Записки научных
семинаров ПОМИ
Том 286, 2002 г.

О. М. Фоменко

О ЧИСЛАХ КЛАССОВ НЕОПРЕДЕЛЕННЫХ БИНАРНЫХ КВАДРАТИЧНЫХ ФОРМ И ВЫЧЕТНЫХ ИНДЕКСАХ ЦЕЛЫХ ЧИСЕЛ ПО ПРОСТОМУ МОДУЛЮ p

§0

В этом параграфе мы введем необходимые определения и сформулируем некоторые из полученных в работе результатов.

Пусть $a \geqslant 2$ – целое число, p – простое число; если $p \nmid a$, то $o(a,p)$ означает наименьшее целое $d > 0$ такое, что $a^d \equiv 1 (\mathrm{mod}\ p)$; $o(a,p)$ называется порядком числа a по модулю p. Очевидно, $o(a,p) \,|\, (p-1)$; отношение

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

называется вычетным индексом числа a по модулю p.

Пусть $\varepsilon_0 = \frac{1+\sqrt{5}}{2}$; $\{F_m\}$ – последовательность чисел Фибоначчи, где $F_0 = 0$, $F_1 = 1$, $F_m = F_{m-2} + F_{m-1}$. Известно, что

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

Пусть $\left(\frac{5}{p}\right) = 1$. $o(\varepsilon_0, p)$ определяется как наименьшее $d > 0$ такое, что в соотношении $\varepsilon_0^d = F_{d-1} + \varepsilon_0 F_d$ имеем $F_{d-1} \equiv 1 (\mathrm{mod} p)$, $F_d \equiv 0 (\mathrm{mod} p)$. Известно, что при $p > 2$, $p \neq 5$ и $\left(\frac{5}{p}\right) = 1$ имеет место делимость $o(\varepsilon_0, p) \,|\, (p-1)$. В этом случае определяем вычетный индекс числа ε_0 по модулю p следующим образом:

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

Интерес к изучению $r(\varepsilon_0, p)$ вызван, в частности, тем, что

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

где γ – одно из чисел 0, 1, 2, 3; $h(d)$ – число классов собственно эквивалентных примитивных бинарных квадратичных форм

$ax^2+bxy+cy^2$ дискриминанта $d=b^2-4ac$; см. [1]. $r(a,p)$ и $r(\varepsilon_0,p)$ обладают сходными свойствами и могут изучаться параллельно сходными методами.

Аналогичная ситуация имеет место для $\left(\frac{5}{p}\right)=-1$, причем теперь $o(\varepsilon_0,p)\mid 2(p+1)$. Ниже при рассмотрении $r(\varepsilon_0,p)$ и $h(5p^2)$ всегда предполагается, что $\left(\frac{5}{p}\right)=1$, кроме нескольких специально отмеченных случаев.

Пусть $K_n=\mathbb{Q}(a^{1/n},\zeta_n)$, где ζ_n – примитивный корень степени n из 1; РГР(a) – расширенная гипотеза Римана для дзета-функций Дедекинда полей вида K_n, $n=1,2,3,\dots$. Первый значительный результат о распределении значений $r(a,p)$ принадлежит Холи [2], который в предположении справедливости РГР(a) доказал гипотезу Артина:

$$\#\{p\leqslant x\mid r(a,p)=1\}=A(a,1)\operatorname{li}x+O\left(\frac{x\log\log x}{\log^2 x}\right);$$

$$A(a,1)>0;\quad a\neq\pm1,a_1^2.$$

Затем Стефенс [3] получил сходную асимптотику для

$$\#\{p\leqslant x\mid r(a,p)=w\}$$

(см. также [4]).

По поводу проблематики, связанной с $r(\varepsilon_0,p)$ и $h(5p^2)$, см. [1, 5–7].

Приведем гипотезы о поведении $r(a,p)$ и $r(\varepsilon_0,p)$ в среднем ($C_1(a)$, $C_2(a)$, C_1, C_2 – положительные константы; $a\geqslant 2$ – бесквадратное целое число).

Гипотеза 1(a).

$$\sum_{p\leqslant x}r(a,p)\sim C_1(a)x.$$

Гипотеза 2(a).

$$\sum_{p\leqslant x}\log r(a,p)\sim C_2(a)\operatorname{li}x.$$

Гипотеза 1(ε_0).

$$\sum_{p\leqslant x,\left(\frac{5}{p}\right)=1}r(\varepsilon_0,p)\sim C_1x.$$

Гипотеза 2(ε_0).

$$\sum_{p\leqslant x,\left(\frac{5}{p}\right)=1} \log r(\varepsilon_0, p) \sim C_2 \operatorname{li} x.$$

Перечисленные гипотезы выдвигались в работах [1, 6–8]. Свидетельства в пользу указанных гипотез можно найти в цитированных выше работах. Результаты настоящей статьи также в той или иной мере подтверждают эти гипотезы.

Сформулируем некоторые из результатов настоящей работы в терминах бинарных квадратичных форм. Пусть $K'_n = \mathbb{Q}(\varepsilon_0^{1/n}, \zeta_{2n})$; РГР($\varepsilon_0$) – расширенная гипотеза Римана для дзета-функций Дедекинда полей вида K'_n, $n = 1, 2, 3, \dots$.

Теорема 2(ε_0). *Пусть выполняется* РГР(ε_0)*. Пусть при* $x \to \infty$ *положительная функция* $\alpha(x)$ *монотонно возрастает и* $\alpha(x) \to \infty$. *Если*

$$\alpha(x) \leqslant (\log x)(\log\log x)^{-3},$$

то

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

Теорема 5(ε_0). *Для бесконечного множества* p, $\left(\frac{5}{p}\right) = 1$, *имеем*

$$h(5p^2) \geqslant (\log\log p)(\log_k p)^{-1},$$

где $\log_k p$ – k *раз итерированный логарифм,* k – *любое постоянное целое число* $\geqslant 3$.

