

Расширенный алгоритм Евклида

{

- ▣ **Расширенный алгоритм Евклида** — это расширение алгоритма Евклида, которое вычисляет кроме наибольшего общего делителя (НОД) целых чисел a и b ещё и коэффициенты соотношения, то есть целые x и y .
- ▣ **Коэффициенты соотношения** — представление наибольшего общего делителя целых чисел в виде их линейной комбинации с целыми коэффициентами.

$$\square x_0 = 1 ; y_0 = 0$$

$$\square X_1 = 0 ; y_1 = 1$$

□ Для вычисления дополнительных коэффициентов:

$$\square X = X(i-2) - (q * X(i-1));$$

$$\square Y = Y(i-2) - (q * Y(i-1));$$

$$\square \text{НОД}(a, b) = a * x + b * y$$

Изначально мы решаем как и по обычному методу:

$$\text{НОД}(a, b) = (a = b * q + r)$$

$$\square x_0 = 1 ; y_0 = 0$$

$$\square X_1 = 0 ; y_1 = 1$$

$$\square X = X(i-2) - (q * X(i-1));$$

$$\square Y = Y(i-2) - (q * Y(i-1));$$

□ Допустим:

$$\square a = 64; b = 42$$

$$\square 64 = 42 * 1 + 22;$$

$$\square 42 = 22 * 1 + 20;$$

$$\square 22 = 20 * 1 + 2$$

$$\square 20 = 2 * 10 + 0$$

$$\square \text{НОД}(64 \text{ и } 42) = 2$$

$$X_2 = 1 - (1 * 0) = 1$$

$$X_3 = 0 - (1 * 1) = -1$$

$$X_4 = 1 - (1 * (-1)) = 2$$

$$Y_2 = 0 - (1 * 1) = -1$$

$$Y_3 = 1 - (1 * (-1)) = 2$$

$$Y_4 = (-1) - (1 * 2) = -3$$

$$\text{НОД}(a, b) = (a * x) + (b * y) =$$

$$= 64 * 2 + 42 * (-3) = 128 + (-126) = 2$$

□ Для взаимно простых чисел:

□ $\text{НОД}(a, b) = 1$

□ $a * x + b * y \equiv 1 \pmod{b}$

□ $a = 21, 88$

□ $\text{НОД}(21, 88) = 21x + 88y = 1$

□ $21 = 88 * 0 + 21$

□ $88 = 21 * 4 + 4$

□ $21 = 4 * 5 + 1$

□ $4 = 1 * 4 + 0$

□ $x_0 = 1 ;$

□ $x_1 = 0 ;$

□ $x = x(i-2) - (q * x(i-1));$

$x_2 = 1 - (0 * 0) = 1$

$x_3 = 0 - (4 * 1) = 4$

$x_4 = 1 - (5 * (-4)) = 21$

$\text{НОД}(21, 88) = 21 * 21 + 88 * 21 = 1$

$a = 88; b = 52$