Записки научных
семинаров ПОМИ
Том 254, 1998 г.

Е. П. Голубева

ОБ ИСКЛЮЧИТЕЛЬНЫХ ЧИСЛАХ ДЛЯ БИНАРНЫХ КВАДРАТИЧНЫХ ФОРМ

1. Пусть φ – примитивная положительно определенная бинарная квадратичная форма над $\mathbb{Z}$ дискриминанта D. Пусть C – класс форм, которому принадлежит φ, и R – род, которому принадлежит C.

Назовем число m исключительным для φ (и для класса C), если m представляется какой-либо формой из R, но не представляется формой φ. Как показано в работах [1, 2], множество $\mathfrak{M}_C$ имеет ту же плотность, что и $\mathfrak{M}_R$.

Основная цель настоящей работы – описать структуру множества исключительных чисел и найти асимптотическую формулу для числа $N(X,C)$ – количества исключительных чисел для класса C, не превосходящих X. До настоящего времени такие асимптотические формулы были известны только в отдельных случаях (см. [2]).

Пусть H – группа классов примитивных бинарных форм дискриминанта D и h – порядок этой группы.

Теорема. *Пусть H является циклической группой нечетного порядка h и C_0 – ее образующая. Пусть p_0 – наименьший простой делитель h и $G \subset H$ – подгруппа, порождаемая элементом $C_0^{p_0}$.*

Тогда, если $C \in G$, то

$$N(X,C) = A_1 X (\log X)^{-1+1/2p_0} \big(\log\log X\big)^{p_0-2}\,(1+o(1)), \qquad (1)$$

если $C \bar{\in} G$, то

$$N(X,C) = A_2 X (\log X)^{-1+1/2p_0} \big(\log\log X\big)^{p_0-3}\,(1+o(1)), \qquad (2)$$

где A_1, A_2 – положительные постоянные.

Доказательство этой теоремы будет приведено ниже.

Заметим, что ограничения, наложенные на группу H, могут быть сняты. В любом случае показатель степени при $\log X$ в формулах (1) и (2) определяется наибольшим из порядков подгрупп главного рода.

В процессе доказательства теоремы мы показываем, что множество исключительных чисел имеет достаточно простую мультипликативную структуру. Это вселяет надежду на то, что оно достаточно хорошо распределено не только во множестве всех целых чисел, но и и в других последовательностях. Например, было бы интересно рассмотреть бинарную задачу

$$n = P + m,$$

где P – простое, а m является исключительным для какой-либо фиксированной формы, принадлежащей неодноклассному роду. Во многих аспектах эта задача аналогична задаче о разрешимости последнего уравнения в числах P (простое) и m, у которых каждый простой делитель принадлежит фиксированной арифметической прогрессии. Обе эти задачи труднее, чем уравнение Харди–Литтлвуда, но, по крайней мере на первый взгляд, проще, чем классическая бинарная задача $n = P_1 + P_2$.

2. Прежде чем приступить к непосредственному изложению доказательства остановимся на общих соображениях, на которых оно основано.

Пусть простое число P не делит $2D$ и представимо классом C. Тогда P представимо и обратным классом C^{-1}. Пусть $C = C_0^k$, тогда P отвечает пара чисел k и $-k$, определенных по модулю h. При перемножении различных простых чисел соответствующие им классы также перемножаются. Таким образом, бесквадратному числу $m = P_1 \dots P_r$ отвечает 2^r чисел $\pm k_1 \pm \dots \pm k_r \pmod h$ с любой комбинацией знаков.

При росте r количество различных $\pmod h$ среди них, вообще говоря, растет. Исключения возникают в тех случаях, когда r мало или когда все k_i, кроме конечного числа, зависящего только от h, делятся на какой-нибудь фиксированный делитель h. Первый случай соответствует редким последовательностям.

