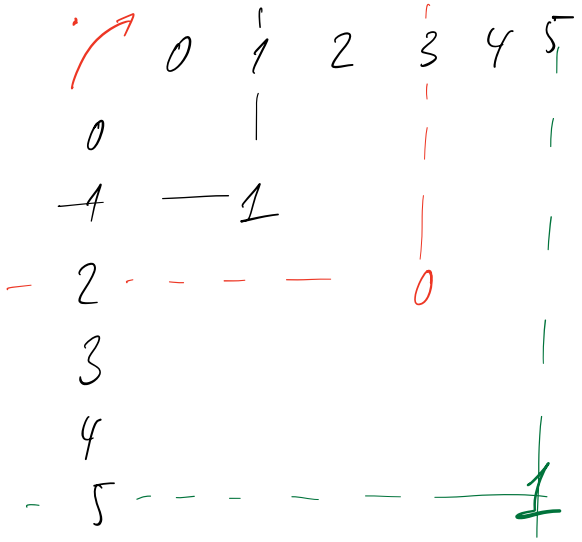
Inverses modulo n

$\mathbb{Z}_6$

$2 \cdot 3 \equiv 0 \mod 6$

$5 \cdot 5 \equiv 1 \mod 6$

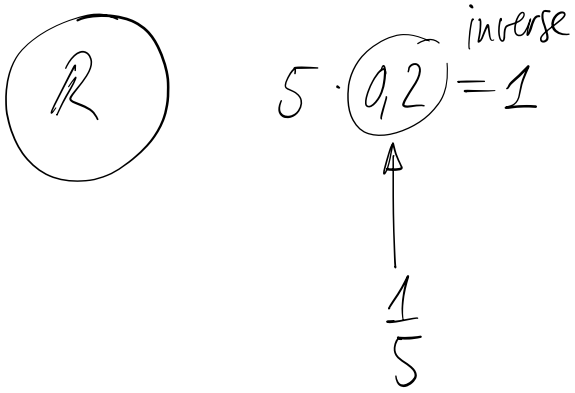


5 est l'inverse de 5 dans $\mathbb{Z}_6$

$\mathbb{R}$ $\quad ax+b=0 \Leftrightarrow x = -\frac{b}{a} \quad (a \neq 0)$

$$\mathbb{R} \longrightarrow \mathbb{R}$$
$$x \longmapsto ax+b$$

$$\mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26}$$
$$z \longmapsto \boxed{a \cdot z + b} \quad \text{pour} \quad a, b \in \mathbb{Z}_{26}$$



4.2.34 a) b)

4.2.35 a) c)

