$$mx \equiv a \pmod{n} \qquad NHD(m,n) = d$$

$d = 1$

$m^{-1} \bmod n$ istnieje

Wyliczamy m^{-1}

$$mx \equiv a \pmod{n} \mid \cdot m^{-1}$$

$$x \equiv a \cdot m^{-1} \pmod{n}$$

$$\boxed{x = a \cdot m^{-1} + kn,\ k \in \mathbb{Z}}$$

$d > 1$

$d \nmid a$

$$mx \equiv a \pmod{n}$$

$$mx = a + kn$$

$$a = \underbrace{mx - kn}$$

$$d \mid mx - kn$$

sprzeczność z $d \nmid a$

brak rozw.

$d \mid a$

$$mx \equiv a \pmod{n}$$

$$mx = a + kn \quad | : d$$

$$\frac{m}{d} x = \frac{a}{d} + k \frac{n}{d}$$

$$m' \qquad a' \qquad n'$$

$$m'x = a' + kn'$$

$$\boxed{m'x \equiv a' \pmod{n'}}$$

$$NHD(m', n') = \underline{1} \quad \boxed{\text{ćw.}}$$

Przykład.

$$20x \equiv 6 \pmod{74} \qquad NHD(20,74) = \underline{\overset{d}{2}} > 1$$

$d \mid a$?

$2 \mid 6$ ✓

$$20x \equiv 6 \pmod{74} \mid : 2$$

$$10x \equiv 3 \pmod{37} \mid \cdot 10^{-1} \qquad NHD(10,37) = 1$$

d	q	s	t
37		1	0
10	3	0	1
7	1	1	-3
3	2	-1	4
$\boxed{1}$	3	$\boxed{5}$	$\boxed{-11}$
0			

$$\to \quad 1 = \underbrace{5 \cdot 37}_{0} + (-11) \cdot 10 \quad | \bmod 37$$

$$1 \equiv \boxed{(-11)} \cdot 10 \pmod{37}$$

$$10^{-1} = -11 = 26$$

$$10^{-1}$$

$$-11 \equiv 26 \pmod{37}$$

$$10x \equiv 3 \pmod{37} \quad | \cdot (-11)$$

$$10 \cdot (-11) = -110$$

$$x \equiv -33 \pmod{37}$$

$$\boxed{x \equiv 4 \pmod{37}}$$

$$\boxed{x = 4 + 37 \cdot k, \quad k \in \mathbb{Z}}$$

Przykład

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

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

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

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

$$\boxed{NWD(13, 15) = 1}$$

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

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

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

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

$$x = 1 + 13(6 + 15l) =$$

$$= 79 + 13 \cdot 15l =$$

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

$$13 \cdot 7 = 91 = \underset{15 \cdot 6}{90} + 1 \equiv 1 \pmod{15}$$

__Tw.__ (Chińskie twierdzenie o resztach)

$m, n \in \mathbb{N}$, $m, n \geq 2$, $NWD(m, n) = 1$

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

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

należące do zbioru $\{0, 1, 2, \ldots, mn-1\}$. Jeżeli $x_1 \in \mathbb{Z}$ spełnia $(*)$, to

$$\underline{x_1 \equiv x_0 \pmod{mn}}.$$

__Tw.__ (uogólnienie CTR)

$n_1, n_2, \ldots, n_k \geq 2$, $\underline{NWD(n_i, n_j) = 1, \quad i \neq j}$

$\cancel{NWD(n_1, n_2, \ldots, n_k) = 1}$

Dla dowolnych $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ ist. dokł. jedno rozw. x_0 układu

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

$\cancel{n_1 = 4}$
$\cancel{n_2 = 8}$
$n_3 = 9$

$NWD(4,8) = 4$

$NWD(4,8,9) = 1$

w zbiorze $\{0, 1, 2, \ldots, n_1 n_2 \ldots n_k - 1\}$.

$$x_1 \equiv x_0 \pmod{n_1 n_2 \ldots n_k}.$$

$\{0,1,\dots,mn-1\}$ CTR $\left\{(a,b) : \begin{array}{l} a\in\{0,1,\dots,m-1\} \\ b\in\{0,1,\dots,n-1\}\end{array}\right\}$

