О. М. Фоменко, Числа классов неопределенных бинарных квадратичных форм, *Зап. научн. сем. ПОМИ*, 2001, том 276, 312–333

Записки научных
семинаров ПОМИ
Том 276, 2001 г.

О. М. Фоменко

ЧИСЛА КЛАССОВ НЕОПРЕДЕЛЕННЫХ БИНАРНЫХ КВАДРАТИЧНЫХ ФОРМ

§0

Пусть a, b, c – целые числа, $h(d)$ – число классов собственно эквивалентных примитивных бинарных квадратичных форм $ax^2 + bxy + cy^2$ дискриминанта $d = b^2 - 4ac$, $H(D)$ – число классов собственно эквивалентных примитивных бинарных квадратичных форм $ax^2 + 2bxy + cy^2$ детерминанта $D = b^2 - ac$. Определение числа классов $H(D)$ принадлежит Гауссу.

Гаусс [1, Art. 302] предположил, что в случае отрицательных детерминантов

$$\sum_{-x\leqslant D<0} H(D) \sim \frac{4\pi x^{3/2}}{21\zeta(3)}.$$

Этот факт доказали Липшиц (1865) и Мертенс (1874). Кроме того, Гаусс предположил, что лишь для конечного множества отрицательных детерминантов в каждом роде форм имеется только один класс. Это было доказано уже в 20 веке.

Гаусс замечает, что "относительно числа классов ... положительные детерминанты ведут себя совершенно не так, как отрицательные" [1, Art. 302]. В [1, Art. 304] он пишет: "... среди положительных неквадратных детерминантов, по крайней мере, пока они не очень велики, напротив, бо́льшая часть обладает такими классификациями, когда в каждом роде имеется только один класс. $\langle\ldots\rangle$ Было бы красивой и достойной внимания математиков задачей определить, по какому закону все реже и реже встречаются детерминанты, обладающие в каждом роде только одним классом; до сих пор мы не можем ни теоретически определить, ни индуктивно с достаточной уверенностью предположить, обрываются ли совершенно в конце концов такие детерминанты (что, однако, представляется маловероятным), или они становятся по крайней мере бесконечно редкими, или же их частота все ближе подходит к постоянному пределу. Среднее число классов растет лишь немного быстрее, чем среднее число родов, и намного медленнее, чем квадратные корни из детерминантов ...".

Существование бесконечного множества родов, обладающих только одним классом, доказал Дирихле (1855):

$$H(5^{2k+1}) = 1 \quad (k = 0, 1, 2, \dots).$$

Последовательность детерминантов в примере Дирихле очень редка. Лишь недавно Е. П. Голубева [2, II] получила значительно более убедительное решение: среди простых чисел $p \leqslant x$ существует не менее $Cx\log^{-2} x$, $C > 0$, таких, что хотя бы одно из значений $H(7p^2)$, $H(11p^2)$, $H(19p^2)$ равно 4. Отметим, что $\tau(7p^2) = \tau(11p^2) = \tau(19p^2) = 4$, где $p \neq 7, 11, 19$ и $\tau(D)$ – число родов форм детерминанта D, так что среди детерминантов $D \leqslant x$ имеется не менее $C'x^{1/2}\log^{-2} x$, $C' > 0$, с одним классом в роде форм.

В настоящее время выдвинуты количественные гипотезы о поведении чисел классов неопределенных бинарных квадратичных форм, подтверждающие предположения Гаусса. Приведем некоторые из них.

Гипотеза 1 (Холи [3]). *При $x \to \infty$ имеем*

$$\sum_{D \leqslant x} H(D) \sim \frac{25}{12\pi^2}\, x \log^2 x.$$

Гипотеза 2 (Холи [3]). *При $x \to \infty$ имеем*

$$\sum_{\substack{p \leqslant x \\ p \equiv 1 \pmod 4}} H(p) \sim \frac{1}{6}\, x.$$

Гипотеза 3 (Холи [3]). *Пусть $N(x, \alpha)$ – число простых $p \equiv 1 \pmod 4$, для которых $p \leqslant x$ и $H(p) > \alpha$. Тогда существует предел*

$$\lim_{x \to \infty} \frac{\log x}{x}\, N(x, \alpha)$$

и при $\alpha \to \infty$ имеем

$$\lim_{x \to \infty} \frac{\log x}{x}\, N(x, \alpha) \sim \frac{1}{3\alpha}.$$

Гипотеза 4 (Е. П. Голубева [4]). *Пусть $l(d)$ – длина периода разложения $\sqrt{d}$ в непрерывную дробь. Тогда справедлива оценка*

$$\#\{d \leqslant x, l(d) = L\} = O(x^{1/2} \log x),$$

где $L \leqslant x^{1/2} \log x$ и константа, входящая в O, абсолютная.

В качестве следствия этой гипотезы имеем оценку:

$$h(d) \ll \log^2 d$$

для почти всех d.

Пока известно не много результатов в направлении предположений Гаусса, касающихся положительных детерминантов (или дискриминантов). Отметим работу Е. П. Голубевой [2, I]. В ней было замечено, что последовательности типа $\{h(5p^2)\}$, p бежит по простым числам, поддаются изучению, причем к ним применимы методы, используемые при исследовании гипотезы Артина о примитивных корнях (см. также [2, II]). Было показано, что

$$\sum_{p \leqslant x} h(5p^2) = O(x^{3/2} (\log x)^{-1}) \tag{1}$$

(тривиальный результат: $O(x^2 (\log x)^{-2})$, предполагаемая наилучшая оценка: $O(x^{1+\varepsilon})$). Результат (1) по силе соответствует оценкам, при доказательстве которых используется теорема Бомбьери–Виноградова; см. [5]. Далее, в [2, I] в предположении справедливости расширенной гипотезы Римана (РГР) для некоторых полей алгебраических чисел было доказано соотношение

$$\#\{p \leqslant x \mid h(5p^2) = 2\} \asymp \frac{x}{\log x}.$$

Отметим, что число родов форм дискриминанта $5p^2$, $p \neq 5$, равно 2.

