12-1994

ХАБАРОВСКОЕ ОТДЕЛЕНИЕ
ИНСТИТУТА ПРИКЛАДНОЙ МАТЕМАТИКИ
ДАЛЬНЕВОСТОЧНОГО ОТДЕЛЕНИЯ
РОССИЙСКОЙ АКАДЕМИИ НАУК

P R E • P R I N T

В. В. Головчанский, М. Н. Смотров

ТОЧНАЯ ОЦЕНКА СВЕРХУ ОТНОШЕНИЯ ЧИСЛА КЛАССОВ ГРУППЫ $\Gamma_0(N)$ К ЧИСЛУ КЛАССОВ МОДУЛЯРНОЙ ГРУППЫ

Khabarovsk

The Institute for Applied Mathematics,
The Far East Branch of
the Russian Academy of Sciences,
Khabarovsk 680 000

Российская Академия наук
Дальневосточное отделение
Институт прикладной математики
Хабаровское отделение

В. В. ГОЛОВЧАНСКИЙ, М. Н. СМОТРОВ

Точная оценка сверху отношения числа классов группы $\Gamma_0(N)$ к числу классов модулярной группы

Препринт

Хабаровск
1994

УДК 511.33

В. В. Головчанский, М. Н. Смотров. Точная оценка сверху отношения числа классов группы $\Gamma_0(N)$ к числу классов модулярной группы. Препринт/ Институт прикладной математики, Дальневосточное отделение, Российская Академия наук. Владивосток; Хабаровск; Дальнаука, 1994, 33 с.

Установлена точная оценка сверху отношения числа классов примитивных гиперболических элементов группы $\Gamma_0(N)$ к числу классов модулярной группы. Вывод этой оценки основан на явных формулах, выражающих число классов группы $\Gamma_0(N)$ через число классов группы $\Gamma_0(N_1)$, где $N_1 \mid N$. Как следствие получена точная оценка роста по N остаточного члена в асимптотической формуле функции распределения числа классов группы $\Gamma_0(N)$. Попутно исследуется арифметическая функция, появляющаяся в формуле следа Сельберга для группы $\Gamma_0(N)$, в частности устанавливается ее мультипликативность по N.

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

Дальневосточное отделение Российской Академии наук

§1. Обозначения и формулировка результатов

Эта работа является непосредственным продолжением работы авторов [1]. На основе формулы из [1] для числа классов примитивных гиперболических элементов конгруэнц-подгруппы $\Gamma_0(N)$ и проективной группы $\overline{\Gamma}_0(N) = \Gamma_0(N)/\pm I$ в этой работе мы получаем оценку числа классов этих групп по N и как следствие устанавливаем порядок роста остаточного члена асимптотической формулы функции распределения $\pi_{\overline{\Gamma}_0(N)}(X)$ как функции N.

Перейдем к более детальному изложению результатов. Прежде всего введем необходимые обозначения.

Пусть $\nu(L,N)$ обозначает число классов примитивных гиперболических элементов группы $\Gamma_0(N)$ ($\overline{\Gamma}_0(N)$) с положительным следом $L \geq 3$ (соответственно с нормой $((L+\sqrt{L^2-4})/2)^2$).

D – фундаментальный дискриминант неопределенной бинарной квадратичной формы, который однозначно определяется из условия

$$L^2 - 4 = Q^2 D. \tag{1.1}$$

(T_1, U_1) – фундаментальное решение уравнения Пелля $t^2 - Du^2 = 4$.

Пара (T_k, U_k) и натуральное m определяются из условий:

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

Одновременно с $\nu(L,N)$ мы рассматриваем арифметическую функцию $B(L,N)$, которая естественным образом возникает в формуле следа Сельберга. Для конгруэнц-подгруппы $\Gamma_0(N)$ формула следа Сельберга может быть записана в следующем виде:

$$\sum_{j=0}^{\infty} h(\varkappa_j) = \{\text{вклад единичного элемента}\} + \{\text{вклад эллиптических элементов}\}$$

$$+ \{\text{вклад параболических элементов}\} + 2\sum_{L=3}^{\infty} B(L,N) g(2\log((L+\sqrt{L^2-4})/2))$$

где $\varkappa_j$ спектральный параметр равный $\sqrt{\lambda_j - 1/4}$ и

$$g(v) = \frac{1}{2\pi}\int_{-\infty}^{+\infty} e^{-irv} h(r)\,dr$$

$$B(L,N) = \frac{\log((L+\sqrt{L^2-4})/2)}{((L+\sqrt{L^2-4})/2) - ((L+\sqrt{L^2-4})/2)^{-1}} \sum_{k|m} \frac{1}{k} \nu\left(T_{\frac{m}{k}}, N\right). \tag{1.3}$$

$B(L,N)$ получаются в результате суммирования по классам примитивных гиперболических элементов в общей формуле следа. Впервые $B(L,1)$ изучались в

работе Н.В. Кузнецова [5], где эти числа определялись как вычеты специальных рядов Дирихле. Явные формулы для $B(L,1)$ были использованы авторами настоящей работы для вычислений собственных значений оператора Лапласа для модулярной группы (см.[2]).

В §2 получена двусторонняя оценка $\nu(L,1)$ и $B(L,1)$, а именно справедлива

Теорема 1.

$$\frac{L}{\log L} D^{-\varepsilon} \ll \nu(L,1) \ll \frac{L}{\log L} \log D \log^2 \log(Q+1),$$
$$D^{-\varepsilon} \ll B(L,1) \ll \log D \log^2 \log(Q+1)$$

для любого $\varepsilon > 0$.

Оценка снизу была получена Н.В. Кузнецовым в [5]. Здесь мы даем иное доказательство этой оценки.

Далее всюду p обозначает простое число. Кроме того зафиксируем следующие обозначения:

$$\begin{aligned} &s \text{ – кратность с которой } p \text{ входит в разложение } N;\\ &\alpha \text{ – кратность с которой } p \text{ входит в разложение } Q;\\ &N_1 = N/p^s; \quad N = \prod_{i=1}^{\omega(N)} p_i^{s_i}. \end{aligned} \tag{1.4}$$

В §3 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 2.

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

где

$$\delta(p,s,\alpha) = \begin{cases} \delta_1(p,s,\alpha), & \text{если } \left(\frac{D}{p}\right) = 1 \text{ при } p \neq 2 \text{ и } D \equiv 1 \pmod 8 \text{ при } p = 2;\\ \delta_2(p,s,\alpha), & \text{если } \left(\frac{D}{p}\right) = -1 \text{ при } p \neq 2 \text{ и } D \equiv 5 \pmod 8 \text{ при } p = 2;\\ \delta_3(p,s,\alpha), & \text{если } p \mid D. \end{cases}$$

и

$$\delta_1(p,s,\alpha) = \begin{cases} 2p^{\alpha}, & \text{если } 2\alpha < s;\\ p^{[s/2]} + p^{[(s-1)/2]}, & \text{если } 2\alpha \geq s; \end{cases}$$

$$\delta_2(p,s,\alpha) = \begin{cases} 0, & \text{если } 2\alpha < s;\\ (p^{[s/2]} + p^{[(s-1)/2]}) \dfrac{p^{\alpha+1} + p^{\alpha} - (p^{[(s+1)/2]} + p^{[s/2]})}{p^{\alpha+1} + p^{\alpha} - 2}, & \text{если } 2\alpha \geq s; \end{cases}$$

$$\delta_3(p,s,\alpha)=\begin{cases}0, & \text{если } 2\alpha<s-1;\\ (p^{[s/2]}+p^{[(s-1)/2]})\dfrac{p^{\alpha+1}-(p^{[(s+1)/2]}+p^{[s/2]})/2}{p^{\alpha+1}-1}, & \text{если } 2\alpha\geq s-1;\end{cases}$$

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* (1.4), *тогда*

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

В §4 на освове результатов §3 получена оценка отношения $\nu(L,N)/\nu(L,1)$ и как следствие этой оценки получено уточнение асимптотической формулы для функции распределения $\pi_{\overline{\Gamma}_0(N)}(X)$. Сформулируем эти результаты:

Пусть N имеет кановическое разложение (1.4) и

$$A(N)=\prod_{i=1}^{\omega(N)}(p_i^{[s_i/2]}+p_i^{[(s_i-1)/2]}+2). \tag{1.5}$$

Тогда в этих обозначениях справедливы

Теорема 3.

$$\frac{\nu(L,N)}{\nu(L,1)}\leq A(N),$$

причем равенство достигается.

Хотя оценка теоремы 3 точна и существует бесконечно много N для которых неравенство обращается в равенство на бесконечном множестве значений L, однако в случае, когда N бесквадратно, имеет место значительно лучшая оценка, а имевно справедлива

Теорема 4. *Пусть* N *бесквадратно, тогда*

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

Теорема 5.

$$\pi_{\overline{\Gamma}_0(N)}(X)=\mathrm{Li}\,(X)+O\left(A(N)X^{\frac{7}{10}}\right).$$

§2. Двусторонняя оценка $\nu(L,1)$ и $B(L,1)$

Отправным пунктом для получения оценок нам будет служить следующая формула из [1]:

$$\nu(L,1) = \sum_{\substack{q \mid U_m, q \nmid U_k \\ k \mid m, k \neq m}} h(q^2 D), \tag{2.1}$$

где U_k и m определяются из условий (1.2) и $h(*)$—число классов неопределенных бинарных квадратичных форм данного дискриминанта.

Предложение 2.1.

$$\nu(L,1) \ll \frac{L}{\log L} \log D \log^2 \log(Q+1),$$

$$B(L,1) \ll \log D \log^2 \log(Q+1).$$

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

$$h(q^2 D) = q \frac{\log((T_1 + \sqrt{D}\,U_1)/2)}{\log((L + \sqrt{D}\,Q)/2)} \prod_{p \mid q} \left(1 - j(D,p)\frac{1}{p}\right) h(D), \tag{2.2}$$

где

$$j(D,p) = \begin{cases} \left(\dfrac{D}{p}\right), & \text{если } p \neq 2; \\ \chi_8(D), & \text{если } p = 2. \end{cases} \tag{2.3}$$

Формула Дирихле для фундаментального дискриминанта нам дает

$$h(D) = \frac{D^{1/2}}{\log((T_1 + \sqrt{D}\,U_1)/2)} L(1, \chi_D), \tag{2.4}$$

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

Тогда из (2.1), (2.2), (2.3) и (2.4) следует

$$\nu(L,1) \leq \frac{\sqrt{L^2-4}\,L(1,\chi_D)}{\log((L+\sqrt{L^2-4})/2)Q} \sum_{q \mid Q} q \prod_{p \mid q} \left(1 + \frac{1}{p}\right). \tag{2.5}$$

Для вещественного примитивного характера χ_D справедлива оценка $L(1,\chi_D) \ll \log D$ (см.[6]). Покажем, что верна оценка:

$$\sum_{q \mid Q} q \prod_{p \mid q} \left(1 + \frac{1}{p}\right) \ll Q \log^2 \log(Q+1). \tag{2.6}$$

Нетрудно заметить, что

$$\sum_{q \mid Q} q \prod_{p \mid q} \left(1 + \frac{1}{p}\right) \leq \sum_{q \mid Q^*} q, \quad \text{где} \quad Q^* = Q \prod_{p \mid Q} \left(1 + \frac{1}{p}\right).$$

Сумма в правой части неравенства оценивается как $Q^* \log\log(Q^*+1)$, а в свою очередь

$$\prod_{p|Q}\left(1+\frac{1}{p}\right) \ll \log\log(Q+1)$$

откуда и следует (2.6).

