Kvadratické zbytky

Matěj Doležálek

Abstrakt. Když se v úloze sejdou druhé mocniny s nějakou dělitelností či kongruencí, často přijde ke slovu jednoduchý fenomén – ne všechny zbytky lze získat ze čtverců. V tomto příspěvku si ukážeme, jak toho využít v „řešení“ diofantických rovnic, a vybudujeme teoretické nástroje k rozhodování, které zbytky jsou kvadratické a které nikoliv. Po cestě vyřešíme spoustu úloh, od jednoduchých hříček až po tvrdé oříšky vyžadující k vyřešení silné kanóny.

Úmluva. Není-li řečeno jinak, uvažovaná čísla jsou celá.

Definice. Řekneme, že a *je kongruentní* b *modulo* m, pokud $m \mid a - b$. Tuto skutečnost zapisujeme $a \equiv b \pmod{m}$.

Definice. Řekneme, že a je *kvadratický zbytek modulo* m, pokud existuje x splňující $a \equiv x^2 \pmod{m}$. V opačném případě řekneme, že a je *kvadratický nezbytek* modulo m.

Cvičení. Najdi všechny kvadratické zbytky modulo m pro $m \in \{3, 4, 5, 7, 8, 9\}$.

Triky s rovnicemi

Každá celočíselná rovnice musí zůstat v platnosti, když ji zeslabíme na kongruenci modulo libovolné číslo. Pokud tedy chceme dokázat, že nějaká rovnice nebo její podpřípad nemá řešení, může nám pomoci vhodně zvolené modulo – pokud by existence řešení vedla k tomu, že nějaký známý kvadratický nezbytek má být kvadratickým zbytkem, dostaneme spor. Dobré volby modula často odstraní nebo zjednoduší nějakou část výrazu.

Úloha 1. Nahlédni, že rovnice $7x^2 + 5y + 14 = 0$ nemá celočíselné řešení.

Úloha 2. Najdi všechny dvojice prvočísel p, q, jež splňují $p^2 = 2q^2 + 1$.

Úloha 3. Nahlédni, že rovnice $x^2 = 3 - 8z + 2y^2$ nemá celočíselné řešení.

Úloha 4. Nahlédni, že čísla tvaru $4^a(8b + 7)$ se nedají vyjádřit jako součet tří čtverců celých čísel.

Úloha 5. Najdi všechna celočíselná řešení rovnice $x^2 + 5y^2 = 11z^2$.

Úloha 6. Řeš v přirozených číslech rovnici $a^2 = 1! + 2! + \cdots + b!$.

Úloha 7. 3000ciferné přirozené číslo je v desítkové soustavě v nějakém pořadí zapsáno tisíci čtyřkami, tisíci jedničkami a tisíci nulami. Může to být čtverec?

Úloha 8. Nahlédni, že rovnice $x^4 + y^4 = z^4 + 4$ nemá celočíselné řešení.

Úloha 9. Pro která n lze tabulku $n \times n$ vyplnit čísly 1 až n^2 tak, aby součet každého řádku i součet každého sloupce byly násobky sedmi?

Úloha 10. Najdi všechny dvojice prvočísel p, q, jež splňují $p^5 - q^3 = (p+q)^2$.

Kvadratické zbytky modulo p a Legendreův symbol

Prvočísla zaujímají výsadní postavení všude tam, kde přichází do hry jakákoliv dělitelnost. Nepřekvapí tedy, že i v kontextu kvadratických zbytků bývá nejpříjemnější počítat modulo prvočíslo. *Legendreův symbol* pak zjednodušuje rozpoznávání kvadratických zbytků od nezbytků.

Věta. (malá Fermatova) *Pro $a \in \mathbb{Z}$ a prvočíslo $p \nmid a$ platí* $a^{p-1} \equiv 1 \pmod{p}$.

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

Definice. Pro $a \in \mathbb{Z}$ a prvočíslo p definujeme *Legendreův symbol* jako

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{pokud } p \mid a, \\ 1, & \text{pokud } a \not\equiv 0 \text{ je kvadratický zbytek mod } p, \\ -1, & \text{pokud } a \not\equiv 0 \text{ je kvadratický nezbytek mod } p. \end{cases}$$

Tvrzení. (Eulerovo kritérium) *Pro liché prvočíslo p platí* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Cvičení. Legendreův symbol je *úplně multiplikativní*, tedy pro $a, b \in \mathbb{Z}$ a prvočíslo p platí $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Cvičení. Modulo liché prvočíslo p existuje $\frac{p+1}{2}$ různých kvadratických zbytků (včetně nuly) a $\frac{p-1}{2}$ různých nezbytků.

