

### 3. Kongruence

Pojem kongruence byl zaveden Gaussem. Ačkoliv je to pojem velice jednoduchý, jeho důležitost a užitečnost v teorii čísel je nedocenitelná; projevuje se zejména ve stručných a přehledných zápisech některých i velmi komplikovaných úvah.

DEFINICE. Jestliže dvě celá čísla  $a, b$  mají při dělení přirozeným číslem  $m$  týž zbytek  $r$ , kde  $0 \leq r < m$ , nazývají se  $a, b$  *kongruentní modulo  $m$*  (též *kongruentní podle modulu  $m$* ), což zapisujeme takto:

$$a \equiv b \pmod{m}.$$

V opačném případě řekneme, že  $a, b$  nejsou kongruentní modulo  $m$ , a píšeme

$$a \not\equiv b \pmod{m}.$$

LEMMA. Pro libovolná  $a, b \in \mathbb{Z}$ ,  $m \in \mathbb{N}$  jsou následující podmínky ekvivalentní:

- (1)  $a \equiv b \pmod{m}$ ,
- (2)  $a = b + mt$  pro vhodné  $t \in \mathbb{Z}$ ,
- (3)  $m \mid a - b$ .

DŮKAZ. „(1) $\Rightarrow$ (3)“ Jestliže  $a = q_1m + r$ ,  $b = q_2m + r$ , pak  $a - b = (q_1 - q_2)m$ .

„(3) $\Rightarrow$ (2)“ Jestliže  $m \mid a - b$ , pak existuje  $t \in \mathbb{Z}$  tak, že  $m \cdot t = a - b$ , tj.  $a = b + mt$ .

„(2) $\Rightarrow$ (1)“ Jestliže  $a = b + mt$ , pak z vyjádření  $b = mq + r$  plyne  $a = m(q + t) + r$ , tedy  $a$  i  $b$  mají při dělení číslem  $m$  týž zbytek  $r$ , tj.  $a \equiv b \pmod{m}$ .  $\square$

**3.1. Základní vlastnosti kongruencí.** Přímo z definice plyne, že kongruence podle modulu  $m$  je reflexivní (tj.  $a \equiv a \pmod{m}$ ) platí pro každé  $a \in \mathbb{Z}$ ), symetrická (tj. pro každé  $a, b \in \mathbb{Z}$  z  $a \equiv b \pmod{m}$  plyne  $b \equiv a \pmod{m}$ ) a tranzitivní (tj. pro každé  $a, b, c \in \mathbb{Z}$  z  $a \equiv b \pmod{m}$  a  $b \equiv c \pmod{m}$  plyne  $a \equiv c \pmod{m}$ ) relace, jde tedy o *ekvivalenci*. Dokážeme nyní další vlastnosti:

VĚTA 12. (*Základní vlastnosti kongruencí*)

- (1) **Kongruence podle téhož modulu můžeme sčítat.** Libovolný sčítanec můžeme přenést s opačným znaménkem z jedné strany kongruence na druhou. **Na libovolnou stranu kongruence můžeme přičíst jakýkoliv násobek modulu.**

DŮKAZ. Je-li  $a_1 \equiv b_1 \pmod{m}$  a  $a_2 \equiv b_2 \pmod{m}$ , existují podle lemmatu  $t_1, t_2 \in \mathbb{Z}$  tak, že  $a_1 = b_1 + mt_1$ ,  $a_2 = b_2 + mt_2$ . Pak ovšem  $a_1 + a_2 = b_1 + b_2 + m(t_1 + t_2)$  a opět podle lemmatu  $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$ . Sečteme-li kongruenci  $a + b \equiv c \pmod{m}$  s kongruencí  $-b \equiv -b \pmod{m}$ , která zřejmě platí, dostaneme  $a \equiv c - b \pmod{m}$ . Sečteme-li

kongruenci  $a \equiv b \pmod{m}$  s kongruencí  $mk \equiv 0 \pmod{m}$ , jejíž platnost je zřejmá, dostaneme  $a + mk \equiv b \pmod{m}$ .  $\square$

- (2) **Kongruence podle téhož modulu můžeme násobit.** Obě strany kongruence je možné **umocnit na totéž přirozené číslo**. Obě strany kongruence je možné **vynásobit stejným celým číslem**.

DŮKAZ. Je-li  $a_1 \equiv b_1 \pmod{m}$  a  $a_2 \equiv b_2 \pmod{m}$ , existují podle  $t_1, t_2 \in \mathbb{Z}$  tak, že  $a_1 = b_1 + mt_1$ ,  $a_2 = b_2 + mt_2$ . Pak ovšem

$$a_1 a_2 = (b_1 + mt_1)(b_2 + mt_2) = b_1 b_2 + m(t_1 b_2 + b_1 t_2 + mt_1 t_2),$$

odkud podle dostáváme  $a_1 a_2 \equiv b_1 b_2 \pmod{m}$ .