Теперь из (2.5), оценки для L–ряда и (2.6) следует требуемая оценка для $\nu(L,1)$.

Из (1.2) и оценки для $\nu(L,1)$ получаем:

$$B(L,1) \ll \log D \log^2\log(Q+1) + \frac{\log D \log^2\log(Q+1)}{L} \sum_{k|m,k>1} \frac{T_{\frac{m}{k}}}{k} \frac{\log T_m}{\log T_{\frac{m}{k}}}.$$

В силу того, что

$$\log T_m / \log T_{\frac{m}{k}} \sim k \quad \text{и} \quad \sum_{k|m,k>1} T_{\frac{m}{k}} \ll L^{1/2}$$

второе слагаемое есть величина порядка $L^{-1/2}\log D \log^2\log(Q+1)$ и значит $B(L,1) \ll \log D \log^2\log(Q+1)$, что и требовалось показать. ∎

Предложéние 2.2.

$$\nu(L,1) \gg \frac{L}{\log L} D^{-\varepsilon},$$
$$B(L,1) \gg D^{-\varepsilon}$$

для любого $\varepsilon > 0$

Доказательство. Из (2.1) легко следует неравенство

$$\nu(L,1) \geq \sum_{q|Q} h(q^2 D) - \sum_{p|m} \sum_{q|U_{\frac{m}{p}}} h(q^2 D). \tag{2.7}$$

Принимая во внимание (2.2), (2.3) и (2.4) получаем

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

где $\varphi(*)$—функция Эйлера. По теореме Зигеля (см.[4]) $L(1,\chi_D) \gg D^{-\varepsilon}$ и кроме **того** $\sum_{q|Q}\varphi(q) = Q$. Тогда получаем:

$$\sum_{q|Q} h(q^2 D) \gg \frac{L}{\log L} D^{-\varepsilon}. \tag{2.8}$$

Далее, как и в предложении 2.1 имеем

$$\sum_{q|U_{\frac{m}{p}}} h(q^2D) \ll T_{\frac{m}{p}} \frac{\log D \log^2 \log(U_{\frac{m}{p}}+1)}{\log T_{\frac{m}{p}}}.$$

Из этой оценки следует, что

$$\sum_{p|m} \sum_{q|U_{\frac{m}{p}}} h(q^2D) \ll L^{1/2}. \tag{2.9}$$

Теперь из (2.7), (2.8) и (2.9) следует оценка $\nu(L,1)$. И наконец из (1.3) и оценки $\nu(L,1)$ следует

$$B(L,1) \geq \frac{\log((L+\sqrt{L^2-4})/2)}{((L+\sqrt{L^2-4})/2)-((L+\sqrt{L^2-4})/2)^{-1}} \nu(L,1) \gg D^{-\varepsilon},$$

что и требовалось доказать. ▪

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

Из соображений краткости, введем ряд обозначений:

$$f(q,N) = 2^{\omega\left(\frac{N}{(q^2D,N)}\right)} \prod_{i=1}^{\omega(N)} (p_i^{[\min(2\alpha_i,s_i)/2]} + \Delta(p_i,s_i,\alpha_i) p_i^{[(\min(2\alpha_i,s_i)-1)/2]}), \tag{3.1}$$

где $\omega(N)$ - число простых, входящих в разложение числа N, $[*]$ - целая часть числа и $(*,*)$ - наибольший общий делитель двух чисел,

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

и

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

$$M_k = \{q \mid U_k : \ q \nmid U_l, \ l \mid k, \ l \neq k\},$$
$$M_{k,p} = \{q \in M_k : \ p \nmid q\}. \tag{3.2}$$

Тогда, как показано в [1], верно

$$\nu(L,N) = \sum_{\substack{q \in M_m \\ X^2 \equiv q^2 D \pmod{4N}}} f(q,N) h(q^2 D), \tag{3.3}$$

2.9)

где m определяется из условия (1.2). Кроме того нам понадобится, как вспомогательный объект, следующая величина:

ники

$$\nu_p(T_k,N) = \sum_{\substack{q \in M_{k,p} \\ X^2 \equiv q^2 D \pmod{4N}}} f(q,N) h(q^2 D). \tag{3.4}$$

Вкратце содержание этого параграфа следующее:
Прежде всего мы получаем разбиение множества M_m в виде объединения множеств

$$p^i M_{k,p} \stackrel{\text{def}}{=} \{p^i q : \ q \in M_{k,p}\}, \tag{3.5}$$

где $k \mid m$. На втором шаге, используя это разбиение, мы 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

(3.1)

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 мы получаем формулу для $B(L,N)$, из которой

асть

непосредственно следует мультипликативность $B(L,N)$ по N.

Введем два параметра характеризующие фундаментальный дискриминант D:

$$\begin{aligned} &m_0 \text{ - наименьшее целое такое, что } p \mid U_{m_0}; \\ &\alpha_0 \text{ - кратность с которой } p \text{ входит в } U_{m_0}; \end{aligned} \tag{3.5}$$

Следует отметить, что из свойств решений уравнения Пелля такое m_0 всегда существует (см.[3]). Справедливо следующее

Предложение 3.1. *Если $p \nmid D$ и $m_0 \mid m$, то*

$$m = p^{\alpha-\alpha_0} m_0 m_1 \ \text{и} \ p \nmid m_0 m_1.$$

2;

Если $p \mid D$, то m_0 равно 1 или p и если $m_0 \mid m$, то

$$m = p^{\alpha-\alpha_0} m_0 m_1 \ \text{и} \ p \nmid m_1.$$

= 2;

Доказательство. Первый случай: $p \nmid D$ и $m_0 \mid m$.

Покажем во первых, что $p \nmid m_0$. Если $p = 2$, то непосредственно проверяется, что m_0 равно 1 или 3. Пусть $p \neq 2$. Допустим, что $p \mid m_0$. Запишем $m_0 = pm_0'$. Из (3.5) следует что $p \nmid U_{m_0'}$. Тогда из равенства

$$2^{p-1}U_{m_0} = U_{m_0'}^p D^{(p-1)/2} + \sum_{\substack{i=1 \\ i\equiv 1 \pmod 2}}^{p-2} C_p^i T_{m_0'}^{p-i} U_{m_0'}^i D^{(i-1)/2}$$

следует, что $p \nmid U_{m_0}$ - противоречие.

Осталось показать, что p входит в m/m_0 с кратностью $\alpha - \alpha_0$. Запишем $m/m_0 = p^\beta m_1$ 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 $4 \mid T_{m_0}$. Положим $T_{m_0} = 4k_1$ и $U_{m_0} = 4k_2 + 2$. Тогда имеем $4k_1^2 - D(2k_2+1)^2 = 1$. Если $D \equiv 1 \pmod 8$, то приходим к уравнению $4k = 2$, если $D \equiv 5 \pmod 8$, то к уравнению $4k = 6$. В обеих случаях уравнение не имеет решения. Пришли к противоречию. Значит $\alpha_0 > 1$ и поэтому $4 \nmid T_{m_0}$. Тогда из равенства

$$2^{m_1-1}U_{m_0 m_1} = m_1 T_{m_0}^{m_1-1} U_{m_0} + \sum_{\substack{i=3 \\ i\equiv 1 \pmod 2}}^{m_1} C_{m_1}^i T_{m_0}^{m_1-i} U_{m_0}^i D^{(i-1)/2}$$

следует, что $U_{m_0 m_1}$ содержит 2 с кратностью α_0.

Далее: $U_{2m_0 m_1} = T_{m_0 m_1} U_{m_0 m_1}$, значит $2^{\alpha_0+1} \mid U_{2m_0 m_1}$ и $2^{\alpha_0+1} \nmid U_{2m_0 m_1}$. Отсюда следует, что U_m содержит 2 с кратностью $\alpha_0 + \beta$ и поэтому $\beta = \alpha - \alpha_0$, что и требовалось доказать.

Мы опускаем доказательство при $p \neq 2$, поскольку рассмотрения аналогичны, но еще проще.

Второй случай: $p \mid D$

Покажем, что m_0 равно 1 или p. Если $p = 2$, то непосредственно проверяется, что m_0 равно 1 или 2. Пусть $p \neq 2$. Во первых $p \nmid T_k$ для любого k. Пусть $p \nmid U_1$. Из равенства

$$2^{k-1}U_k = kT_1^k U_1 + \sum_{\substack{i=3 \\ i\equiv 1 \pmod 2}}^{k} C_k^i T_1^{k-i} U_1^i D^{(i-1)/2}$$

следует, что $p \nmid U_k$ при $1 < k < p$ и $p \mid U_p$, что и требуется.

Доказательство второй части утверждения аналогично доказательству в случае $p \nmid D$ и поэтому мы его опускаем. ▪

Предложение 3.2. *Пусть $q \mid U_{k_0}$ и для любого $k \mid k_0$, $k \neq k_0$ верно $q \nmid U_k$. Тогда $q \mid U_k$ в том и только том случае, когда $k_0 \mid k$.*

Доказательство. Очевидно, что если $k_0 \mid k$, то $q \mid U_k$. Далее будем вести доказательство от противного. Пусть существует l такое, что $q \mid U_l$ и $k_0 \nmid l$. Тогда существует наименьшее l_0 с таким свойством. Нетрудно заметить (см.[1]), что множество всех делителей $U_{k_0 l_0}$ разбивается на множества следующего вида

$\overline{M_k} = \{q \mid U_k : q \nmid U_l$ для любого $l \mid k,\ l \neq k\}$, где k пробегает все множество делителей $k_0 l_0$. Тогда по условию $q \in \overline{M}_{k_0}$ и в силу нашего предположения $q \in \overline{M}_{l_0}$. Отсюда следует что $k_0 = l_0$, но это невозможно, так как $k_0 \nmid l_0$. ▪

Теперь мы докажем утверждение на котором базируются дальнейшие вычисления.

Предложение 3.3. *Пусть $m_0 \mid m$. Тогда*
i) *если $p \nmid D$, то имеем разбиение*

$$M_m = \left(\bigcup_{i=1}^{\alpha-\alpha_0} p^\alpha M_{\frac{m}{p^i},p}\right) \bigcup \left(\bigcup_{\substack{k \mid m_0, k>1 \\ (k,m_1)=1}} \left[\left(\bigcup_{i=1}^{\alpha-\alpha_0} p^\alpha M_{\frac{m}{kp^i}}\right) \bigcup \left(\bigcup_{i=1}^{\alpha} p^i M_{\frac{m}{k}}\right)\right]\right) \bigcup \left(\bigcup_{i=0}^{\alpha} p^i M_{m,p}\right) \tag{3.6}$$

ii) *если $p \mid D$ и $\alpha > \alpha_0$ при $m_0 = p$, то*

$$M_m = \left(\bigcup_{i=1}^{\beta} p^\alpha M_{\frac{m}{p^i},p}\right) \bigcup \left(\bigcup_{i=0}^{\alpha} p^i M_{m,p}\right) \quad \text{где } \beta = \begin{cases} \alpha - \alpha_0, & \text{если } m_0 = 1 \\ \alpha - \alpha_0 + 1, & \text{если } m_0 = p \end{cases} \tag{3.7}$$

iii) *если $p \mid D$, $m_0 = p$ и $\alpha = \alpha_0$, то*

$$M_m = \left(\bigcup_{i=1}^{\alpha} p^i M_{\frac{m}{p}}\right) \bigcup \left(\bigcup_{i=0}^{\alpha} p^i M_{m,p}\right) \tag{3.8}$$

Здесь $m = p^{\alpha-\alpha_0} m_0 m_1$, где $(m_1, p) = 1$, m, α определены в (1.2) и (1.4) соответственно, m_0, α_0 определены в (3.4) и M_k, $M_{k,p}$ определены в (3.2).

