8$ и пара (T_1, U_1) нечетна. Согласно (2.7) $U_2 = T_1 U_1$ и $U_3 = U_1(T_1^2 - 1)$, следовательно, $m_0 = 3$. Пусть $p \neq 2$,

и допустим, что $p \mid m_0$, тогда $p \nmid U_{\frac{m_0}{p}}$. Полагая в (2.7) $k_1 = m_0/p$ и $k_2 = p$, получаем, что $p \nmid U^p_{\frac{m_0}{p}} D^{(p-1)/2}$ и $p \mid C^i_p$ при $i < p$, значит, $p \nmid U_{m_0}$, что приводит к противоречию. Осталось показать, что p входит в m с кратностью $\alpha - \alpha_0$. Запишем m в виде $m = p^\beta m_1 m_0$, где $(m_1, p) = 1$. Если $p = 2$, то $2 \mid T_{m_0}$. Покажем, что $\alpha_0 > 1$. Допустим, что $\alpha_0 = 1$, тогда $T_{m_0} = 4k_1$ и $U_{m_0} = 4k_2+2$, и значит, $4k_1^2 - D(2k_2+1)^2 = 1$. Если $D \equiv 1 \pmod 8$, то приходим к уравнению $4k = 2$, если $D \equiv 5 \pmod 8$, то получаем, что $4k = 6$. В обоих случаях уравнение не имеет решения. Значит, $\alpha_0 > 1$, и поэтому $4 \nmid T_{m_0}$. Положим в (2.7) $k_1 = m_0$ и $k_2 = m_1$. Тогда $2^{m_1 - 1 + \alpha_0}$ в точности делит $m_1 T_{m_0}^{m_1-1} U_{m_0} (i = 1)$ и $2^{m_1 - i + i\alpha_0} \mid C^i_{m_1} T^{m_1-i}_{m_0} U^i_{m_0} D^{(i-1)/2}$ при $i > 1$. Так как $\alpha_0 > 1$, то $m_1 - i + i\alpha_0 > m_1 - 1 + \alpha_0$ при $i > 1$, откуда следует, что $U_{m_0 m_1}$ содержит 2 с кратностью α_0. Из равенства $U_{2m_0m_1} = T_{m_0m_1} U_{m_0m_1}$ следует, что 2^{α_0+1} в точности делит $U_{2m_0m_1}$. Повторяя это β раз, получаем, что U_m содержит 2 с кратностью $\alpha_0 + \beta$ и поэтому $\beta = \alpha - \alpha_0$, что и требовалось показать. Если $p \neq 2$, то $p \nmid T_{m_0}$. Тогда, очевидно, p входит в $U_{m_0 m_1}$ с кратностью α_0. Для $U_{pm_0m_1}$ в (2.7) положим $k_2 = p$, тогда p в правой части (2.7) входит в слагаемое при $i = 1$ с кратностью $\alpha_0 + 1$, а при $i > 1$ — с кратностью не менее $i\alpha_0$, следовательно, p входит в $U_{pm_0m_1}$ с кратностью $\alpha_0 + 1$. Повторяя β раз возведение в степень p, получаем, что p входит в $U_{p^\beta m_0 m_1}$ с кратностью $\alpha_0 + \beta$. Рассмотрим второй случай: $p \mid D$.

Покажем, что m_0 равно 1 или p. Если $p = 2$ и $2 \nmid U_1$, то $2 \mid T_1$, и тогда $2 \mid U_2 = T_1 U_1$. Пусть $p \neq 2$, тогда $p \nmid T_k$ для любого k. Пусть $p \nmid U_1$. Из (2.7) и условия $p \mid D$ следует, что $p \nmid U_k$ при $1 < k < p$ и $p \mid U_p$, что и требовалось показать. Доказательство второй части утверждения проводится аналогично случаю $p \nmid D$, и поэтому мы его опускаем. ∎

Теперь докажем утверждение, на котором базируются дальнейшие вычисления.

Предложение 2.3. *Пусть $m_0 \mid m$. Тогда*

если $m_0 \neq p$ или если $m_0 = p$ и $\alpha = \alpha_0$, то M_m представимо в виде разбиения

$$M_m = \left(\bigcup_{i=0}^{\alpha} p^i M_{m,p}\right) \bigcup \left(\bigcup_{i=1}^{\alpha-\alpha_0} p^\alpha M_{\frac{m}{p^i},p}\right) \bigcup_{\substack{k \mid m_0, k>1 \\ (k,m_1)=1}} \left[\left(\bigcup_{i=1}^{\alpha-\alpha_0} p^\alpha M_{\frac{m}{kp^i}}\right) \bigcup \left(\bigcup_{i=1}^{\alpha} p^i M_{\frac{m}{k}}\right)\right]; \qquad (2.8)$$

если же $m_0 = p$ и $\alpha > \alpha_0$, то

$$M_m = \left(\bigcup_{i=0}^{\alpha} p^i M_{m,p}\right) \bigcup \left(\bigcup_{i=1}^{\alpha-\alpha_0} p^\alpha M_{\frac{m}{p^i},p}\right) \bigcup p^\alpha M_{m_1}. \qquad (2.9)$$

Здесь $m = p^{\alpha-\alpha_0} m_0 m_1$, $(m_1, p) = 1$; m и α определены в (1.6) и (1.8) соответственно; m_0 и α_0 определены в (2.6); M_k и $M_{k,p}$ определены в (2.3).

Доказательство. Пусть $q \in M_m$. Запишем q в виде $q = p^\beta q_1$, где $0 \leq \beta \leq \alpha$ и $p \nmid q_1$. Как было отмечено выше, семейство множеств $\{M_l\}_{l \mid m}$ образует разбиение множества делителей U_m, следовательно, $q_1 \in M_{l,p}$. В первую очередь отметим, что $m_1 \mid l$, так как иначе существует $ll_0 \neq m$ такое, что $p^\alpha \mid U_{ll_0}$, и значит, $q \mid U_{ll_0}$. Поэтому можно записать $l = p^{\alpha-\alpha_0-i} m_0' m_1$, где $m_0' \mid m_0$. Покажем, что $(m_0/m_0', m_1) = 1$. Действительно, если $(m_0/m_0', m_1) = r > 1$, то возьмем $l_1 = lp^i(m_0/(m_0' r)) \neq m$. Тогда $p^\alpha \mid U_{l_1}$, и значит, $q \mid U_{l_1}$, что приводит к противоречию. Таким образом, l может принимать лишь одно из следующих значений: m/p^i, m/k, $m/(kp^i)$, где k удовлетворяет условию $k \mid m_0$, $k > 1$, $(k, m_1) = 1$ и $0 \leq i \leq \alpha - \alpha_0$. Рассмотрим последовательно эти возможности и выясним, какие значения при этом может принимать β.

1. $q \in p^\beta M_{\frac{m}{p^i},p}$ и $q \in M_m$. При $i = 0$ очевидно, что $q \in p^\beta M_{m,p} \subset M_m$ при $0 \leq \beta \leq \alpha$. Пусть $i > 0$. Если $\beta < \alpha$, то $q \mid U_{\frac{m}{p}}$, следовательно, $\beta = \alpha$ и $q \in p^\alpha M_{\frac{m}{p^i},p}$. Наоборот, пусть

$q = p^\alpha q_1$ и $q_1 \in M_{\frac{m}{p^i},p}$. В силу предложения 2.2 $p^\alpha \mid U_k$ только при k, кратном $p^{\alpha-\alpha_0}m_0$. В силу предложения 2.1 $q_1 \mid U_k$ только при k, кратном m/p^i. Следовательно, наименьшее k, при котором $p^\alpha q_1$ делит U_k, равно наименьшему общему кратному $p^{\alpha-\alpha_0}m_0$ и m/p^i, то есть $k = m$, что и требовалось показать. Далее при анализе исключим случай,когда $m_0 = p$, который рассмотрим отдельно.

2. $q \in p^\beta M_{\frac{m}{k},p}$ и $q \in M_m$. Тогда $(k,p) = (k,m_1) = 1$, и следовательно, $M_{\frac{m}{k},p} = M_{\frac{m}{k}}$ и $p \nmid U_{\frac{m}{k'}}$ для $k' \mid k$, поэтому $q \in p^\beta M_{\frac{m}{k}}$ при $\beta > 0$. Наоборот, пусть $q \in p^\beta M_{\frac{m}{k}}$, где $k \mid m_0, k > 1$, $(k,m_1) = 1$ и $\beta > 0$. Тогда наименьшее l, при котором q делит U_l, равно наименьшему общему кратному m/k и m_0. Так как k взаимно просто с m_1, то $l = m$.

3. $q \in p^\beta M_{\frac{m}{kp^i},p}, i > 0$ и $q \in M_m$. Поскольку $(k,p) = (k,m_1) = 1$, то $M_{\frac{m}{kp^i},p} = M_{\frac{m}{kp^i}}$. Если $\beta < \alpha$, то $q \mid U_{\frac{m}{p}}$, следовательно $\beta = \alpha$. Наоборот, пусть $q \in p^\alpha M_{\frac{m}{kp^i}}, i > 0$. Тогда наименьшее l, при котором q делит U_l, равно наименьшему общему кратному m/kp^i и $p^{\alpha-\alpha_0}m_0$, которое равно m.

Осталось рассмотреть случай $m_0 = p$ для пунктов 2 и 3. При этом условии k принимает лишь одно значение, равное p, и пункты 2 и 3 редуцируются к пункту 1, за исключением варианта $q \in p^\beta M_{m_1}$. В этом случае при $\alpha = \alpha_0$ $(m = pm_1)$ β принимает значения от 1 до α, а при $\alpha > \alpha_0$ принимает единственное значение, равное β. ∎

Теперь можно получить формулы, выражающие $\nu(L,N)$ в виде линейной комбинации $\nu(T_{\frac{m}{k}}, N_1)$.

Предложение 2.4. *Пусть* $\left(\frac{D}{p}\right) = 1$ *при* $p \neq 2$ *и* $D \equiv 1 \pmod 8$ *при* $p = 2$, *тогда*

$$\nu(L,N) = \delta(p,s,\alpha)\,\nu(L,N_1) + \eta_1(p,s,\alpha) \sum_{\substack{k \mid m, p \mid k \\ (k,m_1)=1}} \frac{1}{k}\,\nu(T_{\frac{m}{k}}, N_1) + (\delta(p,s,\alpha) - 2) \sum_{\substack{k \mid m_0, k>1 \\ (k,m_1)=1}} \frac{1}{k}\,\nu(T_{\frac{m}{k}}, N_1), \tag{2.10}$$

где $\delta(p,s,\alpha)$ *определена в формулировке теоремы 1 и*

$$\eta_1(p,s,\alpha) = \begin{cases} 2(p^\alpha - p^{\alpha-1}), & \text{если } 0 < 2\alpha < s; \\ p^\alpha - p^{\alpha-1}, & \text{если } 2\alpha = s; \\ 0, & \text{если } 2\alpha > s \text{ или } \alpha = 0. \end{cases}$$

Доказательство.

