Kapitola 1

Teorie čísel

Dělitelnost a kongruence

V této části si představíme pojem kongruence. Uvedeme několik užitečných tvrzení. Jejich důkazy ponecháváme jako jednoduchá cvičení. Zápis $\gcd(a,b)$ značí největší společný dělitel $a,b \in \mathbb{Z}$. Na úvod připomeňme definici dělitelnosti.

Definice 1.1. Nechť $a,b \in \mathbb{Z}$. Řekneme, že a dělí b (též b je dělitelné a), píšeme

$$a \mid b,$$

jestliže existuje $k \in \mathbb{Z}$ takové, že $ak = b$.

Lemma 1.2. *Relace dělitelnosti je tranzitivní, tedy pro $a,b,c \in \mathbb{Z}$ platí*

$$a \mid b,\ b \mid c \quad \Rightarrow \quad a \mid c.$$

Lemma 1.3. *Nechť p je prvočíslo, pak platí*

$$p \mid ab \quad \Rightarrow \quad (p \mid a \ \textit{nebo}\ \ p \mid b).$$

Definice 1.4. Nechť $a,b \in \mathbb{Z}$, $m \in \mathbb{N}$. Řekneme, že a je kongruentní s b modulo m, píšeme

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

jestliže $m \mid a-b$.

Lemma 1.5 (základní operace s kongruencemi)**.** *Nechť $a,b,c,d,k \in \mathbb{Z}$, $m,n \in \mathbb{N}$. Platí*

$$\begin{aligned}
&a \equiv b \pmod{m},\ c \equiv d \pmod{m} && \Rightarrow && a \pm \equiv b \pmod{m},\\
&a \equiv b \pmod{m},\ c \equiv d \pmod{m} && \Rightarrow && ac \equiv bd \pmod{m},\\
&a \equiv b \pmod{m} && \Rightarrow && ak \equiv bk \pmod{m},\\
&a \equiv b \pmod{m} && \Rightarrow && a^n \equiv b^n \pmod{m},\\
&ak \equiv bk \pmod{m},\ \gcd(k,m) = 1 && \Rightarrow && a \equiv b \pmod{m},\\
&an \equiv bn \pmod{m},\ n \mid m && \Rightarrow && a \equiv b \pmod{\frac{m}{n}},\\
&a \equiv b \pmod{m} && \Rightarrow && an \equiv bn \pmod{bn},\\
&a \equiv b \pmod{m},\ d \mid m && \Rightarrow && a \equiv b \pmod{d}.
\end{aligned}$$

Poznámka 1.6. Předchozí lemma nám může dost usnadnit uvažování při řešení příkladů o dělitelnosti.

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

$$5^{20} = 25^{10} \equiv (-1)^{10} = 1 \pmod{26}.$$

2. Dokažte, že pro libovolné $n \in \mathbb{N}$ platí $7 \mid 37^{n+2} + 16^{n+1} + 23^n$.

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

3. Dokažte, že pro libovolné $n \in \mathbb{N}$ platí $11 \mid 5^{3n} - 2^{2n}$.

$$5^{3n} - 2^{2n} = (5 \cdot 25)^n - 4^n \equiv (5 \cdot 3)^n - 4^n = 15^n - 4^n \equiv 4^n - 4^n = 0 \pmod{11}.$$

Nyní ukážeme, že v jistém smyslu lze dělit libovolným prvkem, který je nesoudělný s modulem.

Lemma 1.7. *Nechť $a \in \mathbb{Z}$, $m \in \mathbb{N}$.*

$$\gcd(a,m) = 1 \quad \Leftrightarrow \exists b \in \mathbb{Z} \colon ab \equiv 1 \pmod{m}.$$

K hledání této multiplikativní inverze (tj. inverze k násobení, tedy a^{-1}) využijeme tzv. Euklidův algoritmus a Bezoutovu rovnost.