Доказательство. Прежде всего отметим, что формулы (3.6), (3.7) и (3.8) имеют смысл в силу условия $m_0 \mid m$ и предложения 3.1.

Рассмотрим случай $p \nmid D$. Вначале докажем, что правая часть (3.6) содержится в M_m.

Очевидно, что любое q вида $p^i q_1$, где $0 \leq i \leq \alpha$ и $q_1 \in M_{m,p}$, принадлежит M_m.

Пусть $q = p^\alpha q_1$ и $q_1 \in M_{\frac{m}{p^{i_0}},p}$, где $i_0 > 0$. Очевидно $q \mid U_m$. Покажем что для всякого $k \mid m$, $k \neq m$ верно $q \nmid U_k$.

a) $k \mid \frac{m}{p^{i_0}}$.

Так как $i_0 > 0$, то согласно предложению 3.1 $p^\alpha \nmid U_{\frac{m}{p^{i_0}}}$ и значит $q \nmid U_k$.

b) $k \nmid \frac{m}{p^{i_0}}$.

Если $\frac{m}{p^{i_0}} \nmid k$, то согласно предложению 3.2 $q_1 \nmid U_k$ и значит $q \nmid U_k$.Если $\frac{m}{p^{i_0}} \mid k$, то $k = m/p^{i_0 - i_k}$ и поскольку $k \neq m$ то $i_0 - i_k > 0$. Тогда $p^\alpha \nmid U_k$ и значит $q \nmid U_k$.

Пусть $q = p^{i_0} q_1$, $1 \leq i_0 \leq \alpha$, $q_1 \in M_{\frac{m}{k_0}}$, где

$$k_0 \mid m_0,\ k_0 > 1,\ (k_0, m_1) = 1. \tag{3.9}$$

Покажем, что $q \mid U_m$. Так как $p \nmid D$ то согласно предложению 3.1 $p \nmid m_0 m_1$.Тогда, принимая во внимание (3.9) заключаем, что $m_0 \nmid \frac{m}{k_0}$. Из определения m_0 следует что $p \in M_{m_0}$ Тогда в силу того, что $m_0 \nmid \frac{m}{k_0}$ и предложения 3.2 заключаем что $p \nmid U_{\frac{m}{k_0}}$. Значит $p \nmid q_1$ и тогда $q \mid U_m$. Пусть $k \mid m$, $k \neq m$. Покажем, что $q \nmid U_k$.

a). $k \mid \frac{m}{k_0}$.

Как показано выше $p \nmid U_{\frac{m}{k_0}}$ и значит $p \nmid U_k$. Отсюда следует что $q \nmid U_k$ $(i_0 > 0)$.

b). $k \nmid \frac{m}{k_0}$.

Если $\frac{m}{k_0} \nmid k$, то согласно предложению 3.2 $q_1 \nmid U_k$ и значит $q \nmid U_k$. Если $\frac{m}{k_0} \mid k$ и $k \neq \frac{m}{k_0}$, то $k = \frac{m}{k_1}$, где $k_1 \mid k_0$ и $k_1 > 1$. Тогда k_1 удовлетворяет условию (3.9) и значит $m_0 \nmid \frac{m}{k_1}$. Следовательно $p \nmid U_k$ и значит $q \nmid U_k$ $(i_0 > 0)$, что и требовалось показать.

Пусть $q = p^\alpha q_1$ и $q_1 \in M_{\frac{m}{k_0 p^{i_0}}}$ где $1 \leq i_0 \leq \alpha - \alpha_0$ и k_0 удовлетворяет условию (3.9). Выше было показано, что $p \nmid U_{\frac{m}{k_0}}$, тем более $p \nmid U_{\frac{m}{k_0 p^{i_0}}}$, отсюда следует $q \mid U_m$. Пусть $k \mid m$, $k \neq m$. Покажем, что $q \nmid U_k$.

a). $k \mid \frac{m}{k_0 p^{i_0}}$.

Поскольку $p \nmid U_{\frac{m}{k_0 p^{i_0}}}$, то $p \nmid U_k$ и значит $q \nmid U_k$.

b). $k \nmid \frac{m}{k_0 p^{i_0}}$.

Если $\frac{m}{k_0 p^{i_0}} \nmid k$,то в силу предложения 3.2 $q_1 \nmid U_k$ и значит $q \nmid U_k$. Если $\frac{m}{k_0 p^{i_0}} \mid k$, то $k = m/(k_1 p^{i_1})$ где $k_1 \mid k_0$ и $i_1 \leq i_0$. Если $k_1 = 1$, то $i_1 > 0$ поскольку $k \neq m$. Тогда $p^\alpha \nmid U_k$ и значит $q \nmid U_k$. Если $k_1 > 1$ то k_1 удовлетворяет условию (3.9) и значит $p \nmid U_k$, а тогда $q \nmid U_k$, что и требовалось показать. Таким образом, включение в одну сторону доказано.

Обратно, пусть $q \in M_m$. Тогда для всякого $l \mid m, l \neq m$ имеем $q \nmid U_l$. Запишем q в виде $q = p^\beta q_1$ где $0 \leq \beta \leq \alpha$ и $p \nmid q_1$. Возьмем наименьшее l такое, что $q_1 \mid U_l$. Тогда $q_1 \in M_{l,p}$. Если $l = m$ то $q \in p^\beta M_{m,p}$, поэтому пусть $l < m$. Из условия $l < m$ тогда следует, что $\beta > 0$. Требуется показать,что l принимает одно из следующих значений: $\frac{m}{k}$, $\frac{m}{p^i}$, $\frac{m}{kp^i}$, где k удовлетворяет условию (3.9) и $1 \leq i \leq \alpha - \alpha_0$. Покажем, что $m_1 \mid l$. Пусть $m_1 \nmid l$. Возьмем наименьшее l_0 такое, что $(p^{\alpha - \alpha_0} m_0) \mid (l\, l_0)$. Тогда $l\, l_0 \mid m$, $l\, l_0 \neq m$, $p^\beta \mid U_{l\, l_0}$ и $q_1 \mid U_{l\, l_0}$, значит $q \mid U_{l\, l_0}$- противоречие. Поэтому $l = p^\gamma m_0' m_1$, где $m_0' \mid m_0$ и $\gamma \leq \alpha - \alpha_0$.

Рассмотрим отдельно два возможных случая:

1. $\beta = \alpha$.

a). $m_0 \mid m_0' m_1$.

Тогда необходимо $\gamma < \alpha - \alpha_0$, поскольку в противном случае $p^\alpha \mid U_l$, но это невозможно, так как $q \nmid U_l$ и $q_1 \mid U_l$. Покажем, что $m_0' = m_0$. Допустим, что $m_0' \neq m_0$. Возьмем $l_1 = l\, p^{\alpha - \alpha_0 - \gamma} \neq m$, тогда $p^\alpha \mid U_{l_1}$ и следовательно $q \mid U_{l_1}$- противоречие. Значит $l = \frac{m}{p^i}$, где $i = \alpha - \alpha_0 - \gamma \geq 1$, и тогда $q \in p^\alpha M_{\frac{m}{p^i}, p}$, что и требовалось показать.

b). $m_0 \nmid m_0' m_1$.

Покажем, что $(\frac{m_0}{m_0'}, m_1) = 1$. Действительно, если $(\frac{m_0}{m_0'}, m_1) = r > 1$, то возьмем

$l_1 = p^{\alpha-\alpha_0-\gamma}\frac{m_0}{m_0' r} l \neq m$. Тогда $p^\alpha \mid U_{l_1}$ и значит $q \mid U_{l_1}$- противоречие. Отсюда следует что $l = \frac{m}{p^i k}$, где $k = \frac{m_0}{m_0'} > 1$, $(k, m_1) = 1$ и $i = \alpha - \alpha_0 - \gamma \geq 0$. Поскольку $m_0 \nmid m_0' m_1$, то $M_{l,p} = M_l$. Отсюда заключаем, что $q \in p^\alpha M_{\frac{m}{p^i k}}$, что и требовалось показать.

2. $1 \leq \beta \leq \alpha - 1$.

Допустим, что $\gamma < \alpha - \alpha_0$. Возьмем $l_1 = \frac{m_0}{m_0'} p^{\alpha-\alpha_0-\gamma-1} l \neq m$. Тогда $p^{\alpha-1} \mid U_{l_1}$ и следовательно $p^\beta \mid U_{l_1}$ $(\beta < \alpha)$ и значит $q \mid U_{l_1}$ - противоречие. Следовательно $\gamma = \alpha - \alpha_0$. Из последнего равенства следует, что $m_0 \nmid m_0' m_1$. Тогда, как показано выше, $(\frac{m_0}{m_0'}, m_1) = 1$. Значит $l = \frac{m}{k}$ и k удовлетворяет условию (3.10), следовательно $q \in p^\beta M_{\frac{m}{k}}$, что и требовалось показать.

Таким образом, равенство (3.6) доказано. Осталось показать, что это есть разбиение. Для любых k и k' таких, что $k \mid m$, $k' \mid m$ и $k \neq k'$ верно $M_k \cap M_{k'} = \varnothing$. Поэтому $M_{k,p} \cap M_{k',p} = \varnothing$, а тогда $p^i M_{k,p} \cap p^{i'} M_{k',p} = \varnothing$ и следовательно (3.6) есть разбиение.

Доказательство для случая $p \mid D$ аналогично, но существенно проще, так как m_0 принимает лишь значения 1 и p и поэтому мы его не приводим. ∎

Теперь у нас все готово,чтобы получить формулы, выражающие $\nu(L, N)$ в виде линейной комбинации $\nu(T_{\frac{m}{k}}, N_1)$. Рассматрим последовательно три возможных случая:

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

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

3. $p \mid D$.

Предложение 3.4. *Пусть* $p \neq 2$ *и* $\left(\frac{D}{p}\right) = 1$ *или* $p = 2$ *и* $D \equiv 1 \pmod 8$. *Тогда:*

если $p \nmid Q$, *то*

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

если $p \mid Q$, *то*

$$\begin{aligned} \nu(L, N) = \delta_1(p, s, \alpha)\,\nu(L, N_1) + \eta_1(p, s, \alpha) \sum_{\substack{k \mid \frac{m}{m_1}, p \mid k \\ (k, m_1) = 1}} \frac{1}{k}\,\nu(T_{\frac{m}{k}}, N_1) \\ + (\delta_1(p, s, \alpha) - 2) \sum_{\substack{k \mid m_0, k > 1 \\ (k, m_1) = 1}} \frac{1}{k}\,\nu(T_{\frac{m}{k}}, N_1). \end{aligned} \tag{3.10}$$

где $\delta_1(p, s, \alpha)$ *определена в формулировке теоремы 2 и*

$$\eta_1(p, s, \alpha) = \begin{cases} 2(p^\alpha - p^{\alpha-1}), & \text{если } 2\alpha < s; \\ p^\alpha - p^{\alpha-1}, & \text{если } 2\alpha = s; \\ 0, & \text{если } 2\alpha > s; \end{cases} \tag{3.11}$$

Доказательство. Прежде всего, принимая во внимание условие, наложенное на фундаментальный дискриминант D, из (3.1) следует

$$\frac{f(p^iq,N)}{f(q,N)}=\begin{cases}2, & \text{если } i=0;\\ 2(p^i+p^{i-1}), & \text{если } 0<2i<s;\\ p^i+2p^{i-1}, & \text{если } 2i=s;\\ p^{[s/2]}+p^{[(s-1)/2]}, & \text{если } 2i>s;\end{cases} \tag{3.12}$$

для любого q, взаимно простого с p.

