Lipová-lázně

Sborník, jaro 2022

Fíla Čermák
Matěj Doležálek
Klárka Grinerová
Verča Hladíková
Lenka Kopfová
Terka Kučerová
Anna Mlezivová
Honza Nekarda
Radek Olšák
Daniel Perout
Hedvika Ranošová
Martin Raška
Michal Töpfer
Adéla Karolína Žáčková

Autoři: Fíla Čermák, Matěj Doležálek, Klárka Grinerová, Verča Hladíková, Lenka Kopfová, Terka Kučerová, Anna Mlezivová, Honza Nekarda, Radek Olšák, Daniel Perout, Hedvika Ranošová, Martin Raška, Michal Töpfer, Adéla Karolína Žáčková
Editoři: Matěj Doležálek, Radek Olšák
vydání první, náklad 40 výtisků
duben 2022
Díky za pomoc všem, kterým je za co děkovat.
Realizace projektu byla podpořena Ministerstvem školství, mládeže a tělovýchovy.

Největší společný dělitel

Fíla Čermák

Abstrakt. Největší společný dělitel je základní pojem elementární teorie čísel. I přes svou jednoduchost má nejedno praktické využití, zvláště ve spojení s Eukleidovým algoritmem. V olympiádní matematice nám usnadní řešení spousty příkladů nebo aspoň jejich částí. Tento příspěvek má právě za úkol procvičit techniky jeho výpočtu a jak ho využít při řešení úloh.

Není-li řečeno jinak, číslem budeme myslet celé číslo.

Definice. Řekneme, že číslo $a \neq 0$ *dělí* číslo b (píšeme $a \mid b$), pokud existuje číslo c takové, že $ac = b$.

Tvrzení. *Pokud $a \mid b$ a zároveň $b \neq 0$, pak $|a| \leq |b|$. Pokud navíc $|a| \neq |b|$, tak $2 \cdot |a| \leq |b|$ atd.*

Úloha 1. Určete všechna celá kladná čísla m, n taková, že n dělí $2m - 1$ a zároveň m dělí $2n - 1$. (MO 59–A–II–3)

Definice. Mějme čísla a, b. Pak jejich *největší společný dělitel* (NSD) je největší přirozené číslo d takové, že $d \mid a$, $d \mid b$. Značíme ho (a, b). Podobně nejmenší společný násobek je nejmenší přirozené číslo d takové, že $a \mid d$, $b \mid d$, a značíme jej $[a, b]$.

Na největší společný dělitel se dá také nahlížet jako na číslo, které je dělené všemi ostatními společnými děliteli a obdobně nejmenší společný násobek dělí všechny ostatní společné násobky.

Cvičení. Spočítejte $(-15, 24)$.

Tvrzení. *Platí:*

(i) $(a, a) = (a, 0) = (-a, 0) = [a, a] = [a, 1] = |a|$.
(ii) $(a, b) = (b, a) = (a - b, b) = (b - a, b) = (a - b, a) = (a + b, a)$.
(iii) $(a, b) = |a|$, *právě když* $a \mid b$, *a také právě když* $[a, b] = |b|$.
(iv) $(ab, ac) = a(b, c)$.
(v) $(a, b)[a, b] = ab$.
(vi) *Pokud* $d \mid a, d \mid b$, *tak i* $d \mid (a, b)$.
(vii) $(b, c) \mid (ab, c) \mid (a, c)(b, c) \mid a(b, c)$.

Tvrzení. (Eukleidův algoritmus) *Díky druhé vlastnosti můžeme spočítat* (a, b) *tak, že odečteme menší číslo od většího, dostaneme novou dvojici čísel (se stejným* NSD*) a postup budeme opakovat, dokud nebude jedno z čísel nula.*

Dost často se vyplatí rovnou odečíst menší číslo tolikrát, kolikrát to jde, neboli jím dělit se zbytkem.

Úloha 2. Určete, kolik (uspořádaných) dvojic přirozených čísel a, b splňuje rovnici $[a, 70] + [b, 70] = 210$.

Definice. O číslech a, b řekneme, že jsou *nesoudělná*, pokud $(a, b) = 1$.

Tvrzení. *Platí:*

(i) *Pokud* $(b, c) = 1$, *pak* $(ab, c) = (a, c)$.
(ii) *Pokud* $(b, c) = 1$, *pak* $(a, bc) = (a, b)(a, c)$.

Úloha 3. Určete, pro která čísla a, b, c platí $[a, c] + [b, c] = (a + b)c$.

Úloha 4. Určete možné hodnoty výrazů pro nesoudělná čísla a, b:

(i) $(a + b, ab)$,
(ii) $(a^2 + b^2, ab)$,
(iii) $(a + b, a - b)$,
(iv) $(a^3, (a + 1)^5)$.

Úloha 5. Ukažte, že zlomek

$$\frac{21n + 4}{14n + 3}$$

je v základním tvaru pro každé přirozené číslo n. (IMO 1959)

Úloha 6. Dokažte, že pro každá přirozená m, n platí

$$(2^m - 1, 2^n - 1) = 2^{(m,n)} - 1.$$

Úloha 7. Pro která celá čísla n je výraz

$$\frac{n^3 - 3}{n - 3}$$

celočíselný? (Náboj 2007)

Úloha 8. S využitím vztahu $F_{n+m} = F_{m+1} \cdot F_n + F_m \cdot F_{n-1}$ ukažte, že pro Fibonacciho posloupnost platí $(F_m, F_n) = F_{(m,n)}$.

Úloha 9. Zjistěte, pro která přirozená čísla a, b je hodnota podílu

$$\frac{b^2 + ab + a + b - 1}{a^2 + ab + 1}$$

rovna celému číslu. (MO 57–A–III–3)

Rozklad na du, dv

Často se v úlohách vyplatí rozepsat čísla a, b jako $a = du$, $b = dv$, kde $d = (a, b)$.

Úloha 10. Určete, pro která čísla a, b platí $(a, b) + [a, b] = a + b$.

Úloha 11. Najděte všechny dvojice přirozených čísel a, b takové, že $ab = 2a + 3b$.

Úloha 12. Rozhodněte, zda součet některých dvou přirozených čísel je dělitelem jejich nejmenšího společného násobku.

Úloha 13. Najděte všechny dvojice přirozených čísel x, y takové, že

$$\frac{xy^2}{x+y}$$

je prvočíslo. (MO 58–A–I–3)

Úloha 14. Nechť n, k jsou přirozená čísla a k je navíc bezčtvercové[1]. Předpokládejme, že

$$\frac{n^3 + 2n^2 + k}{n^2 + k}$$

je celé číslo. Dokažte, že pak už platí $n = k$. (MKS 33–9–1)

Úloha 15. Pro dané prvočíslo p najděte všechny trojice přirozených čísel (a, b, c) z množiny $\{1, 2, \ldots, 2p^2\}$ splňující

$$\frac{[a, c] + [b, c]}{a + b} = \frac{p^2 + 1}{p^2 + 2} \cdot c.$$

(MO 59–A–I–6)

Úloha 16. Dokažte, že pro libovolná přirozená čísla a, b, c platí

$$\frac{[a, b, c]^2}{[a, b] \cdot [b, c] \cdot [c, a]} = \frac{(a, b, c)^2}{(a, b) \cdot (b, c) \cdot (c, a)}.$$

(USAMO 1972)

Úloha 17. Nechť $a_1, \ldots, a_k, b_1, \ldots, b_k$ jsou přirozená čísla, která splňují $(a_i, b_i) = 1$ pro každé $i \in \{1, \ldots, k\}$. Dále buď $m = [b_1, \ldots, b_k]$. Ukažte, že platí

$$\left(\frac{a_1 m}{b_1}, \ldots, \frac{a_k m}{b_k}\right) = (a_1, \ldots, a_k).$$

(IMO shortlist 1974)

[1] Bezčtvercové číslo je takové, které pro $a > 1$ není dělitelné číslem a^2

Úloha 18. Ukažte, že pokud je p takové liché prvočíslo, že i $2p+1$ je prvočíslo, pak existují právě čtyři přirozená čísla k taková, že

$$2p + k \mid 2p + k^2.$$

(Variace na MO 58–A–III–4)

Tvrzení. (Bézout) *Mějme čísla a a b. Potom jsou čísla tvaru $ka + \ell b$ pro celá k a ℓ vždy násobky (a, b) a naopak každý násobek (a, b) umíme vyjádřit ve tvaru $ka + \ell b$.*

Návody

1. Rozeberte možnosti $n = 2m-1$ (resp. $m = 2n-1$) a pak využijte první tvrzení.

2. Jedno z čísel musí být dělitel 70 a druhé násobek 4 a dělitel 140.

3. Zřejmě $[a, c] \mid ac$ a musí nastat rovnost.

4. V (i), (ii) použijte $(a, bc) = (a, b)(a, c)$ pro nesoudělná b, c a posléze $(a, b) = (a-b, b)$. Pro (iii) opět $(a, b) = (a-b, b)$. Ve (iv) se zabývejte společným prvočinitelem obou výrazů.

5. Eukleidův algoritmus.

6. Pro $m \geq n$ rozepište $2^m = (2^n-1)2^{m-n}+2^{m-n}$ a uvažujte Eukleidův algoritmus na exponentech.

7. Výraz je celočíselný, právě když $|n-3| = (n^3-3, n-3)$. Následně aplikujte Eukleidův algoritmus.

8. Nejprve dokažte, že po sobě jdoucí členy jsou nesoudělné, poté že pokud $i \mid j$, pak $F_i \mid F_j$. Poté využijte Eukleidův algoritmus na indexech.

9. Jmenovatel musí dělit i součet čitatele se jmenovatelem. Tento součet rozložte na součin a ukažte, že jeden člen je se jmenovatelem nesoudělný.

10. Po substituci $a = du$, $b = dv$ a úpravě výrazu rozložte na součin.

11. Po substituci $a = du$, $b = dv$ zjistěte, jaké jsou mezi čísly vztahy vzhledem k dělitelnosti.

12. Po substituci $a = du$, $b = dv$ a podělení obou stran dělitelnosti d ukažte, že obě strany dělitelnosti jsou nyní nesoudělné.

13. Po substituci $x = du$, $y = dv$ ukažte, že $u + v \mid d^2$ a uv^2 dělí celý zlomek. Rozeberte dva případy, $v = 1$ a $u > 1$ a rozložte $d^2 - 1$ na součin. V druhém případě jen dosaďte za u a v.

14. Po substituci $n = du$, $k = dv$ si uvědomte, že $(d, v) = 1$ a zkuste něco vytknout. Potom si všimněte velikostí.

15. Využijte $[a, c] = \frac{ac}{(a,c)} = \frac{a}{(a,c)}c$. Poté odhadujte podle velikosti (a, c) a (b, c).

16. Pro $d = (a, b, c)$ rozepište $a = d(\frac{a}{d}, \frac{b}{d})(\frac{a}{d}, \frac{c}{d})u$. Uvědomte si, že to jde díky nesoudělnosti. Poté trpělivě upravujte. Alternativně se podívejte na největší mocniny prvočísla p v jednotlivých výrazech.

17. Dokazujte pro jedno prvočíslo. Pokud $p \mid m$, vyberte si takové i, že b_i má největší mocninu p.

18. $(2p-k)(2p+k) = (2p)^2-k^2$ je násobek $2p+k$. Potom rozeberte čtyři možnosti podle toho, čemu se rovná $(2p, k)$.

Literatura a zdroje

[1] Štěpán Šimsa, *Největší společný dělitel*, Staré Město, 2015.

Pravděpodobnostní paradoxy

Fíla Čermák

Abstrakt. Příspěvek obsahuje překvapivé úlohy z pravděpodobnosti. Pravděpodobně budete překvapeni.

Paradox 1. David každý víkend jezdí z plzeňského nádraží buď za manželkou do Dobřan, nebo za milenkou do Rokycan. Rozhoduje se náhodně – vždy nastoupí do prvního vlaku, který jede. Ačkoli vlaky do Rokycan jezdí stejně často jako vlaky do Dobřan, po nějakém čase David shledal, že byl u milenky dvakrát častěji než u manželky. Jak je to možné?

Paradox 2. Kenny, Franta a Jarda se rozhodli, že si zahrají tenis. Kenny se s nimi vsadil o kilo čokolády, že vyhraje dvakrát po sobě. Může si vybrat ze dvou možností: buď bude hrát nejprve s Frantou, pak s Jardou a nakonec s Frantou, nebo nejprve s Jardou, pak s Frantou a nakonec s Jardou. Kterou z možností si má zvolit, jestliže ví, že Jarda hraje podstatně lépe než Franta, aby zvýšil svoji šanci na výhru?

Paradox 3. Do 100místného letadla nastupuje 100 lidí, každý má místenku na jedno sedadlo. První nastupující ale ztratil svou místenku, a tak si sedne náhodně. Každý další si sedne na svoje sedadlo, je-li volné, a v opačném případě si sedne na náhodné volné sedadlo. Jaká je pravděpodobnost, že poslední příchozí si sedne na svoje sedadlo?

Paradox 4. (Monty Hall) Ve finále televizní soutěže je za dvěma dveřmi koza a za třetími auto, přičemž soutěžící chce auto. Postaví se tedy k jedněm dveřím, načež moderátor otevře jedny dveře, za kterými je koza, jiné než ty, ke kterým se soutěžící postavil, a pak dá soutěžícímu možnost ještě svou volbu dveří změnit. Vyplatí se soutěžícímu volbu dveří změnit?

Paradox 5. Pravděpodobnost, že se narodí děvče je stejná jako pravděpodobnost, že se narodí chlapec.

(i) Uvažme náhodnou rodinu se dvěma dětmi, v níž je první narozené dítě děvče. Jaká je pravděpodobnost, že druhé narozené dítě je také děvče?

(ii) Uvažme náhodnou rodinu se dvěma dětmi, z nichž je alespoň jedno děvče. Jaká je pravděpodobnost, že druhé dítě je také děvče?

(iii) Uvažme náhodnou rodinu se dvěma dětmi, z nichž je alespoň jedno děvče se jménem Xénie. Jaká je pravděpodobnost, že druhé dítě je opět děvče?

Paradox 6. Přišli jsme na test jisté vzácné choroby vyskytující se u 1 % populace. Měřil nás přístroj, který v 90 % případů odpoví správně (ve zbylých chybně), a nahlásil, že onou chorobou trpíme. Jaká je pravděpodobnost, že tomu tak skutečně je?

Paradox 7. (Simpsonův) Lukáš a Pepa mají oba svůj žlutý a modrý sáček a v nich černé a bílé kuličky. Pokud Lukáš sáhne do svého žlutého sáčku, má vyšší pravděpodobnost vytažení bílé kuličky, než kdyby sáhl do modrého. Totéž platí pro Pepu. Oba žluté sáčky nyní sesypeme dohromady a totéž provedeme s modrými. Rozhodněte, zda bude vyšší šance na vytáhnutí bílé kuličky u modrého sáčku, nebo u žlutého.

Paradox 8. V $n-1$ vrcholech pravidelného n-úhelníku stojí ovce, ve zbylém vrcholu stojí vlk. V každém kroku se vlk přesune na náhodný (jeden ze dvou) sousední vrchol a pokud v něm stojí ovce, tak ji sežere. Vlk se nasytí až v okamžiku, kdy sežere $n-2$ ovcí, tedy právě jedna ovce přežije. Jaká ovce má nejvyšší šanci na přežití?

Paradox 9. Mirek je velký gurmán a vlastní pytel, ve kterém je 123 karamelek a 321 hašlerek. Aby si své bonbóny pořádně vychutnal, rozhodl se, že je bude konzumovat specifickým způsobem. Když se ráno probudí, začne z pytle náhodně vytahovat jeden bonbón za druhým. První bonbón vytáhne a sní – každý další bonbón vždy vytáhne, a pokud je tento stejného typu jako všechny předchozí, rovněž jej sní. Je-li jiného typu, vrátí jej zpět do pytle, aby si pro tento den nezkazil chuť. Tím Mirkův ranní rituál končí. Uvedeným způsobem konzumuje Mirek bonbóny každý den až do chvíle, kdy už v pytli žádný nezbyde. Jaká je pravděpodobnost, že posledním sněženým bonbónem bude karamelka? (MKS 32–7–6)

Paradox 10. Deseti zvoleným ministrům byly náhodně rozdány ministerské resorty (těch je také 10). Každý ministr zvlášť zajde za králem, který posty rozdal, a musí si tipnout, který post má – konverzace probíhá stylem:
Ministr: „Zemědělství.“,
Král: „Ne, zemědělství má Jánošík.“,
Ministr: „Tak administrativní záležitosti.“,
Král: „Ne, administrativní záležitosti má Jim Hacker.“, ...
Ministři se mohou domlouvat pouze před zkouškou a jako celek uspějí jen tehdy, když každý tipne svůj resort nejhůře na sedmý pokus. Rozhodněte, zda se dokáží dohodnout tak, aby měli nadpoloviční šanci uspět. (Projev před ÚKMO 2014)

Paradox 11. Protihráč napíše na dvě karty různá reálná čísla. Následně vás nechá si náhodně jednu vytáhnout, vy si ji prohlédnete a můžete se rozhodnout, zda si ji necháte nebo vyměníte za jinou. Vyhrává ten z vás, který má na konci v ruce větší číslo. Rozhodněte, zda existuje strategie, která má nadpoloviční šanci na výhru bez ohledu na to, která dvě čísla protihráč napsal.

Paradox 12. Je nám nabídnuta následující hra: Zaplatíme 1000 Kč, pak házíme mincí tak dlouho, dokud nám padá panna, a následně vyhrajeme 2^{n-1} Kč, kde n je počet námi provedených hodů. Vyplatí se nám tuto hru podstoupit?

Náhoda je prevít, nedá se ošálit

Paradox 13. V jisté fiktivní zemi mají tradici, že je třeba rodit děti tak dlouho, dokud se nenarodí děvče. Bude v této zemi více chlapců, nebo děvčat?

Paradox 14. V zaškrtávácím testu můžeme na každou z pěti otázek odpovědět jedním z písmen A, B, C, D, E. Za test dostaneme tolik bodů, na kolik otázek odpovíme správně. Doslechneme-li se, že každé písmeno je použito právě jednou, vyplatí se nám dávat takové tipy, kde je každé písmeno právě jednou?

Paradox 15. Hrajeme jistou hazardní hru. Začínáme s 1000 Kč, vždy vsadíme nějakou částku (nejvýše tolik, kolik právě máme), a následně ji s pravděpodobností $\frac{1}{2}$ vyhrajeme a v opačném případě prohrajeme. K takové hře je možné přistupovat s rozličnými strategiemi:

(i) V každém kroku vsadíme tisíc korun.
(ii) V každém kroku vsadíme polovinu částky, kterou máme.
(iii) (Martingale) Po každé prohře vsadíme dvojnásobek minulé sázky. V opačném případě, nebo pokud to není možné, vsadíme jednu korunu.

Při které z nabízených strategií máme nejvyšší šanci dosáhnout částky 3000 Kč?

Paradox 16. Jirka a Marek hrají svou verzi tenisu. Když podává Marek, má šanci 0,5, že vyhraje míček a když podává Jirka, vyhraje míček s pravděpodobností 0,6. Hraje se do 21 vítězných bodů (bez prodlužování). Marek, který je slabší, podává jako první a navíc si může vybrat způsob, jak se budou střídat podání z následujících možností:

(i) Podání se střídá pravidelně.
(ii) Podává vždy ten, kdo naposled vyhrál míček.
(iii) Podává vždy ten, kdo naposled prohrál míček.

Která volba je pro Marka nejvýhodnější?

Občas je to prostě podvod

Paradox 17. V jedné obálce je 100 Kč a v druhé 200 Kč. Vybereme si náhodnou, zatím ji neotvíráme. Neznámé množství peněz v ní označíme x. V druhé obálce je také náhodně buď $2x$, nebo $0{,}5x$. Průměrně je tak v druhé obálce $1{,}25x$, a proto se nám vyplatí volbu obálky změnit.

Paradox 18. (Bertrandův) Pravděpodobnost, že náhodná tětiva dané kružnice je delší než strana vepsaného rovnostranného trojúhelníku, je rovna $\frac{1}{2}$, $\frac{1}{3}$ a také $\frac{1}{4}$.

Literatura a zdroje

[1] Mirek Olšák, *Pravděpodobnostní paradoxy*, Uhelná Příbram, 2014.

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 $\varphi(n) = n \cdot \prod_{p|n} \frac{p-1}{p}$.

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*.

Konečné projektivní roviny

Klárka Grinerová

Abstrakt. V této přednášce si představíme zajímavé kombinatorické struktury, a to konečné projektivní roviny. Dokážeme si několik různých tvrzení o vlastnostech konečných projektivních rovin a ukážeme si, jak se dané vlastnosti dají využít k řešení některých zajímavých úloh.

Definice. Nechť X je konečná množina a $\mathcal{P}$ je množina podmnožin X, potom dvojici $(X, \mathcal{P})$ nazveme *konečnou projektivní rovinou*, pokud splňuje tři axiomy:

(A1) Pro každé $x, y \in X$, $x \neq y$, existuje právě jedno $P \in \mathcal{P}$ takové, že $x, y \in P$.
(A2) Pro každé $P, Q \in \mathcal{P}$, $P \neq Q$, platí $|P \cap Q| = 1$.
(A3) Existuje čtyřprvková množina $C \subseteq X$, taková, že pro každé $P \in \mathcal{P}$ platí $|C \cap P| \leq 2$.

Prvky množiny X nazýváme *body* a prvky $\mathcal{P}$ *přímky* konečné projektivní roviny. Přímku procházející body x a y budeme značit xy. Axiom (A1) je tak ekvivalentní tvrzení, že každými dvěma body prochází právě jedna přímka, (A2) tvrzení, že se každé dvě přímky protínají v právě jednom bodě, (A3) tvrzení o existenci čtyř bodů v obecné poloze. Tedy existují čtyři body takové, že žádné tři z nich neleží na jedné přímce.

Tvrzení. *V konečné projektivní rovině obsahuje každá přímka stejný počet bodů.*

Důkaz. Chceme dokázat, že libovolné dvě přímky P, Q mají stejný počet bodů. Nejprve ukážeme, že existuje bod $x \in X$ takový, že $x \notin P$ a zároveň $x \notin Q$. Dle axiomu (A3) máme nezávislou množinu C velikosti čtyři. Pokud množina C není podmnožinou $P \cup Q$, můžeme zvolit x z C. Jinak BÚNO $C = \{a, b, c, d\}$ a platí $P \cap C = \{a, b\}$, $Q \cap C = \{c, d\}$. Uvažme přímky ac, bd, pro tyto přímky existuje dle (A2) bod x v jejich průniku a zároveň tento bod x nenáleží P ani Q.

Dále chceme ukázat, že $|P| = |Q|$. Definujeme zobrazení $\varphi\colon P \to Q$ předpisem $\varphi(y) = xy \cap Q$. Ukážeme, že φ je prosté, a proto $|P| \leq |Q|$. Označme body na přímce P jako $P = \{y_1, y_2, y_3, \dots\}$. Dle (A2) každá přímka xy_i protíná Q v jednom bodě z_i. Všechna z_i jsou navzájem různá, protože libovolné dvě různé přímky xy_k a xy_l mají průsečík v bodě x. Analogicky lze dokázat, že $|P| \geq |Q|$. Dohromady z toho plyne $|P| = |Q|$, což jsme chtěli dokázat. □

Cvičení. Z axiomů konečných projektivních rovin dokažte, že pro každý bod $x \in X$ existuje $P \in \mathcal{P}$ takové, že $x \notin P$.

Vlastnosti konečných projektivních rovin řádu n

Definice. *Řád* konečné projektivní roviny $(X, \mathcal{P})$ je $k-1$, kde k je počet bodů na libovolné přímce.

Řád konečné projektivní roviny charakterizuje různé vlastnosti této struktury. Níže jsou uvedená tři tvrzení o počtu přímek, bodů a průniků.

Cvičení. Dokažte, že žádným bodem neprochází všechny přímky.

Tvrzení. *Každým bodem konečné projektivní roviny řádu n prochází $n+1$ přímek.*

Důkaz. Pro každý bod x existuje přímka P taková, že $x \notin P$. Body přímky P označíme $\{y_1, y_2, y_3, \ldots, y_{n+1}\}$. Ukážeme, že bodem x prochází alespoň $n+1$ přímek. Jedná se o přímky $xy_1, xy_2, xy_3, \ldots, xy_{n+1}$, těchto přímek je $n+1$ a jsou navzájem různé.

