$\mathbb{Z}_n$: Nullteiler?

x ist Nullteiler $\Leftrightarrow$

x Vielfaches von p, $p \mid n$

$\mathbb{Z}_p$: p Primzahl

$p \equiv 0 \pmod p$

keine Nullteiler!

Erw. GGT Algor.

$ggT(a,b) \rightarrow (g,x,y) : \quad g = a \cdot x + b \cdot y$

Annahme: x ist Nullteiler $\Rightarrow x \cdot y = 0 \quad (y \neq 0)$
und x^{-1} existiert

$\Rightarrow x^{-1} \cdot \underbrace{x \cdot y}_{0} = x^{-1} \cdot 0 = 0$

$\Leftrightarrow$ ↯

$\underbrace{x^{-1} \cdot x}_{1} \cdot y = 1 \cdot y = y \neq 0$

$p = 7, \; q = 13, \quad n = p \cdot q = 91$

$\varphi(n) = (p-1) \cdot (q-1) = 6 \cdot 12 = 72$

Suche e mit $ggT(e, \varphi) = 1$

$e = 5 : \; ggT(5, 72) = 1$ ✓

Suche: $d = e^{-1} \bmod \varphi$

Allg. ggT:

$$ggT(a,b) \rightarrow (g, x, y)$$

$$g = ggT(a,b) = a \cdot x + b \cdot y$$

$$ggT(e,\varphi) = 1 = e \cdot x + \varphi \cdot y \qquad | \bmod \varphi$$

$$1 = e \cdot x + 0 = e \cdot x$$

$$\Rightarrow x = e^{-1}$$

$$ggT(a,b) = ggT(b, a \bmod b)$$

$$ggT(12,10) = ggT(10,2)$$

$$= ggT(2,0) = 2$$

$12 = 3 \cdot 4 = 2^2 \cdot 3$

$10 = 2 \cdot 5 = 2 \quad \cdot 5$

$\Rightarrow ggT = 2 \cdot$

$x = 2^7 \cdot 3^9 \cdot \quad 7^2$

$y = 2^3 \cdot 3^1 \cdot 5^2 \cdot 7^1$

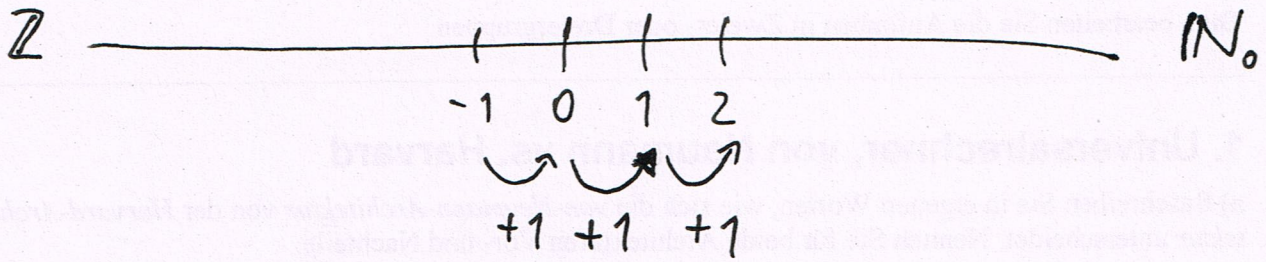
$ggT = 2^3 \cdot 3^1 \cdot \quad 7^1$

$a \mid ggT(a,b) \qquad b \mid ggT(a,b)$

$$ggT(b, a \bmod b)$$

$$a \bmod b =$$

$$x \cdot a = ggT(a,b) \qquad y \cdot b = ggT(a,b)$$



$a \leq b$: $a \xrightarrow{(+1)^*} b$