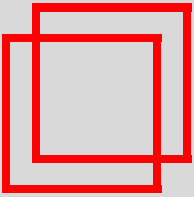


Math-Net.Ru

Общероссийский математический портал

О. М. Фоменко, О распределении корней квадратичного сравнения,
Зап. научн. сем. ЛОМИ, 1990, том 183, 155–165

https://www.mathnet.ru/znsl4801

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
https://www.mathnet.ru/rus/agreement

Параметры загрузки:
IP: 18.97.14.91
18 мая 2025 г., 01:27:42

О.М.Фоменко

О РАСПРЕДЕЛЕНИИ КОРНЕЙ КВАДРАТИЧНОГО СРАВНЕНИЯ

0. Рассмотрим квадратичное сравнение

$$f^2+2\tau f-\beta \equiv 0 \pmod n,$$

где $n, \beta \in \mathbb{N}$, $\tau \in \mathbb{Z}$, причем исключим (для сохранения единообразия доказательств) случаи:

$$\tau^2+\beta = \text{квадрат}; \quad \beta = \text{квадрат}.$$

Рассмотрим сумму

$$\sigma(n) = \sum_{\substack{0<f\le n,\\ f^2+2\tau f-\beta\equiv 0 \pmod n}} \left(\frac{f}{n}\right),$$

где $\left(\frac{f}{n}\right)$ обозначает символ Кронекера.

Основным результатом настоящей работы является следующая

ТЕОРЕМА I. Справедлива оценка

$$\sum_{n\le x} \sigma(n) \ll x^{\frac{5}{6}+\varepsilon}, \qquad (I)$$

где здесь и ниже $\varepsilon>0$ – сколь угодно малое постоянное число.

Оценка (I) выражает новый факт о распределении корней квадратичного сравнения. Действительно, пусть

$\rho_+(k)$ – число корней f сравнения

$f^2+2\tau f-\beta \equiv 0 \pmod k$, $0<f\le k$, с условием $\left(\frac{f}{k}\right)=1$;

$\rho_-(k)$ – число корней f сравнения

$f^2+2\tau f-\beta \equiv 0 \pmod k$, $0<f\le k$, с условием $\left(\frac{f}{k}\right)=-1$.

Пусть

$$T_+(x) = \sum_{k\le x} \rho_+(k),$$

$$T_-(x) = \sum_{k\le x} \rho_-(k).$$

Имеем в силу (I)

$$T_+(x) - T_-(x) \ll x^{\frac{5}{8}+\varepsilon} .$$

С другой стороны,

$$T_+(x) + T_-(x) = T^*(x),$$

где $T^*(x)$ - общее количество решений f сравнений $f^2+2\tau f-\beta \equiv 0 \pmod k$, $0<f\leqslant k$, с условием $(f,k)=1$ при $k\leqslant x$. Легко показать, что

$$x \ll T^*(x) \ll x .$$

Имеем, таким образом, следующий факт о распределении корней квадратичного сравнения:

ТЕОРЕМА I'.

$$T_+(x) = \tfrac{1}{2} T^*(x) + \theta x^{\frac{5}{8}+\varepsilon} ,$$
$$T_-(x) = \tfrac{1}{2} T^*(x) - \theta x^{\frac{5}{8}+\varepsilon} , \qquad (2)$$

где $|\theta| < C$, $\varepsilon > 0$.

Некоторые применения асимптотик (2) см. в пункте 3 настоящей работы. Основой для получения оценки (I) является следующее утверждение, которое будет доказано ниже.

