Povídání k třetí podzimní sérii

Tématem letošní třetí série jsou kongruence. Pokud jsi o nich v životě neslyšel(a), nezoufej! Právě pro Tebe je určen tento text, ve kterém najdeš všechny potřebné informace.

Určitě víš, že se přirozená čísla dají rozdělit na sudá a lichá – ta, která jsou dělitelná dvěma, a ta, která po dělení dvěma dávají zbytek jedna. Kongruence jsou vlastně takovým zobecněním rozlišení čísel na sudá a lichá.

Řekneme, že dvě celá čísla a, b jsou *kongruentní modulo* m, kde m je přirozené číslo, pokud obě dávají po dělení m stejný zbytek. Zapisujeme to jako $a \equiv b \pmod{m}$. Ekvivalentní (a praktičtější) definice je, že dvě čísla a, b jsou kongruentní modulo m, pokud je číslo $a - b$ dělitelné číslem m. Kongruence se mezi sebou dají sčítat a násobit – pracuje se s nimi skoro stejně jako s rovnicemi.

Cvičení. Rozmysli si, že platí následující základní vlastnosti kongruencí:

(1) $a \equiv 0 \pmod{m}$ právě tehdy, když $m \mid a$.

(2) Pokud $a \equiv b \pmod{m}$, potom $a+k \equiv b+k \pmod{m}$ a $ak \equiv bk \pmod{m}$ pro libovolné k celé.

(3) Pokud $a \equiv b \pmod{m}$ a $b \equiv c \pmod{m}$, potom $a \equiv c \pmod{m}$.

(4) Pokud $a \equiv b \pmod{m}$ a $c \equiv d \pmod{m}$, potom $a + c \equiv b + d \pmod{m}$ a $ac \equiv bd \pmod{m}$.

(5) Pokud $a \equiv b \pmod{m}$, potom $a^n \equiv b^n \pmod{m}$ pro libovolné n přirozené.

Řešení.

(1) Z definice kongruence to znamená totéž jako $m \mid a - 0$.

(2) Jestliže $m \mid a - b$, pak $m \mid (a + k) - (b + k)$ a $m \mid k(a - b)$.

(3) – (5) Ostatní body se dokáží stejně přímočaře. Stačí přepsat kongruenci podle definice.

Tyto úvahy se dají jednoduše zužitkovat například při řešení diofantických rovnic (tj. rovnic, u kterých hledáme řešení z oboru přirozených nebo celých čísel). Nyní si ukážeme dva příklady, jak se dají kongruence použít:

Příklad. Vyřeš rovnici $2x + 3 = 4z + 6y$, kde $x, y, z \in \mathbb{N}$.

Řešení. Pokud pro nějaká čísla platí rovnost, určitě musí platit rovnost i modulo libovolné přirozené číslo. Podíváme se tedy na rovnici modulo dva. Vidíme, že po dělení dvěma dává levá strana vždy zbytek jedna, zatímco pravá strana dává vždy zbytek nula, proto rovnost nikdy nemůže platit. Ekvivalentně bychom mohli říct, že levá strana rovnice je vždy liché číslo, zatímco pravá strana je vždy číslo sudé.

Příklad. Vyřeš rovnici $3x + 3 = 4^z + 6y$, kde $x, y, z \in \mathbb{N}$.

Řešení. Opět se na rovnici podíváme modulo nějaké číslo, tentokrát modulo tři. Vidíme, že levá strana je vždy kongruentní s nulou, zatímco pravá strana s $4^z \equiv 1^z = 1$, rovnice tedy nemůže mít žádné řešení.

Při řešení příkladů se často využívá i toho, že druhé mocniny nabývají pouze nějakých zbytků modulo m. Ukážeme si to na příkladu:

Příklad. Najdi všechna přirozená čísla x splňující $x^2 \equiv 2 \pmod 3$.

Řešení. Projdeme všechny možnosti čísla x.

(1) Číslo $x \equiv 0 \pmod 3$. Potom určitě $x^2 \equiv 0^2 \equiv 0 \pmod 3$ a x není řešením této rovnice.
(2) Číslo $x \equiv 1 \pmod 3$. Potom $x^2 \equiv 1^2 \equiv 1 \pmod 3$ a x není řešením rovnice.
(3) Číslo $x \equiv 2 \pmod 3$. Potom $x^2 \equiv 2^2 \equiv 1 \pmod 3$ a x opět není řešením rovnice.

Jiné možnosti už pro číslo x nejsou, rovnice tedy nemá žádné řešení. Kdybys odvození s kongruencemi nevěřil(a), zkus si třeba třetí případ napsat takto: $x = 3k + 2$. Potom $x^2 = (3k + 2)^2 = 9k^2 + 6k + 4 \equiv 1 \pmod 3$. Výsledek je stejný, ale postup s kongruencemi je snazší a elegantnější. Uvědom si, že nevyužíváme nic složitějšího než bod (5) úvodního cvičení.

Viděli jsme, že druhé mocniny přirozených čísel nabývají po dělení třemi pouze zbytků 0 a 1. Tato čísla nazýváme *kvadratickými zbytky* modulo 3. Stejně se dají definovat kvadratické zbytky pro libovolné přirozené číslo. Pokud se o nich chceš dozvědět něco víc, podívej se do některých zdrojů uvedených na konci tohoto textu.

Na závěr si ukážeme jednu trochu těžší větu, kterou můžeš bez důkazu používat ve svých řešeních.

Věta. (Malá Fermatova věta) *Je-li p prvočíslo a a přirozené číslo nedělitelné p, potom*

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

Zobecněním této věty pro obecný modul je Eulerova věta. Její znění nalezneš v loňském seriálu o teorii čísel.

Pokud Tě kongruence zaujaly a chtěl(a) by ses o teorii čísel dozvědět něco víc, loňský seriál si určitě přečti. Najdeš ho na našich stránkách v sekci "Minulé ročníky".

Přejeme Ti hodně zdaru při řešení třetí série!