Если $p\nmid Q$ то из (3.3) и (3.12) очевидным образом следует, что $\nu(L,N)=2\nu(L,N_1)$.

Пусть $p\mid Q$ Тогда, используя разбиение (3.6) и формулу (3.3), получаем:

$$\nu(L,N)=\sum_{i=0}^{\alpha}\sum_{q\in M_{m,p}}f(p^iq,N)h((p^iq)^2D)+\sum_{i=1}^{\alpha}\sum_{\substack{k\mid m_0,k>1\\(k,m_1)=1}}\sum_{q\in M_{\frac{m}{k}}}f(p^iq,N)h((p^iq)^2D)+$$

$$\sum_{i=1}^{\alpha-\alpha_0}\sum_{q\in M_{\frac{m}{p^i},p}}f(p^\alpha q,N)h((p^\alpha q)^2D)+\sum_{i=1}^{\alpha-\alpha_0}\sum_{\substack{k\mid m_0,k>1\\(k,m_1)=1}}\sum_{q\in M_{\frac{m}{kp^i}}}f(p^\alpha q,N)h((p^\alpha q)^2D) \tag{3.13}$$

Кроме того для всякого q такого, что $q\in M_{\frac{m}{l}}$ и $p^iq\in M_m$ из (2.2) следует:

$$h((p^iq)^2D)=(p^i-p^{i-1})\frac{1}{l}h(q^2D) \tag{3.14}.$$

Тогда, подставляя в правую часть (3.13) выражения для $f(p^iq,N)$ и $h((p^iq)^2D)$ из (3.12) и (3.14) соответственно, после очевидных, но утомительных преобразований получаем:

$$\nu(L,N)=\delta_1(p,s,\alpha)\,p^\alpha\left(\nu_p(L,N_1)+\sum_{\substack{k\mid m_0,k>1\\(k,m_1)=1}}\frac{1}{k}\nu(T_{\frac{m}{k}},N_1)\right)-2\sum_{\substack{k\mid m_0,k>1\\(k,m_1)=1}}\frac{1}{k}\nu(T_{\frac{m}{k}},N_1)+$$

$$r(p,s,\alpha)\sum_{i=1}^{\alpha-\alpha_0}\left(\frac{1}{p^i}\nu_p(T_{\frac{m}{p^i}},N_1)+\sum_{\substack{k\mid m_0,k>1\\(k,m_1)=1}}\frac{1}{kp^i}\nu(T_{\frac{m}{kp^i}},N_1)\right). \tag{3.15}$$

где

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

Покажем что для $k = p^\gamma m_0 m_1$ справедливо:

$$\nu_p(T_k, N_1) = \frac{1}{p^{\alpha_0+\gamma}}\nu(T_k, N_1) - \frac{p^{\alpha_0+\gamma}-1}{p^{\alpha_0+\gamma}} \sum_{\substack{l|m_0, l>1 \\ (l,m_1)=1}} \frac{1}{l}\nu(T_{\frac{k}{l}}, N_1) - \frac{p-1}{p^{\alpha_0+\gamma}} \sum_{i=1}^{\gamma} \sum_{\substack{l|m_0 \\ (l,m_1)=1}} \frac{1}{lp^i}\nu(T_{\frac{k}{lp^i}}, N_1). \tag{3.16}$$

Для множества M_k справедливо разбиение (3.6) и значит $\nu(T_k, N_1)$ имеет **представление** вида (3.13), в котором N и m заменены на N_1 и k соответственно. **Тогда,** учитывая, что $f(p^\beta q, N_1) = f(q, N_1)$ и применяя формулу (3.14) после **несложных** преобразований получаем:

$$\nu_p(T_k, N_1) = \frac{1}{p^{\alpha_0+\gamma}}\nu(T_k, N_1) - \frac{p^{\alpha_0+\gamma}-1}{p^{\alpha_0+\gamma}} \sum_{\substack{l|m_0, l>1 \\ (l,m_1)=1}} \frac{1}{l}\nu(T_{\frac{k}{l}}, N_1) - \frac{p-1}{p} \sum_{i=1}^{\gamma} \left(\frac{1}{p^i}\nu_p(T_{\frac{k}{p^i}}, N_1) + \sum_{\substack{l|m_0, l>1 \\ (l,m_1)=1}} \frac{1}{lp^i}\nu(T_{\frac{k}{lp^i}}, N_1) \right). \tag{3.17}$$

Исходя из этого соотношения, индукцией по целому $\gamma \geq 0$, докажем (3.16). При **$\gamma = 0$ формула** (3.16) очевидно верна. Пусть она верна при $0, 1, \ldots, \gamma - 1$. Тогда

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

$1 \leq i \leq \gamma$. Отсюда следует представление:

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

Подсчет коэффициентов $a(lp^i)$ дает:

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

откуда и следует (3.16). Теперь подставляя (3.16) при $k = m/p^i$, $i = 0, .., \alpha - \alpha_0$ в (3.15) получаем:

$$\nu(L,N) = \delta_1(p,s,\alpha)\,\nu(L,N_1) + (\delta_1(p,s,\alpha) - 2) \sum_{\substack{k \mid m_0, k>1 \\ (k,m_1)=1}} \frac{1}{k}\nu(T_{\frac{m}{k}}, N_1) +$$

$$\frac{p\,r(p,s,\alpha) - (p-1)p^{\alpha}\delta_1(p,s,\alpha)}{p^{\alpha}} \sum_{\substack{k \mid \frac{m}{m_1}, p \mid k \\ (k,m_1)=1}} \frac{1}{k}\nu(T_{\frac{m}{k}}, N_1).$$

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

Следствие 1. *Пусть выполнены условия предложения 3.4 и $s = 1$. Тогда*

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

Действительно, если $\alpha = 0$ то равенство выполняется в силу предложения 3.4. В противном случае $2\alpha > s$ и значит $\eta_1(p,s,\alpha) = 0$ и $\delta_1(p,s,\alpha) = 2$ и значит равенство справедливо и в этом случае. ∎

Следствие 2. *Пусть выполнены условия предложения 3.4. Тогда*

$$B(L,N) = \delta_1(p,s,\alpha)B(L,N_1).$$

Доказательство. Покажем, что следствие справедливо для

$$b(L,N) = \sum_{k \mid m} \frac{1}{k}\nu(T_{\frac{m}{k}}, N). \tag{3.18}$$

Тогда, очевидно, оно верно и для $B(L,N)$.

Прежде всего заметим, что

$$b(L,N) = \sum_{k \mid \frac{m}{m_0}} \frac{1}{k}\nu(T_{\frac{m}{k}}, N) + 2 \sum_{k \mid m,\, k \nmid \frac{m}{m_0}} \frac{1}{k}\nu(T_{\frac{m}{k}}, N_1).$$

Далее, согласно (3.10) для $k = p^{\gamma_k}k_1$, $0 \le \gamma_k \le \alpha - \alpha_0$, $k_1 \mid m_1$ получаем:

$$\nu(T_{\frac{m}{k}}, N) = \delta_1(p,s,\alpha-\gamma_k)\nu(T_{\frac{m}{k}}, N_1) + \eta_1(p,s,\alpha-\gamma_k) \sum_{\substack{l \mid m_0 p^{\alpha-\alpha_0-\gamma_k} \\ p \mid l,\, (l, \frac{m_1}{k_1})=1}} \frac{1}{l}\nu(T_{\frac{m}{kl}}, N_1) +$$

$$(\delta_1(p,s,\alpha-\gamma_k) - 2) \sum_{\substack{l \mid m_0, l>1 \\ (l, \frac{m_1}{k_1})=1}} \frac{1}{l}\nu(T_{\frac{m}{kl}}, N_1).$$

$\alpha - \alpha_0$

Из последних двух равенств следует представление:

$$b(L,N) = \sum_{k' \mid m} \frac{a(k')}{k'} \nu(T_{\frac{m}{k'}}, N_1).$$

Запишем k' в виде: $k' = p^{\gamma_{k'}} k_1'$, $p \nmid k_1'$. Покажем, что

$$a(k') = \delta_1(p,s,\alpha - \gamma_{k'}) + \sum_{i=0}^{\gamma_{k'}-1} \eta_1(p,s,\alpha - i). \tag{3.19}$$

$p, s, \alpha)$,

Рассмотрим отдельно два случая.

1. $k' \mid \frac{m}{m_0}$

Из вышеприведенных равенств следует:

$$a(k') = \delta_1(p,s,\alpha-\gamma_{k'}) + \sum_{(k,l)\in R_p(k')} \eta_1(p,s,\alpha-\gamma_k) + \sum_{(k,l)\in R(k')} (\delta_1(p,s,\alpha-\gamma_k) - 2)$$

ожения

значит

где

$$R_p(k') = \{(k,l):\ kl = k',\ k \mid \tfrac{m}{m_0},\ (l, \tfrac{m_1}{k_1}) = 1,\ l \mid m_0 p^{\alpha-\alpha_0-\gamma_k},\ p \mid l\}$$

и

$$R(k') = \{(k,l):\ kl = k',\ k \mid \tfrac{m}{m_0},\ (l, \tfrac{m_1}{k_1}) = 1,\ l \mid m_0,\ l > 1\}.$$

Пусть $(k,l) \in R_p(k') \cup R(k')$. Тогда $l = p^{\gamma_{k'}-\gamma_k} \frac{k_1'}{k_1}$ и поскольку $k_1' \mid m_1$, то $(l, \frac{m_1}{k_1}) = \frac{k_1'}{k_1}$ **и значит** $k_1 = k_1'$. Тогда $k = p^{\gamma_k} k_1'$ и $l = p^{\gamma_{k'}-\gamma_k}$. Следовательно, $R(k') = \varnothing$ и $R_p(k') = \{(p^i k_1', p^{\gamma_{k'}-i})\}_{i=0}^{\gamma_{k'}-1}$ откуда и следует (3.19).

(3.18)

2. $k' \mid m$, $k' \nmid \frac{m}{m_0}$.

В этом случае имеем:

$$a(k') = 2 + \sum_{(k,l)\in R_p(k')} \eta_1(p,s,\alpha-\gamma_k) + \sum_{(k,l)\in R(k')} (\delta_1(p,s,\alpha-\gamma_k) - 2).$$

Пусть $(k,l) \in R_p(k') \cup R(k')$. Тогда $(l, \frac{m_1}{k_1}) = (\frac{k_1'}{k_1}, \frac{m_1}{k_1}) = 1$ и значит $k_1 = (k_1', m_1)$. **Поэтому** $k = p^{\gamma_k}(k_1', m_1)$ и $l = p^{\gamma_{k'}-\gamma_k} \frac{k_1'}{(k_1', m_1)}$, причем $\frac{k_1'}{(k_1', m_1)} > 1$ (иначе $k' \mid \frac{m}{m_0}$). **Отсюда** следует, что

$_1)+$

$$R(k') = \{(p^{\gamma_{k'}}(k_1', m_1), \tfrac{k_1'}{(k_1', m_1)})\} \quad \text{и} \quad R_p(k') = \{(p^i(k_1', m_1), p^{\gamma_{k'}-i} \tfrac{k_1'}{(k_1', m_1)})\}_{i=0}^{\gamma_{k'}-1}$$

и следовательно верно (3.19).

