$a, b \in \mathbb{Z}$, $n \geq 2$

$a \equiv b \pmod{n} \iff n \mid a-b \iff \bigvee_{k\in\mathbb{Z}} a = b + nk$

$a \equiv_n b$

$a =_n b$

---

1. $7^{2025} \bmod 22$?

$7^1 \equiv 7 \pmod{22}$ $\big)\cdot 7$

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

$7^3 \equiv 7^2 \cdot 7 \equiv 5 \cdot 7 \equiv 13 \pmod{22}$ $\big)\cdot 7$

$7^4 \equiv 13 \cdot 7 \equiv 3 \pmod{22}$ $\big)\cdot 7$

$7^5 \equiv 21 \equiv -1 \pmod{22}$

$7^6 \equiv -7 \equiv 15 \pmod{22}$

$7^7 \equiv 17 \equiv -5 \pmod{22}$

$7^8 \equiv 9 \pmod{22}$

$7^9 \equiv 19 \equiv -3 \pmod{22}$

$7^{10} \equiv -21 \equiv \boxed{1} \pmod{22}$ $\leftarrow$

$7^{11} = 7^{10} \cdot 7 \equiv 7 \pmod{22}$

5

13

3

$\vdots$

7^{2025}

$7^{10} \equiv 1 \pmod{22} \quad | \, ()^k$

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

$7^{2025} = 7^{2020+5} = 7^{2020} \cdot 7^5 \equiv$

$\equiv 1 \cdot 7^5 \equiv \underline{\underline{21}} \pmod{22}$

▷ Tw. Małe twierdzenie Fermata.

$$\left.\begin{array}{l} \bullet\ p \text{ jest liczbą pierwszą} \\ \bullet\ NWD(a,p)=1 \ \{p \nmid a\} \end{array}\right\} \Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

Wniosek.

$$24^{36} \equiv 1 \pmod{37}$$

Funkcja Eulera

$$\varphi(n) = \#\{k \in \{1,2,\dots,n\} : NWD(k,n)=1\}$$

$$\varphi(10) = \#\{1,\cancel{2},3,\cancel{4},\cancel{5},\cancel{6},7,\cancel{8},9,\cancel{10}\} = 4$$

- $\boxed{\varphi(p^{\alpha})} = \{1,2,\dots,\cancel{p},\cancel{2p},\dots,p^{\alpha}\} = \boxed{p^{\alpha} - p^{\alpha-1}}$

  $p \cdot p^{\alpha-1}$

  l. pierwsza

  $NWD(k,p^{\alpha}) > 1 \Rightarrow p \mid k$

  $3^5 \quad \{1,2,\cancel{3},4,5,\cancel{6},\dots,\cancel{9},\dots,\cancel{3^5}\}$

  $NWD(k,3^5) > 1 \Rightarrow 3 \mid k$

  $\boxed{1, 3, 3^2, 3^3, 3^4, 3^5}$

  $$\varphi(3^5) = 3^5 - 3^4$$

- $NWD(m,n)=1 \Rightarrow \varphi(m \cdot n) = \varphi(m)\varphi(n)$

$$\varphi(120) = \varphi(20\cdot 6) = \varphi(4\cdot 5\cdot 2\cdot 3) = \varphi(2^3\cdot 3\cdot 5) =$$

$$= \varphi(2^3)\cdot\varphi(3\cdot 5) = \varphi(2^3)\cdot\varphi(3)\cdot\varphi(5) =$$

$= (2^3 - 2^2) \cdot (3^1 - 3^0)(5^1 - 5^0) =$

$= 4 \cdot 2 \cdot 4 = \boxed{32}$

D Twierdzenie Eulera. $a, n \in \mathbb{Z}$

$NWD(a, n) = 1 \implies a^{\varphi(n)} \equiv 1 \pmod{n}$

Wniosek.