ТЕОРЕМА 2. Существует новая форма

$$S^*(\tau) = \sum_{n=1}^{\infty} a(n) q^n , \quad q = e^{2\pi i\tau},$$

веса 1 и характера ε относительно группы $\Gamma_0(N)$ такая, что для всех простых $p \nmid 2\beta(\tau^2+\beta)$ справедливо равенство

$$a(p) = \sigma(p) . \qquad (3)$$

ЗАМЕЧАНИЕ. Отметим, что из $p|N$ следует $p \mid 2\beta(\tau^2+\beta)$; отметим также, что сам ряд

$$\sum_{n=1}^{\infty} \sigma(n) q^n , \quad q = e^{2\pi i\tau},$$

не является параболической формой; это легко доказать, сравнивая эйлеровские множители рядов Дирихле

$$L(s) = \sum_{n=1}^{\infty} a(n)\, n^{-s}$$

и

$$Z(s) = \sum_{n=1}^{\infty} \sigma(n)\, n^{-s}\ .$$

Некоторые непосредственные следствия равенства (3) приведены в пункте 4 работы.

I. Сначала будет доказана теорема 2. Начнем с необходимых лемм. Пусть $\Psi(h) = h^4 + 2\tau h^2 - \beta$. Для простого p положим

$$S(p) = \#\{a \in F_p \mid \Psi(a) \equiv 0 \pmod p\}.$$

Тогда имеет место

ЛЕММА I. Пусть p - простое число, не делящее $2\beta(\tau^2+\beta)$. Тогда

$$S(p) = 1 + \left(\frac{\tau^2+\beta}{p}\right) + \sigma(p)\ . \qquad (4)$$

ДОКАЗАТЕЛЬСТВО.

I. Пусть $\left(\frac{\tau^2+\beta}{p}\right) = 1$. Обозначим через f_1, f_2 решения сравнения

$$f^2 + 2\tau f - \beta \equiv 0 \pmod p\ .$$

Имеем

$$f_1 f_2 \equiv -\beta \pmod p,\quad \sigma(p) = \left(\frac{f_1}{p}\right) + \left(\frac{f_2}{p}\right) = \left(\frac{f_1}{p}\right)\left(1 + \left(\frac{-\beta}{p}\right)\right).$$

1) Пусть $\left(\frac{-\beta}{p}\right) = 1$. Если $\left(\frac{f_1}{p}\right) = 1$, то $\sigma(p)=2$. Легко видеть, что $S(p)=4$; следовательно, равенство (4) доказано.

Если же $\left(\frac{f_1}{p}\right) = -1$, то $\sigma(p) = -2$. Легко видеть, что $S(p) = 0$; следовательно, равенство (4) доказано.

2) Пусть $\left(\frac{-\beta}{p}\right) = -1$. Легко видеть, что $S(p) = 2$ и $\sigma(p) = 0$. Следовательно, равенство (4) доказано.

II. Пусть $\left(\frac{\tau^2+\beta}{p}\right) = -1$. Ясно, что $S(p) = 0$ и $\sigma(p) = 0$. Равенство (4) доказано.

Следовательно, доказана и лемма I.

Получим теперь другое представление для $S(p)$. Рассмотрим уравнение

$$h^4 + 2\tau h^2 - \beta = 0\ .$$

Корни этого уравнения:

$$\varepsilon^{(0)}=\sqrt{\sqrt{\tau^2+\beta}-\tau}\,,\qquad \varepsilon^{(1)}=\sqrt{-\sqrt{\tau^2+\beta}-\tau}\,,$$
$$\varepsilon^{(2)}=-\varepsilon^{(0)}\,,\qquad \varepsilon^{(3)}=-\varepsilon^{(1)}\,.$$