Во втором случае пусть $g \mid (k_1, \dots, k_r)$ и $g \mid h$. Рассмотрим подгруппу $G = \{C_0^g\}$. Все числа вида $m_0 = P_1 \dots P_r$, где $P_i \in \mathfrak{M}_G$, будут исключительными для всех классов $C \bar{\in} G$. Порядок группы G определяет степень $\log X$ в соответствующей асимптотической формуле. Кроме чисел m_0 исключительными для каких-либо классов будут числа вида $m = m_0\, Q_1 \dots Q_t$, где Q_i – различные простые, отвечающие классам $C_0^{l_i}$, $(l_i, g) = 1$, таким, что выражение $\pm l_1 \pm \dots \pm l_t$ пробегает неполную систему вычетов $\pmod g$.

Максимальная длина такого набора определяет показатель, с которым $\log\log X$ входит в соответствующую асимптотическую формулу.

До сих пор мы все время говорили только о бесквадратных числах, взаимно простых с $2D$. Это оправдано в силу того обстоятельства, что их асимптотическое количество отличается от $N(X,C)$ постоянным множителем, а мы не вычисляем значения A_1 и A_2.

3. Для реализации изложенных соображений докажем несколько лемм.

Лемма 1. *Пусть G – подгруппа H, $h(G) < h$ – ее порядок и пусть классы $C_1, \ldots, C_r$ не принадлежат G.*

Обозначим через Σ_X количество бесквадратных чисел, не превосходщяих X, взаимно простых с $2D$ и имеющих вид $mP_1 \ldots P_r$, где каждый простой делитель m принадлежит $\mathfrak{M}_G$, а $P_i \in \mathfrak{M}_{C_i}$.

Тогда

$$\Sigma_X = A\frac{X}{(\log X)^{1-\frac{h(G)}{2h}}}\big(\log\log X\big)^r\ \big(1+o(1)\big),$$

где $A > 0$ – постоянная

Доказательство. Введем функцию $\nu(m)$, пересчитывающую числа m такие, как в формулировке леммы:

$$\nu(m) = \begin{cases} 1, & \text{если } \ m \ \text{ бесквадратно, } \ (m,2D)=1 \ \text{ и} \\ & \text{каждый простой делитель } \ m \ \text{ принадлежит } \ \mathfrak{M}_G, \\ 0 & \text{в противном случае.} \end{cases}$$

Эта функция мультипликативна и удовлетворяет всем остальным условиям, наложенным на функции в работе [3]. В силу результата последней работы,

$$\sum_{m\leqslant Y}\nu(m) = A_3\frac{Y}{\log Y}\exp\left(\sum_{m\leqslant Y}\frac{\nu(P)}{P}\right)\big(1+o(1)\big), \tag{3}$$

где $A_3 > 0$ – постоянная.

Как известно,

$$\sum_{\substack{P\leqslant Y\\ P\in\mathfrak{M}_C}}\frac{1}{P} = \begin{cases} \dfrac{1}{h}\log\log X + A_4(C) + o(1), & \text{если } \ C \neq C_0^0, \\ \dfrac{1}{2h}\log\log X + A_5(C) + o(1), & \text{если } \ C = C_0^0, \end{cases} \tag{4}$$

где $A_4(C)$, $A_5(C)$ – постоянные.

Поскольку для $C \neq C_0^0$ условия $P \in \mathfrak{M}_C$ и $P \in \mathfrak{M}_{C^{-1}}$ выполняются одновременно, то мы имеем

$$\sum_{P \leqslant Y} \frac{\nu(P)}{P} = \frac{1}{2h} \sum_{\substack{P \leqslant Y \\ P \in \mathfrak{M}_{C_0^0}}} \frac{1}{P} + \frac{1}{2} \sum_{\substack{C \in G \\ C \neq C_0^0}} \sum_{\substack{P \leqslant Y \\ P \in \mathfrak{M}_C}} \frac{1}{P}$$

$$= \frac{1}{2h} h(G) \log\log Y + A_6 + o(1), \tag{5}$$

где A_6 – постоянная.

Возвращаясь к равенству (3), получаем отсюда

$$\sum_{m \leqslant Y} \nu(m) = A_7 \frac{Y}{(\log Y)^{1-\frac{h(G)}{2h}}} \big(1 + o(1)\big), \tag{6}$$

где постоянная $A_7 > 0$.

