Kvadratická reciprocita

Filip Bialas

Abstrakt. Zákon kvadratické reciprocity je zajímavá věta z teorie čísel. Jako první ji dokázal Carl Fridrich Gauss v roce 1796, který si tuto větu velmi oblíbil – za svůj život vydal hned osm různých důkazů a označoval ji za *Zlatou větu*. V tomto příspěvku si ji dokážeme a následně ji budeme aplikovat na zajímavé příklady, mimo jiné i na pár speciálních případů Dirichletovy věty.

Definice. Číslo a nazveme *kvadratickým zbytkem* modulo m, pokud existuje celé x takové, že $x^2 \equiv a \pmod{m}$. Zbylým číslům říkáme *kvadratické nezbytky.*

Definice. Nechť p je liché prvočíslo a $a \in \mathbb{Z}$, pak definujeme *Legendreův symbol* $\left(\frac{a}{p}\right)$ následovně:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{pro } p \mid a \\ +1 & \text{pokud } a \text{ je kvadratickým zbytkem a } p \nmid a \\ -1 & \text{pokud } a \text{ není kvadratickym zbytkem} \end{cases}$$

Nyní si ukážeme několik způsobů, jak můžeme spočítat, zda je něco kvadratický zbytek modulo nějaké prvočíslo, nebo ne. Třešničkou na dortu bude poté zákon kvadratické reciprocity, který dává pro různá lichá prvočísla p, q jednoduchý vztah mezi $\left(\frac{p}{q}\right)$ a $\left(\frac{q}{p}\right)$.

Tvrzení. (Eulerovo kritérium) *Nechť p je liché prvočíslo a $a \in \mathbb{Z}$. Pak* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Tvrzení. (Multiplikativita Legendrova symbolu) *Nechť p je liché prvočíslo a $a, b \in \mathbb{Z}$. Pak* $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Tvrzení. *Nechť p je liché prvočíslo, pak* $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Tvrzení. (Gaussovo lemma) *Ať p je liché prvočíslo a a celé číslo s ním nesoudělné. Označme n počet takových čísel $k \in \{1, 2, \ldots, \frac{p-1}{2}\}$, že ak dává po dělení p větší zbytek než $\frac{p}{2}$. Pak* $\left(\frac{a}{p}\right) = (-1)^n$.

Věta. (Zákon kvadratické reciprocity) *Nechť p, q jsou dvě různá lichá prvočísla. Pak* $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.

Speciální případy Dirichletovy věty

Úloha 1. Dokažte, že existuje nekonečně mnoho prvočísel.

Řešení. Předpokládejme pro spor, že by jich bylo jen konečně mnoho. Označme si je $p_1, p_2, \ldots, p_n$. Potom $p_1 p_2 \ldots p_n + 1$ je přirozené číslo větší než jedna, které dává modulo každé z prvočísel zbytek 1, takže není žádným z nich dělitelné. Tedy musí být dělitelné jiným prvočíslem, což je ve sporu s tím, že máme všechny.

Podobně a celkem jednoduše můžeme tvrzení o nekonečném počtu prvočísel dokázat i pro prvočísla vybraná, která jsou obsažena ve speciálních aritmetických posloupnostech. Musíme ale při volbě čísla, které není dělitelné žádným ze zvolených prvočísel, nějak zaručit, aby skutečně muselo být dělitelné některým dalším zvoleného tvaru a ne pouze prvočísly jinými. K tomu se nám bude hodit vypracovaná teorie kvadratických zbytků.

Obecně se dá ukázat, že v každé aritmetické posloupnosti $an + b$, kde a, b jsou nesoudělná přirozená čísla, se nachází nekonečně mnoho prvočísel. Tomuto výsledku se říká *Dirichletova věta*, její důkaz je ale bohužel příliš obtížný na to, abychom si ho zde ukázali.

Příklad 2. Dokažte, že existuje nekonečně mnoho prvočísel tvaru $4k + 3$.

Příklad 3. Dokažte, že existuje nekonečně mnoho prvočísel tvaru $3k + 2$.

Příklad 4. Dokažte, že existuje nekonečně mnoho prvočísel tvaru $4k + 1$.

Příklad 5. Dokažte, že existuje nekonečně mnoho prvočísel tvaru $3k + 1$.

Příklad 6. Dokažte, že existuje nekonečně mnoho prvočísel tvaru $5k + 4$.

Příklad 7. Dokažte, že existuje nekonečně mnoho prvočísel tvar $8k + 1$.

Příklad 8. Dokažte, že existuje nekonečně mnoho prvočísel tvaru $8k + 3$.

Další příklady

Příklad 9. Ukažte, že $2^n + 1$, kde n je přirozené číslo, nemá žádné prvočíselné dělitele tvaru $8k - 1$. (Vietnam TST 2004)

Příklad 10. Dokažte, že pro všechna lichá prvočísla p je nejmenší kvadratický nezbytek menší než $1 + \sqrt{p}$.

Příklad 11. Dokažte, že neexistuje přirozené číslo a takové, že $2^a - 1$, $2^{2a+1} - 1$, $2^{4a+3} - 1$ jsou všechna prvočísla.

Příklad 12. Dokažte, že pokud prvočíslo $p \mid n^2 + n - 1$ pro nějaké přirozené n, pak $p = 5$ nebo $5 \mid p^2 - 1$.

Příklad 13. Najděte všechny dvojice přirozených čísel (m, n) takových, že

$$m^6 = n^{n+1} + n - 1.$$

(iKS 4–3–N3)

Příklad 14. Nechť a je přirozené číslo, které není čtverec. Pak $\left(\frac{a}{p}\right) = -1$ pro nekonečně mnoho prvočísel p.

Příklad 15. Nechť $f(x)$ je kvadratický polynom s celočíselnými koeficienty takový, že pro každé prvočíslo p existuje přirozené n, pro které platí $p|f(n)$. Dokažte, že má f racionální kořeny.

Návody

2. Zvolte $4p_1p_2 \dots p_n + 3$.

3. Zvolte $3p_1p_2 \dots p_n + 2$.

4. Zvolte $(2p_1p_2 \dots p_n)^2 + 1$.

5. Zvolte $(2p_1p_2 \dots p_n)^2 + 3$.

6. Zvolte buď $(2p_1p_2 \dots p_n)^2 - 5$, nebo $(4p_1p_2 \dots p_n)^2 - 5$.

7. Zvolte $(2p_1p_2 \dots p_n)^4 + 1$.

8. Zvolte $(2p_1p_2 \dots p_n)^2 + 2$.

9. Pokud je n liché, tak vynásobte výraz dvěma, aby byl 2^n čtverec.

11. Nutně musí být i $2a + 1, 4a + 3$ prvočísla – pracujte v jejich modulu.

12. Prvočíslo p musí dělit i $4(n^2 + n - 1) = (2n + 1)^2 - 5$.

13. Odhady dojdeme k $n \equiv 0$ nebo $n \equiv 4 \mod 6$. Spočítáme, že pak pravá strana není kvadratický zbytek modulo $n + 1$.

14. Kouzlení s kvadratickou reciprocitou.

15. Stačí ukázat, že je diskriminant čtverec. Ukažte, že je kvadratický zbytek modulo každé prvočíslo, což bude spor s minulým příkladem.

Literatura a zdroje

[1] Titu Andreescu, Gabriel Dospinescu: *Problems from the Book*, XYZ Press, 2010.

[2] Alexandru Gica, David Hruška: *Modular Arithmetics*, Awesome Math Summer Program, Cornell University, 2017.