Если $p \nmid Q$, то из (2.4) и (2.1) очевидным образом следует, что $\nu(L,N) = 2\,\nu(L,N_1)$. Пусть $p \mid Q$. Тогда, используя разбиение (2.8) и формулу (2.4), получаем

$$\nu(L,N) = \sum_{i=0}^{\alpha} \sum_{q \in M_{m,p}} f(p^i q, N) h((p^i q)^2 D) + \sum_{i=1}^{\alpha} \sum_{\substack{k \mid m_0, k>1 \\ (k,m_1)=1}} \sum_{q \in M_{\frac{m}{k}}} f(p^i q, N) h((p^i q)^2 D)$$
$$+ \sum_{i=1}^{\alpha-\alpha_0} \left(\sum_{q \in M_{\frac{m}{p^i},p}} f(p^\alpha q, N) h((p^\alpha q)^2 D) + \sum_{\substack{k \mid m_0, k>1 \\ (k,m_1)=1}} \sum_{q \in M_{\frac{m}{kp^i}}} f(p^\alpha q, N) h((p^\alpha q)^2 D) \right). \tag{2.11}$$

Из (2.1), если принять во внимание условие, наложенное на фундаментальный дискриминант D, следует, что для любого q, взаимно простого с p,

$$\frac{f(p^iq,N)}{f(q,N_1)}=\begin{cases}2, & \text{если } i=0;\\ 2(p^i+p^{i-1}), & \text{если } 0<2\,i<s;\\ p^i+2p^{i-1}, & \text{если } 2\,i=s;\\ p^{[s/2]}+p^{[(s-1)/2]}, & \text{если } 2\,i>s.\end{cases} \tag{2.12}$$

Для функции числа классов хорошо известна формула

$$h((q_1q_2)^2D)=\frac{q_1}{k}\prod_{p|q_1}\left(1-j(D,p)\frac{1}{p}\right)h(q_2^2D), \tag{2.13}$$

где $q_1q_2\in M_m, q_2\in M_{\frac{m}{k}}$ и

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

Тогда для $h((p^iq)^2D)$, если $p^iq\in M_m$ и $q\in M_{\frac{m}{k}}$,

$$h((p^iq)^2D)=(p^i-p^{i-1})\frac{1}{k}h(q^2D). \tag{2.14}$$

Подставляя в правую часть (2.11) выражения для $f(p^iq,N)$ и $h((p^iq)^2D)$ из (2.12) и (2.14) соответственно, после суммирования по степеням простого p получаем

$$\begin{aligned}\nu\,(L,N)=&\delta(p,s,\alpha)\,p^{\alpha}\left(\nu_p(L,N_1)+\sum_{\substack{k|m_0,k>1\\(k,m_1)=1}}\frac{1}{k}\nu\,(T_{\frac{m}{k}},N_1)\right)-2\sum_{\substack{k|m_0,k>1\\(k,m_1)=1}}\frac{1}{k}\nu\,(T_{\frac{m}{k}},N_1)\\&+r_1(p,s,\alpha)\sum_{i=1}^{\alpha-\alpha_0}\left(\frac{1}{p^i}\nu_p(T_{\frac{m}{p^i}},N_1)+\sum_{\substack{k|m_0,k>1\\(k,m_1)=1}}\frac{1}{kp^i}\nu\,(T_{\frac{m}{kp^i}},N_1)\right),\end{aligned} \tag{2.15}$$

где

$$r_1(p,s,\alpha)=\begin{cases}2(p^{\alpha}+p^{\alpha-1})(p^{\alpha}-p^{\alpha-1}), & \text{если } 2\alpha<s;\\ (p^{\alpha}+2p^{\alpha-1})(p^{\alpha}-p^{\alpha-1}), & \text{если } 2\alpha=s;\\ p^{[s/2]}+p^{[(s-1)/2]}, & \text{если } 2\alpha>s;\end{cases}$$

Покажем, что для $l=p^{\gamma}m_0m_1$ справедливо

$$\begin{aligned}\nu_p\,(T_l,N_1)=&\frac{1}{p^{\alpha_0+\gamma}}\nu\,(T_l,N_1)-\frac{p^{\alpha_0+\gamma}-1}{p^{\alpha_0+\gamma}}\sum_{\substack{k|m_0,k>1\\(k,m_1)=1}}\frac{1}{k}\nu\,(T_{\frac{l}{k}},N_1)\\&-\frac{p-1}{p^{\alpha_0+\gamma}}\sum_{i=1}^{\gamma}\sum_{\substack{k|m_0\\(k,m_1)=1}}\frac{1}{kp^i}\nu\,(T_{\frac{l}{kp^i}},N_1).\end{aligned} \tag{2.16}$$

Для множества M_l справедливо разбиение (2.8), и значит, $\nu\,(T_l,N_1)$ имеет представление вида (2.11), в котором N и m заменены на N_1 и l соответственно. Тогда, учитывая, что

$f(p^\beta q, N_1) = f(q, N_1)$, и применяя формулу (2.14), после несложных преобразований получаем

$$\nu_p\,(T_l, N_1) = \frac{1}{p^{\alpha_0+\gamma}}\nu(T_l, N_1) - \frac{p^{\alpha_0+\gamma}-1}{p^{\alpha_0+\gamma}} \sum_{\substack{k|m_0, k>1\\(k,m_1)=1}} \frac{1}{k}\nu\,(T_{\frac{l}{k}}, N_1)$$
$$- \frac{p-1}{p}\sum_{i=1}^{\gamma}\left(\frac{1}{p^i}\nu_p\,(T_{\frac{l}{p^i}}, N_1) + \sum_{\substack{k|m_0, k>1\\(k,m_1)=1}} \frac{1}{kp^i}\nu\,(T_{\frac{l}{kp^i}}, N_1)\right). \qquad (2.17)$$

Исходя из этого соотношения, методом индукции по целому $\gamma \geq 0$ докажем (2.16). При $\gamma = 0$ соотношения (2.16) и (2.17) совпадают. Пусть (2.16) верно при $0, 1, \dots, \gamma - 1$. Тогда

$$\nu_p\,(T_{\frac{l}{p^i}}, N_1) = \frac{1}{p^{\alpha_0+\gamma-i}}\nu\,(T_{\frac{l}{p^i}}, N_1) - \frac{p^{\alpha_0+\gamma-i}-1}{p^{\alpha_0+\gamma-i}} \sum_{\substack{k|m_0, k>1\\(k,m_1)=1}} \frac{1}{k}\nu\,(T_{\frac{l}{kp^i}}, N_1)$$
$$- \frac{p-1}{p^{\alpha_0+\gamma-i}}\sum_{j=1}^{\gamma-i}\sum_{\substack{k|m_0\\(k,m_1)=1}} \frac{1}{kp^j}\nu\,(T_{\frac{l}{kp^{i+j}}}, N_1) \qquad (2.18)$$

для $1 \leq i \leq \gamma$. Подставляя в (2.17) $\nu_p\,(T_{\frac{l}{p^i}}, N_1)$ из (2.18) , получаем представление

$$\sum_{i=1}^{\gamma}\left(\frac{1}{p^i}\nu_p\,(T_{\frac{l}{p^i}}, N_1) + \sum_{\substack{k|m_0, k>1\\(k,m_1)=1}} \frac{1}{kp^i}\nu\,(T_{\frac{l}{kp^i}}, N_1)\right) = \sum_{i=1}^{\gamma}\sum_{\substack{k|m_0,\\(k,m_1)=1}} \frac{a(kp^i)}{kp^i}\nu\,(T_{\frac{l}{kp^i}}, N_1).$$

Подсчет коэффициентов $a(kp^i)$ дает

$$a(kp^i) = \frac{1}{p^{\alpha_0+\gamma-i}} - \sum_{j=1}^{i-1}\frac{p-1}{p^{\alpha_0+\gamma-j}} = \frac{1}{p^{\alpha_0+\gamma-1}},$$

откуда и следует (2.16). Теперь, подставляя (2.16) при $l = m/p^i,\ i = 0, ..., \alpha - \alpha_0$ в (2.15), получаем

$$\nu\,(L, N) = \delta(p, s, \alpha)\,\nu\,(L, N_1) + (\delta(p, s, \alpha) - 2)\sum_{\substack{k|m_0, k>1\\(k,m_1)=1}} \frac{1}{k}\nu\,(T_{\frac{m}{k}}, N_1)$$
$$+ \frac{p\,r_1(p, s, \alpha) - (p-1)p^\alpha\delta(p, s, \alpha)}{p^\alpha}\sum_{\substack{k|m, p|k\\(k,m_1)=1}} \frac{1}{k}\nu\,(T_{\frac{m}{k}}, N_1).$$

Дробь в последнем равенстве, что нетрудно проверить, совпадает с $\eta_1(p, s, \alpha)$, это и завершает доказательство. ▪

Следствие 2.1. *Пусть $s = 1$, тогда*

$$\nu\,(L, N) = 2\nu\,(L, N_1).$$

Утверждение непосредственно следует из (2.10). ▪

Предложение 2.5. *Пусть* $\left(\frac{D}{p}\right) = -1$ *при* $p \neq 2$ *и* $D \equiv 5 \pmod 8$ *при* $p = 2$, *тогда*

$$\nu\,(L,N) = \delta(p,s,\alpha) \sum_{\substack{k|m_0\\(k,m_1)=1}} \frac{1}{k}\,\nu\,(T_{\frac{m}{k}}, N_1) + \eta_2(p,s,\alpha) \sum_{\substack{k|m,p|k\\(k,m_1)=1}} \frac{1}{k}\,\nu\,(T_{\frac{m}{k}}, N_1), \tag{2.19}$$

где

$$\eta_2(p,s,\alpha) = \begin{cases} \delta(p,s,\alpha), & \textit{если } 2\alpha \le s;\\ (p^{\left[\frac{s}{2}\right]} + p^{\left[\frac{s-1}{2}\right]}) \dfrac{(p^{\left[\frac{s+1}{2}\right]} + p^{\left[\frac{s}{2}\right]} - 2)(p^{\alpha+1} - p^{\alpha-1})}{(p^{\alpha+1} + p^{\alpha} - 2)(p^{\alpha} + p^{\alpha-1} - 2)}, & \textit{если } 2\alpha > s. \end{cases}$$

Д о к а з а т е л ь с т в о. Если $2\alpha < s$, то в силу (2.4) $\nu\,(L,N) = 0$. Пусть $2\alpha \ge s$. Воспользуемся разбиением (2.8) множества M_m. Тогда получим представление $\nu\,(L,N)$ вида (2.11). Отличие состоит лишь в том, что суммирование по i в первых двух суммах уравнения (2.11) начинается с $[(s+1)/2]$. В силу (2.1) для любого q, взаимно простого с p,

$$\frac{f(p^i q, N)}{f(q, N_1)} = \begin{cases} p^{s/2}, & \text{если } 2\,i = s;\\ p^{[s/2]} + p^{[(s-1)/2]}, & \text{если } 2\,i > s, \end{cases}$$

и для всякого q такого, что $q \in M_{\frac{m}{k}}$ и $p^i q \in M_m$, из (2.13) следует

$$h((p^i q)^2 D) = (p^i + p^{i-1})\frac{1}{k} h(q^2 D).$$

Тогда, подставляя в представление для $\nu\,(L,N)$ вышеприведенные выражения для $f(p^i q, N)$ и $h((p^i q)^2 D)$, получаем

$$\begin{aligned} \nu\,(L,N) =& \delta(p,s,\alpha)\,\frac{p^{\alpha+1} + p^{\alpha} - 2}{p-1} \left(\nu_p(L,N_1) + \sum_{\substack{k|m_0,k>1\\(k,m_1)=1}} \frac{1}{k}\nu\,(T_{\frac{m}{k}}, N_1) \right)\\ &+ r_2(p,s,\alpha) \sum_{i=1}^{\alpha-\alpha_0} \left(\frac{1}{p^i}\nu_p(T_{\frac{m}{p^i}}, N_1) + \sum_{\substack{k|m_0,k>1\\(k,m_1)=1}} \frac{1}{kp^i}\nu\,(T_{\frac{m}{kp^i}}, N_1) \right), \end{aligned} \tag{2.20}$$

где

$$r_2(p,s,\alpha) = \begin{cases} p^{s/2}(p^{\alpha} + p^{\alpha-1}), & \text{если } 2\alpha = s;\\ (p^{[s/2]} + p^{[(s-1)/2]})(p^{\alpha} + p^{\alpha-1}), & \text{если } 2\alpha > s. \end{cases}$$

При $l = p^{\gamma} m_0 m_1$ справедливо равенство

$$\begin{aligned} \nu_p(T_l, N_1) = \nu\,(T_l, N_1) - \frac{p^{\alpha_0+\gamma+1} + p^{\alpha_0+\gamma} - p - 1}{p^{\alpha_0+\gamma+1} + p^{\alpha_0+\gamma} - 2} \sum_{\substack{k|m_0\\(k,m_1)=1}} \frac{1}{k}\nu\,(T_{\frac{l}{k}}, N_1)\\ - \frac{(p-1)^2(p^{\alpha_0+\gamma} + p^{\alpha_0+\gamma-1})}{(p^{\alpha_0+\gamma+1} + p^{\alpha_0+\gamma} - 2)(p^{\alpha_0+\gamma} + p^{\alpha_0+\gamma-1} - 2)} \sum_{i=1}^{\gamma} \sum_{\substack{k|m_0\\(k,m_1)=1}} \frac{1}{kp^i}\nu\,(T_{\frac{l}{kp^i}}, N_1). \end{aligned} \tag{2.21}$$