Теорема 2 (ε_0) говорит о том, что для большинства дискриминантов вида $5p^2$, $\left(\frac{5}{p}\right) = 1$, числа классов $h(5p^2)$ малы и что в то же время множество $\left\{p \leqslant x \,\middle|\, \left(\frac{5}{p}\right) = 1\right\}$, $x \gg 0$, содержит не менее ($C > 0$)

$$C\frac{x(\log\log x)^3}{\log^2 x}$$

простых p с условием

$$h(5p^2) > (\log p)(\log\log p)^{-3}.$$

Теорема 5 (ε_0) показывает, что очень ослабленный вариант последнего факта можно доказать без использования каких-либо гипотез. Наконец, как отмечено ниже (см. замечание 1 и §5), имеется мало дискриминантов вида $5p^2$, $\left(\frac{5}{p}\right) = \pm 1$, с большим числом классов. Действительно, справедливо соотношение

$$\#\Big\{p \leqslant x \mid h(5p^2) > x^{1-\delta}\Big\} \ll x^{2\delta},$$

где δ – любое постоянное число с условием $0 < \delta < 1/2$. Доказательство этого факта также является безусловным.

Ниже в §§1–4 изучаются свойства $r(a,p)$ (теоремы $1(a)$–$7(a)$); в §5 изучаются свойства $r(\varepsilon_0, p)$ (и $h(5p^2)$) (теоремы $1(\varepsilon_0)$, $3(\varepsilon_0)$ и $4(\varepsilon_0)$); теоремы $2(\varepsilon_0)$ и $5(\varepsilon_0)$ приведены выше.

Обозначения. 1) p и q означают простые числа; суммирование

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

чаще записывается в эквивалентной форме $\sum'_{p\leqslant x} \dots$;

$$\pi(x) = \sum_{p \leqslant x} 1; \qquad \operatorname{li} x = \int\limits_2^x \frac{dt}{\log t}$$

2) В k раз итерированном логарифме $\log_k x$ $k \geqslant 3$ – произвольное постоянное целое число.

3) $a \geqslant 2$ – бесквадратное натуральное число, которое считается постоянным всегда, кроме теоремы $5(a)$.

4) c, C, C_1, $C(a), \dots$ – положительные константы.

5) K_n, РГР(a) и K_n', РГР(ε_0) определены выше; $\delta(n) = [K_n : \mathbb{Q}]$; $\delta'(n) = [K_n' : \mathbb{Q}]$.

§1

Пусть $N(x,a,w) = \#\{p \leqslant x \mid r(a,p) = w\}$, $w = 1, 2, 3, \dots$. В настоящем параграфе будет выведена условная асимптотическая формула для $N(x,a,w)$, $x \to \infty$, и получен аналог для $r(a,p)$ теоремы $2(\varepsilon_0)$ из §0.

Теорема 1(a). *Пусть верна* РГР(a). *Пусть* $w \leqslant \log x$. *Тогда*

$$N(x,a,w) = A(a,w)\,\mathrm{li}\,x + O\left(\frac{x\log\log x}{\varphi(w)\log^2 x}\right),$$

где

$$A(a,w) = \sum_{k=1}^{\infty}\frac{\mu(k)}{\delta(kw)}.$$

Доказательство. Мы следуем работе Стефенса [3] (который, в свою очередь, следовал работе Холи [2]), но более аккуратно следим за зависимостью остаточного члена от w. Это важно для дальнейших приложений.

Символом $R(q,p,w)$ обозначим совместные условия:

$q \mid (p-1)/w$; a является вычетом степени wq по модулю p.

Необходимое и достаточное условие равенства $o(a,p) = \frac{p-1}{w}$ состоит в том, что для каждого простого q $R(q,p,w)$ не выполняется и $a^{(p-1)/w} \equiv 1 (\mathrm{mod}\, p)$. Заметим, что $N(x,a,w)$ в точности равно числу простых $p \leqslant x$ с $a^{(p-1)/w} \equiv 1 (\mathrm{mod}\, p)$, для которых $R(q,p,w)$ не выполняется для любого простого $q \leqslant (x-1)/w$. Пусть $N(x,\eta,a,w)$ означает число простых $p \leqslant x$, для которых $a^{(p-1)/w} \equiv 1 (\mathrm{mod}\, p)$ и $R(q,p,w)$ не выполняется для любого простого $q \leqslant \eta$. Тогда

$$N(x,a,w) = N(x,(x-1)/w,a,w).$$

Через $P(x,k,a,w)$, где k – любое бесквадратное число, обозначим число простых $p \leqslant x$, для которых $R(q,p,w)$ верно для каждого простого делителя $q|k$; $a^{(p-1)/w} \equiv 1 (\mathrm{mod}\, p)$ является единственным подразумеваемым условием, если $k=1$. Наконец, $M(x,\eta_1,\eta_2,a,w)$ означает число простых $p \leqslant x$, для которых $R(q,p,w)$ верно, по крайней мере, для одного простого q с $\eta_1 < q \leqslant \eta_2$. Вводим величины

$$\xi_1 = \frac{1}{6}\log x, \quad \xi_2 = x^{1/2}/\log^5 x \quad \text{и} \quad \xi_3 = x^{1/2}\log x.$$

Как показано в [3],

$$N(x,a,w) = N(x,\xi_1,a,w) + O\{M(x,\xi_1,\xi_2,a,w)\} +$$
$$+ O\{M(x,\xi_2,\xi_3,a,w)\} + O\{M(x,\xi_3,(x-1)/w,a,w)\}. \qquad (1)$$

Пусть l' означает либо 1, либо положительное бесквадратное число, целиком состоящее из простых множителей $q \leqslant \xi_1$; имеем

$$N(x, \xi_1, a, w) = \sum_{l'} \mu(l') P(x, l', a, w). \tag{2}$$

Верхняя граница для l' дается неравенством

$$l' \leqslant \prod_{q \leqslant \xi_1} q \leqslant e^{2\xi_1} \leqslant x^{1/3}. \tag{3}$$

Нам необходима

Лемма 1. *Если верна* РГР(a), *то*

$$P(x, k, a, w) = \frac{\operatorname{li} x}{\delta(kw)} + O\big(x^{1/2} \log(kwx)\big).$$

Лемма – частный случай плотностной теоремы Чеботарева (условный вариант), так как простые числа p, подсчитываемые в $P(x, k, a, w)$, в точности удовлетворяют совместным условиям: $p \leqslant x$; $p \nmid kwa$; p вполне разложимо в K_n на различные линейные простые идеалы. См. [9].

