# 1 СУММЫ КВАДРАТОВ

## ФОРМУЛИРОВКА ТЕОРЕМЫ ФЕРМА-ЭЙЛЕРА-ГАУССА

Мы вооружились гауссовыми числами, поняли, что в них существует понятие делимости, обратимые числа, четверка ассоциированных, и что любое утверждение о делимости происходит с точностью до умножения на обратимое число.

Сформулируем теорему, которая говорит о том, какие простые числа могут быть представлены в виде суммы двух квадратов.

### ТЕОРЕМА ФЕРМА - ЭЙЛЕРА - ГАУССА

Пусть $p \in \mathbb{N}$ — нечетное простое число. Тогда следующие три утверждения эквивалентны друг другу:

(а) $p$ теряет простоту в $\mathbb{Z}[i]$.
(б) Существует решение уравнения $p = x^2 + y^2$, где $x, y \in \mathbb{Z}$.
(в) $p$ имеет остаток 1 при делении на 4 ($p = 4k + 1$).

Утверждение (в) ⇒ (б) — это рождественская теорема Ферма, это самая сложная часть, и мы ее оставим на потом. Наметим план, в каком порядке будем доказывать:

1. эквивалентность (б) и (а);
2. (б) ⇒ (в);
3. (в) ⇒ (а).

## ЭКВИВАЛЕНТНОСТЬ ПЕРВЫХ ДВУХ УТВЕРЖДЕНИЙ ТЕОРЕМЫ

(б) ⇒ (а)

Пусть существует разложение

$p = x^2 + y^2 = (x + yi)(x - yi)$.

Так как это разложение на 2 числа, ни одно из которых не является обратимым, $p$ не является простым в $\mathbb{Z}[i]$.

(а) ⇒ (б)

Пусть $p$ перестает быть простым в $\mathbb{Z}[i]$, т.е. существует нетривиальное разложение числа p на множители:

$p = (a + bi)(c + di)$.

Тогда $\bar{p} = p = (a - bi)(c - di)$.

Рассмотрим $p^2 = (a + bi)(c + di)(a - bi)(c - di) =$
$= (a + bi)(a - bi)(c + di)(c - di) = (a^2 + b^2)(c^2 + d^2)$,
причем оба числа в правой части равенства > 1.

По основной теореме арифметики для обычных целых чисел для квадрата простого числа существует единственное нетривиальное разложение на простые:

$p^2 = p \cdot p$.

Следовательно, оба эти множителя, которые мы получили, равны $p$:

$p = a^2 + b^2 = c^2 + d^2$.

Доказано.

## (Б) ⇒ (В)

Пусть $p = x^2 + y^2$.

Какие остатки при делении на 4 может давать квадрат числа?

Если число четное, оно равно $2k$ для некоторого целого $k$, и его квадрат $(2k)^2 = 4k^2$ имеет остаток 0 при делении на 4.

Если число нечетное, оно равно $2k + 1$ для некоторого целого $k$, и его квадрат $(2k + 1)^2 = 4k^2 + 4k + 1$ имеет остаток 1 при делении на 4.

Значит, у квадрата числа есть только 2 вида остатков: 0 и 1. Сумма этих остатков может быть равна только 0, 1 и 2. Но число $p$ — простое нечетное, и не может иметь остатки 0 или 2. Значит, $p = 4k + 1$.

Доказано.

# ПЛАН ДАЛЬНЕЙШЕГО ДОКАЗАТЕЛЬСТВА

Таким образом, для чисел 3, 7, 11, 19, 23 и всех простых вида $4k + 3$ невозможно представление в виде суммы двух квадратов. Если для небольших чисел мы могли бы это проверить перебором, то для числа 2027, например, перебор был бы долгим.

Итак, нам осталось доказать, что:
$p = 4k + 1 \Rightarrow$
существует представление $p = x^2 + y^2$, где $x, y \in \mathbb{Z}$.

Наметим путь, по которому мы будем идти к этому доказательству:

### ШАГ №1

$p = 4k + 1 \Rightarrow \exists\, c \in \mathbb{N}$ такое, что $c^2 + 1 \vdots p$.

Это важное утверждение, которое имеет отношение к так называемому квадратичному закону взаимности, будет нами доказано в рамках теории многочленов. Но мы его докажем здесь, опираясь на теорию остатков, в частности, теорему Вильсона.

### ШАГ №2

Часть основной теоремы арифметики в $\mathbb{Z}[i]$, а именно, следующее утверждение:

Если $z = a + bi \in \mathbb{Z}[i]$ — простое, то $w_1$, $w_2$ не делятся на $z \Rightarrow w_1 w_2$ не делится на $z$.

То есть в $\mathbb{Z}[i]$, как и в $\mathbb{Z}$, делимость на простые числа не приобретается при умножении.

### ШАГ №3

Полное доказательство ОТА в $\mathbb{Z}[i]$, которое мы применим для завершения решения задачи о двух квадратах и к выводу формулы пифагоровых троек.

## 2 ПРИМЕРЫ $c^2 + 1 \vdots p$

**1** ▶ $p = 5 = 4k + 1$ при $k = 1$
$c^2 + 1 = 5 \vdots 5$ при $c = 2$;

**2** ▶ $p = 13 = 4k + 1$ при $k = 3$
$c^2 + 1 = 5^2 + 1 = 26 \vdots 13$ при $c = 5$;

**3** ▶ $p = 17 = 4k + 1$ при $k = 4$
$c^2 + 1 = 4^2 + 1 = 17 \vdots 17$ при $c = 4$;

**4** ▶ $p = 29 = 4k + 1$ при $k = 7$
$c^2 + 1 = 12^2 + 1 = 145 \vdots 29$ при $c = 12$;

**5** ▶ $p = 37 = 4k + 1$ при $k = 9$
$c^2 + 1 = 6^2 + 1 = 37 \vdots 37$ при $c = 6$.