Справедливость (2.21) устанавливается аналогично выводу равенства (2.16). Теперь, подставляя в (2.20) равенство (2.21) при $l = m/p^i$, $i = 0, \cdots, \alpha - \alpha_0$, получаем

$$\nu\,(L,N) = \delta(p,s,\alpha) \sum_{\substack{k|m_0\\(k,m_1)=1}} \frac{1}{k}\,\nu\,(T_{\frac{m}{k}}, N_1)$$
$$+\frac{(p-1)r_2(p,s,\alpha) - (p^{\alpha+1} - p^{\alpha-1})\delta(p,s,\alpha)}{p^\alpha + p^{\alpha-1} - 2} \sum_{\substack{k|m,p|k\\(k,m_1)=1}} \frac{1}{k}\,\nu\,(T_{\frac{m}{k}}, N_1).$$

Коэффициент перед второй суммой, что нетрудно проверить, равен $\eta_2(p,s,\alpha)$, это и завершает доказательство. ▪

Предложение 2.6. *Пусть $p \mid D$. Тогда*
если $2\alpha < s-1$, то $\nu\,(L,N) = 0$;
если $2\alpha \geq s-1$, то
1. если $\alpha = 0$, то

$$\nu\,(L,N) = \nu\,(L,N_1); \tag{2.22}$$

2. если $m_0 = p,\ \alpha = \alpha_0,\ s = 1$, то

$$\nu\,(L,N) = \delta(p,s,\alpha)\,\nu\,(L,N_1) + \frac{p^\alpha - 1}{p^{\alpha+1} - 1}\,\nu\,(T_{m_1}, N_1); \tag{2.23}$$

3. если $m_0 = p,\ \alpha = \alpha_0,\ s > 1$, то

$$\nu\,(L,N) = \delta(p,s,\alpha)\,\left[\nu\,(L,N_1) + \frac{1}{p}\,\nu\,(T_{m_1}, N_1)\right]; \tag{2.24}$$

4. в остальных случаях

$$\nu\,(L,N) = \delta(p,s,\alpha)\,\nu\,(L,N_1) + \eta_3(p,s,\alpha) \sum_{i=1}^{\beta} \frac{1}{p^i}\nu\,(T_{\frac{m}{p^i}}, N_1), \tag{2.25}$$

где $\delta(p,s,\alpha)$ определена в формулировке теоремы 1, $\beta = \alpha - \alpha_0$ при $m_0 = 1$ и $\beta = \alpha - \alpha_0 + 1$ при $m_0 = p$,

$$\eta_3(p,s,\alpha) = \begin{cases} \delta(p,s,\alpha), & \text{если } 2\alpha = s-1; \\ (p^{[s/2]} + p^{[(s-1)/2]})\dfrac{(p^{[(s+1)/2]} + p^{[s/2]} - 2)(p^{\alpha+1} - p^\alpha)}{2\,(p^{\alpha+1} - 1)(p^\alpha - 1)}, & \text{если } 2\alpha > s-1. \end{cases} \tag{2.26}$$

Д о к а з а т е л ь с т в о. Если $2\alpha < s-1$, то, ввиду (2.4), $\nu\,(L,N) = 0$. Пусть $2\alpha \geq s-1$. Если $\alpha = 0$ и $s = 1$, то $f(q,N) = f(q,N_1)$, и следовательно, (2.22) верно. Если $m_0 = 1$, то третье и четвертое слагаемые в (2.8) отсутствуют, а в первом суммирование начинается с $[s/2]$. Тогда для $m_0 = 1$

$$\nu\,(L,N) = \sum_{i=[s/2]}^{\alpha} \sum_{q\in M_{m,p}} f(p^i q, N)h((p^i q)^2 D) + \sum_{i=1}^{\alpha-\alpha_0} \sum_{q\in M_{\frac{m}{p^i},p}} f(p^\alpha q, N)h((p^\alpha q)^2 D). \tag{2.27}$$

Если $m_0 = p$ и $\alpha = \alpha_0$, то в (2.8) второе и третье слагаемые отсутствуют, тогда

$$\nu(L,N) = \sum_{i=[s/2]}^{\alpha} \sum_{q\in M_{m,p}} f(p^i q, N) h((p^i q)^2 D) + \sum_{i=\max(1,[s/2])}^{\alpha} \sum_{q\in M_{m_1}} f(p^i q, N) h((p^i q)^2 D). \quad (2.28)$$

И, наконец, если $m_0 = p$ и $\alpha > \alpha_0$, то, ввиду (2.9),

$$\nu(L,N) = \sum_{i=[s/2]}^{\alpha} \sum_{q\in M_{m,p}} f(p^i q, N) h((p^i q)^2 D) + \sum_{i=1}^{\alpha-\alpha_0} \sum_{q\in M_{\frac{m}{p^i},p}} f(p^\alpha q, N) h((p^\alpha q)^2 D) +$$

$$\sum_{q\in M_{m_1}} f(p^\alpha q, N) h((p^\alpha q)^2 D). \quad (2.29)$$

Согласно (2.1), для любого q, взаимно простого с p,

$$\frac{f(p^i q, N)}{f(q, N_1)} = \begin{cases} p^{(s-1)/2}, & \text{если } 2\,i = s-1; \\ p^{[s/2]} + p^{[(s-1)/2]}, & \text{если } 2\,i > s-1 \end{cases}$$

и для всякого q такого, что $q \in M_{\frac{m}{k}}$ и $p^i q \in M_m$, из (2.13) следует

$$h((p^i q)^2 D) = \frac{p^i}{k} h(q^2 D).$$

Тогда при $m_0 = 1$, в силу (2.27), получаем

$$\nu(L,N) = \delta(p,s,\alpha)\frac{p^{\alpha+1}-1}{p-1}\nu_p(L,N_1) + r_3(p,s,\alpha)\sum_{i=1}^{\alpha-\alpha_0}\frac{1}{p^i}\nu_p(T_{\frac{m}{p^i}}, N_1), \quad (2.30)$$

где

$$r_3(p,s,\alpha) = \begin{cases} p^{(s-1)/2} p^\alpha, & \text{при } 2\alpha = s-1; \\ (p^{[s/2]} + p^{[(s-1)/2]})p^\alpha, & \text{при } 2\alpha > s-1. \end{cases}$$

При $m_0 = p$ и $\alpha > \alpha_0$, в силу (2.29),

$$\nu(L,N) = \delta(p,s,\alpha)\frac{p^{\alpha+1}-1}{p-1}\nu_p(L,N_1) + r_3(p,s,\alpha)\left(\sum_{i=1}^{\alpha-\alpha_0}\frac{1}{p^i}\nu_p(T_{\frac{m}{p^i}}, N_1) + \frac{\nu(T_{m_1}, N_1)}{p^{\alpha-\alpha_0+1}}\right). \quad (2.31)$$

При $m_0 = p$ и $\alpha = \alpha_0$, в силу (2.28),

$$\nu(L,N) = \begin{cases} \delta(p,s,\alpha)\frac{p^{\alpha+1}-1}{p-1}\nu_p(L,N_1) + 2\frac{p^\alpha-1}{p-1}\nu(T_{m_1}, N_1), & \text{при } s=1; \\ \delta(p,s,\alpha)\frac{p^{\alpha+1}-1}{p-1}\left(\nu_p(L,N_1) + \frac{1}{p}\nu(T_{m_1}, N_1)\right), & \text{при } s>1. \end{cases} \quad (2.32)$$

Используя разбиение (2.9) для $\nu(L,N_1)$ и принимая во внимание, что $f(p^i q, N_1) = f(q, N_1)$, получаем

$$\nu_p(L,N_1) = \frac{p-1}{p^{\alpha+1}-1}\nu(L,N_1) - \frac{p^\alpha-1}{p^{\alpha+1}-1}\nu(T_{m_1}, N_1). \quad (2.33)$$

Теперь, подставляя (2.33) в (2.32) , получаем (2.23) и (2.24).

Вычислим $\nu_p(T_k, N_1)$ для $k = p^\gamma m_0 m_1$. Если $m_0 = p$ и $\gamma = 0$, то для $\nu_p(T_k, N_1)$ справедливо (2.33), где L следует заменить на T_k и m — на k. В противном случае справедливо

$$\nu_p(T_k, N_1) = \frac{p-1}{p^{\alpha_0+\gamma+1}-1}\nu\left(T_k, N_1\right) - \frac{(p-1)^2 p^{\alpha_0+\gamma}}{(p^{\alpha_0+\gamma+1}-1)(p^{\alpha_0+\gamma}-1)}\sum_{i=1}^{\gamma^*}\frac{1}{p^i}\nu\left(T_{\frac{k}{p^i}}, N_1\right), \tag{2.34}$$

где $\gamma^* = \gamma$, если $m_0 = 1$, и $\gamma^* = \gamma + 1$, если $m_0 = p$. Чтобы это показать, используем разбиение (2.9), и учитывая, что $f(p^i q, N_1) = f(q, N_1)$, получаем

$$\nu_p(T_k, N_1) = \frac{p-1}{p^{\alpha_0+\gamma+1}-1}\nu\left(T_k, N_1\right) - \frac{(p-1)p^{\alpha_0+\gamma}}{p^{\alpha_0+\gamma+1}-1}\sum_{i=1}^{\gamma^*}\frac{1}{p^i}\nu_p(T_{\frac{k}{p^i}}, N_1). \tag{2.35}$$

Теперь проведем индукцию по целому $\gamma \geq 0$. При $m_0 = 1$ и $\gamma = 0$, в силу (2.35), формула (2.34) верна. При $m_0 = p$ и $\gamma = 1$ подставляем в (2.35) $\nu_p(T_{\frac{k}{p}}, N_1)$, согласно (2.33), и получаем (2.34). Далее, согласно индуктивному предположению, подставляем в (2.35) $\nu_p(T_{\frac{k}{p^i}}, N_1)$ из (2.34) при $1 \leq i \leq \gamma$ и получаем представление $\nu_p(T_k, N_1)$ в виде линейной комбинации $\nu\left(T_{\frac{k}{p^i}}, N_1\right)/p^i$, $0 \leq i \leq \gamma^*$ с коэффициентами $a(p^i)$. Подсчет коэффициентов при $i > 0$ дает

$$\frac{p^{\alpha_0+\gamma+1}-1}{(p-1)^2 p^{\alpha_0+\gamma}}a(p^i) = \frac{1}{p^{\alpha_0+\gamma-i+1}-1} - \sum_{j=1}^{i-1}\frac{(p-1)p^{\alpha_0+\gamma-j}}{(p^{\alpha_0+\gamma-j+1}-1)(p^{\alpha_0+\gamma-j}-1)} = \frac{1}{p^{\alpha_0+\gamma}-1},$$

что и доказывает (2.34). Теперь подставляем в (2.30) выражения для $\nu_p(T_{\frac{m}{p^i}}, N_1)$ при $0 \leq i \leq \beta$ из (2.34) и (2.33). После несложных преобразований получаем

$$\nu\left(T_m, N\right) = \delta(p, s, \alpha)\,\nu\left(T_m, N_1\right) + \frac{p-1}{p^\alpha - 1}(r(p, s, \alpha) - p^\alpha \delta(p, s, \alpha))\sum_{i=1}^{\beta}\frac{1}{p^i}\nu\left(T_{\frac{m}{p^i}}, N_1\right).$$

Коэффициент перед суммой, в чем нетрудно убедиться, равен $\eta_3(p, s, \alpha)$, это и доказывает (2.25).∎