Zároveň bodem x prochází nejvýše $n+1$ přímek: Uvažme přímku xy procházející bodem x. Tato přímka xy má dle (A2) průsečík s přímkou P v bodě y_i. Tedy přímek procházejících bodem x je nejvýše $n+1$ a zároveň alespoň $n+1$. Celkem je tedy těchto přímek $n+1$. □

Tvrzení. *Konečná projektivní rovina řádu n má n^2+n+1 bodů.*

Tvrzení. *Konečná projektivní rovina řádu n má n^2+n+1 přímek.*

Cvičení. Dokažte tvrzení o počtu bodů a počtu přímek.

Cvičení. Najděte nejmenší konečnou projektivní rovinu.

Definice. *Duálem* konečné projektivní roviny řádu n je dvojice

$$(\mathcal{P}, \{\{P \in \mathcal{P} : x \in P\} : x \in X\}).$$

Dualita se dá vyjádřit jako záměna rolí přímek a bodů. Duálem konečné projektivní roviny řádu n je opět konečná projektivní rovina řádu n.

Konstrukce konečných projektivních rovin

Zatím víme, jaké všechny vlastnosti konečná projektivní rovina splňuje. Zůstává nám otázka, kde se takové konečné projektivní roviny dají najít? Existuje vůbec pro všechna přirozená n konečná projektivní rovina řádu n?

Pokud je n mocnina prvočísla, potom konečná projektivní rovina řádu n skutečně existuje. Panuje zatím nedokázaná domněnka, že platí i opačná implikace. Ukažme si algebraickou konstrukci v případě, kdy n je prvočíslo. Pro konstrukci konečné projektivní roviny řádu n uvážíme množinu $\{0, 1, 2, \ldots, n-1\}$. Definujeme ekvivalenci

nenulových trojic čísel z této množiny tak, že dvě uspořádané trojice (x_1, y_1, z_1) a (x_2, y_2, z_2) jsou ekvivalentní, pokud existuje nenulové přirozené α splňující

$$x_1 \equiv \alpha x_2 \pmod{n}, \qquad y_1 \equiv \alpha y_2 \pmod{n} \qquad \text{a} \qquad z_1 \equiv \alpha z_2 \pmod{n}.$$

K tomu, aby tento vztah skutečně byl ekvivalencí, potřebujeme fakt, že n je prvočíslo, díky čemuž můžeme mezi zbytky modulo n dělit a vše se chová tak pěkně, jak bychom chtěli.

Body X konečné projektivní roviny řádu n tvoří třídy výše uvedené ekvivalence. Uspořádaných nenulových trojic je n^3-1, v každé jedné třídě je $n-1$ trojic, protože všechna možná α náleží do množiny $\{1, 2, \ldots, n-1\}$. Bodů je tedy $\frac{n^3-1}{n-1} = n^2+n+1$. Pomocí bodů pak zadefinujeme i přímky – nechť bod určený trojicí (a, b, c) určuje přímku

$$P_{(a,b,c)} = \{(x, y, z) : ax + by + cz \equiv 0 \pmod{n}\}.$$

Můžete si rozmyslet, že nezávisí na tom, kterou trojici z třídy ekvivalence použijeme – příslušné kongruence budou určovat tu samou množinu bodů.

Příklady

Příklad 1. Ukažte, že (A3) lze nahradit axiomem: Existují dvě různé přímky p, q z $\mathcal{P}$, z nichž každá obsahuje alespoň tři různé body.

Příklad 2. Ukažte, že (A3) lze nahradit axiomem: Celá množina X nelze pokrýt dvěma přímkami.

Příklad 3. Nahradíme axiom (A3) tím, že každá přímka obsahuje alespoň dva body. Které další množinové systémy kromě konečných projektivních rovin tato axiomatizace připouští?

Příklad 4. Ve hře Dobble je 55 karet, přičemž na každé kartě je 8 symbolů a každé dvě karty mají právě jeden symbol společný. Ukažte, že ve hře se nachází alespoň 57 různých symbolů.

Příklad 5. Nechť $(X, \mathcal{P})$ je konečná projektivní rovina řádu n. Kolik bodů je potřeba obarvit, aby platilo, že každá přímka obsahuje alespoň jeden obarvený bod?

Příklad 6. Nechť $(X, \mathcal{P})$ je konečná projektivní rovina řádu n. Kolik bodů je potřeba obarvit, aby platilo, že každá přímka obsahuje alespoň dva obarvené body? Najděte co nejlepší spodní a horní odhad.

Příklad 7. Nechť $(X, \mathcal{P})$ je konečná projektivní rovina řádu q. Vytvořme bipartitní graf $G = G(X, \mathcal{P})$ s částmi X a $\mathcal{P}$ tak, že bod z $x \in X$ a přímka z $P \in \mathcal{P}$ jsou spojeny hranou, právě když bod x náleží P. Tomuto grafu se říká incidenční graf konečné projektivní roviny. Najděte velikost nejmenšího cyklu v grafu G.

Příklad 8. Nechť $G = G(X, \mathcal{P})$ je bipartitní graf z předchozího příkladu. Kolik je v takovém grafu kružnic délky 6?

Příklad 9. Ukažte, že existuje graf s n vrcholy s alespoň $\Omega(n^{3/2})$ hranami, který neobsahuje cyklus na čtyřech vrcholech.

Příklad 10. Mějme $(X, \mathcal{P})$, kde X je množina bodů a P nějaká množina podmnožin X, které nazveme přímkami, a $n \in \mathbb{N}$. Platí následující tři podmínky:

(1) $|X| = n^2 + n + 1$.
(2) Každá přímka obsahuje $n + 1$ bodů.
(3) Každý bod je obsažen v $n + 1$ přímkách.

Je pak $(X, \mathcal{P})$ nutně konečná projektivní rovina?

Příklad 11. Dokažte, že pro každé $k \in \mathbb{N}$ existuje $n \in \mathbb{N}$ takové, že v konečné projektivní rovině $(X, \mathcal{P})$ řádu alespoň n existuje k bodů v obecné poloze.

Návody

1. Uvaž čtyřprvkovou množinu bodů a využij axiom (A1).

2. Opět uvaž čtyřprvkovou množinu bodů, tu pokryj dvěma přímkami a využij axiom (A1).

4. Nalezni vztah karty ve hře ke konečné projektivní rovině řádu 7.

5. Uvaž počet incidencí mezi jedním bodem z množiny X a množinou přímek.

6. Uvaž, kolik různých přímek může pokrýt jeden obarvený bod z množiny.

7. V bipartitním grafu mají všechny kružnice sudou délku.

8. Cyklus délky 6 v G odpovídá trojici bodů z X, které neleží na jedné přímce.

9. Uvaž incidenční graf konečné projektivní roviny řádu n.

10. Uvaž, kolik bodů může být v průniku dvou přímek.

11. Najdi n pro pět bodů v obecné poloze a postupuj indukcí.

Literatura a zdroje

[1] Jiří Matoušek, Jaroslav Nešetřil: *Kapitoly z diskrétní matematiky*, Karolinum, 2002.
[2] Lucien Šíma: *Projektivní roviny*, Horní Lysečiny, 2018.
[3] *Sbírka úloh z matematiky*, *https://kam.mff.cuni.cz/sbirka*.

Konstrukční úlohy

Verča Hladíková

Abstrakt. V geometrii se často setkáváme s typem úloh, ve kterých hledáme konstrukci pomocí kružítka a pravítka. Přednáška představuje úvod do problematiky, ale její součástí jsou i úlohy pro náročné.

Všechny úlohy budeme klasicky konstruovat pravítkem a kružítkem. Pravítkem umíme narýsovat rovnou čáru, ale neumíme s ním měřit délky ani rýsovat kolmice. Nejprve pro připomenutí uvedeme několik známých tvrzení, která se nám budou při řešení úloh hodit.

Věta. (Thaletova) *Na kružnici nad průměrem AB zvolme libovolný bod C různý od A, B. Potom je trojúhelník ABC pravoúhlý s pravým úhlem u vrcholu C. Popsané kružnici se říká Thaletova.*

Tvrzení. *Těžnice trojúhelníka se protínají v jednom bodě (říkáme mu těžiště). Těžiště rozděluje každou z těžnic v poměru $2:1$, tj. pokud má trojúhelník ABC těžiště T, potom platí $|AT| = 2 \cdot |S_aT|$, kde S_a je střed strany BC.*

Tvrzení. (o obvodovém a středovém úhlu) *Nechť k je kružnice se středem O a AB její tětiva. Potom se velikost úhlu AXB nemění, probíhá-li X některý z oblouků kružnice k určených tětivou AB. Navíc je $|\sphericalangle AXB| = \frac{1}{2}|\sphericalangle AOB|$, kde úhlem AOB rozumíme vnější úhel ve čtyřúhelníku $AXBO$.*

Značení

Pro prvky trojúhelníka ABC budeme používat následující značení:

(1) a, b, c – strany trojúhelníka, $a = |BC|$, $b = |AC|$, $c = |AB|$,
(2) v_a, v_b, resp. v_c – výška na stranu a, b, resp. c,
(3) t_a, t_b, resp. t_c – těžnice z vrcholu A, B, resp. C,
(4) α, β, resp. γ – vnitřní úhel u vrcholu A, B, resp. C,
(5) R – poloměr kružnice opsané,
(6) S_{ABC} – obsah trojúhelníka ABC.

Příklady

Pokud je v zadání příkladu uvedeno, že známe nějakou délku, znamená to, že umíme zkonstruovat kružnici s daným poloměrem. Znát úhel znamená, že umíme sestrojit dvě polopřímky vycházející z jednoho bodu, které svírají tento úhel.

Příklad 1. Je dána kružnice k a uvnitř ní dva různé body P a Q. Sestrojte pravoúhlý trojúhelník vepsaný kružnici k tak, aby body P, Q ležely každý na jedné odvěsně.

Řešení. Sestrojíme kružnici ℓ nad průměrem PQ, průsečíky kružnic k a ℓ nazveme K, K'. Množina průsečíků navzájem kolmých přímek, z nichž jedna prochází bodem P a druhá bodem Q, je Thaletova kružnice ℓ nad průměrem PQ. Vrchol u pravého úhlu trojúhelníka tak musí ležet na kružnici ℓ, bude to tedy jeden z bodů K, K'. Nakonec průsečík přímky PK a kružnice k (různý od K) nazveme L, podobně průsečík přímky QK a kružnice k nazveme M. Potom je KLM hledaný trojúhelník.

Stejně tak můžeme najít trojúhelník $K'L'M'$, pokud místo K vezmeme druhý průsečík K'. Úloha tedy

(i) má dvě řešení, pokud se kružnice k a ℓ protínají ve dvou bodech,
(ii) má jedno řešení, pokud se kružnice k a ℓ dotýkají (v tomto případě $K = K'$),
(iii) nemá řešení, pokud se kružnice k a ℓ neprotínají.

Příklad 2. Je dána kružnice k a přímka p. Sestrojte kružnici ℓ o daném poloměru r tak, aby se obou dotýkala.

Příklad 3. Sestrojte trojúhelník ABC, znáte-li a, v_a a R.

Příklad 4. Sestrojte trojúhelník ABC, znáte-li a, t_a a α.

Příklad 5. Sestrojte trojúhelník ABC, znáte-li t_a, t_b a t_c.

Příklad 6. Sestrojte trojúhelník ABC, znáte-li úhly α, β a obvod $a + b + c$.

Příklad 7. Je dán trojúhelník ABC a úsečka délky d. Sestrojte rovnoramenný trojúhelník KLM, který má základnu délky $|KL| = d$ a jehož obsah je stejný jako obsah trojúhelníka ABC. (MKS 21–4–4)

Příklad 8. Uvnitř trojúhelníka ABC sestrojte bod M tak, aby platilo

$$S_{ABM} : S_{BCM} : S_{ACM} = 1 : 2 : 3.$$

Příklad 9. Mějme přímku p a na ní po řadě body A, B, C, D. Nalezněte čtverec $KLMN$ takový, že přímky KL, MN, LM a KN protínají přímku p v bodech A, B, C a D v tomto pořadí. (MKS 27–6–5)

Příklad 10. Sestrojte čtyřúhelník $EFGH$, znáte-li délky úseček EF, FG, GH, HE a XY, kde X je střed úsečky EF a Y je střed úsečky GH. (MKS 27–6–7)

Příklad 11. Sestrojte střed úsečky, pokud máte k dispozici pouze kružítko.

Příklad 12. Mějme úsečku AB a přímku p s ní rovnoběžnou. Rozdělte AB na n stejných úseků pouze pomocí pravítka.

Příklad 13. Je dán trojúhelník ABC a na straně BC bod D. Zkonstruujte body P na AB a Q na AC tak, aby PQ byla rovnoběžná s BC a $\sphericalangle PDQ$ byl pravý.

Příklad 14. Sestrojte kosočtverec, jehož protější strany leží na dvou daných rovnoběžkách p, q a druhé dvě strany prochází dvěma danými body E a F.

Návody

7. Které známé geometrické tvrzení říká něco o součinu délek?

8. Jak vypadá množina bodů M taková, že $S_{ABC} : S_{ACM} = 1 : 2$?

9. Zkuste vyjádřit KL jako součet dvou známých vektorů.

10. Zkonstruujte středový obraz čtyřúhelníku podle X.

11. Nejprve zkonstruujte úsečku dvakrát delší než AB.

12. Zkuste nejprve pro $n = 2$ a pak iterujte.

13. Zkonstruujte trojúhelník podobný $\triangle PDQ$ pod stranou BC.

14. Zkonstruujte bod X tak, aby $|EX| = |pq|$ a $\sphericalangle EXF$ byl pravý.

Literatura a zdroje

Nechala jsem se inspirovat starším sborníkovým příspěvkem *Tondy Češíka*, kterému tímto děkuji.

[1] Tonda Češík: *Konstrukční úlohy*, Hojsova Stráž, 2016.

Odmocniny z jedničky

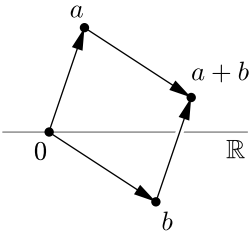
Lenka Kopfová

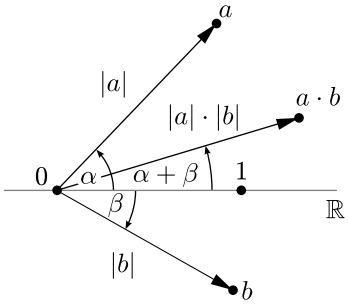
Abstrakt. V příspěvku si nejdříve trochu pohrajeme s komplexními čísly jako takovými a pak se podíváme na zub odmocninám z jedničky. Jejich strukturu se nejprve budeme snažit pořádně pochopit a poté i použít na nějaké příklady. Samozřejmě komplexní čísla, jako například i, mají široké, vysoce praktické využití v reálném světě – například při opravování obzvláště hezkých úloh v PraSeti :-)

Zavedení komplexních čísel

Definice. Mějme rovinu a v ní danou osu reálných čísel. Této rovině budeme říkat *komplexní rovina*, její body budeme nazývat *komplexní čísla*. Bodu 0 na reálné ose říkáme *počátek* a komplexní čísla ztotožňujeme s vektory spojujícími počátek a příslušné komplexní číslo jakožto bod v rovině.

Definice. Součet komplexních čísel definujeme jako součet příslušných vektorů. Dále definujeme součin komplexních čísel jako vektor, který má délku rovnu součinu délek jednotlivých činitelů a svírá s kladnou reálnou polopřímkou úhel rovný součtu orientovaných úhlů jednotlivých činitelů.





Pozorování. *Operace na komplexních číslech splňují očekávané vlastnosti.*

(1) *Na reálné ose fungují jako běžné sčítání a násobení.*
(2) *Při sčítání/násobení nezáleží na pořadí sčítanců/činitelů.*
(3) *Při sčítání/násobení nezáleží na pořadí uzávorkování sčítanců/činitelů.*
(4) *Funguje roznásobování, tedy* $a \cdot (b + c) = a \cdot b + a \cdot c$.

Imaginární jednotka

Pozorování. *Existují právě* 2 *komplexní čísla, jejichž druhá mocnina je rovna* -1.

Definice. Tomu číslu z předchozího pozorování, které leží nad reálnou osou, budeme říkat *imaginární jednotka*. Značíme ji i.

Pozorování. *Každé komplexní číslo se dá jednoznačně napsat ve tvaru* $x+iy$, *kde* $x, y \in \mathbb{R}$.

Definice. Mějme dáno komplexní číslo z. Jako *komplexně sdružené číslo* k z nazveme obraz z v osové souměrnosti dle reálné osy. Značíme jej $\overline{z}$. Tedy pokud $z = x + iy$, tak $\overline{z} = x - iy$.

Definice. Jako ω_n označíme takové komplexní číslo, které leží na jednotkové kružnici a s kladnou reálnou osou svírá úhel $\frac{360^\circ}{n}$ v kladném směru.

Důsledek. (Pythagorova věta) *Pro pravoúhlý trojúhelník s odvěsnami délek* a, b *a přeponou délky* c *platí* $a^2 + b^2 = c^2$.

Důsledek. (součtové vzorce) *Pro úhly* α, β *platí vztahy mezi goniometrickými funkcemi*

$$\cos(\alpha + \beta) = \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta),$$
$$\sin(\alpha + \beta) = \cos(\alpha)\sin(\beta) + \sin(\alpha)\cos(\beta).$$

Důsledek. (Moivreova věta) *Pro úhel* α *a přirozené číslo* n *platí rovnost*

$$(\cos(\alpha) + i\sin(\alpha))^n = \cos(n\alpha) + i\sin(n\alpha).$$

Cvičení. Najděte druhé odmocniny z komplexního čísla $3 - 4i$.

Příkladky

Příklad 1. Nalezněte všechna komplexní řešení polynomiální rovnice $x^n - 1 = 0$.

Příklad 2. Sečtěte

$$\binom{n}{0} + \binom{n}{3} + \binom{n}{6} + \cdots$$

Příklad 3. Sečtěte

$$\binom{n}{1} + \binom{n}{4} + \binom{n}{7} + \cdots$$

Příklad 4. Sečtěte

$$\binom{n}{0} + \binom{n}{4} + \binom{n}{8} + \cdots$$

Odmocniny z jedničky

Definice. O komplexním čísle z řekneme, že je *odmocninou z jedné*, pokud je kořenem polynomu $z^n - 1$ pro nějaké přirozené n. Pokud navíc pro všechna přirozená k menší než n platí $z^k \neq 1$, tak je z *primitivní n-tou odmocninou z jedné*.

Definice. Řádem komplexního čísla α nazveme nejmenší n takové, že $\alpha^n = 1$. Pokud takové číslo n neexistuje, pak považujeme za řád ∞.

Cvičení. Jaký je řád ω_{10}^8?

Cvičení. Kolik komplexních čísel má řád n?

Příklad 5. Nechť m, n jsou přirozená čísla. Dokažte, že $x^n - 1$ dělí polynom $x^m - 1$, právě když $n \mid m$.

Definice. Mějme množinu komplexních čísel $G = \{\alpha_1, \ldots, \alpha_n\}$. Množinou *generovanou* G nazveme co do inkluze nejmenší množinu X takovou, že $G \subset X$ a zároveň pro každá $a, b \in X$ taky $ab \in X$. Značíme ji $\langle G \rangle$.

Příklad 6. Nechť G je konečná množina nějakých odmocnin z jedničky (tedy pro každé $\alpha \in G$ existuje přirozené n takové, že $\alpha^n = 1$). Pak existuje přirozené n, že $\langle G \rangle = \langle \omega_n \rangle$.

Příklad 7. Mějme přirozená čísla k, ℓ, n, pak $\langle \omega_n^k, \omega_n^\ell \rangle = \langle \omega_n^{\gcd(k,\ell)} \rangle$.

Příklad 8. Nalezněte největšího společného dělitele mnohočlenů $x^m - 1$ a $x^n - 1$ v závislosti na přirozených číslech n a m.

Příklad 9. S využitím poznatků z posledního uvedeného příkladu ukažte, že $2^n - 1$ dělí $2^m - 1$, právě když $n \mid m$.

Definice. Pro libovolné přirozené n definujeme *n-tý cyklotomický polynom* jako

$$\Phi_n(x) = \prod_{\substack{1 \leq j \leq n \\ \gcd(n,j)=1}} (x - \omega_n^j).$$

Příklad 10. Nahlédněte, že platí $\prod_{d|n} \Phi_d(x) = x^n - 1$. Z toho odvoďte známou identitu $n = \sum_{d|n} \varphi(d)$, kde $\varphi(d)$ značí Eulerovu funkci.

Příklad 11. Dokažte, že pro libovolné přirozené n má polynom $\Phi_n(x)$ celočíselné koeficienty.

Příklad 12. Nechť n je liché přirozené číslo. Spočtěte

$$\frac{1}{1+1} + \frac{1}{1+\omega_n^1} + \cdots + \frac{1}{1+\omega_n^{n-1}}.$$

Příklad 13. Nechť m, n jsou přirozená čísla. Určete $\sum_{j=0}^{n-1} \omega_n^{jm}$.

Příklad 14. Přirozené číslo $n \geq 4$ nazveme *zajímavým*, pokud pro něj existuje komplexní číslo z takové, že $|z| = 1$ a zároveň $1 + z + z^2 + z^{n-1} + z^n = 0$. Kolik existuje zajímavých čísel menších než 2022? (Rumunská MO 2022)

Příklad 15. Mějme přirozená k, ℓ, n a prostou funkci f na množině $\{1, \ldots, n\}$ takovou, že $f(x) - x \in \{k, -\ell\}$. Dokažte, že $k + \ell \mid n$. (Polská MO 2019)

Příklad 16. Nechť P, Q, R, S jsou polynomy takové, že pro každé $x \in \mathbb{C}$ platí

$$P(x^5) + xQ(x^5) + x^2R(x^5) = (x^4 + x^3 + x^2 + x + 1)S(x).$$

Dokažte, že $P(1) = 0$.

Příklad 17. Mějme přirozená čísla $m, n \geq 2$ a $a_1, a_2, \ldots, a_n$ taková, že žádné z nich není násobkem m^{n-1}. Dokažte, že existují celá čísla $b_1, b_2, \ldots, b_n$ taková, že ne všechny jsou nulová, $|b_j| < m$ pro každé j a $m^n \mid a_1b_1 + a_2b_2 + \cdots + a_nb_n$. (IMO Shortlist 2002)

Návody

1. Označme nějaké řešení z, co musí splňovat jeho absolutní hodnota a úhel, který svírá s reálnou osou?

2. Uvažuj ω_3, jak vypadá $(1 + \omega_3)^n, (1 + \omega_3^2)^n$ a $(1 + 1)^n$?

3. Stejně jako předchozí úloha, jen vhodně přenásob ω_3.

4. Co takhle ω_4?

6. Nejdříve najdi n takové, že prvky G jsou n–té odmocniny z jedničky. Pak vezmi nejmenší k takové, že $\omega_n^k \in \langle G \rangle$ a sporuj.

7. Ukaž obě inkluze.

11. Indukcí s tím, že absolutní člen je vždy ± 1.

12. Popáruj sčítance. Vyjde $\frac{n}{2}$.

13. Vyjde n pokud $n \mid m$, jinak 0.

14. Zkonjuguj danou rovnici.

15. Uvažuj $(k + \ell)$-té odmocniny z jedničky.

16. Co musíme dosadit, aby se pravá strana rovnala nule?

17. Uvažuj množinu všech m^n součtů, pokud dovolujeme jen b_j kladná. Ukaž, že je to množina všech zbytků mod m^n a uvažuj ω_{m^n}.

Literatura a zdroje

[1] Mirek Olšák: *Komplexní čísla geometricky*, Mentaurov, 2013.
[2] Jarda Hančl, Jakub „šnEk“ Opršal: *Komplexní čísla*, seriál MKS, 2010/11.
[3] *https://artofproblemsolving.com/community*.

Derivace

Terka Kučerová

Abstrakt. Tento příspěvek patří k přednášce, na které si názorně vysvětlíme, co je to derivace funkce, naučíme se nejdůležitější pravidla pro její výpočet a objasníme si její hlavní způsoby využití.

