1 ЗНАКОМСТВО С ГАУССОВЫМИ ЧИСЛАМИ

ЗАДАЧА О ПРЕДСТАВЛЕНИИ ЧИСЛА В ВИДЕ СУММЫ ДВУХ КВАДРАТОВ

ЗАДАЧА

Можно ли представить данное число в виде суммы двух квадратов целых чисел?

$n = a^2 + b^2$, где $n, a, b \in \mathbb{Z}$

Если можно, то сколькими способами?

Очевидно, $n < 0$ нельзя представить.
Рассмотрим первые несколько целых неотрицательных чисел и попробуем найти для них представление в таком виде:

$n = 0 \Rightarrow n = 0^2 + 0^2$

$n = 1 \Rightarrow n = 1^2 + 0^2$

$n = 2 \Rightarrow n = 1^2 + 1^2$

Число 3 нельзя представить.

$n = 4 \Rightarrow n = 2^2 + 0^2$

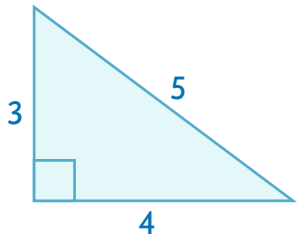
$n = 5 \Rightarrow n = 2^2 + 1^2$

Числа 6, 7 нельзя представить.
Существует ли какая-нибудь закономерность?
Например, для $n = 2017$ есть разложение

$n = 44^2 + 9^2$.

Можно ли было заранее это знать?

Если у нас есть прямоугольный треугольник с целыми длинами сторон (пифагоров треугольник), то для квадрата его гипотенузы точно есть как минимум два способа.



Например, $25 = 5^2 + 0^2 = 3^2 + 4^2$ — два различных разложения.

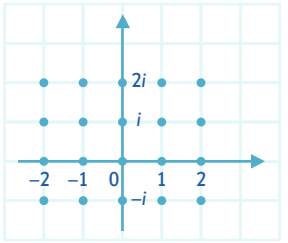
ГАУССОВО ЧИСЛО

Заслугой Гаусса является решение этой задачи с использованием комплексных чисел.

В поле $\mathbb{C}$ задача сводится к нахождению двух взаимно сопряженных комплексных чисел $a + bi$ и $a - bi$ таких, что:

$n = (a + bi)(a - bi) = a^2 + b^2$,
где $a, b \in \mathbb{Z}$.

Все целые (a, b) находятся в узлах целочисленной решетки, которую мы можем ввести на комплексной плоскости.



ОПРЕДЕЛЕНИЕ

Гауссовым числом называется «целое» комплексное число, т. е. число $a + bi$, у которого $a, b \in \mathbb{Z}$.
Множество гауссовых чисел обозначается $\mathbb{Z}[i]$.

Если мы будем складывать, вычитать или умножать гауссовы числа, мы всегда будем получать гауссовы числа.

Действительно, если числа $a + bi$ и $c + di$ — гауссовы, то:
$(a + bi)(c + di) = (ac - bd) + (bc + ad)i$.
$a, b, c, d \in \mathbb{Z} \Rightarrow ac - bd, bc + ad \in \mathbb{Z}$.

Заметим, что результат деления гауссовых чисел не всегда будет гауссовым.

> Множество гауссовых чисел $\mathbb{Z}[i]$ с операциями «$+$» и «$\cdot$» образует кольцо.

Это напрямую следует из того, что $\mathbb{Z}$ — кольцо.

КОЛЬЦО ГАУССОВЫХ ЧИСЕЛ

Как устроено $\mathbb{Z}[i] \subset \mathbb{C}$?

Мы строим минимальное кольцо, содержащее $\mathbb{Z}$ и число i. Так как результат сложения элементов кольца содержится в кольце, автоматически наше кольцо должно содержать все числа вида $a + bi$, где $a, b \in \mathbb{Z}$. Обратно, если мы берем любые два числа такого вида, мы получаем число такого же вида.

Чем $\mathbb{Z}$ интересно по сравнению с $\mathbb{R}$? Наличием понятия делимости и основной теоремы арифметики.

Тем же кольцо $\mathbb{Z}[i]$ отличается от $\mathbb{C}$. Мы можем ввести понятие делимости в $\mathbb{Z}[i]$ следующим образом:

ОПРЕДЕЛЕНИЕ

$a + bi \in \mathbb{Z}[i]$ делится на $c + di \in \mathbb{Z}[i]$, если $\exists x, y \in \mathbb{Z}$ такие, что $a + bi = (c + di)(x + yi)$.

На $\mathbb{Z}[i]$ можно строить теорию делимости: говорить об остатках, простых числах и в том числе сформулировать и доказать ОТА (основную теорему арифметики). Этим мы и займемся на ближайших уроках.

Гауссовы числа нам помогут решить задачу о представлении числа в виде суммы двух квадратов.

Эта задача — классика математики, и знакомство с методами, которые используются при решении этой задачи, используются для решения многих других задач.

Кроме этого, мы рассмотрим приложения гауссовых чисел к задаче о нахождении всех возможных пифагоровых троек и к другим интересным задачам.

3 НЕКОТОРЫЕ ПРИМЕРЫ

Итак, мы решаем задачу

$n = x^2 + y^2 = (x + yi)(x - yi)$, где $x, y \in \mathbb{Z}$

Заметим, что у любого гауссова числа норма является целым числом.

Рассмотрим некоторые примеры.

Число 2 было простым в целых числах, однако в $\mathbb{Z}[i]$ существует разложение:

$2 = 1^2 + 1^2 = (1 + i)(1 - i)$.

Таким образом, число 2 перестает быть простым в $\mathbb{Z}$[i]!

Число 3 не может быть представлено в виде суммы квадратов. Будет ли 3 простым в $\mathbb{Z}[i]$? Оставим пока этот вопрос.

$5 = 2^2 + 1^2 = (2 + i)(2 - i)$.

При простых n задача о представлении в виде суммы двух квадратов носит название **рождественской теоремы Ферма (РТФ)**:

ТЕОРЕМА **(рождественская теорема Ферма)**

Если простое число p имеет остаток 1 при делении на 4, то оно может быть представлено в виде суммы двух квадратов:

$p = 4k + 1 \Rightarrow \exists x, y \in \mathbb{Z}$ такие, что $p = x^2 + y^2$.

Таким образом, для чисел 3, 7, 11 мы не можем найти представление в виде суммы квадратов, а для числа 13 можем:

$13 = 2^2 + 3^2 = (2 + 3i)(2 - 3i)$.

Таким образом, числа 2, 5, 13 перестают быть простыми в $\mathbb{Z}[i]$. А что означает простота в теории делимости гауссовых чисел, мы узнаем на следующем уроке.