Je-li  $a \equiv b \pmod{m}$ , dokážeme indukcí vzhledem k přirozenému číslu  $n$ , že platí  $a^n \equiv b^n \pmod{m}$ . Pro  $n = 1$  není co dokazovat. Platí-li  $a^n \equiv b^n \pmod{m}$  pro nějaké pevně zvolené  $n$ , vynásobením této kongruence a kongruence  $a \equiv b \pmod{m}$  dostáváme  $a^n \cdot a \equiv b^n \cdot b \pmod{m}$ , tedy  $a^{n+1} \equiv b^{n+1} \pmod{m}$ , což je tvrzení pro  $n + 1$ . Důkaz indukcí je hotov.

Jestliže vynásobíme kongruenci  $a \equiv b \pmod{m}$  a kongruenci  $c \equiv c \pmod{m}$ , dostaneme  $ac \equiv bc \pmod{m}$ .  $\square$

- (3) **Obě strany kongruence můžeme vydělit jejich společným dělitelem**, jestliže je tento dělitel **nesoudělný s modulem**.

DŮKAZ. Předpokládejme, že  $a \equiv b \pmod{m}$ ,  $a = a_1 \cdot d$ ,  $b = b_1 \cdot d$  a  $(m, d) = 1$ . Podle lemmatu je rozdíl  $a - b = (a_1 - b_1) \cdot d$  dělitelný číslem  $m$ . Protože  $(m, d) = 1$ , je podle věty 5 číslo  $a_1 - b_1$  také dělitelné číslem  $m$ , odtud podle lemmatu plyne  $a_1 \equiv b_1 \pmod{m}$ .  $\square$

- (4) **Obě strany kongruence i její modul můžeme současně vynásobit tímtož přirozeným číslem**.

DŮKAZ. Je-li  $a \equiv b \pmod{m}$ , existuje podle lemmatu celé číslo  $t$  tak, že  $a = b + mt$ , odkud pro  $c \in \mathbb{N}$  platí  $ac = bc + mc \cdot t$ , odkud opět podle lemmatu plyne  $ac \equiv bc \pmod{mc}$ .  $\square$

- (5) **Obě strany kongruence i její modul můžeme vydělit jejich společným kladným dělitelem**.

DŮKAZ. Předpokládejme, že  $a \equiv b \pmod{m}$ ,  $a = a_1 \cdot d$ ,  $b = b_1 \cdot d$ ,  $m = m_1 \cdot d$ , kde  $d \in \mathbb{N}$ . Podle lemmatu existuje  $t \in \mathbb{Z}$  tak, že  $a = b + mt$ , tj.  $a_1 \cdot d = b_1 \cdot d + m_1 dt$ , odkud  $a_1 = b_1 + m_1 t$ , což podle lemmatu znamená, že  $a_1 \equiv b_1 \pmod{m_1}$ .  $\square$

- (6) **Jestliže kongruence  $a \equiv b$  platí podle různých modulů  $m_1, \dots, m_k$ , platí i podle modulu, kterým je nejmenší společný násobek  $[m_1, \dots, m_k]$  těchto čísel.**

DŮKAZ. Jestliže  $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \dots, a \equiv b \pmod{m_k}$ , podle lemmatu je rozdíl  $a - b$  společný násobek čísel  $m_1, m_2, \dots, m_k$  a tedy je dělitelný jejich nejmenším společným násobkem  $[m_1, m_2, \dots, m_k]$ , odkud plyne  $a \equiv b \pmod{[m_1, \dots, m_k]}$ .  $\square$

- (7) **Jestliže kongruence platí podle modulu  $m$ , platí podle libovolného modulu  $d$ , který je dělitelem čísla  $m$ .**

DŮKAZ. Jestliže  $a \equiv b \pmod{m}$ , je  $a - b$  dělitelné  $m$ , a proto také dělitelem  $d$  čísla  $m$ , odkud  $a \equiv b \pmod{d}$ .  $\square$

- (8) **Jestliže je jedna strana kongruence  $a$  modul dělitelný nějakým celým číslem, musí být tímto číslem dělitelná i druhá strana kongruence.**

DŮKAZ. Předpokládejme, že  $a \equiv b \pmod{m}$ ,  $b = b_1d$ ,  $m = m_1d$ . Pak podle lemmatu existuje  $t \in \mathbb{Z}$  tak, že  $a = b + mt = b_1d + m_1dt = (b_1 + m_1t)d$ , a tedy  $d \mid a$ .  $\square$

POZNÁMKA. Některé vlastnosti kongruencí jsme již používali, aniž bychom si toho povšimli – například příklad ze strany 7 lze přeformulovat do tvaru „jestliže  $a \equiv 1 \pmod{m}$ ,  $b \equiv 1 \pmod{m}$ , pak také  $ab \equiv 1 \pmod{m}$ “, což je speciální případ tvrzení věty 12 (2). Nejde o náhodu. Libovolné tvrzení používající kongruence můžeme snadno přepsat pomocí dělitelnosti. Užitečnost kongruencí tedy netkví v tom, že bychom pomocí nich mohli řešit úlohy, které bez nich řešit nejsme schopni, ale v tom, že jde o velmi vhodný způsob zápisu. Osvojíme-li si ho, výrazně tím zjednodušíme jak vyjadřování, tak i některé úvahy. Je to typický jev: v matematice hraje vhodná symbolika velmi závažnou úlohu.

