Zad. Wyznacz resztę z dzielenia

$$7^{2025}$$

przez 15.

$$7^1 \equiv 7 \pmod{15} \quad | \cdot 7$$

$$7^2 \equiv 49 \equiv 4 \pmod{15} \quad | \cdot 7$$

$$7^3 \equiv 4 \cdot 7 \equiv 28 \equiv 13 \pmod{15} \quad | \cdot 7$$

$$7^4 \equiv 13 \cdot 7 \equiv 91 \equiv 1 \pmod{15} \quad | ()^k$$

$$7^{4k} \equiv 1 \pmod{15}, \quad k \in \mathbb{N}$$

506

$$7^{2025} = 7^{2024+1} = 7^{2024} \cdot 7 = \underbrace{7^{4 \cdot k}}_{\equiv 1} \cdot 7 \equiv 1 \cdot 7 \equiv 7 \pmod{15}$$

$\boxed{\text{Wniosek z RAE: Jeżeli } c | ab \text{ oraz } NWD(c, a) = 1, \text{ to } c | b.}$

$$NWD(c, a) = 1 \overset{RAE}{\Rightarrow} \bigvee_{s, t \in \mathbb{Z}} sc + ta = 1$$

$$\Downarrow$$

$$a = \frac{1 - sc}{t}$$

$$c | ab \Rightarrow ab = kc, \quad k \in \mathbb{Z}$$

$$ab = \frac{1-sc}{t} b \Rightarrow \frac{1-sc}{t} b = kc$$

$$(1-sc)b = tkc \qquad b - scb = tkc$$

$$b = tkc + scb$$

$$\boxed{b = c\underbrace{(tk + sb)}_{\in \mathbb{Z}}} \Rightarrow c \mid b.$$

Małe tw. Fermata

Jeżeli p jest liczbą pierwszą oraz $a \in \mathbb{Z}$, to

$$a^p \equiv a \pmod p.$$

Jeżeli dodatkowo a nie jest wielokrotnością p, to ($\Leftrightarrow NWD(a,p)=1$)

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

$$3^{36} \equiv 1 \pmod{37}$$

Dow. $\boxed{NWD(a,p)=1 \Rightarrow a^{p-1} \equiv 1 \pmod p}$

$$i, j \in \{1, 2, \dots, p-1\}$$

Załóżmy, że

$$ai \equiv aj \pmod p$$

$$ai - aj \equiv 0 \pmod p$$

$$a(i-j) \equiv 0 \pmod p$$

$$\Updownarrow$$

$$p \mid a(i-j)$$

Wniosek ④ $NWD(a,p)=1 \Rightarrow \boxed{p \mid i-j}$

$$\boxed{-(p-2) \leq i-j \leq p-2}$$

$$i-j=0$$

$$\boxed{i=j}$$

$$\boxed{(a\cdot 1)\cdot(a\cdot 2)\cdot(a\cdot 3)\cdot\ldots\cdot(a\cdot(p-1))} = \boxed{a^{p-1}\cdot 1\cdot 2\cdot 3\cdot\ldots\cdot(p-1)}$$

$$\equiv$$

$$\boxed{1\cdot 2\cdot 3\cdot\ldots\cdot(p-1)}$$

$p-1$ różnych reszt mod p

$$\{a1, a2, a3, \ldots, a(p-1)\} \overset{\text{mod } p}{\equiv} \{1, 2, 3, \ldots, p-1\}$$

$$(p-1)! \equiv a^{p-1}(p-1)! \pmod p$$

$$\underline{(p-1)!\,(a^{p-1}-1)} \equiv 0 \pmod p$$

$$\left.\begin{array}{l} p \mid (p-1)!\,(a^{p-1}-1) \\ NWD(p, (p-1)!) = 1 \end{array}\right\} \xRightarrow{\text{wniosek}} p \mid a^{p-1}-1$$

$$\Updownarrow$$

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

$$7^{2015} \equiv \, ? \pmod{15}$$

Tw. Eulera („Ojlera")

Funkcja Eulera φ, $n \in \mathbb{N}$

$\varphi(n) =$ liczba liczb ze zbioru $\{1, 2, \dots, n\}$, które są względnie pierwsze z n

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

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

---

1) p – liczba pierwsza

$$\varphi(p) = p - 1$$

$$\overbrace{1 \cdot p, 2p, 3p, \dots, p^{a-1} \cdot p}^{p^{a-1}}$$

2) $a \in \mathbb{N}$

$$\varphi(p^a) = \#\{1, 2, \dots, \cancel{p}, \dots, \cancel{2p}, \dots, \cancel{3p}, \dots, \cancel{p^2}, \dots, \dots, \cancel{p^a}\}$$

$$= p^a - p^{a-1}$$

$$\varphi(1024) = \varphi(2^{10}) = 2^{10} - 2^9 = 2^9 = 512$$

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

$$\boxed{\varphi(mn) = \varphi(m)\varphi(n)}$$

$$\varphi(120) = \varphi(\underline{2^3 \cdot 3^1 \cdot 5^1}) = \varphi(2^3)\varphi(3)\varphi(5) =$$
$$= (2^3 - 2^2)(3-1)(5-1) = 4 \cdot 2 \cdot 4 = \boxed{32}$$

$$\boxed{\varphi(\underbrace{p \cdot q}_{n}) = (p-1)(q-1)}$$

$$7^{2025} \equiv ? \pmod{15}$$

i	$7^i \bmod 15$
1	7
2	4
3	13
4	$\boxed{1}$

$$7^4 \equiv 1 \pmod{15} \quad |()^k$$
$$7^{4k} \equiv 1 \pmod{15}$$
$$7^{2025} = 7^{2024+1} = 7^{2024} \cdot 7$$
$$\equiv 1 \cdot 7 \equiv 7 \pmod{15}$$

Th. Eulera. $n \in \mathbb{N}$, $a \in \mathbb{Z}$, $NSD(a,n) = 1$.

