НМУ
Алгебра 1

27 сентября 2017
Листок 3

Гауссовы числа

Гауссово число — это комплексное число вида $a+bi$, где $a, b \in \mathbb{Z}$. Множество гауссовых чисел обозначается $\mathbb{Z}[i]$.

Задача 1. Разложите на простые множители в гауссовых числах:
a°) $7+i$, b) 2017.

Задача 2. Пользуясь алгоритмом Евклида, найдите НОД следующих гауссовых чисел:
a°) $7-i$ и $-4+7i$, b) $5+3i$ и $6-4i$.

Выясним, какие простые целые числа остаются простыми и в гауссовых числах.
Ответ: простыми в гауссовых остаются натуральные простые числа вида $4k+3$ (и противоположные им).

Задача 3°. Пусть p — простое целое число, $p \geqslant 3$. Покажите, что:

a) p не просто в гауссовых числах $\iff p = z\bar{z}$, где z — простое гауссово число $\iff p$ представимо в виде суммы двух квадратов $\iff$ уравнение $x^2+1=0$ имеет решения в $\mathbb{Z}$ по модулю p $\iff -1$ является квадратом в $\mathbb{Z}/p\mathbb{Z}$. Подсказка: $x^2+1=(x+i)(x-i)$.

b) p не просто в гауссовых числах $\iff p$ имеет вид $4k+1$.

Подсказка: для $\Leftarrow$ рассмотрите произведение $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-2) \cdot (p-1)$ в поле $\mathbb{Z}/p\mathbb{Z}$ и сгруппируйте сомножители по парам двумя способами: сначала a с $-a$, а потом a с a^{-1}.

Задача 4. Пусть z — простое гауссово число. Покажите, что либо $z = \pm p$ или $\pm i \cdot p$, либо $N(z) = p$, где p — простое целое число.

Выясним теперь, как представляются натуральные числа в виде суммы двух квадратов целых чисел. Иными, словами, как разложить натуральное число n в произведение $z \cdot \bar{z}$, где z — гауссово число.

Задача 5°. Пусть целые числа m и n представляются в виде суммы двух квадратов. Покажите, что и mn представлется в виде суммы двух квадратов.

Разложим число n на простые множители в целых числах:

$$n = 2^c p_1^{d_1} \ldots p_k^{d_k} q_1^{e_1} \ldots q_l^{e_l},$$

где p_i — натуральные простые числа вида $4k+1$, а q_i — натуральные простые числа вида $4k+3$.

Задача 6°. Покажите, что n представляется в виде суммы двух квадратов целых чисел тогда и только тогда, когда все степени $e_1, \ldots, e_l$ четны.

Задача 7. Покажите, что число способов представить n в виде суммы двух квадратов целых чисел равно $4(d_1+1)\ldots(d_k+1)$.

Числами Эйзенштейна называются комплексные числа вида $a+b\xi$, где $a, b \in \mathbb{Z}$, а $\xi = \frac{-1+\sqrt{3}i}{2}$ — кубический корень из 1. Множество чисел Эйзенштейна обозначается $\mathbb{Z}[\xi]$. *Нормой* числа Эйзенштейна z называется целое число $N(z) = z\bar{z}$.

Задача 8. Вычислите норму $a+b\xi$. Найдите обратимые элементы в $\mathbb{Z}[\xi]$. Покажите, что кольцо $\mathbb{Z}[\xi]$ евклидово.

Задача 9. Пусть p — простое целое число, $p \geqslant 3$. Покажите, что:

a) p не просто в $\mathbb{Z}[\xi] \iff p = z\bar{z}$, где z — простое в $\mathbb{Z}[\xi] \iff p$ представимо в виде a^2-ab+b^2 $\iff$ уравнение $x^2-x+1=0$ имеет решения в $\mathbb{Z}$ по модулю $p \iff -3$ является квадратом в $\mathbb{Z}/p\mathbb{Z}$.

b^*) p не просто в $\mathbb{Z}[\xi] \iff p=3$ или p имеет вид $3k+1$.

Задача 10*. Сформулируйте и решите аналоги задач a) 4; b) 5; c) 6; d) 7 для чисел Эйзенштейна.