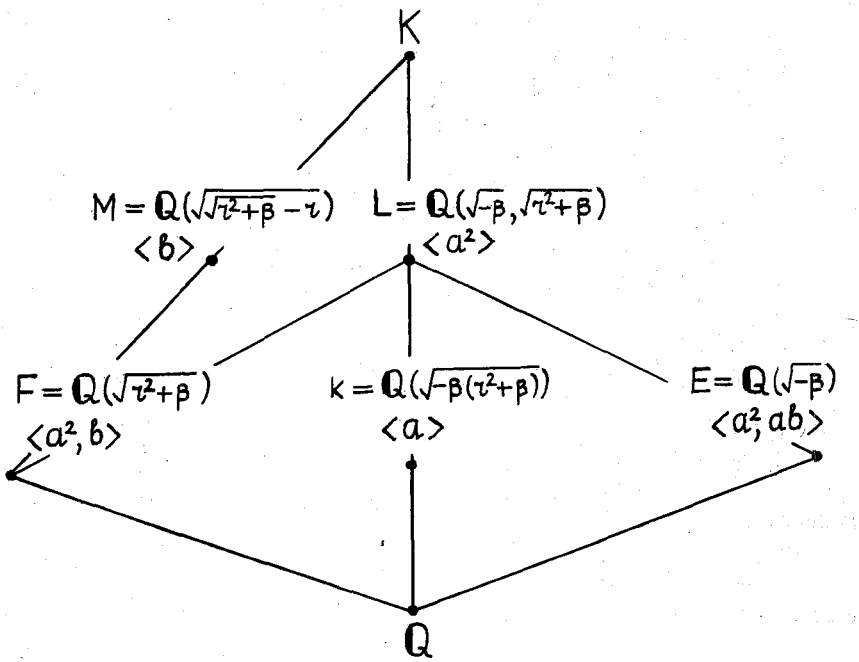
Пусть $K=\mathbb{Q}(\varepsilon^{(0)},\varepsilon^{(1)})$ - поле, порожденное $\varepsilon^{(0)}$ и $\varepsilon^{(1)}$ над полем рациональных чисел $\mathbb{Q}$. Тогда K является расширением Галуа над $\mathbb{Q}$ степени 8 и его группа Галуа $G=G(K/\mathbb{Q})$ изоморфна диэдральной группе D_4 порядка 8. Рассмотрим подстановки

$$a=\begin{pmatrix}\varepsilon^{(0)} & \varepsilon^{(1)} & \varepsilon^{(2)} & \varepsilon^{(3)}\\ \varepsilon^{(1)} & \varepsilon^{(2)} & \varepsilon^{(3)} & \varepsilon^{(0)}\end{pmatrix},\qquad b=\begin{pmatrix}\varepsilon^{(0)} & \varepsilon^{(1)} & \varepsilon^{(2)} & \varepsilon^{(3)}\\ \varepsilon^{(0)} & \varepsilon^{(3)} & \varepsilon^{(2)} & \varepsilon^{(1)}\end{pmatrix}.$$

Можно считать, что

$$G=\langle a,b \mid a^4=1,\ b^2=1,\ bab=a^{-1}\rangle.$$

Имеет место следующая диаграмма подполей поля K :



Сопоставим теперь полю K параболическую форму $S^*(\tau, K) = S^*(\tau)$ веса I. Пусть ψ - (единственное) двумерное комплексное неприводимое представление группы $G = G(K/\mathbf{Q})$, определяемое посредством

$$\psi(a) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \quad \psi(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Тогда представление $\det\psi$ группы G, определяемое посредством $(\det\psi)(g) = \det\psi(g)$, индуцирует характер Дирихле ε.

Определим L-функцию Артина, ассоциированную с ψ:

$$L(s) = L(s, K/\mathbf{Q}, \psi) = \sum_{n=1}^{\infty} a(n)\, n^{-s}.$$

Тогда $L(s, K/\mathbf{Q}, \psi)$ имеет эйлеровское произведение

$$L(s\ K/\mathbf{Q}, \psi) =$$

$$= \prod_{p \mid N} (1 - a(p)\, p^{-s})^{-1} \cdot \prod_{p \nmid N} (1 - a(p)\, p^{-s} + \varepsilon(p)\, p^{-2s})^{-1},$$

где N обозначает кондуктор ψ. Определим функцию $S^*(\tau) = S^*(\tau, K)$:

$$S^*(\tau) = \sum_{n=1}^{\infty} a(n)\, q^n, \quad q = e^{2\pi i \tau}.$$

ЛЕММА 2. $S^*(\tau)$ является параболической формой (новой формой) веса 1 характера ε относительно группы $\Gamma_0(N)$.

