УДК 511

О распределении решений сравнения $x^2 + y^2 \equiv 1 (\mathrm{mod}\, p^l)$

П. Д. Варбанец

В работе [1] с помощью тонких рассуждений арифметического характера получена асимптотическая формула для количества решений сравнения

$$x^2 + y^2 \equiv 1 \ (\mathrm{mod}\, p^l), \quad p \text{ — простое,} \tag{1}$$

в прямоугольнике

$$0 \leqslant x \leqslant T_1, \quad 0 \leqslant y \leqslant T_2, \quad p^{\frac{4l+3}{6}} \leqslant T_2 \leqslant p^l, \quad 1 \leqslant T_1 \leqslant p^l; \quad l \geqslant 12,$$

$$\sum_{\substack{x^2+y^2\equiv 1 \ (\mathrm{mod}\, p^l), \\ 0\leqslant x\leqslant T_1, \\ 0\leqslant y\leqslant T_2}} 1 = \frac{T_1T_2}{p^l} \cdot \frac{p-(-1)^{\frac{p-1}{2}}-2}{p} + O\left(e^{7l^3 \log l}\, T_2^{1-\frac{1}{28l^3 \log 27l^3}}\right). \tag{2}$$

Если $T_2 = p^s$, $\frac{4l+13}{6} \leqslant s \leqslant l$, то формула Постниковой нетривиальна лишь при $T_1 \geqslant c(l)\, p^{l-\frac{s}{28l^3 \log 27l^3}}$, т. е. T_1 должно быть близко к своему максимальному значению.

В настоящей заметке дается формула для количества решений сравнения (1) в более широком диапазоне изменения T_1 и T_2. Для этого используется другой подход к задаче.

Сначала, опираясь на результаты и технику, относящиеся к проблеме целых точек в круге, доказывается теорема.

Теорема 1. *Для количества решений сравнения* (1), $B(T)$, *для которых*

$$x^2 + y^2 \leqslant T, \quad x \geqslant 0, \quad y \geqslant 0,$$

справедлива асимптотическая формула

$$B(T) = \frac{\pi T}{4p^l} \frac{p+1}{p} + O\left(\frac{T^{5/6}}{p^l}\right) \tag{3}$$

с абсолютной постоянной в символе «O».

Теорема 1 относится к распределению решений сравнения в однопараметрической области.

Для решения задачи в прямоугольной области используется аналитическая теория характеров Гекке (второго рода) поля гауссовых чисел. По классической схеме (см., например, [2]) для получения необходимых нам оценок сумм характеров используется комплексное обращение Z-функций Гекке с переносом прямой интегрирования в отрицательную полуплоскость, после чего применяется функциональное уравнение для Z-функций Гекке. Обратим внимание на то, что нам не достаточно тривиальной оценки множителя $\chi(\Xi)$, возникающего в функциональном уравнении.

Мы предполагаем, что модуль имеет специальный вид p^l, $p \equiv 3 \pmod 4$. В этом случае структура группы G_l классов вычетов, взаимно простых с модулем p^l в кольце целых гауссовых чисел, определяется следующей леммой.

Лемма. *Каждый вычет $x+iy$ группы G_l однозначно представим в виде*

$$x+iy \equiv g^{\alpha}(u+iv)^{\beta} \pmod{p^l}, \quad \alpha = 0, 1, \ldots, \quad \frac{p-1}{2}p^{l-1}-1;$$

$$\beta = 0, 1, \ldots, \quad 2(p+1)p^{l-1}-1,$$

где g — первообразный корень по модулю p^l в кольце целых рациональных чисел, а $u+iv$ — некоторое целое гауссово число так, что $(u+iv)^t \equiv 1 \times$ $\times \pmod{p^l}$ только при $t \equiv 0 \pmod{2(p+1)p^{l-1}}$.

Пусть теперь характер Гекке $\Xi(\alpha) = \xi(\alpha, m)\chi(\alpha)$ выбран так, что для соответствующего ему группового характера $\chi(\alpha)$ справедливо равенство $\chi(\alpha) = \chi_{p^l}(N(\alpha))$, где χ_{p^l} — характер группы классов вычетов, взаимно простых с модулем p^l в кольце целых рациональных чисел. В этом случае справедливо утверждение.

