(*) $mx \equiv a \pmod n$ ✓

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

$x = 1 + 13k, \quad k \in \mathbb{Z}$

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

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

$k \equiv 21 \equiv 6 \pmod{15}$

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

	q	t
15		0
13	1	1
2	6	-1
1	2	7
0		

$7 = 13^{-1} \pmod{15}$

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

$13 \cdot 15 l = 195 l$

Tw. (Chińskie twierdzenie o resztach)

$m, n \geq 2, \quad NWD(m,n) = 1$

$\Rightarrow$ Dla dowolnych $a, b \in \mathbb{Z}$ istnieje dokładnie jedno rozwiązanie x_0 układu

$$\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases}$$

w zbiorze $\{0, 1, \dots, m \cdot n - 1\}$. Każde rozwiązanie $x \in \mathbb{Z}$ tego układu jest postaci:

$x = x_0 + m \cdot n \, k, \quad k \in \mathbb{Z}.$

Tw. (CTR)

$n_1, \dots, n_k \geq 2$, $\bigwedge_{i,j \in \{1,\dots,k\}} NWD(n_i, n_j) = 1$.

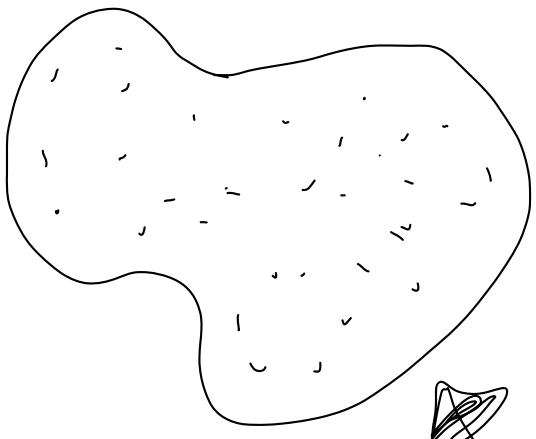
$\Rightarrow NWD(n_1, \dots, n_k) = 1$

$\Rightarrow$ Dla dowolnych $a_1, \dots, a_k \in \mathbb{Z}$ istnieje dokładnie jedno rozwiązanie x_0 układu

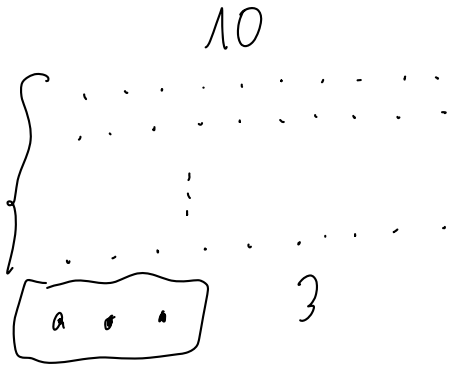
$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

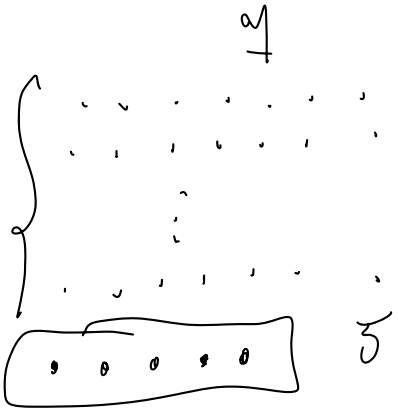
w zbiorze $\{0, 1, \dots, n_1 \cdots n_k - 1\}$. Każde inne rozwiązanie x jest postaci

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



mod 10 · 7





$a \in \mathbb{Z}_m = \{0,1,\dots,m-1\}$ $\quad NWD(m,n)=1$

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

CTR

$(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_n \rightsquigarrow$ rozmieszczenie w $\mathbb{Z}_{m\cdot n}$

$\{0,1,\dots,mn-1\}$

$$\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases} \rightsquigarrow \quad x \in \mathbb{Z}_{m\cdot n}$$

$79 \in \mathbb{Z}_{13\cdot 15} \Rightarrow$ $\quad 79 \equiv 1 \pmod{13}$, $\quad 79 \equiv 4 \pmod{15}$

$79 \in \mathbb{Z}_{13\cdot 15} \overset{CTR}{\Leftarrow} (1,4) \in \mathbb{Z}_{13} \times \mathbb{Z}_{15}$

