$\mathbb{Z}$, $n \mid a-b$ ozn. $a \equiv b \pmod{n}$

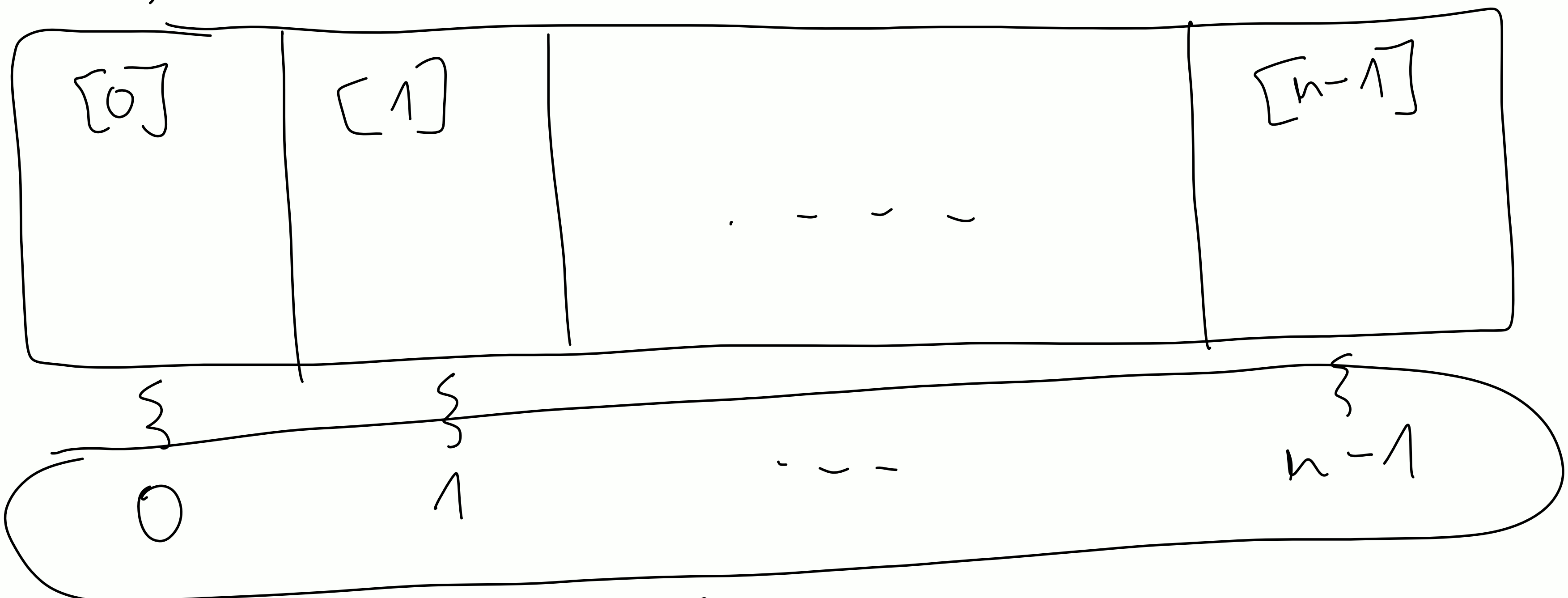
anaquente

$a \bmod n$ diaTonte

$\Updownarrow$

$a \% n$

$\mathbb{Z}$, n



$\{0, 1, \ldots, n-1\} \overset{\text{ozn}}{=} \mathbb{Z}_n$

Element odwrotny względem relacji przystawania

Def. Niech $k \in \mathbb{Z}_n = \{0, 1, \dots, n-1\}$. Jeżeli istnieje liczba $m \in \mathbb{Z}_n$ dla której zachodzi

$$km \equiv 1 \pmod{n},$$

$\{ \iff km = 1 \text{ w } \mathbb{Z}_n \}$

to nazywamy ją elementem odwrotnym do k.

Piszemy wtedy

$$k^{-1} = m \quad (\mathbb{Z}_n).$$

Tw. $k \in \mathbb{Z}_n$ ma element odwrotny wtedy i tylko wtedy, gdy
$$NWD(k,n) = 1.$$

- $NWD(k,n) = 1 \overset{RAE}{\Longrightarrow} \bigvee_{s,t \in \mathbb{Z}} sk + tn = 1 \Rightarrow sk \equiv 1 \pmod{n}$
- $NWD(k,n) = d > 1 \Rightarrow$ gdyby $sk \equiv 1 \pmod{n}$, to $sk = 1 + m \cdot n$, wpc
$$1 = sk - mn.$$
Sprzeczność, bo $d \mid sk - mn$, ale $d \nmid 1$.

Tw. (Jedyność elementu odwrotnego).
Jeżeli $k^{-1} = m$ i $k^{-1} = l$, to $m = l$.