Při zkoumání nějaké funkce (z podmnožiny $\mathbb{R}$ do $\mathbb{R}$) se hodí vědět, jakou má v daném bodě tečnu (Nemusí mít žádnou – lze si představit funkce s různými zubatými a „potrhanými“ grafy –, ale my se budeme zabývat funkcemi, které mají tečnu v každém bodě). Metodu, jak směr této tečny spočítat, objevili (pravděpodobně) nezávisle na sobě Isaac Newton a Gottfried Leibniz, čímž umožnili prudký rozmach matematiky i fyziky.

Definice. *Směrnicí* přímky myslíme tangens úhlu, který svírá s osou x. Jestliže má funkce f v bodě x tečnu, pak směrnici této tečny nazýváme *derivací* f v bodě x a značíme $f'(x)$.

Ona průlomová myšlenka pánů Newtona a Leibnize byla, že pokud se f kolem bodu x chová slušně, pak lze směrnici její tečny dost dobře odhadnout směrnicí sečny, která f protíná v bodech x a $x+d$, kde d je nějaké hodně malé číslo. Spočítat tuto směrnici je snadné; je to $\frac{f(x+d)-f(x)}{d}$.

Na přednášce si ukážeme, že zkoumáním chování tohoto výrazu pro malá d si většinou dovedeme představit, co by se stalo, kdybychom za d „dosadili nulu“ – čímž právě spočítáme derivaci v bodě x. Veškeré naše počínání bude stát na naprosto pevných matematických základech, ale místo rigorózních definic se zaměříme spíše na to jak derivace používat.

Začneme tím, že si odvodíme následující vztahy pro derivace některých elementárních funkcí:

Věta. (tabulka derivací) *Na celém definičním oboru příslušných funkcí platí tyto vztahy:*

(i) $(x^\alpha)' = \alpha x^{\alpha-1}$ *pro každé* $\alpha \in \mathbb{R}$,
(ii) $(e^x)' = e^x$,
(iii) $(\sin(x))' = \cos(x)$,
(iv) $(\cos(x))' = -\sin(x)$,
(v) $(\ln(x))' = \frac{1}{x}$.

Zatím moc funkcí zderivovat neumíme; to se spraví následující větou, která nám ukáže, jak spočítat derivace funkcí, které jsou definovány s využitím funkcí jednodušších. Symbolem $f \circ g$ myslíme složení funkcí f a g, tj. funkci definovanou vztahem $(f \circ g)(x) = f(g(x))$; symbolem f^{-1} označujeme inverzní funkci k funkci f, pokud existuje.

Věta. (aritmetika derivací) *Pro každou konstantu c a funkce f a g, pro něž výraz na pravé straně dává smysl, platí následující vztahy:*

(i) $(cf)'(x) = cf'(x)$,
(ii) $(f+g)'(x) = f'(x) + g'(x)$,
(iii) $(fg)'(x) = f'(x)g(x) + f(x)g'(x)$,
(iv) $(f \circ g)(x)' = f'(g(x))g'(x)$,
(v) $(f^{-1}(x))' = \frac{1}{f'(f^{-1}(x))}$.

Skoro každá funkce, se kterou jsme se v životě setkali, je vybudovaná z funkcí x^α, $\sin(x)$ a e^x pomocí konečného počtu sčítání, násobení, skládání a invertování – takže její derivaci umíme spočítat s využitím předešlých dvou vět. Pojďme si to procvičit.

Příklad. Spočítejte derivace následujících funkcí (na celém definičním oboru, pokud to lze):

(i) $(1+x)^2$,
(ii) $\sin(2x)$,
(iii) $\sin^2(x) + \cos^2(x)$,
(iv) $\mathrm{tg}(x)$,
(v) 2^x,
(vi) $\arcsin x$,
(vii) $\ln(\cos x)$.

Příklad. Odvoďte obecný vzorec pro derivování podílu dvou funkcí.

Využití derivací

No dobrá, většinu funkcí, s nimiž se setkáme, tedy umíme zderivovat. A k čemu nám to bude dobré? Když si uvědomíme, že derivace vyjadřuje směrnici tečny, není pro nás těžké uvěřit následující větě:

Věta. *Jestliže má funkce f v bodě x kladnou derivaci, pak je na nějakém jeho okolí ostře rostoucí. Pokud má derivaci zápornou, je naopak na nějakém okolí ostře klesající.*

Z toho už snadno vyplyne následující veledůležitá věta:

Věta. *Jestliže má funkce f v bodě x lokální minimum nebo maximum, pak derivace v tomto bodě buď neexistuje, nebo je nulová.*

Příklad. Ověřte, že s pomocí předešlé věty správně naleznete body, v nichž může mít funkce sinus maximum či minimum.

Příklad. Nalezněte lokální maximum funkce $\ln(2x) - x$.

Příklad. Zjistěte pomocí derivování, kde leží vrchol paraboly dané rovnicí $f(x) = ax^2 + bx + c$.

Příklad. Nalezněte extrémy funkce $xe^{-x^2/2}$.

Příklady

Příklad 1. Určete rovnici tečny k funkci $\frac{1-x}{x^2-3}$ v bodě odpovídajícím $x = -2$.

Příklad 2. Prasátko si chce na břehu rovné řeky oplotit obdélníkovou zahradu tak, že na straně přilehlé k řece žádný plot nebude. Má k dispozici osm set metrů pletiva. Jakou největší plochu může mít jeho zahrada?

Příklad 3. Helmut by si přál mít krabici ve tvaru kvádru, jehož podstava má poměr stran $a : b$ roven jeho oblíbenému kladnému α. Jak má dosáhnout co největšího objemu, pokud

(a) povrch nesmí překročit zadané S?
(b) součet rozměrů $a + b + c$ nesmí překročit zadané S?

Příklad 4. Barbara balí vánoční dárky. Z čtvercového papíru o straně 30 cm vystřihne v rozích čtyři stejné čtverečky a zbytek přehne tak, aby vznikla otevřená krabice. Jak velké čtverečky má odstřihnout, aby byl objem krabice byl maximální?

Příklad 5. (těžší)

(i) Určete hodnotu výrazu $\sqrt{2}^{\sqrt{2}^{\sqrt{2}^{\sqrt{2}^{\cdot^{\cdot^{\cdot}}}}}}$. (Tím máme na mysli číslo, k němuž se blíží členy posloupnosti $\sqrt{2}, \sqrt{2}^{\sqrt{2}}, \sqrt{2}^{\left(\sqrt{2}^{\sqrt{2}}\right)}, \dots$) Tato část příkladu je zajímavá, ale s derivováním nesouvisí.

(ii) Pro která a lze obdobným způsobem definovat výraz $a^{a^{a^{\cdot^{\cdot^{\cdot}}}}}$?

Příklad 6. (těžší) Mějme v rovině čtyři body tvořící vrcholy čtverce. Máme za úkol nakreslit mezi nimi několik čar tak, aby bylo z každého bodu možné dostat se po čárách do každého jiného (byť třeba po dlouhé cestě procházející některým z ostatních bodů). Jaká může být nejmenší celková délka těchto čar? Místo čtverce zkuste uvažovat i obdélník nebo trojúhelník.

Řešte předešlou úlohu pomocí:

(i) derivování,
(ii) elementární geometrie.

Literatura a zdroje

Tento super příspěvek je téměř beze změn převzat od *Kuby Krásenského* ze soustředění v Zásadě (2017), kterému tímto děkuji.

[1] Kuba Krásenský, *Derivace (s trochou mýdla)*, Zásada, 2017.

Fibonacciho čísla

Anna Mlezivová

Abstrakt. Příspěvek ukazuje některé vlastnosti Fibonacciho čísel a obsahuje několik dokazovacích úloh. Většinu z nich lze interpretovat mnoha způsoby.

Definice. *Fibonacciho posloupnost* je posloupnost celých čísel F_n splňující vztah $F_{n+2} = F_n + F_{n+1}$ pro všechna $n \in \mathbb{N}$ s počáteční podmínkou $F_0 = 0$ a $F_1 = 1$.

Tedy několik prvních Fibonacciho čísel je: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, ...

Příklad. (Fibonacciho králíci) V ZOO žijí králíčci. Na začátku zde bydlel jeden králičí pár, který se ale dále hojně množí. Každému páru trvá dva měsíce, než se jim narodí první mláďata. Potom každý další měsíc zplodí právě jeden nový králičí pár, který opět dva měsíce čeká na svá první mláďata. Žádní králíčci neumírají. Ukažte, že počet párů po n měsících je n-tý člen Fibonacciho posloupnosti.

Fibonacciho číslo si můžeme představit i jinak než na příkladu králíků.

Příklad. Kolika způsoby je možné vydláždit obdélník o rozměrech $1 \times (n-1)$ pomocí dlaždic 1×2 a 1×1?

Příklady

Příklad 1. Ukažte, že počet možností, jak vyjít schodiště o n schodech, vynecháme-li při každém kroku nejvýše jeden schod, je právě F_{n+1}.

Příklad 2. Kolika způsoby je možné vydláždit obdélník o rozměrech $2 \times n$ pomocí dlaždic 1×2?

Příklad 3. Uvědomte si, že počet možností, jak vyskládat tabulku $(n+1) \times 1$ dílky většími než 1×1, je F_n.

Příklad 4. Uvědomte si, že počet možností, jak rozdělit tabulku $n \times 1$ kostičkami s lichými rozměry, je roven F_n.

Příklad 5. Nahlédněte, že počet posloupností nul a jedniček o délce n, které neobsahují dvě nuly vedle sebe, je roven F_{n+2}

Následující identity můžete zkusit vyřešit jak kombinatoricky, tak výpočtem.

Příklad 6. Ukažte, že platí $F_1^2 + F_2^2 + F_3^2 + \cdots + F_n^2 = F_n \cdot F_{n+1}$.

Příklad 7. Dokažte $F_1 + F_3 + \cdots + F_{2n-1} = F_{2n}$.

Příklad 8. Ukažte, že platí $F_1 + F_2 + \cdots + F_n = F_{n+2} - 1$.

Příklad 9. Ukažte $F_1 \cdot F_2 + F_2 \cdot F_3 + \cdots + F_{2n-1} \cdot F_{2n} = F_{2n}^2$.

Příklad 10. Ukažte, že $F_{n+m} = F_{n+1} \cdot F_m + F_n \cdot F_{m-1}$.

Příklad 11. Dokažte, že pro každé $n \geq 4$ platí $F_n^2 = 2F_{n-1}^2 + 2F_{n-2}^2 - F_{n-3}^2$.

Příklad 12. (Cassiniho identita) Ukažte, že $F_{n-1} \cdot F_{n+1} = F_n^2 + (-1)^n$.

Příklad 13. Dokažte, že pro $n > 1$ platí $F_{n+5} > 10F_n$.

Příklad 14. Dokažte, že $F_k \mid F_{nk}$.

Příklad 15. Určete hodnotu $\displaystyle\sum_{n=2}^{\infty} \frac{1}{F_{n-1} \cdot F_{n+1}}$.

Příklad 16. Určete hodnotu $\displaystyle\sum_{n=2}^{\infty} \frac{F_n}{F_{n-1} \cdot F_{n+1}}$.

Literatura a zdroje

Tento příspěvěk je z velké části převzatý z příspěvku Fibonacciho čísla od *Ádi Kostelecké*, které tímto děkuji.

[1] Calda Emil: *Sbírka řešených úloh*, Prometheus, 2006.
[2] Polster Burkard: *Q.E.D. Krása matematického důkazu*, Dokořán, 2014.
[3] Mirek Olšák: *Kombinatorické (Ne)počítání*, Hostětín, 2013.
[4] *Cut The Knot*,
http://www.cut-the-knot.org/arithmetic/combinatorics/FibonacciTilings.shtml.
[5] *Wolfram Math World*,
http://mathworld.wolfram.com/FibonacciNumber.html.

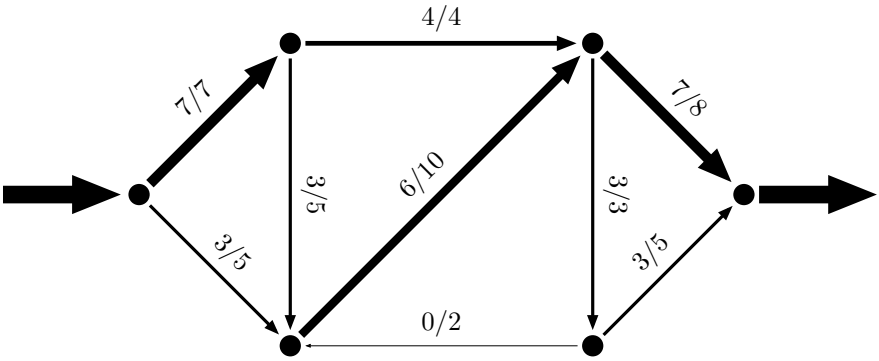
Toky v sítích

Honza Nekarda

Abstrakt. Seznámíme se s oblastí teorie grafů, na kterou se dá převést spousta různých úloh. Vysvětlíme si, co toky v sítích jsou a dokážeme si několik tvrzení o nich. Nakonec s jejich pomocí vyřešíme několik úloh.

Intuitivní pohled na toky v síti

Toky v sítích potkáme všude, kde potřebujeme přenést něco skrze potrubí z jednoho místa do druhého. Síť si můžeme představit jako potrubí s různě širokými trubkami (takže každou může téct jiné maximální množství tekutiny), které má přívod (říkáme mu zdroj) a odvod (říkáme mu stok). Tok pak je situace, když tímto potrubím někudy pustíme tekutinu od zdroje do stoku. V místech, kde se trubky kříží, požadujeme, aby množství, které přiteče, bylo rovno množství, které odteče, tedy aby síť těsnila.



Definice pomocí grafů

Sítí nadále budeme rozumět orientovaný graf G s (konečnou) množinou vrcholů V a hran E spolu se dvěma různými speciálními vrcholy – zdrojem a stokem. Navíc pro každou hranu z vrcholu i do j (pokud nebude hrozit nejasnost, budeme je značit pouze ij) je dána její kapacita $c(ij) \geq 0$ (tedy je to funkce $c\colon E \to \mathbb{R}_0^+$). *Tok* pak

získáme tím, že navíc ke každé hraně (vedoucí z i do j) přiřadíme nezáporné číslo $f(ij) \leq c(ij)$. Po každé hraně tedy teče nejvýše její kapacita. Zároveň pro každý vrchol i musí platit

$$\sum_{ij \in E} f(ij) \; - \sum_{ji \in E} f(ji) = \begin{cases} v, & \text{pokud } i \text{ je zdroj,} \\ -v, & \text{pokud } i \text{ je stok,} \\ 0, & \text{jinak.} \end{cases}$$

To odpovídá tomu, že síť musí těsnit. *Velikost toku* je výše zmíněné v, které si lze představit jako množství kapaliny, jež v nalezené konfiguraci proteče sítí ze zdroje do stoku za jednotku času.

Úmluva. Abychom si usnadnili rozebírání možností, přidáme do G hrany s kapacitou nula tak, aby pro každou hranu ij existovala i opačná hrana ji. Po těchto hranách poteče vždy nula, takže jejich přidání výsledek neovlivní.

Maximální velikost toku

Dále se budeme zabývat hledáním takového toku, jehož velikost je maximální.

Nejdříve by bylo dobré vědět, zda vůbec takový tok existuje. Následující jednoduše vypadající, avšak hůře dokazatelné tvrzení, nám na tuto otázku odpovídá.

Tvrzení. *Každá síť má tok maximální velikosti.*

Definice. *Elementární řez* $E(A, B)$ je množina hran ij takových, že $i \in A$ a $j \in B$, kde A je nějaká množina vrcholů obsahující zdroj a B je množina vrcholů obsahující stok splňující, že $A \cup B = V$ a $A \cap B = \emptyset$. *Kapacitou* elementárního řezu rozumíme

$$c(A, B) = \sum_{ij \in E(A,B)} c(ij).$$

Elementární řezy by nám mohly k hledání maximálního toku pomoci, jelikož intuitivně velikost toku nemůže přesáhnout velikost jakéhokoli řezu. Dokonce platí i silnější tvrzení, ale k jeho dokázání si ještě definujeme *zlepšující cesty.*

Definice. *Zlepšující cesta* mezi vrcholy u a v je posloupnost vrcholů $(v_1, \ldots, v_n)$ taková, že $v_1 = u$ a $v_n = v$, pro každé $i \in \{1, 2, \ldots, n-1\}$ vede mezi vrcholy v_i a v_{i+1} (v nějakém směru) hrana, a navíc buď $c(v_i v_{i+1}) - f(v_i v_{i+1}) > 0$, nebo $f(v_{i+1} v_i) > 0$. Jinými slovy pro každou dvojici sousedních vrcholů na cestě platí, že lze buď zvýšit tok po směru, nebo snížit tok v protisměru, čímž dosáhneme zvýšení ve směru z u do v. Zde využíváme Úmluvu, podle které jsme pro každou hranu přidali i hranu opačnou, takže se můžeme odkazovat na hrany v obou směrech: $v_i v_{i+1}$ i $v_{i+1} v_i$.

Věta. (maximální tok – minimální řez) *V síti je maximální velikost toku rovna minimální kapacitě řezu.*

Myšlenka důkazu. Uvážíme elementární řez daný vrcholy, do kterých vede zlepšující cesta, a jejich doplňkem. Rozmyslíme si, co musí téct po různých typech hran. Odhadem velikosti toku pomocí řezu dostaneme druhou nerovnost. □

Fordův–Fulkersonův algoritmus

Sice již víme, jak ověřit, že daný tok je maximální velikosti, ale neumíme takový tok sami najít. Naštěstí prosté zvyšování toku v některých případech funguje. Přesněji, pokud jsou kapacity racionální čísla, můžeme použít následující algoritmus:

(i) Vezmeme vhodný tok s racionálními x_{ij}, třeba nulový.
(ii) Pokud neexistuje další zlepšující cesta ze zdroje do stoku, jsme hotovi.
(iii) Najdeme zlepšující cestu $v_1, v_2, \ldots, v_n$ ze zdroje do stoku a zvýšíme průtok touto cestou o δ, kde

$$\delta = \min_i \{c(v_i v_{i+1}) - f(v_i v_{i+1}) + f(v_{i+1} v_i)\},$$

přičemž $f(v_{i+1} v_i)$ simuluje zvýšení toku po směru tím, že snížíme tok v protisměru.
(iv) Vrátíme se k (ii).

Tvrzení. *Pro sítě s celočíselnými kapacitami nalezne Fordův–Fulkersonův algoritmus v konečném čase tok maximální velikosti, který navíc bude mít celočíselné hodnoty.*

Myšlenka důkazu. Pokud jsou kapacity celočíselné, pak každá iterace Fordova-Fulkersonova algoritmu zvětší tok aspoň o 1. Myšlenkami z důkazu věty o maximálním toku a minimální řezu pak ukážeme, že kdykoliv ještě nemáme maximální tok, tak existuje nějaká zlepšující cesta. Maximálního toku tudíž dosáhneme v konečném čase a bude celočíselný. □

Důsledek. *Pro síť s racionálními kapacitami existuje tok s maximální velikostí a s racionálními $c(ij)$.*

Úlohy

Úloha 1. Rozmyslete si, že pomocí případu s jedním zdrojem i stokem lze řešit situace s libovolným počtem zdrojů a stoků.

Úloha 2. Na kolejích jsou různé kluby, koleják může být součástí libovolného počtu klubů. Rozhodněte, zda lze vybrat z každého klubu předsedu a místopředsedu tak, aby každý koleják byl vybrán za nejvýš jeden klub a pro něj do právě jedné funkce.

Úloha 3. Řekneme, že graf je hranově k-souvislý, když je souvislý a zůstane souvislý i po odebrání libovolných $k-1$ nebo méně hran. Dokažte, že je graf hranově k-souvislý právě tehdy, když mezi každými dvěma vrcholy vede alespoň k hranově disjunktních cest.

Úloha 4. Máme šachovnici $m \times n$ a na některých políčkách stojí sloupy. Na políčka (bez sloupů) je možno umísťovat věže. Každá věž ohrožuje políčka ve stejné řadě a stejném sloupci, ale pouze k nejbližšímu sloupu v daném směru. Vymyslete, jak zjistit maximální počet věží, který je možno rozmístit tak, aby žádná nestála na políčku ohroženém jinou věží.

Úloha 5. Řekneme, že graf je vrcholově k-souvislý, když má alespoň $k+1$ vrcholů, je souvislý a zůstane souvislý i po odebrání libovolných $k-1$ nebo méně vrcholů. Dokažte, že je graf vrcholově k-souvislý právě tehdy, když mezi každýma dvěma vrcholy vede alespoň k cest vrcholově disjunktních až na počáteční a koncový vrchol.

Úloha 6. (Hallova věta) Máme takový systém množin, že kdykoli sjednotíme několik z nich, bude sjednocení vždy obsahovat alespoň tolik prvků, kolik množin jsme sjednotili. Dokažte, že je možné v každé množině zakroužkovat jeden prvek tak, aby zakroužkované prvky byly navzájem různé.

Návody

1. Přidej do grafu nový zdroj spojený s původními zdroji, podobně pro stok. Porovnej, jak vypadají zlepšující cesty v nové síti.

2. Vytvoř bipartitní graf studentů a klubů a rozmysli si, které kapacity nemají být jednotkové. Pokud má tok velikost dvojnásobku počtu klubů, výběr je možný.

3. U implikace zprava doleva předpokládej existenci množiny hran která má velikost nejvýše $k-1$ a přeruší všechny cesty mezi danými vrcholy a dojdi ke sporu. Mějme dány dva vrchohly u a v. Použij u jako zdroj v jako stok a nahraď hrany $ab \in E$ dvojicí orientovaných hran (ab) a (ba). Každá hrana má kapacitu 1, použij základní větu o tocích. Rozmysli si, že to že tok může používat hranu mezi dvěma vrcholy v obou směrech, lze ošetřit odečtením těchto smyček. Odhadni, že velikost toku musí být alespoň k a indukcí pomocí něj vytvoř jednotlivé cesty.

4. Rozděl si sloupce na souvislé úseky S, stejně tak řady R. Rozmysli si, že pár sloupcového a řádkového úseku jednoznačně určuje pole. Rozmysli si, že hledáme párování R a S, a použij bipartitní graf.

5. U implikace zprava doleva předpokládej existenci množiny vrcholů, která má velikost nejvýše $k-1$ a přeruší všechny cesty mezi danými vrcholy a dojdi ke sporu. Mějme dány dva vrchohly u a v. Použij u jako zdroj v jako stok a nahraď hrany $ab \in E$ dvojicí orientovaných hran (ab) a (ba). Každý vrchol x nahrad dvojicí vrcholů y a z, kde do y vedou všechny příchozí hrany a ze z vedou všechny odchozí hrany původního vrcholu. Kapacitu yz nastav jednotkovou, použij základní větu o tocích. Rozmysli si, že můžeme předpokládat, že minimální řez používá pouze hrany zorientovaného G, zvlášť ošetři hranu uv existuje-li. Odhadni velikost toku a rozmysli si, že cesty v novém grafu odpovídají hranově disjunktním cestám v G a pomocí nich indukcí vytvoř cesty.

6. Jednu implikaci dostaneme pomocí toho, zobrazení z množiny na reprezentanta musí být prosté. Opačnou implikaci dokážeme pomocí toků na bipartitním grafu, kde jednu partitu tvoří množiny a druhou jejich prvky. Kapacita 1 přitéká do jednotlivých množin, z každé množiny pak do jejích prvků a z každého prvku pak kapacita 1 do stoku. Kapacitu hran mezi množinami a prvky nastavíme dostatečně velkou(např. počet vrcholů), takže nalezený nejmenší řez nepoužije žádnou z těchto hran(jinak by nebyl nejmenší). Rozborem případů pak odhadneme velikost sjednocení množin.

Literatura a zdroje

[1] Mirek Olšák: *Toky v sítích*, Staré Město, 2015.
[2] Pavel Turek: *Toky v sítích*, Paseky, 2018.
[3] Zápisky z předmětu *Kombinatorika a grafy I* na MFF UK.
[4] Zápisky z předmětu *Algoritmy a datové struktury II* na MFF UK.