PŘÍKLAD. Nalezněte zbytek po dělení čísla  $5^{20}$  číslem 26.

ŘEŠENÍ. Protože  $5^2 = 25 \equiv -1 \pmod{26}$ , platí podle věty 12 (2)

$$5^{20} \equiv (-1)^{10} = 1 \pmod{26},$$

a tedy zbytek po dělení čísla  $5^{20}$  číslem 26 je jedna.  $\square$

PŘÍKLAD. Dokažte, že pro libovolné  $n \in \mathbb{N}$  je  $37^{n+2} + 16^{n+1} + 23^n$  dělitelné sedmi.

ŘEŠENÍ. Platí  $37 \equiv 16 \equiv 23 \equiv 2 \pmod{7}$ , a tedy podle 12 (2) a (1) platí

$$37^{n+2} + 16^{n+1} + 23^n \equiv 2^{n+2} + 2^{n+1} + 2^n = 2^n(4+2+1) = 2^n \cdot 7 \equiv 0 \pmod{7},$$

což jsme chtěli dokázat.  $\square$

**PŘÍKLAD.** Dokažte, že číslo  $n = (835^5 + 6)^{18} - 1$  je dělitelné číslem 112.

**ŘEŠENÍ.** Rozložíme  $112 = 7 \cdot 16$ . Protože  $(7, 16) = 1$ , stačí ukázat, že  $7 \mid n$  a  $16 \mid n$ . Platí  $835 \equiv 2 \pmod{7}$ , a tedy podle 12  
 $n \equiv (2^5 + 6)^{18} - 1 = 38^{18} - 1 \equiv 3^{18} - 1 = 27^6 - 1 \equiv (-1)^6 - 1 = 0 \pmod{7}$ ,  
 proto  $7 \mid n$ . Podobně  $835 \equiv 3 \pmod{16}$ , a tedy

$$\begin{aligned} n &\equiv (3^5 + 6)^{18} - 1 = (3 \cdot 81 + 6)^{18} - 1 \equiv (3 \cdot 1 + 6)^{18} - 1 = \\ &= 9^{18} - 1 = 81^9 - 1 \equiv 1^9 - 1 = 0 \pmod{16}, \end{aligned}$$

proto  $16 \mid n$ . Celkem tedy  $112 \mid n$ , což jsme měli dokázat.  $\square$

**PŘÍKLAD.** Dokažte, že pro libovolné prvočíslo  $p$  a libovolná  $a, b \in \mathbb{Z}$  platí

$$a^p + b^p \equiv (a + b)^p \pmod{p}.$$

**ŘEŠENÍ.** Podle binomické věty platí

$$(a + b)^p = a^p + \binom{p}{1} a^{p-1} b + \binom{p}{2} a^{p-2} b^2 + \dots + \binom{p}{p-1} a b^{p-1} + b^p.$$

Podle příkladu za větou 6 pro libovolné  $k \in \{1, \dots, p-1\}$  platí  $\binom{p}{k} \equiv 0 \pmod{p}$ , odkud plyne tvrzení.  $\square$

Následující tvrzení je další užitečnou vlastností kongruencí:

**LEMMA.** Dokažte, že pro libovolné přirozené číslo  $m$  a libovolná  $a, b \in \mathbb{Z}$  taková, že  $a \equiv b \pmod{m^n}$ , kde  $n \in \mathbb{N}$ , platí, že  $a^m \equiv b^m \pmod{m^{n+1}}$ .

**DŮKAZ.** Platí

$$a^m - b^m = (a - b)(a^{m-1} + a^{m-2}b + \dots + ab^{m-2} + b^{m-1}) \quad (12)$$

a protože  $m \mid m^n$ , tak podle 12 (7) platí i  $a \equiv b \pmod{m}$ . Jsou tedy všechny sčítance ve druhé závorce v (12) kongruentní s  $a^{m-1}$  modulo  $m$ , a tedy

$$a^{m-1} + a^{m-2}b + \dots + ab^{m-2} + b^{m-1} \equiv m \cdot a^{m-1} \equiv 0 \pmod{m},$$

proto je  $a^{m-1} + a^{m-2}b + \dots + ab^{m-2} + b^{m-1}$  dělitelné  $m$ . Z  $a \equiv b \pmod{m^n}$  plyne, že  $m^n$  dělí  $a - b$ , a tedy  $m^{n+1}$  dělí jejich součin, což vzhledem k (12) vede k závěru, že  $a^m \equiv b^m \pmod{m^{n+1}}$ .  $\square$

**3.2. Aritmetické funkce.** Aritmetickou funkcí zde rozumíme funkci, jejímž definičním oborem je množina přirozených čísel.