Напомним теперь формулу Дирихле для $h(d)$, $d > 0$ – неквадрат:

$$h(d) = \frac{\sqrt{d}}{\log \varepsilon_d} L(1, \chi_d),$$

где $\chi_d(m) = \left(\frac{d}{m}\right)$ – символ Лежандра–Якоби–Кронекера, ε_d – фундаментальное решение уравнения Пелля $t^2 - du^2 = 4$. Известно, что

$$d^{-\varepsilon} \ll L(1, \chi_d) \ll \log d;$$

в предположении гипотезы Римана для L-рядов Дирихле оценки уточняются:

$$(\log\log d)^{-1} \ll L(1,\chi_d) \ll \log\log d.$$

Известно, что

$$\sqrt{d} < \varepsilon_d \leqslant e^{A_0\sqrt{d}\log d},$$

где $A_0 > 0$ – некоторая константа. Тем самым, поведение $h(d)$ определяется, в основном, поведением ε_d.

Пусть $d = 5p^2$, тогда

$$h(5p^2) = \frac{p\sqrt{5}}{\log\varepsilon_{5p^2}}\, L(1,\chi_{5p^2});$$

$L(1,\chi_{5p^2})$ почти константа, и поведение $h(5p^2)$, как и в общем случае, определяется поведением ε_{5p^2}.

Рассмотрим теперь последовательность дискриминантов $d = m^2-4$, дающую экстремально большие числа классов. Имеем

$$\varepsilon_d = \frac{m+\sqrt{m^2-4}}{2}$$

и

$$h(m^2-4) = \frac{\sqrt{m^2-4}}{\log\frac{m+\sqrt{m^2-4}}{2}}\, L(1,\chi_{m^2-4}) \asymp$$

$$\asymp \frac{m}{\log m} L(1,\chi_{m^2-4}) \quad (m\to\infty).$$

Поведение $h(m^2-4)$ определяется поведением L-функции Дирихле в точке $s=1$ и сходство со случаем отрицательных дискриминантов вполне очевидно. Легко видеть (ср. [6]), что

$$\sum_{2<m\leqslant M} h(m^2-4) \sim b\frac{M^2}{\log M} \quad (M\to\infty),$$

где $b>0$ – константа. Существуют и другие последовательности дискриминантов с указанным экстремальным свойством (см. [7]). Однако из сформулированных выше гипотез 1–4 следует, что для большинства положительных дискриминантов (или детерминантов) числа классов малы.

Цель настоящей работы – подтвердить этот факт для последовательности дискриминантов $5p^2$, где p пробегает простые числа с условием $\left(\frac{5}{p}\right) = 1$. Пусть выполнена РГР (ε_0), расширенная гипотеза Римана для дзета функций Дедекинда всех полей $K_n = \mathbb{Q}(\varepsilon_0^{\frac{1}{n}}, \zeta_{2n})$, $n = 1, 2, 3, \ldots$; $\varepsilon_0 = \frac{1+\sqrt{5}}{2}$, ζ_n – примитивный корень n-ой степени из 1. Тогда имеют место следующие результаты.

1) Пусть $\alpha(x)$ – сколь угодно медленно монотонно возрастающая функция с условием $\alpha(x) \to \infty$. Тогда

$$\#\left\{p \leqslant x \mid \left(\frac{5}{p}\right) = 1,\, h(5p^2) > (\log p)^{\alpha(p)}\right\} = o(\pi(x)),$$

где

$$\pi(x) = \sum_{p \leqslant x} 1$$

(справедливо и более сильное утверждение, см. ниже замечание 1).

2) Пусть α – произвольная достаточно большая положительная константа. Тогда для любых $x > x_\alpha$ справедливо соотношение

$$\#\left\{p \leqslant x \mid \left(\frac{5}{p}\right) = 1,\, h(5p^2) > \alpha\right\} \asymp \frac{\pi(x)}{\alpha},$$

где $\asymp$-константы являются абсолютными.

3) Для $35,42739\ldots\%$ всех простых p с условием $\left(\frac{5}{p}\right) = 1$ имеем $h(5p^2) = 2$.

Доказательства этих и других результатов даны в §§1–4. Мы используем идеи работы [2] и метод Холи [8] в условном доказательстве гипотезы Артина, а также варианты этого метода (см. [9–14]).

§1

Пусть $K = \mathbb{Q}(\sqrt{5})$, $\varepsilon_0 = \frac{1+\sqrt{5}}{2}$; $\{F_m\}$ – последовательность чисел Фибоначчи, где $F_0 = 0$, $F_1 = 1$,

$$F_m = F_{m-2} + F_{m-1}.$$

Известно, что

$$\varepsilon_0^m = F_{m-1} + \varepsilon_0 F_m. \tag{2}$$

Обозначим через $\lambda(n)$ длину наименьшего периода последовательности $\{F_m\}_{m\in\mathbb{N}} \mod n$. Пусть $\mathbb{Z}_n$ – кольцо классов вычетов $\mathrm{mod}\ n$, $\mathbb{Z}_n^*[\varepsilon_0]$ – группа единиц кольца $\mathbb{Z}_n[\varepsilon_0]$, $\mathrm{ord}(a, G) = \min\{t > 0 \mid a^t = 1,\ a \in G,\ G$ – конечная группа$\}$, $o(a, n) = \mathrm{ord}(a, \mathbb{Z}_n^*[\varepsilon_0])$. Для $a \in \mathbb{N}$ $o(a, n)$ означает наименьшее целое положительное d, для которого $a^d \equiv 1 \pmod n$, т.е. порядок числа $a \pmod n$. Как доказано в [12], для $n \in \mathbb{N}$, $n \geqslant 2$,

$$\lambda(n) = o(\varepsilon_0, n).$$

Лемма 1 (см. [15]). *Пусть $p > 2$ и $p \neq 5$. Тогда*

1) *если $\left(\frac{5}{p}\right) = 1$, то $\lambda(p) \mid (p-1)$;*

2) *если $\left(\frac{5}{p}\right) = -1$, то $\lambda(p) \mid 2(p+1)$.*

Очевидно,

$$\varepsilon_0^{\lambda(n)} = F_{\lambda(n)-1} + \varepsilon_0 F_{\lambda(n)},$$

где $F_{\lambda(n)-1} \equiv 1 \pmod n$, $F_{\lambda(n)} \equiv 0 \pmod n$. Пусть $i(n)$ – наименьшее натуральное число такое, что $n \mid F_{i(n)}$. По свойствам чисел Фибоначчи, $i(n) \mid \lambda(n)$. Число $i(n)$ называется точкой вхождения n в последовательность чисел Фибоначчи.

