ЗАВЕРШЕНИЕ РОЖДЕСТВЕНСКОЙ ТЕОРЕМЫ ФЕРМА

НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ В $\mathbb{Z}[i]$

Соберем урожай всех рассмотрений в арифметике гауссовых чисел.

Пусть $w_1, w_2 \in \mathbb{Z}[i]$.

Тогда множество $\{w_1z_1 + w_2z_2 \mid z_1,z_2 \in \mathbb{Z}[i]\}$ является идеалом.

В $\mathbb{Z}[i]$ любой идеал — главный, следовательно,
$\exists\, s \in \mathbb{Z}[i]$: $\{w_1z_1 + w_2z_2 \mid z_1,z_2 \in \mathbb{Z}[\mathrm{i}]\} = s\mathbb{Z}[i]$.

s обладает следующими свойствами:

1 ▶ $w_1z_1 + w_2z_2 = sr$ при некотором $r \in \mathbb{Z}[i]$.

В частности, $w_1 = sr_1$, $w_2 = sr_2$ для некоторых $r_1, r_2 \in \mathbb{Z}[i]$ $\Rightarrow$ s — общий делитель чисел w_1 и w_2.

2 ▶ $s = w_1a_1 + w_2a_2$ при некоторых $a_1, a_2 \in \mathbb{Z}[i]$.

Таким образом, s делится на любой общий делитель w_1 и w_2.

3 ▶ s — наибольший (по норме) из общих делителей w_1 и w_2.

В итоге имеем, что s — **наибольший общий делитель** гауссовых чисел w_1 и w_2.

Таким образом, НОД в $\mathbb{Z}[i]$ обладает всеми свойствами, аналогичными свойствам НОД в $\mathbb{Z}$.

В $\mathbb{Z}[i]$ СУЩЕСТВУЕТ ЧЕТЫРЕ НОД

ЗАМЕЧАНИЕ

НОД определяется с точностью до умножения на 1, -1, i и $-i$.

Это следует из определяющего свойства ассоциированных чисел:

$u, v \in \mathbb{Z}[i]$ — ассоциированы $\Leftrightarrow$ $u\mathbb{Z}[i] = v\mathbb{Z}[i]$.

Действительно, идеал, порожденный числом есть множество его кратных, а у ассоциированных чисел множества кратных совпадают.

ДЕЛИМОСТЬ НА ПРОСТОЕ НЕ ПРИОБРЕТАЕТСЯ ПРИ ПРОИЗВЕДЕНИИ

Пусть $w, z \in \mathbb{Z}[i]$ — взаимно простые (общие делители у них — только обратимые числа).

Тогда идеал $(w\alpha + z\beta)\mathbb{Z}[i] = r\mathbb{Z}[i] = \mathbb{Z}[\mathrm{i}]$, т.к. $r \in \{1, i, -1, -i\}$.
$\Rightarrow w\gamma + z\delta = 1 \in \mathbb{Z}$ для некоторых $\gamma, \delta \in \mathbb{Z}[i]$.

Докажем, что если q — гауссово простое $\alpha, \beta \in \mathbb{Z}[i]$, α, β не делятся на q, то и $\alpha\beta$ не делится на q.

Имеем $\alpha\gamma + q\delta = 1$ для некоторых $\gamma, \delta \in \mathbb{Z}[i]$. Домножим на β: $\alpha\beta\gamma + q\delta\beta = \beta$.

Если $\alpha\beta \vdots q$, то левая часть делится на q. Но тогда и правая часть должна делиться на q $\Rightarrow$ противоречие.

Таким образом, произведение двух гауссовых чисел, каждое из которых не делится на простое гауссово число, не приобретает делимость на это число.

ЗАВЕРШЕНИЕ ДОКАЗАТЕЛЬСТВА РТФ

Итак, пусть $p = 4k + 1$. Мы должны доказать, что p теряет простоту в $\mathbb{Z}[i]$.

От противного. Пусть p — простое в $\mathbb{Z}[i]$.

Мы уже знаем, что $\exists\, c \in \mathbb{N}$ такое, что $c^2 + 1 \vdots p$.

Пусть $\alpha = c + i$, $\beta = c - i$.

Тогда $\alpha\beta = c^2 + 1$, а значит, $\alpha\beta \vdots p$.

Но при этом ни α, ни β не делятся на p (иначе для некоторых целых m, n было бы выполнено $c + i = p(m + ni)$, откуда $1 = pn$, что невозможно!).

Получаем противоречие с ранее доказанным свойством. Значит, простое число p, имеющее вид $p = 4k + 1$, теряет простоту в $\mathbb{Z}[i]$.

Рождественская теорема Ферма полностью доказана.

Заметим, что коэффициенты a_1, a_2 в представлении $НОД(w_1, w_2) = w_1a_1 + w_2a_2$, так же, как и в случае целых чисел, можно найти при помощи алгоритма Евклида.

Следующий урок мы посвятим доказательству основной теоремы арифметики в гауссовых числах и некоторым полезным ее следствиям.