$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$

$[k]_n = \{ i \mid i \in \mathbb{Z},\ i \equiv k \pmod n \}$

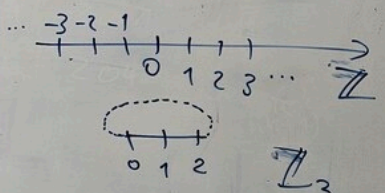
$\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\} = \{0, 1, 2\}$

$= \{ \{\dots, -6, -3, 0, 3, 6, \dots\},$
$\{\dots, -5, -2, 1, 4, 7, \dots\}$
$\{\dots, -4, -1, 2, 5, 8, \dots\} \}$

Mult.:

$[2] \cdot [2] = [2 \cdot 2]$
$= [4] = [1]$

$[2] \cdot [2] = [5] \cdot [-1]$
$= [-5] = [1]$



4.1 5^{-1} in $\mathbb{Z}_{15}$, $x = 5^{-1}$

$(5 \cdot 5^{-1}) \cdot 3 = 3$, aber $(3 \cdot 5) \cdot 5^{-1} = 0 \cdot 5^{-1}$
$= 0$ ↯
1

ggT (12, 20)
ggT (20, 12 % 20)
ggT (20, 12)
ggT (12, 20 % 12)
ggT (12, 8)
ggT (8, 12 % 8)
4
ggT (4, 8 % 4) = 4
0

$12 = 2 \cdot 2 \cdot 3$
$20 = 2 \cdot 2 \cdot 5$ $\Rightarrow$ ggT = 4

Linearkomb.:

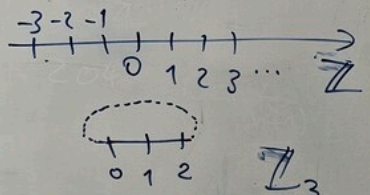
$4 = x \cdot 12 + y \cdot 20$

$7, 7^2, 7^3, \dots$
$7^i = 7^j$
$7^i \cdot \underbrace{7^{j-i}}_{1} = 7^j = 7^i$

Mult.:

$[2] \cdot [2] = [2 \cdot 2]$
$= [4] = [1]$

$[2] \cdot [2] = [5] \cdot [-1]$
$= [-5] = [1]$



Schnelles Potenzieren.

n^{19}, $19 = \underline{10011}_{(2)}$

n, n^2, n^4, n^8, n^{16}

$n^{19} = n^{16} \cdot n^2 \cdot n$

P4

n	0	1	2	3	4
n^{-1}	/	1	3	2	4

$\mathbb{Z}_5$, $\varphi(5) = 4$

n	0	1	2	3	4	5	6	7	8	9
n^{-1}	/	1	/	7	/	/	/	3	/	9

$\mathbb{Z}_{10}$, $\varphi(10) = 4$

$\varphi(5) = 5 \cdot (1 - \frac{1}{5}) = 5 \cdot \frac{4}{5} = 4$

$\varphi(10) = 10 \cdot (1 - \frac{1}{2})(1 - \frac{1}{5}) = 10 \cdot \frac{1}{2} \cdot \frac{4}{5} = 4$

$\varphi(pq) = (p-1)(q-1)$, p, q prim