# Задачи по курсу
# «Простые числа в арифметических прогрессиях»

## Листок 2

1. **(2)** Докажите, что если $m, n$ — два взаимно простых целых числа разной чётности, то числа $m^2 - n^2$ и $2mn$ тоже взаимно простые. Также взаимно простыми будут числа $m^2 - n^2$ и $m^2 + n^2$.

*Определение 1:* Комплексным числом называется выражение вида $a + bi$, где a, b – действительные числа, $i$ – мнимая единица. По определению $i^2 = -1$. Естественным образом комплексные числа можно отождествить с точками (или соответствующими радиус-векторами) на плоскости.

*Определение 2:* Число $\bar{z} = a - bi$ называют комлексно сопряженным к $z = a + bi$.

*Определение 3:* Модулем комплексного числа $z$ называют $\sqrt{z\bar{z}}$.

*Определение 4:* Аргументом комплексного числа $z$ называется число $0 \leq \arg(z) < 2\pi$, равное углу между положительным направлением действительной оси и радиус-вектором, соответствующим числу $z$.

*Определение 5:* На множестве комплексных чисел естественным образом определено сложение, при умножении модули чисел перемножаются, а аргументы складываются.

2. **(2)** Докажите, что при умножении комплексных чисел выполняется следующая формула:

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i$$

*Определение 6:* Гауссовыми числами называется множество $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}[i]\}$ с определенными на нем операциями сложения и умножения (такими же, как на множестве комплексных числел). Иными словами, $\mathbb{Z}[i]$ – наименьшее подкольцо в $\mathbb{C}$, содержащее $\mathbb{Z}$ и $i$.

*Определение 7:* Числами Эйзенштейна называется множество $\mathbb{Z}[\omega] = \{a + bi \mid a, b \in \mathbb{Z}[\omega]\}$, где $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. Операции сложения и умножения такие же, как в комплексных числах.

*Определение 9:* Если на кольцах $\mathbb{Z}[i]$ и $\mathbb{Z}[\omega]$ задана функция нормы $N : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$, удовлетворяющая условиям:

I. $\forall a, b \in R \setminus \{0\} : N(ab) \geq N(a)$.
II. $\forall a, b \in R, b \neq 0 \exists q, r \in R : a = qb + r$, и при этом либо $N(r) < N(b)$, либо $r = 0$.

(то есть в них можно делить с остатком), тогда кольца называются Евклидовыми.

3. **(1)** а) Проверьте, что норма $N(z) = z\bar{z}$ действительно удовлетворяет условиям I, II. Более того, I можно усилить и сказать, что $N(ab) = N(a)N(b)$.

*Замечание:* В дальшейшем по умолчанию под нормой для колец $\mathbb{Z}[\omega]$ и $\mathbb{Z}[i]$ будет подразумеваться именно функция $N(z) = z\bar{z}$.

б) Правда ли, что если $N(z) = p$ – простое в $\mathbb{Z}$, то $z$ – простое в $\mathbb{Z}[i]$? $\mathbb{Z}[\omega]$?

4.**(2)** Разделите в кольце Гауссовых чисел $5 + 4i$ на $1 - 2i$ с остатком. Сколькими способами можно это осуществить? Ещё примеры: 13 на $5 - i$, $2 + i$ на $2 - i$.

5. **(2)** Докажите, что НОД$(a, b)$ для двух обычных целых чисел не меняется при пересчёте его же, но в кольце Гауссовых чисел.

6. **(2)** Сформулируйте и докажите Основную Теорему арифметики для $\mathbb{Z}[i]$ и $\mathbb{Z}[\omega]$.

7. **(5)** (ПРИМЕР КОЛЬЦА БЕЗ ОТА) Проведите анализ кольца $\mathbf{Z}[\sqrt{-5}]$ целых чисел, пополненных корнем из $-5$, лежащим в верхней полуплоскости (то есть, минимального кольца, содержащего $\sqrt{-5}$ и все целые числа). Покажите, что

• это кольцо состоит из всех комплексных чисел, представимых в форме $a + b\sqrt{-5}$ и только их (где $a, b \in \mathbf{Z}$);

• в нём есть только два обратимых элемента (какие?);

• функция $N : \mathbf{Z}[\sqrt{-5}] \to \mathbf{N}$, заданная формулой $N(a + b\sqrt{-5}) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2$, переводит произведение в произведение. (Она называется *нормой* кольца; $N(a) = a^2$ для обычных целых чисел, рассматриваемых как элементы кольца $\mathbf{Z}[\sqrt{-5}.$);

• числа $3, 7, 4 \pm \sqrt{-5}, 1 \pm 2\sqrt{-5}$ все простые;

• имеет место равенство $21 = 3 \cdot 7 = (4 + \sqrt{-5}) \cdot (4 - \sqrt{-5}) = (1 + 2\sqrt{-5}) \cdot (1 - 2\sqrt{-5})$, противоречащее Основной Теореме арифметики.

8. **(3)** Рассмотрим кольцо $\mathbf{Z}[\sqrt{-3}]$ целых чисел, пополненных корнем из $-3$, лежащим в верхней полуплоскости (то есть, минимального кольца, содержащего $\sqrt{-3}$ и все целые числа). Покажите, что в нём числа $2, 1 \pm \sqrt{-3}$ все простые, и что $2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$. Докажите, что кольцо $\mathbf{Z}[\sqrt{-3}]$ содержится в кольце $\mathbf{Z}[\omega]$ чисел Эйзенштейна. Почему вышеприведённое равенство не противоречит ОТА в кольце Эйзенштейна?

9. а) **(1)** Пусть $p = 4k+3$ – простое. Докажите, что и в Гауссовых числах оно останется простым.

б) **(2)** Пусть $p = 6k+5$ – простое. Докажите, что и в чилах Эйзенштейна оно останется простым.