ДОКАЗАТЕЛЬСТВО следует из хорошо известных результатов теории Гекке-Вейля (см. Серр [I]).

ЛЕММА 3. Пусть p - простое число, не делящее $2\beta(\tau^2+\beta)$. Тогда

$$S(p) = 1 + \left(\frac{\tau^2+\beta}{p}\right) + a(p). \qquad (5)$$

ДОКАЗАТЕЛЬСТВО. Мы используем соображения из работы [2].

Рассмотрим все неприводимые представления группы G:

	a	b
ψ_0	1	1
ψ_1	1	-1
ψ_2	-1	1
ψ_3	-1	-1
ψ	$\begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Можно показать, что из $p \mid N$ следует $p \mid 2\beta(\tau^2+\beta)$. Для p, неразветвленного в K (что равносильно $p \nmid N$), обозначим через σ_p подстановку Фробениуса, ассоциированную с p. Пусть χ - характер представления ψ. Между квадратичными подполями k, F, E поля K и представлениями ψ_i $(1 \leqslant i \leqslant 3)$ имеется соответствие. Справедливы соотношения $(p \nmid 2\beta(\tau^2+\beta))$

$$\psi_1(\sigma_p) = \left(\frac{-\beta(\tau^2+\beta)}{p}\right),$$

$$\psi_2(\sigma_p) = \left(\frac{\tau^2+\beta}{p}\right),$$

$$\psi_3(\sigma_p) = \left(\frac{-\beta}{p}\right).$$

Кроме того,

$$\chi(\sigma_p) = a(p).$$

Пусть $H = \langle b \rangle$. Тогда H есть подгруппа группы G, соответствующая подполю $M = \mathbb{Q}(\sqrt{\tau^2+\beta} - \tau)$. Обозначим через $\nu = 1_H^G$ характер группы G, индуцированный единичным характером 1_H подгруппы H. Имеют место следующие формулы для

скалярных произведений:

$$(\nu\,|\,\psi_i) = \begin{cases} 0 & (i=1,3)\ ; \\ 1 & (i=0,2)\ ; \end{cases}$$

$$(\nu\,|\,\chi) = 1\ .$$

Таким образом,

$$\nu = \psi_0 + \psi_2 + \chi\ .$$

Для $p \nmid N$ мы имеем

$$\nu(\sigma_p) = S(p)\ .$$

Следовательно, для $p \nmid 2\beta(\tau^2+\beta)$

$$S(p) = 1 + \left(\frac{\tau^2+\beta}{p}\right) + a(p)\ .$$

Лемма 3 доказана.

Справедливость теоремы 2 следует теперь из лемм I,2,3.

2. Докажем теперь теорему I. Сначала сформулируем необходимую нам лемму, доказательство которой см. в [3], [4].

ЛЕММА 4. Имеем

$$\left|L\left(\tfrac{1}{2}+it\right)\right| \ll (|t|+1)^{\frac{1}{3}+\varepsilon}\ ,$$

где $\varepsilon > 0$.