Сумму Σ_X можно записать в виде:

$$\Sigma_X = \sum_{\substack{P_1 \dots P_r \leqslant \sqrt{X} \\ P_i \in \mathfrak{M}_{C_i} \\ P_i \neq P_j}} \sum_{m \leqslant X/P_1 \dots P_r} \nu(m)$$

$$+ \sum_{m \leqslant \sqrt{X}} \nu(m) \sum_{\substack{\sqrt{X} \leqslant P_1 \dots P_r \leqslant X/m \\ P_i \in \mathfrak{M}_{C_i} \\ P_i \neq P_j}} 1 = \Sigma_1 + \Sigma_2.$$

Оценим сначала Σ_2:

$$\Sigma_2 = O\biggl(\frac{X}{\log X} (\log\log X)^{r-1} \sum_{m \leqslant \sqrt{X}} \frac{\nu(m)}{m}\biggr).$$

Суммируя по частям и используя равенство (6), для последней суммы имеем

$$\sum_{m \leqslant \sqrt{X}} \frac{\nu(m)}{m} = O\biggl(\sum_{m \leqslant \sqrt{X}} \frac{1}{m \log^{\alpha} m}\biggr) = O\left(\log^{1-\alpha} X\right),$$

где $\alpha = 1 - h(G)/2h$. Таким образом,

$$\Sigma_2 = O\biggl(\frac{X}{\log^{\alpha} X} \left(\log\log X\right)^{r-1}\biggr). \tag{7}$$

Для Σ_1 из (6) имеем

$$\Sigma_1 = A_7 X\bigl(1+o(1)\bigr) \sum_{\substack{P_1\dots P_r\leqslant\sqrt{X}\\ P_i\in\mathfrak{M}_{C_i}\\ P_i\neq P_j}} \frac{1}{P_1\dots P_r\bigl(\log\frac{X}{P_1\dots P_r}\bigr)^{\alpha}}.$$

Разобьем, в свою очередь, Σ_1 на две суммы, $\Sigma_1 = \Sigma_3 + \Sigma_4$, следующим образом: к Σ_3 отнесем те слагаемые, для которых все P_i удовлетворяют условию $P_i \leqslant \exp(\log X/\log^2\log X)$, к Σ_4 – все остальные.

Оценим сначала Σ_4:

$$\Sigma_4 = O\Biggl(\frac{X}{\log^{\alpha} X} \sum_{P_2\dots P_r\leqslant\sqrt{X}} \frac{1}{P_2\dots P_r} \sum_{\substack{\exp\left(\frac{\log X}{\log^2\log X}\right)\\ \leqslant P_1\leqslant\sqrt{X}}} \frac{1}{P_1}\Biggr)$$

$$= O\Biggl(\frac{X}{\log^{\alpha} X}\log\log\log X \sum_{P_2\dots P_r\leqslant\sqrt{X}} \frac{1}{P_2\dots P_r}\Biggr)$$

$$= O\Biggl(\frac{X}{\log^{\alpha} X}\log\log\log X\,(\log\log X)^{r-1}\Biggr).$$

Для Σ_3 имеем

$$\Sigma_3 = A_7\frac{X(1+o(1))}{\log^{\alpha} X\bigl(1+O\bigl(\frac{1}{\log^2\log X}\bigr)\bigr)}\Biggl(\prod_{1\leqslant i\leqslant r} \sum_{\substack{P_i\in\mathfrak{M}_{C_i}\\ P_i\leqslant\exp\left(\frac{\log X}{\log^2\log X}\right)}} \frac{1}{P_i}$$

$$+O\Biggl(\sum_{\substack{P_i\leqslant\exp\left(\frac{\log X}{\log^2\log X}\right)\\ P_i=P_j}} \frac{1}{P_1\dots P_r}\Biggr)\Biggr).$$

В силу (4), первое слагаемое в последнем соотношении равно

$$\frac{1}{h^r}\log^r\log X\left(1+O\left(\frac{\log\log\log X}{\log\log X}\right)\right).$$

Собирая соотношения для Σ_3 и Σ_4, для Σ_1 имеем

$$\Sigma_1 = A\frac{X}{\log^{\alpha} X}(\log\log X)^r\ \bigl(1+o(1)\bigr),$$

где $A > 0$. С учетом оценки (7), получаем отсюда утверждение леммы.

