Записки научных
семинаров ПОМИ
Том 330, 2006 г.

А. И. Генералов

КОМБИНАТОРНОЕ ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ ЭЙЛЕРА–ФЕРМА О ПРЕДСТАВЛЕНИИ ПРОСТЫХ ЧИСЕЛ ВИДА $p=8k+3$ КВАДРАТИЧНОЙ ФОРМОЙ x^2+2y^2

В [1] Д. Цагир предложил чрезвычайно короткое и изящное доказательство теоремы Ферма о представлении простых чисел вида $p = 4k+1$ суммой двух квадратов целых чисел: на некотором конечном множестве Ω рассматривается действие двух инволюций; одна инволюция имеет единственную неподвижную точку, что доказывает нечётность мощности $|\Omega|$, а неподвижные точки второй инволюции доставляют требуемое представление простого числа. В настоящей заметке аналогичный подход применяется для доказательства следующей теоремы.

Теорема 1. *Пусть p – простое число, сравнимое с 3 по модулю 8. Тогда p представляется в виде $p = x^2 + 2y^2$ для некоторых натуральных чисел x и y.*

Доказательство. Пусть

$$\Omega = \{(x, y, z) \in \mathbb{N}^3 \mid p = x^2 + 2yz\}. \tag{1}$$

Заметим, что множество Ω конечно (поскольку для $(x, y, z) \in \Omega$ имеем $x, y, z < p/2$) и непусто (так как точка $\omega_0 = (1, 1, (p-1)/2)$ принадлежит Ω). Отметим также, что если $(x, y, z) \in \Omega$, то x, y, z нечётны; кроме того, так как $p = x^2 + 2y^2 + 2y(z - y)$ и $x^2 \equiv y^2 \equiv 1 (\mathrm{mod}\, 8)$, то $2y(z-y)$ делится на 8 и, следовательно, $z-y$ делится на 4.

Множество Ω является дизъюнктным объединением следую-

Работа поддержана грантом РФФИ 06-01-00200.

щих множеств:

$$\begin{aligned}
\Omega_0 &= \left\{(x,y,z)\in\Omega \mid y-\frac{z}{2}<x<2y\right\},\\
\Omega_1 &= \{(x,y,z)\in\Omega \mid x>2y\},\\
\Omega_2 &= \left\{(x,y,z)\in\Omega \mid x<\frac{y}{2}-z\right\},\\
\Omega_3 &= \left\{(x,y,z)\in\Omega \mid \frac{y}{2}-z<x<\frac{2}{3}(y-z)\right\},\\
\Omega_4 &= \left\{(x,y,z)\in\Omega \mid \frac{2}{3}(y-z)<x<y-\frac{z}{2}\right\};
\end{aligned}$$

действительно, если $(x,y,z)\in\Omega$, то $y-\frac{z}{2}\neq x\neq\frac{y}{2}-z$ (так как y и z нечётны), $2y\neq x\neq\frac{2}{3}(y-z)$ (так как x нечётно). Построим следующее отображение $\Phi\colon\Omega\to\Omega$:

$$\Phi(x,y,z)= \tag{2}$$

$$\begin{cases}
(2y-x,\ y,\ z+2x-2y), & \text{если } (x,y,z)\in\Omega_0,\\
(x-2y,\ z+2x-2y,\ y), & \text{если } (x,y,z)\in\Omega_1,\\
(x+2z,\ z,\ y-2x-2z), & \text{если } (x,y,z)\in\Omega_2,\\
(-3x+2y-2z,-2x+2y-z,2x-y+2z), & \text{если } (x,y,z)\in\Omega_3,\\
(3x-2y+2z,2x-y+2z,-2x+2y-z), & \text{если } (x,y,z)\in\Omega_4.
\end{cases}$$

Непосредственно проверяется, что

$$\left.\begin{aligned}\Phi(\Omega_0)\subset\Omega_0,\Phi(\Omega_1)\subset\Omega_2,\Phi(\Omega_2)\subset\Omega_1,\\ \Phi(\Omega_3)\subset\Omega_3,\Phi(\Omega_4)\subset\Omega_4,\end{aligned}\right\} \tag{3}$$

и затем устанавливается, что $\Phi\circ\Phi=\mathrm{id}_\Omega$. Отсюда, в частности, следует, что в (3) все включения можно заменить на равенства.

Легко проверяется, что ω_0 – единственная неподвижная точка инволюции Φ. Следовательно, мощность $|\Omega|$ нечётна.

Теперь рассмотрим другую инволюцию на множестве Ω:

$$\Psi\colon\Omega\to\Omega,\quad (x,y,z)\mapsto(x,z,y).$$

Эта инволюция должна иметь неподвижную точку $(x_0,y_0,y_0)\in\Omega$, и таким образом, $p=x_0^2+2y_0^2$. □

Замечание 2. Предположим, что простое p сравнимо с 1 по модулю 8. Вновь рассмотрим множество Ω из (1) и инволюцию Φ, определенную в (2). Если $(x, y, z) \in \Omega$, то легко проверяется, что x нечётно, а yz делится на 4, однако, как и в условиях теоремы 1, $\Omega = \bigcup_{i=0}^{4} \Omega_i$. Но сейчас, кроме точки ω_0, Φ имеет ещё две неподвижные точки: по точке в Ω_3 и Ω_4 (таким образом, и в этом случае применимы рассуждения из доказательства теоремы 1). Единственность неподвижной точки в области Ω_4 (соответственно в Ω_3) устанавливается с использованием арифметики кольца $\mathbb{Z}[i]$ целых гауссовых чисел (соответственно кольца целых поля $\mathbb{Q}(\sqrt{2})$)... Но в таком случае для доказательства существования (и единственности) представления $p = x^2+2y^2$ значительно проще использовать напрямую арифметику кольца целых поля $\mathbb{Q}(\sqrt{-2})$.

Литература

1. D. Zagier, *A one-sentence proof that every prime $p \equiv 1 (\mathrm{mod}\, 4)$ is a sum of two squares.* — Amer. Math. Monthly **97**, No. 2 (1990), 144.

Generalov A. I. A combinatorial proof of Euler–Fermat's theorem on presentation of primes of the form $p = 8k + 3$ by the quadratic form $x^2 + 2y^2$.

An elementary and extremely short proof of the theorem on presentation of primes of the form $p = 8k + 3$ by the quadratic form $x^2 + 2y^2$ with integers x, y.

С.-Петербургский
государственный университет

Поступило 10 декабря 2005 г.