1 АРИФМЕТИКА ДЕЛИМОСТИ В ГАУССОВЫХ ЧИСЛАХ

ВВЕДЕНИЕ

Заметим, что $\forall a + bi \in \mathbb{Z}[i]$ верно, что $a + bi \vdots i$.

Действительно $a + bi = (b - ai)i$.

Есть такие гауссовы числа, на которые делятся все гауссовы числа. Что это за числа?

В целых числах простое число 7 имеет четыре делителя: 1, –1, 7, –7. Но мы не считаем разными разложения $7 = 7 \cdot 1 = (-7) \cdot (-1)$. Оба эти разложения содержат числа 1 и –1. Эти два числа являются единственными обратимыми в $\mathbb{Z}$.

Обратимые числа образуют в кольце группу по умножению: $<\{1,-1\}, \cdot >$. На обратимые числа делится любое число.

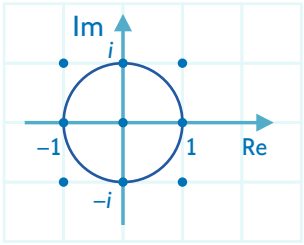
ОПРЕДЕЛЕНИЕ

Гауссово число z называется простым, если в любом его разложении $z = wr$ одно из чисел w и r делит 1.

ВОПРОС: какие в $\mathbb{Z}[i]$ есть делители 1?

ОБРАТИМЫЕ ЧИСЛА

Рассмотрим пересечение сетки гауссовых чисел с единичной окружностью. Это множество, состоящее из четырех чисел: $\{1, i, -1, -i\}$.



УТВЕРЖДЕНИЕ

Других обратимых гауссовых чисел нет.

ДОКАЗАТЕЛЬСТВО

От противного. Пусть мы нашли $a + bi$ — делитель 1.

Тогда $(a + bi)(c + di) = 1$.

Норма произведения есть произведение норм, а значит: $(a^2 + b^2)(c^2 + d^2) = 1 \Rightarrow$
$a^2 + b^2 = 1$, $c^2 + d^2 = 1 \Rightarrow$
либо $a^2 = 0$, $b^2 = 1$, либо $a^2 = 1$, $b^2 = 0$.

А значит, возможны только 4 варианта: $\{1, i, -1, -i\}$.

СЛЕДСТВИЕ

Если норма $a^2 + b^2$ гауссова числа — простое натуральное число, то $a + bi$ — простое число.

Таким образом, мы уже умеем определять простоту некоторых гауссовых чисел.

ГРУППА ОБРАТИМЫХ ЧИСЕЛ И ЕЕ ИЗОМОРФИЗМ ГРУППЕ ВЫЧЕТОВ ПО МОДУЛЮ 4

Легко убедиться, что множество из четырех чисел $\{1, i, -1, -i\}$ образует группу по умножению.

Эта группа устроена так же, как множество остатков по модулю 4 $\{0, 1, 2, 3\}$ по сложению. Действительно, построим соответствующие таблицы умножения и сложения:

×	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Эти две группы изоморфны.
Изоморфизм: $0 \to 1$; $1 \to i$; $2 \to -1$; $3 \to -i$.

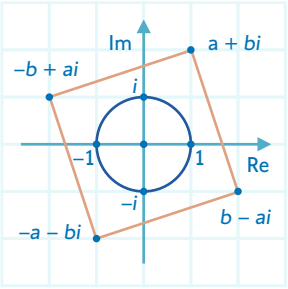
ПРОСТЫЕ ГАУССОВЫ ЧИСЛА

Пусть $z = a + bi$ — любое гауссово число.

Оно делится на само себя и на 4 обратимых числа. Если разделить это число на обратимые, получим еще 3 делителя этого числа:

$(a + bi) : i = -b + ai$;
$(a + bi) : (-1) = -a - bi$;
$(a + bi) : (-i) = b - ai$.

Эти три числа и само число $a + bi$ лежат в вершинах квадрата на гауссовой сетке, т. к. являются результатами поворотов друг друга на угол, кратный 90°.



ОПРЕДЕЛЕНИЕ

Гауссово число называется простым, если оно имеет ровно 8 делителей.

АССОЦИИРОВАННЫЕ ЧИСЛА

ОПРЕДЕЛЕНИЕ

Гауссовы числа $a + bi$, $-b + ai$, $-a - bi$, $b - ai$ называются ассоциированными.

Минимальная по модулю четверка ассоциированных чисел - это обратимые числа $1, i, -1, -i$.

Свойства ассоциированных чисел

а) $\frac{w_1}{w_2}, \frac{w_2}{w_1} \in \{1, i, -1, -i\}$;

б) $\forall z \in \mathbb{Z}[i] \quad z \vdots w_1 \Leftrightarrow z \vdots w_2$;

в) $\forall z \in \mathbb{Z}[i] \quad w_1 \vdots z \Leftrightarrow w_2 \vdots z$.

(У ассоциированных чисел одно и то же множество делителей и одно и то же множество кратных).

3 ПРИМЕРЫ РАЗЛОЖЕНИЯ НА ГАУССОВЫ ПРОСТЫЕ

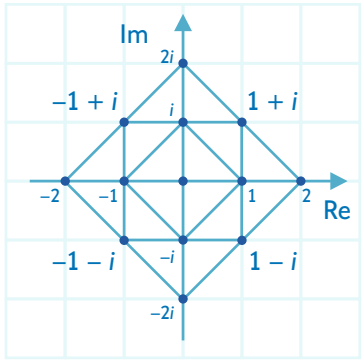
1 ▶ Число 2 — составное в гауссовых числах. Оно имеет 12 делителей.

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

Более того, число 2 с точностью до обратимого числа является квадратом гауссова числа:

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

Заметим, что для числа 2 мы получили разложение на пару ассоциированных. Такое возможно только в случае, когда ассоциированное число является сопряженным, а это верно, когда $\arg z = 45^\circ$.



2 ▶ Число $2 + i$ является простым, и множество его делителей есть

$\{1, i, -1, -i, 2 + i, -1 + 2i, -2 - i, 1 - 2i\}$.

3 ▶ Число $1 + 3i$ имеет норму $1^2 + 3^2 = 10$, это составное число, значит, можно предположить, что существует его разложение.

Действительно,

$1 + 3i = (1 + i)(2 + i)$ — составное число.

Заметим, что это означает наличие еще 3-х разложений:

$1 + 3i = (-1 + i)(-1 - 2i) = (1 - i)(-1 + 2i) = (-1 - i)(-2 - i)$.