Д о к а з а т е л ь с т в о Теоремы 1. Достаточно доказать утверждение теоремы для величины

$$b\left(L, N\right) = \sum_{k|m} k\nu\left(T_k, N\right). \tag{2.36}$$

Подставим в правую часть (2.36) выражения для $\nu\left(T_k, N\right)$, согласно (2.4), и выразим $h(q^2 D)$ через $h(D)$, согласно (2.13). Тогда коэффициенты k в сумме (2.36) и множители $1/k$, которые появляются при переходе от $h(q^2 D)$ к $h(D)$, дают 1. Множества делителей M_k, когда k пробегает все делители m, образуют разбиение множества всех делителей Q, поэтому

$$b(L, N) = h(D)\sum_{q|Q} qf(q, N)\prod_{p|q}\left(1 - j(D, p)\frac{1}{p}\right). \tag{2.37}$$

Выделяя в делителях q степени p и используя (2.12), после суммирования по степеням p получаем $b(L, N) = \delta(p, s, \alpha)p^\alpha b_p(L, N_1)$, где величина $b_p(L, N_1)$ отличается от $b(L, N_1)$ только тем, что суммирование в ней ведется только по делителям, не содержащим p. Аналогично для $b(L, N_1)$, выделяя в q степени p и учитывая, что $f(p^i q, N_1) = f(q, N_1)$, после суммирования по степеням p получаем $b(L, N_1) = p^\alpha b_p(L, N_1)$. ∎

Учитывая (2.37), получаем арифметическое выражение для $B(L, N)$

$$B(L, N) = \frac{\log((L + \sqrt{L^2 - 4})/2)}{\sqrt{L^2 - 4}}\frac{h(D)}{m}\sum_{q|Q} qf(q, N)\prod_{p|q}\left(1 - j(D, p)\frac{1}{p}\right). \tag{2.38}$$

3. Оценка сверху $\nu\,(L,N)$ как функции N

В этом разделе получаем оценку

$$\nu\,(L,N) \leq (p^{[s/2]} + p^{[(s-1)/2]} + 2)\nu\,(L,N_1). \tag{3.1}$$

Многократное применение этой оценки дает теорему 3.

В силу предложений 2.4, 2.5, 2.6 можно записать $\nu\,(L,N) = \delta(p,s,\alpha)\nu\,(L,N_1) + R(L,N)$, где $R(L,N)$ есть линейная комбинация $\nu\,(T_{\frac{m}{k}},N_1)$ и k пробегает некоторые делители m. Покажем, что $2\nu\,(L,N_1) \geq R(L,N)$. Для этого, используя разбиения (2.8), (2.9), выразим $\nu\,(L,N_1)$ в виде линейной комбинации $\nu_p(T_{\frac{m}{k}},N_1)$. Центральным моментом в доказательстве служит получение достаточно хорошей оценки снизу отношения $\nu_p(T_l,N_1)/\nu\,(T_{\frac{l}{p}},N_1)$. Применяя эту оценку для $\nu\,(L,N_1)$, получим неравенство $\nu\,(L,N_1) \geq \overline{R}(L,N_1)$, где $\overline{R}(L,N_1)$ есть сумма линейной комбинации тех же $\nu\,(T_{\frac{m}{k}},N_1)$, что входят в представление $R(L,N)$ и некоторой неотрицательной величины. И наконец, сравнивая соответствующие коэффициенты в $R(L,N)$ и $\overline{R}(L,N_1)$, убеждаемся, что $2\overline{R}(L,N_1) \geq R(L,N)$, что и приводит к неравенству (3.1.

Следующее неравенство служит основой для дальнейших оценок.

Предложение 3.1. *Пусть $pm_0 \mid m$, тогда*

$$\nu_p(T_m,N) \geq \sum_{i=1}^{\alpha-\alpha_0}\left[\left(\frac{U_m}{p\,U_{\frac{m}{p}}}-1\right)\frac{\nu_p(T_{\frac{m}{p^i}},N)}{p^i} + \frac{U_m}{p\,U_{\frac{m}{p}}\log_2\left(\frac{U_m}{p\,U_{\frac{m}{p}}}+2\right)}\sum_{\substack{k\mid m_0,k>1\\(k,m_1)=1}}\frac{\nu(T_{\frac{m}{kp^i}},N)}{kp^i}\right]. \tag{3.2}$$

Д о к а з а т е л ь с т в о. В первую очередь докажем включение

$$\bigcup_{i=1}^{\alpha-\alpha_0}\left(\bigcup_{\substack{d\left|\left(U_m/p\,U_{\frac{m}{p}}\right)\right.\\ d>1}} dM_{\frac{m}{p^i},p}\bigcup_{\substack{k\mid m_0,k>1\\(k,m_1)=1}}\frac{U_m}{p\,U_{\frac{m}{p}}}M_{\frac{m}{kp^i}}\right) \subset M_{m,p}. \tag{3.3}$$

Так как $p \mid U_{\frac{m}{p}}$, то из (2.7) при $k_1 = m/p$ и $k_2 = p$ следует

$$\left(\frac{U_m}{p\,U_{\frac{m}{p}}},\ U_{\frac{m}{p}}\right) = 1. \tag{3.4}$$

Пусть $q \in M_{\frac{m}{p^i},p}$ и $k \mid m$, $k \neq m$. Поскольку $q \mid U_k$ только в том случае, когда $\frac{m}{p^i} \mid k$, то $k = \frac{m}{p^j}$ и $0 < j \leq i$. Из (3.4) и сотношения $U_k \mid U_{\frac{m}{p}}$ следует, что $d \nmid U_k$, и значит, $dq \nmid U_k$. Так как $p \mid U_{\frac{m}{p}}$, то в силу (3.4) $p \nmid d$, и значит, $dq \in M_{m,p}$.

Покажем, что $U_m/(p\,U_{\frac{m}{p}}) \in M_{m,p}$. Пусть $k \mid m$, $k \neq m$. Если $k \mid \frac{m}{p}$, то из (3.4) следует, что U_k взаимно просто с $U_m/(p\,U_{\frac{m}{p}})$. Пусть $k \nmid \frac{m}{p}$. Тогда k кратно p и $U_{\frac{k}{p}} \mid U_{\frac{m}{p}}$. Отсюда и из (3.4) заключаем, что $U_{\frac{k}{p}}$ взаимно просто с $U_m/(p\,U_{\frac{m}{p}})$. Значит, чтобы U_k не делилось на $U_m/(p\,U_{\frac{m}{p}})$, достаточно показать, что $U_m/(p\,U_{\frac{m}{p}}) > U_k/U_{\frac{k}{p}}$. Используем очевидную оценку: $T_1^{k-1} < U_k < T_1^k$. Тогда $U_m/(p\,U_{\frac{m}{p}}) > T_1^{(p-1)(m/p-1)}$ и $U_k/U_{\frac{k}{p}} < T_1^{k-k/p+1}$. Значит, требуемое неравенство будет выполнено, если $(p-1)(m-k)-p^2>0$. Это неравенство выполняется во всех случаях, за исключением

1. $p=2$.
2. $m=2p$, $k=p$.

Если $p=2$, то $U_k/U_{k/2}=T_{k/2}$, и значит, $(U_m/U_{m/2})/(U_k/U_{k/2}) \geq T_k/T_{k/2}>2$. Последнее неравенство справедливо, так как $T_1 \geq 3$. Если $m=2p$, $k=p$, $p>2$, то $U_{2p}/(pU_2) > U_p^2/(pU_2)$ и $(U_pU_1)/(pU_2) > T_1^{p-2}/p \geq 1$ при $p>2$. Следовательно, $U_m/(pU_{\frac{m}{p}}) \in M_{m,p}$ и (3.3) доказано.

Поскольку $U_{\frac{m}{kp^i}} \mid U_{\frac{m}{p}}$, то множества в левой части (3.3) попарно различны, и значит, справедливо неравенство

$$\nu_p(T_m,N) \geq \sum_{i=1}^{\alpha-\alpha_0} \sum_{q\in M_{\frac{m}{p^i},p}} \sum_{\substack{d|(U_m/pU_{\frac{m}{p}})\\ d>1}} f(qd,N)h((qd)^2D)$$
$$+\sum_{i=1}^{\alpha-\alpha_0} \sum_{\substack{k|m_0,k>1\\ (k,m_1)=1}} \sum_{q\in M_{\frac{m}{kp^i}}} f\left(\frac{U_m}{pU_{\frac{m}{p}}}q,N\right) h\left(\left(\frac{U_m}{pU_{\frac{m}{p}}}q\right)^2 D\right). \tag{3.5}$$

Так как $(q,d)=1$, то в силу свойств функции f, определенной в (2.1), выполняется неравенство $f(qd,N)\geq f(q,N)$. Кроме того ,для $q\in M_{\frac{m}{p^i}}$

$$h((qd)^2D) \geq \frac{d}{kp^i}\prod_{r|d}\left(1-\frac{1}{r}\right)h(q^2D),$$

где r пробегает все простые делители d. Подставляя правые части последних двух неравенств в (3.5), получаем

$$\nu_p(T_m,N) \geq \sum_{\substack{d|(U_m/pU_{\frac{m}{p}})\\ d>1}} d\prod_{r|d}\left(1-\frac{1}{r}\right)\sum_{i=1}^{\alpha-\alpha_0}\frac{1}{p^i}\nu_p(T_{\frac{m}{p^i}},N)$$
$$+\frac{U_m}{U_{\frac{m}{p}}}\prod_{r|(U_m/pU_{\frac{m}{p}})}\left(1-\frac{1}{r}\right)\sum_{i=1}^{\alpha-\alpha_0}\sum_{\substack{k|m_0,k>1\\ (k,m_1)=1}}\frac{1}{kp^i}\nu\,(T_{\frac{m}{kp^i}},N).$$

Применяя стандартные соотношения

$$\sum_{d|K} d\prod_{r|d}\left(1-\frac{1}{r}\right)=K \quad \text{и} \quad \prod_{r|K}\left(1-\frac{1}{r}\right)\geq \frac{1}{\log_2(K+2)},$$

приходим к неравенству (3.2). ∎

В предыдущем разделе получены формулы, выражающие число классов $\nu(L,N)$ группы $\Gamma_0(N)$ через числа классов группы $\Gamma_0(N_1)$, и эти формулы существенно различаются в зависимости от того, каков фундаментальный дискриминант D. Поэтому и здесь при получении оценки (3.1) необходимо рассмотреть отдельно три возможных случая.

Предложение 3.2. *Пусть* $\left(\frac{D}{p}\right)=1$ *при* $p\neq 2$ *и* $D\equiv 1 \pmod 8$ *при* $p=2$, *тогда справедливо неравенство* (3.1).

