Poznámka: Redukcí čísla $n \in \mathbb{Z}$ modulo m budeme rozumět nalezení čísla $x \in \{0, 1, 2, \dots, m-1\}$ takového, že

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

Př. 1: Redukujte n modulo m

a) $n = 32$, $m = 7$

$$\Rightarrow \quad 32 \equiv \underbrace{28}_{0} + 4 \equiv \underline{\underline{4 \pmod 7}}$$

b) $n = -35$, $m = 6$

$$-35 \equiv -35 + 36 \equiv \underline{\underline{1 \pmod 6}}$$

Př. 2: Redukujte:

a) $\underbrace{108 + 2534 + 3976 + 321\,539}_{\equiv} \pmod 4$

$$0 + 34 + 76 + 39 \pmod 4$$

$$\equiv \quad 2 - 4 + 3 \pmod 4$$

$$\equiv \quad 1 \pmod 4$$

b) $1486 \cdot 2356 \cdot 63704 \cdot 186\,474 \pmod 9 \equiv$

($1486 \equiv 500$, $2356 \equiv -1800$, $63704 \equiv -63\,000$, $186\,474 \equiv -180\,000$)

$\equiv 586 \cdot 556 \cdot 704 \cdot 6\,474 \equiv 46 \cdot 16 \cdot 74 \cdot 174 \equiv 1 \cdot 7 \cdot 2 \cdot (-6) \equiv -30 \equiv \underline{\underline{6 \pmod 9}}$

($586 \equiv -540$, $556 \equiv -540$, $704 \equiv -630$, $6\,474 \equiv -6\,300$; $46 \equiv -45$, $16 \equiv -9$, $74 \equiv -72$, $174 \equiv -180$; $7 \cdot 2 = 14 \equiv 5$; $-30 \equiv +36$)

c) $(231 + 458)^{53} \pmod{19}$

$x \equiv (231 + 458)^{53} \equiv (41 + 78)^{53} \equiv (3 + 2)^{53} \equiv 5^{53} \pmod{19}$

($231 \equiv -190$, $458 \equiv -380$, $78 = 4 \cdot 19 + 2$)

$x \equiv 5^{53} \equiv 5^{32} \cdot 5^{16} \cdot 5^{4} \cdot 5 \equiv 9 \cdot (+3) \cdot (+2) \cdot 5 \equiv -1 \cdot (-4) \equiv 4 \pmod{19}$

$5 \equiv 5 \pmod{19}$
$5^2 \equiv 25 \equiv 6 \pmod{19}$
$5^4 \equiv 6^2 \equiv 36 \equiv -2 \pmod{19}$
$5^8 \equiv (-2)^2 \equiv 4 \pmod{19}$
$5^{16} \equiv 4^2 \equiv 16 \equiv -3 \pmod{19}$
$5^{32} \equiv 3^2 \equiv 9 \pmod{19}$

Př. Ukažte, že $63! \equiv 61! \pmod{71}$

$$63 \cdot 62 \equiv X \pmod{71}$$

$$X \equiv 3 \cdot 3 \cdot 7 \cdot 2 \cdot 31 \pmod{71}$$
$$X \equiv \underbrace{93}_{22} \cdot 3 \cdot 7 \cdot 2 \pmod{71}$$
$$X \equiv \underbrace{22}_{66} \cdot 3 \cdot 7 \cdot 2 \pmod{71}$$
$$X \equiv -5 \cdot 7 \cdot 2 \pmod{71}$$
$$X \equiv -70 \pmod{71}$$
$$X \equiv 1 \pmod{71} \quad \Rightarrow \quad 63 \cdot 62 \equiv 1 \pmod{71}$$

$$\Rightarrow 63! \equiv \underbrace{63 \cdot 62}_{1} \cdot 61! \equiv 61! \pmod{71}$$

Př. Redukujte 10^n pro všechna $n \in \mathbb{N} \cup \{0\}$ modulo 4.

$10^0 \equiv 1 \pmod 4$
$10^1 \equiv 2 \pmod 4$
$10^2 \equiv 0 \pmod 4$
$\vdots \quad \vdots$
$10^n \equiv 0 \pmod 4$ pro všechna $n \in \mathbb{N}$, $n \geq 2$

Př. Nalezněte kriteriium dělitelnosti čísla d, jehož cifernýn zápisem v 10-kové soustavě je $d = d_n d_{n-1} \dots d_0$

a) modulo 4:

$$d = d_n \cdot 10^n + d_{n-1} 10^{n-1} + \dots + d_1 \cdot 10 + d_0$$

$$4 \mid d \iff d \equiv 0 \pmod 4 \iff \underbrace{d_n \cdot 10^n}_{0} + \underbrace{d_{n-1} 10^{n-1}}_{0} + \dots + \underbrace{d_1 \cdot 10}_{2} + d_0 \equiv 0 \pmod 4 \iff$$

$$\iff \boxed{2 \cdot d_1 + d_0 \equiv 0 \pmod 4}$$

b) modulo 3:

