# Kongruence a aritmetické funkce

### Řešené příklady

*Příklad.* Určete, zda jsou čísla $a$, $b$ kongruentní podle modulu $m$:

1. $a = 5, b = 15, m = 4$
2. $a = 3, b = 1, m = 2$
3. $a = 7, b = 25, m = 3$
4. $a = 7, b = 25, m = 4$

*Řešení.* 1.

$$\begin{aligned} 5 - 15 &= -10 \\ 4 &\nmid -10 \\ 5 &\not\equiv 15 \pmod 4 \end{aligned}$$

2.

$$\begin{aligned} 3 &= 1 \cdot 2 && +1 \\ 1 &= 0 \cdot 2 && +1 \\ 3 &\equiv 1 && \pmod 2 \end{aligned}$$

3.

$$\begin{aligned} 7 - 25 &= -12 \\ 3 &\mid -12 \\ 7 &\equiv 25 \pmod 3 \end{aligned}$$

4.

$$\begin{aligned} 7 &= 1 \cdot 4 && +3 \\ 25 &= 6 \cdot 4 && +1 \\ 7 &\not\equiv 25 && \pmod 6 \end{aligned}$$

□

*Příklad.* Udejte příklad aritmetické funkce.

*Řešení.* Například funkce $\tau(a)$, $\sigma(a)$. □

*Příklad.* Určete $\mu(72)$.

*Řešení.* $72 = 2^3 \cdot 3^2$
$\mu(72) = 0$ □

*Příklad.* Určete, zda je Möbiova funkce multiplikativní. Zdůvodněte.

*Řešení.* Funkce je multiplikativní, pokud je aritmetická a pro všechna nesoudělná čísla $a, b$ splňuje rovnost $f(a \cdot b) = f(a) \cdot f(b)$.
Möbiova funkce je definovaná na množině přirozených čísel, je tedy aritmetická. Zbývá dokázat, že je funkcí multiplikativní.
Nechť $a = p_1^{k_1} \cdot p_2^{k_2} \cdot \cdots \cdot p_n^{k_n}$, $b = p_1^{l_1} \cdot p_2^{l_2} \cdot \cdots \cdot p_n^{l_n}$, kde $p_i$ je prvočíslo, $k_i, l_i \in \mathbb{N}_0$, $k_i + l_i \geq 1$, $i \in \{1, 2, \ldots, n\}$, $n$ je největší přirozené číslo takové, že $k_n > 0 \vee l_n > 0$.

$$a \cdot b = p_1^{k_1+l_1} \cdot p_2^{k_2+l_2} \cdot \cdots \cdot p_n^{k_n+l_n}$$

1. $\exists i \in \{1, 2, \ldots, n\} : k_i > 1 \vee l_i > 1 \Rightarrow \mu(a) = 0 \vee \mu(b) = 0 \Rightarrow \mu(a) \cdot \mu(b) = 0 = \mu(a \cdot b)$
2. $\forall i \in \{1, 2, \ldots, n\} : k_i \leq 1 \wedge l_i \leq 1$. Protože čísla $a$, $b$ jsou ze zadání multiplikativní funkce nesoudělná, platí také $(k_i = 0 \wedge l_i = 1) \vee (k_i = 1 \wedge l_i = 0)$. Označme $k$ počet prvočísel, pro která platí $k_i = 1$, $l$ počet prvočísel, pro která platí $l_i = 1$. Platí tedy: $\mu(a \cdot b) = (-1)^{k+l} = (-1)^k \cdot (-1)^l = \mu(a) \cdot \mu(b)$.

Möbiova funkce tedy je funkcí multiplikativní. □

*Příklad.* Určete $\varphi(10)$ podle definice.

*Řešení.*

$$\varphi(10) = |\{a \in \mathbb{N} | 0 < a \leq 10, (a, 10) = 1\}| = |\{1, 3, 7, 9\}| = 4$$

□

*Příklad.* Určete $\varphi(1377)$.

*Řešení.* $1377 = 3^4 \cdot 17$
$\varphi(1377) = \varphi(3^4) \cdot \varphi(17) = (3 - 1) \cdot 3^3 \cdot (17 - 1) = 864$ □

*Příklad.* Dokažte, že pro všechna přirozená čísla $m, k$ platí:
$\varphi(m^k) = m^{k-1} \cdot \varphi(m)$.

*Řešení.* Označme $m = p_1^{k_1} \cdot p_2^{k_2} \cdot \cdots \cdot p_n^{k_n}$.
$\varphi(m^k) = \varphi((p_1^{k_1} \cdot p_2^{k_2} \cdot \cdots \cdot p_n^{k_n})^k) = \varphi(p_1^{k \cdot k_1} \cdot p_2^{k \cdot k_2} \cdot \cdots \cdot p_n^{k \cdot k_n}) = \varphi(p_1^{k \cdot k_1}) \cdot \varphi(p_2^{k \cdot k_2}) \cdot \cdots \cdot \varphi(p_n^{k \cdot k_n}) =$
$= p_1^{k \cdot k_1 - 1} \cdot \varphi(p_1) \cdot p_2^{k \cdot k_2 - 1} \cdot \varphi(p_2) \cdot \cdots \cdot p_n^{k \cdot k_n - 1} \cdot \varphi(p_n) =$
$= (p_1^{k_1})^{k-1} \cdot p_1^{k_1 - 1} \cdot \varphi(p_1) \cdot (p_2^{k_2})^{k-1} \cdot p_2^{k_2 - 1} \cdot \varphi(p_2) \cdot \cdots \cdot (p_n^{k_n})^{k-1} \cdot p_n^{k_n - 1} \cdot \varphi(p_n) =$
$= (p_1^{k_1} \cdot p_2^{k_2} \cdot \cdots \cdot p_n^{k_n})^{k-1} \cdot \varphi(p_1^{k_1}) \cdot \varphi(p_2^{k_2}) \cdot \cdots \cdot \varphi(p_n^{k_n}) = m^{k-1} \cdot \varphi(m)$ □

