Malá Fermatova a Eulerova veta

Jozef Rajník

Na prednáške budeme pracovať so zvyškami po delení celých čísel. Na množine zvyškov po delení nejakým číslom d vieme predpísať, ako sa s nimi počíta – ako sa sčítavajú (a z toho nám vychádza aj násobenie) a ako sa násobia (a z toho nám vychdáza, ako sa delia, ak je d prvočíslo).

Zaujímavosť pre rozšírenie obzoru. Tento proces definovania nejakého počítania na nejakej množine je vo vysokoškolskej matematike podchytený pojmom grupa. Čo presne to je? Zoberieme si ľubovoľnú množinu M a na nej si definujeme operáciu $\star$. Teda pre každú dvojicu (nie nutne rôznych) prvkov $a, b \in M$ predpíšeme, aký je výsledok operácie $a \star b$. Aby, sme dostali grupu, musíme pri tom dodržať nasledovné podmienky:

- Pre nejaký prvok $n \in M$ platí $\forall m \in M\colon n \star m = n$. Takýto prvok sa nazýva *neutrálny prvok*.
- Pre každý prvok $m \in M$ existuje prvok $i \in M$, pre ktorý platí $m \star i = i \star m = n$ (kde n je neutárlny prvok). Tento prvok i sa nazýva *inverzný prvok* k prvku m a zvykne sa označovať m^{-1}, príp. niekedy aj $-m$.
- Pre každé $a, b, c \in M$ platí $a \star (b \star c) = (a \star b) \star c$, teda tzv. *asociatívny zákon*.
- Ešte máme jedno nepovinnú podmienku: pre všetky $a, b \in M$ platí $a \star b = b \star a$, teda operácia $\star$ je *komutatívna*.

Ak platia všetky štyri podmienky, tak hovoríme o *komutatívnej* alebo aj *Abelovskej* grupe. Grupa však vo všeobecnosti komutatívna byť nemusí.

Príklady grúp

- $M = \mathbb{Z}$ a $a \star b = a + b$;
- $M = \mathbb{Q}$ a $a \star b = a + b$;
- $M = \mathbb{Q}$ a $a \star b = a \cdot b$ (pozor, tu nemôžeme $\mathbb{Q}$ nahradiť za $\mathbb{Z}$);
- predošlé príklady na množinách $\mathbb{R}$, $\mathbb{C}$ alebo aj $\{a + b\sqrt{2};\ a, b \in \mathbb{Q}\}$;
- $M = \{0, 1, \ldots, d-1\}$ a $a \star b = (a + b) \bmod d$ – táto grupa sa nazýva aj $\mathbb{Z}_d$.
- $M = 1, 2, \ldots, p-1$ a $a \star b = (a \cdot b) \bmod p$, kde p je prvočíslo – nazýva sa aj $\mathbb{Z}_p^*$.

Veta 1 (Malá Fermatova)**.** Pre každé prvočíslo p a každé celé číslo n, ktoré nie je deliteľné p platí

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

Pre prirodzené číslo n definujeme číslo $\varphi(n)$ ako počet prirodzených čísel menších ako n, ktoré sú s číslom n nesúdeliteľné.

Veta 2 (Eulerova)**.** Pre každé nesúdeliteľné prirodzené čísla n, a platí

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$