**DEFINICE.** Rozložíme přirozené číslo  $n$  na prvočísla:  $n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$ . Hodnotu Möbiovy funkce  $\mu(n)$  definujeme rovnu 0, pokud pro některé  $i$  platí  $\alpha_i > 1$  a rovnu  $(-1)^k$  v opačném případě. Dále definujeme  $\mu(1) = 1$ .

**PŘÍKLAD.**  $\mu(4) = \mu(2^2) = 0$ ,  $\mu(6) = \mu(2 \cdot 3) = (-1)^2$ ,  $\mu(2) = \mu(3) = -1$ .

Dokážeme nyní několik důležitých vlastností Möbiovy funkce, zejména tzv. *Möbiovu inverzní formuli*.

LEMMA. Pro  $n \in \mathbb{N} \setminus \{1\}$  platí

$$\sum_{d|n} \mu(d) = 0.$$

DŮKAZ. Zapišeme-li  $n$  ve tvaru  $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ , pak všechny dělitele  $d$  čísla  $n$  jsou tvaru  $d = p_1^{\beta_1} \cdots p_k^{\beta_k}$ , kde  $0 \leq \beta_i \leq \alpha_i$  pro všechna  $i \in \{1, \dots, k\}$ . Proto

$$\begin{aligned} \sum_{d|n} \mu(d) &= \sum_{\substack{(\beta_1, \dots, \beta_k) \in (\mathbb{N} \cup \{0\})^k \\ 0 \leq \beta_i \leq \alpha_i}} \mu(p_1^{\beta_1} \cdots p_k^{\beta_k}) = \\ &= \sum_{(\beta_1, \dots, \beta_k) \in \{0, 1\}^k} \mu(p_1^{\beta_1} \cdots p_k^{\beta_k}) \\ &= \binom{k}{0} + \binom{k}{1} \cdot (-1) + \binom{k}{2} \cdot (-1)^2 + \cdots + \binom{k}{k} \cdot (-1)^k \\ &= (1 + (-1))^k = 0. \end{aligned}$$

□

S Möbiovou funkcí úzce souvisí pojem *Dirichletův součin*:

DEFINICE. Buďte  $f, g$  aritmetické funkce. Jejich *Dirichletův součin* je definován předpisem

$$(f \circ g)(n) = \sum_{d|n} f(d) \cdot g\left(\frac{n}{d}\right) = \sum_{d_1 d_2 = n} f(d_1) \cdot g(d_2).$$

LEMMA. *Dirichletův součin je asociativní.*

DŮKAZ.

$$((f \circ g) \circ h)(n) = \sum_{d_1 d_2 d_3 = n} f(d_1) \cdot g(d_2) \cdot h(d_3) = (f \circ (g \circ h))(n)$$

□

PŘÍKLAD. Definujme dvě pomocné funkce  $\mathbb{I}$  a  $I$  předpisem  $\mathbb{I}(1) = 1$ ,  $\mathbb{I}(n) = 0$  pro všechna  $n > 1$ , resp.  $I(n) = 1$  pro všechna  $n \in \mathbb{N}$ . Pak pro každou aritmetickou funkci  $f$  platí:

$$f \circ \mathbb{I} = \mathbb{I} \circ f = f$$

a

$$(I \circ f)(n) = (f \circ I)(n) = \sum_{d|n} f(d).$$

Dále platí  $I \circ \mu = \mu \circ I = \mathbb{I}$ , neboť

$$\begin{aligned} (I \circ \mu)(n) &= \sum_{d|n} I(d)\mu\left(\frac{n}{d}\right) = \sum_{d|n} I\left(\frac{n}{d}\right)\mu(d) = \\ &= \sum_{d|n} \mu(d) = 0 \quad \text{pro všechna } n > 1 \end{aligned}$$

podle lemmatu za definicí Möbiovy funkce (pro  $n = 1$  je tvrzení zřejmé).

**VĚTA 13.** (*Möbiova inverzní formule*) *Nechť je aritmetická funkce  $F$  definovaná pomocí aritmetické funkce  $f$  předpisem  $F(n) = \sum_{d|n} f(d)$ . Pak lze funkci  $f$  vyjádřit ve tvaru*

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot F(d).$$

**DŮKAZ.** Vztah  $F(n) = \sum_{d|n} f(d)$  lze jiným způsobem zapsat jako  $F = f \circ I$ . Proto  $F \circ \mu = (f \circ I) \circ \mu = f \circ (I \circ \mu) = f \circ \mathbb{I} = f$ , což je tvrzení věty.  $\square$

**DEFINICE.** Multiplikativní funkcí přirozených čísel rozumíme takovou aritmetickou funkci, která splňuje, že pro všechny dvojice nesoudělných čísel  $a, b \in \mathbb{N}$  platí

$$f(a \cdot b) = f(a) \cdot f(b).$$

**PŘÍKLAD.** Multiplikativními funkcemi jsou např. funkce  $f(n) = \sigma(n)$ ,  $f(n) = \tau(n)$ , či  $f(n) = \mu(n)$  nebo, jak brzy dokážeme i tzv. Eulerova funkce  $f(n) = \varphi(n)$ .