Lemma 1.8 (Euklidův algoritmus)**.** *Nechť $a_1, a_2 \in \mathbb{Z}$. Pak $(a_1, a_2) = d$ dostaneme jako **poslední nenulový zbytek**, který získáme pomocí postupného dělení se zbytkem.*

$$\begin{aligned}
a_1 &= q_1 a_2 + a_3 \\
a_2 &= q_2 a_3 + a_4 \\
a_3 &= q_3 a_4 + a_5 \\
&\vdots \\
a_{k-2} &= q_{k-2} a_{k-1} + a_k \\
a_{k-1} &= q_{k-1} a_k + 0
\end{aligned}$$

kde $|a_i| > |a_{i+1}|$ pro všechna $i = 1, \ldots, k-1$ a navíc $a_k \neq 0$. Pak platí: $(a_1, a_2) = a_k$

Lemma 1.9 (Bezoutova identita)**.** *Nechť $a, b \in \mathbb{Z}$, $(a,b) = d$, pak $\exists k, l \in \mathbb{Z} \colon ak + bl = d$.*

Poznámka 1.10. Předvedeme si, jak nyní využít Euklidův algoritmus ke hledání multiplikativní inverze. Hledejme $b \in \mathbb{Z}$ takové, aby

$$17 \cdot b \equiv 1 \pmod{31}$$

Spočtěme $\gcd(31, 17)$ a nalezněme koeficienty z Bezoutovy identity.

$$\begin{aligned}
31 &= 17 + 14 \\
17 &= 14 + 3 \\
14 &= 4 \cdot 3 + 2 \\
3 &= 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{aligned}$$

Dostáváme tedy, že $\gcd(31,17) = 1$. Nyní opačným postupem vyjádříme 1 pomocí 31 a 17

$$\begin{aligned}
1 &= 3-2,\\
1 &= 3-(14-4\cdot 3) = 5\cdot 3-14,\\
1 &= 5\cdot(17-14)-14 = 5\cdot 17-6\cdot 14,\\
1 &= 5\cdot 17-6\cdot(31-17) = 11\cdot 17-6\cdot 31.
\end{aligned}$$

Podívejme se na rovnost $1 = 11\cdot 17-6\cdot 31$ modulo 31. Dostáváme

$$1 \equiv 11\cdot 17 \pmod{31}.$$

Hledané b je tedy 11.

Ukázali jsme si, že prvky nesoudělné s modulem jsou poměrně význačné. Tento fakt se projeví zejména v Eulerově větě. Řekněme si proto na závěr této úvodní části ještě něco málo o Eulerově funkci.

Definice 1.11. *Eulerovou funkci* $\varphi\colon \mathbb{N}\to\mathbb{N}$ definujeme předpisem

$$\varphi(n) = |\{k\in\mathbb{N} \mid k\le n, (k,n)=1\}|,$$

tj. Eulerova funkce nám udává počet čísel nesoudělných s číslem n, která nepřesáhnou n.

Lemma 1.12. *Buď* $n\in\mathbb{N}$ *libovolné číslo a* $n = p_1^{\alpha_1}\cdot\ldots\cdot p_k^{\alpha_k}$ *jeho rozklad na prvočísla, kde* $p_i\neq p_j$ *pro* $i\neq j$ *a* $\alpha_i\ge 1$. *Pak platí*

$$\varphi(n) = \prod_{i=1}^{k}(p_i-1)\cdot p_i^{\alpha_i-1} = n\cdot\prod_{i=1}^{k}\left(1-\frac{1}{p}\right).$$

1.1 Teorie

Věta 1.13 (malá Fermatova)**.** *Buď te $a \in \mathbb{Z}$ a p prvočíslo. Pak platí*

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

Pokud navíc $p \nmid a$, tak

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

Věta 1.14 (Eulerova)**.** *Buď te $a, m \in \mathbb{N}$ takové, že $\gcd(a,m) = 1$. Pak*

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

kde $\varphi\colon \mathbb{N} \to \mathbb{N}$ je Eulerova funkce.

Věta 1.15 (čínská zbytková)**.** *Buď te $m_1, m_2 \ldots, m_k \in \mathbb{N}$ po dvou nesoudělná čísla, $a_1, a_2 \ldots, a_k \in \mathbb{Z}$. Pak soustava*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

má právě jedno řešení modulo $m_1 \cdot m_2 \cdot \ldots \cdot m_k$.

