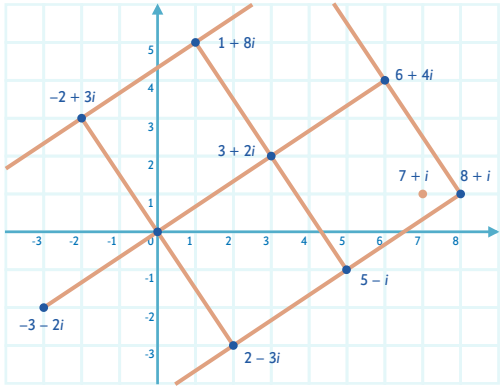
ГЕОМЕТРИЯ $\mathbb{Z}[i]$. ДЕЛЕНИЕ С ОСТАТКОМ. ИДЕАЛЫ

ГЕОМЕТРИЧЕСКИЙ МЕТОД ДЕЛЕНИЯ С ОСТАТКОМ

Рассмотрим на решетке гауссовых чисел множество

$(3 + 2i)\mathbb{Z}[i] = \{(3 + 2i)z$, где $z \in \mathbb{Z}[i]\}$.

Это множество всех кратных числа $3 + 2i$. Геометрически оно представляет собой сетку с равными квадратными ячейками со стороной $|\ 3 + 2i\ |$, повернутую относительно вещественной оси под углом, равным аргументу числа $3 + 2i$.



Мы должны найти точку этой сетки, максимально близкую к числу $7 + i$, чтобы расстояние от нее до $7 + i$ было меньше, чем сторона квадрата. Мы видим, что в нашем случае это число $8 + i$, то же самое, что мы нашли алгебраически на прошлом уроке. При этом:

$7 + i = (3 + 2i)(2 - i) + (-1)$;

$(3 + 2i)(2 - i) = 6 + 4i - 3i + 2 = 8 + i$;

остаток -1 имеет модуль $|\ -1\ | < |\ 3 + 2i\ |$.

Отметим 2 момента:

1 Деление с остатком можно выполнить не единственным способом. Вот еще один вариант:

$7 + i = (3 + 2i) \cdot 2 + (1 - 3i)$.

Точка $(3 + 2i) \cdot 2 = 6 + 4i$ является еще одной из вершин квадрата сетки, образованной кратными числа $3 + 2i$, внутри которого находится число $7 + i$. Модуль остатка $1 - 3i$ тоже будет меньше модуля числа $3 + 2i$. Возьмем еще одну вершину этого квадрата — число $1 - i$:

$7 + i = (3 + 2i)(1 - i) + (2 + 2i)$

Если возьмем 4-ю вершину квадрата, то получим остаток, больший по модулю, чем $|\ 3 + 2i\ |$. Значит в данном случае возможны 3 способа деления с остатком, а максимально может быть 4.

2 Решетка кратных числа $3 + 2i$ выглядит практически как сама решетка гауссовых чисел. Она обладает свойствами:

а) это аддитивная подгруппа в $\mathbb{Z}[i]$ (все суммы и разности чисел из этого множества принадлежат ему же);

б) эта решетка «съедает» все гауссовы числа внутрь себя: $\forall\ z \in \mathbb{Z}[i],\ w \in (3 + 2i)\ \mathbb{Z}[i] \quad zw \in (3 + 2i)\mathbb{Z}[i]$.

Такие подмножества называются **идеалами**.

2 ИДЕАЛ

ОПРЕДЕЛЕНИЕ

Пусть K — коммутативное кольцо с 1.
Тогда аддитивная подгруппа $\langle I, + \rangle \subset \langle K, + \rangle$ такая, что $\forall\, x \in K, \forall\, y \in I \quad xy \in I$, называется идеалом.

ПРИМЕР

$(a + bi)\mathbb{Z}[i]$ — идеал при любом $a + bi \in \mathbb{Z}[i]$.
Множество кратных любого гауссова числа образует идеал.

ТЕОРЕМА

Любой идеал $I \subset \mathbb{Z}[i]$ имеет вид $(a + bi)\mathbb{Z}[i]$
(это главный идеал).

Вспомним наш пример. Будем рассматривать множество всех таких выражений:

$\{(m + ni)(3 + i) + (k + li)(7 + i)\}$, где $m + ni, k + li \in \mathbb{Z}[i]$.

Очевидно, что это идеал. Если мы докажем, что любой идеал в $\mathbb{Z}[i]$ — главный, то этот тоже будет главный, а значит он имеет вид $(a + bi)\mathbb{Z}[i]$ для некоторого $a + bi \in \mathbb{Z}[i]$.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ О ИДЕАЛЕ В $\mathbb{Z}[i]$

Понятно, что нулевой идеал $\{0\}$ — главный.

Пусть $I \subset \mathbb{Z}[i]$ — произвольный нетривиальный идеал.

Тогда $\exists\, a + bi \in I$, $a + bi \neq 0$. $N(a + bi) = a^2 + b^2$.

Т. к. все элементы идеала можно упорядочить по величине нормы, можно выбрать элемент с минимальной, не равной нулю, нормой.

Можно считать, что это и будет $a + bi$.

Утверждается, что $I = (a + bi)\mathbb{Z}[i]$ (идеал порождается своим элементом, имеющим минимальную норму).

Докажем это от противного.

Пусть $\exists\, k + li \in I$ такое число, что оно не является кратным $a + bi$.

Поделим его на $a + bi$ с остатком:
$k + li = (a + bi)(\alpha + \beta i) + (\tau + \sigma i)$,
где $\tau + \sigma i$ — остаток, $N(\tau + \sigma i) < N(a + bi)$.

Выразим $\tau + \sigma i = k + li - (a + bi)(\alpha + \beta i)$. В правой части стоит выражение, принадлежащее идеалу I, а значит, $\tau + \sigma i \in I$.

Но мы выбрали элемент $a + bi$, как имеющий минимальную норму в идеале I! Противоречие.

Теорема доказана.

Таким образом, любой идеал в $\mathbb{Z}[i]$ имеет вид главного идеала.