Гауссовы числа, числа Эйзенштейна.

Задача 1. Найдите в $\mathbb{Z}[i]$ наибольший общий делитель элементов **а)** 85 и $1+13i$; **б)** $47-13i$ и $53+56i$ и его линейное выражение.

Задача 2. Найдите все целочисленные решения уравнения **а)** $x^2+1=y^3$; **б*)** $x^2+1=y^n$.

Задача 3. **а)** Пусть $p=a+bi$ — простое гауссово число. Докажите, что $\mathbb{Z}[i]/(p\mathbb{Z}[i])$ — конечное поле. Сколько в нём элементов?

б) Пусть $z=a+bi$ и НОД$(a,b)=1$. Докажите, что $\mathbb{Z}[i]/(z\mathbb{Z}[i])\simeq\mathbb{Z}/(a^2+b^2)\mathbb{Z}$.

в) Пусть $p=a+bi$ — простое гауссово число, $a,b\neq 0$ и $p\neq 1+i$. Докажите, что $\mathbb{Z}[i]/p^r\mathbb{Z}[i]\simeq\mathbb{Z}/(a^2+b^2)^r\mathbb{Z}$.

Задача 4. Докажите, что натуральное число представимо в виде сумму двух квадратов тогда и только тогда когда в разложение на простые множители простые числа вида $p=4k+3$ входят в чётных степенях.

Задача 5. Пусть $\omega=\dfrac{-1+i\sqrt{3}}{2}$. Определим $\mathbb{Z}[\omega]=\{a+b\omega\mid a,b\in\mathbb{Z}\}\subset\mathbb{C}$.

а) Докажите, что $\mathbb{Z}[\omega]$ – кольцо. Докажите, что $|a+b\omega|=a^2-ab+b^2$.

б) Докажите, что в $\mathbb{Z}[\omega]$ возможно деление с остатком.

в) Найдите все обратимые элементы в $\mathbb{Z}[\omega]$.

г*) Докажите, что любое простое число Эйзенштейна это либо

- $x\cdot p$, где $x\in\mathbb{Z}[\omega]$ — обратим, а $p=3k+2\in\mathbb{Z}$ — простое;
- $(a+b\omega)$, где $a^2-ab+b^2=p$. Здесь $p=3$ или $p=3k+1\in\mathbb{Z}$ — простое.

д) Опишите все поля, которые получаются как кольца остатков при делении на простые числа Эйзенштейна.

Задача 6. Используя равенство $x^3+y^3=(x+y)(x+\omega y)(x+\omega^2 y)$ докажите *теорему Ферма* для $n=3$: не существует решений уравнения $x^3+y^3=z^3$, где $x,y,z\in\mathbb{Z}\setminus\{0\}$.

Задача 7. Пусть $d\in\mathbb{Z}_{>0}$. Пусть $\mathbb{Z}[\sqrt{-d}]=\{a+b\sqrt{-d}\,|\,a,b\in\mathbb{Z}\}\subset\mathbb{C}$.

а) Докажите, что $\mathbb{Z}[\sqrt{-d}]$ – кольцо.

б) Докажите, что в кольце $\mathbb{Z}[\sqrt{-2}]$ возможно деление с остатком.

в) Предъявите элемент в кольце $\mathbb{Z}[\sqrt{-d}], d\geq 3$, который разлагается в произведение простых двумя различными способами (прежде, объясните, что означает быть простым элементом в этом кольце). Возможно ли деление с остатком в этом кольце?