Билет 10. Обратный элемент по модулю

Определение

Число a^{-1} называется **обратным по модулю** m, если:

$$a \cdot a^{-1} \equiv 1 \pmod{m}$$

Обратный элемент существует только если $\gcd(a, m) = 1$.

Метод 1: Теорема Эйлера

Метод

Если $\gcd(a, m) = 1$, то по теореме Эйлера:

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

Умножаем на a^{-1}:

$$a^{\phi(m)-1} \equiv a^{-1} \pmod{m}$$

Пример: Найти $7^{-1} \pmod{15}$
$\phi(15) = 8$, тогда:

$$7^{-1} \equiv 7^{7} \pmod{15}$$

Вычисляем: $7^2 = 49 \equiv 4$, $7^4 \equiv 4^2 = 16 \equiv 1$, $7^7 = 7^4 \cdot 7^2 \cdot 7^1 \equiv 1 \cdot 4 \cdot 7 = 28 \equiv 13$
Ответ: $7^{-1} \equiv 13 \pmod{15}$

Метод 2: Теорема Ферма

Теорема

Если p — простое и $(p, a) = 1$, то:

$$a^{p-1} \equiv 1 \pmod{p}$$

Следовательно:

$$a^{-1} \equiv a^{p-2} \pmod{p}$$

Метод 3: Расширенный алгоритм Евклида

Метод

Решаем уравнение:

$$a \cdot x + m \cdot y = 1$$

$$a \cdot x = 1(mod.m)$$

Тогда x — искомый обратный элемент $a^{-1} \pmod{m}$.

Алгоритм:

1. **Базовый случай:** Если $b = 0$: вернуть $(a, 1, 0)$
2. **Рекурсивный шаг:**
   - $(g, x_1, y_1) = \text{extGCD}(b, a \bmod b)$
   - $x = y_1$
   - $y = x_1 - \lfloor a/b \rfloor \cdot y_1$
   - Вернуть (g, x, y)

Пример: Найти $7^{-1} \pmod{15}$ алгоритмом Евклида
Решаем: $7x + 15y = 1$

$$15 = 2 \cdot 7 + 1$$
$$7 = 7 \cdot 1 + 0$$

Обратный ход:

$$1 = 15 - 2 \cdot 7 \Rightarrow 7 \cdot (-2) + 15 \cdot 1 = 1$$

Ответ: $7^{-1} \equiv -2 \equiv 13 \pmod{15}$