Ниже мы рассматриваем только простые числа p с условием $\left(\frac{5}{p}\right) = 1$; будем использовать соглашение

$$\sum_{p\leqslant x}{}' \ldots = \sum_{p\leqslant x,\left(\frac{5}{p}\right)=1} \ldots .$$

Вводим величину

$$r(\varepsilon_0, p) = \frac{p-1}{o(\varepsilon_0, p)}.$$

Рассмотрим поле $K_n = \mathbb{Q}\left(\varepsilon_0^{\frac{1}{n}}, \zeta_{2n}\right)$, где ζ_{2n} – примитивный корень $2n$-ой степени из 1. Пусть $\delta(n) = [K_n : \mathbb{Q}]$. В [12] доказано, что

$$\delta(n) = \begin{cases} n\varphi(n), & \text{если} \quad 2 \nmid n \ \text{ и } \ 5 \mid n; \\ 2n\varphi(n), & \text{если} \quad 2 \mid n \ \text{ и } \ 5 \mid n \\ & \text{или} \quad 2 \nmid n \ \text{ и } \ 5 \nmid n; \\ 4n\varphi(n), & \text{если} \quad 2 \mid n \ \text{ и } \ 5 \nmid n. \end{cases} \qquad (3)$$

Можно показать, что если $p \nmid 5n$, то p вполне разложимо в поле K_n тогда и только тогда, когда $n \mid r(\varepsilon_0, p)$ (ср. [12, 14, 16]). Введем величину

$$\pi^{(1)}(x,n) = \#\left\{p \leqslant x \mid \left(\frac{5}{p}\right) = 1,\, n \mid r\,(\varepsilon_0, p)\right\}.$$

Лемма 2 (плотностная теорема Чеботарева)**.**

1) *Пусть верна РГР для дзета функции Дедекинда поля K_n. Тогда*

$$\pi^{(1)}(x,n) = \frac{1}{\delta(n)}\operatorname{li} x + O(x^{\frac{1}{2}}\log(xn)),$$

где

$$\operatorname{li} x = \int_2^x \frac{dt}{\log t}.$$

2) *Безусловный вариант: если $n \leqslant (\log x)^{1/7}$, то существует абсолютная константа $A > 0$ такая, что*

$$\pi^{(1)}(x,n) = \frac{1}{\delta(n)}\operatorname{li} x + O\left(x\exp\left(-A\sqrt{\log x}/n\right)\right).$$

Доказательство см. в [17, 12].

Основная цель настоящего параграфа – исследовать сумму

$$\sum_{p\leqslant x}{}' \log r(\varepsilon_0, p).$$

Имеем

$$\sum_{p\leqslant x}{}' \log r(\varepsilon_0, p) = \sum_{n\leqslant x} \Lambda(n)\pi^{(1)}(x,n), \tag{4}$$

где $\Lambda(n)$ – функция Мангольдта. Из пункта 2) леммы 2 непосредственно следует (ср. [14]), что

$$\sum_{p\leqslant x}{}' \log r(\varepsilon_0, p) \gtrsim C \cdot \operatorname{li} x,$$

где

$$C = \sum_{n=1}^{\infty} \Lambda(n)/\delta(n)$$

и $F(x) \lesssim G(x)$ означает, что для каждого $\varepsilon > 0$ существует x_ε такое, что

$$F(x) \leqslant (1+\varepsilon)G(x)$$

при $x > x_\varepsilon$.

Теорема 1. *Пусть верна РГР* (ε_0), *расширенная гипотеза Римана для дзета функций Дедекинда всех полей* K_n, $n = 1, 2, 3, \dots$. *Тогда*

$$\sum_{p\leqslant x}{}' \log r(\varepsilon_0, p) \ll \frac{x\log\log x}{\log x}.$$

Для доказательства воспользуемся равенством (4). Имеем

$$\sum_{p\leqslant x}{}' \log r(\varepsilon_0, p) =$$

$$= \sum_{n\leqslant\sqrt{x}/\log^3 x} \Lambda(n)\pi^{(1)}(x,n) + \sum_{\sqrt{x}/\log^3 x<n\leqslant x} \Lambda(n)\pi^{(1)}(x,n) =$$

$$= \sum\nolimits_1 + \sum\nolimits_2 .$$

К первой сумме применим плотностную теорему Чеботарева (пункт 1) леммы 2). Имеем

$$\sum\nolimits_1 \ll \sum_{n\leqslant\sqrt{x}/\log^3 x} (\log n)\left\{\frac{x\log\log n}{n^2\log x} + O\left(\sqrt{x}\log(xn)\right)\right\} \ll \pi(x).$$

Пусть q означает простое число. Сумму $\sum_2$ разбиваем на две суммы:

$$\sum\nolimits_2 = \sum_{q>\sqrt{x}/\log^3 x} (\log q)\pi^{(1)}(x,q) + \sum_{\substack{q^\alpha>\sqrt{x}/\log^3 x,\\ \alpha>1}} (\log q)\pi(x,q^\alpha) =$$

$$= \sum\nolimits_{2,1} + \sum\nolimits_{2,2} .$$

Оцениваем сумму $\sum_{2,2}$:

$$\sum\nolimits_{2,2} \leqslant \sum_{\substack{q^\alpha>\sqrt{x}/\log^3 x,\\ \alpha>1}} (\log q)\frac{x}{q^\alpha} \ll x \sum_{q>\sqrt{x}/\log^3 x} \frac{\log q}{q^2} \ll \pi(x).$$