Используя (2), лемму 1 и (3), имеем

$$\begin{aligned} N(x, \xi_1, a, w) &= \sum_{l'} \mu(l') \big\{ \big(\operatorname{li} x / \delta(l'w)\big) + O\big(x^{1/2} \log(l'wx)\big) \big\} = \\ &= \operatorname{li} x \sum_{l'} \big(\mu(l')/\delta(l'w)\big) + O\big(x^{5/6} \log x\big). \end{aligned}$$

Точное значение $\delta(n)$ вычислил Стефенс [3]; нам достаточно неравенств

$$kw\varphi(kw) \geqslant \delta(kw) \geqslant \frac{1}{2} kw\varphi(kw).$$

В дальнейшем нам также потребуется известная оценка

$$\sum_{n > \alpha} \frac{1}{n\varphi(n)} \ll \frac{1}{\alpha}, \quad \text{где} \quad \alpha \geqslant 1.$$

Так как все бесквадратные числа $k \leqslant \xi_1$ имеют тип l', мы получаем с учетом вышеприведенных неравенств:

$$N(x, \xi_1, a, w) = \operatorname{li} x \sum_{k=1}^{\infty} \frac{\mu(k)}{\delta(kw)} + O\bigg\{ \operatorname{li} x \sum_{k > \xi_1} \frac{1}{kw\varphi(kw)} \bigg\} + O\big(x^{5/6} \log x\big);$$

$$\sum_{k>\xi_1}\frac{1}{kw\varphi(kw)}\ll\frac{1}{w\varphi(w)}\sum_{k>\xi_1}\frac{1}{k\varphi(k)}\ll\frac{1}{w\varphi(w)}\cdot\frac{1}{\xi_1}.$$

Следовательно,

$$N(x,\xi_1,a,w)=\operatorname{li}x\sum_{k=1}^{\infty}\frac{\mu(k)}{\delta(kw)}+O\Big(\frac{x}{w\varphi(w)\log^2 x}\Big)+ \\ +O\big(x^{5/6}\log x\big). \tag{4}$$

Член $M(x,\xi_1,\xi_2,a,w)$ оценивается с помощью леммы 1.

Имеем

$$M(x,\xi_1,\xi_2,a,w)\leqslant\sum_{\xi_1<q\leqslant\xi_2}P(x,q,a,w)\ll$$

$$\ll\frac{x}{w\varphi(w)\xi_1\log x}+\frac{\xi_2x^{1/2}\log x}{\log\xi_2}\ll\frac{x}{w\varphi(w)\log^2 x}+\frac{x}{\log^5 x}. \tag{5}$$

Для оценки $M(x,\xi_2,\xi_3,a,w)$ требуются теорема Бруна–Титчмарша и формула Мертенса. Имеем

$$M(x,\xi_2,\xi_3,a,w)\ll\frac{x\log\log x}{\varphi(w)\log^2 x}. \tag{6}$$

Наконец,

$$M(x,\xi_3,(x-1)/w,a,w)\ll\frac{x}{w^2\log^2 x}. \tag{7}$$

Подставляя в (1) соотношения (4)–(7), получаем утверждение теоремы.

Теорема 2(a). *Пусть выполняется РГР(a). Пусть при $x\to\infty$ положительная функция $\alpha(x)$ монотонно возрастает и $\alpha(x)\to\infty$. Тогда*

1) *если $\alpha(x)\geqslant(\log x)(\log\log x)^{-2}$, то*

$$\#\{p\leqslant x\mid r(a,p)<\alpha(x)\}\ll\frac{\pi(x)}{(\log x)(\log\log x)^{-2}};$$

2) *если $\alpha(x)\leqslant(\log x)(\log\log x)^{-2}$, то*

$$\#\{p\leqslant x\mid r(a,p)<\alpha(x)\}\ll\frac{\pi(x)}{\alpha(x)};$$

причем

3) *если* $\alpha(x) = o\{(\log x)(\log\log x)^{-2}\}$, *то*

$$\#\{p \leqslant x \mid r(a,p) < \alpha(x)\} \asymp \frac{\pi(x)}{\alpha(x)}.$$

Доказательство. Плотность $A(a,w)$, $a \geqslant 2$ бесквадратно и $w \in \mathbb{N}$, из теоремы 1(*a*) вычислил Мурата [4]. Пусть

$$C = \sum_{w=1}^{\infty} \frac{\mu(w)}{w\varphi(w)} = 0.37395\ldots \ (\text{константа Артина}),$$

$$(a,w) = \text{н.о.д. } a \ \text{ и } \ w,$$

$$E(w) = \frac{1}{w^2}\prod_{p|w}\frac{p^2-1}{p^2-p-1},$$

$$A = \frac{a}{(a,w)}, \qquad B(a,w) = \prod_{p|A}\frac{-1}{p^2-p-1}.$$

Приведем таблицу значений $A(a,w)$:

