Арифметика IV: Гауссовы целые числа

▷ **Определение 1.** Подкольцо $\mathbb{Z}[i] \subset \mathbb{C}$ комплексных чисел вида $a + bi$, где числа a и b целые, называется кольцом *целых чисел Гаусса*.

Задача 1. Когда гауссово число $a + bi$ делится на число $1 + i$?

▷ **Определение 2.** *Нормой* гауссова числа z называется целое число $N(z) = z\bar{z} = |z|^2$.

Задача 2. Докажите, что гауссово целое число z *обратимо* (т. е. $1/z$ — тоже гауссово целое) тогда и только тогда, когда $N(z) = 1$ и найдите все такие числа.

▷ **Определение 3.** Пусть u и v — линейное независимые вектора в $\mathbb{R}^2$. Множество $\langle u, v\rangle := \{au + bv : a, b \in \mathbb{Z}\}$ называется *решеткой*, порожденной векторами u и v.

Задача 3*. а) Ни порождаемая векторами решетка, ни площадь ее ячейки не меняется при замене пары (u, v) на пару $(u, v + ku)$ (для любого целого числа k).
б) Если пара векторов порождает решетку $\mathbb{Z}^2$, то последовательностью преобразований вида $(u, v) \mapsto (u, v + ku)$ и $(u, v) \mapsto (v, u)$ ее можно перевести в пару (e_1, e_2).
в) Объем ячейки решетки определен корректно (в том смысле, что он зависит только от самой решетки, а не от выбора порождающих ее векторов).

Задача 4. а) Убедитесь, что множество (π) гауссовых чисел, кратных данному гауссовому числу π, образуют решетку. Как выглядит ее (естественная) ячейка?
б) В гауссовых числах *возможно деление с остатком*: для любых чисел a и b найдутся такие числа q и r, что $b = aq + r$, причем $N(r) < N(a)$. в) Единственны ли такие q и r?

▷ **Определение 4.** *Вычетом* по модулю гауссова числа π называется класс эквивалентности относительно отношения «$a \sim b \Leftrightarrow a - b \in (\pi)$».

Задача 5. Сколько существует вычетов по модулю π?

▷ **Определение 5.** Гауссово число называется *простым*, если оно делится только на обратимые элементы (т. е. если оно не представимо в виде произведения двух чисел с нормой больше 1).

Задача 6. Гауссово число π просто тогда и только тогда, когда *кольцо вычетов* $\mathbb{Z}[i]/(\pi)$ является полем.

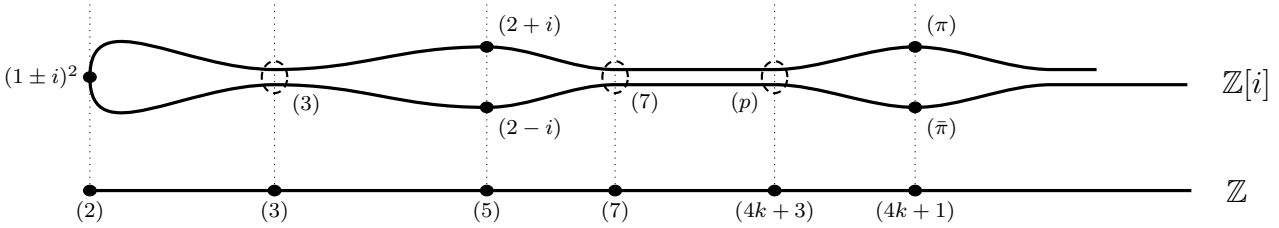
Задача 7. Сформулируйте и докажите основную теорему арифметики для гауссовых целых чисел.

Задача 8. Пусть p — простое *целое* число.
а) $\mathbb{F}_p[i]$ является полем тогда и только тогда, когда $\left(\frac{-1}{p}\right) = -1$.
б) p просто как гауссово число тогда и только тогда, когда $\left(\frac{-1}{p}\right) = -1$.

▷ Напомним, что $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Задача 9. Простое целое число p
- имеет вид $p = \varepsilon\pi^2$ при $p = 2$;
- имеет вид $p = \pi\bar{\pi}$ при $p = 4k + 1$;
- является простым гауссовым при $p = 4k + 3$

(π — простое гауссово, ε — обратимое гауссово).



Соглашение. Далее все числа по умолчанию предполагаются целыми.

Задача 10. Простое число представимо в виде суммы двух квадратов тогда и только тогда, когда оно имеет вид $4k + 1$ *("рождественская теорема Ферма").*

Задача 11. а) Если два числа представимы в виде суммы двух квадратов, то и их произведение представимо в виде суммы двух квадратов.
б*) Докажите аналогичное утверждение для сумм четырех квадратов.
в*) Верно ли аналогичное утверждение для сумм трех квадратов?

Задача 12. Какие натуральные числа представимы в виде суммы двух квадратов?

Задача 13. Сколькими способами представимо в виде суммы двух квадратов целых чисел число $5 \cdot 13 \cdot 17$?

Задача 14*. Для каких натуральных n существует окружность с центром в начале координат, на которой лежит ровно n узлов сетки?

Задача 15*. Найдите все рациональные кратные π, тангенс которых также рационален.