И наконец, из определения функций δ_1 и η_1 непосредственно следует, что $\delta_1(p,s,i) + \eta_1(p,s,i+1) = \delta_1(p,s,i+1)$, что вместе с (3.19) дает равенство $a(k') = \delta_1(p,s,\alpha)$. ▪

Предложение 3.5. *Пусть* $p \neq 2$ *и* $\left(\frac{D}{p}\right) = -1$ *или* $p = 2$ *и* $D \equiv 5 \pmod 8$. *Тогда: если* $2\alpha < s$, *то*

$$\nu(L, N) = 0.$$

если $2\alpha \geq s$, *то*

$$\nu(L,N) = \delta_2(p,s,\alpha) \sum_{\substack{k|m_0 \\ (k,m_1)=1}} \frac{1}{k}\nu(T_{\frac{m}{k}}, N_1) + \eta_2(p,s,\alpha) \sum_{\substack{k|\frac{m}{m_1}, p|k \\ (k,m_1)=1}} \frac{1}{k}\nu(T_{\frac{m}{k}}, N_1) \quad (3.20),$$

где $\delta_2(p,s,\alpha)$ *определена в формулировке теоремы 2 и*

$$\eta_2(p,s,\alpha) = \begin{cases} \delta_2(p,s,\alpha), & \text{если } 2\alpha = s; \\ (p^{[\frac{s}{2}]} + p^{[\frac{s-1}{2}]}) \dfrac{(p^{[\frac{s+1}{2}]} + p^{[\frac{s}{2}]} - 2)(p^{\alpha+1} - p^{\alpha-1})}{(p^{\alpha+1} + p^{\alpha} - 2)(p^{\alpha} + p^{\alpha-1} - 2)}, & \text{если } 2\alpha > s; \end{cases} \quad (3.21)$$

Доказательство. Если $2\alpha < s$, то сравнение $X^2 \equiv q^2 D \pmod{4N}$ для $q \mid Q$ не имеет решения и значит в силу (3.3) $\nu(L,N) = 0$.

Пусть $2\alpha \geq s$. Воспользуемся разбиением (3.6) множества M_m. Тогда получим представление $\nu(L,N)$ вида (3.13). Отличие состоит лишь в том, что суммирование по i в первых двух суммах начинается с $[(s+1)/2]$. Далее, в силу (3.1) для любого q взаимно простого с p имеем:

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

и для всякого q такого, что $q \in M_{\frac{m}{l}}$ и $p^i q \in M_m$ из (2.2) следует

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

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

$$\nu(L,N) = \delta_2(p,s,\alpha)\frac{p^{\alpha+1} + p^{\alpha} - 2}{p-1}\left(\nu_p(L, N_1) + \sum_{\substack{k|m_0, k>1 \\ (k,m_1)=1}} \frac{1}{k}\nu(T_{\frac{m}{k}}, N_1)\right) +$$

$$r(p,s,\alpha)\sum_{i=1}^{\alpha-\alpha_0}\left(\frac{1}{p^i}\nu_p(T_{\frac{m}{p^i}}, N_1) + \sum_{\substack{k|m_0, k>1 \\ (k,m_1)=1}} \frac{1}{kp^i}\nu(T_{\frac{m}{kp^i}}, N_1)\right). \quad (3.22)$$

Тогда:

где

$$r(p,s,\alpha)=\begin{cases} p^{s/2}(p^{\alpha}+p^{\alpha-1}), & \text{если } 2\alpha=s;\\ (p^{[s/2]}+p^{[(s-1)/2]})(p^{\alpha}+p^{\alpha-1}), & \text{если } 2\alpha>s;\end{cases} \tag{3.23}$$

Покажем, что для $k=p^{\gamma}m_0m_1$ верно

(3.20),

$$\nu_p(T_k,N_1)=\nu(T_k,N_1)-\frac{p^{\alpha_0+\gamma+1}+p^{\alpha_0+\gamma}-p-1}{p^{\alpha_0+\gamma+1}+p^{\alpha_0+\gamma}-2}\sum_{\substack{l\mid m_0\\(l,m_1)=1}}\frac{1}{l}\nu(T_{\frac{k}{l}},N_1)- \tag{3.24}$$

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

Для $\nu(T_k,N_1)$ используем разбиение (3.6) и получаем

(3.21)

$$\nu_p(T_k,N_1)=\nu(T_k,N_1)-\frac{p^{\alpha_0+\gamma+1}+p^{\alpha_0+\gamma}-p-1}{p^{\alpha_0+\gamma+1}+p^{\alpha_0+\gamma}-2}\sum_{\substack{l\mid m_0\\(l,m_1)=1}}\frac{1}{l}\nu(T_{\frac{k}{l}},N_1)- \tag{3.25}$$

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

$\mid Q$ не

а полу-

то сум-

в силу

Теперь индукцией по целому $\gamma\geq 0$ докажем (3.24). При $\gamma=0$ равенство (3.24) в силу (3.25) верно. Пусть (3.24) верно при $0,1,\ldots,\gamma-1$. Тогда третье слагаемое в (3.25) есть линейная комбинация величин $\nu(T_{\frac{k}{lp^i}},N_1)/(lp^i)$ где $l\mid m_0,(l,m_1)=1$ и $1\leq i\leq\gamma$ с некоторыми коэффициентами $a(lp^i)$. Подсчет коэффициентов нам дает

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

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

ажения

откуда и следует (3.24). Теперь, подставляя (3.24) при $k=m/p^i$, $i=0,\cdots,\alpha-\alpha_0$ в (3.23), получаем:

$$\nu(L,N)=\delta_2(p,s,\alpha)\sum_{\substack{k\mid m_0\\(k,m_1)=1}}\frac{1}{k}\nu(T_{\frac{m}{k}},N_1)+$$

+

$$\left(r(p,s,\alpha)\frac{p-1}{p^{\alpha}+p^{\alpha-1}-2}-\delta_2(p,s,\alpha)\frac{p^{\alpha+1}-p^{\alpha-1}}{p^{\alpha}+p^{\alpha-1}-2}\right)\sum_{\substack{k\mid\frac{m}{m_1},p\mid k\\(k,m_1)=1}}\frac{1}{k}\nu(T_{\frac{m}{k}},N_1).$$

(3.22)

Легко убедиться, что коэффициент перед второй суммой равен $\eta_2(p,s,\alpha)$, что и завершает доказательство. ∎

Следствие. *Пусть выполнены условия предложения 3.5. Тогда:*

$$B(L,N) = \delta_2(p,s,\alpha)B(L,N_1).$$

Доказательство. Докажем это утверждение для $b(L,N)$, определенной в (3.18). Тогда оно, очевидно, верно и для $B(L,N)$. Непосредственно из определения $b(L,N)$ следует, что $b(L,N) = 0$ при $2\alpha < s$. Далее, принимая во внимание, что $\nu(T_{\frac{m}{k}},N) \neq 0$ только в том случае, когда $k \mid m_1 p^\gamma$ где $\gamma = \min(\alpha-\alpha_0, \alpha-[(s+1)/2])$ и применяя формулу (3.20) получаем

$$b(L,N) = \sum_{i=0}^{\gamma} \delta_2(p,s,\alpha-i) \cdot \sum_{k_1 \mid m_1} \sum_{\substack{l \mid m_0 \\ (l,\frac{m_1}{k_1})=1}} \frac{1}{p^i k_1 l} \nu(T_{\frac{m}{p^i k_1 l}}, N_1) +$$

$$\sum_{i=0}^{\gamma} \eta_2(p,s,\alpha-i) \cdot \sum_{k_1 \mid m_1} \sum_{\substack{l \mid \frac{m}{m_1 p^i}, p \mid l \\ (l,\frac{m_1}{k_1})=1}} \frac{1}{p^i k_1 l} \nu(T_{\frac{m}{p^i k_1 l}}, N_1) \equiv \sum_{r \mid m} \frac{a(r)}{r} \nu(T_{\frac{m}{r}}, N_1).$$

Определим множество пар (k_1, l) во второй тройной сумме, которые дают r. Положим $r = r_1 p^\rho$, $l = l_1 p^t$ где $(r_1, p) = 1$ и $(l_1, p) = 1$. Тогда $r = k_1 l_1 p^{i+t}$ и значит $i + t = \rho$. Кроме того $(l, m_1/k_1) = (l_1, m_1/k_1) = (r_1/k_1, m_1/k_1) = 1$. Отсюда $k_1 = (r_1, m_1)$ и $l_1 = r_1/(r_1, m_1)$.

1. $0 \leq \rho \leq \gamma$.

При этом условии имеем $a(r) = \delta_2(p,s,\alpha-\rho) + \sum_{i=0}^{\rho-1} \eta_2(p,s,\alpha-i)$. Непосредственно проверяется, что $\delta_2(p,s,i) + \eta_2(p,s,i+1) = \delta_2(p,s,i+1)$ при $i \geq [(s-1)/2]$ откуда и следует, что $a(r) = \delta_2(p,s,\alpha)$.

2. $\rho > \gamma$.

В этом случае $\gamma = \alpha - [(s+1)/2]$ и $a(r) = \sum_{i=0}^{\gamma} \eta_2(p,s,\alpha-i)$. Так как $\eta_2(p,s,\alpha-\gamma) = \delta_2(p,s,\alpha-\gamma)$, то $a(r) = \delta_2(p,s,\alpha-\gamma) + \sum_{i=0}^{\gamma-1} \eta_2(p,s,\alpha-i) = \cdots = \delta_2(p,s,\alpha)$, что и требовалось показать. ∎

Предложение 3.6. *Пусть $p \mid D$. Тогда*
если $2\alpha < s-1$, то $\nu(L,N) = 0$.
если $2\alpha \geq s-1$, то
1. если $\alpha = 0$, $s = 1$, то

$$\nu(L,N) = \nu(L,N_1). \tag{3.26}$$

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

$$\nu(L,N) = \delta_3(p,s,\alpha)\nu(L,N_1) + \frac{p^{\alpha+1}-p}{p^{\alpha+1}-1} \frac{1}{p} \nu(T_{\frac{m}{p}}, N_1). \tag{3.27}$$

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

$$\nu(L,N) = \delta_3(p,s,\alpha) \left[\nu(L,N_1) + \frac{1}{p} \nu(T_{\frac{m}{p}}, N_1) \right]. \tag{3.28}$$

4. в остальных случаях

$$\nu(L,N)=\delta_3(p,s,\alpha)\,\nu(L,N_1)+\eta_3(p,s,\alpha)\sum_{i=1}^{\beta}\frac{1}{p^i}\nu(T_{\frac{m}{p^i}},N_1) \tag{3.29}$$

где $\delta_3(p,s,\alpha)$ *определена в формулировке теоремы 2,* β *определена в (3.7) и*

$$\eta_3(p,s,\alpha)=\begin{cases}\delta_3(p,s,\alpha), & \text{если } 2\alpha=s-1;\\ (p^{[\frac{s}{2}]}+p^{[\frac{s-1}{2}]})\dfrac{(p^{[\frac{s+1}{2}]}+p^{[\frac{s}{2}]}-2)(p^{\alpha+1}-p^{\alpha})}{2(p^{\alpha+1}-1)(p^{\alpha}-1)}, & \text{если } 2\alpha>s-1;\end{cases} \tag{3.30}$$

