Kongruence

Karolína Kuchyňová

Abstrakt. Kongruence jsou jednou z oblastí studia teorie čísel, vychází z dělitelnosti a umožňují nám rozšířit pohled na ni. Přestože se na středních školách standardně neprobírají, dají se uplatnit v matematické olympiádě i jiných soutěžích. Na přednášce si představíme jejich základní vlastnosti a ukážeme jejich využití na různých typech příkladů.

Definice. Jestliže dvě celá čísla a, b dávají při dělení přirozeným číslem m týž zbytek r, kde $0 \leq r < m$, říkáme, že a a b jsou *kongruentní modulo* m, což zapisujeme takto:

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

Tvrzení. (Ekvivalentní podmínky) *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) $m \mid a - b$.

Tvrzení. *Pokud $a \equiv b \pmod{m}$ a $k \in \mathbb{Z}$, platí:*

(1) $a + k \equiv b + k \pmod{m}$,
(2) $a \cdot k \equiv b \cdot k \pmod{m}$.

Tvrzení. *Pokud $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$ a $n \in \mathbb{N}$, platí:*

(1) $a + c \equiv b + d \pmod{m}$,
(2) $ac \equiv bd \pmod{m}$,
(3) $a^n \equiv b^n \pmod{m}$.

Cvičení. Ukažte, že pokud $a \cdot c \equiv b \cdot c \pmod{m}$, tak obecně nemusí platit $a \equiv b \pmod{m}$.

Tvrzení. *Pokud $a \cdot c \equiv b \cdot c \pmod{m}$ a $(m, c) = 1$, tak $a \equiv b \pmod{m}$.*

Tvrzení. *Nechť $a \equiv b \pmod{m}$ a $m' \in \mathbb{N}$. Pak platí:*

(1) $a + k \cdot m \equiv b \pmod{m}$.
(2) *pokud $m' \mid m$, pak $a \equiv b \pmod{m'}$,*
(3) *pokud $ca \equiv cb \pmod{m}$, tak $a \equiv b \pmod{m/(m, c)}$.*

Příklady

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

Příklad 2. Mějme číslo $N = 22 \cdot 31 + 11 \cdot 17 + 13 \cdot 19$. Určete:

(1) paritu čísla N,
(2) poslední číslici N,
(3) zbytek po dělení čísla N sedmi.

Příklad 3. Dokažte, že číslo n je dělitelné číslem m pro

(1) $n = 2^{60} + 7^{30}$ a $m = 13$,
(2) $n = (835^5 + 6)^{18} - 1$ a $m = 112$.

Příklad 4. Dokažte, že

(1) pro libovolné $n \in \mathbb{N}$ je číslo $37^{n+2} + 16^{n+1} + 23^n$ dělitelné sedmi,
(2) pro libovolné $n \in \mathbb{N}$ je číslo $72^{2n+2} - 47^{2n} + 28^{2n-1}$ dělitelné číslem 25,
(3) pro libovolné $k, m, n \in \mathbb{N}$ je číslo $5^{5k+1} + 4^{5m+2} + 3^{5n}$ dělitelné číslem 11.

Příklad 5. Dokažte, že žádné číslo tvaru $8k \pm 3$, $k \in \mathbb{N}$, není možné zapsat ve tvaru $x^2 - 2y^2$ pro žádná celá čísla x, y.

Příklad 6. Dokažte, že

(1) pokud $a, b \in \mathbb{Z}$ a $a^2 + b^2 \equiv 0 \pmod 3$, pak $a \equiv b \equiv 0 \pmod 3$,
(2) pokud $a, b \in \mathbb{Z}$ a $a^2 + b^2 \equiv 0 \pmod 7$, pak $a \equiv b \equiv 0 \pmod 7$,
(3) existují celá čísla a, b taková, že ačkoli platí $a^2 + b^2 \equiv 0 \pmod 5$, přesto neplatí $a \equiv b \equiv 0 \pmod 5$.
(4) pokud $a, b, c \in \mathbb{Z}$ a $a^3 + b^3 + c^3 \equiv 0 \pmod 9$, pak $abc \equiv 0 \pmod 3$.

Příklad 7. Řešte v celých číslech rovnice:

(1) $5x + 7y = 8$,
(2) $91x - 28y = 35$,
(3) $18x + 20y + 15z = 1$,
(4) $15x - 12y + 48z - 51u = 1$.

Příklad 8. Najděte všechna celá čísla x, y taková, že $x^2 = 4y + 2$.

Příklad 9. Dokažte, že rovnice $x^2 = 3 - 8z + 2y^2$ nemá řešení v celých číslech.

Příklad 10. Řešte v přirozených číslech rovnici $a^6 + b^4 + c^2 = 1234567$.

Příklad 11. Ukažte, že jestliže jsou čísla p a $p + 2$ obě prvočísla, tak potom buď $p = 3$, nebo $6 \mid p + 1$. (Kanada 1973)

Příklad 12. Značme ciferný součet přirozeného čísla n jako $C(n)$. Najděte všechna n, pro která platí $n + C(n) + C(C(n)) = 2015$. (Brkos XXI–6–5)

Příklad 13. *Transformací* čísla budeme rozumět jeho nahrazení vlastním ciferným součtem. Začneme s 2007^{2007} a uděláme čtyři transformace. Jaký dostaneme výsledek?

Příklad 14. Ukažte, že napíšeme-li čísla $1, 2, \ldots, 1986$ bez mezer za sebe v libovolném pořadí, nedostaneme nikdy číslo, které by bylo třetí mocninou přirozeného čísla.

Příklad 15. Nechť n je přirozené číslo takové, že $n(n+1)/3$ je čtverec. Ukažte, že pak n je násobek tří a čísla $n+1$ a $n/3$ jsou také čtverce. (Brazílie 1989)

Příklad 16. Najděte všechny dvojice prvočísel p, q takové, že $p + q = (p - q)^3$. (Ruská MO 2001)

Příklad 17. Číslo n je součinem tří (ne nutně různých) prvočísel. Zvětšíme-li každé z nich o jedna, zvětší se jejich součin o 963. Určete původní číslo n. (MO 63–I–1)

Literatura a zdroje

[1] J.Herman, R.Kučera, J.Šimša: *Metody řešení matematických úloh I*, MU, 2001,
[2] Kuba Krásenský: *Dělitelnost pro začátečníky*, Domašov, 2012,
[3] Pavel Paták: *Využití dělitelnosti v praxi*, Ramzová, 2006,
[4] Franta Kopecký: *Lehká teorie čísel na brutalitách*, Hutisko-Solanec, 2007,
[5] Michal „Kenny“ Rolínek: *Důkazové metody v teorii čísel*, Domaslav, 2010,
[6] Seriál MKS: Teorie čísel, 33. ročník (2013/2014).