$11^{\varphi(120)} \equiv 11^{32} \equiv 1 \pmod{120}$

$mx = a \quad | \cdot m^{-1}$ (o ile $m \neq 0$)

$x = a \cdot m^{-1}$

$m, a \in \mathbb{Z} \not\Rightarrow x \in \mathbb{Z}$

$mx \equiv a \pmod{n} \quad | \cdot m^{-1}$???

$6x \equiv 5 \pmod{13} \quad | \cdot \{6^{-1}\} \cdot 11 \quad \{-2\}$

$6 \cdot 11 \equiv 1 \pmod{13}$

$6^{-1} = 11$

$6 \cdot 11 \cdot x \equiv 5 \cdot 11 \pmod{13}$

$x \equiv 3 \pmod{13}$

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

$6x \equiv 5 \pmod{14} \quad | \cdot 6^{-1}$???

$\bigvee_{k \in \mathbb{Z}} 6x = 5 + 14k$

$6x - 14k = 5$ sprzeczność, bo $2 \mid 6x - 14k$

$2 \nmid 5$

Def. (Element odwrotny) m, n, $m \in \{0,1,\dots,n-1\} = \mathbb{Z}_n$

Jeżeli istnieje liczba $k \in \{0,1,\dots,n-1\}$, dla której

$$m \cdot k \equiv 1 \pmod{n},$$

to k nazywamy odwrotnością m modulo n i oznaczamy

$$k = m^{-1} \pmod{n}.$$

Fakt. Jeżeli $m^{-1} \pmod{n}$ istnieje, to jest jedyne.

Dow. Załóżmy, że

$$m \cdot k \equiv 1 \pmod{n} \quad i \quad m \cdot k' \equiv 1 \pmod{n},$$

gdzie $\boxed{k, k' \in \mathbb{Z}_n}$. Wtedy

$$k = k \cdot 1 \equiv_n k \cdot (m \cdot k') = \underbrace{(k \cdot m)}_{\equiv_n 1} k' \equiv_n 1 \cdot k' = k'.$$

$$\Downarrow$$

$$k \equiv k' \pmod{n}$$

$$k = k'.$$

Fakt. $m^{-1} \pmod{n}$ istnieje $\iff NWD(m,n) = 1$.

Dlaczego? Bo RAE.

$$NWD(m,n) = 1 \overset{RAE}{\Longrightarrow} \bigvee_{s,t \in \mathbb{Z}} \underbrace{sm + tn = 1}\ \Big| \pmod{n}$$

$$\Downarrow$$

$$sm + \underset{\overset{|||_n}{0}}{tn} \equiv 1 \pmod{n}$$

$$\Downarrow$$

$$m^{-1} \pmod{n}$$

$$sm \equiv 1 \pmod{n}$$

$$mx \equiv a \pmod n$$

$$d = NWD(m,n)$$

$d = 1$

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

Wyliczamy

$k = m^{-1} \pmod n$ z RAE

$mx \equiv a \pmod n \; | \cdot k$

$kmx \equiv ka \pmod n$

$x \equiv ka \pmod n$

$x = ka + n \cdot l, \; l \in \mathbb{Z}$

$d > 1$

$d \nmid a$

$mx \equiv a \pmod n$

$\bigvee_k \; mx = a + kn$

$mx - kn = a$

$d \mid mx - kn \wedge d \nmid a$

spr.

$d \mid a$

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

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

$m'x = a' + kn'$

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

$NWD(m', n') = 1$

- $20x \equiv 7 \pmod{74}$

  $NWD(20, 74) = 2$

  $2 \mid 7$? F

  $\Downarrow$

  spr.

74	
20	
14	
6	
$\boxed{2}$	
0	

- $20x \equiv 6 \pmod{74} \quad |:2$

  $NWD(20, 74) = 2$

  $10x \equiv 3 \pmod{37}$

$10^{-1} \pmod{37}$

$\downarrow$

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

$NWD(37, 10) = 1 = s \cdot 37 + (-11) \cdot 10$

$10^{-1} \pmod{37} \cong -11 = 26$

0

$$10x \equiv 3 \pmod{37} \quad | \cdot 26$$

$$x \equiv 3 \cdot 26 \pmod{37}$$

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

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