

# Алгоритм Евклида

## 1 Алгоритм

Даны два целых неотрицательных числа  $a$  и  $b$ . Требуется найти их наибольший общий делитель (greatest common divisor, gcd). Алгоритм описывается следующей формулой:

$$\gcd(a, b) = \begin{cases} a, & \text{if } b = 0 \\ \gcd(b, a \bmod b), & \text{otherwise} \end{cases}.$$

Зная наибольший общий делитель двух чисел, можно вычислить их наименьшее общее кратное (least common multiplier, lcm) по формуле:

$$\text{lcm}(a, b) = \frac{a \cdot b}{\gcd(a, b)}.$$

### 1.1 Доказательство корректности

Оба аргумента являются неотрицательными целыми числами. Если хотя бы один из них равен 0, то ответом является другой аргумент, алгоритм **завершается**. В случае, когда оба аргумента равны 0, ответ не определен (подойдет любое бесконечно большое число). Не теряя общности, положим  $a \geq b$ . Заметим, что второй аргумент строго убывает, следовательно, поскольку он неотрицательный, алгоритм Евклида **всегда завершится**.

Осталось показать, что  $\gcd(a, b) = \gcd(b, a \bmod b)$  для любых  $a > 0, b > 0$ . Покажем, что величина, стоящая в левой части равенства, делится на стоящую в правой, а стоящая в правой — делится на стоящую в левой. Очевидно, это будет означать, что левая и правая части совпадают, что и докажет корректность алгоритма Евклида. Обозначим  $d = \gcd(a, b)$ . Тогда, по определению,  $d|a$  и  $d|b$ .

Разложим остаток от деления:

$$a \bmod b = a - b \left\lfloor \frac{a}{b} \right\rfloor.$$

Отсюда следует:

$$\begin{cases} d|b, \\ d|(a \bmod b) \end{cases}.$$

Воспользуемся фактом: если для каких-то трех чисел  $p, q, r$  выполнено  $p|q$  и  $p|r$ , то выполняется и  $p|\gcd(q, r)$ . В нашем случае:

$$d|\gcd(b, a \bmod b).$$

Заменяя  $d$  на его определение, получаем:

$$\gcd(a, b) \mid \gcd(b, a \bmod b).$$

Таким образом мы доказали, что левая часть делит правую. Аналогичным образом доказывается, что правая часть делит левую.

## 1.2 Время работы

Время работы алгоритма оценивается теоремой Ламе, которая устанавливает связь алгоритма и последовательности Фибоначчи. Формулировка и доказательство теоремы здесь не приводятся. В результате доказательства теоремы время работы алгоритма оценивается как  $O(\log \min(a, b))$ .

## 2 Реализация

Алгоритм Евклида может быть реализован как с помощью цикла, так и с помощью рекурсии. Далее предполагается, что  $a \geq b$ .

Реализация с циклом

```
def gcd(a, b):  
    while b:  
        a, b = b, a % b  
    return a
```

Рекурсивная реализация

```
def gcd(a, b):  
    if b == 0:  
        return a  
    else:  
        return gcd(b, a % b)
```

Вычисление НОК

```
def lcm(a, b):  
    return a / gcd(a, b) * b
```

## Список литературы

Кормен, Томас и др. (2005). *Алгоритмы. Построение и анализ*. Второе издание. Издательский дом «Вильямс».