Multiplikative Inverse modulo m, erweiterter Euklidischer Algorithmus

$x, m \in \mathbb{Z}$

SATZ: Wenn $ggT(x,m) = 1$ ist, dann gibt es ein $y \in \mathbb{Z}$ mit $x \cdot y \equiv 1 \pmod m$ $\left(y = x^{-1}\right)$.

$ggT(u,v)$:

$a,b := u,v$; $x_a = 1; y_a = 0$; $x_b = 0; y_b = 1$

$\{a > 0, b \geq 0\}$

while $b > 0$:

$q := \lfloor a/b \rfloor$

$r := a - b \cdot q$

$x_r := x_a - x_b \cdot q$

$y_r := y_a - y_b \cdot q$

$a,b := b,r$

$x_a, y_a, x_b, y_b := x_b, y_b, x_r, y_r$

return a

$ggT(u,v) = g = a = x_a \cdot u + y_a \cdot v$

Jedes Zwischenergebnis a,b ist eine ganzzahlige Linearkombination $x \cdot u + y \cdot v$ $(x,y \in \mathbb{Z})$

INVARIANTEN:

$$\begin{cases} a = x_a \cdot u + y_a \cdot v \\ b = x_b \cdot u + y_b \cdot v \\ r = x_r \cdot u + y_r \cdot v \end{cases}$$

BEISPIEL

$a = 12u - 7v$

$b = 1u + 2v$

$a - 3b = 9u - 13v$

$ggT(x,m) = 1 = \underbrace{x_a}_{s} \cdot x + \underbrace{y_a}_{t} \cdot m = sx + t \cdot m$

$s \cdot x = 1 + tm \equiv 1 \pmod m$

Wähle $y := s$ □