Билет 9. Расширенный алгоритм Евклида

Определение

Тождество Безу: Для любых целых a, b существуют такие $x, y \in \mathbb{Z}$, что:

$$a \cdot x + b \cdot y = \gcd(a, b)$$

Теорема

Если $\gcd(a, m) = 1$, то существует обратный элемент $a^{-1} \pmod m$:

$$a \cdot x \equiv 1 \pmod m$$

где x находится из тождества Безу.

Алгоритм

Расширенный алгоритм Евклида
Вход: a, b
Выход: $(\gcd(a, b), x, y)$ такие, что $a \cdot x + b \cdot y = \gcd(a, b)$

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

Доказательство

Корректность алгоритма:
Базовый случай: $b = 0$

$$a \cdot 1 + 0 \cdot 0 = a = \gcd(a, 0) \quad \checkmark$$

Рекурсивный шаг: Пусть для $(b, a \bmod b)$ найдены x_1, y_1:

$$b \cdot x_1 + (a \bmod b) \cdot y_1 = \gcd(b, a \bmod b) = \gcd(a, b)$$

Выразим $a \bmod b$:

$$a \bmod b = a - b \cdot \lfloor a/b \rfloor$$

Подставим:

$$b \cdot x_1 + (a - b \cdot \lfloor a/b \rfloor) \cdot y_1 = \gcd(a, b)$$

Преобразуем:

$$b \cdot x_1 + a \cdot y_1 - b \cdot \lfloor a/b \rfloor \cdot y_1 = \gcd(a, b)$$

$$a \cdot y_1 + b \cdot (x_1 - \lfloor a/b \rfloor \cdot y_1) = \gcd(a, b)$$

Следовательно:

$$x = y_1, \quad y = x_1 - \lfloor a/b \rfloor \cdot y_1 \quad \checkmark$$

Пример: Найти обратный элемент

Найти $13^{-1} \pmod{17}$: Нужно решить: $13x + 17y = 1$

Обратный ход:

$$1 = 13 - 3 \cdot 4 = 13 - 3 \cdot (17 - 1 \cdot 13) = 13 - 3 \cdot 17 + 3 \cdot 13 = 4 \cdot 13 - 3 \cdot 17$$

Получили: $13 \cdot 4 + 17 \cdot (-3) = 1$

Ответ: $13^{-1} \equiv 4 \pmod{17}$

```java
public static int[] gcd(int a, int b) {
  if (b == 0) {
    return new int[]{a, 1, 0};
  }

  int[] result = gcd(b, a % b);
  int gcd = result[0];
  int x1 = result[1];
  int y1 = result[2];

  int x = y1;
  int y = x1 - (a/b) * y1;

  return new int[]{gcd, x, y};
}

public static int modInverse(int a, int m) {
  int[] result = gcd(a, m);
  int gcd = result[0];
  int x = result[1];

  if (gcd != 1) {
    throw new RuntimeException("Обратного элемента не существует");
  }

  return (x % m + m) % m;
}
```

Рис. 1: ExtendedGCD