Листок 14
Тема 14 (4.1). Кольцо целых гауссовых чисел

Упражнения и задачи

1. Пусть R — евклидово кольцо (с нормой $N(\cdot)$). Докажите, что u — единица $R \iff N(u) = 1$.

2. Пусть R — кольцо. Докажите следующие утверждения (свойства делимости на языке идеалов):
   - $a|b \Leftrightarrow (b) \subseteq (a)$;
   - u — единица $\Leftrightarrow (u) = R$;
   - a, b — ассоциированы $\Leftrightarrow (a) = (b)$;
   - p — простой элемент $\Leftrightarrow ab \in (p) \Rightarrow a \in (p)$ или $b \in (p)$;
   - p — неприводимый элемент $\Leftrightarrow (p) \subseteq (a) \Rightarrow (a) = R$ или $(a) = (p)$.

3. Пусть R — кольцо главных идеалов, $a, b \in R$ d — НОД a, b. Докажите, что $\exists d \in R : (d) = (a, b)$.

4. Пусть R — кольцо главных идеалов. Докажите, что $p \in R$ — неприводимый элемент $\iff p$ — простой.

5. Докажите свойство показателя в кольце главных идеалов: если p — неприводимый элемент, $a, b \in R^*$, то $\nu_p(ab) = \nu_p(a) + \nu_p(b)$.

6. Докажите теорему об однозначности разложения на простые множители в кольцах главных идеалов.

7. Пусть $\pi \in \mathbb{Z}[i]$ — простой элемент, $\nu_\pi(\alpha)$ — соответствующий показатель, $|\alpha|_\pi = (\mathrm{N}\, p)^{-\nu_\pi(\alpha)}$ — метрика заданная на $\mathbb{Z}[i]$ и $\mathbb{Q}(i)$. Опишите ограничение этой метрики на $\mathbb{Q}$.

8. Докажите, что $\mathbb{Z}[\omega]$ — евклидово кольцо. Найдите единицы $\mathbb{Z}[\omega]$.

9. Докажите, что для функций определенных в лекции выполняется $d(n_1) = d_1(n) - d_3(n)$.

10. Докажите оценку для числа представлений в виде суммы двух квадратов: $r_2(n) = \mathcal{O}_\varepsilon(n^\varepsilon)$.

SageMath

- Рассмотрите примеры арифметики кольца гауссовых чисел: `ZZ[I]`, исследуйте базовые функции такие как `gcd(), xgcd(), factor(), ....`

- Исследуйте функции для нахождения разложений целых чисел в виде суммы двух и четырёх квадратов, например, библиотека `sum_of_squares`.

Темы для самостоятельного изучения

- Арифметика кольца чисел Эйзенштейна $\mathbb{Z}[\omega]$, [IR], §§9.1–9.2.

- Алгебра кватернионов, число представлений суммой четырёх квадратов, [DSV], §§2.5–2.6.