$ggT(6,15) = ggT(15,6) = ggT(6,3) = ggT(3,0) = 3$

$3 = x \cdot 6 + y \cdot 15$

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

$g = ggT(a,b)$

$g \mid a,\ g \mid b$

$a \bmod b = a - r \cdot b$

$g \mid b,\ g \mid a,\ g \mid rb$

$g \mid a - rb = a \bmod b$

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

$= 3$

ohne Alg.:

$6 = 2^1 \cdot 3^1$

$15 = 3^1 \cdot 5^1$

$ggT = 3^1$

$2^7 \cdot 3^2 \cdot 5^9 \cdot 11^2$

$2^2 \cdot 3^1 \cdot 7^8 \cdot 11^3$

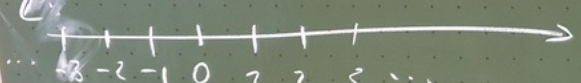
$ggT = 2^2 \cdot 3^1 \cdot 11^2$

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

$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$

$\mathbb{Z}_{11}$: $[3] \cdot [4] = [3 \cdot 4] = [12] = [1]$

$\mathbb{Z}$:



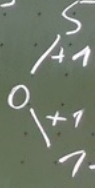
$[a] < [b] \Leftrightarrow a < b$

geht nicht

Zahlenstrahl

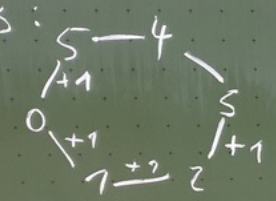
Kreis:

$\mathbb{Z}_6$:



Zahlenkreis für $\mathbb{Z}_n$ ist Kreis:

$\mathbb{Z}_6$:



$\mathbb{Z}_n$, $\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n, \exists y \in \mathbb{Z}_n, x \cdot y = 1\}$

p Primzahl:

$\mathbb{Z}_p$, $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$

$\mathbb{Z}_n$ hat Nullteiler, wenn n nicht prim.

Annahme: m Nullteiler, m^{-1} existiert in $\mathbb{Z}_n$

$m \mid 0$: $\exists x: m \cdot x = 0, x \neq 0$

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

Annahme falsch $1 \cdot x = 0 \Rightarrow x = 0$ ↯

$(a \cdot b \cdot c$

$(((a \; b) \; \%$

$(a \cdot b \cdot c \cdot d) \bmod n$

$(((a \; b) \; \%n) \cdot c) \; \%n) \cdot d \; \%n$