Kvadratické (a jiné) zbytky

Lukáš Zavřel

Abstrakt. Tento příspěvek seznamuje s úplně základními vlastnostmi zbytků čtverců po dělení různými čísly a na jednoduchých až středně těžkých úlohách ukazuje využití těchto zbytků.

Všechna čísla v tomto příspěvku jsou přirozená.

Definice. Nechť $a \in \mathbb{Z}$ a $n \in \mathbb{N}$. Řekneme, že a je *kvadratickým zbytkem* modulo n, pokud existuje $c \in \mathbb{N}$ takové, že $c^2 \equiv a \pmod{n}$. V opačném případě řekneme, že a je *kvadratickým nezbytkem*. Podobně definujeme zbytky kubické i vyšších řádů.

Zajímavé výsledky často dostaneme, zvolíme-li za modulo n z předchozí definice takové číslo, aby počet kvadratických (případně kubických či jiných) zbytků byl co nejmenší. V praxi se pro kvadratické zbytky často používají hodnoty $n = 4$ (jediné možné kvadratické zbytky jsou pak 0 a 1) a $n = 8$ (0, 1 a 4). Pro kubické zbytky se vyplatí zkusit $n = 7$ (zbytky 0, 1, 6) či $n = 9$ (0, 1, 8).

Lemma. (Počet kvadratických zbytků) *Nechť p je liché prvočíslo. Pak mezi čísly $1, 2, \ldots, p-1$ je právě $\frac{p-1}{2}$ kvadratických zbytků modulo p a stejně tolik kvadratických nezbytků.*

Velmi lehké příklady

Příklad 1. Dokažte, že pokud 7 dělí $a^2 + b^2$, poté 7 dělí a i b. Dokažte, že obdobné tvrzení pro pětku neplatí.

Příklad 2. Dokažte, že čísla tvaru $4k + 3$ nejdou zapsat jako součet dvou čtverců.

Příklad 3. Najděte všechna řešení rovnice $1! + 2! + \cdots + n! = x^2$.

Příklad 4. Najděte všechna řešení rovnice $x^2 + y^2 + z^2 = 2007$.

Klíčová slova. diofantické rovnice, kvadratické zbytky, modulo, teorie čísel

Lehké příklady

Příklad 5. Mějme $x^2 + y^2 = z^2$. Dokažte, že hodnota alespoň jedné z neznámých x, y, z je dělitelná třemi, alespoň jedna čtyřmi a alespoň jedna pěti.

Příklad 6. Mějme čísla x, y, z taková, že $x^3 + y^3 = z^3$. Dokažte, že alespoň jedno z nich je dělitelné sedmi.

Příklad 7. Dokažte, že součet tří, čtyř, pěti ani šesti čtverců po sobě jdoucích čísel není čtverec.

Méně lehké

Příklad 8. Pepa s Lukášem mají stádo oveček. Jednoho krásného dne ale okolo jejich pastviny jel bohatý developer a rozhodl se, že stádo koupí. Pastýři se dohodli a nakonec souhlasili s tím že každá ovečka bude stát tolik, kolik jich je ve stádu.

Manažer tedy vytáhl jednoeurové mince a začal je mezi Pepu s Lukášem rozdělovat. Deset Pepovi, deset Lukášovi, deset Pepovi... Až dal nakonec deset mincí Pepovi a částku menší než 10 Euro Lukášovi. Pepa proto vytáhl z kapsy nůž a podal ho Lukášovi se slovy: „Nyní jsme si kvit.“ Kolik stál nůž?

Příklad 9. *Lagrangeova věta o čtyřech čtvercích* tvrdí, že každé číslo lze zapsat jako součet nejvýše čtyř druhých mocnin. Dokažte, že tři by nestačily.

Příklad 10. Najděte všechna řešení rovnice $n! + 5 = x^3$.

Příklad 11. Uvažujme prvočísla $n_1 < n_2 < \cdots < n_{31}$. Dokažte, že pokud 30 dělí $n_1^4 + n_2^4 + \cdots + n_{31}^4$, potom se mezi těmito prvočísly vyskytují tři po sobě jdoucí.
(Rumunsko 2003)

Lehce těžké

Příklad 12. Dokažte, že pokud dva čtverce jdou zapsat jako $4x - 3y$ a $4y + 3x$, kde x, y jsou přirozená čísla, pak jsou oba dva dělitelné pěti. (PraSe 29, 7)

Příklad 13. Najděte všechna řešení rovnice $2^n + 12^n + 2011^n = x^2$.
(USAJMO 2011)

Příklad 14. Mějme množinu čtyř čísel $\{2, 5, 13, d\}$, kde $d \in \mathbb{N}$, $d \neq 2, 5, 13$. Dokažte, že si umíme zvolit dvě různá čísla a, b z této množiny taková, že $ab - 1$ nebude čtverec. (IMO 1986)

Literatura

Čerpal jsem ze staršího příspěvku *Jakuba „šnEka“ Opršala* na totéž téma a z knihy

[1] Titu Andreescu, Dorin Andrica, Zuming Feng: *104 Number Theory Problems*, Birkhäuser, Boston, 2007.