Povídání ke třetí podzimní sérii

Ve třetí sérii s námi budeš pronikat do tajů dělitelnosti. Určitě Tě nepřekvapí, že dělitelnost je ústřední pojem teorie čísel a (nejenom) v úlohách se vyskytuje velmi často. I když už o dělitelnosti jistě něco víš, připravili jsme si pro Tebe úvodní text, který jistě oceníš při řešení úloh třetí série.

Úmluva. V celé sérii budeme pracovat pouze s celými čísly, občas budeme dokonce požadovat, aby byla přirozená.

Dělitelnost

Řekneme, že číslo a je *dělitelné* číslem b, pokud existuje přirozené číslo k takové, že $a = kb$. Stejně tak můžeme říci, že b *dělí* a. Symbolicky pak dělitelnost zapisujeme jako $b \mid a$. Můžeme také říci, že a je *násobkem* b nebo že b je *dělitelem* a. Dělitelnost splňuje několik hezkých vlastností, které si nyní uvedeme.

Cvičení. Rozmysli si, že platí následující vlastnosti dělitelnosti:

(i) $1 \mid a$ a $a \mid 0$.
(ii) Pokud $ab \mid c$, potom $a \mid c$.
(iii) Pokud $a \mid b$, potom $a \mid bc$ pro libovolné celé c.
(iv) Pokud $a \mid b$ a $a \mid c$, potom $a \mid b + c$. (Obecně tedy $a \mid kb + lc$ pro libovolná celá čísla k, l)
(v) Pokud $a \mid b$ a $b \mid c$, potom $a \mid c$. (Proto si můžeme dovolit zkrácený zápis $a \mid b \mid c$)
(vi) Pokud $a \mid b$ a $c \mid d$, potom $ac \mid bd$.
(vii) Pokud $a \mid b$ a $b \neq 0$, potom $|a| \leq |b|$.

Kongruence

Zcela jistě víš, že se čísla dají rozdělit na sudá a lichá. Kongruence je pokročilejší nástroj, který zobecňuje dělení na sudá a lichá rozdělením čísel do skupinek podle zbytků po dělení nějakým číslem.

Definice. Čísla a, b nazveme *kongruentní modulo* n, pokud platí $n \mid b - a$. Zapisujeme $a \equiv b \pmod{n}$.

Značení kongruencí není náhodné – kongruence můžeme sčítat, odčítat, násobit, umocňovat a za určitých předpokladů i dělit jako klasické rovnice. Pokud se chceš o kongruencích dozvědět něco více, odkážeme Tě na úvodní text k 3. podzimní sérii 34. ročníku[1], která se tomuto tématu věnovala.

[1] http://mks.mff.cuni.cz/common/show.php?title=Kongruence&file=archive/34/uvod3p

Se znalostí zápisu pomocí kongruencí se také dá zformulovat několik těžších vět, které ve svých řešeních můžeš používat bez důkazu.

Věta. (Malá Fermatova věta) *Pro libovolné prvočíslo p a libovolné a platí*

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

Věta. (Wilsonova věta) *Pro libovolné prvočíslo p platí*

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

Pár příkladů na závěr

Úloha. Dokažte, že 6 dělí $n^3 - n$ pro všechna celá n.

Řešení. Uvědomíme si, že nám stačí dokázat dělitelnost výrazu dvěma a třemi. Výraz $n^3 - n$ se dá rozložit jako $(n-1) \cdot n \cdot (n+1)$, což je součin tří po sobě jdoucích čísel. Z nich musí jedno být dělitelné třemi, protože to jsou tři po sobě jdoucí čísla, a aspoň jedno dělitelné dvěma, čímž máme dokázáno.

Úloha. Je známo, že 27 dělí číslo s desítkovým zápisem $\overline{abc}$. Dokažte, že 27 dělí i čísla s desítkovými zápisy $\overline{bca}$ a $\overline{cab}$.

Řešení. Podmínka v zadání nám říká, že $27 \mid 100a + 10b + c$. Číslo $\overline{abc}$ je zároveň dělitelné i třemi. Z kritéria dělitelnosti třemi dostaneme $3 \mid a+b+c$, což po vynásobení devíti dává $27 \mid 9a+9b+9c$. Nyní zkombinujeme předchozí vztahy a využijeme toho, že pokud 27 dělí každý sčítanec, pak už dělí i samotný součet.

$$\begin{aligned}
&27 \mid (100a + 10b + c) - 10 \cdot (9a + 9b + 9c) + 27 \cdot (3b) + 27 \cdot (7c), \\
&27 \mid 10a + b + 100c, \\
&27 \mid \overline{cab}.
\end{aligned}$$

Konečně důkaz vztahu $27 \mid \overline{bca}$ je velmi podobný postupu výše a určitě ho zvládneš provést samostatně.

Přejeme Ti hodně zdaru při řešení třetí série!