$m=5$, $n=6$ NWD$(5,6)$ $5\cdot 6=30$ par

$\{0,1,\dots,29\} \longleftrightarrow \left\{(a,b) : \begin{array}{l} a\in\{0,1,2,3,4\} \\ b\in\{0,1,2,3,4,5\}\end{array}\right\}$

CTR

$\begin{cases} x\equiv a \pmod 5 \\ x\equiv b \pmod 6\end{cases}$

system bez przeniesień (carry-free system) (a,b)

0	(0,0)
1	(1,1)
2	(2,2)
3	(3,3)
4	(4,4)
5	(0,5)
6	(1,0)
7	(2,1)
8	(3,2)
⋮	
20	(0,2)
⋮	
27	(2,3)
28	(3,4)
29	(4,5)

$7 + 20 = 27$

$$\boxed{(2,1)+(0,2)=(2,3)}$$

$(1,3)+(4,2) = (0,5)$

$2^3=8$

$(2,2)^3=(4,4)\cdot(2,2)=(3,2)$

$\boxed{\text{int } 32b}$

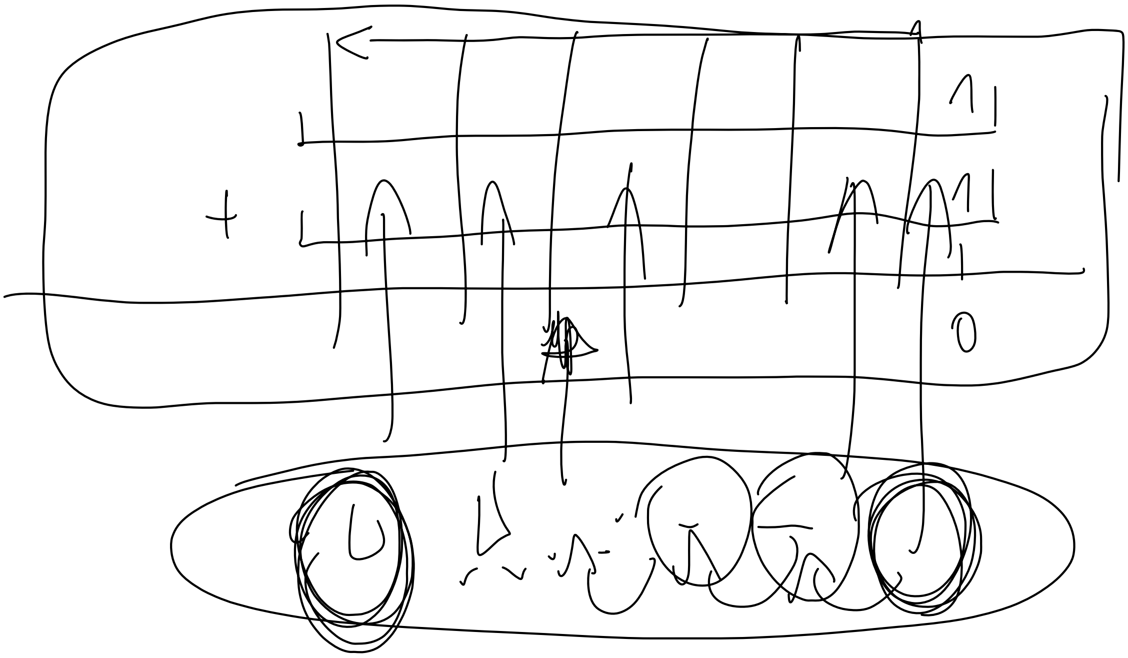
(int, int)
32b 32b

$2^{31}-1$, $2^{31}+1$

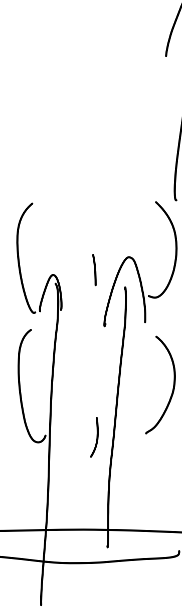
64b.