Chinese dumbass notation a SOS

Radek Olšák

Abstrakt. Co dělat, když dostanete v olympiádě nerovnost a dojde vám zásoba triků? Roznásobit, roznásobit, roznásobit. Většina metod na řešení nerovností dává krátká elegantní řešení. Toto není jedna z nich. Metoda CDN (Chinese dumbass notation) je široce aplikovatelná metoda, která nerovnosti dokazuje bez velkých triků.

Definice. Polynom tří proměnných x, y, z nazveme *homogenní*, pokud pro všechny členy platí, že součet stupňů všech tří proměnných je konstantní v celém polynomu.

Zápis polynomů v CDN

V této přednášce se budeme zabývat zápisem homogenních polynomů ve třech kladných proměnných. Aby byl celý výraz přehlednější, zapíšeme si jejich koeficienty do trojúhelníka o $d+1$ řádcích, kde d je stupeň polynomu. V každém řádku jsou všechny členy s pevným stupněm proměnné x a tento stupeň se snižuje odshora dolů. Obdobná vlastnost platí i pro ostatní proměnné – stačí si natočit trojúhelník jiným vrcholem nahoru. Vše objasní následující příklady zápisu polynomů:

$$\begin{pmatrix} [x] \\ [y] \quad [z] \end{pmatrix}, \quad \begin{pmatrix} [x^2] \\ [xy] \quad [xz] \\ [y^2] \quad [yz] \quad [z^2] \end{pmatrix}, \quad \begin{pmatrix} [x^3] \\ [x^2y] \quad [x^2z] \\ [xy^2] \quad [xyz] \quad [xz^2] \\ [y^3] \quad [y^2z] \quad [yz^2] \quad [z^3] \end{pmatrix}, \quad \begin{pmatrix} [x^4] \\ [x^3y] \quad [x^3z] \\ [x^2y^2] \quad [x^2yz] \quad [x^2z^2] \\ [xy^3] \quad [xy^2z] \quad [xyz^2] \quad [xz^3] \\ [y^4] \quad [y^3z] \quad [y^2z^2] \quad [yz^3] \quad [z^4] \end{pmatrix}.$$

Sčítání dvou trojúhelníků, které mají stejnou velikost, funguje po složkách. Tečky značí nuly.

$$\begin{pmatrix} & & \cdot & & \\ & \cdot & & \cdot & \\ \cdot & & -1 & & \cdot \\ 1 & 1 & & 1 & 1 \end{pmatrix} + \begin{pmatrix} & & 3 & & \\ & \cdot & & \cdot & \\ 2 & & 2 & & 2 \\ -3 & \cdot & & \cdot & -3 \end{pmatrix} = \begin{pmatrix} & & 3 & & \\ & \cdot & & \cdot & \\ 2 & & 1 & & 2 \\ -2 & 1 & & 1 & -2 \end{pmatrix}.$$

Abychom mohli trojúhelníky mezi sebou násobit, uvědomíme si nejdříve, jak se násobí trojúhelníkem obsahujícím jen jeden nenulový člen. Celý trojúhelník zakořeníme na pozici tohoto členu a pronásobíme jeho velikostí:

$$\begin{pmatrix} \cdot & \\ \cdot & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & & \\ 2 & 3 & \\ 4 & 5 & 6 \end{pmatrix} = 2 \cdot \begin{pmatrix} \cdot & & \\ \cdot & 1 & \\ 2 & 3 & \\ 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} \cdot & & & \\ \cdot & 2 & & \\ \cdot & 4 & 6 & \\ \cdot & 8 & 10 & 12 \end{pmatrix}.$$

Na obecné dva trojúhelníky pak aplikujeme základní roznásobování:

$$\begin{pmatrix} \cdot & & \\ \cdot & 2 & \\ 3 & \cdot & \cdot \end{pmatrix} \cdot \begin{pmatrix} 1 & \\ 3 & 2 \end{pmatrix} = 2 \begin{pmatrix} \cdot & & & \\ \cdot & 1 & & \\ \cdot & 3 & 2 & \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix} + 3 \begin{pmatrix} \cdot & & & \\ \cdot & \cdot & & \\ 1 & \cdot & \cdot & \\ 3 & 2 & \cdot & \cdot \end{pmatrix} = \begin{pmatrix} \cdot & & & \\ \cdot & 2 & & \\ 3 & 6 & 4 & \\ 9 & 6 & \cdot & \cdot \end{pmatrix}.$$

Cvičení. Zapište v trojúhelníkovém tvaru:

- $x^3 + y^3 + z^3$,
- $(x + y + z)^3$,
- $(x + y + z)(x^2 + y^2 + z^2)$,
- $(x + y + z)(xy + yz + zx)$,
- $(x + y)(y + z)(z + x)$,
- $\sum_{\text{cyc}} (x + y - z)^2$,
- $\sum_{\text{cyc}} x(x + y)(x + z)$,
- $\sum_{\text{cyc}} (2x + y + z)^2$,
- $\sum_{\text{cyc}} (3x + y)^3$.

Nerovnosti v CDN

Věta. (vážená AG nerovnost) *Máme několik kladných čísel v trojúhelníku a v místě jejich váženého průměru máme záporně jejich součet (viz příklady). Pak hodnota polynomu, který tento trojúhelník představuje, je nezáporná.*

$$\begin{pmatrix} & 1 & \\ \cdot & -2 & \\ \cdot & \cdot & 1 \end{pmatrix}, \quad \begin{pmatrix} & \cdot & & \\ \cdot & & \cdot & \\ \cdot & \cdot & & \cdot \\ 2 & -3 & \cdot & 1 \end{pmatrix}, \quad \begin{pmatrix} & 1 & & \\ \cdot & & \cdot & \\ \cdot & -3 & & \cdot \\ 1 & \cdot & \cdot & 1 \end{pmatrix}.$$

Věta. (sudé mocniny) *Další šikovnou, triviálně platnou, nerovností je nerovnost* $(x - y)^{2n} \geq 0$. *Pro* $n = 1$ *a* $n = 2$ *vypadá následovně:* $(1, -2, 1)$, $(1, -4, 6, -4, 1)$. *První již máme pomocí AG dokázanou, oproti tomu ta druhá pomocí jednoduchého sčítání AG dokázat nelze.*

Věta. (Muirheadova nerovnost) *Máme dva symetrické šestiúhelníky. Jeden tvoří jedničky, druhý mínus jedničky a oba mají stejné těžiště (viz první dva obrazce). Přitom šestiúhelník z mínus jedniček je uvnitř konvexního obalu šestiúhelníka z jedniček. Šestiúhelník může zdegenerovat do trojúhelníka dvojek (třetí ukázka). Pak hodnota polynomu, který tento trojúhelník představuje, je nezáporná.*

$$\begin{pmatrix} & & & \cdot & & & \\ & & \cdot & & \cdot & & \\ & 1 & \cdot & & \cdot & 1 & \\ \cdot & -1 & -1 & & \cdot & & \\ 1 & -1 & \cdot & -1 & \cdot & 1 & \\ \cdot & \cdot & -1 & -1 & \cdot & \cdot & \\ \cdot & \cdot & 1 & \cdot & 1 & \cdot & \cdot \end{pmatrix}, \quad \begin{pmatrix} & & & \cdot & & & \\ & & \cdot & & \cdot & & \\ & 1 & -1 & & 1 & & \\ -1 & \cdot & \cdot & & \cdot & -1 & \\ 1 & \cdot & \cdot & & \cdot & & 1 \\ \cdot & -1 & \cdot & \cdot & -1 & \cdot & \\ \cdot & \cdot & 1 & -1 & 1 & \cdot & \cdot \end{pmatrix}, \quad \begin{pmatrix} & & 2 & & \\ & -1 & & -1 & \\ -1 & & \cdot & & -1 \\ 2 & -1 & & -1 & 2 \end{pmatrix}.$$

Věta. (Schurova nerovnost) *Máme tři stejně velké kosočtverce z jedniček a mínus jedniček, které tvoří symetrický útvar jako na obrázku. Kosočtverce se mohou překrývat, v překrytém místě se jejich hodnoty sečtou. Hodnota takto vytvořeného polynomu je nezáporná.*

$$\begin{pmatrix} & & 1 & & \\ & -1 & & -1 & \\ \cdot & & 1 & & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ -1 & 1 & \cdot & \cdot & 1 & -1 \\ 1 & -1 & \cdot & \cdot & \cdot & -1 & 1 \end{pmatrix}, \quad \begin{pmatrix} & & 1 & & \\ & -1 & & -1 & \\ \cdot & & 1 & & \cdot \\ -1 & 1 & \cdot & 1 & -1 \\ 1 & -1 & \cdot & -1 & 1 \end{pmatrix}, \quad \begin{pmatrix} & & 1 & & \\ & -1 & & -1 & \\ -1 & & 3 & & -1 \\ 1 & -1 & -1 & & 1 \end{pmatrix}, \quad \begin{pmatrix} & & & 1 & & & \\ & & \cdot & & \cdot & & \\ & -1 & & \cdot & & -1 & \\ \cdot & & \cdot & & \cdot & & \cdot \\ -1 & & \cdot & 3 & \cdot & & -1 \\ \cdot & & \cdot & & \cdot & & \cdot \\ 1 & \cdot & -1 & \cdot & -1 & \cdot & 1 \end{pmatrix}.$$

$$\begin{pmatrix} & & 1 & & \\ & \cdot & & \cdot & \\ -1 & & \cdot & & -1 \\ -1 & 1 & & 1 & -1 \\ \cdot & \cdot & 1 & \cdot & \cdot \\ 1 & \cdot & -1 & -1 & \cdot & 1 \end{pmatrix}, \quad \begin{pmatrix} & & \cdot & & \\ & \cdot & & \cdot & \\ \cdot & & \cdot & & \cdot \\ 1 & -1 & -1 & 1 & \\ \cdot & -1 & 3 & -1 & \cdot \\ \cdot & \cdot & -1 & -1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \end{pmatrix}, \quad \begin{pmatrix} & & \cdot & & \\ & \cdot & & \cdot & \\ \cdot & & 1 & & \cdot \\ & \cdot & -1 & -1 & \cdot \\ \cdot & & \cdot & & 1 & \cdot \\ & -1 & & 1 & & \cdot \\ \cdot & & 1 & -1 & & 1 & -1 \\ & \cdot & & \cdot & & -1 & 1 & \cdot \end{pmatrix}.$$

Všechny nerovnosti budeme řešit tím způsobem, že se nejdříve zbavíme zlomků vynásobením všech členů jejich společným jmenovatelem. Pracujeme s nerovností, takže je potřeba si hlídat, jestli to, čím násobíme, je kladné nebo záporné. Pokud nerovnost není homogenní, využijeme podmínku a tím ji homogenizujeme. Zapíšeme vše pomocí CDN a roznásobíme. Následně převedeme do tvaru $P \geq 0$ a od tohoto polynomu P odčítáme známé nerovnosti dokud se tím nezbavíme všech záporných členů. Až se nám to povede, je úloha dokázána.

Příklad. (Nesbittova nerovnost) Pro $x, y, z \geq 0$ dokažte:

$$\frac{x}{y+z} + \frac{y}{z+x} + \frac{z}{x+y} \geq \frac{3}{2}.$$

Řešení. Roznásobíme celou nerovnost výrazem $2(y+z)(z+x)(x+y)$, abychom se zbavili zlomků, a dostáváme:

$$2\sum_{\text{cyc}} x(x+y)(x+z) \geq 3(x+y)(y+z)(z+x).$$

Zapíšeme v CDN a roznásobíme:

$$2\sum_{\text{cyc}}\begin{pmatrix} 1 \\ \cdot\ \ \cdot \end{pmatrix}\begin{pmatrix} 1 \\ 1\ \ \cdot \end{pmatrix}\begin{pmatrix} 1 \\ \cdot\ \ 1 \end{pmatrix} \geq 3\begin{pmatrix} 1 \\ 1\ \ \cdot \end{pmatrix}\begin{pmatrix} \cdot \\ 1\ \ 1 \end{pmatrix}\begin{pmatrix} 1 \\ \cdot\ \ 1 \end{pmatrix},$$

$$\sum_{\text{cyc}}\begin{pmatrix} 2 \\ 2\ \ 2 \\ \cdot\ \ 2\ \ \cdot \\ \cdot\ \ \cdot\ \ \cdot\ \ \cdot \end{pmatrix} \geq 3\begin{pmatrix} \cdot \\ 1\ \ 1 \\ 1\ \ 2\ \ 1 \\ \cdot\ \ 1\ \ 1\ \ \cdot \end{pmatrix},$$

$$\begin{pmatrix} 2 \\ 2\ \ 2 \\ 2\ \ 6\ \ 2 \\ 2\ \ 2\ \ 2\ \ 2 \end{pmatrix} \geq \begin{pmatrix} \cdot \\ 3\ \ 3 \\ 3\ \ 6\ \ 3 \\ \cdot\ \ 3\ \ 3\ \ \cdot \end{pmatrix},$$

$$\begin{pmatrix} 2 \\ -1\ \ -1 \\ -1\ \ \ 0\ \ -1 \\ 2\ \ -1\ \ -1\ \ \ 2 \end{pmatrix} \geq 0.$$

Dostali jsme tedy tvar, který potřebujeme. Zbývá najít, jak tuto nerovnost zapsat jako součet známých nerovností. To uděláme postupným odečítáním známých nerovností. Pokud se takto zbavíme všech záporných čísel, nerovnost jsme nutně zapsali jako součet platných nerovností, jinými slovy platí. Můžeme rovnou říct, že tato nerovnost je přímo speciálním případem Muirheadovy nerovnosti, ale ukážeme si, jak ji dokázat pomocí AG. Využijeme následující AG k eliminaci jedné mínus jedničky:

$$\begin{pmatrix} \cdot \\ \cdot\ \ \cdot \\ \cdot\ \ \cdot\ \ \cdot \\ \frac{1}{3}\ \ \cdot\ \ -1\ \ \frac{2}{3} \end{pmatrix}.$$

Tento trojúhelník symetricky sečteme. Tím jsme se zbavili všech šesti mínus jedniček, takže jsme zapsali nalezený polynom jako součet nezáporných polynomů, tedy i tento polynom musí být nezáporný. □

Cvičení. Dokažte o následujících polynomech, že jsou nezáporné:

$$\begin{pmatrix} \cdot \\ 4\ \ 4 \\ -1\ \ 2\ -1 \\ -6\ -2\ -2\ -6 \\ -1\ -2\ \ 6\ -2\ -1 \\ 4\ \ 2\ -2\ -2\ \ 2\ \ 4 \\ \cdot\ \ 4\ -1\ -6\ -1\ \ 4\ \ \cdot \end{pmatrix}, \quad \begin{pmatrix} 3 \\ \cdot\ -4 \\ -4\ \ 3\ \ \cdot \\ 3\ \ \cdot\ -4\ \ 3 \end{pmatrix}, \quad \begin{pmatrix} 50 \\ 230\ \ 230 \\ 115\ \ 160\ \ 115 \\ 10\ -336\ -336\ \ 10 \\ 115\ -336\ -714\ -336\ \ 115 \\ 230\ \ 160\ -336\ -336\ \ 160\ \ 230 \\ 50\ \ 230\ \ 115\ \ 10\ \ 115\ \ 230\ \ 50 \end{pmatrix}.$$

Úlohy

Poznámka. Ve všech úlohách předpokládáme $x, y, z \geq 0$.

Dokažte následující nerovnosti.

Úloha 1. $(x+y-z)(y+z-x)(z+x-y) \leq xyz$.

Úloha 2. $(xy+yz+zx)^2 \geq 3xyz(x+y+z)$.

Úloha 3. $\frac{x^3}{yz}+\frac{y^3}{zx}+\frac{z^3}{xy} \geq x+y+z$.

Úloha 4. $(x+y+z)^2+\frac{9xyz}{x+y+z} \geq 4(xy+yz+zx)$.

Úloha 5. $\frac{xy}{x+y}+\frac{yz}{y+z}+\frac{zx}{z+x} \leq \frac{3(xy+yz+zx)}{2(x+y+z)}$.

Úloha 6. $\frac{x^2}{y+z}+\frac{y^2}{z+x}+\frac{z^2}{y+x} \geq \frac{x+y+z}{2}$.

Úloha 7. (Česko-slovensko-polské střetnutí) $\frac{x}{y+2z}+\frac{y}{z+2x}+\frac{z}{x+2y} \geq 1$.

Úloha 8. $8(x^3+y^3+z^3)^2 \geq 9(x^2+yz)(y^2+zx)(z^2+xy)$.

Úloha 9. $\sum_{\text{cyc}} \frac{x^2+y^2}{z} \geq 2(x+y+z)$.

Úloha 10. $\sum_{\text{cyc}} \frac{1}{a} \geq \sum_{\text{cyc}} \frac{a+b}{ab+c^2}$

Úloha 11. $\sum_{\text{cyc}} \frac{x^2-z^2}{y+z} \geq 0$.

Úloha 12. $(x+2y+z)(x+y+z)^2 \geq 4(x+y)(y+z)(z+x)$.

Úloha 13. $xy+\frac{y}{x}+\frac{x}{y} \geq x+y+1$.

Úloha 14. $\frac{yz}{2x+y+z}+\frac{zx}{2y+z+x}+\frac{xy}{2z+x+y} \leq \frac{1}{4}(x+y+z)$.

Úloha 15. Pro $x+y+z=1$ dokažte $x^3+y^3+z^3+6xyz \geq \frac{1}{4}$.

Úloha 16. $(x^2y+y^2z+z^2x)(x^2z+z^2y+y^2x) \geq 9x^2y^2z^2$.

Úloha 17. (USAMO 1997) $\sum_{\text{cyc}} \frac{1}{x^3+y^3+xyz} \leq \frac{1}{xyz}$.

Úloha 18. Pro $a+b+c=3$ dokažte $\sum_{\text{cyc}} \frac{x(y+z)}{y^2+z^2} \geq \frac{9}{2(xy+yz+zx)-3xyz}$

Úloha 19. (IMO 1984/1) Pro $x+y+z=1$ dokažte $0 \leq xy+yz+zx-2xyz \leq \frac{7}{27}$.

Úloha 20. (Iran 1996) $(xy+yz+zx)(\frac{1}{(x+y)^2}+\frac{1}{(y+z)^2}+\frac{1}{(z+x)^2}) \geq \frac{9}{4}$.

Úloha 21. Pro $x+y+z=3$ dokažte $\frac{1}{x}+\frac{1}{y}+\frac{1}{z}-1 \geq 2\sqrt{\frac{x^2+y^2+z^2}{3xyz}}$.

Úloha 22. (IMO 2002/2) Pro $xyz=1$ dokažte $\left(x-1+\frac{1}{y}\right)\left(y-1+\frac{1}{z}\right)\left(z-1+\frac{1}{x}\right) \leq 1$.

Úloha 23. (Turnaj měst 1997) Pro $xyz=1$ dokažte $\frac{1}{x+y+1}+\frac{1}{y+z+1}+\frac{1}{z+x+1} \leq 1$.

Úloha 24. (IMO 2005) Pro $xyz=1$ dokažte $\sum_{\text{cyc}} \frac{x^5-x^2}{x^5+y^2+z^2} \geq 0$.

Úloha 25. (IMO 1995) Pro $xyz=1$ dokažte $\sum_{\text{cyc}} \frac{1}{x^3(y+z)} \geq \frac{3}{2}$.

Úloha 26. Pro $\frac{1}{x}+\frac{1}{y}+\frac{1}{z}=x+y+z$ dokažte $\sum_{\text{cyc}} \frac{1}{(2x+y+z)^2} \leq \frac{3}{16}$.

Úloha 27. Pro $x+y+z=1$ dokažte $\left(\frac{1}{x}+1\right)\left(\frac{1}{y}+1\right)\left(\frac{1}{z}+1\right) \geq 64$.

Úloha 28. (Japan TST 2004) Pro $x+y+z=1$ dokažte $\frac{1+x}{1-x}+\frac{1+y}{1-y}+\frac{1+z}{1-z} \leq \frac{2x}{y}+\frac{2y}{z}+\frac{2z}{x}$.

SOS

Příklad 29. (nerovnost Vasileho Cirtoajeho) Pro kladná a, b, c dokažte

$$(a^2+b^2+c^2)^2 \geq 3(a^3b+b^3c+c^3a).$$

Řešení. Tahle nerovnost je velmi zrádná. Na první pohled působí nevinně, má stupeň 4, jen tři proměnné a je homogenní. Po zapsání do CDN vypadá následovně:

$$\begin{pmatrix} & & 1 & & \\ & -3 & \cdot & & \\ 2 & \cdot & 2 & & \\ \cdot & \cdot & \cdot & -3 & \\ 1 & -3 & 2 & \cdot & 1 \end{pmatrix}$$

Hned je vidět v čem je problém, záporné trojky jsou hrozně blízko kraje a v rozích máme jen jedničky. To pomocí našich kanónů nepadne. A jak tedy vypadá řešení? Polynom přepíšeme do tvaru

$$\frac{1}{2}\sum_{\text{cyc}}(a^2-b^2-ab+2bc-ca)^2,$$

čímž je nerovnost dokázána.

Jak na tohle někdo přišel? To vám nepovím, ale co si z příkladu odnést je, že cyklické nerovnosti se často dají dokázat kouzelným přepsáním do součtu čtverců. Zároveň to je způsob jak vymýšlet netriviální nerovnosti – vzít si nějaký náhodný polynom, umocnit ho na druhou a cyklicky sečíst.

Úloha 30. Vymysli si vlastní úlohu, kterou nedokážeš vyřešit jednoduchým AG a Schurem.

Protože převod do obecných součtů čtverců je těžký, budeme si muset vystačit s nějakým jednodušším tvarem. Ten tvar bude

$$S = S_a(b-c)^2 + S_b(c-a)^2 + S_c(a-b)^2,$$

je znám pod názvem „Sum Of Squares“ a zkratkou SOS. Ještě budeme pro větší přehlednost chtít, aby se výrazy S_a, S_b, S_c lišily pouze cyklickou záměnou proměnných. Převod do takového tvaru není složitý, v trojúhelníčku stačí odčítat cyklicky $(1,-2,1)$ a zapisovat si, kde jsme je odečetli.[1]

[1] Dokonce každý cyklický polynom se součtem koeficientů rovným 0 lze v SOS nějak zapsat.

Příklad 31. Pro $a, b, c > 0$ dokažte nerovnost

$$2(a^2+b^2+c^2)^2 \geq 3(a^3(b+c)+b^3(c+a)+c^3(a+b)).$$

Řešení. Nerovnost zapíšeme v CDN jako

$$\begin{pmatrix} & & 2 & & \\ & -3 & & -3 & \\ 4 & & \cdot & & 4 \\ & -3 & & -3 & \\ 2 & & -3 & & 2 \end{pmatrix},$$

což následně rozepíšeme jako součet cyklických $(1,-2,1)$:

$$\begin{pmatrix} & & 1 & & \\ & -2 & & \cdot & \\ \cdot & & 1 & & 1 \\ & \cdot & & -2 & \\ 1 & & -2 & & 1 \end{pmatrix} + \begin{pmatrix} & & \cdot & & \\ & -1 & & -1 & \\ 2 & & \cdot & & 2 \\ & -1 & & -1 & \\ \cdot & & -1 & & \cdot \end{pmatrix} + \begin{pmatrix} & & 1 & & \\ & \cdot & & -2 & \\ 1 & & \cdot & & 1 \\ & -2 & & \cdot & \\ 1 & & -2 & & 1 \end{pmatrix}.$$

Tím dostáváme rozklad na

$$\sum_{\text{cyc}} \begin{pmatrix} & \cdot & \\ \cdot & & \cdot \\ 1 & -1 & 1 \end{pmatrix} (b-c)^2,$$

ale všechny tyto členy jsou kladné, tedy jsme dokázali nerovnost.

Může se stát, že nám nevyjdou všechny členy přímo kladné. Pak ale stále nemusíme zoufat, může nám pomoci následující tvrzení.