### 3.3. Eulerova funkce $\varphi$ .

**DEFINICE.** Nechť  $n \in \mathbb{N}$ . Definujme Eulerovu funkci  $\varphi$  předpisem

$$\varphi(n) = |\{a \in \mathbb{N} \mid 0 < a \leq n, (a, n) = 1\}|$$

**PŘÍKLAD.**  $\varphi(1) = 1$ ,  $\varphi(5) = 4$ ,  $\varphi(6) = 2$ , je-li  $p$  prvočíslo, je zřejmé  $\varphi(p) = p - 1$ .

Nyní dokážeme několik důležitých tvrzení o funkci  $\varphi$ :

**LEMMA.** *Nechť  $n \in \mathbb{N}$ . Pak  $\sum_{d|n} \varphi(d) = n$ .*

**DŮKAZ.** Uvažme  $n$  zlomků

$$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \dots, \frac{n-1}{n}, \frac{n}{n}.$$

Zkrátíme-li zlomky na základní tvar a seskupíme podle jmenovatelů, snadno dostaneme právě uvedené tvrzení.  $\square$

**VĚTA 14.** *Nechť  $n \in \mathbb{N}$ , jehož rozklad je tvaru  $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ . Pak*

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

DŮKAZ. S využitím předchozího lemmatu a Möbiovy inverzní formule dostáváme

$$\begin{aligned}\varphi(n) &= \sum_{d|n} \mu(d) \frac{n}{d} = n - \frac{n}{p_1} - \dots - \frac{n}{p_k} + \dots + (-1)^k \frac{n}{p_1 \cdots p_k} = \\ &= n \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right).\end{aligned}\tag{13}$$

□

POZNÁMKA. Předchozí výsledek lze obdržet i bez použití Möbiovy inverzní formule pomocí principu inkluze a exkluze na základě zjištění počtu čísel soudělných s  $n$ .

DŮSLEDEK. *Nechť  $a, b \in \mathbb{N}$ ,  $(a, b) = 1$ . Pak*

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

DŮKAZ. Zřejmý.

□

POZNÁMKA. Rovněž toto tvrzení lze odvodit nezávisle na základě poznatku  $(n, ab) = 1 \iff (n, a) = 1 \wedge (n, b) = 1$ . Spolu se snadno odvoditelným výsledkem

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = (p-1) \cdot p^{\alpha-1}\tag{14}$$

pak lze odvodit vztah (13) již třetím způsobem.

PŘÍKLAD. Vypočtete  $\varphi(72)$ .

ŘEŠENÍ.  $72 = 2^3 \cdot 3^2 \implies \varphi(72) = 72 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 24$ , alternativně  $\varphi(72) = \varphi(8) \cdot \varphi(9) = 4 \cdot 6 = 24$ . □

PŘÍKLAD. Dokažte, že  $\forall n \in \mathbb{N} : \varphi(4n+2) = \varphi(2n+1)$ .

ŘEŠENÍ.  $\varphi(4n+2) = \varphi(2 \cdot (2n+1)) = \varphi(2) \cdot \varphi(2n+1) = \varphi(2n+1)$ . □

**3.4. Malá Fermatova věta, Eulerova věta.** Tvrzení v tomto odstavci patří mezi nejdůležitější výsledky teorie čísel.

VĚTA 15 (Fermatova, Malá Fermatova). *Nechť  $a \in \mathbb{Z}$ ,  $p$  prvočíslo,  $p \nmid a$ . Pak*

$$a^{p-1} \equiv 1 \pmod{p}.\tag{15}$$

DŮKAZ. Tvrzení vyplyne jako snadný důsledek Eulerovy věty 16. □

DŮSLEDEK. *Nechť  $a \in \mathbb{Z}$ ,  $p$  prvočíslo. Pak*

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

DŮKAZ. Pokud  $p \mid a$ , pak jsou obě strany kongruentní s  $0 \pmod{p}$ , jinak tvrzení snadno plyne vynásobením obou stran kongruence (15) číslem  $a$ . □

DEFINICE. *Úplná soustava zbytků modulo  $m$*  je libovolná  $m$ -tice čísel po dvou nekongruentních modulo  $m$  (nejčastěji  $0, 1, \dots, m-1$ ).  
*Redukovaná soustava zbytků modulo  $m$*  je libovolná  $\varphi(m)$ -tice čísel nesoudělných s  $m$  a po dvou nekongruentních modulo  $m$ .

POZNÁMKA. Snadno lze vidět, že jsou-li  $a, b \in \mathbb{Z}$ ,  $a \equiv b \pmod{m}$ , a  $(a, m) = 1$ , pak i  $(b, m) = 1$ .

