Kongruence a teorie čísel

Víťa Kala

Teorie čísel se zabývá vztahy mezi celými čísly, zejména pak dělitelností. Na přednášce se tedy seznámíme se základními pojmy a tvrzeními, ale také s tím, k čemu se nám vlastně můžou (třeba v matematické olympiádě nebo v PraSátku) hodit.

Velmi důležitým pojmem v teorii čísel je **kongruence**.

Definice. *Mějme celá čísla a a b a přirozené číslo n. Pokud $n|(a-b)$, řekneme, že čísla a a b jsou kongruentní podle modulu n (případně kongruentní modulo n), a píšeme $a \equiv b \pmod{n}$.*

S kongruencemi se dá pracovat skoro stejně jako s rovnicemi. K oběma stranám kongruence můžeme přičíst (nebo odečíst) libovolné celé číslo a můžeme je vynásobit jakýmkoli nenulovým číslem. Dělit je ale možné jen čísly nesoudělnými s modulem (tak se říká tomu číslu n z předchozí definice). Také můžeme sečíst, odečíst nebo vynásobit libovolné dvě kongruence podle stejného modulu.

O kongruencích platí několik zajímavých tvrzení, která si na přednášce pořádně vysvětlíme:

Věta. (malá Fermatova) *Mějme přirozené číslo a a prvočíslo p, které nedělí a. Potom platí $a^{p-1} \equiv 1 \pmod{p}$.*

Definice. (Eulerova funkce) *Ať je n přirozené číslo. Počet všech s n nesoudělných přirozených čísel, jež jsou menší nebo rovna n, značíme $\varphi(n)$. Této funkci říkáme Eulerova.*

Věta. *Ať je n přirozené číslo větší než 1 a ať je $n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k}$ jeho rozklad na součin prvočísel ($p_1, p_2, \ldots, p_k$ jsou po dvou různá prvočísla, $\alpha_1, \alpha_2, \ldots, \alpha_k$ jsou přirozená čísla). Potom platí $\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k})$.*

Věta. (Eulerova) *Buďte a celé číslo a m přirozené číslo nesoudělné s a. Potom platí $a^{\varphi(m)} \equiv 1 \pmod{m}$.*

Věta. (Wilsonova) *Mějme přirozené číslo n různé od 1. Potom platí: n je prvočíslo právě tehdy, když $(n-1)! \equiv -1 \pmod{n}$.*

Abyste si nemysleli, že v celé teorii čísel jde jen o kongruence, uveďme si ještě pár zajímavých pojmů a tvrzení.

Definice. *Uvažujme jakékoliv reálné číslo x. Symbolem $\lfloor x \rfloor$ označujeme jeho dolní celou část, tedy to celé číslo, pro něž platí $x - 1 < \lfloor x \rfloor \leq x$. Obdobně symbolem $\lceil x \rceil$*

značíme horní celou část x, která splňuje $x \leq \lceil x \rceil < x + 1$. A konečně $\{x\}$ (někdy ale též $\langle x \rangle$) je desetinná (případně necelá) část x, pro niž platí $\{x\} = x - \lfloor x \rfloor$.

Věta. (Bezoutova) *Nechť jsou a a b celá čísla, jejich největšího společného dělitele značme $d = (a, b)$. Potom existují celá čísla x a y taková, že $ax + by = d$.*