В свою очередь сумму $\sum_{2,1}$ разбиваем на две суммы:

$$\sum\nolimits_{2,1} = \sum_{\sqrt{x}/\log^3 x<q\leqslant\sqrt{x}\log x} (\log q)\pi^{(1)}(x,q) +$$

$$+\sum_{q>\sqrt{x}\log x}(\log q)\pi^{(1)}(x,q)=\sum\nolimits_{2,1,1}+\sum\nolimits_{2,1,2}.$$

Сумма $\sum_{2,1,2}$ ограничена сверху величиной

$$\#\left\{p\mid p \text{ делит } \prod_{m\leqslant\sqrt{x}/\log x}|N(\varepsilon_0^m-1)|\right\}\cdot\log x\ll\pi(x).$$

Чтобы оценить $\sum_{2,1,1}$, используем теорему Бруна–Титчмарша и формулу Мертенса. Напомним, что

$$\pi(x,a,k)=\#\{p\leqslant x\mid p\equiv a\pmod k\};$$

По теореме Бруна–Титчмарша, для $(a,k)=1$ и $k\leqslant x$

$$\pi(x,a,k)<\frac{(2+\eta)x}{\varphi(k)\log(2x/k)}$$

($\eta>0$ и $x>x_0(\eta)$). Имеем

$$\sum\nolimits_{2,1,1}\ll\sum_{\sqrt{x}/\log^3 x<q\leqslant\sqrt{x}\log x}(\log q)\pi(x,1,q)\ll$$

$$\ll\frac{x}{\log x}\sum_{\sqrt{x}/\log^3 x<q\leqslant\sqrt{x}\log x}\frac{\log q}{q}\ll\frac{x\log\log x}{\log x},$$

и теорема доказана.

Из теоремы 1 вытекают интересные следствия. Формула (2), в частности, дает

$$\varepsilon_0^{i(p)}=F_{i(p)-1}+\varepsilon_0F_{i(p)}.$$

Ясно, что $\varepsilon_0^{i(p)}$ – фундаментальная единица порядка $\mathfrak{O}_p=\{1,p\varepsilon_0\}$ квадратичного поля $\mathbb{Q}(\sqrt{5})$, а $i(p)$ – индекс группы единиц порядка $\mathfrak{O}_p$ в группе единиц максимального порядка $\mathfrak{O}=\{1,\varepsilon_0\}$ поля $\mathbb{Q}(\sqrt{5})$.

Пусть $\bar{h}(d)$ – число классов несобственно эквивалентных примитивных бинарных квадратичных форм $ax^2+bxy+cy^2$ дискриминанта $d=b^2-4ac$. Справедливо соотношение

$$h(5p^2)=\begin{cases}2\bar{h}(5p^2), & \text{если } i(p) \text{ четно };\\ \bar{h}(5p^2), & \text{если } i(p) \text{ нечетно }.\end{cases}$$

Нам необходим частный случай формулы Гаусса (см. [18, 19]):

$$\bar{h}(5p^2) = \frac{p - \left(\frac{5}{p}\right)}{i(p)} = \frac{p-1}{i(p)}.$$

Легко показать, что

$$\lambda(p) = 2^{\beta} i(p), \quad \text{где} \quad \beta = 0 \ \text{ или } \ 1, \text{ или } 2.$$

Теорема 1 и указанные выше соотношения дают следующий результат.

Теорема 2. *Пусть верна РГР* (ε_0)*. Тогда*

$$\sum_{p\leqslant x}{}' \log h(5p^2) \ll \frac{x \log\log x}{\log x}.$$

Следствие 1. *Пусть* $\alpha(x)$ *– сколь угодно медленно монотонно возрастающая положительная функция с условием* $\alpha(x) \to \infty$ $(x \to \infty)$*. Если верна РГР* (ε_0)*, то имеем*

$$\# \left\{ p \leqslant x \mid \left(\frac{5}{p}\right) = 1,\, h(5p^2) > (\log p)^{\alpha(p)} \right\} = \\ = o(\pi(x)), \quad x \to \infty.$$

Замечание 1. Можно предположить, что при $x \to \infty$

$$\sum_{p\leqslant x}{}' \log r(\varepsilon_0, p) \sim c' \operatorname{li} x, \tag{5}$$

где $c' > 0$, и, как следствие, что

$$\sum_{p\leqslant x}{}' \log h(5p^2) \asymp \operatorname{li} x.$$

Из гипотетической оценки

$$\sum_{p\leqslant x}{}' \log h(5p^2) \ll \operatorname{li} x$$

вытекает, что

$$\# \left\{ p \leqslant x \mid \left(\frac{5}{p}\right) = 1,\, h(5p^2) > \alpha(p) \right\} = o(\pi(x)).$$

В последующей работе последнее соотношение будет выведено из РГР (ε_0) методом, сходным с использованным ниже методом доказательства теоремы 5.

§2

В настоящем параграфе рассматривается поведение суммы

$$\sum_{p\leqslant x}\log r(a,p), \tag{6}$$

где $a\geqslant 2$ – натуральное число,

$$r(a,p)=\frac{p-1}{o(a,p)}.$$

Эта сумма вполне аналогична сумме

$$\sum_{p\leqslant x}{}'\log r(\varepsilon_0,p).$$

Изучение суммы (6) представляет интерес, в частности, в связи с гипотезой (5). Гипотеза

$$\sum_{p\leqslant x}\log r(a,p)\sim c(a)\mathrm{li}\,x$$

($a>1$, $x\to\infty$) была выдвинута в работе [20]; там же она подтверждалась на численном материале (при $a=2,3,5$). В работе [14] было показано, что

$$\sum_{p\leqslant x}\log r(2,p)\gtrsim \gamma\,\mathrm{li}\,x,$$

где

$$\gamma=\sum_{n=1}^{\infty}\frac{\Lambda(n)}{\delta(n)},\qquad \delta(n)=[\mathbb{Q}(2^{1/n},\zeta_n):\mathbb{Q}],$$

и что при выполнении РГР для дзета функций Дедекинда полей $\mathbb{Q}(2^{1/n},\zeta_n)$ справедлива оценка

$$\sum_{p\leqslant x}\log r(2,p)\ll\frac{x\log\log x}{\log x}.$$

В настоящем параграфе без каких-либо гипотез доказывается, что оценка

$$\sum_{p\leqslant x}\log r(a,p)\ll \mathrm{li}\,x$$

верна в среднем по a. Доказательство использует метод Стефенса [9, II]. Пусть $N > \exp\{c_1(\log x)^{1/2}\}$, $c_1 > 0$,

$$S_1 = N^{-1} \sum_{a \leqslant N} \sum_{p \leqslant x} \log r(a,p).$$

Наша задача – дать точную по порядку оценку сверху суммы S_1. Для характера χ по модулю p и для $r \mid (p-1)$ введем величину

$$c_r(\chi) = (1/(p-1)) \sum_a{}' \chi(a), \tag{7}$$

где a пробегает по всем целым числам порядка $(p-1)/r$ в интервале длины p.