Věta 1.16 (Wilsonova)**.** *Přirozené číslo $n \geq 2$ je prvočíslo právě tehdy, když*

$$(n-1)! \equiv -1 \pmod{n}.$$

1.2 Příklady

Příklad 1.1. Buď $n \in \mathbb{N}$. Ukažte, že existuje n po sobě jdoucích čísel takových, že každé z nich je dělitelné alespoň dvěma různými prvočísly.

Řešení. Hledáme x splňující

$$\begin{aligned} x &\equiv 0 \pmod{p_0 q_0}, \\ x+1 &\equiv 0 \pmod{p_1 q_1}, \\ &\vdots \\ x+n-1 &\equiv 0 \pmod{p_{n-1} q_{n-1}}, \end{aligned}$$

pro nějaká po dvou různá prvočísla $p_0, \ldots, p_{n-1}$, $q_0, \ldots, q_{n-1}$. Zvolíme-li libovolná různá prvočísla, budou moduly po dvou nesoudělné. Čínská zbytková věta nám pak přímo říká, že existuje celé číslo x splňující soustavu

$$\begin{aligned} x &\equiv 0 \pmod{p_0 q_0}, \\ x &\equiv -1 \pmod{p_1 q_1}, \\ &\vdots \\ x &\equiv -n+1 \pmod{p_{n-1} q_{n-1}}. \end{aligned}$$

■

Příklad 1.2. Dokažte, že existuje číslo $n \in \mathbb{Z}$ takové, že pro libovolné $k \in \mathbb{Z}$ nemá číslo k^2+k+n žádného prvočíselného dělitele menšího než 2016.

Řešení. Nechť p je prvočíslo. Zkoumejme, jaký zbytek po dělení p může dávat číslo k^2+k. Zjevně stačí dosadit čísla $0, 1, \ldots p-1$, dále se už budou zbytky periodicky opakovat. Pro $k = 0$ a $k = p-1$ je $k^2+k \equiv 0 \pmod{p}$. Z Dirichletova principu proto plyne, že existuje $r \in 0, 1, ..., p-1$ pro které platí

$$\forall k \in \mathbb{Z} : k^2+k \not\equiv r \pmod{p}.$$

Nechť $p_1, ..., p_m$ jsou prvočísla menší než 2016 a $r_1, ..., r_m$ jsou příslušné zbytky, jichž k^2+k nenabývá. Hledáme tedy n splňující

$$\begin{aligned} n &\equiv -r_1 \pmod{p_1}, \\ n &\equiv -r_2 \pmod{p_2}, \\ &\vdots \\ n &\equiv -r_m \pmod{p_m}, \end{aligned}$$

protože pak $k^2+k+n \equiv k^2+k-r_i \not\equiv 0 \pmod{p_i}$ pro všechna i. Existence takového n vyplývá z čínské zbytkové věty. ■

Příklad 1.3. Rozhodněte, zda existuje posloupnost obsahující každé přirozené číslo právě jednou taková, aby součet jejích prvních k členů byl dělitelný k pro všechna $k \in \mathbb{N}$.

Řešení. Označme posloupnost $\{a_n\}_{n=1}$ a $s_k = \sum_{i=1}^{k} a_i$. Položme $a_1 = 1$. Předpokládejme, že máme prvních k členů splňujících podmínky. Hledáme a_{k+1} a a_{k+2} taková, že a_{k+2} je nejmenší přirozené číslo, které se nevyskytuje v $a_1, \ldots, a_k$. Tedy chceme, aby

$$\begin{aligned} a_{k+1} &\equiv -s_k \pmod{k+1} \\ a_{k+2} &\equiv -s_k - a_{k+2} \pmod{k+2}. \end{aligned}$$

Jelikož $(k+1, k+2) = 1$ pak nám čínská zbytková věta říká, že takové a_{k+1} různé od $a_1, \ldots, a_k, a_{k+2}$ opravdu existuje. ■

Příklad 1.4. Nechť $n \in \mathbb{N}$ a $a_1, \ldots, a_k$ ($k \geq 2$) jsou navzájem různá celá čísla z množiny $\{1, \ldots, n\}$ taková, že pro každé $i = 1, \ldots, k-1$ je číslo $a_i(a_{i+1} - 1)$ dělitelné n. Dokažte, že číslo $a_k(a_1 - 1)$ není dělitelné n.

