Числа Гаусса и Эйзенштейна

Определение 1. Комплексные числа вида $a+bi \in \mathbb{C}$, где a и b — целые числа, называются *числами Гаусса.*

Определение 2. Комплексные числа вида $a + b\rho \in \mathbb{C}$, где $\rho = \frac{\sqrt{3}i-1}{2}$, а a и b — целые числа, называются *числами Эйзенштейна.*

Задача 1. a) Нарисуйте на плоскости множество чисел Гаусса и Эйзенштейна.

b) Докажите, что числа Гаусса/Эйзенштейна образуют коммутативные кольца.

c) Найдите поля частных этих колец.

d) Найдите обратимые числа Гаусса и обратимые числа Эйзенштейна.

Задача 2. Докажите, что эти кольца евклидовы. В качестве нормы возьмите квадрат модуля комплексного числа $\|z\| = z\overline{z}$.

Задача 3. Разложите числа 2 и 3 в произведение простых чисел Гаусса/Эйзенштейна.

Задача 4. Пусть K - кольцо чисел Гаусса или чисел Эйзенштейна. Используя однозначность разложения на простые множители, докажите следующие утверждения.

a) Пусть p — простое целое число. Тогда либо p является простым в K, либо p представляется в виде $z\overline{z}$, где z — простой элемент K.

b) Норма простого элемента K равна p или p^2, где p — простое натуральное число.

c) Всякий простой элемент K является делителем некоторого простого натурального p.

Задача 5. a) Докажите, что простое натуральное число p является простым числом Гаусса тогда и только тогда, когда уравнение $x^2 + 1 = 0$ не имеет решения по модулю p, то есть -1 не является квадратом в $\mathbb{Z}/p\mathbb{Z}$.

Подсказка: Числа вида $n + i$ не имеют необратимых целых делителей.

b) Докажите, что простое натуральное число p является простым числом Эйзенштейна тогда и только тогда, когда уравнение $x^2 - x + 1 = 0$ не имеет решения по модулю p, то есть $p = 2$, или -3 не является квадратом в $\mathbb{Z}/p\mathbb{Z}$.

c) Докажите, что простое натуральное число p является простым числом Гаусса тогда и только тогда, когда оно имеет вид $4k - 1$,

d) Докажите, что простое натуральное число p является простым числом Эйзенштейна тогда и только тогда, когда оно равно 2 или имеет вид $6k - 1$.

Подсказка: Загляните на обратную сторону листка.

Задача 6*. a^*) Докажите, что натуральное число представимо в виде суммы двух квадратов натуральных чисел тогда и только тогда, когда все простые (натуральные) делители вида $4k - 1$ входят в него в чётной степени.

b^*) Сколькими способами можно представить число $n \in \mathbb{N}$ в виде суммы двух квадратов?

c^*) Докажите, что всякое натуральное число можно представить в виде суммы 4-х квадратов.

d^*) Какие значения принимает многочлен $x^2 + xy + y^2$ при целых x и y?

Задача 7*. a^*) Докажите, что всякая пифагорова тройка целых чисел $x^2 + y^2 = z^2$ может быть записана в виде $x = d(u^2 - v^2)$, $y = d(uv)$, $z = d(u^2 + v^2)$, где u, v, d — целые.

b^*) Решите уравнение $x^2 - xy + y^2 = z^2$.

Задача 8*. Докажите, что уравнение Ферма $x^n + y^n = z^n$

a^*) не имеет решений ненулевой степени в кольце многочленов $\mathbb{C}[x]$ при $n > 2$;

b^*) не имеет нетривиальных $(x, y \neq 0)$ решений в натуральных числах при $n = 4$;

c^{**}) не имеет нетривиальных $(x, y \neq 0)$ решений в натуральных числах при $n = 3$.

Подсказка: Используя комплексные числа, разложите $z^n - x^n$ на линейные множители. Воспользуйтесь однозначностью разложения на множители в соответствующих кольцах.

Дополнение: символ Лежандра.

Определение 3. Для целого a и простого p определим *символ Лежандра (Legendre)*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \neq 0 \text{ является квадратом в } \mathbb{Z}/p\mathbb{Z}, \\ -1 & a \text{ не является квадратом в } \mathbb{Z}/p\mathbb{Z}, \\ 0 & a = 0 \text{ в } \mathbb{Z}/p\mathbb{Z}. \end{cases}$$

Упражнение 1 *Имеет место равенство* $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Цикличность мультипликативной группы $(\mathbb{Z}/p\mathbb{Z})^*$ влечёт за собой такое следствие.

Упражнение 2 *Имеет место равенство* $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$ *в* $\mathbb{Z}/p\mathbb{Z}$.

Отсюда легко найти $\left(\frac{-1}{p}\right)$. Для поиска остальных значений полезна следующая теорема

Теорема 1 Квадратичный закон взаимности. *Пусть $p \neq q$ — нечётные простые числа. Тогда*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Один из вариантов доказательства (принадлежащий Е.И.Золотарёву, опубл. 1872) выглядит так. Заметим, что умножение на ненулевой элемент a в $\mathbb{Z}/p\mathbb{Z}$ задаёт перестановку σ_a элементов $\mathbb{Z}/p\mathbb{Z}$.

Упражнение 3 *Докажите, что* $\left(\frac{a}{p}\right)$ *равно знаку перестановки* σ_a.

Теперь определим перестановки σ_1 и σ_2 множества $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ так:

$$\sigma_1(x, y) = (qx + y, y) \qquad \sigma_2(x, y) = (x, x + py).$$

Упражнение 4 *Докажите, что знак σ_1 равен $\left(\frac{q}{p}\right)$, а знак σ_2 равен $\left(\frac{p}{q}\right)$.*

Теперь вспомним, что $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$.

Упражнение 5 *Вычислите в $\mathbb{Z}/pq\mathbb{Z}$ и найдите знак перестановки $\sigma_2\sigma_1^{-1}$.*

Упражнение 6 *Что в рассуждении изменится для $q = 2$?*