$5 \cdot 5 \equiv 1 \pmod 6$

$\mathbb{Z}_6$

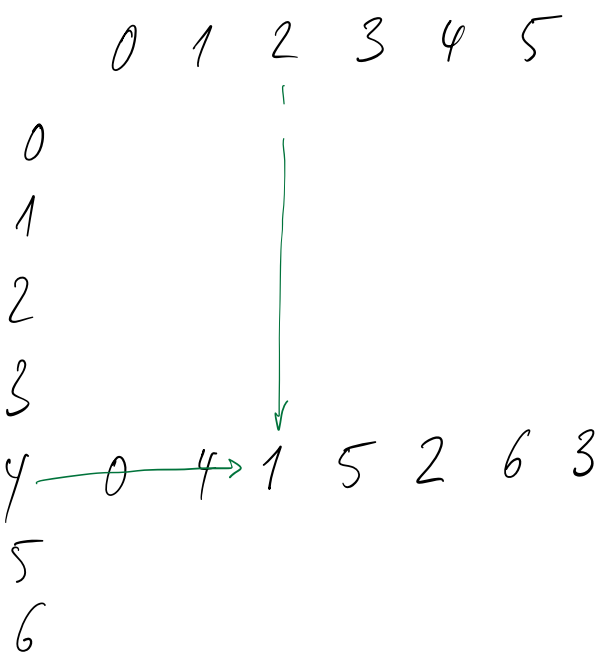
$5x \equiv 3 \pmod 6$

$5 \cdot (5 \cdot x) \equiv 5 \cdot 3 \pmod 6$

$\underbrace{(5 \cdot 5)}_{1} \cdot x \equiv 5 \cdot 3 \pmod 6$

$x \equiv 15 \pmod 6$

$x \equiv 3 \pmod 6$



$\mathbb{Z}_7$

$4x \equiv 2 \pmod 7$

$\ll \frac{1}{4} = 2 \gg$

$2 \cdot (4x) \equiv 2 \cdot 2 \pmod 7$

$8x \equiv 4 \pmod 7$

$x \equiv 4 \pmod 7$

$16x + 17 \equiv 13 \pmod{26}$

$16x \equiv 22 \pmod{26}$

$16 \cdot z \equiv 1 \pmod{26}$ pas possible

$16x = 22 + k \cdot 26$

$8x = 11 + k \cdot 13$

$8x - 11 = k \cdot 13$

$$8x + k \cdot 13 = 11$$

$$13 = 1 \cdot 13 + 0 \cdot 8$$

$$8 = 0 \cdot 13 + 1 \cdot 8$$

$$5 = 1 \cdot 13 - 1 \cdot 8$$

$$3 = -1 \cdot 13 + 2 \cdot 8$$

$$2 = 2 \cdot 13 - 3 \cdot 8$$

$$1 = -3 \cdot 13 + 5 \cdot 8$$

$$8 \cdot 5 - 3 \cdot 13 = 1$$

$$8 \cdot 55 - 33 \cdot 13 = 11$$

$$8 \cdot 55 = 33 \cdot 13 + 11$$

$$16 \cdot 55 - 22 = 880 - 22 = 858 = 33 \cdot 26$$

$$\Rightarrow \quad x \equiv 55 \pmod{13} \quad \Leftrightarrow \quad \boxed{x \equiv 3 \pmod{13}}$$

$$\boxed{6x \equiv 9 \pmod{15}}$$

$$\Leftrightarrow \quad 6x - 9 \equiv 0 \pmod{15}$$

$$\Leftrightarrow \quad 6x - 9 = k \cdot 15$$

$$\Leftrightarrow \quad 6x + k \cdot 15 = 9$$

$$\Leftrightarrow \quad 2x + 5k = 3$$

$$5 = 1 \cdot 5 + 0 \cdot 2$$

$$2 = 0 \cdot 5 + 1 \cdot 2$$

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

$2 \cdot (-2) + 5 \cdot 1 = 1$

$2 \cdot (-6) + 5 \cdot 3 = 3$

$2 \cdot 4 + 5 \cdot (-1) = 3$

$6x \equiv 9 \pmod{15} \Leftrightarrow \boxed{x \equiv 4 \pmod{5}}$

$4x \equiv 5 \pmod{14}$

$4x - 5 = k14$

$\underbrace{4x + 14 \cdot k}_{\text{pair}} = 5$

$\uparrow$ impair

$\downarrow$

$(\exists x, k \in \mathbb{Z} \text{ tq. } 4x + 14k = 2 = gcd(4, 14))$

$16x + 18 \equiv 13 \pmod{26}$

$16x + 5 \equiv 0 \pmod{26}$

$16x + 5 = k26$

$16x + k \cdot 26 = 5$

$16x + k \cdot 26$ — par

5 — impar ↯

$(\exists\, x, k \in \mathbb{Z} \text{ tq. } 16x + k \cdot 26 = 2 = \gcd(16; 26))$

$\boxed{9x + 11 \equiv 3 \pmod{26}}$ $\quad 9 \cdot 3 \equiv 1 \pmod{26}$

$3 \cdot 9 \cdot x + 33 \equiv 3 \cdot 3 \pmod{26}$

$x \equiv 9 - 33 \mod(26)$

$\boxed{x \equiv 2 \pmod{26}}$

$$5x + 6 \equiv 13 \pmod{26}$$

$$5x \equiv 7 \pmod{26}$$

$$\underbrace{21 \cdot 5}_{1 \bmod 26} \cdot x \equiv 21 \cdot 7 \pmod{26}$$

$$x \equiv 147 \pmod{26}$$

$$x \equiv 17 \pmod{26}$$