Věta 32. *Mějme $S = S_a(b-c)^2 + S_b(c-a)^2 + S_c(a-b)^2$. Pokud je splněna nějaká z následujících podmínek, tak je $S \geq 0$.*

1. *(Vyvážíme dvojnásobek) S_a, S_c, $S_a + 2S_b$ a $S_c + 2S_b$ jsou nezáporné.*
2. *(Prostřední převáží) S_b, $S_a + S_b$ a $S_b + S_c$ jsou nezáporné, kde b je medián a, b, c.*
3. *(Dva proti jednomu) S_b, S_c a $b^2S_a + a^2S_b$ jsou nezáporné, kde $a \geq b \geq c$ nebo $c \geq b \geq a$.*
4. *(Cyklické součty) $S_a + S_b + S_c$ a $S_aS_b + S_bS_c + S_cS_a$ jsou nezáporné.*

Důkaz. Pro důkazy se hodí postupně tato pozorování

1. $2(a-b)^2 + 2(b-c)^2 - (a-c)^2 = (a+c-2b)^2 \geq 0$
2. $(b-c)(b-a) \leq 0 \Rightarrow (a-c)^2 \geq (a-b)^2 + (b-c)^2$
3. $\frac{a-c}{b-c} \geq \frac{a}{b} \Rightarrow (a-c)^2 \geq \frac{a^2}{b^2}(b-c)^2$
4. BÚNO $S_a + S_b \geq 0$. Diskriminant polynomu kde $x = b-c$ a $t = a-b$. □

Příklad 33. (Schurova nerovnost) Zatím jsme si ukazovali Schurovu nerovnost jen v jejím trojúhelníkovém tvaru, standardně ale vypadá takto

$$a^t(a-b)(a-c)+b^t(b-a)(b-c)+c^t(c-a)(c-b)\geq 0$$

Řešení. Nejdříve si vyzkoušíme našeho známého Schura pro $t=1$:

$$\begin{pmatrix} & & 1 & \\ & -1 & -1 & \\ -1 & & 3 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

Kvůli zachování symetrie si odečteme $\frac{1}{2}\sum_{\text{cyc}}(b+c)(b-c)^2$. Zbude nám šestiúhelníček, který zapíšeme jako $\frac{1}{2}\sum_{\text{cyc}} -a(b-c)^2$, tedy celkově máme

$$S_a=\frac{1}{2}\begin{pmatrix} & -1 & \\ 1 & & 1 \end{pmatrix},\qquad S_b=\frac{1}{2}\begin{pmatrix} & 1 & \\ -1 & & 1 \end{pmatrix},\qquad S_c=\frac{1}{2}\begin{pmatrix} & 1 & \\ 1 & & -1 \end{pmatrix}.$$

Protože je nerovnost symetrická, tak BÚNO $a\geq b\geq c$, pak je $S_b\geq 0$, zároveň

$$S_b+S_c=\frac{1}{2}\begin{pmatrix} & 2 & \\ \cdot & & \cdot \end{pmatrix}\geq 0,\qquad S_b+S_a=\frac{1}{2}\begin{pmatrix} & \cdot & \\ \cdot & & 2 \end{pmatrix}\geq 0.$$

Tedy z tvrzení *Prostřední převáží* Schurova nerovnost pro $t=1$ platí.

Pro obecný důkaz se podíváme se na člen $(a-b)(a-c)$ a zapíšeme ho jako součet nějakých výrazů $(1,-2,1)$. Dostaneme identitu

$$(a-b)(a-c)=\frac{1}{2}((a-c)^2+(a-b)^2-(b-c)^2).$$

V CDN to vypadá následovně:

$$\begin{pmatrix} & 1 & \\ -1 & -1 & \\ \cdot & 1 & \cdot \end{pmatrix}=\frac{1}{2}\left(\begin{pmatrix} & 1 & \\ -2 & \cdot & \\ 1 & \cdot & \cdot \end{pmatrix}+\begin{pmatrix} & 1 & \\ \cdot & -2 & \\ \cdot & \cdot & 1 \end{pmatrix}+\begin{pmatrix} & \cdot & \\ \cdot & \cdot & \\ -1 & 2 & -1 \end{pmatrix}\right).$$

Tedy výraz ze zadání můžeme přepsat jako

$$\frac{1}{2}\sum_{\text{cyc}}(b^t+c^t-a^t)(b-c)^2.$$

Tedy znovu pomocí *Prostřední převáží* nerovnost platí.

Poznámka 34. Tvar SOS není jednoznačný, takže i když se nám povede polynom nějak zapsat, ale ne dokázat nerovnost, můžeme se jej pokusit zapsat v jiném SOS tvaru, který by se s úlohou zvládl lépe poprat.

Další úlohy

Ve všech následujících úlohách předpokládáme $a, b, c \geq 0$.

Úloha 35. Dokažte, že

$$2(a^6+b^6+c^6)+16(a^3b^3+b^3c^3+c^3a^3) \geq 9a^4(b^2+c^2)+9b^4(c^2+a^2)+9c^4(a^2+b^2).$$

Úloha 36. $a^5+2b^5+8b^3a^2 \geq 7b^4a+2a^3b(a+b)$.

Úloha 37. Dokažte o následujících polynomech, že jsou nezáporné:

$$\begin{pmatrix} & & & 1 & & & \\ & & -1 & -1 & & & \\ & & 1 & -4 & 1 & & \\ & 1 & 3 & 3 & 1 & & \\ -1 & -4 & 3 & -4 & -1 & & \\ 1 & -1 & 1 & 1 & -1 & 1 \end{pmatrix}, \quad \begin{pmatrix} & & & \cdot & & & \\ & & & 1 & 1 & & \\ & & 1 & -10 & 1 & & \\ & 1 & 6 & 6 & 1 & & \\ 1 & -10 & 6 & -10 & 1 & & \\ \cdot & 1 & 1 & 1 & 1 & \cdot \end{pmatrix}, \quad \begin{pmatrix} & & & 1 & & & \\ & & \cdot & -1 & & & \\ & & \cdot & -8 & 2 & & \\ & 2 & 6 & 6 & \cdot & & \\ -1 & -8 & 6 & -8 & \cdot & & \\ 1 & \cdot & \cdot & 2 & -1 & 1 \end{pmatrix}.$$

Úloha 38. Jsou-li a, b, c délky stran trojúhelníka, dokažte

$$a^3(b-c)+b^3(c-a)+c^3(a-b)+2(a^2b^2+b^2c^2+c^2a^2) \geq 2abc(a+b+c).$$

Úloha 39. $\frac{a^2+b^2+c^2}{ab+bc+ca}+\frac{8abc}{(a+b)(b+c)(c+a)} \geq 2$.

Úloha 40. $\sum_{\text{cyc}} \frac{(a+b)^2}{c^2+ab} \geq 6$.

Úloha 41. Pro $a+b+c=1$ dokažte $\frac{1}{abc}+\frac{4}{a^2+b^2+c^2} \geq \frac{13}{ab+bc+ca}$.

Úloha 42. $\frac{a^2}{b+c}+\frac{b^2}{c+a}+\frac{c^2}{a+b} \geq \frac{3}{2}\cdot\frac{a^3+b^3+c^3}{a^2+b^2+c^2}$.

Úloha 43. $\sum_{\text{cyc}} \left(\frac{1}{b+c}\right)+\frac{abc}{2(a^3+b^3+c^3)} \geq \frac{5}{3}$.

Úloha 44. $8a^2b^2c^2 \geq (a+b)(b+c)(c+a)(a+b-c)(b+c-a)(c+a-b)$.

Úloha 45. $\frac{a^3+b^3+c^3}{3abc}+\sum_{\text{cyc}} \frac{a(b+c)}{b^2+c^2} \geq 4$.

Úloha 46. $a(a-b)(a-2b)+b(b-c)(b-2c)+c(c-a)(c-2a) \geq 0$.

Úloha 47.

$$\begin{pmatrix} & & & \cdot & & & \\ & & \cdot & & \cdot & & \\ & & 1 & -2 & 1 & & \\ & -2 & 2 & 2 & -2 & & \\ 1 & 2 & -6 & 2 & 1 & & \\ \cdot & -2 & 2 & 2 & -2 & \cdot & \\ \cdot & \cdot & 1 & -2 & 1 & \cdot & \cdot \end{pmatrix} \geq 0.$$

Návody

13. Přidej třetí proměnnou a homogenizuj pomocí $z=1$.

15. Nahraď podmínkou jedničku na pravé straně. Roznásob a nelekni se, že nesedí součet koeficientů.

21. Nahraď $1 = \frac{3}{x+y+z}$, umocni na druhou a bij.

22. Homogenizuj pomocí $(xyz)^{\frac{1}{3}} = 1$. Pokud se děsíš necelých exponentů, substituuj $x^3 = a$, $y^3 = b$, $z^3 = c$.

23. Homogenizuj pomocí $(xyz)^{\frac{1}{3}} = 1$. Pokud se děsíš necelých exponentů, substituuj $x^3 = a$, $y^3 = b$, $z^3 = c$.

25. Homogenizuj pomocí $(xyz)^{\frac{4}{3}} = 1$. Substituuj třetí mocniny. Kdopak by se 24. stupně bál.

26. Zbav se zlomků, stupně stran se liší o 2. Využij podmínku ve tvaru $xy + yz + zx = x^2yz + xy^2z + xyz^2$.

35. $\sum_{\text{cyc}}(b^4 + c^4 + 2b^3c + 2c^3b - 6b^2c^2)(b-c)^2$.

36. $(a^3 - 3ab^2 + 2b^3)(a-b)^2$.

38. $\sum_{\text{cyc}} a(a + c - b)(b-c)^2$.

39. $\sum_{\text{cyc}}(b^2c + c^2b - abc)(b-c)^2$.

40. $\sum_{\text{cyc}}(b^3c + c^3b + 3b^2c^2 - ab^2c - ac^2b + a^2bc)(b-c)^2$.

42. $\sum_{\text{cyc}}(b^4 + c^4 + bc^3 + cb^3 + a^3b + a^3c - 2b^2ac - 2c^2ab)(b-c)^2$.

43. $\sum_{\text{cyc}}(3b^4 + 3c^4 + 2b^3c + 2c^3b - 3b^2c^2 + a^3b + a^3c - b^2ac - c^2ab - a^2bc)(b-c)^2$.

44. $\sum_{\text{cyc}}(b^3c + c^3b + 2b^2c^2 - a^2bc)(b-c)^2$.

45. $\sum_{\text{cyc}}(b^5a^2 + c^5a^2 + a^5b^2 + a^5c^2 + 5ab^4c^2 + 5ac^4b^2 - a^2b^3c^2 - a^2c^3b^2 - 2a^4cb^2 - 2a^4bc^2 + 4b^2c^2a^3)(b-c)^2$.

46. $\frac{1}{3}\sum_{\text{cyc}}(4b-c)(b-c)^2$. Případ $c \geq b \geq a$ je lehký. Pro případ $a \geq b \geq c$ rozeber v neroznásobené formě podpřípad kdy $a \geq 2b$. Pro kouzelné řešení polynom vynásob polynomem $\sum_{\text{cyc}}(b-c)^2$.

47. Součet každého řádku je 0, takže pokud úloha platí, tak je polynom dělitelný $(b-c)^2$. A co symetrie? Už víš, co za polynom šestého stupně se v zadání skrývá? :-) Alternativně v SOS $S_a = b^2c^2 - abc^2 - acb^2 + a^2bc$, spočti cyklické součty.

Literatura a zdroje

[1] Brian Hamrick: *The Art of Dumbassing*, *https://www.tjhsst.edu/~2010bhamrick/files/dumbassing.pdf*.

[2] *https://www.quora.com/What-is-Chinese-Dumbass-Notation*.

[3] Evan Chen: *Supersums of Square-Weights (SOS) – A Dumbass Perspective*, *http://web.evanchen.cc/handouts/SOS_Dumbass/SOS_Dumbass.pdf*.

[4] Matěj Konečný: *Dvě techniky na nerovnosti*, *https://iksko.org/files/sbornik5.pdf*.

[5] Michal „Kenny“ Rolínek, Pavel Šalom: *Zdolávání nerovností*, seriál MKS, 2009/10.

Hilbertovský kalkulus

Daniel Perout

Abstrakt. Ve formální výrokové logice je mnohdy výhodné se nezabývat významem formulí, ale dívat se pouze na logické vztahy mezi nimi, resp. na strukturní vlastnosti logických spojek. Na rozdíl od významu jde struktura např. daleko lépe zpracovávat strojově. Tyto strukturní vlastnosti jde popsat několika systémy (zvané *kalkuly*), z nichž jeden v tomto příspěvku rozebereme podrobněji.

Definice. (formule) Nechť At označuje množinu atomických formulí. Dále budiž Fle nejmenší množina taková, že At $\subseteq$ Fle a navíc kdykoliv $\varphi, \psi \in$ Fle, pak i $\neg\varphi$, $\varphi \wedge \psi$, $\varphi \vee \psi$ a $\varphi \to \psi$ jsou prvky Fle. Prvky Fle pak nazýváme *formulemi*.

Definice. (důkaz v Hilbertovském kalkulu) Nechť T je množina formulí a φ je formule. Existuje-li posloupnost formulí $\psi_1, \ldots, \psi_n$ taková, že $\psi_n = \varphi$ a pro každou ψ_i platí jedno z následujích:

(i) ψ_i je prvkem T,
(ii) ψ_i je *instancí axiomu Hilbertovského kalkulu*,
(iii) ψ_i vznikla pravidlem *modus ponens* aplikovaným na nějaké dvě předcházející formule,

pak řekneme, že φ je *dokazatelná z* T, a zapisujeme $T \vdash \varphi$.

Axiomy Hilbertovského kalkulu:

(A1) $\varphi \to (\psi \to \varphi)$,
(A2) $(\varphi \to (\psi \to \chi)) \to ((\varphi \to \psi) \to (\varphi \to \chi))$,
(A3) $(\neg\varphi \to \neg\psi) \to ((\neg\varphi \to \psi) \to \varphi)$,
(A4) $\varphi \wedge \psi \to \varphi$, $\varphi \wedge \psi \to \psi$,
(A5) $\varphi \to (\psi \to (\varphi \wedge \psi))$,
(A6) $\varphi \to (\varphi \vee \psi)$, $\psi \to (\varphi \vee \psi)$,
(A7) $(\varphi \to \chi) \to ((\psi \to \chi) \to ((\varphi \vee \psi) \to \chi))$.

Pravidlo modus ponens (MP): $\varphi,\ \varphi \to \psi\ /\ \psi$ (čteme „z φ a $\varphi \to \psi$ odvoď ψ“).

Je nutné poznamenat, že výše uvádím jen jednu z mnoha variant Hilbertovského kalkulu. Jiné varianty můžou mít více či méně axiomů, které potom usnadňují dokazování nebo naopak se snaží předpoklady minimalizovat. Společným znakem je malý počet odvozovacích pravidel (většinou pouze MP). Konkrétní důkazy se sice mohou lišit, ale dokazovací síla kalkulů je (ve většině případů) stejná.

Věta. (o dedukci) *Nechť T je množina formulí a φ, ψ jsou formule.*[1] *Pak platí ekvivalence*

$$T \vdash \varphi \to \psi \iff T, \varphi \vdash \psi.$$

Důkaz. (náčrt) Implikaci zleva doprava dokážeme jednoduše: nechť $T \vdash \varphi \to \psi$, potom i $T, \varphi \vdash \varphi \to \psi$ (přidáním předpokladu si důkaz nerozbijeme), ale zároveň $T, \varphi \vdash \varphi$ a z toho už pravidlem MP $T, \varphi \vdash \psi$.

Opačná implikace je náročnější, bude vyžadovat indukci na délce důkazu $T, \varphi \vdash \psi$. V indukčním kroku uvážíme formuli χ_i, která je dokazatelná z T, φ, a ukážeme, že platí $T \vdash \varphi \to \chi_i$. Z toho pak už bude plynout $T \vdash \varphi \to \psi$. Netriviálním krokem tohoto postupu bude nalezení důkazu formule tvaru $\varphi \to \varphi$ z prázdné množiny předpokladů. Proto tuto speciální formuli dokážeme zvlášť. □

Věta. (o ekvivalenci) *Nechť φ a ψ jsou formule, kde ψ vznikne z φ nahrazením podformule ξ za ξ'. Pak platí:* $\{\xi \leftrightarrow \xi'\} \vdash \varphi \leftrightarrow \psi$. [2]

Důkazy formulí v bázi $\neg$, $\to$

Příklad. Nalezněte důkaz $\vdash \varphi \to \varphi$ bez využití věty o dedukci.

Řešení.

(1)	$(\varphi \to ((\varphi \to \varphi) \to \varphi)) \to ((\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi))$	A2
(2)	$\varphi \to ((\varphi \to \varphi) \to \varphi)$	A1
(3)	$\varphi \to (\varphi \to \varphi)$	A1
(4)	$(\varphi \to (\varphi \to \varphi)) \to (\varphi \to \varphi)$	MP(1,2)
(5)	$\varphi \to \varphi$	MP(4,3)

Úloha 1. (tranzitivita implikace) Nalezněte důkaz

$$\vdash (\varphi \to \psi) \to ((\psi \to \chi) \to (\varphi \to \chi)).$$

Úloha 2. Nalezněte důkaz $\vdash (\neg\varphi \to \varphi) \to \varphi$.

Úloha 3. Nalezněte důkaz $\vdash \neg\neg\varphi \to \varphi$.

Úloha 4. Nalezněte důkaz $\vdash \varphi \to \neg\neg\varphi$ bez využití věty o dedukci.[3]

Úloha 5. (obměna implikace) Nalezněte důkaz $\vdash (\neg\varphi \to \neg\psi) \leftrightarrow (\psi \to \varphi)$.

Úloha 6. Nalezněte důkaz $\vdash (\psi \to \varphi) \to ((\neg\psi \to \varphi) \to \varphi)$.

Úloha 7. Nalezněte důkaz

$$\{p_n \to p_m : n < m,\ n, m \in \mathbb{N}\} \vdash (p_{15} \to p_{15}) \to (p_{10} \to p_{15}).$$

Úloha 8. Nalezněte důkaz

$$\{p_n \to p_m : n < m,\ n, m \in \mathbb{N}\} \vdash (p_{15} \to p_{10}) \to (p_{14} \to p_{11}).$$

[1] Poznámka k notaci: prázdnou množinu nezapisujeme (tj. $\vdash \varphi \iff \emptyset \vdash \varphi$) a $T, \varphi = T \cup \{\varphi\}$.

[2] V HK formálně spojka $\leftrightarrow$ není, chápeme ji jako zkratku: $\varphi \leftrightarrow \psi = (\varphi \to \psi) \wedge (\psi \to \varphi)$.

[3] Dříve dokázané formule použít můžete.

Důkazy formulí se spojkami $\wedge$, $\vee$

Úloha 9. (komutativita konjunkce) Nalezněte důkaz $\vdash (\varphi \wedge \psi) \to (\psi \wedge \varphi)$.

Úloha 10. (asociativita konjunkce) Nalezněte důkaz $\vdash ((\varphi \wedge \psi) \wedge \chi) \to (\varphi \wedge (\psi \wedge \chi))$.

Úloha 11. Nalezněte důkaz $\vdash (\varphi \to (\psi \to \chi)) \leftrightarrow ((\varphi \wedge \psi) \to \chi)$.

Úloha 12. (komutativita disjunkce) Nalezněte důkaz $\vdash (\varphi \vee \psi) \to (\psi \vee \varphi)$.

Úloha 13. (asociativita disjunkce) Nalezněte důkaz $\vdash ((\varphi \vee \psi) \vee \chi) \to (\varphi \vee (\psi \vee \chi))$.

Úloha 14. (negace konjunkce) Nalezněte důkaz $\vdash \neg(\varphi \vee \psi) \to (\neg\varphi \wedge \neg\psi)$.

Úloha 15. (těžší) Nalezněte důkaz $\vdash (\varphi \to \psi) \leftrightarrow (\neg\varphi \vee \psi)$.

Úloha 16. Nalezněte důkaz $\vdash ((\varphi \vee \psi) \wedge (\varphi \vee \chi)) \to (\varphi \vee (\psi \wedge \chi))$.

Úplnost Hilbertovského kalkulu

Definice. (ohodnocení) Nechť v: Fle $\to \{0, 1\}$ je zobrazení. O v řekneme, že je *ohodnocením*, platí-li pro libovolnou formuli φ:

(i) Je-li φ tvaru $\neg\psi$, pak $v(\varphi) = 1$, právě když $v(\psi) = 0$,
(ii) Je-li φ tvaru $\psi \to \chi$, pak $v(\varphi) = 1$, právě když $v(\psi) = 0$ nebo $v(\chi) = 1$,
(iii) Je-li φ tvaru $\psi \wedge \chi$, pak $v(\varphi) = 1$, právě když $v(\psi) = 1$ a $v(\chi) = 1$,
(iv) Je-li φ tvaru $\psi \vee \chi$, pak $v(\varphi) = 1$, právě když $v(\psi) = 1$ nebo $v(\chi) = 1$.

Úmluva. Řekneme, že ohodnocení v splňuje formuli φ, pokud $v(\varphi) = 1$. Dále řekneme, že ohodnocení splňuje množinu formulí T, pokud splňuje každou formuli $\psi \in T$.

Definice. (vyplývání) Nechť T je množina formulí a φ je formule. Pak řekneme, že φ *vyplývá* z T (značíme $T \vDash \varphi$), pokud každé ohodnocení, které splňuje T, splňuje i φ.

Věta. (o úplnosti) *Nechť T je množina formulí a φ formule. Pak platí*

$$T \vDash \varphi \iff T \vdash \varphi.$$

Příklad. Rozhodněte, zda jsou formule φ, $\varphi \wedge \neg\varphi$ a $\varphi \vee \neg\varphi$ dokazatelné z prázdné množiny předpokladů.

Řešení. Z věty o úplnosti víme, že formule je dokazatelná z prázdné množiny předpokladů, právě když je tautologií (tj. platí při libovolném ohodnocení). Jediná tautologie ze zadaných formulí je $\varphi \vee \neg\varphi$, tudíž pouze tato formule je dokazatelná z $\emptyset$, ostatní jsou nedokazatelné.

Úloha. Rozhodněte, zda platí (najděte důkaz, nebo protipříklad):

$$\{\varphi \to \psi, \chi \to \varphi\} \vdash \neg\chi \to \varphi.$$

Návody

1. Použij třikrát větu o dedukci.

2. A3.

3. Použij větu o dedukci. Uvaž jediný axiom, ve kterém se mluví o negaci.

4. Využij dokazatelnost formule $\neg\neg\varphi \to \varphi$ (za φ dosaď něco jiného). Z axiomu A3 umíš dokázat část, zbytek dokážeš pomocí A2 a dalších jednodušších úprav.

5. Nejprve dokaž první formuli (věta o dedukci), z ní dokaž druhou.

6. Věta o dedukci, uvaž obměnu obou implikací.

7. Použij větu o dedukci. Podívej se na množinu předpokladů.

8. Použij větu o dedukci. Uvaž vzájemné vztahy mezi p_{10}, p_{11}, p_{14}, p_{15}, využij tranzitivitu implikace.

9. Rozlož první konjunkci na konjunkty a druhou konjunkci z nich poskládej.

10. Rozlož první konjunkci na konjunkty a druhou konjunkci z nich poskládej.

11. $\leftarrow$: Věta o dedukci, sestav konjunkci.
$\rightarrow$: Věta o dedukci, rozlož konjunkci.

12. A7.

13. A7.

14. Použij obměnu.

15. $\leftarrow$: Pomůže ti dokazatelnost formule $\vdash \varphi \to (\neg\psi \to \neg(\varphi \to \psi))$.
$\rightarrow$: A7, dokaž si bokem $\vdash \neg\varphi \to (\varphi \to \psi)$.

16. Použij větu o ekvivalenci a $\vdash (\varphi \to \psi) \leftrightarrow (\neg\varphi \vee \psi)$.

Literatura a zdroje

[1] Vítězslav Švejdar: *Logika: neúplnost, složitost a nutnost*, Academia, 2002.
[2] Antonín Sochor: *Klasická matematická logika*, Karolinum, 2001.
[3] Přednášky a cvičení k předmětu *Základy výrokové a predikátové logiky I* od Šárky Stejskalové a Víta Fojtíka.

Náhodné procházky

Hedvika Ranošová

Abstrakt. V tomto příspěvku se seznámíme s náhodnými procházkami a do detailů prozkoumáme některé jejich vlastnosti. Na začátku se seznámíme s pravděpodobností a náhodnými veličinami, intuitivně si představíme podmíněnou pravděpodobnost a střední hodnotu. Představíme si několik klasických příkladů na náhodné procházky.