Доказательство. Если $2\alpha<s-1$, то квадратичное сравнение $X^2\equiv q^2D \pmod{4N}$ для $q\mid Q$ не имеет решения и значит $\nu(L,N)=0$. Пусть $2\alpha\geq s-1$. Прежде всего отметим, что в силу (3.1) для любого q взаимно простого с p имеем:

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

и для всякого q такого, что $q\in M_{\frac{m}{l}}$ и $p^iq\in M_m$ из (2.2) следует

$$h((p^iq)^2D)=p^i\frac{1}{l}h(q^2D).$$

Если $\alpha=0$ и $s=1$ то $f(q,N)=f(q,N_1)$ и следовательно (3.26) верно. Если $m_0=p$ и $\alpha=\alpha_0$, то для множества M_m справедливо разбиение (3.8). Тогда получаем:
если $s=1$, то

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

если $s>1$ и $2\alpha=s-1$ то

$$\nu(L,N)=p^{s-1}\left[\nu_p(L,N_1)+\frac{1}{p}\nu_p(T_{\frac{m}{p}},N_1)\right].$$

если $s>1$ и $2\alpha>s-1$ то

$$\nu(L,N)=\delta_3(p,s,\alpha)\frac{p^{\alpha+1}-1}{p-1}\left[\nu_p(L,N_1)+\frac{1}{p}\nu(T_{\frac{m}{p}},N_1)\right].$$

Используя разбиение (3.8) для $\nu(L,N_1)$ и принимая во внимание, что $f(p^iq,N_1)=f(q,N_1)$ получаем

$$\nu_p(L,N_1)=\frac{p-1}{p^{\alpha+1}-1}\nu(L,N_1)-\frac{p^{\alpha+1}-p}{p^{\alpha+1}-1}\frac{1}{p}\nu(T_{\frac{m}{p}},N_1). \tag{3.31}$$

Теперь, подставляя (3.31) в вышеприведенные выражения для $\nu(L,N)$, получаем (3.27) и (3.28).

В противном случае для множества M_m справедливо разбиение (3.7). Если $2\alpha = s-1$ то из (3.7) следует

$$\nu(L,N) = p^{s-1}\left[\nu_p(L,N_1) + \sum_{i=1}^{\beta}\frac{1}{p^i}\nu_p(T_{\frac{m}{p^i}},N_1)\right]. \tag{3.32}$$

Если $2\alpha > s-1$ то имеем

$$\nu(L,N) = \delta_3(p,s,\alpha)\frac{p^{\alpha+1}-1}{p-1}\nu_p(L,N_1) + r(p,s,\alpha)\sum_{i=1}^{\beta}\frac{1}{p^i}\nu_p(T_{\frac{m}{p^i}},N_1) \tag{3.33}$$

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

Вычислим $\nu_p(T_k,N_1)$ для $k = p^{\gamma}m_0m_1$. Если $m_0 = p$ и $\gamma = 0$ то для $\nu_p(T_k,N_1)$ справедливо (3.31) где L следует заменить на T_k и m на k. В противном случае справедливо

$$\nu_p(T_k,N_1) = \frac{p-1}{p^{\alpha_0+\gamma+1}-1}\nu(T_k,N_1) - \frac{(p-1)^2p^{\alpha_0+\gamma}}{(p^{\alpha_0+\gamma+1}-1)(p^{\alpha_0+\gamma}-1)}\sum_{i=1}^{\gamma^*}\frac{1}{p^i}\nu(T_{\frac{k}{p^i}},N_1). \tag{3.34}$$

где $\gamma^* = \gamma$ если $m_0 = 1$ и $\gamma^* = \gamma+1$ если $m_0 = p$. Чтобы это показать используем разбиение (3.7) и учитывая, что $f(p^iq,N_1) = f(q,N_1)$, получаем

$$\nu_p(T_k,N_1) = \frac{p-1}{p^{\alpha_0+\gamma+1}-1}\nu(T_k,N_1) - \frac{(p-1)p^{\alpha_0+\gamma}}{p^{\alpha_0+\gamma+1}-1}\sum_{i=1}^{\gamma^*}\frac{1}{p^i}\nu_p(T_{\frac{k}{p^i}},N_1). \tag{3.35}$$

Теперь проведем индукцию по целому $\gamma \geq 0$. При $m_0 = 1$ и $\gamma = 0$ в силу (3.35) формула (3.34) верна. При $m_0 = p$ и $\gamma = 1$ подставляем в (3.35) $\nu_p(T_{\frac{k}{p}},N_1)$ согласно (3.31) и получаем (3.34). Далее, согласно индуктивному предположению подставляем в (3.35) $\nu_p(T_{\frac{k}{p^i}},N_1)$ из (3.34) при $1 \leq i \leq \gamma$ и получаем представление $\nu_p(T_k,N_1)$ в виде линейной комбинации величин $\nu(T_{\frac{k}{p^i}},N_1)/p^i$, $0 \leq i \leq \gamma^*$ с коэффициентами $a(p^i)$. Подсчет коэффициентов при $i > 0$ нам дает

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

что и доказывает (3.34). Теперь подставляем в (3.33) выражения для $\nu_p(T_{\frac{m}{p^i}},N_1)$ при $0 \leq i \leq \beta$ из (3.34) и (3.31). После несложных преобразований получаем

$$\nu(T_m,N) = \delta_3(p,s,\alpha)\nu(T_m,N_1) + \frac{p-1}{p^{\alpha}-1}(r(p,s,\alpha) - p^{\alpha}\delta_3(p,s,\alpha))\cdot\sum_{i=1}^{\beta}\frac{1}{p^i}\nu(T_{\frac{m}{p^i}},N_1).$$

Нетрудно убедиться, что коэффициент перед суммой равен $\eta_3(p,s,\alpha)$, что и доказывает (3.29) в случае $2\alpha > s-1$. Аналогично, подставляя в (3.32) формулы (3.34) и (3.31) получаем (3.29) в случае $2\alpha = s-1$. ∎

Следствие. *Пусть выполнены условия предложения 3.6. Тогда*

$$B(L,N) = \delta_3(p,s,\alpha)B(L,N_1).$$

Доказательство. Как и ранее, доказательство проведем для $b(L,N)$, определенной в (3.18). Если $\alpha = 0$ и $s = 1$ или $m_0 = p$ и $\alpha = \alpha_0$, то проверка не представляет труда.

Легко проверяется, что справедливо равенство $\delta_3(p,s,i) + \eta_3(p,s,i+1) = \delta_3(p,s,i+1)$ при $2i \geq s-2$ и в частности $\eta_3(p,s,[s/2]) = \delta_3(p,s,[s/2])$. Рассмотрим вначале случай $m_0 = 1$. $\nu(T_{\frac{m}{k}},N) \neq 0$ только тогда, когда $k \mid p^\gamma m_1$ где $\gamma = \min(\alpha-\alpha_0, \alpha-[s/2])$. Тогда применяя формулу (3.29), получаем

$$\begin{aligned} b(L,N) = \sum_{i=0}^{\gamma} \delta_3(p,s,\alpha-i) \cdot \sum_{k_1 \mid m_1} \frac{1}{k_1 p^i} \nu(T_{\frac{m}{k_1 p^i}}, N_1) + \\ \sum_{i=0}^{\gamma} \eta_3(p,s,\alpha-i) \cdot \sum_{k_1 \mid m_1} \sum_{j=1}^{\beta-i} \frac{1}{k_1 p^{i+j}} \nu(T_{\frac{m}{k_1 p^{i+j}}}, N_1) \equiv \sum_{r \mid m} \frac{a(r)}{r} \nu(T_{\frac{m}{r}}, N_1). \end{aligned} \tag{3.36}$$

Легко видеть, что подсчет коэффициентов $a(r)$ проводится также как и в доказательстве следствия предложения 2.5.

Теперь рассмотрим случай $m_0 = p$. $b(L,N)$ при $s = 1$ есть сумма двух величин. Одна из них имеет вид (3.36) и отличие состоит лишь в том, что суммирование по i ведется до $\alpha - \alpha_0 - 1$. Вторая величина есть сумма

$$\sum_{k_1 \mid m_1} \frac{1}{k_1 p^{\alpha-\alpha_0}} \left(\delta_3(p,s,\alpha_0) \nu(T_{\frac{m}{k_1 p^{\alpha-\alpha_0}}}, N_1) + \frac{1}{p} \left(\frac{p^{\alpha_0+1}-p}{p^{\alpha_0+1}-1} + 1 \right) \nu(T_{\frac{m}{k_1 p^{\alpha-\alpha_0+1}}}, N_1) \right).$$

Значит $a(r_1 p^i) = \delta_3(p,s,\alpha)$ при $i \leq \alpha - \alpha_0 - 1$ и $a(r_1 p^{\alpha-\alpha_0}) = a(r_1 p^{\alpha-\alpha+1}) = \delta_3(p,s,\alpha_0) + \sum_{i=0}^{\alpha-\alpha_0-1} \eta_3(p,s,\alpha-i) = \delta_3(p,s,\alpha)$.

Если $s > 1$, то $\nu(T_{\frac{m}{k}},N)$ отлично от нуля лишь при $k \mid m_1 p^\gamma$, где $\gamma = \min(\alpha - \alpha_0, \alpha - [s/2])$. Если $\gamma < \alpha - \alpha_0$, то $b(L,N)$ имеет представление вида (3.36) и значит $a(r) = \delta_3(p,s,\alpha)$. Если $\gamma = \alpha - \alpha_0$, то $b(L,N)$ есть сумма вида (3.36), где суммирование по i ведется до $\alpha - \alpha_0 - 1$ плюс дополнительное слагаемое

$$\sum_{k_1 \mid m_1} \frac{\delta_3(p,s,\alpha_0)}{k_1 p^{\alpha-\alpha_0}} \left(\nu(T_{\frac{m}{k_1 p^{\alpha-\alpha_0}}}, N_1) + \frac{1}{p} \nu(T_{\frac{m}{k_1 p^{\alpha-\alpha_0+1}}}, N_1) \right)$$

Из этого представления, аналогично предыдущему случаю, следует, что $a(r) = \delta_3(p,s,\alpha)$, что и завершает доказательство. ∎

Теперь, объединяя результаты следствий предложений 3.4, 3.5, 3.6 получаем теорему 2. Следствие 1 получается путем многократного применения теоремы 2 к $B(L,N_1N_2)$, $B(L,N_1)$, $B(L,N_2)$ и сравнения $B(L,N_1N_2)$ с произведением $B(L,N_1) \cdot B(L,N_2)$. Следствие 2 получается в результате многократного применения теоремы 2 и очевидной оценки $\delta(p,s,\alpha) \leq p^{[s/2]} + p^{[(s-2)/2]}$.

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

В этом параграфе мы получим оценку

$$\nu(L,N) \le (p^{[s/2]} + p^{[(s-1)/2]} + 2)\nu(L,N_1). \tag{4.1}$$

Тогда многократное применение этой оценки дает теорему 3.

