# 1 ОСНОВНАЯ ТЕОРЕМА АРИФМЕТИКИ В ГАУССОВЫХ ЧИСЛАХ И ЕЕ СЛЕДСТВИЯ

## ОСНОВНАЯ ТЕОРЕМА АРИФМЕТИКИ В $\mathbb{Z}[i]$

Прежде чем сформулировать основную теорему арифметики в гауссовых числах, заметим, что единственность в $\mathbb{Z}[i]$ возможна только с точностью до ассоциированности.

Например,

$5 = 22 + 12 = (2 + i)(2 - i)$ и, в то же время,
$5 = 12 + 22 = (1 + 2i)(1 - 2i)$.

На самом деле,

$(2 + i)(-i) = 1 - 2i$;
$(2 - i)i = 1 + 2i$,
то есть это пары ассоциированных чисел.

Таким образом два разложения для числа 5 получаются друг из друга умножением на $(-i)i = 1$.

**ТЕОРЕМА** (Основная теорема арифметики в $\mathbb{Z}[i]$)

Любое гауссово число $w$ может быть разложено в произведение гауссовых простых:

$w = z_1z_2 \ldots z_l$, где $z_1, z_2, \ldots z_l \in \mathbb{Z}[i]$.

Если при этом для $w$ существует другое разложение на простые: $w = s_1s_2 \ldots s_k$, то:

а) $l = k$;

б) каждое из $z_1, z_2, \ldots z_l$ ассоциировано с некоторым из $s_1, s_2, \ldots s_k$.

**ДОКАЗАТЕЛЬСТВО**

**1 ▶** Существование разложения.

Так как норма числа $w$ равна произведению норм множителей в его разложении, каждая из которых — целое число, большее $1$. Поэтому процесс разложения на простые гауссовы множители не может продолжаться бесконечно.

**1 ▶** Единственность разложения.

Предположим, что существуют два разных разложения: $w = z_1z_2 \ldots z_l = s_1s_2 \ldots s_k$.

Можем считать, что мы уже сократили все пары ассоциированных в этом равенстве.

Тогда ни одно $z_j$ не делится на $s_1$, а их произведение делится на $s_1$.

Получаем противоречие с утверждением о делимости произведения.

Следовательно, два данных разложения могут состоять только из пар ассоциированных гауссовых простых.

## СЛЕДСТВИЕ 1 ИЗ ОТА В $\mathbb{Z}[i]$

Пусть $w_1 w_2 \ldots w_r$ — попарно взаимно простые гауссовы числа, и при этом $w_1 w_2 \ldots w_r = z^n$.

Тогда для каждого из $w_j$ выполнено: $w_j = \sigma_j v_j^n$, где $\sigma_j$ — обратимое, $v_j$ — некоторое гауссово число.

### ДОКАЗАТЕЛЬСТВО

Представим число $z$ в виде произведения гауссовых простых:

$z = s_1^{\alpha_1} s_2^{\alpha_2} \ldots s_d^{\alpha_d} \sigma$, где — произведение обратимых, а значит, само обратимое.

Тогда $z^n = s_1^{n\alpha_1} s_2^{n\alpha_2} \ldots s_d^{n\alpha_d} \sigma^n$.

Каждая из групп $s_k^{n\alpha_k}$ должна полностью содержаться в некотором $w_j$, т.к. иначе $w_1, w_2, \ldots w_r$ не будут взаимно простыми.

Таким образом, замечая, что $\sigma^n$ будет обратимым, получаем что каждое из $w_j$ с точностью до обратимого есть $n$-я степень некоторого гауссова числа.

Следствие 1 доказано.

## СЛЕДСТВИЕ 2 ИЗ ОТА В $\mathbb{Z}[i]$ (ПОЛНОЕ ОПИСАНИЕ ПРОСТЫХ ЧИСЕЛ)

Во-первых, $q = 4k + 3$ — простое в $\mathbb{Z}$ сохраняет простоту в $\mathbb{Z}[i]$. Рассмотрим теперь гауссово простое $a + bi$, где $a, b \neq 0$.

### УТВЕРЖДЕНИЕ

Норма простого гауссова числа $N(a + bi) = a^2 + b^2$ есть простое число в $\mathbb{Z}$.

### ДОКАЗАТЕЛЬСТВО

От противного.

Пусть $a^2 + b^2 = (a + bi)(a - bi) = kl$, составное.