$$\begin{array}{llll}
a \equiv 1(\operatorname{mod} 4), & 2|w, & a|w & A(a,w) = 2E(w)C \\
a \equiv 1(\operatorname{mod} 4), & 2|w, & a\nmid w & A(a,w) = (1+B(a,w))E(w)C \\
a \equiv 1(\operatorname{mod} 4), & 2\nmid w, & a|w & A(a,w) = 0 \\
a \equiv 1(\operatorname{mod} 4), & 2\nmid w, & a\nmid w & A(a,w) = (1-B(a,w))E(w)C \\
a \equiv 2(\operatorname{mod} 4), & 4\nmid w & & A(a,w) = E(w)C \\
a \equiv 2(\operatorname{mod} 4), & 2^2\|w & & A(a,w) = \Bigl(1-\frac{1}{3}B(a,w)\Bigr)E(w)C \\
a \equiv 2(\operatorname{mod} 4), & 8|w & & A(a,w) = (1+B(a,w))E(w)C \\
a \equiv 3(\operatorname{mod} 4), & 2\nmid w & & A(w) = E(w)C \\
a \equiv 3(\operatorname{mod} 4), & 2\|w & & A(w) = \Bigl(1-\frac{1}{3}B(a,w)\Bigr)E(w)C \\
a \equiv 3(\operatorname{mod} 4), & 4|w & & A(w) = (1+B(a,w))E(w)C.
\end{array}$$

Из приведенных выше выражений для $A(a,w)$ следует, что в случае $A(a,w) \neq 0$ имеем

$$\frac{1}{w^2} \ll A(a,w) \ll \frac{1}{w\varphi(w)}. \tag{8}$$

Как показал Вагстаф [10],

$$\sum_{u=1}^{\infty} A(a,w) = 1.$$

В силу (8), справедливо соотношение

$$\sum_{w>\alpha} A(a,w) \asymp \frac{1}{\alpha}. \tag{9}$$

Имеем

$$\#\{p \leqslant x \mid r(a,p) > \alpha(x)\} = \pi(x) - \#\{p \leqslant x \mid r(a,p) \leqslant \alpha(x)\}.$$

Можно считать, что $\alpha(x) \leqslant \log x$, тогда, по теореме $1(a)$, имеем

$$\#\{p \leqslant x \mid r(a,p) \leqslant \alpha(x)\} = \sum_{1 \leqslant w \leqslant \alpha(x)} \left\{ A(a,w)\operatorname{li} x + O\left(\frac{x \log\log x}{\varphi(w)\log^2 x}\right)\right\}.$$

Используя равенство Вагстафа и (9), имеем

$$\#\{p \leqslant x \mid r(a,p) > \alpha(x)\} \asymp \frac{\operatorname{li} x}{\alpha(x)} + O\left(\frac{x(\log\log x)\log\alpha(x)}{\log^2 x}\right).$$

Отсюда непосредственно следует утверждение теоремы.

Замечание 1. Пункт 1) теоремы $2(a)$ для функций $\alpha(x) \gg x^{1/2+\delta}$ можно улучшить, причем результат будет безусловным. Точнее, справедливо утверждение:

для любых постоянных $c > 0$ и $0 < \delta < \frac{1}{2}$ и функции $\alpha(x) \geqslant x^{1/2+\delta}\log^{-c} x$ имеем

$$\#\{x\log^{-c} x < p \leqslant x \mid r(a,p) > \alpha(x)\} \ll x^{1-2\delta}.$$

Утверждение сразу вытекает из следующего легко доказываемого факта:

$$I = \#\{p \leqslant x \mid o(a,p) \leqslant x^{1/2-\delta}\} \ll x^{1-2\delta}.$$

В самом деле, имеем

$$I \leqslant \sum_{e \leqslant x^{1/2-\delta}} \#\{p \mid p \mid (a^e-1)\} \ll$$

$$\ll \sum_{e \leqslant x^{1/2-\delta}} \log(a^e-1) \ll \sum_{e \leqslant x^{1/2-\delta}} e \ll x^{1-2\delta}.$$

§2

Настоящий параграф посвящен оценкам средних значений вычетного индекса $r(a,p)$.

Теорема 3(a). *Имеют место соотношения*

$$\frac{x\log\log x}{\log x} \ll \sum_{p\leqslant x} r(a,p) \ll \frac{x^{3/2}}{\log x},$$

причем доказательство оценки снизу требует предположения о справедливости РГР(a).

Доказательство. 1) Получим оценку сверху

$$\sum_{p\leqslant x} r(a,p) \ll \frac{x^{3/2}}{\log x}. \tag{10}$$

Пусть $G_n = a^n - 1$, где $n = 1,2,3,\ldots$. Тогда наименьшее $n>0$ со свойством $p \mid G_n$ равно $n = o(a,p)$. Используем метод работы [1]. Пусть

$$S(x) = \sum_{p\leqslant x} r(a,p)\log p.$$

Тогда

$$S(x) = \sum_{\substack{p\leqslant x\\ o(a,p)\leqslant x^{1/2}}} r(a,p)\log p + \sum_{\substack{p\leqslant x\\ o(a,p)>x^{1/2}}} r(a,p)\log p = \sum\nolimits_1 + \sum\nolimits_2.$$

Сумма $\sum_2$ оценивается тривиально:

$$\sum\nolimits_2 < x^{1/2}\sum_{p\leqslant x}\log p \sim x^{3/2}.$$

Оценим сумму $\sum_1$, принимая во внимание, что при $\alpha>1$ $2[\alpha]\geqslant\alpha$. Имеем

$$\sum\nolimits_1 \ll x^{1/2}\sum_{\substack{p\leqslant x\\ o(a,p)\leqslant x^{1/2}}}\left[\frac{x^{1/2}}{o(a,p)}\right]\log p \ll$$

$$\ll x^{1/2}\sum_{o(a,p)\leqslant x^{1/2}}\left[\frac{x^{1/2}}{o(a,p)}\right]\log p \ll x^{1/2}\log\prod_{l\leqslant x^{1/2}} G_l \ll x^{3/2}.$$

Следовательно, $S(x) \ll x^{3/2}$, и оценка (10) доказана.

