Задачи к курсу

«Непростые простые»

Обозначение: Пусть $d \in \mathbb{Z}$, d — не квадрат. Полагаем

$$\mathbb{Z}[\sqrt{d}] = \left\{ a + b\sqrt{d} \;\middle|\; a, b \in \mathbb{Z} \right\}, \qquad \mathbb{Q}[\sqrt{d}] = \left\{ a + b\sqrt{d} \;\middle|\; a, b \in \mathbb{Q} \right\}.$$

Задача 1. Норма в квадратичном расширении. Положим $N(a + b\sqrt{d}) = a^2 - db^2$. Докажите, что

а) $N(\alpha\beta) = N(\alpha)N(\beta)$;

б) число α из $\mathbb{Z}[\sqrt{d}]$ обратимо по умножению, то есть $\alpha^{-1} \in \mathbb{Z}[\sqrt{d}]$, тогда и только тогда, когда $N(\alpha) = \pm 1$.

Задача 2. Факториальность. Докажите однозначность разложения на простые в $\mathbb{Z}[\sqrt{d}]$ для $d = \pm 2, 3$.

Задача 3. Нефакториальность. Приведите пример неоднозначности разложения на простые в $\mathbb{Z}[\sqrt{d}]$ для $d = \pm 5, -6$.

Задача 4. Простые в $\mathbb{Z}[i]$. Пусть p — простое в $\mathbb{N}$. Докажите, что

а) если $p = 2$, то p не является простым в $\mathbb{Z}[i]$;

б) если $p \equiv 3 \pmod 4$, то p является простым в $\mathbb{Z}[i]$;

в) если $p \equiv 1 \pmod 4$, то $p = (a + bi)(a - bi)$, $a, b \in \mathbb{Z}$, причём $a \pm bi$ — не ассоциированные простые элементы $\mathbb{Z}[i]$.

Задача 5. Целые точки на эллиптической кривой. Решите в $\mathbb{Z}$ уравнение

а) $x^3 - y^2 = 1$;

б) $x^3 - y^2 = 2$;

в) $x^3 - y^2 = 4$.

Подсказка: используйте однозначность разложения на простые в $\mathbb{Z}[i]$ и в $\mathbb{Z}[\sqrt{-2}]$.

Задача 6. Уравнение Пелля. Решите в $\mathbb{Z}$ уравнение

а) $x^2 - 3y^2 = 1$;

б) $x^2 - 5y^2 = 1$;

в) $x^2 - 7y^2 = 1$.

Задача 7. Аналог Малой теоремы Ферма для $\mathbb{Z}[i]$. Пусть $z = a + bi$ — простое целое гауссово число. Докажите, что для любого $w \in \mathbb{Z}[i]$ справедливо сравнение

$$w^{a^2+b^2} \equiv w \pmod z.$$

Задача 8. Целые алгебраические числа степени 2. Докажите, что множество целых алгебраических чисел, лежащих в $\mathbb{Q}[\sqrt{d}]$, совпадает с $\mathbb{Z}[\theta]$, где

$$\theta = \begin{cases} \sqrt{d} & \text{при } d \equiv 2, 3 \pmod 4 \\ \frac{-1+\sqrt{d}}{2} & \text{при } d \equiv 1 \pmod 4 \end{cases}.$$

Задача 9. Опять нефакториальность. Докажите, что при $d \equiv 1 \pmod 4$ в $\mathbb{Z}[\sqrt{d}]$ нет однозначности разложения на простые.