

Обобщенный алгоритм Евклида



Теорема Пусть $a, b \in \mathbb{Z}$; $a, b > 0$. Тогда $\exists x, y \in \mathbb{Z}$ такие, что $ax + by = \gcd(a, b)$ (*)

Обобщенный ал. Евклида служит для нахождения $\gcd(a, b)$ и x, y , удовлетворяющих (*)

Алг: $u = (a, 1, 0)$

$v = (b, 0, 1)$

while $v[0] \neq 0$:

$q = u[0] // v[0]$ # integer division

$t = (u[0] \% v[0], u[1] - q \cdot v[1], u[2] - q \cdot v[2])$

$u = v$

$v = t$

return u # $u = (\gcd(a, b), x, y)$