Билет 11. Китайская теорема об остатках

Китайская теорема об остатках

Пусть $p_1, p_2, \ldots, p_k$ — различные попарно взаимно простые числа и $P = p_1 \cdot p_2 \cdots p_k$.
Тогда существует единственное неотрицательное решение по модулю P системы уравнений:

$$\begin{cases} x \equiv a_1 \pmod{p_1} \\ x \equiv a_2 \pmod{p_2} \\ \vdots \\ x \equiv a_k \pmod{p_k} \end{cases}$$

Пример

Решить систему:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 6 \pmod{11} \end{cases}$$

Шаг решения

Шаг 1: Решаем первые два уравнения
$x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$
Из первого уравнения: $x = 2 + 3s$
Подставляем во второе:

$$\begin{aligned} 2 + 3s &\equiv 3 \pmod{5} \\ 3s &\equiv 1 \pmod{5} \end{aligned}$$

Находим обратный к 3 по модулю 5:

$$3^{-1} \equiv 3^{\phi(5)-1} \equiv 3^3 \equiv 27 \equiv 2 \pmod{5}$$

$$\begin{aligned} s &\equiv 2 \cdot 1 \equiv 2 \pmod 5 \\ s &= 2 + 5t \\ x &= 2 + 3(2+5t) = 8 + 15t \end{aligned}$$

Получили: $x \equiv 8 \pmod{15}$

Шаг решения

Шаг 2: Добавляем третье уравнение
Теперь решаем систему:

$$\begin{cases} x \equiv 8 \pmod{15} \\ x \equiv 6 \pmod{11} \end{cases}$$

Из первого: $x = 8 + 15t$
Подставляем во второе:

$$\begin{aligned} 8 + 15t &\equiv 6 \pmod{11} \\ 15t &\equiv -2 \equiv 9 \pmod{11} \\ 4t &\equiv 9 \pmod{11} \quad (\text{т.к. } 15 \equiv 4 \pmod{11}) \end{aligned}$$

Находим обратный к 4 по модулю 11:

$$4^{-1} \equiv 4^{\phi(11)-1} \equiv 4^9 \pmod{11}$$

Быстрое вычисление:

$$\begin{aligned} &4^2 = 16 \equiv 5 \pmod{11} \\ &4^4 \equiv 5^2 = 25 \equiv 3 \pmod{11} \\ &4^8 \equiv 3^2 = 9 \pmod{11} \\ &4^9 = 4^8 \cdot 4 \equiv 9 \cdot 4 = 36 \equiv 3 \pmod{11} \end{aligned}$$

$$\begin{aligned} t &\equiv 3 \cdot 9 = 27 \equiv 5 \pmod{11} \\ t &= 5 + 11r \\ x &= 8 + 15(5 + 11r) = 8 + 75 + 165r = 83 + 165r \end{aligned}$$

Шаг решения

Шаг 3: Финальный ответ

$$
\begin{aligned}
x &= 83 + 165r \\
x &\equiv 83 \pmod{165}
\end{aligned}
$$

Проверка:

- $83 \div 3 = 27$ остаток 2
- $83 \div 5 = 16$ остаток 3
- $83 \div 11 = 7$ остаток 6

Проверка уникальности

Модуль произведения: $P = 3 \times 5 \times 11 = 165$

Решение $x \equiv 83 \pmod{165}$ — единственное в диапазоне $[0, 164]$

Любое другое решение отличается на кратное 165:

$$83, 248, 413, \ldots \quad \text{и} \quad -82, -247, -412, \ldots$$