Семинар 1. Простые числа и неприводимые многочлены

Алгебра в криптографии, осенний семестр 2021 г.

ФАКУЛЬТЕТ МАТЕМАТИКИ, НИУ ВШЭ

Задача 1. Известно, что

$$78227 \cdot 244999 = 99599 \cdot 192427.$$

Разложите число 78227 на простые множители.

Задача 2. Примените решето Эратосфена, чтобы найти все неприводимые многочлены степени не выше четыре с коэффициентами в поле из двух элементов.

Задача 3. (а) Докажите, что простых чисел вида $4k + 3$, где k — целое, бесконечно много.

(б) Докажите, что неприводимых многочленов с коэффициентами в поле из двух элементов бесконечно много.

(в) Докажите, что простых чисел вида $4k + 1$ бесконечно много.

Задача 4. Классифицируйте все неприводимые многочлены над $\mathbb{R}$ и над $\mathbb{C}$.

Задача 5. Является ли многочлен $x^5 + x + 1$ неприводимым над

$$\text{(а) } \mathbb{F}_2; \qquad \text{(б) } \mathbb{Q}?$$

Задача 6. (а) Приведите пример неприводимого многочлена степени 5 над $\mathbb{F}_2$.

(б) Докажите, что над $\mathbb{F}_2$ существует неприводимый многочлен любой ненулевой степени.

(в) Обозначим через I_m количество неприводимых многочленов степени m над $\mathbb{F}_2$. Докажите тождество

$$1 - 2z = \prod_{m=1}^{\infty} (1 - z^m)^{I_m}. \tag{1}$$

(Одним из элементов доказательства должно быть объяснение, в каком смысле нужно понимать бесконечное произведение в правой части.)

(г) Придумайте аналог тождества (1) для простых чисел в $\mathbb{Z}$.