Potom

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

---

p – l. prvočíslo

$\varphi(p) = p - 1$

Dov. CU (tohle samo jako MTF)

$$7^{2025} \equiv ? \pmod{15}$$

$NSD(7, 15) = 1$

$$\varphi(15) = \varphi(3 \cdot 5) = \varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8$$

$$7^8 \equiv 1 \pmod{15} \quad |()^k$$
$$7^{8k} \equiv 1 \pmod{15}$$

$7^{2025} = 7^{8\cdot(\overset{?}{253})+1} = 7^{8k+1} =$

$= \underbrace{7^{8k}}_{1} \cdot 7 \equiv 7 \pmod{15}.$

$$\begin{array}{l} \ \ 253 \\ 2025:8 \\ 16 \\ \ \ 42 \\ \ \ 40 \\ \ \ \ 25 \end{array}$$

Znajdź dwie ostatnie cyfry liczby

$3^{3^{2025}}$.

$3^{3^{2025}} \equiv ? \pmod{100}$

$3^{3^{2025}} \neq 3^{3\cdot 2025}$

$(a^b)^c = a^{bc}$

$a^{(b^c)} \neq (a^b)^c$

$3^{\boxed{k}} \equiv ? \pmod{100}$ $\qquad k = 3^{2025}$

i	$3^i \bmod 100$
1	3
2	9
3	27
4	81
5	43
⋮	⋮
?	$\boxed{1}$
⋮	
40	1

$NWD(3, 100) = 1$

TE: $3^{\varphi(100)} \equiv 1 \pmod{100}$

$\varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(2^2)\varphi(5^2) =$

$= (2^2 - 2)(5^2 - 5) =$

$= \underline{40}$

$$\boxed{3^{40} \equiv 1 \pmod{100}} \qquad 10^k$$

$$3^{40k} \equiv 1 \pmod{100}$$

$$3^{3^{2025}} \equiv ? \pmod{100} \rightsquigarrow 3^{2025} \equiv ? \pmod{40}$$

$$NWD(3, 40) = 1$$

$$\varphi(40) = \varphi(8 \cdot 5) = \varphi(8) \cdot \varphi(5) = 4 \cdot 4 = \underline{16}$$

TE:

$$3^{16} \equiv 1 \pmod{40}$$

i	$3^i \bmod 40$
1	3
2	9
⋮	⋮
	$\boxed{1}$

$$3^{16k} \equiv 1 \pmod{40}$$

$$\boxed{3^{2025}} = 3^{16 \cdot (126) + 9} \equiv$$

$$\equiv \underbrace{3^{16k}}_{1} \cdot 3^9 \equiv 3^9 \equiv 3^8 \cdot 3 \equiv$$

$$\equiv (3^4)^2 \cdot 3 \equiv 1 \cdot 3 \equiv \boxed{3} \pmod{40}$$

$$\begin{array}{l} 126 \\ \hline 2025 : 16 \\ 16 \\ \hline 425 \\ 32 \\ \hline 105 \\ 96 \\ \hline \boxed{9} \end{array}$$

$$3^2 \equiv 9$$

$$3^4 = 81 \equiv 1 \pmod{40}$$

$$\boxed{3^{3^{2025}}} \equiv 3^{40\cdot(\quad)+3} = \underbrace{3^{40k}}_{1}\cdot 3^3 \equiv$$

$$\equiv 3^3 = \boxed{27} \pmod{100}.$$

$$2^{2^{2025}} \equiv ? \pmod{100}$$

$$\text{NWD}(2,100) = 2 \neq 1$$

$\boxed{\text{CTI}}$

Liniowe równania kongruencyjne

$$\boxed{\begin{aligned} 6x &= 5 \quad \big|:6 \\ x &= \frac{5}{6} \end{aligned}}$$

$$6x \equiv 5 \pmod{13} \quad \cancel{|:6} \qquad x = ? \qquad x \in \mathbb{Z}$$

$$5:8 \overset{DEF}{=} 5\cdot\boxed{8^{-1}}$$

$\|$

liczba, którą pomnożona przez 8 daje 1.

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

číslo, ktoré pomocou prenásobenia 6 dopočíta 1, v zbierke vedúcej mod 13.

$$6^{-1} = ? \pmod{13}$$

$$6 \cdot 2 = 12 \equiv -1 \pmod{13} \quad \Big| \cdot (-1)$$

$$6 \cdot 2 \cdot (-1) \equiv 1 \pmod{13}$$

$$6 \cdot \boxed{(-2)} \equiv 1 \pmod{13}$$

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

$$\downarrow$$

$$6^{-1}$$

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

$$\underbrace{(-2) \cdot 6}_{1} x \equiv -10 \pmod{13}$$

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

$$\boxed{x \equiv 3 \pmod{13}} \qquad x = 3 + 13k, \ k \in \mathbb{Z}$$

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

$6^{-1} \bmod 14$ nie istnieje

$6, 13$ ✓ $\qquad$ $6, 14$ ✗ $\quad NWD(6, 14) \neq 1$

$m, n \in \mathbb{N} \qquad m^{-1} \bmod n$?

$m^{-1} \bmod n$ istnieje wtedy i tylko wtedy, gdy $NWD(m, n) = 1$.

RAE $\Rightarrow \bigvee_{s,t \in \mathbb{Z}} \; sm + tn = 1$

$sm + tn = 1 \quad | \; (\;) \bmod n$

$sm + \underbrace{tn}_{\equiv 0} \equiv 1 \pmod{n}$

$\downarrow$

$sm \equiv 1 \pmod{n}$

$s = m^{-1}$