Используя (7), имеем

$$S_1 = N^{-1} \sum_{a \leqslant N} \sum_{p \leqslant x} \sum_{\substack{w \mid (p-1), \\ o(a,p)=(p-1)/w}} \log w =$$

$$= N^{-1} \sum_{a \leqslant N} \sum_{p \leqslant x} \sum_{w \mid (p-1)} \log w \sum_{\chi \pmod p} c_w(\chi)\chi(a) =$$

$$= N^{-1} \sum_{p \leqslant x} \sum_{w \mid (p-1)} \log w \sum_{\chi \pmod p} c_w(\chi) \sum_{a \leqslant N} \chi(a).$$

В суммировании $\sum_{\chi \pmod p} \ldots$ выделим главный характер:

$$\sum_{\chi \pmod p} \ldots = \sum_{\chi_0} \ldots + \sum_{\chi \neq \chi_0} \ldots .$$

Нам потребуется следующий результат из [9, II], который мы сформулируем в виде леммы. Предварительно введем обозначение, которое используется ниже: порядок характера χ обозначается либо через k, либо через $\operatorname{ord}\chi$.

Лемма 3. *Если* $\chi \neq \chi_0$, *то*

$$|c_r(\chi)| \leqslant (r,k)/rk; \tag{8}$$

далее,

$$c_r(\chi_0) = \varphi((p-1)/r)/(p-1). \tag{9}$$

С помощью (8) и (9) имеем

$$S_1 = N^{-1}\sum_{p\leqslant x}\sum_{w\,|(p-1)}(\log w)\frac{\varphi((p-1)/w)}{p-1}([N]-[N/p])+$$

$$+O\left\{N^{-1}\sum_{p\leqslant x}\sum_{w\,|(p-1)}(\log w)\sum_{\chi\neq\chi_0}|c_w(\chi)|\left|\sum_{a\leqslant N}\chi(a)\right|\right\}=$$

$$=\sum_{p\leqslant x}\sum_{w\,|(p-1)}(\log w)\frac{\varphi((p-1)/w)}{p-1}+O(N^{-1}\mathrm{li}\,x)+$$

$$+O((\log x)^2\log\log x)+$$

$$+O\left\{N^{-1}\sum_{p\leqslant x}\sum_{w\,|(p-1)}(\log w)\sum_{\chi\neq\chi_0}\frac{(\mathrm{ord}\,\chi,w)}{w\cdot\mathrm{ord}\,\chi}\left|\sum_{a\leqslant N}\chi(a)\right|\right\}=$$

$$=P_1+I_1+I_2+P_2.$$

Член I_1 получается при помощи оценки

$$\sum_{p\leqslant x}\sum_{w\,|(p-1)}(\log w)\frac{\varphi((p-1)/w)}{p-1}\leqslant$$

$$\leqslant\sum_{p\leqslant x}\sum_{w\,|(p-1)}\frac{\log w}{w}\leqslant C\mathrm{li}\,x+O(x/(\log x)^D),$$

где D – произвольная константа >1; подробности см. ниже при рассмотрении P_1.

Член I_2 получается при помощи оценки

$$\sum_{p\leqslant x}\frac{1}{p}\sum_{w\,|(p-1)}\frac{\log w}{w}\ll\sum_{p\leqslant x}\frac{1}{p}(\log p)d(p-1)\ll(\log x)^2\log\log x.$$

Введем обозначение

$$S_2=\sum_{p\leqslant x}d(p-1)\sum_{\chi\neq\chi_0}\frac{(\mathrm{ord}\,\chi,w)}{w\cdot\mathrm{ord}\,\chi}\left|\sum_{1\leqslant N}\chi(a)\right|.$$

Тогда

$$P_2=O(N^{-1}(\log x)S_2).$$

Пусть $\sum^*$ означает суммирование по примитивным характерам. Имеем

$$S_2 \ll \sum_{p\leqslant x} d(p-1) \sum_{\chi \,(\mathrm{mod}\ p)}{}^{*} (1/\operatorname{ord}\chi) \left|\sum_{a\leqslant N} \chi(a)\right|.$$

По неравенству Гельдера, получаем

$$S_2^{2r} \leqslant \left\{ \sum_{p\leqslant x} d(p-1)^{2r/(2r-1)} \sum_{\chi \,(\mathrm{mod}\ p)}{}^{*} k^{-2r/(2r-1)} \right\}^{2r-1} \times$$

$$\times \sum_{p\leqslant x} \sum_{\chi \,(\mathrm{mod}\ p)}{}^{*} \left|\sum_{a\leqslant N} \chi(a)\right|^{2r};$$

$r \geqslant 1$ – целое число. Очевидно,

$$\sum_{\chi \,(\mathrm{mod}\ p)}{}^{*} k^{-2r/(2r-1)} \ll d(p-1).$$

Хорошо известно (М. Б. Барбан [21]), что

$$\sum_{p\leqslant x} d^l(p-1) \asymp x(\log x)^{2^l-2}, \tag{10}$$

где $l \in \mathbb{N}$. Нам необходима оценка (см. [9, II]):

$$\sum_{d\leqslant K} \sum_{\chi \,(\mathrm{mod}\ d)}{}^{*} \left|\sum_{a\leqslant N} \chi(a)\right|^{2r} \ll$$

$$\ll (K^2+N^r) \sum_{a\leqslant N^r} \{\tau_r'(a)\}^2, \tag{11}$$

где $\tau_r'(a)$ – количество способов записи a в виде упорядоченного произведения r множителей, каждый из которых не превосходит N. Используя (10) при $l=3$ и (11) при $K=x$, получаем

$$S^{2r} \ll \{c_2 x \log^6 x\}^{2r-1}(x^2+N^r) \sum_{a\leqslant N^r} \{\tau_r'(a)\}^2, \tag{12}$$

где $c_2>0$ – константа. Нам потребуются результаты из [9, II], которые мы оформим в виде следующей леммы.