2) В предположении верности РГР(a) докажем соотношение

$$\sum_{\substack{p \leqslant x \\ r(a,p) \leqslant (\log x)(\log\log x)^{-1}}} r(a,p) \asymp \frac{x \log\log x}{\log x}. \tag{11}$$

Пусть

$$\alpha(x) = \frac{\log x}{\log\log x},$$

тогда, по теореме 1 с использованием (8), имеем

$$\sum_{\substack{p \leqslant x \\ r(a,p) \leqslant \alpha(x)}} r(a,p) = \sum_{w \leqslant \alpha(x)} w \biggl\{ A(a,w) \operatorname{li} x + O\biggl(\frac{x \log\log x}{\varphi(w) \log^2 x} \biggr) \biggr\} \asymp$$

$$\asymp \operatorname{li} x \sum_{w \leqslant \alpha(x)} \frac{1}{\varphi(w)} + O\biggl(\frac{x \log\log x}{\log^2 x} \sum_{w \leqslant \alpha(x)} \frac{w}{\varphi(w)} \biggr) \asymp$$

$$\asymp (\operatorname{li} x) \log \alpha(x) + O\biggl(\frac{x \log\log x}{\log^2 x} \alpha(x) \biggr) \asymp \frac{x \log\log x}{\log x},$$

и соотношение (11) доказано. Тем самым, теорема 3(a) доказана.

Теорема 4(a). *Пусть верна* РГР(a). *Тогда*

$$\sum_{\substack{p \leqslant x \\ r(a,p) \leqslant x^{1/4}}} r(a,p) \ll x \log^2 x.$$

Доказательство. Пусть $\xi_1 = \frac{1}{2} \log\log x$, l' означает либо 1, либо положительное бесквадратное число, целиком состоящее из простых множителей $q \leqslant \xi_1$; тогда

$$l' \leqslant e^{2\xi_1} = \log x.$$

Имеем (ср. §1)

$$N(x,a,w) \leqslant N(x,\xi_1,a,w) \leqslant \sum_{l'} P(x,l',a,w).$$

Отсюда, по лемме 1, получаем

$$N(x,a,w) \leqslant \sum_{l'} \bigl\{ (\operatorname{li} x)/\delta(l'w) + O\bigl(x^{1/2} \log(l'wx)\bigr) \bigr\} \ll$$

$$\ll (\operatorname{li} x)\frac{1}{w\varphi(w)} + x^{1/2}(\log(wx))\log x.$$

Следовательно,

$$\sum_{\substack{p\leqslant x\\ r(a,p)\leqslant x^{1/4}}} r(a,p) = \sum_{w\leqslant x^{1/4}} wN(x,a,w) \ll$$

$$\ll \operatorname{li} x \sum_{w\leqslant x^{1/4}} \frac{1}{\varphi(w)} + \sum_{w\leqslant x^{1/4}} \bigl(wx^{1/2}(\log(wx))\log x\bigr) \ll$$

$$\ll (\operatorname{li} x)\log x + x\log^2 x \ll x\log^2 x,$$

и теорема доказана.

Рассмотрим теперь усреднение суммы

$$\sum_{x<p\leqslant 2x} r(a,p)$$

по a. Полученную оценку можно сравнить с гипотезой $1(a)$. Более тонкое усреднение, свяанное с гипотезой $1(\varepsilon_0)$, рассматривается в [7].

Теорема 5(a).

$$\sum_{2\leqslant a\leqslant x}\ \sum_{x<p\leqslant 2x} r(a,p) \ll x^2. \tag{12}$$

Доказательство. Обозначим левую часть неравенства (12) через S. Напомним, что $o(a,p) \mid (p-1)$ и что при фиксированных p и $m = o(a,p)$ сравнение $a^m \equiv 1(\operatorname{mod} p)$ имеет не более m решений. Поэтому

$$S = \sum_{2\leqslant a\leqslant x}\ \sum_{x<p\leqslant 2x} \frac{p-1}{o(a,p)} \ll x \sum_{x<p\leqslant 2x}\ \sum_{2\leqslant a\leqslant x} \frac{1}{o(a,p)} \ll$$

$$\ll x \sum_{x<p\leqslant 2x}\ \sum_{m|(p-1)} \frac{1}{m} m \ll x \sum_{x<p\leqslant 2x} d(p-1) \ll x^2,$$

и теорема доказана.

Замечание 2. Элементарно получаемая оценка (10) является весьма сильной. Чтобы в этом убедиться, сравним (10) со следующей оценкой, полученной с помощью теоремы Бомбьери–Виноградова,

$$\sum_{p\leqslant x} o(a,p) \gg x^{3/2}/\log x \tag{13}$$

(см. [11]). Из (13) сразу вытекает оценка

$$\sum_{p\leqslant x} \frac{o(a,p)}{p-1} \gg \frac{x^{1/2}}{\log x}. \tag{14}$$

С другой стороны, если взять неравенство Коши

$$\pi^2(x) \leqslant \Bigl(\sum_{p\leqslant x} r(a,p)\Bigr)\Bigl(\sum_{p\leqslant x}\frac{1}{r(a,p)}\Bigr)$$

и применить (10), то снова получим (14).

