Семинар 4. Китайская теорема об остатках

Алгебра в криптографии, осенний семестр 2021 г.

ФАКУЛЬТЕТ МАТЕМАТИКИ, НИУ ВШЭ

Задача 1. Найдите натуральное число x, не превосходящее 120, такое что

$$x \equiv 1 \pmod 8, \quad x \equiv 2 \pmod 5, \quad x \equiv 0 \pmod 3.$$

Задача 2 (Китайская теорема об остатках)**.** Пусть p и q — два взаимно простых целых числа.

(а) Найдите такие целые числа x и y, что $qy \equiv 1 \pmod p$, и $px \equiv 1 \pmod q$.

(б) Для произвольных целых чисел a и b найдите такое целое число n, что $n \equiv a \pmod p$, и $n \equiv b \pmod q$.

(в) Найдите все решения системы сравнений

$$\begin{cases} n \equiv a \pmod p; \\ n \equiv b \pmod q. \end{cases}$$

Задача 3. Используя, что

$$718865222040754575648532881408 = n^{13}$$

для некоторого целого n, найдите n без калькулятора.

Задача 4. (а) Сформулируйте и докажите китайскую теорему об остатках для многочленов.

(б) Найдите квадратный многочлен f с рациональными коэффициентами, такой что

$$f(1) = 2, \quad f(2) = 20, \quad f(3) = 200.$$

Задача 5 (Интерполяционный многочлен Лагранжа)**.** Найдите многочлен $f(x)$ степени не выше трёх с вещественными коэффициентами, значения которого в точках 0, 1, 2 и 3 совпадают со значениями функции

$$\text{(а) } 2^x; \quad \text{(б) } \frac{1}{x+1}; \quad \text{(в) } \sin\left(\frac{\pi x}{2}\right).$$

Задача 6. Пусть p и q — различные простые натуральные числа. Докажите, что сравнение

$$p^x + q^y \equiv 1 \pmod{pq}$$

разрешимо в натуральных числах.