Úloha 11. Nahlédni, že pro každé přirozené n a prvočíslo p má kongruence $n \equiv x^2 + y^2 \pmod{p}$ řešení.

Úloha 12. V závislosti na prvočísle p urči součet všech kvadratických zbytků modulo p.

Úloha 13. Je dáno liché prvočíslo p. Kolik z čísel $x \in \{1, \ldots, p-2\}$ splňuje, že x i $x+1$ jsou kvadratické zbytky?

Úloha 14. Dokaž, že existuje nekonečně mnoho prvočísel tvaru $4k+1$.

Úloha 15. Rozhodni, zda má rovnice $x^5 = y^2 + 4$ celočíselné řešení.

Úloha 16. Najdi všechna přirozená čísla, pro něž je $n! + 5$ třetí mocninou celého čísla.

Cvičení. (Gaussovo lemma) Je dáno $a \in \mathbb{Z}$ a liché prvočíslo $p \nmid a$. Uvažujme taková čísla $i \in \{1, 2, \ldots, \frac{p-1}{2}\}$, která splňují $a \cdot i \in \{\frac{p+1}{2}, \ldots, p-1\} \pmod p$. Označme n počet všech takových i. Potom platí $\left(\frac{a}{p}\right) = (-1)^n$.

Úloha 17. Buď p prvočíslo tvaru $4k+3$. Nahlédni, že $\left(\frac{p-1}{2}\right)! \equiv (-1)^{|N|} \pmod p$, kde N je množina kvadratických nezbytků mezi čísly 1 až $\frac{p-1}{2}$.

Úloha 18. Dokaž, že pro každé liché prvočíslo p existuje přirozené $a < \sqrt{p} + 1$, které je kvadratickým nezbytkem modulo p.

Úloha 19. Nechť $a_1, \ldots, a_{\frac{p-1}{2}}$ jsou všechny nenulové kvadratické zbytky modulo liché prvočíslo p. Zjednoduš modulo p polynom $(x + a_1) \cdots (x + a_{\frac{p-1}{2}})$.

Reciprocita

Eulerovo kritérium a z něj plynoucí multiplikativita Legendreova symbolu dávají dobrý způsob, jak poznat, která a jsou kvadratickými zbytky modulo jedno dané p. Úkonem o úroveň obtížnějším je poznat, modulo která prvočísla p je jedno dané a kvadratickým zbytkem. K tomu se hodí umět dát do vztahu Legendreovy symboly modulo dvě různá prvočísla.

Tvrzení. (zákon kvadratické reciprocity) *Pro lichá prvočísla $p \neq q$ platí*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Ekvivalentní formulace je

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} -1, & \text{pokud } p \equiv q \equiv 3 \pmod 4, \\ 1, & \text{jinak.} \end{cases}$$

Nástin důkazu (podle [7]). Jedna z ekvivalentních formulací Čínské zbytkové věty říká $\mathbb{Z}_{pq}^* \simeq \mathbb{Z}_p^* \times \mathbb{Z}_q^*$, tedy že „počítat mod pq je jako počítat mod p a mod q naráz“. Obě množiny

$$L = \left\{(k,k) : 0 < k < \frac{pq}{2} \text{ a zároveň } p, q \nmid k\right\},$$
$$R = \left\{(a,b) : 0 < a < p \text{ a zároveň } 0 < b < \frac{q}{2}\right\}$$

obsahují právě jeden prvek z každé dvojice $x, -x \in \mathbb{Z}_{pq}^*$, takže

$$\prod_{(k,k)\in L} (k,k) = \pm \prod_{(a,b)\in R} (a,b).$$

To se s pomocí malé Fermatovy věty, Wilsonovy věty a Eulerova kritéria upraví na dvojici rovností – jedna určí $\pm$ a z druhé zbude kvadratická reciprocita.

Detaily pro zájemce na konzultacích. □

Tvrzení. (druhý suplement) *Pro liché prvočíslo p je*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{pokud } p \equiv \pm 1 \pmod 8, \\ -1, & \text{pokud } p \equiv \pm 3 \pmod 8. \end{cases}$$

Důkaz. Stačí nahlédnout z Gaussova lemmatu. □

Jako *první suplement* kvadratické reciprocity se někdy označuje tvrzení

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{pokud } p \equiv 1 \pmod 4, \\ -1, & \text{pokud } p \equiv 3 \pmod 4, \end{cases}$$

což je jen speciální případ Eulerova kritéria.