Motivace

Nejprve se podívejme na několik typických příkladů:

Příklad 1. Kobylka skáče mezi vrcholy trojúhelníku, přičemž každým skokem přeskočí na jeden ze zbylých dvou vrcholů se stejnou pravděpodobností. Jaká je pravděpodobnost, že po n skocích bude kobylka na tom samém vrcholu, na kterém začala?

Příklad 2. Na řece mezi dvěma břehy leží 99 leknínů. Na 30. z nich (počítáno zleva) sedí žába, která každou minutu přeskočí na leknín doprava nebo doleva se stejnou pravděpodobností.

(1) Jaká je pravděpodobnost, že žába skočí na levý břeh řeky dřív, než skočí na pravý břeh?
(2) Jaký je průměrný počet skoků, než žába skočí na některý břeh?

Příklad 3. Po útesu se pohybuje opilec. Začíná jeden krok od srázu a každou minutu udělá krok směrem k útesu s pravděpodobností p nebo opačným směrem s pravděpodobností $1-p$. S jakou pravděpodobností přežije? Určete, ze jak dlouho průměrně spadne, pokud víme, že $p > \frac{1}{2}$.

Všechny tyto úlohy jsou v principu stejné a představují příklady obecnější třídy náhodných procesů, kterým říkáme *náhodné procházky*. Můžeme si třeba představit blechu nebo žabku, která přeskakuje mezi vrcholy grafu podle pravděpodobností, které popisují, kam má z vrcholu skočit. Důležité je, že tato pravidla závisí pouze na tom, kde se blecha nachází právě teď, a nikoliv na jejích dřívějších pozicích.

Definice. *Pravděpodobnostní prostor* je uspořádaná trojice $(\Omega, \mathcal{F}, \mathrm{P})$, kde Ω je množina elementárních jevů daného experimentu, $\mathcal{F}$ je množina jevů (tj. podmnožin Ω) a P: $\mathcal{F} \to \langle 0, 1\rangle$ je funkce splňující:

(1) $\mathrm{P}(A) \geq 0$ pro každé $A \in \mathcal{F}$,
(2) $\mathrm{P}(\Omega) = 1$,
(3) pro posloupnost po dvou disjunktních jevů $\{A_n\}$ je $\mathrm{P}(\bigcup A_n) = \sum \mathrm{P}(A_n)$.

Definice. Je dán pravděpodobnostní prostor $(\Omega, \mathcal{F}, \mathrm{P})$ a $A, B \in \mathcal{F}$ jsou jevy takové, že $\mathrm{P}(B) > 0$. *Podmíněnou pravděpodobnost* jevu A za podmínky, že nastal jev B, definujeme jako

$$\mathrm{P}(A \mid B) = \frac{\mathrm{P}(A \cap B)}{\mathrm{P}(B)}.$$

Cvičení. Hlavními favority dostihů jsou koně Amarant a Baklažán. Před závodem je pravděpodobnost, že vyhraje Amarant, rovna $\frac{1}{2}$, a pravděpodobnost, že vyhraje Baklažán, rovna $\frac{1}{3}$. Bohužel Amarant na začátku závodu upadl a nemůže vyhrát. S jakou pravděpodobností vyhraje Baklažán?

Věta. (o úplné pravděpodobnosti) *Je dán pravděpodobnostní prostor $(\Omega, \mathcal{F}, \mathrm{P})$ a disjunktní jevy $B_1, B_2, \ldots$ takové, že $B_1 \cup B_2 \cup \cdots = \Omega$ a $\mathrm{P}(B_i) > 0$ pro všechna i. Potom pro libovolný jev A platí*

$$\begin{aligned}\mathrm{P}(A) &= \mathrm{P}(A \cap B_1) + \mathrm{P}(A \cap B_2) + \cdots = \\ &= \mathrm{P}(B_1) \cdot \mathrm{P}(A \mid B_1) + \mathrm{P}(B_2) \cdot \mathrm{P}(A \mid B_2) + \cdots\end{aligned}$$

Této větě se také říká *rozkladová věta*, protože jevy B_i tvoří rozklad množiny Ω.

Definice. Mějme pravděpodobnostní prostor $(\Omega, \mathcal{F}, \mathrm{P})$. *Náhodná veličina* X na tomto prostoru je libovolná funkce z Ω do $\mathbb{R}$. Pak jev $\{\omega \in \Omega \mid X(\omega) = x\}$ značíme také $\{X = x\}$ a jeho pravděpodobnost $\mathrm{P}(X = x)$.

Definice. *Oborem hodnot* náhodné veličiny X myslíme množinu[1]

$$\operatorname{Im} X = \{x \in \mathbb{R} \mid \mathrm{P}(X = x) > 0\}.$$

Definice. Mějme náhodnou veličinu[2] X definovanou pro prostor $(\Omega, \mathcal{F}, \mathrm{P})$. Potom *střední hodnotou* X myslíme výraz

$$\mathrm{E}(X) = \sum_{x \in \operatorname{Im} X} x \cdot \mathrm{P}(X = x).$$

[1] Označení Im pochází z anglického *image*.

[2] Tato definice zahrnuje pouze *diskrétní* náhodné veličiny, ostatními (například spojitými) náhodnými veličinami se nebudeme trápit.

Stejně jako počítáme podmíněnou pravděpodobnost, můžeme počítat i *podmíněnou střední hodnotu* za podmínky $B \in \mathcal{F}$, $\mathrm{P}(B) > 0$ jako

$$\mathrm{E}(X \mid B) = \sum_{x \in \operatorname{Im} X} x \cdot \frac{\mathrm{P}(\{X = x\} \cap B)}{P(B)}.$$

Cvičení. Jaká je střední hodnota počtu ok, hodíme-li třemi šestistěnnými kostkami?

Věta. (rozkladová věta pro střední hodnotu) *Je dána náhodná veličina X definovaná pro prostor Ω a disjunktní jevy $B_1, B_2, \ldots$ takové, že $B_1 \cup B_2 \cup \cdots = \Omega$ (tj. tvořící rozklad prostoru Ω) a $\mathrm{P}(B_i) > 0$ pro všechna i. Potom platí*

$$\mathrm{E}(X) = \mathrm{E}(X \mid B_1) \cdot \mathrm{P}(B_1) + \mathrm{E}(X \mid B_2) \cdot \mathrm{P}(B_2) + \cdots$$

Důkaz.

$$\begin{aligned}
\mathrm{E}(X) &= \sum_{x \in \operatorname{Im} X} x \cdot \mathrm{P}(X = x) \\
&= \sum_{x \in \operatorname{Im} X} x \left(\sum_i \mathrm{P}(X = x \mid B_i)\, \mathrm{P}(B_i) \right) \quad \text{[dle věty o úplné pravděpodobnosti]} \\
&= \sum_{x \in \operatorname{Im} X} \sum_i x \cdot \mathrm{P}(X = x \mid B_i)\, \mathrm{P}(B_i) \\
&= \sum_i \mathrm{P}(B_i) \left(\sum_{x \in \operatorname{Im} X} x \cdot \mathrm{P}(X = x \mid B_i) \right) \\
&= \sum_i \mathrm{E}(X \mid B_i)\, \mathrm{P}(B_i).
\end{aligned}$$

□

Příklady

Příklad 4. (gamblerova zkáza) Gambler opakovaně hraje hru, ve které vyhraje 1 korunu s pravděpodobností p a prohraje 1 korunu s pravděpodobností $q = 1 - p$ (nezávisle na ostatních hrách). Kasino opustí, když ztratí všechny peníze nebo bude mít M korun. Jaká je pravděpodobnost, že odejde s prázdnou, pokud má na začátku obnos n korun?

Příklad 5. Jaká je střední hodnota počtu her odehraných před tím, než gambler opustí kasino?

Příklad 6. Kolem kruhového jezera se nachází N měst označených od 0 do $N-1$. Turista, který se právě nachází ve městě 0, se každou hodinu přesune o město po směru nebo proti směru hodinových ručiček se stejnou pravděpodobností.

(1) Jaká je střední hodnota doby, za kterou turista projde všechna města na jezeře?
(2) Pro každé $k = 1, 2, \ldots, N-1$ určete, jaká je pravděpodobnost, že město k je poslední turistou navštívené.

Příklad 7. Blecha skáče po celých číslech, každou vteřinu skočí buď o jedno číslo níže s pravděpodobností p, nebo výše s pravděpodobností $1-p$. Začíná na 0. Jaká je pravděpodobnost, že se po n skocích vrátí na nulu? Jaká je střední hodnota její polohy v n-tém kroku? Jaká je pravděpodobnost, že se do nuly vrátila poprvé až po n skocích?

Příklad 8. (zrcadlový princip) Uvažujme blechu na celých číslech jako v předchozím příkladu.

(1) Kolika způsoby umí blecha za n skoků doskákat z pozice a na pozici b? Co když při tom ještě musí (nebo naopak nesmí) skočit na nulu?
(2) Ukažte, že počet způsobů, kterými blecha přeskáče v n krocích z $a > 0$ do $b > 0$ přes nulu, je roven počtu způsobů, kterými blecha přeskočí z $-a$ do b.

Příklad 9. (volební problém) Ve volbách se dvěma kandidáty Miloš získal m hlasů a Karel získal k hlasů, kde $m > k$. Jaká je pravděpodobnost, že po celou dobu sčítání hlasů Miloš vedl v průběžných výsledcích?

Příklad 10. (maximum náhodné procházky) Hodnota akcie každý den klesne o 1 korunu nebo vyroste o 1 korunu s pravděpodobnostmi $\frac{1}{2}$. Nechť akcie začíná na nule a může nabývat kladných i záporných hodnot. Jaká je pravděpodobnost, že je po n dnech hodnota akcie b a zároveň v průběhu měla hodnotu alespoň r?

Návody

1. Napiš si prvních pár pravděpodobností a zkus z toho vykoumat rekurentní vztah (a pak si ho odůvodnit :-)).

2. Rozepiš si pravděpodobnosti a střední hodnoty rekurentně.

3. Pravděpodobnost, že udělá krok směrem ke srázu (nebo dva kroky směrem ke srázu), je v každém místě stejná. Můžeme proto rekurentně spočítat pravděpodobnost, že spadne, pokud je k kroků od srázu.

4. Zkus si rozmyslet rekurenci pro pravděpodobnosti.

5. Podmíníme výsledkem první hry, buď výhrou, nebo prohrou. Tak jako tak přičteme jednu hru, ale dostaneme se do analogické situace, kde má gambler o korunu více nebo méně. Pak si vyrobíme rekurentní vztah.

6. (1) Jak vypadá množina navštívených měst těsně po tom, co turista navštíví nové město?

6. (2) Před tím, než turista navštíví město k, musí navštívit buď město $k-1$, nebo $k+1$. Co se muselo stát pak?

7. Urči nejprve pravděpodobnost, že se vrátí po lichém počtu kroků. Pravděpodobnost, že se vrátí po sudém počtu kroků, lze nahlédnout z Pascalova trojúhelníku.

8. Pomůže obrázek a symetrie a s $-a$ podle nuly.

9. Co spočítat počet cest z 0 (nic není sečteno) do $m-k$ (konečný rozdíl hlasů) v $m+k$ krocích?

10. Symetrická procházka a zrcadlový princip.

Literatura a zdroje

Části tohoto příspěvku byly převzaty z přednášky *Jáchyma Soleckého* na soustředění v Branné, tímto mu děkuji.

[1] James Martin: *Prelims Probability*, Oxford University Mathematical Institute, 2018.
[2] Danil Koževnikov, Václav Rozhoň: *Pravděpodobnost*, seriál MKS, 2018/19.
[3] Petr Čoupek, Michaela Prokešová: Sbírka úloh z *Náhodných procesů I.*, 2020.
[4] Sven Erick Alm: *Simple random walk*, *http://www2.math.uu.se/~sea/kurser/stokprocmn1/slumpvandring_eng.pdf*.

Izogonály a kamarádi

Martin Raška

Abstrakt. Isogonal conjugates (*kamarádi*) a práce s nimi je oblíbené téma moderní eukleidovské geometrie. V příspěvku jsou popsána některá základní tvrzení, po kterých následuje několik úloh, které se kamarády buď zabývají, nebo je přímo využívají.

Definice. Mějme daný úhel XVY a dvě přímky p, q procházející bodem V. Řekneme, že přímky p a q jsou *izogonální* v úhlu XVY, pokud je jedna obrazem druhé v osové souměrnosti podle osy úhlu XVY.

Definice. Nechť bod P leží v rovině trojúhelníku ABC. Přímky AP, BP a CP zobrazíme podle os úhlů $\sphericalangle CAB$, $\sphericalangle ABC$ a $\sphericalangle BCA$. Pokud se tyto tři přímky protínají v jednom bodě Q, pak tento bod nazveme *isogonal conjugate* bodu P vzhledem k $\triangle ABC$; neformálně mu budeme říkat *kamarád* bodu P vzhledem k $\triangle ABC$).

Tvrzení. (alternativní definice kamaráda) *Kamarád bodu P je středem kružnice opsané trojúhelníku s vrcholy v osových obrazech P přes strany $\triangle ABC$.*

Tvrzení. *Pokud P neleží na kružnici opsané $\triangle ABC$, pak vzhledem k $\triangle ABC$ má P kamaráda.*

Tvrzení. (Six feet theorem) *Nechť P a Q jsou kamarádi vzhledem k $\triangle ABC$. Nechť P_a je projekce bodu P na BC. Analogicky definujme P_b, P_c, Q_a, Q_b a Q_c. Pak P_a, P_b, P_c, Q_a, Q_b a Q_c leží na jedné kružnici, jejíž střed splývá se středem PQ.*

Úmluva. Budeme používat *opsiště*, *vepsiště* a *připsiště* jako zkrácená označení pro střed kružnice opsané, kružnice vepsané a kružnice připsané. Navíc budeme místo „ortocentrum“ používat pojem *kolmiště*.

Úmluva. Pokud nebude řečeno jinak, pak v trojúhelníku ABC bude I, O a H označovat vepsiště, opsiště a kolmiště.

Příklad. Kamarád kamaráda je opět původní bod.

Příklad. Body O a H jsou kamarádi vzhledem k $\triangle ABC$.

Příklad. (Brocardovy body) Uvnitř $\triangle ABC$ leží dvojice bodů P a Q tak, že

$$\sphericalangle PAB = \sphericalangle PBC = \sphericalangle PCA = \varphi \quad \text{a} \quad \sphericalangle QBA = \sphericalangle QCB = \sphericalangle QAC = \phi.$$

Potom tyto dva body jsou kamarádi.

Úloha 1. Najděte všechny body, které jsou svými vlastními kamarády.

OH, oni jsou kamarádi!

Úloha 2. V trojúhelníku ABC platí, že výška a těžnice z vrcholu A rozdělí úhel BAC na třetiny. Určete vnitřní úhly v $\triangle ABC$.

Úloha 3. V $\triangle ABC$ osa úsečky BH protíná strany AB a BC v bodech D a E. Ukažte, že $\sphericalangle BOD = \sphericalangle BOE$. (Crux)

Úloha 4. V $\triangle ABC$ leží body D a E na stranách AB a BC tak, že čtyřúhelník $ADEC$ je tětivový. Kružnice opsaná $\triangle DBE$ protne stranu AC ve dvou bodech X a Y. Nechť M je střed XY. Ukažte, že $BM \perp AC$. (Baltic Way 2010)

Úloha 5. V tětivovém čtyřúhelníku $ABCD$ si označme průsečík úhlopříček jako P. Dále si označme opsiště čtyřúhelníku $ABCD$ jako O a opsiště trojúhelníků APB, BPC, CPD a DPA jako O_1, O_2, O_3 a O_4. Ukažte, že přímky PO, O_1O_3 a O_2O_4 se protínají v jednom bodě. (Čína 1990)

Úloha 6. Kružnice k_1 a k_2 se středy I_1 a I_2 se protínají ve dvou bodech A a B. Nechť je úhel I_1AI_2 tupý. Tečna ke k_1 v bodě A protíná k_2 ještě v bodě C a tečna ke k_2 v bodě A protíná k_1 ještě v bodě D. Označme k_3 kružnici opsanou trojúhelníku BCD. Nechť E je střed toho oblouku CD kružnice k_3, který obsahuje bod B. Přímky AC a AD protínají k_3 po řadě ještě v bodech K a L. Dokažte, že přímky AE a KL jsou navzájem kolmé. (MEMO 2011)

Symediány

Definice. *Symediány* trojúhelníka jsou přímky izogonální s jeho těžnicemi. Symediánu procházející vrcholem A nazveme A-symediánou.

Tvrzení. *A-symediána prochází průsečíkem tečen ke kružnici opsané $\triangle ABC$ v bodech B a C.*

Úloha 7. Symediána z vrcholu A je množina vnitřních bodů X úhlu BAC, jejichž poměr vzdáleností od strany b a c je roven b/c.

Úloha 8. Je dán trojúhelník ABC, v němž $|AC| = 2 \cdot |AB|$. Ke kružnici k jemu opsané sestrojme tečny v bodech A a C a jejich průsečík označme P. Dokažte, že průsečík přímky BP a osy strany BC leží na kružnici k. (Výběrko 2013)

Úloha 9. Nechť ABC je rovnoramenný trojúhelník se základnou BC. Bod P leží uvnitř trojúhelníka tak, že $|\sphericalangle CBP| = |\sphericalangle ACP|$. Označme M střed strany BC. Ukažte, že $|\sphericalangle BPM| + |\sphericalangle CPA| = 180°$. (Poland 2000)

Tvrzení. *Symediány se protínají v jednom bodě, který nazveme Lemoinovým bodem.*

Úloha 10. (kosinová kružnice) Buď ABC trojúhelník s Lemoinovým bodem L. Když bodem L vedeme antirovnoběžky se stranami, vytnou na stranách trojúhelníka (přesněji na přímkách jimi určených) šestici bodů ležících na jedné kružnici. Středem této kružnice je bod L.

Úloha 11. (Lemoinova kružnice) Buď ABC trojúhelník s Lemoinovým bodem L. Když bodem L vedeme rovnoběžky se stranami, vytnou na stranách trojúhelníka (přesněji na přímkách jimi určených) šestici bodů ležících na jedné kružnici. Středem této kružnice je střed úsečky OL.

Další hrátky s kamarády

Úloha 12. Elipsa s ohnisky P a Q se dotýká stran $\triangle ABC$. Ukažte, že P a Q jsou kamarádi.

Úloha 13. V rovině trojúhelníku ABC leží kružnice k se středem X. Tato kružnice protíná stranu AC v bodech B_1 a B_2. Kružnici nad průměrem B_1B_2 nazveme k_b. Analogicky vytvoříme kružnice k_a a k_c. Potenční střed k_a, k_b a k_c označme jako Y. Ukažte, že X a Y jsou kamarádi. (zobecněné IMO 2008)

Úloha 14. Uvnitř trojúhelníku ABC je dán bod P. Nechť A', B', C' jsou paty kolmic z P na příslušné strany. Kružnice opsaná $\triangle A'B'C'$ protíná stranu BC podruhé v bodě A''. Na úsečce $A''B'$ nalezneme bod X takový, že $\sphericalangle XAC = \sphericalangle PAB$. Ukažte, že $\sphericalangle AXB = 90°$. ($i$KS 1 – G3)

Úloha 15. Je dán úhel o velikosti α s hlavním vrcholem A sevřený mezi polopřímkami u_1 a u_2 vycházejícími z A. Uvnitř úhlu u_1u_2 je dán bod B neležící na jeho ose a je dána velikost úhlu β, kde $\alpha < \beta < 180°$. Uvažme všechny možné dvojice bodů X, Y takové, že $X \in u_1$, $Y \in u_2$, A leží mimo úhel XBY a $\sphericalangle XBY = \beta$. Pak každý z bodů A, B má tu vlastnost, že vidí úsečku XY stále pod stejným úhlem. Ukažte, že existuje třetí bod s touto vlastností. (iKS 4 – G6)

Úloha 16. V konvexním čtyřúhelníku $ABCD$ platí, že přímka BD nepůlí ani úhel $\sphericalangle ABC$, ani $\sphericalangle CDA$. Bod P ležící uvnitř $ABCD$ splňuje $\sphericalangle PBC = \sphericalangle DBA$ a $\sphericalangle PDC = \sphericalangle BDA$. Ukažte, že $ABCD$ je tětivový právě tehdy, když $AP = CP$. (IMO 2004)

Tvrzení. *V trojúhelníku ABC označíme body dotyku kružnice vepsané s BC, CA, AB jako D, E, F. Body dotyku kružnic připsaných se stranami BC, CA a AB si označíme jako X, Y, Z. Pak trojice přímek AD, BE a CF se protíná v jednom bodě a stejně tak i trojice přímek AX, BY, CZ.*

Definice. Ve výše použitém značení se průsečík AD, BE a CF nazývá *Gergonnův bod*. Pro průsečík AX, BY, CZ se používá označení *Nagelův bod*.

Úloha 17. Nechť H^- je střed záporné stejnolehlosti, jež převádí kružnici vepsanou $\triangle ABC$ na kružnici tomuto trojúhelníku opsanou. Potom H^- je kamarád Gergonnova bodu. Podobně střed kladné stejnolehlosti H^+ je kamarád Nagelova bodu.

Návody

1. Jsou čtyři.

2. Střed kružnice opsané leží na těžnici.

3. Ukaž $\triangle BOC \sim \triangle BDH$ a ukaž podobnost $\triangle BDO \sim \triangle BHC$.

4. Pokud S je opsiště $\triangle BDE$, pak $BS \perp AC$.

5. Díky izogonálnosti O s H a tětivovosti $ABCD$ je $O_1P \perp CD$ a analogicky pro ostatní, z čehož plyne, že O_1PO_3O a O_2PO_3O jsou rovnoběžníky.

6. Vyúhli, že E je opsiště $\triangle ACD$.

7. Pro každý bod těžnice je tento poměr přesně opačný.

8. Najdi symediánu a doúhli střed oblouku BC.

9. Poznej symediánu.

10. Dokaž si, že L je přesně střed zmíněných antirovnoběžek (jakožto úseček s krajními body na stranách).

11. Pomocí antirovnoběžnosti ukaž, že nám rovnoběžky vytnou trojici „rohových" trojúhelníků podobných s původním ABC.

12. Pokud se elipsa dotýká AC v D, pak $\sphericalangle PDA = \sphericalangle QDC$. Překlop Q podle stran.

13. Dokresli středy k_a, k_b a k_c. Chordála je kolmá na jejich spojnici. Použij alternativní definici kamaráda.

14. Dokresli kamaráda k P a použij six feet theorem. Doúhli.

15. Ten bod je kamarád k B vzhledem k (libovolnému) trojúhelníku XAY. Na dokázání toho, že je to pro všechny ten samý bod, použij definici kamaráda jako střed kružnice opsané obrazům přes strany.

16. Body A a C jsou kamarádi vzhledem k $\triangle BPD$.

17. Překlop si body D, E, F podle os úhlů a sestroj kamaráda Gergonnova bodu. Zkus vyúhlit chtěnou stejnolehlost.

Zdroje

Příspěvek je silně inspirovaný příspěvkem od *Rada Švarce* ze soustředění ve Sklenném 2015, kterému tímto děkuji. Ten jako primární zdroj označil příspěvek od *Michala „Kennyho" Rolínka*, kterému bychom tímto chtěli oba poděkovat.

[1] Michal Rolínek: *Antirovnoběžnost*, Oldřichov, 2012.
[2] András Hraskó: *The Isogonal Conjugate*.
[3] Yufei Zhao: *Lemmas in Euclidean Geometry*.
[4] Tran Quang Hung, Pham Huy Hoang: *Generalization of a Problem with Isogonal Conjugate Points*.
[5] *www.artofproblemsolving.com/community/*.

p-adická čísla

Martin Raška

Abstrakt. Celá čísla jsou ve skutečnosti pěkně zamotaný objekt a mnoho drsných nástrojů algebry a analýzy se na ně přímočaře použít nedá. V běžném životě si je často představujeme jako podmnožinu racionálních, resp. reálných čísel, čímž se otevírají nové možnosti jejich zkoumání. Nejde je ale vnořit do něčeho exotičtějšího, co by nám o nich prozradilo další věci? Jde!