Замечание. В работе [1] в равенстве, аналогичном (4), была допущена неточность, которая не повлекла за собой неточностей в остальных формулах.

Лемма 2. *Пусть $m \in \mathfrak{M}_C$ для какого-то C, $n \in \mathfrak{M}_H = \mathfrak{M}$ и $(n,m) = 1$, тогда $mn \in \mathfrak{M}$.*

Доказательство очевидно, поскольку $CH = H$.

Лемма 3. *Пусть $m_i \in \mathfrak{M}_{C_0}$ для $1 \leqslant i \leqslant h$ и $(m_i, m_j) = 1$. Тогда $m_1 \dots m_h \in \mathfrak{M}$.*

Доказательство. Пусть C_0^k – произвольный элемент H. Положим $k_1 = k(h+1)/2 \pmod h$, $1 \leqslant k_1 \leqslant h$, $k_2 = h - k_1$. Тогда $m_1 \dots m_{k_1} \in \mathfrak{M}_{C_0^{k_1}}$, $m_{k_1+1} \dots m_h \in \mathfrak{M}_{C_0^{-k_1}}$. Поскольку $k_1 - k_2 = k \pmod h$, то $m_1 \dots m_h \in \mathfrak{M}_{C_0^{k_1-k_2}} = \mathfrak{M}_{C_0^k}$.

Лемма 4. *Пусть $m_{ij} \in \mathfrak{M}_{C_0^{k_i}}$ $(1 \leqslant i \leqslant t,\ 1 \leqslant j \leqslant h^{h+1})$, $1 < t \leqslant h$, m_{ij} попарно взаимно просты и $(k_1, \dots, k_t) = 1$. Тогда*

$$\prod_{\substack{1\leqslant i\leqslant t\\ 1\leqslant j\leqslant h^{h+1}}} m_{ij} \in \mathfrak{M}.$$

Доказательство. Пусть числа $l_1, \dots, l_t$ таковы, что $k_1 l_1 + \dots + k_t l_t = 1$ и $|l_i| < h^t$. Тогда для любого $a \geqslant 1$

$$\prod_{\substack{a\leqslant j\leqslant\\ \leqslant|l_i|+a-1}} m_{ij} \in \mathfrak{M}_{C_0^{k_i l_i}}.$$

Следовательно,

$$\prod_{\substack{a\leqslant i\leqslant t\\ a\leqslant j\leqslant|l_i|+a-1}} m_{ij} \in \mathfrak{M}_{C_0}.$$

В силу результата леммы 3, отсюда вытекает, что

$$\prod_{\substack{a\leqslant i\leqslant t\\ 1\leqslant j\leqslant|l_i|h}} m_{ij} \in \mathfrak{M},$$

а из леммы 2 получаем, что тогда и

$$\prod_{\substack{a\leqslant i\leqslant t\\ 1\leqslant j\leqslant h^{h+1}}} m_{ij}\in\mathfrak{M}.$$

Лемма 5. *Пусть p – простое, $p|h$, $p>3$ и группа G порождена элементом C_0^p. Пусть классы $C_1,\ldots,C_{p-2}$ не принадлежат G и хотя бы два из них таковы, что $C_iC_j^{\pm1}\bar{\in}G$. Пусть $P_i\in\mathfrak{M}_{C_i}$ $(1\leqslant i\leqslant p-2)$, $P_i\neq P_j$ и $m\in\mathfrak{M}_G$. Тогда $mP_1\ldots P_{p-2}\in\mathfrak{M}$.*

Доказательство. Пусть классы C_i имеют вид $C_i=C_0^{k_i}$ $(1\leqslant i\leqslant p-2)$. Тогда $(k_i,p)=1$ и существует пара i, j такая, что $k_i\neq\pm k_j$. Покажем, что тогда выражение $\pm k_1\ldots\pm k_{p-2}$, где знаки $\pm$ выбираются независимо друг от друга, пробегает полную систему вычетов $(\mathrm{mod}\ p)$.