Kvadratickou reciprocitu se často vyplatí používat v kombinaci s dalšími větami – v tomto příspěvku využijeme Čínskou zbytkovou a Dirichletovu větu.

Věta. (Čínská zbytková) *Jsou-li $m_1, \ldots, m_k$ po dvou nesoudělná přirozená čísla a $a_1, \ldots, a_k$ libovolná celá čísla, pak existuje celé číslo x splňující*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

a všechna taková x jsou si navzájem kongruentní modulo $m_1 \cdots m_k$.

Věta. (Dirichletova) *Je-li a přirozené číslo a b celé číslo nesoudělné s a, pak existuje nekonečně mnoho prvočísel p splňujících $p \equiv b \pmod a$.*

Úloha 20. Dokaž, že pro přirozené n nemá číslo $2^n + 1$ žádné prvočíselné dělitele tvaru $8k - 1$.

Úloha 21. Dokaž, že neexistuje přirozené číslo a takové, že $2^a - 1$, $2^{2a+1} - 1$ i $2^{4a+3} - 1$ jsou prvočísla.

Úloha 22. Je dáno prvočíslo p. Dokaž, že dělitelnost $p \mid n^2 + n - 1$ má řešení, právě když $5 \mid p(p^2 - 1)$.

Úloha 23. Dokaž, že kongruence $x^8 \equiv 16 \pmod p$ má řešení pro každé prvočíslo p.

Úloha 24. Najdi všechna přirozená n splňující $2^n - 1 \mid 3^n - 1$.

Úloha 25. Je dáno prvočíslo p tvaru $4k + 1$. Nahlédni, že $k^k \equiv 1 \pmod p$.

Úloha 26. Nechť celé číslo a není čtverec celého čísla. Dokaž, že pak je a kvadratický nezbytek modulo nějaké prvočíslo q.

Úloha 27. Je dán celočíselný kvadratický polynom, jenž má kořen modulo každé prvočíslo p. Nahlédni, že potom má i racionální kořen.

Úloha 28. Najdi celočíselný polynom, který má kořen modulo každé prvočíslo p, ale nemá racionální kořen.

Úloha 29. Najdi všechna prvočísla p, pro než je $p! + p$ čtverec.

Úloha 30. Dokaž, že přirozená čísla m, n splňující

$$\varphi(5^m - 1) = 5^n - 1$$

musí být soudělná.[1]

Úloha 31. Dokaž, že pro každé liché číslo $n > 1$ lze zvolit taková celá čísla a, b, že označíme-li $f(x) = (x + a)^2 + b$, pak platí:

(i) $\gcd(a, n) = \gcd(b, n) = 1$,
(ii) $f(0)$ je násobkem n,
(iii) ale pro každé přirozené k má $f(k)$ prvočíselného dělitele, který nedělí n.

(USEMO 2020)

Jacobiho symbol

Má-li Legendreův symbol $\left(\frac{a}{p}\right)$ nějakou vadu, pak je to ta, že p musí být (liché) prvočíslo. Tento nedostatek, za cenu ztráty části vypovídací hodnoty o kvadratických zbytcích, napravuje *Jacobiho symbol*, který rozšiřuje definici na všechna lichá přirozená čísla. Hodí se hlavně ke snadnému počítání Legendreových symbolů. V olympiádních úlohách se příliš nevyužije, ale neuškodí jej znát.

Definice. Mějme $a \in \mathbb{Z}$ a liché přirozené n s prvočíselným rozkladem $n = p_1 \cdots p_k$, přičemž p_i se nemusí lišit. Potom *Jacobiho symbol* $\left(\frac{a}{n}\right)$ definujeme pomocí součinu Legendreových symbolů jako

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_k}\right).$$

Tvrzení. (vlastnosti Jacobiho symbolu) *Pro celá a, b a lichá přirozená m, n platí*

(a) $$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right), \qquad \left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right),$$

(b) $$a \equiv b \pmod{n} \implies \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right),$$

(c) $$\mathrm{NSD}(a, n) = 1 \implies \left(\frac{a^2}{n}\right) = 1,$$

(d) $$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}, \qquad \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}},$$

(e) $$\left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2} \cdot \frac{m-1}{2}} \left(\frac{m}{n}\right).$$

[1] φ zde značí Eulerovu funkci $\varphi(n) = n \cdot \prod_{p \mid n} \frac{p-1}{p}$.