$10^0 \equiv 1 \pmod 3$

$10^1 \equiv 1 \pmod 3$

$10^2 \equiv (1)^2 \equiv 1 \pmod 3$

$\vdots$

$10^n \equiv 1 \pmod 3 \quad \forall n \in \mathbb{N} \cup \{0\}$

$\Rightarrow \quad 3 \mid d \iff d \equiv 0 \pmod 3 \iff d_n \underbrace{10^n}_{1} + d_{n-1} \underbrace{10^{n-1}}_{1} + \dots + d_1 \underbrace{10^1}_{1} + \underbrace{d_0}_{1} \equiv 0 \pmod 3 \iff$

$$\boxed{3 \mid d \iff d_n + d_{n-1} + \dots + d_0 \equiv 0 \pmod 3}$$

c) modulo 9:

$10^0 \equiv 1 \pmod 9$

$10^1 \equiv 1 \pmod 9$

$10^2 \equiv 1 \pmod 9$

$\vdots$

$10^n \equiv 1 \pmod 9 \quad \forall n \in \mathbb{N} \cup \{0\}$

$\Rightarrow$ $$\boxed{9 \mid d \iff \sum_{i=0}^{n} d_i \equiv 0 \pmod 9}$$

d) modulo 11:

$10^0 \equiv 1 \pmod{11}$

$10^1 \equiv -1 \pmod{11}$

$10^2 \equiv 1 \pmod{11}$

$\vdots$

$10^n \equiv \begin{cases} 1 \pmod{11} & \forall n \in \mathbb{N} \cup \{0\},\ n \text{ sudé} \\ -1 \pmod{11} & \forall n \in \mathbb{N} \cup \{0\},\ n \text{ liché} \end{cases}$

$\Rightarrow$ $$\boxed{11 \mid d \iff \sum_{i=0}^{n} d_i (-1)^i \equiv 0 \pmod{11}}$$

Př: Redukujte

$d = d_n 10^n + \dots d_1 \cdot 10 + d_0 \Rightarrow$

1.) $X \equiv 1328 + 431 + 329 \equiv X \pmod 3$ / $d \equiv \sum_{i=0}^{n} d_i \pmod 3$

$X \equiv 14 + 8 + 14 \equiv X \pmod 3$

$X \equiv 5 + 8 + 5 \equiv X \pmod 3$

$X \equiv 18 \equiv X \pmod 3$

$X \equiv 9 \equiv X \pmod 3$

$X \equiv 0 \pmod 3$

2.) $(328 - 521 \cdot 356)\, 6\,531\,821 \equiv X \pmod{11}$

3-2+8 5-2+1 3-5+6 6-5+3-1+8-2+1

$(9 - 4 \cdot 4) \cdot 10 \equiv X \pmod{11}$

$-70 \equiv X \pmod{11}$

7+0

$7 \equiv X \pmod{11}$

Př.: Nalezněte kritéria dělitelnosti čísel d modulo m, jestliže jsou čísla d zapsána v sedmičkové soustavě. Tzn.

$$d = d_n \cdot 7^n + d_{n-1} 7^{n-1} + \dots + d_1 \cdot 7 + d_0$$

a) $m = 4 \Rightarrow$

$7^0 \equiv 1 \pmod 4$

$7^1 \equiv 3 \pmod 4$

$7^2 \equiv 3^2 \equiv 1 \pmod 4$

$7^3 \equiv 3 \pmod 4$

$7^4 \equiv 1 \pmod 4$

$\vdots$

$7^n \equiv \begin{cases} 1 \pmod 4 & \Leftrightarrow n \in \mathbb{N} \cup \{0\},\ n \text{ je sudé} \\ 3 \pmod 4 & \Leftrightarrow n \in \mathbb{N} \cup \{0\},\ n \text{ je liché} \end{cases}$

$$\Rightarrow \boxed{4 \mid d \Leftrightarrow d \equiv 0 \pmod 4 \Leftrightarrow \sum_{m=0}^{n} d_m \left(2 + (-1)^{m+1}\right) \equiv 0 \pmod 4}$$

b) $m = 3 \Rightarrow$

$7^0 \equiv 1 \pmod 3$

$7^1 \equiv 1 \pmod 3$

$7^2 \equiv 1^2 \equiv 1 \pmod 3$

$\vdots$

$7^n \equiv 1 \pmod 3 \quad \forall n \in \mathbb{N} \cup \{0\}$

$$\Rightarrow \boxed{3 \mid d \Leftrightarrow d \equiv 0 \pmod 3 \Leftrightarrow \sum_{i=0}^{n} d_i \equiv 0 \pmod 3}$$