Далее, используя мультипликативность $\sigma(n)$, легко получить свойства функции

$$Z(s) = \sum_{n=1}^{\infty} \sigma(n)\, n^{-s}$$

в полуплоскости $\sigma = \operatorname{Re} s \geqslant \frac{1}{2}+\varepsilon$, $\varepsilon > 0$, из хорошо известных свойств функции $L(s)$; в частности, функция $Z(s)$ в этой полуплоскости голоморфна. С помощью леммы 4 доказываем, что в полосе $\frac{1}{2}+\varepsilon \leqslant \sigma \leqslant 1+\varepsilon$, $\varepsilon > 0$, имеет место оценка ($s=\sigma+it$)

$$|Z(s)| \ll (|t|+1)^{\frac{2}{3}(1-\sigma)+\varepsilon}\ , \quad \varepsilon > 0\ . \qquad (6)$$

По хорошо известной формуле обращения для рядов Дирихле имеем

$$\sum_{n \leqslant x} \sigma(n) =$$

$$= \frac{1}{2\pi i}\int_{1-iT}^{1+iT} Z(s)\,\frac{x^s}{s}\,ds \;+\; O\left(\frac{x^{1+\varepsilon}}{T}\right).$$

Сдвигая прямую интегрирования до прямой $\operatorname{Re} s = \frac{1}{2}+\varepsilon$ и произведя необходимые вычисления с помощью оценки (6), получаем

$$\sum_{n\le x} \sigma(n) \ll x^{\frac{1}{2}+\varepsilon} T^{\frac{1}{3}+\varepsilon} + \frac{x^{1+\varepsilon}}{T}.$$

Полагая $T = x^{3/8}$, доказываем теорему I.

3. Дадим теперь одно приложение теоремы I′. Рассмотрим суммы

$$P_+(x) = \sum_{k\le x} \sum_{\substack{\nu^2+2\tau\nu-\beta\equiv 0 \,(\mathrm{mod}\, k),\\ 0<\nu\le k,\ (\frac{\nu}{k})=+1}} e^{2\pi i h\nu/k}, \qquad P_-(x) = \sum_{k\le x} \sum_{\substack{\nu^2+2\tau\nu-\beta\equiv 0 \,(\mathrm{mod}\, k),\\ 0<\nu\le k,\ (\frac{\nu}{k})=-1}} e^{2\pi i h\nu/k}.$$

Применяя соображения работы Холи [5], можно получить следующую лемму, доказательство которой здесь не приводится.

ЛЕММА 5. Имеют место оценки ($h \neq 0$ целое)

$$P_+(x) \ll \frac{\tau(|h|)\, x\, (\log\log x)^{5/2}}{\log^{\delta} x}, \qquad (7)$$

$$P_-(x) \ll \frac{\tau(|h|)\, x\, (\log\log x)^{5/2}}{\log^{\delta} x},$$

где $\delta = \frac{1}{2}(2-\sqrt{2}) = 0{,}292\ldots$; $\tau(n)$ – число делителей n.

Возьмем теперь все числа вида $\frac{\nu}{k}$, где

$$\nu^2+2\tau\nu-\beta \equiv 0 \,(\mathrm{mod}\, k), \quad 0<\nu\le k, \quad (\tfrac{\nu}{k}) = +1.$$

Расположим их в виде последовательности $p_1^+, p_2^+, \ldots, p_m^+, \ldots$ в порядке возрастания знаменателей (расположение чисел в группе, соответствующей фиксированному значению k, несущественно).

Рассмотрим сумму

$$\sum_{m\le N} e^{2\pi i h p_m^+}$$

для каждого ненулевого целого значения h. Если M – знаменатель

в p_N^+ , то из теоремы I′ имеем

$$N > \sum_{k<M} \rho_+(k) > AM ,$$

где $A>0$ - константа. Далее по лемме 5

$$\sum_{m\leqslant N} e^{2\pi i h p_m^+} =$$

$$= \sum_{k<M} \sum_{\substack{\nu^2+2\tau\nu-\beta\equiv 0 \,(\mathrm{mod}\, k) \\ 0<\nu\leqslant k,\ (\frac{\nu}{k})=+1}} e^{2\pi i h\nu/k} + O(\rho_+(M)) \ll$$

$$\ll \tau(|h|)\,\frac{N(\log\log N)^{5/2}}{\log^{\delta} N} ,$$

и, таким образом, для любого целого $h\neq 0$

$$\frac{1}{N}\left|\sum_{m\leqslant N} e^{2\pi i h p_m^+}\right| \longrightarrow 0 \quad (N\to\infty) .$$

Аналогичный факт верен и для сходно определяемой (с заменой условия $(\frac{\nu}{k})=+1$ на $(\frac{\nu}{k})=-1$) последовательности $p_1^-, p_2^-, \cdots, p_m^-, \cdots$.

