Алгоритм Евклида

НОД(a, б) - максимальное число, на которое делится a и б без остатка

НОД(60, 45) = 15
НОД(128, 36) = 4
НОД(29, 107) = ?

НОД(a, B) = НОД(B, a). Верно?

Считаем $a < B$. для $a = B$ очевидно.

$\exists$ НОД(a, B) = k $\Rightarrow$ $a \% k = 0$, $B \% k = 0$ $\Rightarrow (B - a) \% k = 0$

$(B - 2a) \% k = 0$

. . .

$(B \% a) \% k = 0$

Но если $\begin{cases} (B \% a) \% k = 0 \\ a \% k = 0 \end{cases}$ $\Rightarrow a \% (B \% a) \% k = 0$

↑ это понятно?

$B > a > B \% a > a \% (B \% a) > \ldots > 0$

↑ конечно, мы получим ответ

Наш алгоритм

1. a, B : $a < B$
2. a, B = B % a, a пока $a > 0$
3. B - НОД

45, 60
15, 45
0, 15
↑

36, 128
20, 36
16, 20
4, 16
0, 4 ←

Оценки

$a, b \to b \% a, a$

$b \% a < b/2$ – подумайте, почему?

→ число операций не более $O(\log n)$

Оценки снизу не будет :)

Быстрое возведение в степень.

$x^8 = \underbrace{x \cdot x \cdot x \cdot x \cdot x \cdot x \cdot x \cdot x}_{7 \text{ умн.}}$ $O(n)$

$x^8 = (x^4)^2 = \underbrace{((x^2)^2)^2}_{3 \text{ умн.}}$ $O(\log n)$!

Общий случай

$$\begin{cases} x^{2k} = ((x)^k)^2 \\ x^{2k+1} = x \cdot x^{2k} \end{cases}$$

Дальше код.