1. Najděte všechna $x \in \mathbb{Z}$ splňující

(a) $x \equiv 2 \pmod 3$, $x \equiv 4 \pmod 7$ a $x \equiv 3 \pmod 8$.

(b) $2x+1 \equiv 2 \pmod 3$, $3x+2 \equiv 3 \pmod 4$ a $4x+3 \equiv 2 \pmod 5$.

(c) $10x \equiv 6 \pmod{32}$ a $3x \equiv 1 \pmod 5$.

$a_1, a_2, \dots, a_k$ po 2 nesoudělné

$x \equiv b_1 \pmod{a_1}$

$\vdots$

$x \equiv b_k \pmod{a_k}$

právě 1 řešení v množině $\{0, \dots, \prod_{i=1}^{k} a_i - 1\}$

a) $x \equiv 3 \pmod 8$

$\Rightarrow x = 8k+3 = 8(7l+1)+3 =$

$= 56l + 8 + 3 =$

$= 56l + 11 = 56 \cdot 3 \cdot m + 11 =$

$= \boxed{168m + 11}$

$x \equiv 4 \pmod 7$

$8k+3 \equiv 4 \pmod 7$

$k \equiv 1 \pmod 7 \Rightarrow k = 7l+1$

$x \equiv 2 \pmod 3$

$56l + 11 \equiv 2 \pmod 3$

$2l + 2 \equiv 2 \pmod 3$

$2l \equiv 0 \pmod 3 \quad / \cdot 2$

$l \equiv 0 \pmod 3 \Rightarrow l = 3m$

---

2. **Spočítejte**

(a) $100^{99^{98}}$ mod 39.

(b) $100^{99^{98}}$ mod 40.

$a, b$ nesoudělné

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

$\varphi(p_1^{k_1} \cdots p_m^{k_m}) =$

$= (p_1 - 1) \cdot p_1^{k_1 - 1} \cdot \ldots \cdot (p_m - 1) p_m^{k_m - 1}$

a) $\varphi(39) = \varphi(3 \cdot 13) =$

$= (3-1) \cdot 3^0 \cdot (13-1) \cdot 13^0 =$

$= 2 \cdot 12 = 24$

$99^{98} = 24 \cdot k + l \qquad l \in \{0, \dots, 23\}$

$99^{98} \bmod 24 = ? \; 9$

$100^{\varphi(39)} \equiv 1 \pmod{39}$

$100^{24} \equiv 1 \pmod{39}$

$100^{(99^{98})} = 100^{24 \cdot k + l} = 100^{24k} \cdot 100^{l} =$

$= \underbrace{(100^{24})^k}_{\text{Euler}} \cdot \boxed{100^l} \equiv 100^9 \equiv 22^9 \pmod{39}$

$\overset{\text{Euler}}{=} 1^k \equiv 1 \pmod{39}$

$99^{98} \equiv 3^{98} \pmod{24}$

1) $\overset{4}{\cancel{\varphi}}$ mod 8 $\longrightarrow$ 1 $\quad \varphi(8) = \varphi(2^3) = 4$

mod 3 $\longrightarrow$ 0

$x \equiv 0 \pmod 3$

$x \equiv 1 \pmod 8$

$x = 9$

98 mod 4 = 2

$3^{98} = 3^{4 \cdot 24} \cdot 3^2 =$

$= (3^4)^{24} \cdot 3^2 \overset{\text{Euler}}{\equiv} 1^{24} \cdot 3^2 \equiv$

$\equiv 3^2 \equiv 9 \equiv 1 \pmod 8$

$22^9 \bmod 39$

$\bmod 3: \ 1$

$\bmod 13: \ 22^9 \equiv 9^9 \equiv (3^2)^9 \equiv 3^{18} \equiv (3^3)^6 \equiv 27^6 \equiv 1^6 \equiv 1 \pmod{13}$

$x \equiv 1 \pmod 3$, $x \equiv 1 \pmod{13}$ $\xrightarrow{?}$ mod 39 ? $\rightsquigarrow$ $\boxed{22^9 \bmod 39 = 1}$