Тем самым в силу критерия Г.Вейля имеет место следующая

ТЕОРЕМА 3. *Последовательности*

$$p_1^+, p_2^+, \ldots, p_m^+, \ldots \quad \text{и} \quad p_1^-, p_2^-, \ldots, p_m^-, \ldots$$

равномерно распределены на интервале (0,I).

ЗАМЕЧАНИЕ. Впервые сходный результат о распределении дробей ν/k , где

$$\nu^2 \equiv D \,(\mathrm{mod}\, k) \quad \text{и} \quad 0<\nu\leqslant k ,$$

получил Холи [6]. Для тригонометрической суммы $(h\neq 0)$

$$P(x) = \sum_{k\leqslant x} \sum_{\substack{\nu^2\equiv D\,(\mathrm{mod}\,k), \\ 0<\nu\leqslant k}} e^{2\pi i h\nu/k}$$

он сумел получить следующую оценку:

$$|P(x)| \leqslant A(h)\, x^{\frac{3}{4}} \log^2 x$$

(впоследствии В.А.Быковский [7] понизил показатель 3/4 до 2/3).

4. Получим также одно непосредственное следствие теоремы 2. Пусть p - простое число, $\rho_+(p)$ и $\rho_-(p)$ имеют прежний смысл. Пусть

$$\pi_+(x) = \sum_{p \le x} \rho_+(p), \qquad \pi_-(x) = \sum_{p \le x} \rho_-(p).$$

Применяя методы аналитической теории чисел, используемые при доказательстве асимптотического закона распределения простых чисел, имеем

$$\sum_{p \le x} a(p) \log p \ll x e^{-A\sqrt{\log x}}, \quad A > 0. \qquad (8)$$

Из теоремы 2 и оценки (8) легко получаем следующие асимптотические формулы

$$\pi_+(x) = \frac{1}{2} \mathrm{Li}(x) + O(x e^{-B\sqrt{\log x}}),$$

$$\pi_-(x) = \frac{1}{2} \mathrm{Li}(x) + O(x e^{-B\sqrt{\log x}}),$$

где $B > 0$, $\mathrm{Li}(x)$ - интегральный логарифм.

Литература

1. S e r r e J.-P. Modular forms of weight one and Galois representations. - In: Proc.Symposium on Algebraic Number Fields. London, 1977, p.193-268.
2. I s h i i N. Cusp forms of weight one, quartic reciprocity and elliptic curves. - Nagoya Math.J., 1985, vol.98, p.117-137.
3. G o o d A. The square mean of Dirichlet series associated with cusp forms. - Mathematika, 1982, vol.29, N 58, p.278-295.
4. J u t i l a M. Lectures on a method in the theory of exponential sums. - Tata Institute of Fundamental Research. Berlin etc., 1987. 134 p.
5. H o o l e y C. On the distribution of the roots of polynomial congruences. - Mathematika, 1964, vol.11, N 21, p.39-49.
6. H o o l e y C. On the number of divisors of quadratic polynomials. - Acta math., 1963, vol.110, N 1-2, p.97-114. (есть русский перевод: Математика. Периодический сборник переводов иностранных статей, 1968, т.12, № 5, с.3-18).
7. Б ы к о в с к и й В.А. Спектральные разложения некоторых автоморфных функций и их теоретико-числовые приложения. - В кн.: Автоморфные функции и теория чисел. 2. Зап.научн.семин. ЛОМИ, 1984, т.134, с.15-33.