§3

В настоящем параграфе при некоторых предположениях будет доказана гипотеза $2(a)$. Ранее Паппаларди [12] получил неравенства (Λ – функция Мангольдта)

$$\operatorname{li} x \sum_{n=1}^{\infty} \frac{\Lambda(n)}{\delta(n)} \lesssim \sum_{p\leqslant x} \log r(a,p) \ll \frac{x\log\log x}{\log x}; \tag{15}$$

доказательство оценки сверху требует привлечения РГР(a), оценка снизу является безусловной. Автор [6] доказал: если $N > \exp\{c_1(\log x)^{1/2}\}$ и константа c_1 достаточно велика, то

$$N^{-1}\sum_{a\leqslant N}\sum_{p\leqslant x} \log r(a,p) \leqslant C \operatorname{li} x + O\bigl(x/(\log x)^D\bigr), \quad \text{где} \quad C = \sum_{n=2}^{\infty} \frac{\log n}{n\varphi(n)},$$

D – произвольная константа >1.

Теорема 6(a). *Пусть выполняются* РГР(a) *и гипотеза А Холи* [13, *с.* 121]. *Тогда*

$$\sum_{p\leqslant x} \log r(a,p) = \operatorname{li} x \sum_{n=1}^{\infty} \frac{\Lambda(n)}{\delta(n)} + O\Bigl(\frac{x\log\log x}{\log^2 x}\Bigr).$$

Доказательство. Введем функцию

$$\pi(x,n)=\#\{p\leqslant x \mid n \mid r(a,p)\}.$$

По лемме 1 (в предположении верности РГР(a)), имеем

$$\pi(x,n)=\frac{1}{\delta(n)}\operatorname{li}x+O\big(x^{1/2}\log(xn)\big). \tag{16}$$

Воспользуемся равенством

$$\sum_{p\leqslant x}\log r(a,p)=\sum_{n\leqslant x}\Lambda(n)\pi(x,n).$$

Имеем

$$\sum_{p\leqslant x}\log r(a,p)=\sum_{n\leqslant\sqrt{x}/\log^4 x}\Lambda(n)\pi(x,n)+$$
$$+\sum_{\sqrt{x}/\log^4 x<n\leqslant x}\Lambda(n)\pi(x,n)=\sum\nolimits_1+\sum\nolimits_2.$$

К сумме $\sum_1$ применим (16):

$$\sum\nolimits_1=\sum_{n\leqslant\sqrt{x}/\log^4 x}\Lambda(n)\left\{\frac{1}{\delta(n)}\operatorname{li}x+O\big(x^{1/2}\log(xn)\big)\right\}=$$
$$=\operatorname{li}x\sum_{n\leqslant\sqrt{x}/\log^4 x}\frac{\Lambda(n)}{\delta(n)}+O\big(x/\log^3 x\big)=$$
$$=\operatorname{li}x\sum_{n=1}^{\infty}\frac{\Lambda(n)}{\delta(n)}-\operatorname{li}x\sum_{n>\sqrt{x}/\log^4 x}\frac{\Lambda(n)}{\delta(n)}+O\big(x/\log^3 x\big)=$$
$$=\operatorname{li}x\sum_{n=1}^{\infty}\frac{\Lambda(n)}{\delta(n)}+O\big(x/\log^3 x\big).$$

Сумму $\sum_2$ разбиваем на две:

$$\sum\nolimits_2=\sum_{q>\sqrt{x}/\log^4 x}(\log q)\pi(x,q)+\sum_{q^\alpha>\sqrt{x}/\log^4 x,\,\alpha>1}(\log q)\pi(x,q^\alpha)=$$
$$=\sum\nolimits_{2,1}+\sum\nolimits_{2,2}.$$

Оцениваем сумму $\sum_{2,2}$:

$$\sum\nolimits_{2,2} \ll x \sum_{q>\sqrt{x}/\log^4 x} \frac{\log q}{q^2} \ll x^{1/2+\varepsilon}.$$

Сумму $\sum_{2,1}$ разбиваем на две:

$$\sum\nolimits_{2,1} = \sum_{\sqrt{x}/\log^4 x<q\leqslant\sqrt{x}\log^2 x} (\log q)\pi(x,q) + \sum_{q>\sqrt{x}\,\log^2 x} (\log q)\pi(x,q) =$$

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

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

$$\#\{p \mid p \ \text{ делит } \prod_{m\leqslant\sqrt{x}/\log^2 x} (a^m-1)\} \log x;$$

поскольку

$$\#\{\dots\} < \sum_{m\leqslant\sqrt{x}/\log^2 x} m \ll \frac{x}{\log^4 x},$$

имеем

$$\sum\nolimits_{2,1,2} \ll \frac{x}{\log^3 x}.$$

Рассмотрим сумму $\sum_{2,1,2}$. Величина $\pi(x,q)$ при $\sqrt{x}/\log^4 x < q \leqslant \sqrt{x}\log^2 x$ оценивается, по гипотезе А Холи, следующим образом:

$$\pi(x.q) \ll \frac{x}{q\log^2 x}. \tag{17}$$

Поэтому, применяя (17) и формулу Мертенса, получаем

$$\sum\nolimits_{2,1,1} \ll \frac{x}{\log^2 x} \sum_{\sqrt{x}/\log^4 x<q\leqslant\sqrt{x}\log^2 x} \frac{\log q}{q} \ll \frac{x\log\log x}{\log^2 x},$$

и теорема доказана.

§4

Доказательство следующей теоремы не зависит от каких-либо гипотез.

Теорема 7(*a*). *Для бесконечного множества p имеем*

$$r(a,p) \geqslant (\log\log p)(\log_k p)^{-1}.$$

Доказательство. Пусть $\xi_1 = (1/15)\log\log x$, тогда

$$l' \leqslant e^{2\xi_1} \leqslant (\log x)^{2/15}$$

(ср. §1). Имеем ($w \leqslant \log x$)

$$N(x,a,w) \leqslant N(x,\xi_1,a,w) = \sum_{l'} \mu(l') P(x,l',a,w). \tag{18}$$

Имеет место следующая

Лемма 2. *Справедливо соотношение*

$$P(x,l',a,w) = \frac{\operatorname{li} x}{\delta(l'w)} + O\left\{x \exp\left(\frac{-A\sqrt{\log x}}{l'w}\right)\right\},$$

где $A > 0$ – некоторая константа, при условии, что $l'w \leqslant (\log x)^{1/7}$.