LEMMA. *Nechť  $x_1, x_2, \dots, x_{\varphi(m)}$  tvoří redukovanou soustavu zbytků modulo  $m$ . Je-li  $a \in \mathbb{Z}$ ,  $(a, m) = 1$  pak i čísla  $a \cdot x_1, \dots, a \cdot x_{\varphi(m)}$  tvoří redukovanou soustavu zbytků modulo  $m$ .*

DŮKAZ. Protože  $(a, m) = 1$  a  $(x_i, m) = 1$ , platí  $(a \cdot x_i, m) = 1$ . Kdyby pro nějaká  $i, j$  platilo  $a \cdot x_i \equiv a \cdot x_j \pmod{m}$ , po vydělení obou stran kongruence číslem  $a$  nesoudělným s  $m$  dostaneme  $x_i \equiv x_j \pmod{m}$ .  $\square$

VĚTA 16 (Eulerova). *Nechť  $a \in \mathbb{Z}$ ,  $m \in \mathbb{N}$ ,  $(a, m) = 1$ . Pak*

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \quad (16)$$

DŮKAZ. Buď  $x_1, x_2, \dots, x_{\varphi(m)}$  libovolná redukovaná soustava zbytků modulo  $m$ . Podle předchozího lemmatu je i  $a \cdot x_1, \dots, a \cdot x_{\varphi(m)}$  redukovaná soustava zbytků modulo  $m$ . Platí tedy, že pro každé  $i$  existuje  $j$  (oba indexy jsou z množiny  $\{1, 2, \dots, \varphi(m)\}$ ) tak, že  $a \cdot x_i \equiv x_j \pmod{m}$ . Vynásobením čísel obou redukovaných soustav zbytků dostáváme

$$(a \cdot x_1) \cdot (a \cdot x_2) \cdots (a \cdot x_{\varphi(m)}) \equiv x_1 \cdot x_2 \cdots x_{\varphi(m)} \pmod{m}.$$

Po úpravě

$$a^{\varphi(m)} \cdot x_1 \cdot x_2 \cdots x_{\varphi(m)} \equiv x_1 \cdot x_2 \cdots x_{\varphi(m)} \pmod{m}$$

a protože  $(x_1 \cdot x_2 \cdots x_{\varphi(m)}, m) = 1$ , můžeme obě strany kongruence vydělit číslem  $x_1 \cdot x_2 \cdots x_{\varphi(m)}$  a dostaneme  $a^{\varphi(m)} \equiv 1 \pmod{m}$ .  $\square$

POZNÁMKA. Eulerova věta je rovněž důsledkem Lagrangeovy věty uplatněným na grupu  $(\mathbb{Z}_m^\times, \cdot)$ .

PŘÍKLAD. Nalezněte všechna prvočísla  $p$ , pro která  $5^{p^2} + 1 \equiv 0 \pmod{p^2}$ .

ŘEŠENÍ. Snadno se přesvědčíme, že  $p = 5$  úloze nevyhovuje. Pro  $p \neq 5$  platí  $(p, 5) = 1$ , a tedy podle Fermatovy věty  $5^{p-1} \equiv 1 \pmod{p}$ . Umocněním na  $p+1$  dostaneme  $5^{p^2-1} \equiv 1 \pmod{p}$ , odkud  $5^{p^2} \equiv 5 \pmod{p}$ . Z podmínky  $5^{p^2} + 1 \equiv 0 \pmod{p^2}$  plyne  $5^{p^2} \equiv -1 \pmod{p}$ , celkem tedy  $5 \equiv -1 \pmod{p}$ , a proto  $p \mid 6$ . Je tedy buď  $p = 2$ , nebo  $p = 3$ . Pro  $p = 2$  však  $5^4 + 1 \equiv 1^4 + 1 = 2 \not\equiv 0 \pmod{4}$ . Pro  $p = 3$  dostáváme  $5^9 + 1 = 5^6 \cdot 5^3 + 1 \equiv 5^3 + 1 = 126 \equiv 0 \pmod{9}$ , kde jsme užili důsledek Eulerovy věty  $5^6 \equiv 1 \pmod{9}$ . Jediným prvočíslem, vyhovujícím úloze je tedy  $p = 3$ .  $\square$



**PŘÍKLAD.** Pro liché číslo  $m > 1$  nalezněte zbytek po dělení čísla  $2^{\varphi(m)-1}$  číslem  $m$ .

**ŘEŠENÍ.** Z Eulerovy věty plyne  $2^{\varphi(m)} \equiv 1 \equiv 1 + m = 2r \pmod{m}$ ), kde  $r = \frac{1+m}{2}$  je přirozené číslo,  $0 < r < m$ . Podle 12 (3) platí  $2^{\varphi(m)-1} \equiv r \pmod{m}$ , a tedy hledaný zbytek po dělení je  $r = \frac{1+m}{2}$ .  $\square$

**TVRZENÍ 3.1.** *Je-li  $p$  prvočíslo,  $p \equiv 3 \pmod{4}$ , pak pro libovolná celá čísla  $a, b$  z kongruence  $a^2 + b^2 \equiv 0 \pmod{p}$  plyne  $a \equiv b \equiv 0 \pmod{p}$ .*

**DŮKAZ.** Předpokládejme, že pro  $a, b \in \mathbb{Z}$  platí  $a^2 + b^2 \equiv 0 \pmod{p}$ . Jestliže  $p \mid a$ , platí  $a \equiv 0 \pmod{p}$ , proto  $b^2 \equiv 0 \pmod{p}$ , tedy  $p \mid b^2$ , odkud vzhledem k tomu, že  $p$  je prvočíslo, dostáváme  $p \mid b$ , a proto  $a \equiv b \equiv 0 \pmod{p}$ , což jsme chtěli dokázat.