Лемма 3.1. *Пусть выполнены условия предложения* 3.2 и $pm_0 \mid m$, тогда

$$\nu_p(T_m,N_1) \geq \frac{1}{p}\nu\,(T_{\frac{m}{p}},N_1).$$

Д о к а з а т е л ь с т в о. Из (2.17) при $\gamma = \alpha - \alpha_0 - 1$ ($m = p^{\alpha-\alpha_0} m_0 m_1$) следует, что $\nu\,(T_{\frac{m}{p}}, N_1)$ есть линейная комбинация величин $\nu_p(T_{\frac{m}{p}}, N_1)/(kp)$ с коэффициентами, не превосходящими p^α. Тогда получаем неравенство

$$\nu\,(T_{\frac{m}{p}}, N_1) \le p^\alpha \sum_{i=1}^{\alpha-\alpha_0} \sum_{\substack{k|m_0 \\ (k,m_1)=1}} \frac{1}{kp^i} \nu_p(T_{\frac{m}{p^i}}, N_1).$$

С другой стороны, для $\nu_p(T_m, N_1)$ справедлива оценка (3.2), поэтому

$$\begin{aligned} p\,\nu_p(T_m, N_1) - \nu\,(T_{\frac{m}{p}}, N_1) \ge & \left(\frac{U_m}{U_{\frac{m}{p}}} - p^\alpha - p \right) \sum_{i=1}^{\alpha-\alpha_0} \frac{1}{p^i} \nu_p(T_{\frac{m}{p^i}}, N_1) \\ & + \left(\frac{U_m}{U_{\frac{m}{p}} \log_2 \left(\frac{U_m}{pU_{\frac{m}{p}}} + 2 \right)} - p^\alpha \right) \sum_{i=1}^{\alpha-\alpha_0} \sum_{\substack{k|m_0, k>1 \\ (k,m_1)=1}} \frac{1}{kp^i} \nu\,(T_{\frac{m}{kp^i}}, N_1). \end{aligned}$$

Покажем, что коэффициенты перед суммами неотрицательны. Поскольку $U_m/U_{m/p} > p\,U_{m/p}^{p-1}$ и $p^{\alpha-1} \mid U_{m/p}$, то $U_m/U_{m/p} > p^{(\alpha-1)(p-1)+1} \ge p^\alpha$. Так как $U_m/U_{m/p}$ кратно p, то $U_m/U_{m/p} \ge p^\alpha + p$, что и требовалось показать. При $p = 2$ по условию $D \equiv 1 \pmod 8$, и значит, $m_0 = 1$. Поэтому при оценке второго коэффициента $p > 2$. Из предыдущих оценок и неравенства $U_m/(p\,U_{m/p}) + 2 < U_m/U_{m/p}$ следует $U_m/(p^\alpha U_{m/p} \log_2(U_m/(p\,U_{m/p}) + 2)) > (U_{m/p})^{p-2}/\log_2(U_m/U_{m/p})$. Используя двустороннюю оценку $T_1^{k-1} < U_k < T_1^k$, получаем

$$\frac{(U_{m/p})^{p-2}}{\log_2(U_m/U_{m/p})} > \frac{T_1^{(p-2)(\overline{m}-1)}}{((p-1)(\overline{m}-1)+p)\log_2 T_1} \equiv f(\overline{m}, p, T_1),$$

где $\overline{m} = m/p$. Поскольку $p \ge 3$, $T_1 \ge 3$ и $\overline{m} \ge 2$, то $f(\overline{m}, p, T_1)$ есть возрастающая функция $\overline{m}$ и p. При $\overline{m} \ge 4$ $f(\overline{m}, p, T_1) \ge f(4, 3, T_1) > 1$. При $\overline{m} = 3$ наименьшее возможное p равно 5 и $f(3, 5, T_1) > 1$. И наконец, $f(2, 5, T_1) > 1$ и $f(2, 3, T_1) = T_1/(5\log_2 T_1)$. Поэтому при $p = 3$ и $m_0 = 2$ требуется более точная оценка. Поскольку $3^{\alpha-1} \mid (U_2/U_1)$ и $U_6/U_2 = (T_1^2-1)(T_1^2-3)$, то

$$\frac{U_6}{3^\alpha U_2 \log_2(U_6/(3U_2)+2)} \ge \frac{(T_1^2-1)(T_1^2-3)}{3T_1 \log_2((T_1^2-1)(T_1^2-3)/3+2)} \ge \frac{16}{3\log_2(18)} > 1,$$

что и завершает доказательство. ▪

Д о к а з а т е л ь с т в о Предложения 3.2. Для $\nu\,(L, N_1)$ из (2.17) при $\gamma = \alpha - \alpha_0$ следует представление

$$\begin{aligned} \nu\,(L, N_1) =& (p^\alpha - 1) \sum_{\substack{k|m_0, k>1 \\ (k,m_1)=1}} \frac{1}{k} \nu\,(T_{\frac{m}{k}}, N_1) + (p^\alpha - p^{\alpha-1}) \sum_{\substack{k|m/m_1, p|k \\ (k,m_1)=1}} \frac{1}{k} \nu\,(T_{\frac{m}{k}}, N_1) \\ & + \left\{ p^\alpha \nu_p(T_m, N_1) - (p^\alpha - p^{\alpha-1}) \sum_{i=1}^{\alpha-\alpha_0} \frac{1}{p^i} (\nu\,(T_{\frac{m}{p^i}}, N_1) - \nu_p(T_{\frac{m}{p^i}}, N_1)) \right\}. \end{aligned} \tag{3.6}$$

Покажем, что выражение в фигурных скобках неотрицательно. Обозначим его для краткости $\Phi(\alpha)$ и проведем индукцию по $\alpha \ge \alpha_0$. Очевидно, что $\Phi(\alpha_0) \ge 0$. Для доказательства шага индукции воспользуемся равенством $\Phi(\alpha+1) = (p^{\alpha+1}\nu_p(T_m, N_1) - p^\alpha \nu\,(T_{\frac{m}{p}}, N_1)) + p^{\alpha-1}(\nu\,(T_{\frac{m}{p}}, N_1) - \nu_p(T_{\frac{m}{p}}, N_1)) + \Phi(\alpha)$. Первое слагаемое в правой части неотрицательно в силу леммы 3.1, второе — в силу определения ν_p и третье — согласно индуктивному предположению, что и доказывает неотрицательность $\Phi(\alpha)$.

С другой стороны, $\nu(L,N)$ имеет представление (2.10). Отсюда получаем $\nu(L,N) = \delta(p,s,\alpha)\nu(L,N_1)+R(L,N)$. Из (2.10) и (3.6), принимая во внимание, что $\Phi(\alpha)$ неотрицательно, следует $2\nu(L,N_1) - R(L,N) \geq 0$, и значит, верна оценка (3.1). В заключение укажем случаи, когда в (3.1) равенство достигается. Возьмем простое $p \equiv 1 \pmod 4$. Тогда пара (p,q), определяемая из представления $p^2-4 = q^2 D$, есть некоторое решение (T_m, U_m) уравнения Пелля с дискриминантом D, причем $(\frac{D}{p}) = 1$. Возьмем решение (T_{2m}, U_{2m}). Тогда $U_{2m} = pq$ и $p \nmid q$, значит, $m_0 = 2m$ и $p \nmid 2m$. Поэтому получаем $\nu(T_{2m}, p^3)/\nu(T_{2m},1) = \delta(p,3,1)+(\delta(p,3,1)-2)\nu(T_m,1)/((p^\alpha-1)\nu(T_m,1)) = 2p+2$, и значит, равенство достигается. ▪

Предложение 3.3. *Пусть* $\left(\frac{D}{p}\right) = -1$ *при* $p \neq 2$ *и* $D \equiv 5 \pmod 8$ *при* $p=2$, *тогда*

$$\nu(L,N) \leq (p^{[s/2]} + p^{[(s-1)/2]})\nu(L,N_1). \tag{3.7}$$

Для доказательства предложения 3.3 нам понадобится следующее вспомогательное утверждение.

Лемма 3.2. *Пусть выполнены условия предложения* 3.3 *и* $p m_0 \mid m$, *тогда*

$$\nu_p(T_m, N_1) \geq \frac{p^{\alpha-1}-p^{\alpha-2}}{p^\alpha+p^{\alpha-1}-2}\nu(T_{\frac{m}{p}}, N_1).$$

Д о к а з а т е л ь с т в о. Из (3.8) при $\gamma = \alpha-\alpha_0-1$ получаем

$$\nu(T_{\frac{m}{p}}, N_1) = \frac{p^\alpha+p^{\alpha-1}-2}{p-1}\nu_p(T_{\frac{m}{p}}, N_1) + (p^{\alpha-1}+p^{\alpha-2}) \sum_{\substack{k\mid \frac{m}{pm_1}, p\mid k \\ (k,m_1)=1}} \frac{1}{k}\nu_p(T_{\frac{m}{p^k}}, N_1)$$
$$+ \frac{p^\alpha+p^{\alpha-1}-p-1}{p-1} \sum_{\substack{k\mid m_0, k>1 \\ (k,m_1)=1}} \frac{1}{k}\nu(T_{\frac{m}{p^k}}, N_1).$$

Принимая во внимание, что коэффициенты перед суммами меньше $(p^\alpha+p^{\alpha-1}-2)/(p-1)$, и применяя неравенство (3.2) к $\nu_p(T_m,N_1)$, получаем

$$p^2\nu_p(T_m,N_1) - q\frac{p^{\alpha+1}-p^\alpha}{p^\alpha+p^{\alpha-1}-2}\nu(T_{\frac{m}{p}}, N_1) \geq \left(\frac{U_m}{U_{\frac{m}{p}}} - p^\alpha - p\right)\sum_{i=1}^{\alpha-\alpha_0} \frac{1}{p^{i-1}}\nu_p(T_{\frac{m}{p^i}}, N_1)$$
$$+ \left(\frac{U_m}{U_{\frac{m}{p}}\log_2(U_m/(pU_{\frac{m}{p}})+2)} - p^\alpha\right)\sum_{i=1}^{\alpha-\alpha_0}\sum_{\substack{k\mid m_0, k>1 \\ (k,m_1)=1}} \frac{1}{kp^{i-1}}\nu(T_{\frac{m}{kp^i}}, N_1).$$

Оценка коэффициентов перед суммами проводилась при доказательстве леммы 3.1, и она, очевидно, остается в силе и в данном случае. Однако при оценке второго коэффициента был исключен случай $p=2$, поскольку при $D \equiv 1 \pmod 8$ m_0 всегда равно 1. В рассматриваемом случае $D \equiv 5 \pmod 8$ и m_0 может принимать два значения: 1 и 3. Поэтому при оценке второго коэффициента необходимо рассмотреть дополнительный случай: $p=2$, $m_0=3$. Тогда можно записать $m = 2^{\alpha-\alpha_0}3m_1$, и поскольку 2^{α_0} делит $U_3/U_1 = T_1^2-1$ и $T_{m/2} > T_1^{m/2-1}$, то

$$\frac{U_m}{2^\alpha U_{m/2}\log_2(U_m/(2U_{m/2})+2)} = \frac{T_{m/2}}{2^\alpha\log_2(T_{m/2}/2+2)} > \frac{T_1^{m/2-3}}{2^{\alpha-\alpha_0}\frac{m}{2}\log_2 T_1}.$$

Правая часть неравенства есть возрастающая функция $\alpha(\alpha > \alpha_0)$ и m_1. Число m_1 нечетно и при $m_1 = 3$, $\alpha = \alpha_0 + 1$ получаем $T_1^6/(18\log_2 T_1) > 1$ $(T_1 \geq 3)$, поэтому далее считаем $m_1 = 1$. Если $m = 12$, то при $T_1 > 3$ выполняется неравенство $T_1^3/(4\log_2(T_1^6/2+2)) \geq 1$. Если $T_1 = 3$, то $D = 5$, $\alpha_0 = 3$, и поэтому $T_6/(2^\alpha \log_2(T_6/2+2)) = (18^2-2)/(2^5\log_2(18^2/2+1)) > 1$. Осталось рассмотреть случай, когда $m = 6$. Принимая во внимание, что $T_3 = T_1(T_1^3 - 3)$, $2^{\alpha-1} \mid (U_3/U_1)$ и $U_3/U_1 = T_1^2 - 1$, получаем неравенство

$$\frac{T_3}{2^\alpha \log_2(T_3/2+2)} \geq \frac{T_1(T_1^2-3)}{2(T_1^2-1)\log_2(T_1(T_1^2-3)/2+2)}.$$

При $T_1 \geq 30$ правая часть неравенства больше 1, поэтому остается рассмотреть лишь конечное число дискриминантов, а именно $D = 5, 21, 77, 13, 165, 221, 285, 357, 437, 69, 29, 93$. Прямая проверка показывает, что $T_3/(2^\alpha \log_2(T_3/2+2)) > 1$ для всех указанных дискриминантов, кроме $D = 5$. Для $D = 5$ вычислим $\nu_2(T_6, N_1)$ и $\nu\,(T_3, N_1)$ непосредственно по формулам (2.4) и (2.5). Получаем $(T_3, U_3) = (18, 2^3)$ и $(T_6, U_6) = (322, 2^4 \cdot 3^2)$. Отсюда следует, что если $3 \mid N_1$, то $\nu\,(T_3, N_1) = 0$ и $\nu_2(T_6, N_1) = \frac{2}{7}\nu\,(T_3, N_1) > \frac{2}{11}\nu\,(T_3, N_1)$ — в противном случае. Таким образом, требуемая оценка доказана. ▪

