Kongruencje

$n \geq 2 \qquad a, b \in \mathbb{Z} \qquad \boxed{n \mid a-b} \iff a \equiv b \pmod{n}$

a przystaje do b modulo n

$n = 8$

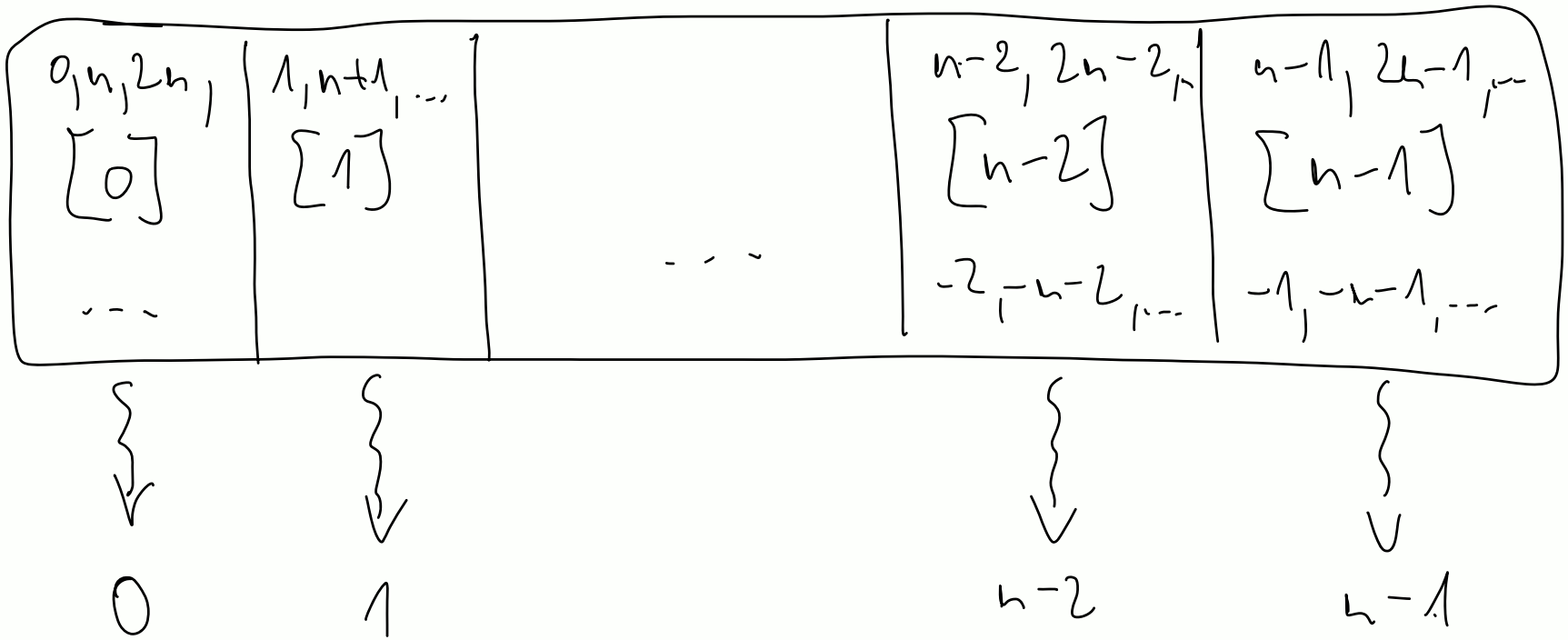
$$3 \equiv 11 \pmod{8}$$
$$11 \equiv -5 \pmod{8}$$

$a \equiv b \pmod{n} \qquad a \equiv_n b$

$a \equiv_n b$

$0, 1, \ldots, n-1$

$\mathbb{Z}$



Własności relacji przystawania

Fakt. Jeśli $a \equiv b \pmod n$ i $c \equiv d \pmod n$,

to

$$a + c \equiv b + d \pmod n$$

oraz

$$a \cdot c \equiv b \cdot d \pmod n.$$

Dow. CH.

$a \equiv b \pmod n$

$\Leftrightarrow \; n \mid a - b$

$\Leftrightarrow \; \bigvee_{k \in \mathbb{Z}} \; a - b = n \cdot k$

Wniosek.