Zbývá prošetřit případ, kdy  $a$  není dělitelné prvočíslem  $p$ . Odtud dostáváme, že  $p$  nedělí ani  $b$  (kdyby  $p \mid b$ , dostali bychom  $p \mid a^2$ ). Vynásobíme-li obě strany kongruence  $a^2 \equiv -b^2 \pmod{p}$  číslem  $b^{p-3}$ , dostaneme podle Fermatovy věty

$$a^2 b^{p-3} \equiv -b^{p-1} \equiv -1 \pmod{p}.$$

Protože  $p \equiv 3 \pmod{4}$ , je  $p-3$  sudé číslo, a proto  $\frac{p-3}{2} \in \mathbb{N}_0$ . Označme

$$c = ab^{\frac{p-3}{2}}.$$

Pak  $c$  není dělitelné  $p$  a platí  $c^2 = a^2 b^{p-3} \equiv -1 \pmod{p}$ . Umocníme-li poslední kongruenci na  $\frac{p-1}{2} \in \mathbb{N}$ , dostaneme

$$c^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Protože  $p \equiv 3 \pmod{4}$ , existuje celé číslo  $t$  tak, že  $p = 3+4t$ . Pak ovšem  $\frac{p-1}{2} = 1 + 2t$ , což je číslo liché a proto  $(-1)^{(p-1)/2} = -1$ . Podle Fermatovy věty naopak platí  $c^{p-1} \equiv 1 \pmod{p}$ , odkud  $1 \equiv -1 \pmod{p}$  a  $p \mid 2$ , spor.  $\square$

S Eulerovou funkcí a Eulerovou větou úzce souvisí důležitý pojem *řád čísla modulo  $m$*  - jde přitom pouze o jinak nazvaný řád prvku v grupě invertibilních zbytkových tříd modulo  $m$ :

**DEFINICE.** Nechť  $a \in \mathbb{Z}$ ,  $m \in \mathbb{N}$  ( $a, m$ ) = 1. *Řádem čísla  $a$  modulo  $m$*  rozumíme nejmenší přirozené číslo  $n$  splňující

$$a^n \equiv 1 \pmod{m}.$$

**PŘÍKLAD.** Pro libovolné  $m \in \mathbb{N}$  má číslo 1 modulo  $m$  řád 1. Číslo  $-1$  má řád

- 1 pro  $m = 1$  nebo  $m = 2$
- 2 pro  $m > 2$

**PŘÍKLAD.** Určete řád čísla 2 modulo 7.

ŘEŠENÍ.

$$2^1 = 2 \not\equiv 1 \pmod{7}$$

$$2^2 = 4 \not\equiv 1 \pmod{7}$$

$$2^3 = 8 \equiv 1 \pmod{7}$$

Řád čísla 2 modulo 7 je tedy roven 3.  $\square$

Uvedme nyní několik zásadních tvrzení udávajících možné hodnoty řádu čísla modulo  $m$ :

LEMMA. *Nechť  $m \in \mathbb{N}$ ,  $a, b \in \mathbb{Z}$ ,  $(a, m) = (b, m) = 1$ . Jestliže  $a \equiv b \pmod{m}$ , pak obě čísla  $a, b$  mají stejný řád modulo  $m$ .*

DŮKAZ. Umocněním kongruence  $a \equiv b \pmod{m}$  na  $n$ -tou dostaneme  $a^n \equiv b^n \pmod{m}$ , tedy  $a^n \equiv 1 \pmod{m} \iff b^n \equiv 1 \pmod{m}$ .  $\square$

LEMMA. *Nechť  $m \in \mathbb{N}$ ,  $a \in \mathbb{Z}$ ,  $(a, m) = 1$ . Je-li řád čísla  $a$  modulo  $m$  roven  $r \cdot s$ , (kde  $r, s \in \mathbb{N}$ ), pak řád čísla  $a^r$  modulo  $m$  je roven  $s$ .*

DŮKAZ. Protože žádné z čísel  $a, a^2, a^3, \dots, a^{r \cdot s - 1}$  není kongruentní s 1 modulo  $m$ , není ani žádné z čísel  $a^r, a^{2r}, a^{3r}, \dots, a^{(s-1)r}$  kongruentní s 1. Platí ale  $(a^r)^s \equiv 1 \pmod{m}$ , proto je řád  $a^r$  modulo  $m$  roven  $s$ .  $\square$

POZNÁMKA. Opak obecně neplatí – z toho, že řád čísla  $a^r$  modulo  $m$  je roven  $s$  ještě neplyne, že řád čísla  $a$  modulo  $m$  je  $r \cdot s$ .