Теорема 2. *Пусть $m \neq 0$, $-1/2 \leqslant \sigma_1 \leqslant 0$, $1 \leqslant \sigma_2 \leqslant 2$. В области*

$$\sigma_1 - \frac{1}{2l}\,\overset{-1}{\log}(MT) \leqslant \sigma \leqslant \sigma_2 + \overset{-1}{\log}(MT), \quad M = |m|+3, \quad T = |t|+1$$

имеет место оценка

$$\sum_{\chi_{p^l}} Z(s, \Xi) = O\left(l^{\frac{\sigma_2-\sigma}{\sigma_2-\sigma_1}}\, p^{l\left(1-\left(2\sigma_1-\frac{1}{2}\right)\frac{\sigma_2-\sigma}{\sigma_2-\sigma_1}+\frac{1}{l}\right)}(MT)^{\frac{1-2\sigma_1}{\sigma_2-\sigma_1}(\sigma_2-\sigma)}\log(MT)\right) \qquad (4)$$

с абсолютной постоянной в символе «O».

Суммирование в (4) ведется по всем характерам χ_{p^l}.

При доказательстве этой теоремы существенно используется то, что множитель $\varkappa(\Xi)$ «порождает» рациональную тригонометрическую сумму, оценку которой дает теорема Хуа Ло Кена (см. [3], стр. 64).

Следствие. *При $m \neq 0$ справедлива оценка*

$$\sum_{\chi_{p^l}} Z(0, \Xi) = O\left(l p^{\frac{3}{2}l+1} M \log M\right). \qquad (5)$$

Теоремы 1 и 2 позволяют получить асимптотическую формулу для количества решений сравнения (1) в секториальной области.

Теорема 3. *Пусть $p^{\frac{3l+2}{2-4\alpha}} \leqslant x \leqslant p^{2l}$, p — простое, $p \equiv 3 \pmod 4$, $l > 3$ — натуральное, $\alpha \leqslant \frac{1}{8} - \frac{1}{4l}$, $\varphi_2 - \varphi_1 > x^{-\alpha}$. Тогда имеет место асимптотическая формула*

$$\sum_{\substack{u^2+v^2 \leqslant x,\\ u^2+v^2 \equiv 1 \pmod{p^l},\\ \varphi_1 < \arg(u+iv) \leqslant \varphi_2}} 1 = \frac{\varphi_2-\varphi_1}{2}\cdot\frac{x}{p^l}\frac{p+1}{p} + O\left(\frac{x^{1-\alpha}}{p^l}\log x^{\alpha}\right). \qquad (6)$$

Постоянная в символе «O» зависит от l.

Проводя теперь секторную аппроксимацию прямоугольной области, получим следующее.

Теорема 4. *Пусть* $A(T_1, T_2)$ *означает количество решений сравнения* (1) *при условии* $0 \leqslant x \leqslant T_1$, $0 \leqslant y \leqslant T_2$, *где* $p^{\frac{3l+2}{4-8\alpha}} \leqslant T_1 \leqslant p^l$, $T_1^{1-\alpha} \leqslant T_2 \leqslant p^l$, $\alpha \leqslant \frac{1}{8} - \frac{1}{4l}$, $l > 3$.

Тогда имеем

$$A(T_1, T_2) = \frac{T_1 T_2}{p^l} \frac{p+1}{p} + O\left(\frac{T_1^{1-\alpha} T_2}{p^l} \log T_1^{\alpha}\right) \tag{7}$$

с постоянной в символе «О», зависящей от l.

ЛИТЕРАТУРА

1. Л. П. Постникова, Распределение решений сравнения $x^2 + y^2 \equiv 1 \pmod{p^n}$, Матем. сб., т. 65, вып. 2, 1964.
2. И. П. Кубилюс, Об одной задаче многомерной аналитической теории чисел, Ученые труды Вильнюсского гос. ун-та, сер. матем., физ. и хим. наук, т. 4, стр. 5—41.
3. Хуа Ло Кен, Метод тригонометрических сумм и его применения в теории чисел, М., 1964.

Поступила 14.XI 1966 г.

Одесский государственный университет