Jeśli $a \equiv b \pmod n$, to

$$a^k \equiv b^k \pmod n$$

$k \in \mathbb{N}$

Przykład

Jaka jest reszta z dzielenia 7^{2024} przez 22?

$\{0, 1, \ldots, 21\}$

k	$7^k \bmod 22$
1	7
2	5
3	13
4	3
5	$21 \equiv -1$
$\vdots$	$\vdots$
10	1

$7^2 \equiv 5 \pmod{22} \mid \cdot 7$

$7^3 \equiv 5 \cdot 7 \pmod{22}$

$7^3 \equiv 13 \pmod{22}$

$21 \equiv -1 \pmod{22}$

$7^5 \equiv -1 \pmod{22} \mid ()^2$

$7^{10} \equiv 1 \pmod{22} \mid ()^k$

$7^{10k} \equiv 1 \pmod{22}$

$7^{2024} = \underbrace{7^{2020}}_{\equiv 1} \cdot 7^4 \equiv 1 \cdot 7^4 \equiv 3 \pmod{22}$

Małe twierdzenie Fermata

$n \geq 2, \quad a \in \mathbb{Z}$ $\quad a^k \equiv 1 \pmod{n}$?

$k = ?$

Małe tw. Fermata: Jeżeli p jest liczbą pierwszą oraz p nie dzieli a, to

$$a^{p-1} \equiv 1 \pmod{p}.$$

$p = 37 \qquad a = 30$

MTF $\Rightarrow \quad 30^{36} \equiv 1 \pmod{37}$

Funkcja Eulera

$n \in \mathbb{N}$

$\varphi(n) =$ "liczba liczb naturalnych $\leq n$, które są względnie pierwsze z n"

$= |\{m \in \{1, 2, \ldots, n\} : NWD(m, n) = 1\}|$

$\varphi(10) = 1 \not 2 \not 3 \not 4 \not 5 \not 6 \not 7 \not 8 \not 9 \not 10$

$= 4$

---

1. Jeżeli p jest liczbą pierwszą i $a \in \mathbb{N}$, to
$$\varphi(p^a) = p^a - p^{a-1}$$

2. Jeżeli $NWD(m, n) = 1$, to $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$

$$\varphi(2^3 \cdot 3^2 \cdot 7^4) \overset{2.}{=} \varphi(2^3) \cdot \varphi(3^2) \cdot \varphi(7^4) \overset{1}{=}$$

$$= (2^3 - 2^2)(3^2 - 3^1)(7^4 - 7^3) =$$

$$= \dots$$

Tw. Eulera: Jeżeli $n \geq 2$ i $a \in \mathbb{Z}$ oraz $NWD(n, a) = 1$, to

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

$n = 22$, $a = 7$

$$\varphi(22) = \varphi(2 \cdot 11) = \varphi(2) \cdot \varphi(11) = 1 \cdot 10 = 10$$

$$TE \Rightarrow \quad 7^{10} \equiv 1 \pmod{22}$$

Kongruencje liniowe z jedną niewiadomą

$mx = a \qquad x = \frac{a}{m}$

$x \equiv \frac{a}{m} \pmod{n}$

$mx \equiv a \pmod{n}$

$6x \equiv 5 \pmod{13} \quad | \cdot 2$

$2 \cdot 6 = 12 \equiv -1 \pmod{13}$

$12x \equiv 10 \pmod{13}$

$-x \equiv 10 \pmod{13} \quad | \cdot (-1)$

$x \equiv -10 \pmod{13}$

$x \equiv 3 \pmod{13}$

$x = 3 + 13k, \quad k \in \mathbb{Z}$

$$20x \equiv 6 \pmod{74} \qquad NWD(20,74)=2$$

$$\Updownarrow$$

$$\bigvee_{k\in\mathbb{Z}} \quad 20x = 6 + 74k \quad | : NWD(20,74)=2$$

$$10x = 3 + 37k$$

$$\Updownarrow$$

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

$NWD(10,37)=1$

$= s\cdot 10 + t\cdot 37$

$\bigvee_{s,t\in\mathbb{Z}}$

d	q	s	t
10		1	0
37	0	0	1
10	3	1	0
7	1	-3	1
3	2	4	-1
1	3	-11	3
0			

$1 = (-11)\cdot 10 + 3\cdot 37$

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

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

$\equiv 1$

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

$x \equiv 4 \pmod{37}$

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