Лемма 4. 1) *Если* $x^2 \geqslant N > \exp\{c_1(\log x)^{1/2}\}$, *то*

$$x^{-1/2r}\{\Psi(N, 9\log x)\}^{1/2} \ll$$
$$\ll \exp\{-c_3(\log x)^{1/2}/\log\log x\}, \tag{13}$$

где

$$r = [2\log x/\log N] + 1 \tag{14}$$

и $c_3 > 0$ *при условии, что константа* c_1 *достаточно велика;*

$$\Psi(v, y) = \sum_{\substack{n \leqslant v,\\ p(n) \leqslant y}} 1$$

и $p(n)$ *означает наибольший простой делитель* n.

2) *Если* $N^r \leqslant x^8$, *то*

$$\sum_{a \leqslant N^r} \{\tau_r'(a)\}^2 < N^r\{\Psi(N, 9\log x)\}^r. \tag{15}$$

Выберем r как в (14). Если $N > x^2$, то $r = 1$, и из (12) следует оценка

$$S_2 \ll x^{1/2}(\log x)^3 N.$$

Если $x^2 \geqslant N > \exp\{c_1(\log x)^{1/2}\}$, то $r \geqslant 2$ и (12), (15), (13) дают

$$S_2 \ll xN(\log x)^{6\frac{2r-1}{2r}} \exp\{-c_3(\log x)^{1/2}/\log\log x\}.$$

Обратимся теперь к члену P_1. Имеем

$$P_1 = \sum_{p \leqslant x} \sum_{w|(p-1)} \frac{\log w}{w} \frac{\varphi((p-1)/w)}{(p-1)/w} \leqslant$$
$$\leqslant \sum_{p \leqslant x} \sum_{w|(p-1)} \frac{\log w}{w} \leqslant \sum_{n \leqslant x} \frac{\log n}{n} \pi(x, 1, n) \leqslant$$
$$\leqslant \sum_{2 \leqslant n \leqslant (\log x)^A} \pi(x, 1, n)\frac{\log n}{n} + \sum_{n > (\log x)^A} \pi(x, 1, n)\frac{\log n}{n} = S_3 + T_1.$$

Сумма S_3 вычисляется с помощью теоремы Зигеля–Вальфиша (см. [22]). Имеем

$$S_3 = \operatorname{li} x \sum_{2 \leqslant n \leqslant (\log x)^A} \frac{\log n}{n\varphi(n)} + O(x/(\log x)^B),$$

где B – произвольная константа > 1.

Сумма T_1 оценивается с помощью теоремы Бруна–Титчмарша. Имеем

$$T_1 \ll \sum_{n>(\log x)^A} \frac{\log n}{n} \frac{x}{\varphi(n)} \ll x/(\log x)^{B(A)},$$

где константа $B(A) > 0$ достаточно велика при достаточно большом A.

Тем самым, доказана

Теорема 3. *Пусть* $N > \exp\{c_1(\log x)^{1/2}\}$ *и константа* $c_1 > 0$ *достаточно велика. Тогда*

$$N^{-1} \sum_{a\leqslant N} \sum_{p\leqslant x} \log r(a,p) \leqslant C \operatorname{li} x + O(x/\log x)^D),$$

где

$$C = \sum_{n=2}^{\infty} \frac{\log n}{n\varphi(n)},$$

D *– произвольная константа* > 1.

§3

В настоящем параграфе простые числа обозначаются не только буквой p, но и q. Введем обозначение:

$$N_{\varepsilon_0,w}(x) = \#\left\{p \leqslant x \middle| \left(\frac{5}{p}\right) = 1,\ r(\varepsilon_0, p) = w\right\}.$$

Теорема 4. *Пусть верна РГР* (ε_0). *Тогда для любого* $\varepsilon > 0$ *справедлива асипмтотика*

$$N_{\varepsilon_0,w}(x) = A(\varepsilon_0, w) \operatorname{li} x + O\left\{w^{\varepsilon}(\log\log x)\frac{x}{(\log x)^2}\right\}, \qquad (16)$$

где

$$A(\varepsilon_0, w) = \begin{cases} \frac{27}{38}Ag(w), & \text{если} \quad (w,10) = 1; \\ \frac{9}{38}Ag(w), & \text{если} \quad (w,10) = 2; \\ \frac{3}{2}Ag(w), & \text{если} \quad (w,10) = 5; \\ \frac{1}{2}Ag(w), & \text{если} \quad (w,10) = 10; \end{cases} \qquad (17)$$

$$A = \prod_q \left(1 - \frac{1}{q(q-1)}\right) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n\varphi(n)} =$$
$$= 0.373955813619202\ldots \textit{(константа Артина)};$$

$$g(w) = \frac{1}{w^2} \prod_{q|w} \frac{q^2-1}{q^2-q-1}.$$

O-константа зависит только от ε.

Замечание 2. Результат можно формулировать в терминах чисел Фибоначчи, так как

$$N_{\varepsilon_0,w}(x) = \#\left\{p \leqslant x \Big| \left(\frac{5}{p}\right) = 1, \lambda(p) = \frac{p-1}{w}\right\}.$$

Доказательство теоремы основано на результатах работ [10, 11, 13]. Мы приведем лишь вычисление плотности $A(\varepsilon_0, w)$, существование которой в очень общей ситуации (вместе с соответствующей формулой) было доказано Ленстрой [10]. При этом использовалась некоторая РГР. Получение асимптотической формулы с остаточным членом (16) идет (с использованием РГР (ε_0)) по схеме работы [13], однако вывод остаточного члена нами не приводится. Отметим, что для $w = 1$ теорема была доказана в [12].