2) $3^{98} \bmod 24 \equiv 9 \pmod{24}$

$3^1 \equiv \boxed{3} \pmod{24}$
$3^2 \equiv 9 \pmod{24}$
$3^3 \equiv 27 \equiv \boxed{3} \pmod{24}$
$3^4 \equiv 9 \pmod{24}$

$\Rightarrow$ $3 \equiv 3^{2k+1} \pmod{24}$, $9 \equiv 3^{2k} \pmod{24}$

---

b) $100^{99^{98}} \equiv 20^{99^{98}} \equiv (20 \cdot 20) \cdot 20^{(99^{98}-2)} \equiv$

$400 \equiv 0 \pmod{40}$

$\equiv 0 \pmod{40}$

MŮŽE SE HODIT:

$25^{53} \bmod 26 = (-1)^{53} \equiv -1 \equiv 25 \pmod{26}$

---

5. **Spočítejte**

(a) $3^{3^{3^{3^{3^3}}}}$ mod 28.

(b) $3^{5^{7^{9^{11^{13}}}}}$ mod 28.

b) 3, 28 nesoudělné; $\varphi(28) = 12$

$\Rightarrow$ Chceme $5^{7^{9^{11^{13}}}} \bmod 12$ *

5, 12 nesoudělné; $\varphi(12) = 4$

$\Rightarrow$ chceme $7^{9^{11^{13}}} \bmod 4$

$7^{9^{11^{13}}} \equiv (-1)^{9^{11^{13}}} \equiv 3 \pmod 4$

* $5^{7^{9^{11^{13}}}} \equiv 5^{4k+3} \equiv \underbrace{(5^4)^k}_{\equiv 1 \pmod{12}} \cdot 5^3 \equiv 5^3 \equiv 5 \pmod{12}$

Euler

* $3^{5^{7^{9^{11^{13}}}}} \equiv 3^{12\ell+5} \equiv \underbrace{(3^{12})^\ell}_{\equiv 1 \pmod{28}} \cdot 3^5 \equiv 3^5 \equiv \boxed{19} \pmod{28}$

Euler

3. Najděte všechna $x \in \mathbb{Z}$ splňující

(a) $x^2 \equiv 1 \pmod 3$ a $x^2 \equiv 1 \pmod 7$.

(b) $x^2 \equiv -1 \pmod{65}$.

a) $x^2 \equiv 1 \pmod 3 \Rightarrow 3 \mid (x^2-1) = (x-1)(x+1)$

$\xRightarrow{3 \text{ je prvočíslo}}$ $3 \mid (x-1)$ nebo $3 \mid (x+1)$

$\Downarrow$ $x = 3k+1$ $\qquad$ $\Downarrow$ $x = 3k-1$

$\boxed{x \equiv 1 \pmod 3 \text{ NEBO } x \equiv 2 \pmod 3}$

$x^2 \equiv 1 \pmod 7$

$\Downarrow$ ... stejný argument

$x = 7l+1$ nebo $x = 7l-1$

$\boxed{x \equiv 1 \pmod 7 \text{ NEBO } x \equiv 6 \pmod 7}$

$\rightarrow$ celkem 4 možnosti:

(i) $x \equiv 1 \pmod 3$ & $x \equiv 1 \pmod 7$

(ii) $x \equiv 1 \pmod 3$ & $x \equiv 6 \pmod 7$

(iii) $x \equiv 2 \pmod 3$ & $x \equiv 1 \pmod 7$

(iv) $x \equiv 2 \pmod 3$ & $x \equiv 6 \pmod 7$

$\hookrightarrow$ každou možnost zvlášť, použít např. Čínskou zbytk. větu

b) $x^2 \equiv -1 \equiv 64 \pmod{65}$ $\qquad$ $65 = 5 \cdot 13$

$65 \mid (x^2 - 64) = (x-8)(x+8)$

- $5 \mid (x-8)$ NEBO $5 \mid (x+8)$
- $13 \mid (x-8)$ NEBO $13 \mid (x+8)$

$\hookrightarrow$ postupovat jako v a)