Д о к а з а т е л ь с т в о Предложения 3.3. Будем считать, что $2\alpha \geq s$, поскольку в противном случае $\nu\,(L, N) = 0$. Запишем (2.19) в виде

$$\nu\,(L, N) = (p^{[s/2]} + p^{[(s-1)/2]})\nu\,(L, N_1) - r(p, s, \alpha)\nu\,(L, N_1) + R(L, N),$$

где

$$r(p, s, \alpha) = \frac{(p^{[s/2]} + p^{[(s-1)/2]})(p^{[(s+1)/2]} + p^{[s/2]} - 2)}{p^{\alpha+1} + p^\alpha - 2}.$$

Покажем, что $\nu\,(L, N_1) \geq R(L, N)/r(p, s, \alpha)$, откуда будет следовать оценка (3.7). Для $\nu\,(T_k, N_1)$ используем разбиение (2.8) и получаем

$$\nu_p(T_k, N_1) = \nu\,(T_k, N_1) - \frac{p^{\alpha_0+\gamma+1} + p^{\alpha_0+\gamma} - p - 1}{p^{\alpha_0+\gamma+1} + p^{\alpha_0+\gamma} - 2} \sum_{\substack{l \mid m_0 \\ (l, m_1) = 1}} \frac{1}{l}\nu\,(T_{\frac{k}{l}}, N_1)$$

$$- \frac{p^{\alpha_0+\gamma+1} - p^{\alpha_0+\gamma-1}}{p^{\alpha_0+\gamma+1} + p^{\alpha_0+\gamma} - 2} \sum_{i=1}^{\gamma} \left(\frac{1}{p^i}\nu_p(T_{\frac{k}{p^i}}, N_1) + \sum_{\substack{l \mid m_0, l > 1 \\ (l, m_1) = 1}} \frac{1}{lp^i}\nu\,(T_{\frac{k}{lp^i}}, N_1) \right). \qquad (3.8)$$

Для $\nu\,(L, N_1)$ воспользуемся формулой (3.8) при $\gamma = \alpha - \alpha_0$. Тогда разность $\nu\,(L, N_1) - R(L, N)/r(p, s, \alpha)$ запишется в виде

$$\left(\frac{p^{\alpha+1} + p^\alpha - p - 1}{p-1} - \frac{\delta(p, s, \alpha)}{r(p, s, \alpha)} \right) \sum_{\substack{k \mid m_0, k > 1 \\ (k, m_1) = 1}} \frac{1}{k}\nu\,(T_{\frac{m}{k}}, N_1)$$

$$+ \left(p^\alpha + p^{\alpha-1} - \frac{\eta_2(p, s, \alpha)}{r(p, s, \alpha)} \right) \sum_{i=1}^{\alpha-\alpha_0} \sum_{\substack{k \mid m_0, k > 1 \\ (k, m_1) = 1}} \frac{1}{kp^i}\nu\,(T_{\frac{m}{kp^i}}, N_1) + \Bigg\{ (p^\alpha + p^{\alpha-1}) \times$$

$$\sum_{i=1}^{\alpha-\alpha_0} \frac{1}{p^i}\nu_p(T_{\frac{m}{p^i}}, N_1) + \frac{p^{\alpha+1} + p^\alpha - 2}{p-1}\nu_p(T_m, N_1) - \frac{\eta_2(p, s, \alpha)}{r(p, s, \alpha)} \sum_{i=1}^{\alpha-\alpha_0} \frac{1}{p^i}\nu\,(T_{\frac{m}{p^i}}, N_1) \Bigg\}. \qquad (3.9)$$

Покажем, что коэффициенты перед суммами и выражение в фигурных скобках неотрицательны. Поскольку

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

то первый коэффициент неотрицателен и равен нулю при $s = 1$.

$$\frac{(p^\alpha + p^{\alpha-1})r(p,s,\alpha)}{\eta_2(p,s,\alpha)} = \begin{cases} \dfrac{p^\alpha + p^{\alpha-1} - 2}{p-1} \geq 1, & \text{если } 2\alpha > s; \\ \dfrac{2(p+1)(p^{s/2}-1)}{p^2-p} > 2, & \text{если } 2\alpha = s, \end{cases}$$

и следовательно, второй коэффициент также неотрицателен и обращается в нуль при $\alpha = s = 1$. Для оценки последнего слагаемого используем неравенство леммы 3.2. Из него следует, что это слагаемое не меньше

$$\left(\frac{p^{\alpha-1}(p^{\alpha+1}+p^\alpha-2)}{p^\alpha+p^{\alpha-1}-2} - \frac{\eta_2(p,s,\alpha)}{r(p,s,\alpha)}\right)\frac{1}{p}\nu\,(T_{\frac{m}{p}}, N_1)$$
$$+\sum_{i=2}^{\alpha-\alpha_0}\left(\frac{p^{\alpha-i}(p^{\alpha+1}-p^{\alpha-1})}{p^{\alpha-i+1}+p^{\alpha-i}-2} - \frac{\eta_2(p,s,\alpha)}{r(p,s,\alpha)}\right)\frac{1}{p^i}\nu\,(T_{\frac{m}{p^i}}, N_1).$$

В полученной сумме наименьшим является коэффициент при $\nu\,(T_{\frac{m}{p}}, N_1)/p$, и для него, учитывая, что $\alpha \geq 2$, получаем оценку

$$\frac{p^{\alpha-1}(p^{\alpha+1}+p^\alpha-2)r(p,s,\alpha)}{(p^\alpha+p^{\alpha-1}-2)\eta_2(p,s,\alpha)} = \begin{cases} \dfrac{p^{\alpha+1}+p^\alpha-2}{p^2-1} > p^{\alpha-1}, & \text{если } 2\alpha > s; \\ \dfrac{2(p^\alpha-1)(p^{\alpha+1}+p^\alpha-2)}{(p^2-p)(p^\alpha+p^{\alpha-1}-2)} > 2p, & \text{если } 2\alpha = s, \end{cases}$$

что и завершает доказательство. ▪

Осталось рассмотреть случай $p \mid D$.

Предложение 3.4. *Пусть $p \mid D$, тогда справедлива оценка* (3.7).

Лемма 3.3. *Пусть выполнены условия предложения* 3.4 *и $p\,m_0 \mid m$, тогда*

$$\nu_p(T_m, N_1) \geq \frac{p^{\alpha-1}-p^{\alpha-2}}{p^\alpha-1}\nu\,(T_{\frac{m}{p}}, N_1).$$

Д о к а з а т е л ь с т в о. Вначале рассмотрим случай $m_0 = 1$. Из (3.2) следует оценка

$$\nu_p(T_m, N_1) \geq \left(\frac{U_m}{p\,U_{\frac{m}{p}}} - 1\right)\sum_{i=1}^{\alpha-\alpha_0}\frac{1}{p^i}\nu_p(T_{\frac{m}{p^i}}, N_1). \tag{3.10}$$

С другой стороны, из (2.35) при $\gamma = \alpha - \alpha_0 - 1$ получаем

$$\nu\,(T_{\frac{m}{p}}, N_1) = \frac{p^\alpha-1}{p-1}\nu_p(T_{\frac{m}{p}}, N_1) + p^\alpha\sum_{i=2}^{\alpha-\alpha_0}\frac{1}{p^i}\nu_p(T_{\frac{m}{p^i}}, N_1). \tag{3.11}$$

Тогда

$$p\,\nu_p(T_m, N_1) - \frac{p^\alpha-p^{\alpha-1}}{p^\alpha-1}\nu\,(T_{\frac{m}{p}}, N_1) \geq \left(\frac{U_m}{U_{\frac{m}{p}}} - p^\alpha - p\right)\sum_{i=1}^{\alpha-\alpha_0}\frac{1}{p^i}\nu_p(T_{\frac{m}{p^i}}, N_1). \tag{3.12}$$

Коэффициент перед суммой в (3.12), как показано в лемме 3.1, неотрицателен, и следовательно, лемма 3.3 верна при $m_0 = 1$. Пусть $m_0 = p$. В этом случае в правых частях (3.10) и (3.11) появляется по одному дополнительному слагаемому, что приводит к появлению в (3.12) следующего слагаемого:

$$\left(\frac{U_m}{U_{\frac{m}{p}}\log_2(\frac{U_m}{p\,U_{\frac{m}{p}}}+2)} - p^\alpha\right)\frac{1}{p^{\alpha-\alpha_0+1}}\nu\,(T_{\frac{m}{p^{\alpha-\alpha_0+1}}}, N_1).$$

В лемме 3.1 показано, что первый сомножитель положителен при $p \neq 2$. Поэтому остается рассмотреть только случай $p = 2,\ m_0 = 2$. Представим m в виде $m = 2^{\alpha-\alpha_0+1}m_1$. Тогда справедливо неравенство

$$\frac{T_{\frac{m}{2}}}{2^\alpha \log_2(T_{\frac{m}{2}}/2+2)} \geq \frac{T_1^{\frac{m}{2}-2}}{2^{\alpha-\alpha_0}\frac{m}{2}\log_2 T_1}. \tag{3.13}$$

Правая часть (3.13), очевидно, есть возрастающая функция m_1 и α. При $m_1 = 3$ и $\alpha = \alpha_0 + 1$ правая часть (3.13) больше 1, поэтому остается рассмотреть случай $m_1 = 1$. Пусть $m = 8$. Для пары $(T_1, U_1) = (8, 1)$, которой соответствует $D = 60$, правая часть (3.13) больше 1, и следовательно, это верно для всех $T_1 > 8$. Для пары $(T_1, U_1) = (4, 1)$, которой соответствует $D = 12$, получаем $\alpha = 4,\ T_4 = 174$, и значит, левая часть (3.13) больше 1. Осталось рассмотреть случай $m = 4$. При $T_1 \geq 16$ правая часть (3.13) больше 1, а при $T_1 = 12$ получаем $\alpha = 3,\ T_2 = 142$, и следовательно, левая часть (3.13) больше 1. Для двух оставшихся дискриминантов $D = 12, 60$ левая часть (3.13) меньше 1, и для них $\nu_2(T_4, N_1)$ и $\nu\,(T_2, N_1)$ вычислим непосредственно по формулам (2.5) и (2.4). Если $D = 60$, то $U_4 = 2^4{\cdot}31,\ U_2 = 2^3$. Тогда если $31 \mid N_1$, то $\nu\,(T_2, N_1) = 0$, поскольку $\left(\frac{D}{31}\right) = -1$. В противном случае получаем $\nu_2(T_4, N_1) = \frac{30}{14}\nu\,(T_2, N_1) > \frac{4}{15}\nu\,(T_2, N_1)$. Если $D = 12$, то $U_4 = 2^3 \cdot 7,\ U_2 = 2^2$. Если $7 \mid N_1$, то также $\nu\,(T_2, N_1) = 0$, иначе $\nu_2(T_4, N_1) = \nu\,(T_2, N_1) > \frac{2}{7}\nu\,(T_2, N_1)$. ∎

Д о к а з а т е л ь с т в о Предложения 3.4. $\nu\,(L, N) = 0$ при $\alpha < [s/2]$, поэтому далее будем считать, что $\alpha \geq [s/2]$. При этом условии $\nu\,(L, N) = (p^{[s/2]} + p^{[(s-1)/2]})\nu\,(L, N_1) - r(p, s, \alpha)\nu\,(L, N_1) + R(L, N)$, где

$$r(p, s, \alpha) = \frac{(p^{[s/2]} + p^{[(s-1)/2]})(p^{[(s+1)/2]} + p^{[s/2]} - 2)}{2(p^{\alpha+1} - 1)}$$

и $R(L, N)$ есть линейная комбинация $\nu\,(T_{\frac{m}{p^i}}, N_1)/p^i$. Покажем, что $\nu\,(L, N_1) \geq R(L, N)/r(p, s, \alpha)$. Поскольку $R(L, N)$ имеет различное аналитическое представление в зависимости от условий, которым удовлетворяют $\alpha,\ s$ и m_0, то необходимо рассмотреть 4 различных случая.

1. $\alpha = 0,\ s = 1$.