Из общей формулы Ленстры (см. [10, Th. 3.1]) следует, что

$$A(\varepsilon_0, w) = \sum_{k \in \mathbb{N}} \frac{\mu(k)}{\delta(kw)},$$

где

$$\delta(kw) = [K_{kw} : \mathbb{Q}].$$

Используя формулу (3), получаем

$$A(\varepsilon_0, w) = \frac{1}{2} \sum_{k \in \mathbb{N}} \frac{\mu(k)}{kw\varphi(kw)} + \frac{1}{2} \sum_{\substack{k \in \mathbb{N}, \\ 2 \nmid kw}} \frac{\mu(k)}{kw\varphi(kw)} -$$
$$-\frac{1}{4} \sum_{\substack{k \in \mathbb{N}, \\ 5 \nmid kw}} \frac{\mu(k)}{kw\varphi(kw)} - \frac{1}{4} \sum_{\substack{k \in \mathbb{N}, \\ 2 \nmid kw, \\ 5 \nmid kw}} \frac{\mu(k)}{kw\varphi(kw)}.$$

Введем сумму [11]

$$S(h,t,m)=\sum_{k=1}^{\infty}\frac{\mu(k)(kt,h)}{kt\varphi(kt)}.$$

Имеем

$$A(\varepsilon_0,w)=\frac{1}{2}S(1,w,1)-\frac{1}{4}S(1,w,2)+\frac{1}{2}S(1,w,5)-\frac{1}{4}S(1,w,10).$$

Сумма $S(1,w,m)$ преобразуется к виду

$$S(1,w,m)=\mu(M)Ag(w)\prod_{q|(M,w)}\frac{1}{q^2-1}\prod_{\substack{q|M,\\ q\nmid w}}\frac{1}{q^2-q-1},$$

где

$$M=m/(m,w).$$

Удобно рассматривать отдельно случаи: $(w,10)=1$, $(w,10)=2$, $(w,10)=5$, $(w,10)=10$. После некоторых вычислений получаем выражение (17) для $A(\varepsilon_0,w)$.

Из теоремы 4 выводится доказательство аналога гипотезы 3 Холи (см. §0) для последовательности дискриминантов

$$\left\{5p^2\middle|\left(\frac{5}{p}\right)=1\right\}.$$

Сначала доказываем (ср. [11]), что

$$\sum_{w=1}^{\infty}A(\varepsilon_0,w)=\frac{1}{2},$$

а также, что (ср. [13])

$$\sum_{w\leqslant z}A(\varepsilon_0,w)=\frac{1}{2}+O(z^{-1}).$$

Справедливо соотношение (как всегда, $\left(\frac{5}{p}\right)=1$)

$$h(5p^2)=2^{\gamma}r(\varepsilon_0,p),$$

где γ – одно из чисел 0, 1, 2, 3. Вводим величины

$$N(x,\alpha)=\#\left\{p\leqslant x\middle|\left(\frac{5}{p}\right)=1,\ h(5p^2)>\alpha\right\},$$

$$N_0(x,\alpha) = \#\left\{p \leqslant x \middle| \left(\frac{5}{p}\right) = 1,\ r(\varepsilon_0, p) > \alpha\right\}.$$

Имеем

$$\#\left\{p \leqslant x \middle| \left(\frac{5}{p}\right) = 1\right\} = \#\left\{p \leqslant x \middle| \left(\frac{5}{p}\right) = 1,\ r(\varepsilon_0, p) \leqslant \alpha\right\} +$$

$$+\#\left\{p \leqslant x \middle| \left(\frac{5}{p}\right) = 1,\ r(\varepsilon_0, p) > \alpha\right\} = K + N_0(x,\alpha).$$

Хорошо известно, что

$$\#\left\{p \leqslant x \middle| \left(\frac{5}{p}\right) = 1\right\} = \frac{1}{2}\operatorname{li} x + O(x/\log^2 x).$$

По теореме 4 выполняется асимптотика

$$K = \sum_{w=1}^{[\alpha]} A(\varepsilon_0, w) \cdot \operatorname{li} x + O\left\{\sum_{w=1}^{[\alpha]} \frac{w^{\varepsilon}(\log\log x)x}{\log^2 x}\right\}.$$

Поэтому справедливо соотношение

$$\lim_{x\to\infty} \frac{N_0(x,\alpha)}{\operatorname{li} x} = \frac{1}{2} - \sum_{w=1}^{[\alpha]} A(\varepsilon_0, w).$$

В силу сказанного выше, имеем

$$\sum_{w=1}^{[\alpha]} A(\varepsilon_0, w) = \frac{1}{2} - B\alpha^{-1},$$

где

$$0 < C_2 < B < C_1,$$

C_1, C_2 – константы. Тем самым, доказана следующая

Теорема 5. 1) *Справедливо соотношение*

$$N_0(x,\alpha) \leqslant N(x,\alpha) \leqslant N_0\left(x, \frac{\alpha}{8}\right).$$

2) *В предположении верности РГР* (ε_0) *при* $\alpha \to \infty$ *имеем*

$$\lim_{x\to\infty} \frac{N_0(x,\alpha)}{\operatorname{li} x} \asymp \alpha^{-1}.$$

Замечание 3. Легко доказать асимптотику ($x \to \infty$)

$$\sum_{w \leqslant x} wA(\varepsilon_0, w) \sim c'' \log x,$$

где $c'' > 0$. Поэтому можно предположить, что ($x \to \infty$)

$$\sum_{p \leqslant x}{}' r(\varepsilon_0, p) \sim c'' x$$

и, как следствие, что

$$\sum_{p \leqslant x}{}' h(5p^2) \asymp x.$$

§4

Теорема 6. *Пусть верна РГР (ε_0). Тогда*

$$\# \left\{ p \leqslant x \middle| \left(\frac{5}{p}\right) = 1,\, h(5p^2) = 2 \right\} \sim \frac{9}{19} A \operatorname{li} x,$$

где

$$\frac{9}{19} A = 0.17713696434593\ldots.$$

Остановимся на основных моментах доказательства. Пусть

$$S = \left\{ p \middle| \left(\frac{5}{p}\right) = 1,\, \lambda(p) = p - 1 \right\}.$$

Тогда (см. [12] или теорему 4)

$$\# \left\{ p \leqslant x \middle| \left(\frac{5}{p}\right) = 1,\, \lambda(p) = p - 1 \right\} \sim \frac{27}{38} A \operatorname{li} x,$$

где $\frac{27}{38} A = 0.265705\ldots$.