Př:  $m = 13$

$a = 3$ ,  $a^2 = 9 \pmod{13}$ ,  $a^3 = 27 \equiv 1 \pmod{13} \Rightarrow 3$  má řád 3 mod 13.  
 $b = -4$ ,  $b^2 = 16 \not\equiv 1 \pmod{13}$ ,  $b^3 = -64 \equiv 1 \pmod{13} \Rightarrow -4$  má řád 3 modulo 13.

Přitom  $(-4)^2 = 16 \equiv 3 \pmod{13}$  má stejný řád 3 jako číslo 3, ale číslo  $-4$  nemá řád  $2 \cdot 3$ .

Přesný popis závislosti řádu na exponentu dávají následující 2 věty:

VĚTA 17. *Nechť  $m \in \mathbb{N}$ ,  $a \in \mathbb{Z}$ ,  $(a, m) = 1$ . Označme  $r$  řád čísla  $a$  modulo  $m$ . Pak pro libovolná  $t, s \in \mathbb{N} \cup \{0\}$  platí*

$$a^t \equiv a^s \pmod{m} \iff t \equiv s \pmod{r}.$$

DŮKAZ. Bez újmy na obecnosti lze předpokládat, že  $t \geq s$ . Vydělíme-li číslo  $t - s$  číslem  $r$  se zbytkem, dostaneme  $t - s = q \cdot r + z$ , kde  $q, z \in \mathbb{N}_0$ ,  $0 \leq z < r$ .

„ $\Leftarrow$ “ Protože  $t \equiv s \pmod{r}$ , máme  $z = 0$ , a tedy  $a^{t-s} = a^{qr} = (a^r)^q \equiv 1^q \pmod{m}$ . Vynásobením obou stran kongruence číslem  $a^s$  dostaneme tvrzení.

„ $\Rightarrow$ “ Z  $a^t \equiv a^s \pmod{m}$  plyne  $a^s \cdot a^{qr+z} \equiv a^s \pmod{m}$ . Protože je  $a^r \equiv 1 \pmod{m}$ , je rovněž  $a^{qr+z} \equiv a^z \pmod{m}$ . Celkem po vydělení

obou stran kongruence číslem  $a^s$  (které je nesoudělné s modulem), dostáváme  $a^z \equiv 1 \pmod{m}$ . Protože  $z < r$ , plyne z definice řádu, že  $z = 0$ , a tedy  $r \mid t - s$ .  $\square$

Zřejmým důsledkem předchozí věty a Eulerovy věty je následující tvrzení (jehož druhá část je přeformulováním Lagrangeovy věty z Algebry pro naši situaci):

**DŮSLEDEK.** *Nechť  $m \in \mathbb{N}$ ,  $a \in \mathbb{Z}$ ,  $(a, m) = 1$ . Označme  $r$  řád čísla  $a$  modulo  $m$ .*

(1) *Pro libovolné  $n \in \mathbb{N} \cup \{0\}$  platí*

$$a^n \equiv 1 \pmod{m} \iff r \mid n.$$

(2)  *$r \mid \varphi(m)$*

**DŮKAZ.**

(1) stačí v předchozí větě volit  $t = n$ ,  $s = r$ .

(2) zřejmé z (1) díky Eulerově větě volbou  $n = \varphi(m)$ .  $\square$

Následující věta je zobecněním předchozího Lemmatu.

**VĚTA 18.** *Nechť  $m, n \in \mathbb{N}$ ,  $a \in \mathbb{Z}$ ,  $(a, m) = 1$ . Je-li řád čísla  $a$  modulo  $m$  roven  $r \in \mathbb{N}$ , je řád čísla  $a^n$  modulo  $m$  roven  $\frac{r}{(n,r)}$ .*

**DŮKAZ.** Protože  $\frac{r \cdot n}{(r,n)} = [r, n]$ , což je zřejmě násobek  $r$ , máme

$$(a^n)^{\frac{r}{(n,r)}} = a^{[r,n]} \equiv 1 \pmod{m}$$

(plyne z předchozího Důsledku neboť  $r \mid [r, n]$ ). Na druhou stranu, je-li  $k \in \mathbb{N}$  libovolné takové, že  $(a^n)^k = a^{n \cdot k} \equiv 1 \pmod{m}$ , dostáváme ( $r$  je řád  $a$ ), že  $r \mid n \cdot k$  a dále z Věty 5 plyne, že  $\frac{r}{(n,r)} \mid \frac{n}{(n,r)} \cdot k$  a díky nesoudělnosti čísel  $\frac{r}{(n,r)}$  a  $\frac{n}{(n,r)}$  dostáváme  $\frac{r}{(n,r)} \mid k$ . Proto je  $\frac{r}{(n,r)}$  řádem čísla  $a^n$  modulo  $m$ .  $\square$