Značení

$\mathbb{N}$	přirozená čísla
$\mathbb{N}_0$	přirozená čísla s 0
$\mathbb{Z}$	celá čísla
$\mathbb{Q}$	racionální čísla
$\mathbb{Z}_n$	zbytky modulo n
$\mathcal{O}_p$	celá p-adická čísla
$\mathbb{Q}_p$	p-adická čísla

Lepší modulení

Když se člověk dívá na přirozená čísla modulo prvočíslo p, často mu to něco prozradí. Hodně informací se tím ale ztrácí. Možným řešením je modulit vyššími a vyššími mocninami $p\ldots$ ale na rozlišení všech přirozených čísel to nikdy stačit nemůže. Pokud bychom však uměli přirozené číslo vymodulit všemi mocninami p najednou, už by to stačilo ...

Definice. Mějme dáno pevné prvočíslo p. Dále mějme nekonečnou posloupnost $(a_i)_{i=1}^{\infty}$, kde $a_i \in \mathbb{Z}_{p^i}$. Tuto posloupnost nazveme *konzistentní*, jestliže pro každé i platí $a_i \equiv a_{i+1} \pmod{p^i}$.

Konzistence tedy znamená, že číslo a_{i+1} dává postupně zbytky $a_1, \ldots, a_{i+1}$ po dělení čísly $p, \ldots, p^{i+1}$.

Definice. Pro prvočíslo p označme $\mathcal{O}_p$ množinu všech konzistentních posloupností vzhledem k p. Na nich definujme sčítání a násobení po složkách, tj.

$$(a_i)_{i=1}^{\infty} + (b_i)_{i=1}^{\infty} = (a_i + b_i)_{i=1}^{\infty}, \qquad (a_i)_{i=1}^{\infty} \cdot (b_i)_{i=1}^{\infty} = (a_i \cdot b_i)_{i=1}^{\infty}.$$

Množinu $\mathcal{O}_p$ s těmito operacemi nazýváme *celými p-adickými čísly.*

Cvičení 1. Rozmyslete si, že součet i součin konzistentních posloupností je opět konzistentní posloupnost, tedy definice $\mathcal{O}_p$ skutečně dává smysl.

Všimněme si, že $\mathcal{O}_p$ v sobě ukrývá celá čísla $\mathbb{Z}$. Každému celému číslu totiž můžeme přiřadit posloupnost jeho zbytků modulo $p, p^2, p^3, \ldots$, což samozřejmě dává konzistentní posloupnost. Sčítání a násobení takových posloupností skutečně odpovídá sčítání a násobení přirozených čísel.

Tvrzení. (obor integrity) *Součin libovolných dvou nenulových prvků $\mathcal{O}_p$ je opět nenulový.*

Důkaz. Mějme dvě taková nenulová $a, b \in \mathcal{O}_p$. To znamená, že pro nějaká $i, j \in \mathbb{N}_0$ platí $a_i \neq 0, b_j \neq 0$. Z konzistence vyplývá, že každý vyšší člen posloupnosti $(a_i)_{i=1}^{\infty}$ je dělitelný p^i, ale již nemůže být dělitelný p^{i+1}. Podobně každý vyšší člen posloupnosti $(b_i)_{i=1}^{\infty}$ je dělitelný p^j, ale nemůže být dělitelný p^{j+1}. Součin členů $a_{i+j+1} \cdot b_{i+j+1}$ proto není dělitelný p^{i+j+1}, tedy číslo $a + b$ má na této pozici nenulový koeficient a proto je nenulové. □

Prvky $\mathcal{O}_p$ si ale můžeme představit i jiným způsobem jako *mocninné řady*, tj. jako „nekonečné“ zápisy čísel v soustavě o základu p. Sčítání a násobení takových řad pak ale nestačí provést „po členech“, je potřeba „převádět přes desítky“ a roznásobovat „nekonečné závorky“ (tj. provádět ho jako sčítání a násobení „pod sebou jako ve škole“).

Tvrzení. (mocninné řady) *Prvky $\mathcal{O}_p$ si lze představit jako mocninné řady $\sum_{i=0}^{\infty} d_i p^i$, pro $d_i \in \mathbb{Z}_p$, které se sčítají a násobí „jako ve škole“.*

Pro $a \in \mathbb{Z} \subset \mathcal{O}_p$ jsou koeficienty d_i od nějakého členu dál všechny nulové a daná řada odpovídá dobře známému zápisu přirozených čísel v soustavě o základu p. Každé celé p-adické číslo má také jednoznačně určený zápis a každý zápis definuje nějaké celé p-adické číslo.

Cvičení 2. Pokud by p nebylo prvočíslo, musel by být pořád součin dvou nenulových prvků $\mathcal{O}_p$ nenulový?

Henselovo lemma

Dostáváme se k tvrzení, které z velké části motivovalo zkoumání p-adických čísel. Rádi bychom totiž uměli řešit polynomiální rovnice modulo mocnina prvočísla p. Pokud se nám povede vyřešit takovou rovnici nad $\mathcal{O}_p$, vyřešíme ji tím vlastně modulo všechny mocniny prvočísla p najednou. Henselovo lemma (a jeho různé varianty) mluví právě o takovém řešení.

Definice. Mějme polynom $f = \sum_{i=0}^{n} a_i x^i$ v proměnné x. Jeho *derivací* rozumíme polynom $f' = \sum_{i=0}^{n} i \cdot a_i x^{i-1}$.

Pro reálné polynomy naše definice odpovídá skutečnému derivování, to nám ale může být jedno. Derivace je pro nás prostě operace, která z jednoho polynomu vyrobí jiný. Pojďme si nyní formulovat základní verzi Henselova lemmatu.

Lemma. (Henselovo) *Ať f je celočíselný polynom, $m \in \mathbb{Z}$. Je-li $f(m) \equiv 0 \pmod{p}$ a zároveň $f'(m) \not\equiv 0 \pmod{p}$, potom existuje jednoznačně určené $a \in \mathcal{O}_p$ splňující $f(a) = 0$ takové, že $a \equiv m \pmod{p}$.*

Důkaz. Důkaz provedeme indukcí, tj. postupně zkonstruujeme členy konzistentní posloupnosti odpovídající číslu a. Budeme chtít, aby pro každé i platilo $f(a_i) \equiv 0 \pmod{p}$, $f'(a_i) \not\equiv 0 \pmod{p}$. Volme $a_1 = m$.

Máme-li už a_i, uvažme čísla $a_i, a_i + p^i, a_i + 2p^i, \ldots, a_i + (p-1)p^i$. Vezměme dvě sousední z nich a označme je $x < y$. Protože $y - x = p^i$, platí kongruence $f(y) - f(x) \equiv f'(a_i) \cdot p^i \pmod{p^{i+1}}$. Díky podmínce $f'(a_i) \not\equiv 0 \pmod{p}$ pak kongruenci $f(z) \equiv 0 \pmod{p^{i+1}}$ splňuje právě jedno z uvažovaných p čísel. Toto číslo označme a_{i+1}. Z jeho tvaru vidíme, že $a_i \equiv a_{i+1} \pmod{p^i}$. Potom také $f'(a_{i+1}) \equiv f'(a_1) \not\equiv 0 \pmod{p}$. Tím je indukční krok dokončen. Zároveň je z postupu jasné, že číslo a_{i+1} bylo určené jednoznačně. □

Cvičení 3. Rozhodněte, zda v $\mathcal{O}_7$ existuje $\sqrt{3}$. *Existencí* $\sqrt{3}$ myslíme, že rovnice $x^2 = 3$ má řešení.

Cvičení 4. Rozhodněte, zda v $\mathcal{O}_7$ existuje $\sqrt{-3}$.

Cvičení 5. Existuje přirozené číslo, jehož třetí mocnina dává po dělení 5^{2018} zbytek 2?

Cvičení 6. Existuje přirozené číslo, jehož sedmá mocnina dává po dělení 30^{2018} zbytek 31?

Cvičení 7. Ať $p \geq 3$ je prvočíslo a přirozené číslo n dává náhodný nenulový zbytek po dělení p. Jaká je šance, že v $\mathcal{O}_p$ existuje $\sqrt{n}$?

Valuace

Mějme přirozené číslo n. Jeho *p-valuací* myslíme exponent v nejvyšší mocnině prvočísla p, která ho dělí. Pro celá p-adická čísla lze tento koncept rozumně dodefinovat, což se vyplatí.

Definice. Prvek $u \in \mathcal{O}_p$ nazveme *jednotkou*, jestliže existuje nějaké $v \in \mathcal{O}_p$ splňující $uv = 1$.

Všimněme si, že součin jednotek je vždy jednotka.

Tvrzení. (popis jednotek) *Prvek $a = (a_i)_{i=1}^{\infty} \in \mathcal{O}_p$ je jednotka právě tehdy, když $a_1 \neq 0$ v $\mathbb{Z}_p$.*

Tvrzení. (rozklad na mocninu a jednotku) *Každý nenulový prvek $a \in \mathcal{O}_p$ lze jednoznačně zapsat ve tvaru $a = p^k u$, pro $k \in \mathbb{N}_0$ a jednotku $u \in O_p$.*

Předchozí tvrzení nám umožňuje definovat p-adickou valuaci, která rozšiřuje běžnou valuaci na celých číslech.

Definice. Pro $0 \neq a \in \mathcal{O}_p$ definujeme *p-adickou valuaci* $v_p(a)$ jako to jednoznačně určené $k \in \mathbb{N}_0$, pro které lze psát $a = p^k u$ pro nějakou jednotku u. Navíc bereme $v_p(0) = \infty$.

Je vidět, že na celých číslech se tato valuace chová jako běžná prvočíselná valuace, tj. $v_p(a)$ odpovídá nejvyššímu exponentu k, pro který ještě p^k dělí a. Hned si všimněme dvou základních vlastností valuace, které platí pro libovolná celá p-adická čísla.

Tvrzení. (vlastnosti valuace) *Pro libovolná $a, b \in \mathcal{O}_p$ platí*

(1) $v_p(a \cdot b) = v_p(a) + v_p(b)$,
(2) $v_p(a + b) \geq \min(v_p(a), v_p(b))$, *přičemž pokud $v_p(a) \neq v_p(b)$, tak už nutně nastává rovnost.*

S pomocí valuace není problém mluvit o kongruenci modulo p^i na celých p-adických číslech. Dvě čísla budou kongruentní, pokud má jejich rozdíl dostatečně velkou valuaci. Na celých číslech se definice opět shoduje s tou dobře známou.

Definice. Pro $a, b \in \mathcal{O}_p$ budeme psát $a \equiv b \pmod{p^i}$ právě když $v_p(a - b) \geq i$.

Zlomky

Racionální čísla vzniknou z celých tak, že si dovolíme dělit nenulovými prvky. Podobně můžeme z celých p-adických čísel $\mathcal{O}_p$ vyrobit „racionální“ p-adická čísla $\mathbb{Q}_p$. Těm se pro jednoduchost říká prostě *p-adická čísla*.

Definice. Pro prvočíslo p definujeme *p-adická čísla* $\mathbb{Q}_p$ jako všechny zlomky tvaru $\frac{a}{b}$ pro $a, b \in \mathcal{O}_p$, kde navíc $b \neq 0$. Dva takové zlomky $\frac{a}{b}$, $\frac{c}{d}$ považujeme ze stejné, právě když $ad = cb$.

S trochou práce není těžké ukázat, že tato definice $\mathbb{Q}_p$ skutečně dává smysl a že pro počítání s p-adickými čísly platí v zásadě stejná „pravidla“ jako pro počítání s racionálními. Důležitou ingrediencí je (nám už dobře známý) fakt, že dva nenulové prvky $a, b \in \mathcal{O}_p$ se opět vynásobí na nenulový prvek. Pojďme si ale nyní právě vzniklé $\mathbb{Q}_p$ prohlédnout podrobněji.

Tvrzení. (mocninné řady v $\mathbb{Q}_p$) *Každé $a \in \mathbb{Q}_p$ lze jednoznačně vyjádřit ve tvaru $p^k u$, pro $k \in \mathbb{Z}$ a jednotku $u \in \mathcal{O}_p$.*

Důkaz. Číslo $\frac{a}{b}$ lze přepsat do tvaru $\frac{p^k u}{p^l v}$ pro $k, l \in \mathbb{N}$, u, v jednotky. Pronásobením čitatele i jmenovatele číslem inverzním k v a označením $w = uv$ dostáváme $\frac{p^k w}{p^l} = p^{k-l} w$. □

Celkem tedy můžeme popsat $\mathbb{Q}_p$ jako všechny mocninné řady od $-\infty$ do ∞ s koeficienty ze $\mathbb{Z}_p$, které mají od nějakého indexu níže všechny koeficienty nulové. Naše p-adická čísla si tedy lze představovat jako „čísla s nekonečným zápisem doleva“. (Na rozdíl od běžných racionálních čísel $\mathbb{Q}$, která umíme zapisovat v soustavě o základu

p, až na znaménko, jako ty řady od $-\infty$ do ∞ s koeficienty ze $\mathbb{Z}_p$, které mají od nějakého indexu *výše* všechny koeficienty nulové.)

Definice. Pro $a, b \in \mathcal{O}_p$ definujme $v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$.

Přitom je zřejmé, že tato definice nezáleží na konkrétním zlomku, kterým dané p-adické číslo reprezentujeme. Na celých (a tedy i na racionálních) číslech se právě definovaná valuace shoduje s tou běžnou. Valuace na $\mathbb{Q}_p$ navíc stále splňuje vlastnosti (1) a (2), které má na $\mathcal{O}_p$. Stejně jako dříve můžeme definovat kongruenci modulo p:

Definice. Pro $a, b \in \mathbb{Q}_p$ budeme psát $a \equiv b \pmod{p^i}$ právě když $v_p(a-b) \geq i$.

Raději si nyní pojďme na vlastní kůži vyzkoušet, jak se p-adická čísla chovají. Mocninnou řadu příslušnou některému p-adickému číslu si přitom skutečně chceme představovat jako jakýsi jeho „zápis v soustavě o základu p“. Ten se často pro přehlednost zapisuje zleva doprava, tedy naopak, než jsme zvyklí – číslu $6 = 2 + 2^2$ bychom tak přiřadili zápis 011, číslu $\frac{13}{2} = 6 + \frac{1}{2}$ zápis 1,011 atd.

Cvičení 8. Rozhodněte, zda rovnice $x^2 = p$ má řešení v $\mathbb{Q}_p$.

Cvičení 9. Je-li $a = d_j p^j + d_{j+1} p^{j+1} + d_{j+2} p^{j+2} + \cdots$ mocninná řada příslušná číslu $a \in \mathbb{Q}_p$, potom číslo $-a$ odpovídá mocninné řadě

$$(p - d_j)p^j + (p - 1 - d_{j+1})p^{j+1} + (p - 1 - d_{j+2})p^{j+2} + \cdots$$

Cvičení 10. Upravte číslo $1 + 2 + 2^2 + 2^3 + \cdots$ v $\mathbb{Q}_2$ na co nejhezčí tvar.

Cvičení 11. Vyjádřete $\frac{1}{5}$ v $\mathbb{Q}_2$ jako mocninnou řadu.

Cvičení 12. Vyjádřete $\frac{1}{6}$ v $\mathbb{Q}_3$ jako mocninnou řadu.

Cvičení 13. Dokažte, že v $\mathbb{Q}_p$ platí vzorec pro součet geometrické řady:

$$\frac{1}{1 - p^k} = 1 + p^k + p^{2k} + \cdots$$

Všimněme si, jak pěkně předchozích pár cvičení vyšlo. To není náhoda – existuje totiž elegantní charakterizace skutečných racionálních čísel v rámci těch p-adických. K obecnému hledání rozvojů p-adických čísel nám velmi pomůže znalost malé Fermatovy věty a vzorec pro součet geometrické řady.

Tvrzení. ($\mathbb{Q}$ uvnitř $\mathbb{Q}_p$) *Mějme číslo $a \in \mathbb{Q}_p$. Potom $a \in \mathbb{Q}$ právě tehdy, když je jemu příslušná mocninná řada od jistého členu periodická.*

Dále umíme rozumně popsat ta racionální čísla s nulovou valuací, jejichž řada je periodická hned od začátku (tj. od prvního nenulového členu, který se nachází na pozici jednotek).

Tvrzení. (čistě periodické řady) *Ať $a \in \mathbb{Q}$ splňuje $v_p(a) = 0$. Potom je řada $a = d_0 + d_1 p + d_2 p^2 + \cdots$ čistě periodická, právě když $-1 \leq a < 0$.*

Nakonec této části si ukážeme jednu úlohu ilustrující použití počítání v $\mathbb{Q}_p$ na běžnou úlohu o dělitelnosti.

Úloha 14. Ať $p > 5$ je prvočíslo. Ukažte, že p^4 dělí čitatel čísla

$$2\sum_{k=1}^{p-1}\frac{1}{k} + p\sum_{k=1}^{p-1}\frac{1}{k^2}.$$

Vzdálenost

Abychom na problémy z teorie čísel uměli efektivně vypustit monstra matematické analýzy, potřebujeme jenom jediné – definovat vzdálenost mezi prvky $\mathbb{Q}_p$. K tomu nám poslouží dříve definovaná valuace.

Definice. *Normou* p-adického čísla $0 \neq a \in \mathbb{Q}_p$ myslíme číslo $|a|_p = p^{-v_p(a)}$. Speciálně klademe $|0|_p = 0$.

Z vlastností valuace hned vyplývají analogické vlastnosti normy.

Tvrzení. (vlastnosti normy)

(1) $|a|_p \geq 0$, *přičemž rovnost nastává pouze pro* $a = 0$,
(2) $|(a \cdot b)|_p = |a|_p \cdot |b|_p$,
(3) $|(a+b)|_p \leq \max(|a|_p, |b|_p)$, *přičemž pro* $|a|_p \neq |b|_p$ *už nutně nastává rovnost.*

Definice. Vzdálenost dvou p-adických čísel $a, b \in \mathbb{Q}_p$ definujeme jako normu jejich rozdílu, tedy jako číslo $|a - b|_p$.

Speciálně si všimněme, že vzdálenost každých dvou různých čísel je kladná. Navíc je díky třetímu bodu předchozího tvrzení pro libovolná $a, b, c \in \mathbb{Q}_p$ splněna trojúhelníková nerovnost $|a - c|_p \leq |a - b|_p + |b - c|_p$.

Tato vzdálenost funguje na první pohled trochu neintuitivně. Dvě čísla jsou k sobě tím blíže, čím větší mocnina prvočísla p dělí jejich rozdíl. Třeba čísla 1000 a 2000 jsou v 2-adické vzdálenosti mnohem blíž, než čísla 1 a 2.

Dovolme si nyní krátkou analýznickou odbočku. Definujme si dva základní pojmy, které lze zavést s použitím pojmu vzdálenosti – limitu posloupnosti a součet řady. Následně se můžeme chvíli kochat, jak hezky se tyto pojmy na p-adických číslech chovají.

Definice. Nekonečná posloupnost čísel $(q_i)_{i=0}^{\infty} \in \mathbb{Q}_p$ *konverguje* k číslu $q \in \mathbb{Q}_p$, jestliže pro libovolně malé $\varepsilon > 0$ už od nějakého indexu dál platí $|q - q_i|_p < \varepsilon$. Číslo q nazýváme *limitou* této posloupnosti.

Definice. Nekonečná řada čísel $\sum_{i=1}^{\infty} r_i$, kde $r_i \in \mathbb{Q}_p$, *konverguje* k číslu $r \in \mathbb{Q}_p$, jestliže k tomuto číslu konverguje nekonečná posloupnost $q_m = \sum_{i=0}^{m} r_i$. Číslo r nazýváme *součtem* této řady.

Vzdálenost na p-adických číslech má následující hezké vlastnosti, které vzdálenost na běžných reálných číslech obecně nemá.

Tvrzení. (konvergence řad) *Řada $\sum_{i=0}^{\infty} r_i$, kde $r_i \in \mathbb{Q}_p$, konverguje k nějakému $r \in \mathbb{Q}_p$ právě tehdy, když posloupnost čísel r_i konverguje k 0.*

Tvrzení. (přerovnávání řad) *Součet konvergentní řady čísel $r_i \in \mathbb{Q}_p$ nezávisí na jejich pořadí.*

Tvrzení. (kompaktnost $\mathcal{O}_p$) *Každá posloupnost $(q_i)_{i=0}^{\infty}$ prvků $\mathcal{O}_p$ obsahuje podposloupnost, která konverguje k nějakému $q \in \mathcal{O}_p$.*

Z předchozího tvrzení mimo jiné vyplývá, že pokud posloupnost prvků $\mathcal{O}_p$ konverguje v rámci $\mathbb{Q}_p$, konverguje k nějakému prvku $\mathcal{O}_p$.

Tvrzení. (návrat mocninných řad) *Pro každé $r \in \mathcal{O}_p$ existují jednoznačně určená čísla $r_i \in \{0, 1, \ldots, p-1\}$ taková, že $\sum_{i=0}^{\infty} r_i p^i$ konverguje k r.*

To už jsme tu jednou měli – hned na začátku jsme si uvědomili, že celá p-adická čísla odpovídají takovýmto řadám. Tenkrát jsme ale vůbec nepřemýšleli o nějaké konvergenci – prostě se nám tak jednotlivá čísla hodilo zapisovat. Oba přístupy naštěstí splývají.

Analogický výsledek platí obecněji pro čísla $r \in \mathbb{Q}_p$. Pro každé takové r existuje jednoznačně určené číslo $m \in \mathbb{Z}$ a čísla $r_i \in \{0, 1, \ldots, p-1\}$ taková, že $r_m \neq 0$ a $\sum_{i=m}^{\infty} r_i p^i$ konverguje k r.

Nyní si ale raději pojďme procvičit, jak se pracuje s vzdálenostmi mezi p-adickými čísly. Tato vzdálenost je totiž na první pohled celkem divná.

Cvičení 15. Každá trojice různých čísel $a, b, c \in \mathbb{Q}_p$ určuje rovnoramenný trojúhelník.

Cvičení 16. Každý kruh v $\mathbb{Q}_p$ má střed v libovolném svém vnitřním bodě.

Cvičení 17. Spočtěte součet řady $1 - 2 + 2^2 - 2^3 + \cdots$ v $\mathbb{Q}_2$.

Dovolme si ještě předvést jeden zdánlivě nesouvisející problém, který několik vysokoškolských triků společně se znalostí p-adických čísel snadno vyřeší.

Definice. Pro $r \in \mathbb{Q}$, $k \in \mathbb{N}$ definujeme *binomický koeficient*

$$\binom{r}{k} = \frac{r \cdot (r-1) \cdots (r-k+1)}{1 \cdot 2 \cdots k}.$$

Úloha 18. Ukažte, že každé prvočíslo, které dělí jmenovatel čísla $\binom{r}{k}$, musí dělit i jmenovatel čísla r.

Úloha 19. Každé prvočíslo, které dělí jmenovatel čísla r, dělí i jmenovatel čísla $\binom{r}{k}$.

Něco na závěr

Teorie p-adických čísel je samozřejmě mnohem hlubší a bohatší, my jsme do ní jen rychle nahlédli. Důležitým výsledkem je například známá Ostrowského věta, která říká, že běžná vzdálenost a p-adické vzdálenosti jsou v podstatě jediné rozumné vzdálenosti na racionálních číslech.

Pojem p-adické vzdálenosti jde jednoznačně rozšiřovat dokonce ještě dál. Krásným důsledkem související teorie je například velmi překvapivá Monskyho věta: „Čtverec nelze rozřezat na lichý počet trojúhelníků se stejným obsahem.“ Pro sudé počty trojúhelníků je konstrukce jednoduchá, pro liché ale neexistuje – a není znám žádný elementárnější důkaz!

Návody

1. Přímočaré.

2. Ne, stačí rozložit p na netriviální součin dvou nesoudělných čísel a z nich induktivně vyrobit dvě nenulové řady s nulovým součinem.