Рассмотрим простые числа $p \in S$. Используя несложные рассуждения, имеем

1) если $p \equiv 3 \pmod 4$, то $i(p) = \lambda(p) = p - 1$ – четное число, и

$$h(5p^2) = 1;$$

2) если $p \equiv 1 \pmod 4$, то либо $i(p) = \frac{\lambda(p)}{2} = \frac{p-1}{2}$ – четное число, либо $i(p) = \frac{\lambda(p)}{4} = \frac{p-1}{4}$ – нечетное число, и в обоих случаях

$$h(5p^2) = 4.$$

Дальнейшее исследование показывает, что простые числа вида $p \equiv 5 \pmod 8$ исключаются из рассмотрения, поскольку для них $\lambda(p) \neq p-1$. Далее, можно показать, что для простых чисел из множества

$$\left\{ p \middle| \left(\frac{5}{p}\right) = 1,\ \lambda(p) = \frac{p-1}{2} \right\}$$

имеем

$$h(5p^2) = 4 \quad \text{или} \quad 8.$$

Следовательно, если разбить множество S на два подмножества,

$$S = M_3 \smile M_1,$$

в соответствии с $p \equiv 3 \pmod 4$ и $p \equiv 1 \pmod 4$, то

$$p \in M_3 \Longleftrightarrow h(5p^2) = 2.$$

Рассмотрим плотности $d(S)$, $d(M_3)$, $d(M_1)$. Имеем

$$d(S) = d(M_3) + d(M_1).$$

Можно показать (ср. [10, Th. 8.1]), что

$$d(M_3) = 2d(M_1).$$

По сказанному выше,

$$d(S) = \frac{27}{38}A,$$

откуда следует, что

$$d(M_3) = \frac{9}{19}A.$$

Литература

1. C. F. Gauss, *Disquisitiones Arithmeticae,* 1801; русский перевод в книге: К. Ф. Гаусс, Труды по теории чисел, М., 1959.
2. Е. П. Голубева, *О длинах периодов разложения в непрерывеную дробь квадратичных иррациональностей и числах классов вещественных квадратичных полей. I; II,* Зап. научн. семин. ЛОМИ **160** (1987), 72–81; **168** (1988), 11–22.
3. C. Hooley, *On the Pellian equation and the class number of indefinite binary quadratic forms,* J. reine und angew. Math. **353** (1984), 98–131.
4. Е. П. Голубева, *О неопределенных бинарных квадратичных формах с большим числом классов,* Зап. научн. семин. ЛОМИ, **185** (1990), 13–21.
5. M. Goldfeld, *On the number of primes p for which p+a has a large prime factor,* Mathematika **16**, No. 1 (1969), 23–27.

6. P. C. Sarnak, *Class numbers of indefinite binary quadratic forms. II,* J. Number Theory **21**, No. 3 (1985), 333–346.
7. Е. П. Голубева, *О числах классов вещественных квадратичных полей дискриминанта 4p,* Зап. научн. семин. ПОМИ **204** (1993), 11–36.
8. C. Hooley, *On Artin's conjecture,* J. reine und angew. Math. **225** (1967), 209–220.
9. P. J. Stephens, *Prime divisors of second-order linear recurrences. I; II,* J. Number Theory **8**, No. 3 (1976), 313–332; 333–345.
10. H. W. Lenstra Jr., *On Artin's conjecture and Euclid's algorithm in global fields,* Invent. Math. **42** (1977), 201–224.
11. S. S. Wagstaff Jr., *Pseudoprimes and a generalization of Artin's conjecture,* Acta Arithm. **41** (1982), 141–150.
12. J. A. Antoniadis, *Über die Periodenlänge mod p einer Klasse rekursiver Folgen,* Arch. Math. **42**, No. 3 (1984), 242–252.
13. L. Murata, *A problem analogous to Artin's conjecture for primitive roots and its applications,* Arch. Math. **57** (1991), 555–565.
14. F. Pappalardi, *On Hooley's theorem with weights,* Rendiconti Sem. Mat. Univ. Pol. Torino **53**, No. 4 (1995), 375–388.
15. P. Bundschuh and J.-S. Shiue, *A generalization of a paper by D. D. Wall,* Rendiconti d. Accad. Naz. dei Lincei. Ser. 8, **56**, No. 2 (1974), 135–144.
16. P. J. Weinberger, *On euclidean rings of algebraic integers,* Analytic Number Theory (Proc. Symp. Pure Math., **24**), Providence, R. I., 1973, 321–332.
17. J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem,* Algebraic Number Fields (Ed. A. Fröhlich), New York, 1977, 409–464.
18. Б. А. Венков, *Элементарная теория чисел,* М.-Л., 1937.
19. З. И. Боревич, И. Р. Шафаревич, *Теория чисел,* М., 1985.
20. E. Bach, R. Lukes, J. Shallit, and H. C. Williams, *Results and estimates on pseudopowers,* Math. Comp. **65** (1996), 1737–1747.
21. М. Б. Барбан, *Мультипликативные функции от $^{\Sigma}R$-равнораспределенных последовательностей,* Изв. АН Уз. ССР. Серия физ.-мат. наук, No. 6 (1964), 13–19.
22. К. Прахар, *Распределение простых чисел,* М., 1967.

С.-Петербургское отделение
Математического института
им. В. А. Стеклова РАН
E-mail:fomenko@pdmi.ras.ru

Поступило 26 марта 2001 г.