

## 28. Вокруг рождественской теоремы Ферма

18 июля

**Упражнение.** Дано натуральное число  $m$ . Известно, что для некоторого натурального  $n$  число  $2^n \cdot m$  представимо в виде суммы квадратов двух целых чисел. Докажите, что тогда и  $m$  представимо в таком виде.

**Решение.** Пусть  $2^n \cdot m = x^2 + y^2$ . Заметив, что  $x$  и  $y$  одной четности, получаем

$$\left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 = \frac{x^2+y^2}{2} = 2^{n-1} \cdot m.$$

Спускаясь далее аналогично, получаем требуемое.

Осознаем, что подобная замена была вполне естественной. Действительно, рассмотрим уравнение  $a^2 + b^2 = 2$  (в нашем случае  $a = b = 1$ ). Разложив в кольце  $\mathbb{Z}[i]$ , получаем  $(a + bi)(a - bi) = 2$ . С другой стороны  $(x + yi)(x - yi) = 2^n \cdot m$ . У нас возникает желание по аналогии с уравнением Пелля разделить одно решение на другое, чтобы получить  $2^{n-1} \cdot m$ . Имеем

$$\frac{x + yi}{a + bi} \cdot \frac{x - yi}{a - bi} = (x + yi) \left(\frac{a}{2} - \frac{b}{2}i\right) \cdot \overline{(x + yi) \left(\frac{a}{2} - \frac{b}{2}i\right)} = \left(\frac{xa + yb}{2} + \frac{ya - xb}{2}i\right) \cdot \left(\frac{xa + yb}{2} - \frac{ya - xb}{2}i\right).$$

Мы воспользовались, тем, что  $\frac{a}{2} - \frac{b}{2}i$  является обратным к числу  $a + bi$ . Осталось лишь заметить, что в паре  $\left(\frac{xa + yb}{2}, \frac{ya - xb}{2}\right)$  оба числа являются целыми.

Подобная техника спуска достаточно естественна и применяется при попытке обобщения Рождественской теоремы Ферма. Теперь временно забудем про все вышесказанное.

**1. Рождественская теорема Ферма.** Нечетное простое число  $p$  представимо в виде суммы двух квадратов целых чисел тогда и только тогда, когда  $p \equiv 1 \pmod{4}$ .

(a) Докажите, что если  $p = a^2 + b^2$  для целых  $a$  и  $b$ , то  $p \equiv 1 \pmod{4}$ ;

(b) Пусть  $p \equiv 1 \pmod{4}$ . Обозначим через  $i$  вычет по модулю  $p$  такой, что  $i^2 \equiv -1 \pmod{p}$ . Пусть каждое из чисел  $a$  и  $b$  бегаёт в диапазоне  $0, 1, 2, 3, \dots, [\sqrt{p}]$ . Докажите, что найдутся различные пары  $(a_1, b_1)$  и  $(a_2, b_2)$  из данного диапазона такие, что  $a_1 - ib_1 \equiv a_2 - ib_2 \pmod{p}$ ;

(c) Завершите доказательство рождественской теоремы Ферма.

**2. (a)** Два числа представляются в виде суммы двух квадратов целых чисел. Докажите, что их произведение представляется в виде двух квадратов.

(b) Докажите, что натуральное число  $N$  представимо в виде суммы квадратов двух целых чисел тогда и только тогда, когда каждое простое число вида  $4k + 3$  входит в разложение  $n$  на простые множители в четной степени.

**3.** Докажите, что уравнение  $x^2 + y^2 = z^5 + z$  имеет бесконечно много целых решений, в которых  $x$ ,  $y$  и  $z$  попарно взаимно просты.

**4.** Какие простые числа представимы

(a) в виде  $x^2 + 2y^2$  для целых  $x$  и  $y$ ?

*Подсказка.* Сначала поймите, по каким простым модулям  $-2$  является квадратичным вычетом. Затем попробуйте сделать то же, что и в первой задаче. Из рассуждения должно получиться, что  $p = x^2 + 2y^2$  или  $2p = x^2 + 2y^2$ .

(b) в виде  $x^2 + 3y^2$  для целых  $x$  и  $y$ ?

**5.** Какие простые числа представимы в виде (a)  $x^2 - 2y^2$ ; (b)  $x^2 - 7y^2$  для целых  $x$  и  $y$ ?

**6.** Какие простые числа представимы в виде  $x^2 + 5y^2$  для целых  $x$  и  $y$ ?

**7.** Какие простые числа представимы в виде  $x^2 + xy + y^2$  для целых  $x$  и  $y$ ?

**8.** Докажите, что не существует целого  $n$  такого, что  $n^7 + 7$  является квадратом целого числа.

**9.** Все числа, которые можно представить в виде суммы квадратов двух взаимно простых натуральных чисел, выписаны в порядке возрастания. Докажите, что для любого  $n$  в этой последовательности можно найти  $n$  последовательных нечётных членов.