Пусть для определенности $k_1\neq\pm k_2$. Тогда комбинация $\pm k_1\pm k_2$ принимает четыре различных значения $(\mathrm{mod}\ p)$. Покажем, что если

$$\pm k_1\pm\ldots\pm k_r\quad(2\leqslant r<p-2)\tag{8}$$

принимает $T_r<p$ различных значений $(\mathrm{mod}\ p)$, то для любого k_{r+1} выражение $\pm k_1\pm\ldots\pm k_{r+1}$ принимает не менее T_r+1 различных значений $(\mathrm{mod}\ p)$.

Действительно, пусть $n_1,\ldots,n_{T_r}$ – различные значения, принимаемые комбинацией (8) $(\mathrm{mod}\ p)$. Тогда числа $t_1=n_1+k_{r+1},\ldots,t_{T_r}=n_{T_r}+k_{r+1}$ различны $(\mathrm{mod}\ p)$. Если ряд чисел t_i совпадает с рядом чисел $n_i-k_{r+1}=t_i-2k_{r+1}$ $(\mathrm{mod}\ p)$, то для каждого t_i найдется t_j (очевидно, единственное) такое, что $t_i=t_j-2k_{r+1}$. Складывая эти равенства при всех i, имеем $2k_{r+1}T_r=0$ $(\mathrm{mod}\ p)$, что невозможно. Таким образом, $T_r\geqslant r+2$ и, значит, $T_{p-2}=p$.

Пусть теперь k – произвольное число, тогда $P_1\ldots P_{p-2}\in\mathfrak{M}_{C_0^n}$ для некоторого $n=k$ $(\mathrm{mod}\ p)$. Поскольку $m\in\mathfrak{M}_{C_0^{pr}}$ для любого r, то $mP_1\ldots P_{p-2}\in\mathfrak{M}_{C_0^k}$ и лемма доказана.

Лемма 6. *Пусть G – та же группа, что и в лемме 5. Пусть $P_i\in\mathfrak{M}_{C_1}$, где $C_1\bar{\in}G$, $1\leqslant i\leqslant p-2$, P_i – различные простые.*

Тогда $mP_1\ldots P_{p-2}\bar{\in}\mathfrak{M}_G$, $mP_1\ldots P_{p-2}\in\mathfrak{M}_C$, если $C\bar{\in}G$; $mP_1\ldots P_{p-3}\bar{\in}\mathfrak{M}_C$ в том и только том случае, когда $C\bar{\in}C_1^{\pm1}G$.

Доказательство. Пусть $C_1=C_0^k$, где $(k,p)=1$. Рассуждая так же, как в доказательстве предыдущей леммы, можно показать, что $mP_1 \ldots P_{p-2} \in \mathfrak{M}_{C_0^r}$ тогда и только тогда, когда $r = k(n_1 - n_2) \pmod p$, здесь $n_1 + n_2 = p - 2$, n_1, $n_2 \geqslant 0$. Таким образом $r = 2k(n_1 + 1) \pmod p$ и принимает все значения $\pmod p$ кроме 0.

Аналогично, $mP_1 \ldots P_{p-3} \in \mathfrak{M}_{C_0^r}$ тогда и только тогда, когда $r = k(n_1 - n_2) \pmod p$, здесь $n_1 + n_2 = p - 3$, n_1, $n_2 \geqslant 0$. Таким образом, $r = k(2n_1 + 3) \pmod p$. Последнее выражение принимает все значения $\pmod p$ кроме $\pm k$.

4. Доказательство теоремы. Пусть $m \in \mathfrak{M}$, m – бесквадратно, $m = P_1 \ldots P_r$. Пусть $P_i \in \mathfrak{M}_{C_0^{k_i}}$ и множество чисел k_i содержит l различных.