Лемма – частный случай плотностной теоремы Чеботарева (безусловный вариант); см. [9]. Пусть $w \leqslant (\log x)^{1/105}$; по сказанному выше, $l' \leqslant (\log x)^{2/15}$. Напомним, что все бесквадратные числа $k \leqslant \xi_1$ имеют тип l'. Применяя (18) и лемму 2, получаем

$$N(x,\xi_1,a,w) = \sum_{l'} \mu(l')\left\{\frac{\operatorname{li} x}{\delta(l'w)} + O\left(x \exp\left(\frac{-A\sqrt{\log x}}{l'w}\right)\right)\right\} =$$

$$= \operatorname{li} x \sum_{l'} (\mu(l')/\delta(l'w)) + O\left\{(\log x)^{\frac{2}{15}} x \exp\left(\frac{-A\sqrt{\log x}}{(\log x)^{1/7}}\right)\right\}.$$

Имеем

$$N(x,\xi_1,a,w) = \operatorname{li} x \sum_{k=1}^{\infty} \frac{\mu(k)}{\delta(kw)} + O\left((\operatorname{li} x)\frac{1}{w\varphi(w)}\ \frac{1}{\xi_1}\right) +$$

$$+O\left\{(\log x)^{2/15} x \exp\left(-A(\log x)^{5/14}\right)\right\}. \tag{19}$$

Пусть при всех $x \gg 0$ и всех $p \leqslant x$

$$r(a,p) < \frac{\log\log x}{\log_k x} = C(x).$$

Тогда

$$\sum_{w<C(x)} N(x,a,w) = \operatorname{li} x + O\biggl(\frac{x}{\log^2 x}\biggr). \tag{20}$$

В силу (18) и (19),

$$\sum_{w<C(x)} N(x,a,w) \leqslant \operatorname{li} x \sum_{1\leqslant w\leqslant C(x)} A(a,w) + O\Bigl((\operatorname{li} x)\frac{1}{\xi_1}\Bigr) +$$

$$+O\biggl\{\frac{\log\log x}{\log_k x}(\log x)^{2/15} x \exp\Bigl(-A(\log x)^{5/14}\Bigr)\biggr\}. \tag{21}$$

Как и выше, имеем ($x \gg 0$)

$$\sum_{1\leqslant w\leqslant C(x)} A(a,w) = 1 - B\frac{\log_k x}{\log\log x},$$

где

$$C_2 < B < C_1.$$

Из (20) и (21) поэтому следует неравенство

$$B(\operatorname{li} x)\frac{\log_k x}{\log\log x} + O\biggl(\frac{x}{\log^2 x}\biggr) \leqslant$$

$$\leqslant O\biggl(\frac{\operatorname{li} x}{\xi_1}\biggr) + O\biggl\{\frac{\log\log x}{\log_k x}(\log x)^{2/15} x \exp\Bigl(-A(\log x)^{5/14}\Bigr)\biggr\},$$

и мы приходим к противоречию. Теорема доказана.

§5

В настоящем параграфе изучаются свойства $r(\varepsilon_0, p)$ (и, следовательно, $h(5p^2)$). Из пяти теорем, относящихся к данной теме, здесь мы приводим три, остальные две перенесены в §0. Доказательства повторяют доказательства аналогичных результатов для $r(a,p)$ и здесь не приводятся.

Основную роль в приложениях играет (условная) асимптотическая формула для

$$N(x,\varepsilon_0,w)=\#\Big\{p\leqslant x\,\Big|\Big(\frac{5}{p}\Big)=1,r(\varepsilon_0,p)=w\Big\}.$$

Ранее в [6] мы уже доказали такую формулу, но ниже в теореме $1(\varepsilon_0)$ будет получена асимптотика с лучшим остаточным членом.

Сделаем несколько предварительных замечаний. Пусть $K=\mathbb{Q}(\sqrt{5})$, $\varepsilon_0=\frac{1+\sqrt{5}}{2}$ – основная единица этого поля. Поскольку, по предположению, $(5/p)=1$, p разлагается в произведение различных простых идеалов поля K:

$$p=\mathfrak{p}_1\mathfrak{p}_2.$$

Через $R'(q,p,w)$ обозначим совместные условия:

$qw\mid(p-1)$; сравнения $t_i^{qw}\equiv\varepsilon_0(\operatorname{mod}\mathfrak{p}_i)$ $(i=1,2)$ разрешимы.

Для бесквадратного k и $w\in\mathbb{N}$ $P(x,k,\varepsilon_0,w)$ означает число простых $p\leqslant x$, $(5/p)=1$, для которых $R'(q,p,w)$ верно для каждого простого делителя $q|k$.

Простые числа, подсчитываемые в $P(x,k,\varepsilon_0,w)$, в точности удовлетворяют совместным условиям: $p\leqslant x$, $(5/p)=1$; $p\nmid 5kw$; p вполне разложимо в K_n' на различные линейные простые идеалы. Аналоги лемм 1 и 2 верны для $P(x,k,\varepsilon_0,w)$ и сводятся к плотностной теореме Чеботарева (условный и безусловный варианты); см. [9].