$\#\mathbb{Z}_{mn} = \#\mathbb{Z}_m \cdot \#\mathbb{Z}_n$

$m=5, \quad n=7$

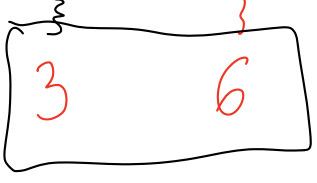
0	(0,0)
1	(1,1)
2	(2,2)
3	(3,3)
4	(4,4)
5	(0,5)
6	(1,6)
7	(2,0)
8	(3,1)
9	(4,2)
⋮	⋮
34	(4,6)

$(3,2)$

$(4,5)$

zbiór różnych par.

$(3,3)+(1,6) = (4,9) \equiv (4,2) \quad (\bmod 5, \bmod 7)$



$$\mathbb{Z}_{m \cdot n} \cong \mathbb{Z}_m \times \mathbb{Z}_n$$

$x, y \in \mathbb{Z}_{m \cdot n} \rightsquigarrow x \sim (a, b)$, $y \sim (c, d)$

$x + y = ?$

$$(a, b) + (c, d) = (e, f)$$

$x + y = (e, f) = z$

---

int 3 bity 111

$\{0, 1, \dots, 7\}$ 10110101

5, 7 $\mathbb{Z}_5 \times \mathbb{Z}_7$

2 × int $\rightsquigarrow$ $\{0, 1, \dots, 34\}$

$\mathbb{Z}_5 \times \mathbb{Z}_6 \times \mathbb{Z}_7 \sim (a, b, c)$

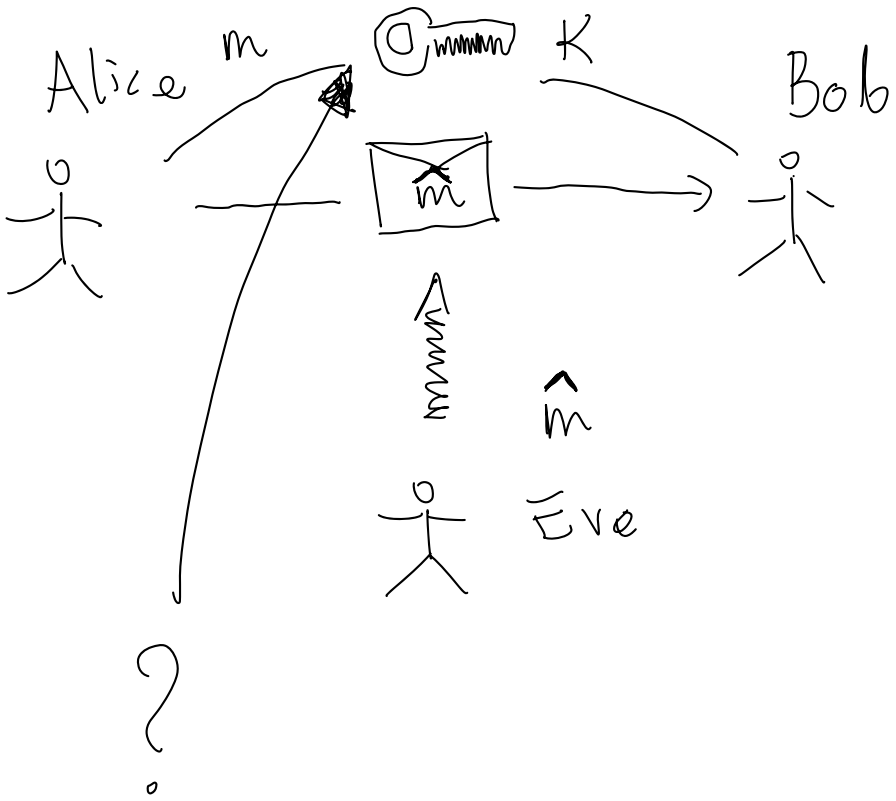
$\cong \mathbb{Z}_{5 \cdot 6 \cdot 7}$

$30 \cdot 7 = 210$

$\{0, \dots, 209\}$

int 32 bit $\rightarrow$ 128 bit

RNS (residue number system)


Alice
m
K
Bob
m
$\hat{m}$
Eve
?