Выберем те числа k_i $(1 \leqslant i \leqslant r)$, которые встречаются не менее, чем h^{h+1} раз. Обозначим их количество через $t \leqslant l$. Обозначим эти числа через $k_1, \ldots, k_t$.

Поскольку $m \bar{\in} \mathfrak{M}$, то, в силу результатов леммы 4, либо $t = 0$, либо $(k_1, \ldots, k_t) = k > 1$.

Обозначим через $N_0(X, C)$ количество чисел $m \leqslant X$, для которых $t = 0$. Тогда, очевидно,

$$N_0(X, C) = O\left(\frac{X}{\log X} (\log\log X)^B\right), \tag{9}$$

где постоянная B зависит только от h.

Если $t = 1$ и $(k_1, h) = 1$, то, в силу результата леммы 3, $m \in \mathfrak{M}$, что невозможно. Таким образом, $k_1 = k_0 K$, где $(K, h) = 1$, а все простые делители k_0 делят h. Очевидно, мы можем считать, что $K = 1$, поскольку в противном случае в качестве образующей можно взять C_0^K.

Пусть p – наименьший простой делитель k_0. В силу всего вышеизложенного, число m можно записать в виде

$$m = m_0\, Q_1 \ldots Q_w, \tag{10}$$

где $m_0 \bar{\in} \mathfrak{M}_C$, если $C \bar{\in} G$, группа G порождается элементом C_0^p, числа Q_i – различные простые, а w ограничено постоянной, зависящей только от h.

Если $t \geqslant 2$, то мы имеем такую же ситуацию: $k = h_0 K$, где $k_0 > 1$, $(K, h) = 1$, можно считать, что $K = 1$, и число m можно записать в виде (10).

Обозначим через $N_p(X)$ количество $m \leqslant X$ таких, что $m \bar{\in} \mathfrak{M}$ и они записываются в виде (10). В силу результата леммы 1, при

$p > p_0$

$$N_p(X) = O\left(\frac{X}{\log^{1-\frac{1}{2p}} x} (\log\log X)^w\right). \tag{11}$$

Пусть теперь $p = p_0$. Если $t < h/p_0$, то из леммы 1 вытекает, что количество таких m, которое мы обозначаем через $N_{p_0,t}(X)$, допускает оценку

$$N_{p_0,t}(X) = O\left(\frac{X}{\log^{1-\frac{t}{2h}} x} (\log\log X)^w\right). \tag{12}$$

При $t = h/p_0$ из той же леммы имеем

$$N_{p_0,t}(X) = A\frac{X}{\log^{1-\frac{1}{2p_0}} x} (\log\log X)^w \ \ \bigl(1 + o(1)\bigr),$$

где $A > 0$ – постоянная.

Сравнивая соотношения (9), (11) и (12), мы получаем для $N_1(X,C)$ – количества бесквадратных чисел $m \bar{\in} \mathfrak{M}_C$, $(m, 2D) = 1$, асимптотическое равенство

$$N_1(X,C) = A\frac{X}{\log^{1-\frac{1}{2p_0}} x} (\log\log X)^w \ \ \bigl(1 + o(1)\bigr),$$

где $A > 0$.

Максимальное значение w определено в леммах 5 и 6. Для $C \in G$ $w = p_0 - 2$, для $C \bar{\in} G$ $w = p_0 - 3$.

Для завершения доказательства теоремы нам осталось только заметить, что величины $N_1(X,C)$ и $N(X,C)$ асимптотически отличаются лишь постоянным множителем.

Литература

1. Е. П. Голубева, *О представлении больших чисел бинарными квадратичными формами,* Зап. научн. семин. ПОМИ **226** (1996), 60–64.
2. О. М. Фоменко, *Распределение значений коэффициентов Фурье модулярных форм веса 1,* Зап. научн. семин. ПОМИ **226** (1996), 196–227.
3. E. Wirsing, *Das asymptotische Verhalten von Summen über multiplicative Functionen. I,* Math. Ann. **143**, No. 1 (1961), 75–102.

Государственный университет
телекоммуникаций
им. М. А. Бонч-Бруевича

Поступило 18 ноября 1998 г.