Řešení. Nechť $n = pq$ tak, že $p | a_1$ a $q | a_2 - 1$. Předpokládejme pro spor, že $n | a_k(a_1 - 1)$. Jelikož $q | a_2 - 1$, pak (q, a_2), a tudíž $q | a_3 - 1$. Obdobně pro ostatní členy dostáváme, že $q | a_i - 1$ pro všechna i. Dále $p | a_1$, z čehož plyne $(p, a_1 - 1) = 1$ a tedy $p | a_k$. Podobně máme $p | a_i$ pro všechna i. Všechna a_i jsou řešením dvojice kongruencí

$$\begin{aligned} x &\equiv 0 \pmod{p}, \\ x &\equiv 1 \pmod{q}. \end{aligned}$$

Nutně navíc $(p, q) = 1$, protože $p | a_1$ a $q | a_1 - 1$. Čínská zbytková věta nám říká, že existuje jedno takové $0 \leq x < pq = n$. My jich máme ale hned k. Máme hledaný spor. ■

Příklad 1.5. Dokažte, že pro každé liché prvočíslo p existuje nekonečně mnoho $n \in \mathbb{N}$ splňujících $p \mid (n \cdot 2^n + 1)$.

Řešení. Hledáme nekonečně mnoho n pro které platí

$$n \cdot 2^n \equiv -1 \pmod{p}.$$

Z malé Fermatovy věty máme

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

Zřejmě tedy je-li $n = p - 1$, pak

$$(p-1) \cdot 2^{p-1} \equiv -1 \cdot 1 = -1 \pmod{p}.$$

Zvolíme-li n jako k-tou mocninu čísla $p - 1$, pak

$$n \cdot 2^n = (p-1)^k \cdot 2^{(p-1)^k} \equiv (-1)^k \cdot 1^{(p-1)^{k-1}} = (-1)^k \pmod{p}.$$

Vidíme, že řešením jsou všechna $n = (p-1)^k$ pro k liché. ■

Příklad 1.6. Dokažte, že pro všechna lichá $n \in \mathbb{N}$ platí $n \mid \left(2^{n!} - 1\right)$.

Řešení. V řeči kongruencí chceme dokázat, že $\forall n \in \mathbb{N}, 2 \nmid n$ platí

$$2^{n!} \equiv 1 \pmod{n}.$$

Protože n je liché, je $\gcd 2, n = 1$, můžeme tedy použít Eulerovu větu. Protože $\varphi(n) \leq n$ platí $\varphi(n) \mid n!$ a tedy existuje $k \in \mathbb{N}$ takové, že $k\varphi(n) = n!$. Platí tedy

$$2^{n!} = \left(2^{\varphi(n)}\right)^k \equiv 1^k = 1 \pmod{n},$$

což jsme chtěli dokázat. ■

Příklad 1.7. Nechť p je liché prvočíslo. Dokažte

$$p \equiv 1 \pmod 4 \quad \Leftrightarrow \quad \exists m \in \mathbb{N}\colon\ p \mid m^2+1.$$

Řešení. „$\Leftarrow$“: Nechť

$$m^2 \equiv -1 \pmod p.$$

Umocněme na $\frac{p-1}{2}$, dostáváme

$$1 \overset{MFV}{\equiv} m^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod p,$$

což nastává právě tehdy, je-li $\frac{p-1}{2}$ sudé, tedy $p \equiv 1 \pmod 4$.

„$\Rightarrow$“: Nechť naopak $p \equiv 1 \pmod 4$, tj. $p = 4k+1$. Z Wilsonovy věty máme

$$-1 \equiv (4k)! \equiv 1\cdot 2\cdot \ldots \cdot 2k\cdot (p-2k)\cdot (p-(2k-1))\cdot \ldots \cdot (p-1) = (-1)^{2k}\cdot [(2k)!]^2 = m^2 \pmod p$$

■

Příklad 1.8. Žádné prvočíslo nelze zapsat jako součet dvou čtverců více než jedním způsobem.