64

x	y



$(a,b)+(c,d) =$
$(a+c,\, b+d)$



RNS - residue number systems

$5, 6$

$(3,5) \quad \begin{matrix} < \\ > \end{matrix} \quad (4,2)$

$(3,5)-(4,2) =$
$= \boxed{(4,3)} \quad \begin{matrix} > 0 \\ < 0 \end{matrix}$

CTR

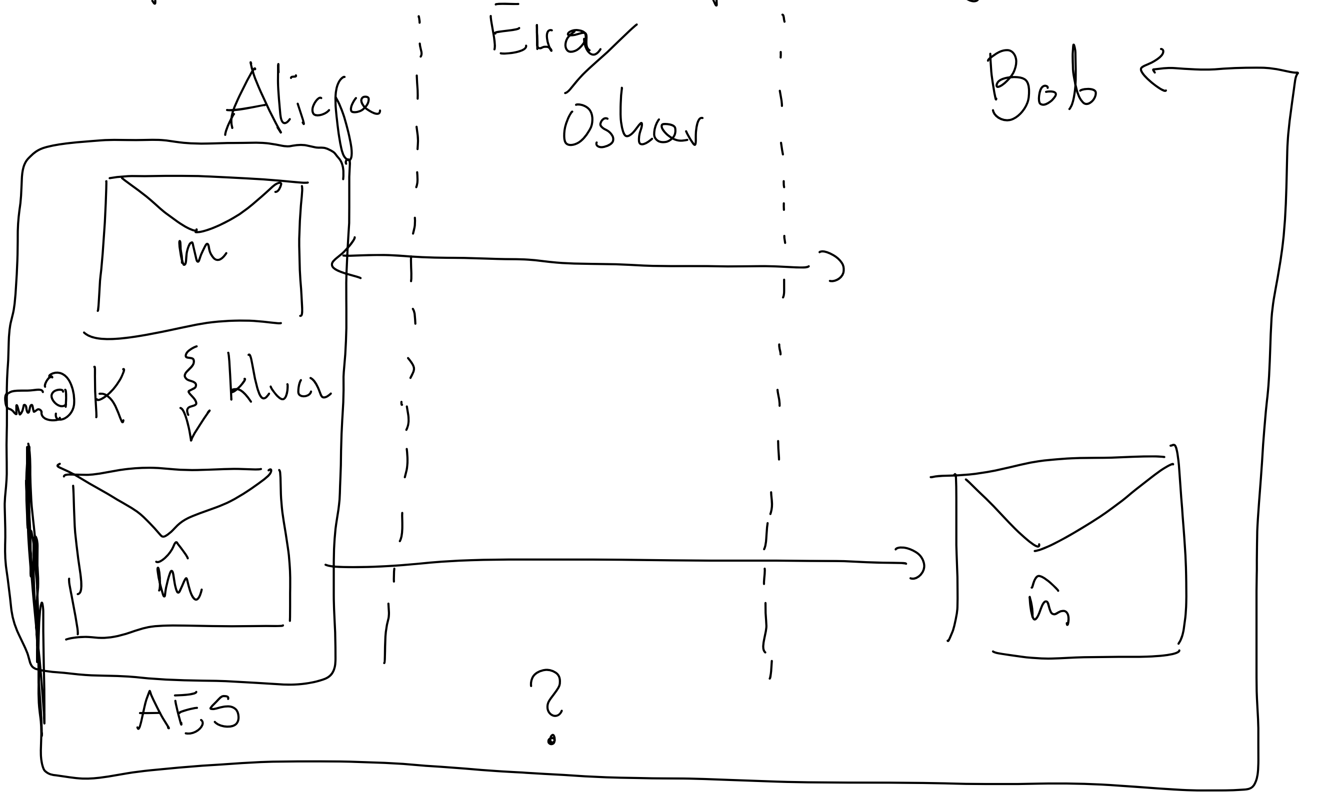
?

$2^0 \quad 2^1 \quad 2^2 \quad \dots$

$n_1 \quad n_1 n_2 \quad n_1 n_2 n_3 \quad \dots$

$2^n-1,\ 2^n+1$

Kryptografia klucza publicznego



1970' Protokół Diffiego-Hellmana 1973

System RSA 1976