Теорема $1(\boldsymbol{\varepsilon_0})$. *Пусть верна* РГР$(\varepsilon_0)$. *Пусть* $w\leqslant\log x$. *Тогда*

$$N(x,\varepsilon_0,w)=A(\varepsilon_0,w)\operatorname{li}x+O\bigg(\frac{x\log\log x}{\varphi(w)\log^2 x}\bigg),$$

где

$$A(\varepsilon_0,w)=\sum_{k=1}^{\infty}\frac{\mu(k)}{\delta'(kw)};$$

константа, входящая в O, *абсолютная.*

Доказательство аналогично доказательству теоремы $1(a)$. Отметим, что решетную часть схемы Холи–Стефенса на случай $r(\varepsilon_0,p)$ перенес Антониадис [5]. Он же вычислил $\delta'(n)$. Приведем лишь неравенства

$$n\varphi(n)\leqslant\delta'(n)\leqslant 4n\varphi(n).$$

Плотность $A(\varepsilon_0, w)$ вычислил автор [6]. Из этого вычисления следует, что

$$A(\varepsilon_0, w) \neq 0 \quad (w \in \mathbb{N})$$

и что

$$\frac{1}{w^2} \ll A(\varepsilon_0, w) \ll \frac{1}{w\varphi(w)}.$$

В [6] было показано, что

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

и

$$\sum_{w>\alpha} A(\varepsilon_0 . w) \asymp \frac{1}{\alpha}.$$

Из теоремы 1 (ε_0) и только что приведенных результатов следует теорема $2(\varepsilon_0)$. Теорема $2(\varepsilon_0)$, которая в §0 приводилась в упрощенной форме, на самом деле может быть сформулирована в более точном виде, аналогичном теореме $2(a)$. Можно доказать также следующий аналог утверждения из замечания 1:

для любых постоянных $c > 0$ и $0 < \delta < 1/2$ и функции $\alpha(x) \geqslant x^{1/2+\delta} \log^{-c} x$ имеем $((5/p) = \pm 1)$

$$\#\{x \log^{-c} x < p < x \mid h(5p^2) > \alpha(x)\} \ll x^{1-2\delta}.$$

Отметим, что случай, когда в теореме 2 (ε_0) вместо $\alpha(x)$ берется произвольная достаточно большая положительная константа, рассматривался в [6].

Отметим также, что аналог оценки сверху (10) для $h(5p^2)$ уже был доказана Е. П. Голубевой [1], причем сразу для всех дискриминантов $5p^2$.

Объединим теперь аналоги соотношения (11) и теоремы $4(a)$ в одну теорему 3 (ε_0).

Теорема 3($\boldsymbol{\varepsilon_0}$). *Пусть верна* РГР$(\varepsilon_0)$. *Тогда*

1)

$$\sideset{}{'}\sum_{\substack{p \leqslant x \\ h(5p^2) \leqslant (\log x)(\log\log x)^{-1}}} h(5p^2) \asymp \frac{x \log\log x}{\log x};$$

2)
$$\sideset{}{'}\sum_{\substack{p\leqslant x\\ h(5p^2)\leqslant x^{1/4}}} h(5p^2)\leqslant x\log^2 x.$$

Теорема 5(a) впрямую на случай $r(\varepsilon_0,p)$ не переносится, см. по этому поводу работу [7].

Переходим к теореме 4 (ε_0). Отметим, что аналог результата (15) для $r(\varepsilon_0,p)$ доказан в [6]. Отметим также, что, по гипотезе А Холи (точнее, по некоторому её обобщению), величина

$$\pi'(x,q)=\#\Big\{p\leqslant x \mid \Big(\frac{5}{p}\Big)=1,\ q\mid r(\varepsilon_0,p)\Big\}$$

оценивается при

$$\sqrt{x}/\log^4 x<q\leqslant\sqrt{x}\,\log^2 x$$

следующим образом:

$$\pi'(x,q)\ll\frac{x}{q\log^2 x}.$$

Теорема 4(ε_0). *Пусть выполняются* РГР(ε_0) *и (обобщенная) гипотеза А Холи. Тогда*

$$\sideset{}{'}\sum_{p\leqslant x}\log r(\varepsilon_0,p)=\operatorname{li}x\sum_{n=1}^{\infty}\frac{\Lambda(n)}{\delta'(n)}+O\bigg(\frac{x\log\log x}{\log^2 x}\bigg).$$

Теорема 5 (ε_0) сформулирована в §0.

Литература

1. Е. П. Голубева, *О длинах периодов разложения в непрерывную дробь квадратичных иррациональностей и числах классов вещественных квадратичных полей. I; II,* Зап. научн. семин. ЛОМИ **160** (1987), 72–81; **168** (1988), 11–22.
2. C. Hooley, *On Artin's conjecture,* J. reine und angew. Math. **225** (1967), 209–220.
3. P. J. Stephens, *Prime divisors of second-order linear recurrences. I; II,* J. Number Theory **8**, No. 3 (1976), 313–332; 333–345.
4. L. Murata, *A problem analogous to Artin's conjecture for primitive roots and its applications,* Arch. Math. **57** (1991), 555–565.
5. J. A. Antoniadis, *Über die Periodenlänge mod p einer Klasse rekursiver Folgen,* Arch. Math. **42**, No. 3 (1984), 242–252.

6. О. М. Фоменко, *Числа классов неопределенных бинарных квадратичных форм,* Зап. научн. семин. ПОМИ **276** (2001), 312–333.
7. Е. П. Голубева, *О числах классов неопределенных бинарных квадратичных форм дискриминанта dp^2,* Зап. научн. семин. ПОМИ **286** (2002), 40–47.
8. E. Bach, R. Lukes, J. Shallit, and H. C. Williams, *Results and estimates on pseudopowers,* Math. Comp. **65** (1996), 1737–1747.
9. 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.
10. S. S. Wagstaff Jr., *Pseudoprimes and a generalization of Artin's conjecture,* Acta Arithm. **41** (1982), 141–150.
11. M. Goldfeld, *On the number of primes p for which $p+a$ has a large prime factor,* Mathematika **16**, No. 1 (1969), 23–27.
12. F. Pappalardi, *On Hooley's theorem with weights,* Rendiconti Sem. Mat. Univ. Pol. Torino **53**, No. 4 (1995), 375–388.
13. К. Хооли, *Применения методов решета в теории чисел,*. М., 1987.

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

Поступило 26 июня 2002 г.