Řešení. Nechť $p = a^2+b^2 = c^2+d^2$, kde $a \neq c$. Jistě též $a \neq b$ a $c \neq d$. BÚNO $a > b$, $c > d$, $a > c$. Pak

$$p^2 = (a^2+b^2)\cdot(c^2+d^2) = a^2c^2+b^2d^2+a^2d^2+b^2c^2$$

můžeme psát dvěma způsoby jako

$$p^2 = (ac \pm bd)^2 + (ad \mp bc)^2,$$

přitom

$$(ac+bd)(ad+bc) = a^2cd+b^2cd+abc^2+abd^2 = (a^2+b^2)cd+(c^2+d^2)ab = p(ab+cd).$$

Nutně tedy $p \mid (ac+bd)$ nebo $p \mid (ad+bc)$.
Pokud $p \mid (ac+bd)$, pak z

$$p^2 = (ac+bd)^2+(ad-bc)^2$$

dostáváme, že $ad = bc$. Přitom $a > c$ dává $d < b$. Pak ale $a^2+b^2 > c^2+d^2$, což je spor.
Pokud $p \mid (ad+bc)$, pak z

$$p^2 = (ad+bc)^2+(ac-bd)^2$$

dostáváme, že $ac = bd$. Protože ale $a > b$ a $c > d$, dostáváme spor. ■

Příklad 1.9. Nechť p je liché prvočíslo. Dokažte

$$p \equiv 1 \pmod 4 \quad \Leftrightarrow \quad \exists x,y \in \mathbb{N}\colon\ p = x^2+y^2.$$

Řešení. „$\Leftarrow$“: Jistě právě jedno z x,y je sudé, nechť tedy například $2 \mid x$, pak

$$p = x^2+y^2 \equiv 0+1 = 1 \pmod 4.$$

„$\Rightarrow$“: Nechť $p \equiv 1 \pmod 4$, tj. $p = 4k+1$. Z Wilsonovy věty podobně jako v příkladu 1.7 máme pro $m = (2k)!$

$$m^2 \equiv -1 \pmod p.$$

Jistě

$$x^2+y^2 \equiv (x+my)(x-my) \pmod{p}.$$

Počet dvojic $(x,y) \in \mathbb{Z}$ takových, že

$$0 \le x < \sqrt{p}, \quad 0 \le y < \sqrt{p}$$

existuje právě $\lceil \sqrt{p} \rceil \cdot \lceil \sqrt{p} \rceil > \sqrt{p}^2 = p$. Nutně tedy existují dvě různé dvojice $(x,y), (x',y')$ takové, že

$$x+my \equiv x'+my' \pmod{p}.$$

Položme $x_0 = x-x'$ a $y_0 = y-y'$. Pak platí

$$x_0+my_0 = (x-x')+m(y-y') = (x+my)-(x'+my') \equiv 0 \pmod{p}.$$

Přitom jistě $(x_0,y_0) \neq (0,0)$ a zároveň $|x_0| < \sqrt{p}$, $|y_0| < \sqrt{p}$. Odtud

$$0 < x_0^2+y_0^2 < 2p,$$

přitom $p \mid x_0^2+y_0^2$, tedy

$$x_0^2+y_0^2 = p.$$

■

Příklad 1.10. Řešte v $\mathbb{Z}$

$$x^2+y^2+z^2 = 2xyz.$$

Řešení. Jistě $x=y=z=0$ je řešení. Ukažme, že je jediné. Předpokládejme sporem, že $(x,y,z) \neq (0,0,0)$ je řešení. Buď 2^k, $k \ge 0$ největší mocnina dvou, která dělí x,y,z. Pak

$$x = 2^k x_1, \quad y = 2^k y_1, \quad z = 2^k z_1.$$

Dosazením do původní rovnice dostáváme

$$\begin{aligned} 2^{2k}x_1^2+2^{2k}y_1^2+2^{2k}z_1^2 &= 2^{3k+1}x_1y_1z_1, \\ x_1^2+y_1^2+z_1^2 &= 2^{k+1}x_1y_1z_1. \end{aligned}$$

Dvojka dělí pravou stranu, musí dělit i levou. S ohledem na volbu k je právě jeden člen sudý. BÚNO $x_1 = 2x_2$, přitom y_1, z_1 jsou liché.

$$2 \equiv y_1^2+z_1^2 = 2^{k+2}x_2y_1z_1 - 4x_2^2 \equiv 0 \pmod{4},$$

což je spor. ■