В силу предложений 3.4, 3.5, 3.6 мы можем записать $\nu(L,N) = \delta(p,s,\alpha)\nu(L,N_1) + R(L,N)$, где $R(L,N)$ есть линейная комбинация $\nu(T_{\frac{m}{k}},N_1)$, где k пробегает некоторые делители m. Мы покажем, что $2\nu(L,N_1) \ge R(L,N)$. Для этого, используя разбиения (3.6),(3.7),(3.8) получим представление $\nu(L,N_1)$ в виде линейной комбинации величин $\nu_p(T_{\frac{m}{k}},N_1)$ где k пробегает некоторые делители m. Центральным моментом в доказательстве служит получение достаточно хорошей оценки снизу отношения $\nu_p(T_l,N_1)/\nu(T_{\frac{l}{p}},N_1)$ для l кратных p. Тогда, применяя эту оценку для $\nu(L,N_1)$, получим неравенство $\nu(L,N_1) \ge \overline{R}(L,N_1)$, где $\overline{R}(L,N_1)$ есть линейная комбинация тех же $\nu(T_{\frac{m}{k}},N_1)$, что входят в $R(L,N)$ плюс некоторое неотрицательное слагаемое. И наконец, сравнивая соответствующие коэффициенты в $R(L,N)$ и $\overline{R}(L,N_1)$ убеждаемся что $2\overline{R}(L,N_1) \ge R(L,N)$, что и требуется.

В основе последующих оценок лежит следующая оценка:

Предложение 4.1. *Пусть $pm_0 \mid m$. Тогда*

$$\nu_p(T_m,N) \ge \sum_{i=1}^{\alpha-\alpha_0}\left(\frac{U_m}{pU_{\frac{m}{p}}}-1\right)\frac{1}{p^i}\nu_p(T_{\frac{m}{p^i}},N) + \frac{U_m}{pU_{\frac{m}{p}}\log_2(\frac{U_m}{pU_{\frac{m}{p}}}+2)}\sum_{\substack{k\mid m_0\\k>1}}\frac{1}{kp^i}\nu_p(T_{\frac{m}{kp^i}},N). \tag{4.2}$$

Доказательство. Во первых докажем включение

$$\bigcup_{i=1}^{\alpha-\alpha_0}\left(\left(\bigcup_{\substack{d\mid(U_m/pU_{\frac{m}{p}})\\d>1}} d\cdot M_{\frac{m}{p^i},p}\right)\bigcup\left(\bigcup_{\substack{k\mid m_0\\k>1}}\frac{U_m}{pU_{\frac{m}{p}}}\cdot M_{\frac{m}{kp^i}}\right)\right) \subset M_{m,p} \tag{4.3}$$

Из равенства $(T_m+\sqrt{D}U_m)/2 = ((T_{\frac{m}{p}}+\sqrt{D}U_{\frac{m}{p}})/2)^p$ и поскольку $p \mid U_{\frac{m}{p}}$ следует

$$\left(\frac{U_m}{pU_{\frac{m}{p}}},\ U_{\frac{m}{p}}\right) = 1 \tag{4.4}$$

Пусть $q \in M_{\frac{m}{p^i},p}$ и $k \mid m$, $k \ne m$. Поскольку $q \mid U_k$ только в том случае когда $\frac{m}{p^i} \mid k$, то $k = \frac{m}{p^j}$ и $0 < j \le i$. Из (4.4) и поскольку $U_k \mid U_{\frac{m}{p}}$ следует, что $d \nmid U_k$ и значит $dq \nmid U_k$. Так как $p \mid U_{\frac{m}{p}}$, то в силу (4.4) $p \nmid d$ и значит $dq \in M_{m,p}$.

Покажем, что $U_m/(pU_{\frac{m}{p}}) \in M_{m,p}$. Пусть $k \mid m, k \neq m$. Если $k \mid \frac{m}{p}$, то из (4.4) следует, что U_k взаимно просто с $U_m/(pU_{\frac{m}{p}})$. Пусть $k \nmid \frac{m}{p}$. Тогда k кратно p и $U_{\frac{k}{p}} \mid U_{\frac{m}{p}}$. Отсюда и из (4.4) тогда заключаем, что $U_{\frac{k}{p}}$ взаимно просто с $U_m/(pU_{\frac{m}{p}})$. Значит, чтобы U_k не делилось на $U_m/(pU_{\frac{m}{p}})$, достаточно показать, что $U_m/(pU_{\frac{m}{p}}) > U_k/U_{\frac{k}{p}}$. Используем очевидную оценку: $T_1^{k-1} < U_k < T_1^k$. Тогда $U_m/(pU_{\frac{m}{p}}) > T_1^{(p-1)(m/p-1)}$ и $U_k/U_{\frac{k}{p}} < T_1^{k-k/p+1}$. Значит требуемое неравенство будет выполнено, если $(p-1)(m'-k') - p > 0$, где $m' = m/p$, $k' = k/p$. Это неравенство выполняется за исключением случаев:
1. $p = 2$.
2. $m' = 2$, $k' = 1$.
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 (4.3) доказано.

Поскольку $U_{\frac{m}{kp^i}} \mid U_{\frac{m}{p}}$, то множества в левой части (4.3) попарно различны и значит справедливо неравенство

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

Так как $(q,d) = 1$, то в силу свойств функции f, определенной в (3.1) имеем $f(qd, N) \geq f(q, N)$ и поскольку для $q \in M_{\frac{m}{kp^i}}$ верно

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

где r пробегает все простые делители d, то продолжаем:

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

Легко проверяется,что

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

откуда и следует требуемое неравенство (4.2). ∎

В предыдущем параграфе 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 (4.1) нам необходимо рассмотреть отдельно три возможных случая.

Предложение 4.2. *Пусть* $\left(\frac{D}{p}\right) = 1$ *при* $p \neq 2$ *и* $D \equiv 1 \pmod 8$ *при* $p = 2$. *Тогда для* $\nu(L,N)$ *справедлива оценка (4.1).*

Доказательство.

Лемма. *Пусть выполнены условия предложения 4.2 и* $pm_0 \mid m$. *Тогда*

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

Доказательство. Из (3.17) 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 $\nu_p(T_{\frac{m}{kp}}, N_1)/(kp)$ с коэффициентами не превосходящими p^α. Тогда получаем неравенство

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

С другой стороны, для $\nu_p(T_m, N_1)$ справедлива оценка (4.2), поэтому имеем

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

Покажем, что коэффициенты перед суммами неотрицательны. Поскольку $U_m/U_{m/p} > pU_{m/p}^{p-1}$ и $p^{\alpha-1} \mid U_{m/p}$, то $U_m/U_{m/p} > p^{(\alpha-1)(p-1)+1} \geq p^\alpha$. Так как $U_m/U_{m/p}$ кратно p, то $U_m/U_{m/p} \geq p^\alpha + p$, что и требуется. 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 $U_m/(pU_{m/p}) + 2 < U_m/U_{m/p}$ следует оценка $U_m/(p^\alpha U_{m/p} \log_2(U_m/(pU_{m/p}) + 2)) > (U_{m/p})^{p-2}/\log_2(U_m/U_{m/p})$. 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 $p \geq 3$, $T_1 \geq 3$ и $\overline{m} \geq 2$, то $f(\overline{m}, p, T_1)$ есть возрастающая функция $\overline{m}$ и p. При $\overline{m} \geq 4$ $f(\overline{m}, p, T_1) \geq f(4, 3, T_1) > 1$. 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 аккуратная оценка. Поскольку $3^{\alpha-1} \mid (U_2/U_1)$ и $U_6/U_2 = (T_1^2 - 1)(T_1^2 - 3)$ то

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

что и завершает доказательство. ▪

Для $\nu(L, N_1)$ $(L = T_m,\ m = p^{\alpha-\alpha_0} m_0 m_1)$ из (4.17) следует представление

$$\begin{aligned}\nu(L, N_1) = (p^\alpha - 1) \sum_{\substack{k \mid m_0,\, k>1 \\ (k, m_1)=1}} \frac{1}{k} \nu(T_{\frac{m}{k}}, N_1) + (p^\alpha - p^{\alpha-1}) \sum_{\substack{k \mid m/m_1,\, p \mid k \\ (k, m_1)=1}} \frac{1}{k} \nu(T_{\frac{m}{k}}, N_1) \\ + \left\{ p^\alpha \nu_p(T_m, N_1) - (p^\alpha - p^{\alpha-1}) \sum_{i=1}^{\alpha-\alpha_0} \frac{1}{p^i} (\nu(T_{\frac{m}{p^i}}, N_1) - \nu_p(T_{\frac{m}{p^i}}, N_1)) \right\}.\end{aligned} \tag{4.5}$$

Покажем, что выражение в фигурных скобках неотрицательно. Обозначим его для краткости $\Phi(\alpha)$ и проведем индукцию по $\alpha \geq \alpha_0$ Очевидно $\Phi(\alpha_0) \geq 0$. Далее имеем: $\Phi(\alpha+1) = (p^{\alpha+1}\nu_p(T_m, N_1) - p^\alpha \nu(T_{\frac{m}{p}}, N_1)) + p^{\alpha-1}(\nu(T_{\frac{m}{p}}, N_1) - \nu_p(T_{\frac{m}{p}}, N_1)) + \Phi(\alpha)$. Первое слагаемое в правой части неотрицательно в силу леммы, 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 (3.10). Отсюда получаем $\nu(L, N) = \delta_1(p, s, \alpha)\nu(L, N_1) + R(L, N)$. Из (3.10) и (4.5), принимая во внимание, что $\Phi(\alpha)$ неотрицательно, следует $2\nu(L, N_1) - R(L, N) \geq 0$ и значит верна оценка (4.1). В заключение укажем случаи, когда в (4.1) 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 $m_0 = 2$ и $p \nmid 2m$. Поэтому получаем $\nu(T_{2m}, p^3)/\nu(T_{2m}, 1) = \delta_1(p, 3, 1) + (\delta_1(p, 3, 1) - 2)\nu(T_m, 1)/((p^\alpha - 1)\nu(T_m, 1)) = 2p + 2$ и значит равенство достигается. ▪

Предложение 4.3. *Пусть* $\left(\frac{D}{p}\right) = -1$ *при* $p \neq 2$ *и* $D \equiv 5 \pmod 8$ *при* $p = 2$. *Тогда*

$$\nu(L, N) \leq (p^{[s/2]} + p^{[(s-1)/2]})\nu(L, N_1). \tag{4.6}$$

Доказательство. Нам понадобится следующая

Лемма. *Пусть выполнены условия предложения 4.3 и* $pm_0 \mid m$. *Тогда*

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

Доказательство. Ход доказательства аналогичен доказательству леммы предыдущего предложения. Из (3.25) при $\gamma = \alpha - \alpha_0 - 1$ получаем

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

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

Принимая во внимание, что коэффициенты перед суммами меньше $(p^\alpha + p^{\alpha-1} - 2)/(p-1)$ и применяя неравенство (4.2) к $\nu_p(T_m, N_1)$ получаем

$$p^2\nu_p(T_m, N_1) - \frac{p^{\alpha+1} - p^\alpha}{p^\alpha + p^{\alpha-1} - 2}\nu(T_{\frac{m}{p}}, N_1) \geq \left(\frac{U_m}{U_{\frac{m}{p}}} - p^\alpha - p\right) \sum_{i=1}^{\alpha-\alpha_0} \frac{1}{p^{i-1}}\nu_p(T_{\frac{m}{p^i}}, N_1)$$

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

Оценка коэффициентов перед суммами проводилась при доказательстве леммы предыдущего предложения 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 данном 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 $\alpha > \alpha_0$ и m_1. m_1 нечетно и при $m_1 = 3$ и $\alpha = \alpha_0 + 1$ получаем $T_1^6/(18\log_2 T_1) > 1$ $(T_1 \geq 3)$, поэтому далее считаем $m_1 = 1$. При $m = 12$ имеем $T_1^3/(4\log_2(T_1^6/2+2)) \geq 1$ при $T_1 > 3$. Для $T_1 = 3$ имеем $D = 5$ и $\alpha_0 = 3$ 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 $m = 6$. 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 $D = 5, 21, 77, 13, 165, 221, 285, 357, 437, 69, 29, 93$. Непосредственная 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 (3.3) и (3.4). Имеем $(T_3, U_3) = (18, 2^3)$ 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. ▪

Далее будем считать, что $2\alpha \geq s$ поскольку в противном случае $\nu(L, N) = 0$ и доказывать нечего. Запишем (3.20) 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 $\nu(L, N_1) \geq R(L, N)/r(p, s, \alpha)$. Тогда из этого неравенства немедленно следует оценка (4.6). Для $\nu(L, N_1)$ воспользуемся формулой (3.25) при $\gamma = \alpha - \alpha_0$. Тогда разность $\nu(L, N_1) - R(L, N)/r(p, s, \alpha)$ равна

$$\left(\frac{p^{\alpha+1} + p^\alpha - p - 1}{p-1} - \frac{\delta_2(p, s, \alpha)}{r(p, s, \alpha)}\right) \sum_{\substack{k \mid m_0, k>1 \\ (k, m_1)=1}} \frac{1}{k}\nu(T_{\frac{m}{k}}, N_1) +$$

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

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

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

$$\frac{(p^{\alpha+1} + p^\alpha - p - 1)r(p, s, \alpha)}{(p-1)\delta_2(p, s, \alpha)} = \frac{(p^{\alpha+1} + p^\alpha - p - 1)(p^{[(s+1)/2]} + p^{[s/2]} - 2)}{(p^{\alpha+1} + p^\alpha - p^{[(s+1)/2]} - p^{[s/2]})(p-1)} \geq 1,$$

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. Из него следует, что это слагаемое больше либо равно следующей величине

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

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

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

что и завершает доказательство. ∎

Осталось рассмотреть случай $p\mid D$.

