Počítání modulo p

Pepa Tkadlec

Abstrakt. Příspěvek uvádí Malou Fermatovu větu, Wilsonovu větu a několik úloh, v nichž lze s výhodou uplatnit to, že na množině zbytkových tříd po dělení prvočíslem lze nejen sčítat, odčítat a násobit, ale i dělit.

Úmluva. Nebude-li řečeno jinak, jsou všechny níže uvedené proměnné z oboru celých čísel.

Teorie

Definice. (Dělitelnost) Řekneme, že číslo a *je dělitelem* čísla b, jestliže existuje číslo c takové, že $a \cdot c = b$. Píšeme $a \mid b$.

Definice. (Kongruence) Řekneme, že čísla a, b jsou *kongruentní modulo* d, jestliže dávají stejný zbytek po dělení číslem d (tj. jestliže $d \mid a - b$). Píšeme $a \equiv b \pmod{d}$.

Definice. ($\mathbb{Z}_p$) Buď p prvočíslo. Množinu $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ nazýváme *úplnou sadou zbytků* modulo p.

Tvrzení. *Prvky množiny $\mathbb{Z}_p$ lze přirozeně sčítat, odčítat a násobit.*

Tvrzení. (Stěžejní) *Buď p prvočíslo. Nenulovým násobkem $\mathbb{Z}_p$ je opět $\mathbb{Z}_p$. Jinými slovy je-li p prvočíslo, pak pro každé $a \in \mathbb{Z}_p$, $a \neq 0$ platí*

$$\{a \cdot 0, a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)\} = \{0, 1, 2, \ldots, p-1\}.$$

Důsledek. („Zbytky lze dělit“) Buď p prvočíslo a $a \in \mathbb{Z}_p$, $a \neq 0$. Pak existuje právě jedno $b \in \mathbb{Z}_p$ takové, že $ab \equiv 1 \pmod{p}$.

Věta. (Malá Fermatova) *Buď p prvočíslo a a číslo s ním nesoudělné. Pak*

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

Věta. (Wilsonova) *Buď p prvočíslo. Pak* $(p-1)! \equiv -1 \pmod{p}$.

Příklady

Příklad 1. Buď p prvočíslo a $0 < k < p$.

(i) Ukažte, že kombinační číslo $\binom{p}{k}$ je násobkem p.

(ii) Jaký zbytek dává $\binom{p}{k}$ po dělení číslem p^2?

Příklad 2. Určete všechna kladná celá čísla, která jsou nesoudělná s každým členem posloupnosti

$$a_n = 2^n + 3^n + 6^n - 1 \quad (n = 1, 2, \dots).$$

(IMO 2005)

Příklad 3. Buď $p \geq 3$ prvočíslo. Dokažte, že je-li

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} = \frac{m}{n},$$

pak m je násobkem p.

Příklad 4. Dokažte, že jsou-li p, q přirozená čísla taková, že

$$\frac{p}{q} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots - \frac{1}{1318} + \frac{1}{1319},$$

pak p je dělitelné číslem 1979. (IMO 1979)

Příklad 5. Najděte všechna prvočísla p, pro která je číslo

$$\binom{p}{1}^2 + \binom{p}{2}^2 + \cdots + \binom{p}{p-1}^2$$

dělitelné číslem p^3. (CPS 2008)

Příklad 6. Pro liché prvočíslo p dokažte

$$1^{p-2} + 2^{p-2} + \cdots + \left(\frac{p-1}{2}\right)^{p-2} \equiv \frac{2 - 2^p}{p} \pmod{p}.$$

(*i*KS 2012, N3)

Příklad 7. (Wolstenholmova věta) Buď $p \geq 5$ prvočíslo. Dokažte, že je-li

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} = \frac{m}{n},$$

pak m je dokonce násobkem p^2.