*Příklad.* Určete řád čísla 7 modulo 15.

*Řešení.* Řád čísla $a$ modulo $m$ je nejmenší takové číslo, pro nějž platí $a^r \equiv 1 \pmod{m}$. Také víme, že řád $r$ dělí $\varphi(m)$. Protože $\varphi(15) = 2 \cdot 4 = 8$, stačí ověřit čísla 1, 2, 4 a 8.
$7^1 \equiv 7 \pmod{15}$
$7^2 \equiv 49 \equiv 4 \pmod{15}$
$7^4 \equiv (7^2)^2 \equiv 4^2 \equiv 16 \equiv 1 \pmod{15}$.
Řád čísla 7 modulo 15 je roven 4. □

*Příklad.* Určete poslední číslici dekadického zápisu čísla $3^{123456}$.

*Řešení.* Určení poslední číslice dekadického zápisu je ekvivalentí otázce, jaký zbytek dává zadané číslo po dělení deseti, a tedy i kongruenci modulo deset. Řešíme tedy kongruenci $3^{123456} \equiv? \pmod{10}$.
$\varphi(10) = \varphi(2)\varphi(5) = 1 \cdot 4 = 4$
Z Eulerovy věty víme, že platí $3^4 \equiv 1 \pmod{10}$.
Protože $123456 : 4 = 30864$, můžeme zadanou kongruenci snadno vyřešit:
$3^{123456} \equiv (3^4)^{30864} \equiv 1^{30864} \equiv 1 \pmod{10}$. □

*Příklad.* Určete poslední číslici dekadického zápisu čísla $17^{15^{13^{11}}}$.

*Řešení.* Řešíme kongruenci $17^{15^{13^{11}}} \equiv? \pmod{10}$. Využijeme vlastnosti řádu $r$ čísla $a$, pro který platí:
$a^m \equiv a^n \pmod{m} \Leftrightarrow m \equiv n \pmod{r}$
V našem případě je $a = 17 \equiv 7 \pmod{10}$, hledáme tedy řád čísla 7 modulo 10.
$\varphi(10) = 4 \Rightarrow r \in \{1, 2, 4\}$
$7^1 \equiv 7 \pmod{10}$
$7^2 \equiv 9 \equiv -1 \pmod{10}$
$7^4 \equiv (7^2)^2 \equiv (-1)^2 \equiv 1 \pmod{10} \Rightarrow r = 4$.
$17^{15^{13^{11}}} \equiv 7^{15^{13^{11}}} \equiv 7^x \pmod{10} \Leftrightarrow 15^{13^{11}} \equiv x \pmod{4}$.
$15^{13^{11}} \equiv (-1)^{13^{11}} \pmod{4} \wedge$ řád čísla -1 modulo 4 je roven číslu 2 $\Rightarrow$
$\Rightarrow (-1)^{13^{11}} \equiv x \equiv (-1)^y \pmod{4} \Leftrightarrow 13^{11} \equiv y \pmod{2} \Rightarrow y \equiv 1 \pmod{2} \Rightarrow$
$\Rightarrow x \equiv -1 \equiv 3 \pmod{4} \Rightarrow 7^x \equiv 7^3 \equiv 3 \pmod{10} \Rightarrow 17^{15^{13^{11}}} \equiv 3 \pmod{10}$
Poslední číslicí čísla $17^{15^{13^{11}}}$ je číslice 3. □

*Příklad.* Kolik $m \in \mathbb{N} : 10^6 < m < 10^7$ je dělitelných 786?

*Řešení.* $m \in \{k \cdot 786, (k+1) \cdot 786, \ldots, (k+l) \cdot 786 : k \cdot m > 10^6 \wedge (k+l) \cdot 786 < 10^7\}$
počet: $[(x < 10^7) - (x < 10^6)]$
$\underline{\left[\frac{10^7-1}{786}\right] - \left[\frac{10^6}{786}\right]}$ □

*Příklad.* Určete počet $n \in \mathbb{N} : n < 100 \wedge (n, 36) = 1$.

*Řešení.* $36 = 2^2 \cdot 3^2$
počet čísel dělitelných 2... $\left[\frac{99}{2}\right] = 49$
počet čísel dělitelných 3... $\left[\frac{99}{3}\right] = 33$
počet čísel dělitelných 6... $\left[\frac{99}{6}\right] = 16$
$99 - (49 + 33) + 16 = \underline{33}$ □