Предложение 4.4. *Пусть $p\mid D$. Тогда справедлива оценка (4.6).*

Доказательство.

Лемма. *Пусть выполнены условия предложения 4.4 и $pm_0\mid m$. Тогда*

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

Доказательство. Рассмотрим случай $m_0=1$. Из (4.2) следует оценка

$$\nu_p(T_m,N_1)\geq\left(\frac{U_m}{pU_{\frac{m}{p}}}-1\right)\sum_{i=1}^{\alpha-\alpha_0}\frac{1}{p^i}\nu_p(T_{\frac{m}{p^i}},N_1). \tag{4.7}$$

С другой стороны, из (3.34) при $\gamma=\alpha-\alpha_0-1$ получаем

$$\nu(T_{\frac{m}{p}},N_1)=\frac{p^{\alpha}-1}{p-1}\nu_p(T_{\frac{m}{p}},N_1)+p^{\alpha}\sum_{i=2}^{\alpha-\alpha_0}\frac{1}{p^i}\nu_p(T_{\frac{m}{p^i}},N_1). \tag{4.8}$$

Тогда имеем

$$p\,\nu_p(T_m,N_1)-\frac{p^{\alpha}-p^{\alpha-1}}{p^{\alpha}-1}\nu(T_{\frac{m}{p}},N_1)\geq\left(\frac{U_m}{U_{\frac{m}{p}}}-p^{\alpha}-p\right)\sum_{i=1}^{\alpha-\alpha_0}\frac{1}{p^i}\nu_p(T_{\frac{m}{p^i}},N_1). \tag{4.9}$$

Коэффициент перед суммой в (4.9), как показано в лемме предложения 4.2, неотрицателен и следовательно лемма верна при $m_0=1$. Пусть $m_0=p$. В этом

случае в правых частях (4.7) и (4.8) появляется по одному дополнительному слагаемому, что приводит к появлению в (4.9) следующего слагаемого

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

В лемме предложения 4.2 показано, что первый сомножитель положителен при $p\neq 2$. Поэтому остается рассмотреть только случай $p=2$, $m_0=2$. В лемме предложения 4.3 рассмотрен случай $p=2$, $m_0=3$ и здесь мы поступаем аналогичным образом. Представим m в виде $m=2^{\alpha-\alpha_0+1}m_1$. Тогда справедливо неравенство

$$\frac{T_{\frac{m}{2}}}{2^\alpha\log_2(T_{\frac{m}{2}}/2+2)}\geq\frac{T_1^{\frac{m}{2}-2}}{2^{\alpha-\alpha_0}\frac{m}{2}\log_2 T_1}. \tag{4.10}$$

Правая часть (4.10), очевидно есть возрастающая функция m_1 и α. Нетрудно видеть, что при $m_1=3$ и $\alpha=\alpha_0+1$ правая часть (4.10) больше 1, поэтому остается случай $m_1=1$. Рассмотрим $m=8$. Для $(T_1,U_1)=(8,1)$, которому соответствует $D=60$, правая часть (4.10) больше 1 и, следовательно это верно для всех $T_1>8$. Для $(T_1,U_1)=(4,1)$, которому соответствует $D=12$ имеем $\alpha=4$, $T_4=174$ и левая часть (4.10) больше 1. Осталось рассмотреть случай $m=4$. При $T_1\geq 16$ правая часть (4.10) больше 1, а при $T_1=12$ имеем $\alpha=3$, $T_2=142$ и левая часть (4.10) больше 1. Для двух оставшихся дискриминантов $D=12$ и 60 левая часть (4.10) меньше 1 и для них вычислим $\nu_2(T_4,N_1)$ и $\nu(T_2,N_1)$ непосредственно по формулам (3.4) и (3.3). Для $D=60$ имеем $U_4=2^4\cdot 31$, $U_2=2^3$. Тогда если $31\mid N_1$, то $\nu(T_2,N_1)=0$, поскольку $\left(\frac{D}{31}\right)=-1$. В противном случае получаем $\nu_2(T_4,N_1)=\frac{30}{14}\nu(T_2,N_1)>\frac{4}{15}\nu(T_2,N_1)$. Для $D=12$ имеем $U_4=2^3\cdot 7$, $U_2=2^2$. Если $7\mid N_1$, то также $\nu(T_2,N_1)=0$, а иначе $\nu_2(T_4,N_1)=\nu(T_2,N_1)>\frac{2}{7}\nu(T_2,N_1)$. ▪

$\nu(L,N)$ равно нулю при $\alpha<[s/2]$, поэтому далее будем считать, что $\alpha\geq[s/2]$. Согласно предложению 3.6 $\nu(L,N)$ представим 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

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

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 α, s и m_0, то необходимо рассмотреть 4 различных случая.

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

Тогда $\nu(L,N)=\nu(L,N_1)$ и (4.6) очевидным образом выполняется.

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

В этом случае $R(L,N)$ определяется из (3.27), а $\nu(L,N_1)$ согласно (3.31) 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 (3.28), а $\nu(L,N_1)$ имеет тот же вид, что и в предыдущем случае, поэтому имеем

$$\nu(L,N_1)-\frac{R(L,N)}{r(p,s,\alpha)}\geq\left(\frac{p^{\alpha}-1}{p-1}-\frac{\delta_3(p,s,\alpha)}{pr(p,s,\alpha)}\right)\nu(T_{\frac{m}{p}},N_1)$$

и

$$\frac{p(p^{\alpha}-1)r(p,s,\alpha)}{(p-1)\delta_3(p,s,\alpha)}=\frac{(p^{\alpha}-1)(p^{[(s+1)/2]}+p^{[s/2]}-2)}{(p-1)(2p^{\alpha}-p^{[(s-1)/2]}-p^{[(s-2)/2]})}\geq 1.$$

4. $m_0=1$ или ($m_0=p$ и $\alpha>\alpha_0$).
В этом случае $R(L,N)$ определяется из (3.29), а формула для $\nu(L,N_1)$ следует из (3.35) при $\gamma=\alpha-\alpha_0$ и имеет следующий вид

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

где β определена в (3.7). Согласно лемме 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

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

В правой части неравенства, рассматриваемой как линейная комбинация величин $\nu(T_{\frac{m}{p^i}},N_1)/p^i$, наименьшим коэффициентом является коэффициент с индексом

$i = 2$ (здесь следует учесть, что в нашем случае $\alpha \geq 2$). Тогда мы получаем оценку

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

Осталось показать, что коэффициент перед суммой неотрицателен. Имеем

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

что и дает нам оценку (4.6) ▪

Из предложений 4.2, 4.3 и 4.4 немедленно следует теорема 3, а из следствия 1 предложения 3.4, и оценки (4.6) получаем теорему 4. Теорема 3 дает равномерную по L оценку отношения $\nu(L,N)/\nu(L,1)$ и поэтому порядок роста остаточного члена в асимптотической формуле функции распределения примитивных гиперболических элементов $\pi_\Gamma(X)$ для $\Gamma = \Gamma_0(N)$ оценивается величиной $A(N)$, определенной в (1.5). Недавно W.Luo, Z.Rudnick и P.Sarnak в совместной работе [7] получили существенное степенное понижение остаточного члена в асимптотической формуле $\pi_\Gamma(X)$ для конгруэнц-подгрупп модулярной группы, а именно они показали, что для любой конгруэнц-подгруппы $\Gamma \subset SL_2(\mathbb{Z})$ справедлива асимптотика

$$\pi_\Gamma(X) = \mathrm{Li}(X) + O_\Gamma(X^{7/10}).$$

Используя этот результат, мы получаем теорему 5.

В заключение, мы выражаем благодарность Н.В.Кузнецову и В.А.Быковскому за полезные консультации, а также мы весьма признательны P.Sarnak за то, что он нас ознакомил с работой [7].

Список литературы

1] Головчанский В.В., Смотров М.Н., *Явная формула для числа классов примитивных сопряженных гиперболических элементов группы $\Gamma_0(N)$*, ХО ИПМ (Хабаровск), Препринт (1994), 3-32.

2] Головчанский В.В., Смотров М.Н., *Первые собственные значения оператора Лапласа на фундаментальной области модулярной группы*, ВЦ(Хабаровск), Препринт (1982), 3-10.

3] Дирихле П.Г.Л., *Лекции по теории чисел*, ОНТИ., М-Л., 1936.

4] Дэвенпорт Г., *Мультипликативная теория чисел*, Наука., М., 1971.

5] Кузнецов Н.В., *Арифметическая форма формулы следа Сельберга и распределение норм примитивных гиперболических классов модулярной группы*, ХабКНИИ (Хабаровск), Препринт (1978), 3-44.

6] Чудаков Н.Г., *Введение в теорию L-функций Дирихле*, ОГИЗ., М-Л., 1947.

7] Luo W., Rudnick Z., Sarnak P., *On Selberg's eigenvalue conjecture*, Prinseton Univ., Preprint (1994), 1-16.

Владимир Васильевич Головчанский,
Михаил Николаевич Смотров

ТОЧНАЯ ОЦЕНКА СВЕРХУ ОТНОШЕНИЯ ЧИСЛА КЛАССОВ ГРУППЫ $\Gamma_0(N)$ К ЧИСЛУ КЛАССОВ МОДУЛЯРНОЙ ГРУППЫ

Препринт

Утвержден к печати Ученым советом
Хабаровского отделения Института прикладной математики ДВО РАН

Лицензия ЛР № 040118 от 15.10.91.
Подписано к печати 11.12.94. Формат 60x84/8.
Усл. печ. л. 1,86. Уч. изд. л. 3,00
Тираж 100 экз. Заказ 184

Издательство "Дальнаука"
690041, г. Владивосток, ул. Радио, 7

Отпечатано Хабаровским отделением
Института прикладной математики ДВО РАН
680000, г. Хабаровск, ул. Шевченко, 9