Dow.
$$m = m \cdot 1 = m \cdot (k \cdot l) = (m \cdot k) \cdot l = \quad (w\ \mathbb{Z}_n)$$
$$= 1 \cdot l = l$$

Układy kongruencji

$$\begin{cases} x \equiv 1 \pmod{13} \\ x \equiv 4 \pmod{15} \end{cases}$$

$$\underline{x} = 1 + 13k, \quad k \in \mathbb{Z} \implies x = 1 + 13k = 1 + 13(6 + 15l) = \boxed{79 + 13 \cdot 15 l}, \; l \in \mathbb{Z}$$

$$= \boxed{79 + 195 l}, \quad l \in \mathbb{Z}.$$

$$1 + 13k \equiv 4 \pmod{15}$$

$$13k \equiv 3 \pmod{15} \quad \Big| \cdot 7 = 13^{-1}$$

$$7 \cdot 13k \equiv 7 \cdot 3 \pmod{15}$$

$$k \equiv 6 \pmod{15}$$

$$\implies k = 6 + 15l, \quad l \in \mathbb{Z}$$

d	q	s	t
15		1	0
13	1	0	1
2	6	1	−1
$\boxed{1}$	2	$\boxed{-6}$	$\boxed{7}$
0			

$$\implies 1 = (-6) \cdot 15 + 7 \cdot 13 \quad \big| \pmod{15}$$

$$1 \equiv 7 \cdot 13 \pmod{15} \implies 13^{-1} = 7 \; (\mathbb{Z}_{15})$$

Chińskie twierdzenie o resztach

$$(*) \quad \begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

Tw. Jeżeli $a, b \in \mathbb{Z}$ i $m, n \in \mathbb{N}$, $m, n \geq 2$ oraz $\boxed{NWD(m,n) = 1}$, to w zbiorze $\{0, 1, \ldots, m \cdot n - 1\}$ istnieje dokładnie jedno rozwiązanie x_0 spełniające $(*)$.

Każde inne rozwiązanie x kongruencji $(*)$ różni się od x_0 o wielokrotność $m \cdot n$.

$$\left\{ \begin{array}{l} 0 \leq x_0 \leq m \cdot n - 1 \\ x = x_0 + k \cdot n \cdot m, \quad k \in \mathbb{Z} \end{array} \right\}$$

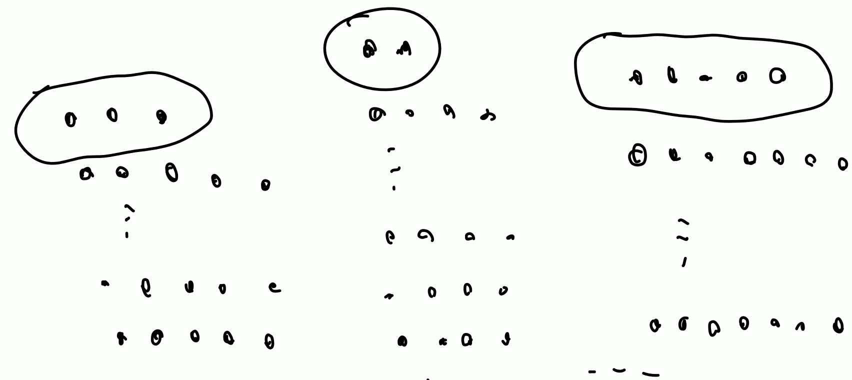
Chińskie twierdzenie o resztach

Tw. Jeżeli $a_1, \dots, a_k \in \mathbb{Z}$, $n_1, \dots, n_k \geq 2$ i

$\mathrm{NWD}(n_i, n_j) = 1$ dla $i, j \in \{1, \dots, k\}$, $i \neq j$,

to układ

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$



ma dokładnie jedno rozwiązanie x_0 w zbiorze

$\{0, 1, \dots, n_1 n_2 \cdots n_k - 1\}$.

$$x = x_0 + n_1 \cdot n_2 \cdots n_k \cdot m, \quad m \in \mathbb{Z}.$$

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{4} \\ x \equiv 5 \pmod{7} \end{cases}$$

Systemy resztowe (RNS)

Residue Number System

m, n - moduły, $NWD(m,n) = 1$

$$\{0, 1, \dots, m \cdot n - 1\} \overset{CTR}{\longleftrightarrow} \left\{(a, b) : \begin{array}{l} a \in \mathbb{Z}_m \\ b \in \mathbb{Z}_n \end{array}\right\}$$

$m = 13, \quad n = 15$

$$\{0, 1, \dots, 194\} \ni 79 \longleftrightarrow (1, 4) \in \mathbb{Z}_{13} \times \mathbb{Z}_{15}$$

$$\mathbb{Z}_{195} \cong \mathbb{Z}_{13} \times \mathbb{Z}_{15}$$

Systemy resztowe

$m = 3, \quad n = 4 \qquad \mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_4$

$\mathbb{Z}_{12}$	$\mathbb{Z}_3 \times \mathbb{Z}_4$
0	(0, 0)
1	(1, 1)
2	(2, 2)
3	(0, 3)
4	(1, 0)
5	(2, 1)
6	(0, 2)
7	(1, 3)
8	(2, 0)
9	(0, 1)
10	(1, 2)
11	(2, 3)

różne!

int 32 bity

$m = 2^{32}, \quad 2^{32} - 1 = n$

$\mathbb{Z}_{2^{64} - \cancel{2^{32}}} \cong \mathbb{Z}_{2^{32}} \times \mathbb{Z}_{2^{32}-1}$

$2 + 7 = 9$

$(2,2) + (1,3) = (0,1)$

Kryptografia