Cvičení. Najdi vhodná a, n, aby platilo $\left(\frac{a}{n}\right) = 1$, ale a nebyl kvadratický zbytek modulo n.

Cvičení. Ukaž, že pokud $\left(\frac{a}{n}\right) = -1$, pak už musí a být kvadratický nezbytek modulo n.

Cvičení. Rozmysli si, jak z vlastností (a) až (e) sestavit algoritmus, který počítá Jacobiho symboly v logaritmickém čase.

Úloha 32. Je dáno $a \in \mathbb{Z}$ a prvočíslo $p \nmid a$. Dokaž, že pro každé prvočíslo q splňující $q \equiv \pm p \pmod{4a}$ platí $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

Úloha 33. Najdi všechna řešení rovnice

$$a + b + d^2 = 4abc$$

v přirozených číslech. (Problems from the Book)

Návody

1. Modulo 5.

2. Modulo 4.

3. Modulo 8.

4. Modulo 8.

5. Modulo 11.

6. Najdi dobré modulo, kterým se z pravé strany stane kvadratický nezbytek.

7. Modulo 3.

8. Modulo 8.

9. Uvaž celkový součet v tabulce modulo 7.

10. Modulo 3.

11. Když v $n - y^2$ volíme různá y, vyrobí to spoustu nezbytků.

12. Co se stane, když množinu kvadratických zbytků přenásobíme jedním fixním kvadratickým zbytkem?

13. Upravuj $\sum_{x=1}^{p-2} \left(\left(\frac{x}{p}\right) + 1\right) \cdot \left(\left(\frac{x+1}{p}\right) + 1\right)$.

14. Uprav klasický důkaz existence nekonečně mnoha prvočísel tak, aby vyloučil prvočísla $4k + 3$.

15. Modulo 11.

16. Modulo 7.

17. Zkus do součinu přidat znaménka podobně jako v důkazu Gaussova lemmatu.

18. Je-li a nejmenší nezbytek, uvaž $b = \left\lfloor \frac{p}{a} \right\rfloor + 1$.

19. Koeficienty jsou symetrické výrazy v a_i. Co je něčím přenásobit a zneužít symetrii?

20. Použij první a druhý suplement.

21. S pomocí prvočíselnosti exponentů vyrob Legendreovy symboly.

22. Kdy je 5 kvadratický zbytek modulo p?

23. Rozlož na kvadratické polynomy.

24. Najdi dělitele se špatným $\left(\frac{3}{p}\right)$.

25. Druhý suplement.

26. Klidně polož $q \equiv 1 \pmod 4$ a libovolně navol hodnoty Legendreových symbolů $\left(\frac{p}{q}\right)$ pro $p \mid a$. Pozor na dvojku.

27. Nepomůže předchozí úloha?

28. Využij multiplikativitu Legendreova symbolu.

29. Řekni něco o prvočíslech $q < p$.

30. Popiš prvočíselný rozklad $5^m - 1$ a zbytky jednotlivých prvočísel mod 5.

31. Pokus se zvolit b tak, aby pro velká x byly relevantní valuace čísla $x^2 + b$ omezené.

32. Použij (e), (d) a (b). Pozor na paritu!

33. Využij čtverec k dvojímu vyjádření nějakého Jacobiho symbolu. Bude potřeba trochu rozlišit paritu.

Literatura a zdroje

[1] Filip Bialas: *Kvadratická reciprocita*, Zásada, 2017.
[2] Rado van Švarc: *Úvod do diofantických rovnic*, Lipová-lázně, 2016.
[3] David Hruška: *Kvadratické zbytky*, Sklené, 2015.
[4] Kuba Svoboda: *Diofantické rovnice*, Zásada, 2014.
[5] Alexander „Olin“ Slávik: *Primitivní prvek a kvadratická reciprocita*, *i*KS 2012, Hostětín.
[6] Jakub „šnEk“ Opršal: *Kvadratické zbytky*, Rápotín, 2007.
[7] Leo Goldmakher: *Quadratic reciprocity*, *https://web.williams.edu/Mathematics/lg5/QR.pdf*.
[8] Víťa Kala: *skripta z Teorie čísel*, *https://www.karlin.mff.cuni.cz/˜kala/files/TC22.pdf*.