Тогда $\nu\,(L, N) = \nu\,(L, N_1)$, и (3.7) очевидным образом выполняется.

2. $m_0 = p,\ \alpha = \alpha_0,\ s = 1$.

В этом случае $R(L, N)$ определяется из (2.23), а $\nu\,(L, N_1)$, согласно (2.33), имеет вид

$$\nu\,(L, N_1) = \frac{p^{\alpha+1} - 1}{p - 1}\nu_p(L, N_1) + \frac{p^\alpha - 1}{p - 1}\nu\,(T_{\frac{m}{p}}, N_1).$$

Отсюда получаем оценку

$$\nu\,(L, N_1) - \frac{R(L, N)}{r(p, s, \alpha)} \geq \left(\frac{p^\alpha - 1}{p - 1} - \frac{p^\alpha - 1}{(p^{\alpha+1} - 1)r(p, s, \alpha)}\right)\nu\,(T_{\frac{m}{p}}, N_1) = 0.$$

3. $m_0 = p,\ \alpha = \alpha_0,\ s > 1$.

В этом случае $R(L, N)$ определяется из (2.24), а $\nu\,(L, N_1)$ имеет тот же вид, что и в предыдущем случае, поэтому

$$\nu\,(L, N_1) - \frac{R(L, N)}{r(p, s, \alpha)} \geq \left(\frac{p^\alpha - 1}{p - 1} - \frac{\delta(p, s, \alpha)}{p\, r(p, s, \alpha)}\right)\nu\,(T_{\frac{m}{p}}, N_1)$$

и

$$\frac{p(p^\alpha - 1)r(p, s, \alpha)}{(p - 1)\delta(p, s, \alpha)} = \frac{(p^\alpha - 1)(p^{[(s+1)/2]} + p^{[s/2]} - 2)}{(p - 1)(2p^\alpha - p^{[(s-1)/2]} - p^{[(s-2)/2]})} \geq 1.$$

4. $m_0 = 1$ или $m_0 = p$ и $\alpha > \alpha_0$.
В этом случае $R(L, N)$ определяется из (2.25), а формула для $\nu\,(L, N_1)$ следует из (2.35) при $\gamma = \alpha - \alpha_0$ и имеет следующий вид:

$$\nu\,(T_m, N_1) = \frac{p^{\alpha+1}-1}{p-1}\nu_p(T_m, N_1) + p^\alpha \sum_{i=1}^{\beta} \frac{1}{p^i}\nu_p(T_{\frac{m}{p^i}}, N_1).$$

Согласно лемме 3.3 получаем

$$\nu_p(T_{\frac{m}{p^i}}, N_1) \geq \frac{p^{\alpha-i}-p^{\alpha-i-1}}{p^{\alpha-i+1}-p}\nu\,(T_{\frac{m}{p^{i+1}}}, N_1)$$

для $i \leq \beta - 1$ при $m_0 = 1$ и для $i \leq \beta - 2$ при $m_0 = p$, однако в этом случае $\nu_p(T_{\frac{m}{p^\beta}}, N_1) = \nu\,(T_{\frac{m}{p^\beta}}, N_1)$. Отсюда следует оценка

$$\nu\,(T_m, N_1) \geq \frac{p^{2\alpha}-p^{\alpha-1}}{p^\alpha-1}\,\frac{1}{p}\nu\,(T_{\frac{m}{p}}, N_1) + \sum_{i=2}^{\beta-1} \frac{p^\alpha(p^{\alpha-i+1}-p^{\alpha-i})}{p^{\alpha-i+1}-1}\,\frac{1}{p^i}\nu\,(T_{\frac{m}{p^i}}, N_1)$$
$$+\begin{cases} p^\alpha\,\dfrac{1}{p^\beta}\nu\,(T_{\frac{m}{p^\beta}}, N_1), & \text{если } m_0 = p;\\ \dfrac{p^\alpha(p^{\alpha-\beta+1}-p^{\alpha-\beta})}{p^{\alpha-\beta+1}-1}\,\dfrac{1}{p^\beta}\nu\,(T_{\frac{m}{p^\beta}}, N_1), & \text{если } m_0 = 1.\end{cases}$$

В правой части неравенства, рассматриваемой как линейная комбинация $\nu\,(T_{\frac{m}{p^i}}, N_1)/p^i$, наименьшим является коэффициент с индексом $i = 2$ (здесь следует учесть, что в нашем случае $\alpha \geq 2$). Тогда получаем оценку

$$\nu\,(L, N_1) - \frac{R(L,N)}{r(p,s,\alpha)} \geq \left(\frac{p^{2\alpha-1}-p^{2\alpha-2}}{p^{\alpha-1}-1} - \frac{\eta_3(p,s,\alpha)}{r(p,s,\alpha)}\right)\sum_{i=1}^{\beta}\frac{1}{p^i}\nu\,(T_{\frac{m}{p^i}}, N_1).$$

Коэффициент перед суммой неотрицателен, поскольку

$$\frac{(p^{2\alpha-1}-p^{2\alpha-2})r(p,s,\alpha)}{(p^{\alpha-1}-1)\eta_3(p,s,\alpha)} = \begin{cases} \dfrac{(p^{\alpha-1}-p^{\alpha-2})(p^\alpha-1)}{(p-1)(p^{\alpha-1}-1)} > p+1, & \text{если } 2\alpha > s-1;\\ \dfrac{p^{\alpha-2}(p^{\alpha+1}+p^\alpha-2)}{p^{\alpha-1}-1} > p^2, & \text{если } 2\alpha = s-1,\end{cases}$$

что в результате и приводит к оценке (3.7) ▪

Из предложений 3.2, 3.3 и 3.4 непосредственно следует теорема 2, а из следствия 2.1 предложения 2.4 и оценки (3.7) получаем теорему 3.

4. Численные эксперименты по оценке остаточного члена в асимптотической формуле функции распределения $B(L, N)$.

В работе [7] для конгруэнц-подгрупп модулярной группы получено степенное понижение остаточного члена в асимптотической формуле (1.4):

$$\Psi(X) = X + \sum_{0<\varkappa_j<1/2} \frac{X^{1/2+\varkappa_j}}{1/2+\varkappa_j} + O_N(X^{7/10+\varepsilon}). \tag{4.1}$$

Тогда в силу (4.1)

$$\sum_{L\le X} B(L,N) = X + \sum_{0<\varkappa_j<1/2} \frac{X^{2\varkappa_j}}{2\varkappa_j} + O_N(X^{2/5+\varepsilon}). \tag{4.2}$$

Следствие 2 теоремы 1 дает равномерную по L оценку отношения $B(L,N)/B(L,1)$, поэтому порядок роста остаточного члена в (4.2) по уровню N оценивается величиной $A(N)$ (см (1.9)), и эта оценка точна. Это доказывает теорему 4. Возникает вопрос: каков истинный порядок роста остаточного члена по X? В работе авторов [1] для числа классов $\nu(L,1)$ получена оценка $\nu(L,1) \ll L\ln L$, однако, по-видимому, точная оценка $\nu(L,1) \ll L$. Тогда для $B(L,1)$ будет справедлива оценка $B(L,1) \ll \ln L$ и, в силу следствия 2 теоремы 1, $B(L,N) \ll A(N)\ln L$. Мы проверяем гипотезу о том, что остаточный член по величине не превосходит первое отброшенное слагаемое, умноженное на некоторую абсолютную константу. Поэтому для проверки этой гипотезы рассчитывается следующая величина:

$$R(X,N) = \frac{\sum_{L\le X} B(L,N) - X}{A(N)\ln X}.$$

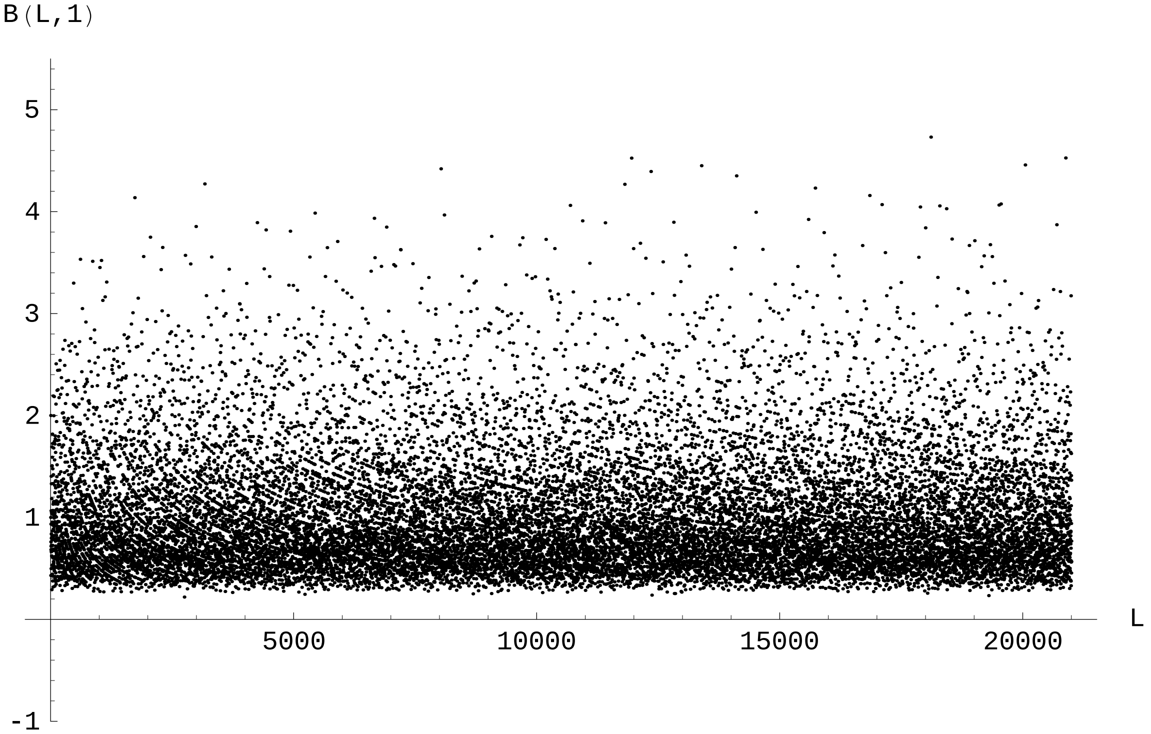
$B(L,1)$ рассчитывается по формуле

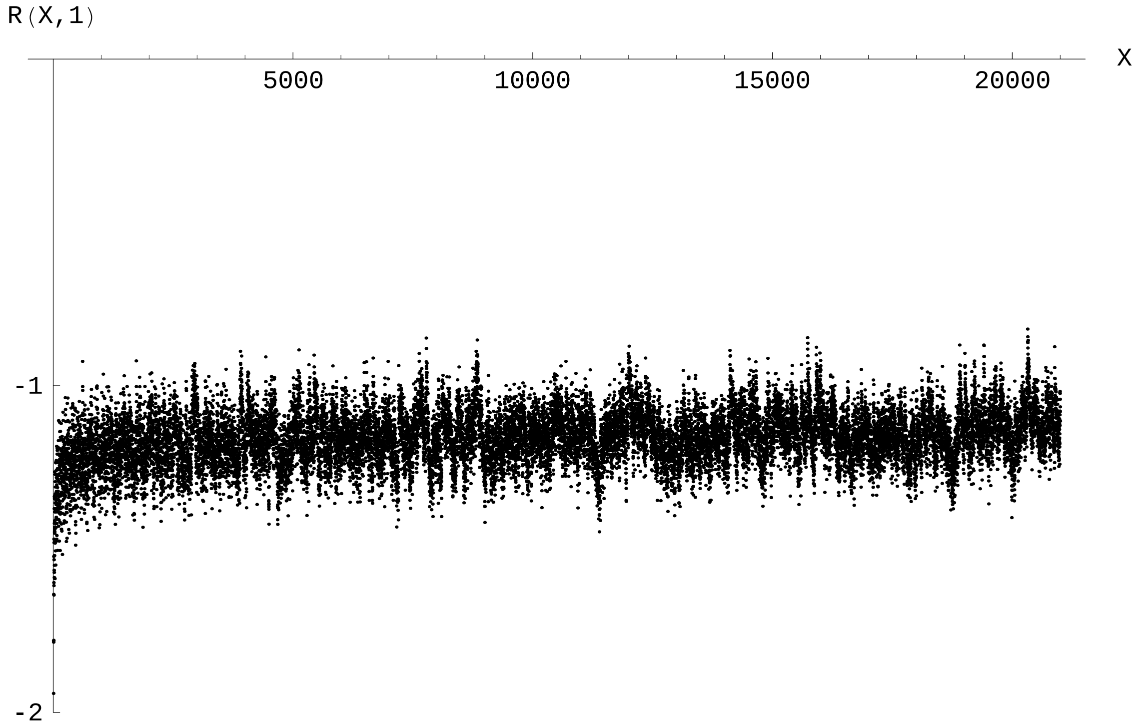
$$B(L,1) = \frac{\log((L+\sqrt{L^2-4})/2)}{\sqrt{L^2-4}} \frac{h(D)}{m} \sum_{q|Q} q \prod_{p|q} \left(1 - j(D,p)\frac{1}{p}\right),$$

