

Расширенный алгоритм Евклида

Лесников Юрий, seagest

1 Расширенный алгоритм Евклида

Замечание 1.1. Алгоритм находит не только $\gcd(n, m)$, но и такие коэффициенты $a, b \in \mathbb{Z}$, что выполняется **тождество Безу**:

$$an + bm = \gcd(n, m)$$

Замечание 1.2. Если $\gcd(n, m) = 1$, то тождество Безу принимает вид:

$$an + bm = 1$$

Взяв это равенство по модулю m , получаем:

$$an \equiv 1 \pmod{m}$$

Значит, $n \equiv a^{-1} \pmod{m}$

Алгоритм(индуктивное построение).

База индукции: Если $m = 0$, то $\gcd(n, 0) = n$, $a = 1$, $b = 0$.

Шаг индукции: Пусть найдено решение для $(m, n \bmod m)$. Пусть a_1 и b_1 таковы, что:

$$a_1 m + b_1 (n \bmod m) = \gcd(m, n \bmod m) = \gcd(n, m)$$

Выразим через них решение для (n, m) :

$$an + bm = \gcd(n, m) = a_1 m + b_1 (n \bmod m) = a_1 m + b_1 (n - m \left\lfloor \frac{n}{m} \right\rfloor) = b_1 n + (a_1 - b_1 \left\lfloor \frac{n}{m} \right\rfloor) m$$

Значит, искомые коэффициенты для (n, m) :

$$a = b_1, \quad b = a_1 - b_1 \left\lfloor \frac{n}{m} \right\rfloor$$

Algorithm 1 Расширенный алгоритм Евклида

```
1: function ExtendedGCD( $n, m$ ) {Предполагается, что  $n \geq m$ }
2: if  $m = 0$  then
3:   return ( $n, 1, 0$ )
4: end if
5:  $(gcd, a_1, b_1) \leftarrow \text{ExtendedGCD}(m, n \bmod m)$ 
6:  $b \leftarrow a_1 - \left\lfloor \frac{n}{m} \right\rfloor \cdot b_1$ 
7:  $a \leftarrow b_1$ 
8: return ( $gcd, a, b$ )
```