Если $a + bi$ — простое, то и $a - bi$ — простое. Для гауссова числа $a^2 + b^2$ получили два разложения на простые, что противоречит основной теореме арифметики.

Доказано.

Итак, $N(a + bi) = a^2 + b^2 = 4k + 1 = p$ — простое число в $\mathbb{Z}$.

Заметим, что $N(1 + i) = 2$, и при этом $1 + i$ и $1 - i$ — ассоциированные простые гауссовы числа.

В остальных случаях $a + bi$ и $a - bi$ — не ассоциированные простые, и каждое простое число $p \in \mathbb{Z}$ вида $4k + 1$ имеет единственное разложение на простые в $\mathbb{Z}[i]$: $p = (a + bi)(a - bi)$.

## 3 СЛЕДСТВИЕ 3 ИЗ ОТА В $\mathbb{Z}[i]$ (ПРЕДСТАВЛЕНИЕ В ВИДЕ СУММЫ КВАДРАТОВ)

Пусть $n = x^2 + y^2$. Тогда $n = (x + iy)(x - iy)$.

Сначала предположим, что $n$ нечетно.
Разложим каждый из множителей в произведение гауссовых простых.

$x + iy = q_1^{\alpha_1} \dots q_r^{\alpha_r}(a_1 + b_1 i) \dots (a_s + b_s i) \Rightarrow$
$x - iy = q_1^{\alpha_1} \dots q_r^{\alpha_r}(a_1 - b_1 i) \dots (a_s - b_s i)$.

Тогда $n = q_1^{2\alpha_1} \dots q_r^{2\alpha_r}(a_1^2 + b_1^2) \dots (a_s^2 + b_s^2)$.

Заметим, что произведение сумм двух квадратов тоже является суммой двух квадратов.

### КРИТЕРИЙ ГАУССА

Если число представимо в виде суммы двух квадратов, то все простые числа вида $4k + 3$ входят в его разложение в четных степенях. И обратно, если разложение числа на простые множители содержит все простые вида $4k + 3$ в четных степенях, то существует хотя бы одно его представление в виде суммы двух квадратов.

Сложность с подсчетом количеств разложений возникнет, если в разложении простые числа будут входить в некоторых степенях. Если все степени — первые, то получим:

$n = Q^2(a_1 + b_1 i) \dots (a_s + b_s i)(a_1 - b_1 i) \dots (a_s - b_s i)$,
где $Q = q_1^{\alpha_1} \dots q_r^{\alpha_r}$.

Из каждой пары сопряженных мы можем выбрать любое и таким образом составить $2^{s-1}$ различных разложений вида $(x + iy)(x - iy)$.

Тогда: $n = Q^2x^2 + Q^2y^2$.

## ПРЕДСТАВЛЕНИЕ В ВИДЕ СУММЫ КВАДРАТОВ ЧЕТНОГО ЧИСЛА

Пусть теперь $n$ четно.

### ТЕОРЕМА

Числа $n$ и $2n$ одновременно раскладываются или не раскладываются в сумму двух квадратов.

### ДОКАЗАТЕЛЬСТВО

Если $n = x^2 + y^2$,
то $2n = (1 + i)(1 - i)(x^2 + y^2) = (x + y)^2 + (x - y)^2$.

Если $2n = \tilde{x}^2 + \tilde{y}^2$, то $\tilde{x}$, $\tilde{y}$ имеют одинаковую четность, а значит мы можем поделить $\tilde{x} + \tilde{y}i$ на $1 + i$.

Тогда получим разложение для $n$:

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

Теорема доказана.

### СЛЕДСТВИЕ

$(a + bi) \vdots (1 + i) \Leftrightarrow a$ и $b$ имеют одинаковую четность.

Можно рассмотреть идеал из кратных $1 + i$, который представляет собой решетку, наклоненную под углом $45^\circ$ и проходящую через целочисленные точки с четной суммой координат.

## ЗАДАЧА ЭРДЁША

Как расположить данное количество точек $n$ на плоскости таким образом, чтобы из всех отрезков, соединяющих их попарно, количество отрезков равной длины было максимальным?

Мы не знаем как количество равных отрезков в оптимальной конфигурации растет с ростом числа $n$.

Самая лучшая конфигурация, которая известна на данный момент — это ситуация, когда число $n$ представимо в виде произведения простых вида $4k + 1$. Тогда окружность радиуса $\sqrt{n}$ пройдет через большое количество точек с целочисленными координатами.