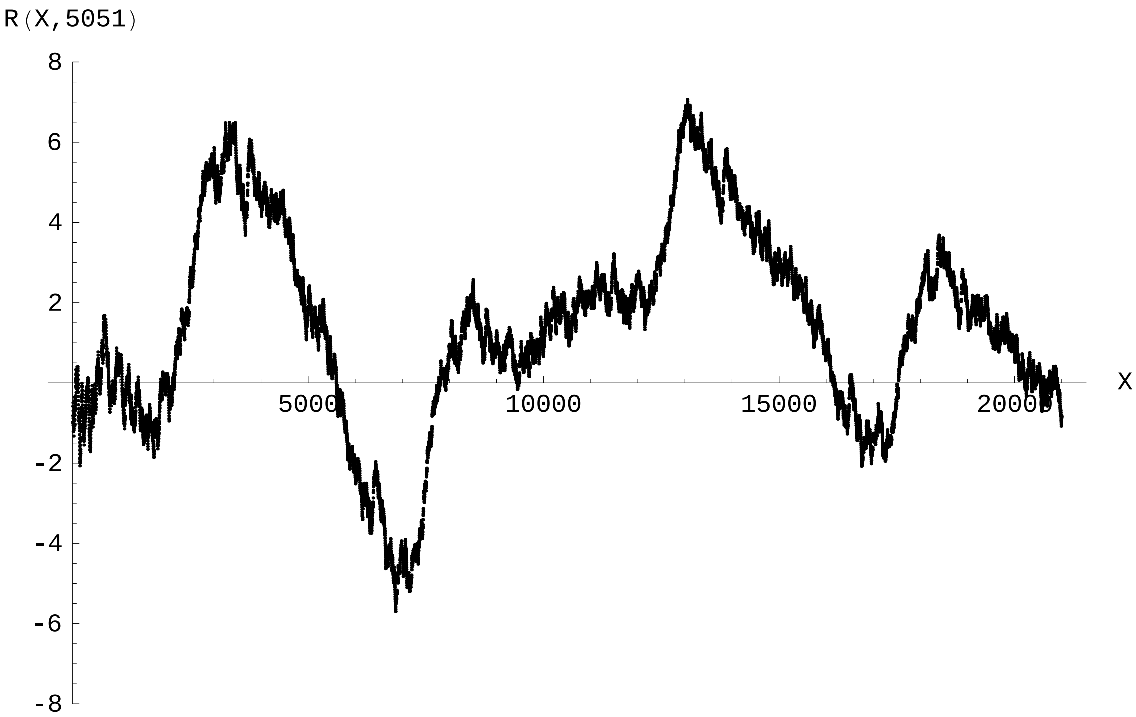
а $B(L,N)$ рассчитывается по формуле

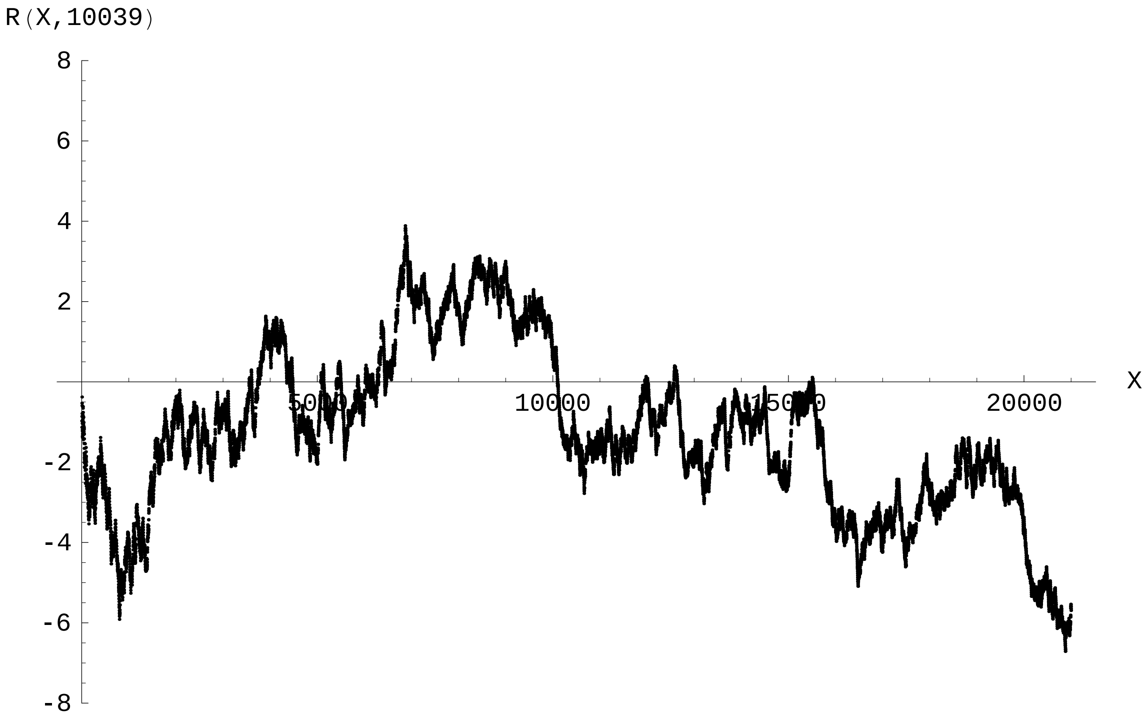
$$B(L,N) = \prod_{p_i|N} \delta(p_i,s_i,\alpha_i) B(L,1).$$

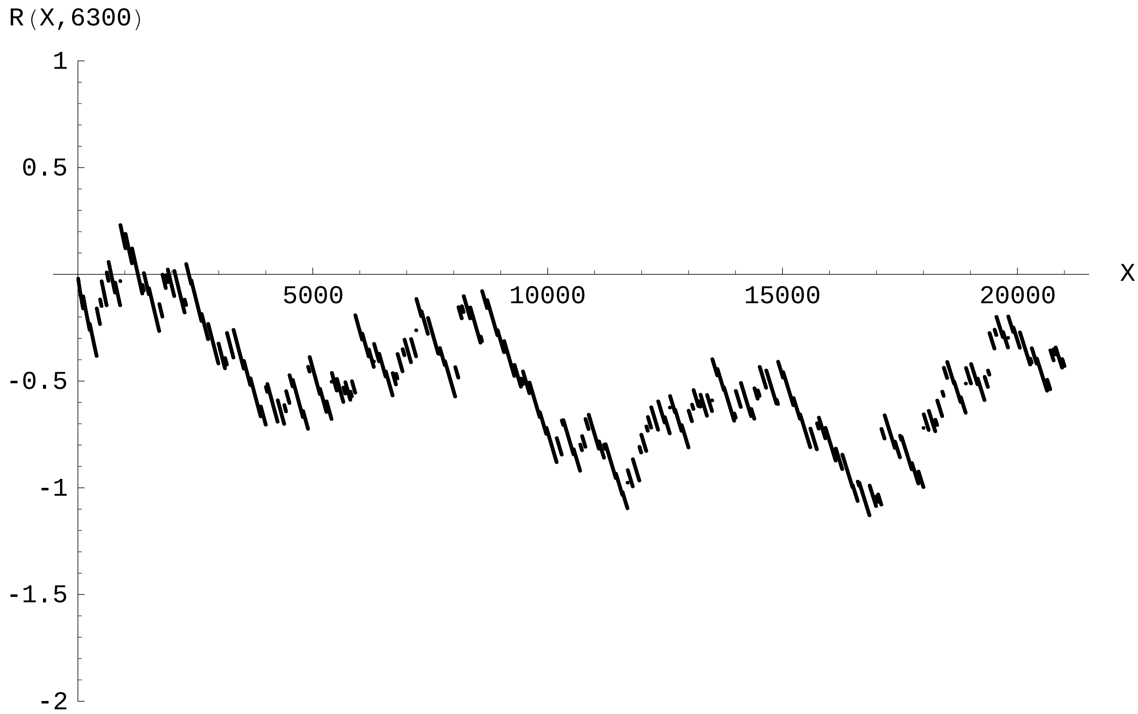
Результаты расчетов приведены в графической форме. Расчеты проведены для $L \le 21000$. На первом рисунке изображено поле значений $B(L,1)$, на последующих — графики функций $R(X,N)$ для значений $N = 1$, 5051, 10039, $6300 = 2^2 3^2 5^2 7$. Результаты вычислений согласуются с проверяемой гипотезой.




R(X,1)
X
5000
10000
15000
20000
-1
-2


R(X,5051)
8
6
4
2
-2
-4
-6
-8
X
5000
10000
15000
20000


R(X,10039)
8
6
4
2
-2
-4
-6
-8
5000
10000
15000
20000
X


R(X,6300)
1
0.5
-0.5
-1
-1.5
-2
5000
10000
15000
20000
X

Список литературы

1. *Головчанский В.В., Смотров М.Н.* Явная формула числа классов примитивных гиперболических элементов группы $\Gamma_0(N)$ // Матем. сб. Т. 199, № 7 (2008), 63–84.

2. *Кузнецов Н.В.* Распределение норм примитивных гиперболических классов модулярной группы и асимптотические формулы для собственных значений оператора Лапласа – Бельтрами на фундаментальной области модулярной группы // ДАН Т. 242, № 1 (1978), 40–43.

3. *Peter M.* The correlation between multiplicities of closed geodesics on the modular surface // Comm.Math.Phys. 225 (2002), 171–189.

4. *Lukianov V.* A central limit theorem for congruence subgroups of the modular group //Ph.D.Thesis. Tel Aviv Univ. 2005.

5. *Arakawa T., Koyama S., Nakasuji M.* Arithmetic foms of Selberg zeta functioms with applications to prime geodesic theorem // Proc. Japan Acad. 78, Ser.A (2002), 120–125.

6. *Hashimoto Y.* Arithmetic expressions of Selberg's zeta functions for congruence subgroups // J. Number Theory 122 (2007), 324–335.

7. *Luo W., Rudnick Z., Sarnak P.* On Selberg's eigenvalue conjecture // Geom. Funct. Anal. 1995. V.5. № 2. P. 387–401.

Представлено в Дальневосточный математический журнал 25 мая 2009 г.

Golovchanskii V.V., Smotrov M.N. Multiplicative characteristics of function for the number of classes of primitive hyperbolic elements in the group $\Gamma_0(N)$ by level N. Far Eastern Mathematical Journal. 2009. V. 9. № 1–2. P. 48–73.

ABSTRACT

An arithmetical forms of Selberg's trace formula and Selberg's zeta-function for the congruence subgroup $\Gamma_0(N)$, explicit expression for the number of classes of primitive hyperbolic elements in the congruence subgroup level N in terms of the number of classes of primitive elements in the congruence subgroup level $N_1 = N/P^i, (N, N_1) = 1$ and sharp upper bound of the number classes by level N are obtained.

Key words: *congruence subgroup of modular group, classes of primitive hyperbolic elements, Pell's equation, Selberg's trace formula.*