3. Ne, tato rovnice nemá řešení ani modulo 7.

4. Ano, rovnice $x^2 + 3 = 0$ má modulo 7 řešení například $x = 2$, které splňuje předpoklady Henselova lemmatu.

5. Ano, polynom $f = x^3 - 2$ splňuje $f(3) \equiv 0 \pmod 5$ a $f'(3) \equiv 2 \not\equiv 0 \pmod 5$.

6. Ano, použijte Henselovo lemma zvlášť pro $p = 2, 3, 5$ a zakončete Čínskou zbytkovou větou.

7. Přesně $\frac{1}{2}$. Jde jen o to, zda je n kvadratický zbytek modulo p.

8. Nemá. Levá strana má sudou valuaci, zatímco valuace pravé strany je 1.

9. Koeficienty výsledné řady jsou čísla ze $\mathbb{Z}_p$ a obě řady se sečtou na 0.

10. Vyjde -1.

11. Začněte zápisem čísla 5 a postupně hledejte inverz; nakonec vyjde $1+2^2+2^3+2^6+2^7+\cdots$, tj. číslo s periodickým zápisem $1,\overline{1100}$.

12. Násobení mocninou trojky jenom posouvá řády, vyjde $2\cdot 3^{-1}+1+3+3^2+\cdots$, tj. číslo s periodickým zápisem $2,\overline{1}$.

13. Součin závorek $(1+(p-1)p^k+(p-1)p^{2k}+\cdots)\cdot(1+p^k+p^{2k}+\cdots)$ je 1.

14. Upravujte, využijte p-adické identity $\frac{1}{k(p-k)} = -\frac{1}{k^2}\left(1+\frac{p}{k}+\frac{p}{k^2}+\cdots\right)$.

15. Zkoumejte čísla $(a-b)$, $(b-c)$, $(c-a)$. Mohou se tři čísla s různými normami sečíst na 0?

16. K číslu $a \in \mathbb{Q}_p$ jsou blízko ta čísla, jejichž mocninné řady mají od jisté pozice ty samé koeficienty.

17. Součty geometrických řad, vyjde $\frac{1}{3}$.

18. Chceme ukázat, že $|r|_p \le 1$ implikuje $\left|\binom{r}{k}\right|_p \le 1$. K číslu r jde dokonvergovat čísly z $\mathcal{O}_p$, funkce $\binom{x}{k}$ je spojitá funkce $\mathbb{Q}_p \to \mathbb{Q}_p$.

19. Dokazujte, že $|r|_p > 1$ implikuje $\left|\binom{r}{k}\right|_p > 1$.

Zdroje

Příspěvek je podmnožinou příspěvku *Kuby Löwita* z Pasek 2018, kterému bych tímto chtěl moc poděkovat.

[1] Titu Andreescu, Gabriel Dospinescu: *Problems from the Book.*
[2] Titu Andreescu, Gabriel Dospinescu: *Straight from the Book.*
[3] Keith Conrad: *Hensel's Lemma.*
[4] Keith Conrad: *The p-adic expansion of Rational Numbers.*
[5] Keith Conrad: *Binomial Coefficients and p-adic Limits.*
[6] Jakub Opršal: *Celá čísla p-naruby*, Blansko-Obůrka, 2011.
[7] Radovan Švarc: *Monskyho věta*, Hojsova Stráž, 2016.

Konečné automaty

Michal Töpfer

Abstrakt. Jedním z hlavních objektů, které zkoumá teoretická informatika, jsou Turingovy stroje. Protože o Turingových strojích je ale za jednu přednášku obtížné dokázat cokoli zajímavého, podíváme se na jejich (o několik stupňů) slabší brášky – konečné automaty.

V teoretické informatice často řešíme, jak složité je pro různé množiny řetězců rozhodnout, který řetězec do nich patří a který ne. Abychom ale mohli mluvit o řetězcích, musíme nejprve nadefinovat terminologii.

Definice. Konečné množině znaků budeme říkat *abeceda* a budeme ji značit Σ. Abeceda může být například $\{a, b, c, \ldots, z\}$, ale taky třeba množina obsahující #, @, § a !. My však budeme nejčastěji používat binární abecedu $\{0, 1\}$, či dokonce unární abecedu obsahující pouze nulu nebo pouze jedničku. Prvkům abecedy budeme říkat *znaky abecedy*, nebo prostě *znaky*. *Řetězec* (nebo taky *slovo*) pak bude konečná (klidně prázdná) posloupnost znaků. *Délkou řetězce* w budeme rozumět počet jeho znaků a budeme ji značit $|w|$. Řetězec délky 0 (prázdné slovo) budeme značit ε. Máme-li řetězce u a v, budeme uv nebo $u \cdot v$ značit jejich zřetězení, tedy řetězec w takový, že $|w| = |u| + |v|$ a ve w jsou nejprve všechny znaky u v tom samém pořadí jako v u a potom obdobně všechny znaky v. Podobně budeme u^k pro $k \in \mathbb{N}_0$ značit řetězec u k-krát zřetězený sám za sebe (tedy například zápisem $1(10)^3$ budeme rozumět řetězec 1101010). Pro řetězec u budeme u^R značit ten samý řetězec pozpátku. Máme-li řetězec w, tak pro $k \in \mathbb{N}$, $k \leq |w|$ budeme $w[k]$ značit k-tý znak řetězce w.

Dále budeme potřebovat terminologii a značení mluvící o množinách řetězců. Dovolíme si jistou formální nepřesnost a budeme tam, kde to dává smysl, volně zaměňovat řetězec s jednoprvkovou množinou, která obsahuje právě tento řetězec.[1]

Dovolíme si podobně, jako zřetězujeme řetězce, zřetězovat i množiny. Tedy například $\{0, 1\} \cdot \{2, 3\} = \{02, 03, 12, 13\}$. Dále pokud M je množina řetězců, M^* budeme značit libovolný počet opakování něčeho z M, tedy $M^* = \{\varepsilon\} \cup M \cup M^2 \cup M^3 \cup \cdots$ Například Σ^* je tedy množina všech možných konečných řetězců nad abecedou Σ. $\{01, 02\}^*$ obsahuje například ε, 01, 01020102, ale ne 010.

[1] Také budeme zaměňovat znak a řetězec délky jedna obsahující právě tento znak.

Definice. *Jazykem* nad abecedou Σ budeme značit množinu $L \subseteq \Sigma^*$. Jejím prvkům budeme říkat *slova* jazyka L.

Příkladem jazyka nad abecedou $\{0, 1\}$ může být například množina všech řetězců reprezentujících prvočíslo, množina všech řetězců, které reprezentují ve dvojkové soustavě číslo menší než 42. Nebo množina všech řetězců, které začínají jedničkou. Nyní již konečně máme vše, co potřebujeme, abychom nadefinovali konečný automat.

Definice. *Konečný automat* je pětice $(Q, \Sigma, \delta, q_0, F)$, kde:

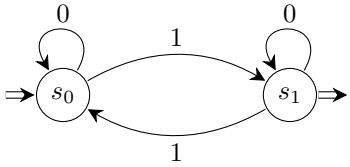
- Q je konečná množina stavů,
- Σ je konečná abeceda,
- $\delta : Q \times \Sigma \to Q$ je přechodová funkce,
- $q_0 \in Q$ je počáteční stav,
- $F \subseteq Q$ je množina přijímajících stavů.

Výpočet konečného automatu nad řetězcem w probíhá následovně: Automat začne v počátečním stavu q_0. Poté přečte první znak řetězce $w[1]$ a přejde do stavu $q_1 = \delta(q_0, w[1])$ (ne nutně různého od q_0). Dále přečte znak $w[2]$ a přejde do stavu $q_2 = \delta(q_1, w[2])$. Tak pokračuje, dokud nepřečte poslední znak w a nepřejde do stavu $s_{|w|}$. Pak řekneme, že automat řetězec w přijal, právě když výpočet skončil v přijímajícím stavu, tedy pokud $s_{|w|} \in F$.

Definice. *Jazyk $L(A)$ přijímaný automatem A* je množina všech slov z Σ^*, které automat přijme.

Průběh výpočtu si tedy můžeme představit tak, že automat čte řetězec znak po znaku a do svého stavu si ukládá nějakou informaci o tom, co už přečetl. Ve většině případů si však například nemůže uložit celou část řetězce, kterou už přečetl, protože jeho stav může nabývat jen konečně mnoha různých hodnot, kdežto řetězce můžou být obecně libovolně dlouhé.

Protože tento zápis automatu je (obzvlášť u větších automatů) velmi nepřehledný, často se používá ilustrace automatu pomocí orientovaného grafu, kde vrcholy odpovídají stavům automatu a orientované hrany označené znaky abecedy přechodové funkci. Mějme například automat nad abecedou $\{0, 1\}$, který má množinu stavů $\{s_0, s_1\}$, kde s_0 je počáteční stav a s_1 jediný přijímající stav. Přechodová funkce říká, že při přečtení nuly zůstaneme v témže stavu a při přečtení jedničky přejde do druhého z možných stavů. Tento automat by též šel popsat následujícím obrázkem:



Úloha 1. Jaký jazyk automat na obrázku vlastně přijímá?

Úloha 2. Nakreslete konečný automat nad abecedou $\{0,1\}$, který přijímá právě slova začínající 01. Co slova končící 01?

Úloha 3. Nakreslete konečný automat nad abecedou $\{0,1\}$, který přijímá právě ta slova, která reprezentují binární zápis sudého čísla. Co čísla dělitelná trojkou?

Úloha 4. Nakreslete konečný automat nad abecedou $\{0,1\}$, který přijímá právě slova se sudým počtem nul. Pak nakreslete automat, který přijímá ta, v nichž je počet jedniček dělitelný třemi. Nakonec najděte automaty, které přijímají slova splňující alespoň jednu z těchto vlastností, respektive obě tyto vlastnosti.

Definice. O jazyku řekneme, že je *regulární*, pokud existuje konečný automat, který přijímá právě tento jazyk.

Úloha 5. Dokažte, že pro libovolné dva regulární jazyky L_1, L_2 nad abecedou Σ jsou jazyky $L_1 \cup L_2$, $L_1 \cap L_2$ a $\Sigma^* \setminus L_1$ také regulární.

Úloha 6. Rozmyslete si, že libovolný konečný jazyk je regulární.

Nedeterminismus

Doteď jsme měli pouze konečné automaty, které vždy věděly, co mají dělat. Co kdybychom jim ale dali na výběr?

Definice. *Nedeterministický konečný automat* je pětice $(Q, \Sigma, \delta, S, F)$, kde:

- Q je konečná množina stavů,
- Σ je konečná abeceda,
- $\delta : Q \times (\Sigma \cup \{\lambda\}) \to \mathcal{P}(Q)$ je přechodová funkce ($\lambda \notin \Sigma$ značí přechod bez čtení vstupu),
- $S \subseteq Q$ je množina startovních stavů,
- $F \subseteq Q$ je množina přijímajících stavů.

Výpočet nedeterministického konečného automatu nad řetězcem w probíhá následovně: Automat začne v nějakém počátečním stavu $q_0 \in S$. Poté přečte první znak řetězce $w[1]$ a přejde do nějakého stavu $q_1 \in \delta(q_0, w[1])$ (ne nutně různého od q_0). Případně může také nečíst znak a přejít do nějakého stavu z množiny $\delta(q_0, \lambda)$ (a v příštím kroku pokračovat ve čtení tam, kde předtím skončil; tomu říkáme, že automat využil λ-přechod). Takto pokračuje ve výpočtu, dokud nepřečte poslední znak a případně ještě nevyužije nějaké λ přechody. Řekneme, že automat řetězec w přijímá, pokud existuje výběr počátečního stavu a stavů v průběhu výpočtu takový, že automat skončí v nějakém stavu z F.

Pokud během výpočtu nastane situace, že je automat ve stavu q, čte znak z a $\delta(q, z) = \emptyset$, výpočet se považuje za nepřijímající.

Zajímavé je, že přidání nedeterminismu nijak nezvyšuje sílu konečných automatů – pořád pomocí nich umíme přijímat jen regulární jazyky.

Věta. *Pro každý nedeterministický konečný automat existuje deterministický konečný automat, který přijímá ten samý jazyk.*

Myšlenka důkazu. Nejprve si rozmyslíme, že λ přechody umíme odstranit poměrně jednoduše. Potom sestrojíme konečný automat, jehož stavy jsou všechny podmnožiny množiny stavů původního nedeterministického automatu. Rozmyslete si, jak nadefinovat přechodovou funkci. □

Příklad. Nakreslete nedeterministický konečný automat nad abecedou $\{0,1\}$, který přijímá právě slova končící 01, a převeďte ho na deterministický.

Pumping lemma

Zatím jsme pouze konstruovali automaty, ale chyběly nám prostředky, jak dokázat, že nějaký jazyk regulární není. K tomu nám poslouží pumping lemma.

Věta. (pumping lemma) *Pro každý regulární jazyk L existují konstanty k a ℓ, takové, že pro každé slovo $u \in L$, kde $|u| \geq \ell$, existují řetězce w, x a y, takové, že:*

- $u = w \cdot x \cdot y$,
- $|w \cdot x| \leq k$,
- $|x| \geq 1$,
- *pro každé $n \in \mathbb{N}_0$ je slovo $w \cdot x^n \cdot y$ také v jazyce L.*

Myšlenka důkazu. Máme-li regulární jazyk, pak existuje konečný automat, který ho přijímá. Tento automat má $|Q|$ stavů a je nad $|\Sigma|$-prvkovou abecedou, takže pokud má slovo alespoň $|Q| \cdot |\Sigma| + 1$ znaků, musí se z Dirichletova principu nějaká kombinace čteného znaku a stavu stroje zopakovat (dokonce již mezi prvními $|Q| \cdot |\Sigma| + 1$ znaky). Část slova mezi těmito opakováními je ale možné vynechat či naopak libovolněkrát zopakovat, protože pokud stroj čte týž znak a je v témže stavu, bude se vždy chovat stejně bez ohledu na to, co již přečetl. □

Příklad. Rozhodněte, zda jazyk $L = \{0^j \mid j \text{ je mocnina dvojky}\}$ je regulární.

Řešení. Jazyk regulární není. Pro spor připusťme, že by regulární byl. Pak existují k a ℓ s vlastnostmi ze znění pumping lemmatu. Najdeme n takové, že $2^{n-1} > \max(k, \ell)$. Pak slovo 0^{2^n} lze rozdělit na slova w, x a y podle pumping lemmatu. Protože ale $k < 2^{n-1}$, tak $1 \leq |x| < 2^{n-1}$, tedy $w \cdot y = w \cdot x^0 \cdot y$ je v L, ale současně $2^{n-1} < |w \cdot y| < 2^n$, což je ve sporu s definicí L. Jazyk L tedy není regulární.

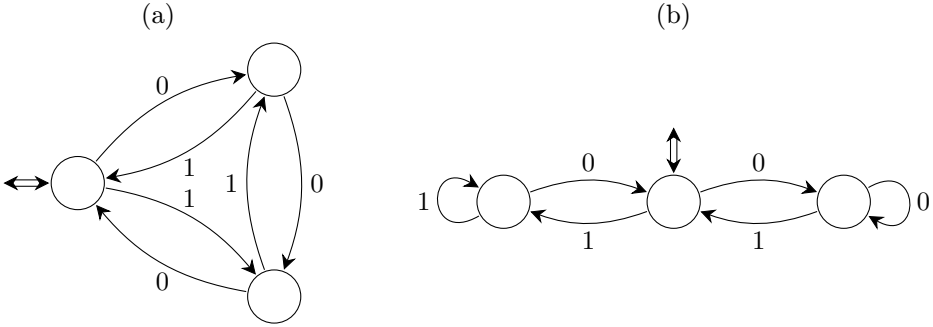
Úloha 7. O následujících jazycích rozhodněte, zda jsou regulární: (Prostředky, které k tomu máte, jsou pumping lemma a uzavřenost regulárních jazyků na doplněk, průnik a sjednocení.)

(1) $L_1 = \{0^p \mid p \text{ je prvočíslo}\}$,
(2) $L_2 = \{0^n \cdot 1^m \mid n, m \in \mathbb{N}\}$,
(3) $L_3 = \{0^n \cdot 1^n \mid n \in \mathbb{N}\}$,
(4) $L_4 = \{0^n \cdot 1^m \mid n, m \in \mathbb{N}, n > m\}$,
(5) $L_5 = \{0^n \cdot 1^m \mid n, m \in \mathbb{N}, n \neq m\}$,
(6) $L_6 = \{w \cdot w^R \mid w \in \{0,1\}^*\}$.

Úloha 8. Nechť K_1 a K_2 jsou regulární jazyky. Pak rozhodněte, zda jsou následující jazyky regulární (pro každou volbu K_1 a K_2):

(1) $L_1 = \{w \mid w^r \in K_1\}$,
(2) $L_2 = \{w^* \mid w \in K_1\}$,
(3) $L_3 = K_1^*$ – tento příklad se od předchozího liší tím, že v předchozím případě se požaduje, aby w bylo pořád stejné, zde se za sebe můžou řetězit různá slova K_1,
(4) $L_4 = \{w \cdot v \mid w \in K_1, v \in K_2\}$,
(5) $L_5 = \{w \cdot v \mid v \cdot w \in K_1\}$.

Cvičení 9. Rozhodněte, jaké jazyky přijímají následující automaty:



Návody

5. Jazyky L_1 a L_2 jsou regulární, tedy máte konečné automaty, které je přijímají. Zkuste z nich tedy vyrobit automat, který by přijímal jazyky $L_1 \cup L_2$ a $L_1 \cap L_2$. Bude se vám hodit rozmyslet si, jak vypadá „kartézský součin“ dvou automatů.

7. Jazyk L_2 je jediný regulární. V části (5) si uvědomte, že doplněk L_5 je jazyk všech řetězců, které vypadají jinak, než nějaké nuly a pak jiný počet jedniček. Kdyby ale L_5 byl regulární, je regulární i jeho doplněk a následně průnik jeho doplňku s L_2, což je přesně L_3. V části (6) si můžeme vzít například $w = 0^n \cdot 1$ pro nějaké dostatečně vysoké n.

8. Jazyk L_2 není regulární, myšlenka důkazu je podobná L_6 z Úlohy 7. Ostatní regulární jsou, popište konstrukci nedeterministického automatu.

9. (a) Podívejte se, kolik jedniček a kolik nul mají přijímaná slova.
(b) Co se stane, když přijdou dva stejné znaky po sobě.

Literatura a zdroje

Příspěvek je upravenou verzí přednášky od *Vikiho Němečka* z Branné na jaře 2019, kterému tímto děkuji.

[1] Viki Němeček, *Konečné automaty*, Branná, 2019.

Kreslení grafů na plochy

Michal Töpfer

Abstrakt. V první části příspěvku si vysvětlíme základní pojmy týkající se ploch. Dále si ukážeme a procvičíme možné způsoby jejich zobrazování do roviny, abychom na ně následně v druhé části příspěvku mohli kreslit grafy, a rozmyslíme si, co takové grafy musí splňovat.

Příklad. (motivační) Představte si, že na celé Zemi (předpokládejte, že má tvar dokonalé koule) se vyskytují právě tři domy a tři studny. Postavte cesty mezi každým domem a studnou tak, aby se vzájemně neprotínaly.

Úvod

Jistě jste se už v životě mnohokrát setkali s grafem, například odpovídajícím silniční síti. Pokud jste ovšem potřebovali nakreslit složitější graf, jistě jste si všimli, že ne vždy ho lze nakreslit tak, aby se jeho hrany nikde nekřížily – z tohoto důvodu je třeba stavět na silnicích různé tunely a mosty. Ukážeme si, že kdyby Země nebyla kulatá, ale například měla tvar toru, tak bychom na ní mohli postavit některé silniční sítě, které na kouli bez mostů postavit nelze.

Pro úplnost nejprve definujme, čím je graf ve smyslu teorie grafů:

Definice. *Graf* $G = (V, E)$ je uspořádaná dvojice množin vrcholů $V = \{1, 2, \ldots, n\}$ a hran $E \subseteq \binom{V}{2}$. Řekneme, že graf na $|V| = n$ vrcholech je *úplný* (značený K_n), pokud $E = \binom{V}{2}$.

Ukážeme si, že grafy na rovinu nenakreslitelné bez křížení hran lze mnohdy nakreslit na jiné plochy, například torus či Kleinovu láhev.

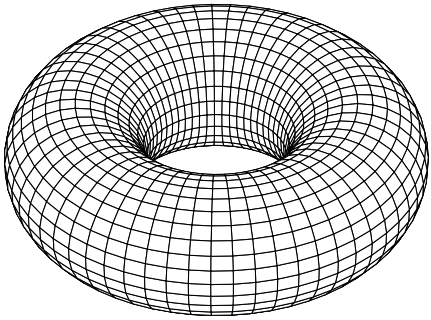
Co to vlastně je ta plocha?

Jelikož plochy mohou vypadat velmi různorodě (například povrch hrníčku, ale třeba i tohoto sborníčku), jejich matematický popis je poměrně složitý. Pro zajímavost, jedna z možných definic je následující:

Definice. *Plocha* Γ je souvislá kompaktní množina $X \subseteq \mathbb{R}^n$ taková, že pro každé $y \in X$ existuje otevřené okolí y takové, že jeho průnik s X je homeomorfní otevřenému kruhu v $\mathbb{R}^2$.

Definice ve skutečnosti pouze říká, že *plocha* vypadá „rozumně“, tj. je konečně velká, mezi každými jejími dvěma body vede cesta a neobsahuje žádné „díry“ či okraj. Pojem *homeomorfní* ještě později použijeme, v podstatě platí, že A je *homeomorfní* s B právě tehdy, když lze A zdeformovat tak, že vznikne B (a také B lze zdeformovat na A).

Mezi plochy řadíme například sféru či torus (na obrázku), ovšem rovina či uzavřený čtverec plochami nejsou (rovina není konečná, tudíž ani kompaktní, naopak bod na okraji čtverce nemá okolí homeomorfní otevřenému kruhu). Přesto jsme za pomoci malého triku schopni všechny plochy nakreslit na papír.



Zobrazování ploch do roviny

Nejprve si ukážeme, že platí následující tvrzení:

Tvrzení. *Každý graf, který lze nakreslit na sféru, lze nakreslit i do roviny.*

Důkaz. Stačí, když si zvolíme nějaký bod na sféře, který není vrcholem ani není na hraně grafu, sféru „položíme“ na rovinu s tímto bodem x_0 nahoře a poté každý bod $x \neq x_0$ sféry zobrazíme na takový bod roviny, kde ji protne přímka x_0x. □

Ukážeme si (neformálně) dvě operace, jak kreslit různé plochy na papír, a také pro vzniklé plochy definujeme jejich tzv. Eulerovu charakteristiku χ.

Definice. *Přidání ucha* provedeme tak, že z papíru „vyřízneme“ dva kruhy a body na jejich okrajích v opačných orientacích ztotožníme. *Přidání křižítka* provedeme tak, že „vyřízneme“ pouze jeden kruh a ztotožníme protější body na jeho okraji.

Definice. *Eulerova charakteristika* χ plochy Γ vzniklé ze sféry přidáním u uší a k křižítek je

$$\chi = 2 - 2u - k.$$

Jako cvičení si můžete rozmyslet, že po přidání ucha či křižítka nám zůstane plocha. Ovšem platí dokonce následující věta:

Věta. *Každou plochu lze vytvořit ze sféry přidáním nějakého počtu u uší a k křižítek. Pokud $k = 0$, nazývá se tato plocha orientovatelná a značí se Σ_u. Pokud $k > 0$, nazývá se tato plocha neorientovatelná, je homeomorfní ploše vzniklé ze sféry přidáním právě $n = 2u + k$ křižítek a značí se Π_n.*

Nejznámější plochy jsou *sféra* (Σ_0), *torus* (Σ_1), *projektivní rovina* (Π_1) a *Kleinova láhev* (Π_2).

Úloha. Jakou charakteristiku mají zmíněné plochy?

Poznámka. Každou plochu je možné reprezentovat pomocí mnohoúhelníku s orientovanými a spárovanými hranami.

A kde vlastně jsou ty grafy?

Nyní máme připraveno vše, abychom mohli začít kreslit grafy na naše vytvořené plochy. Pro úplnost začněme definicí nakreslení grafu:

Definice. *Nakreslení grafu* $G = (V, E)$ na plochu Γ je takové zobrazení, kde všechny vrcholy z G jsou zobrazeny na různé body Γ a všechny hrany z G na neprotínající se křivky spojující obrazy vrcholů.

Pokud jste zkoušeli vyřešit motivační příklad výše, nejspíše jste zjistili, že úloha bez použití „mostů“ vyřešit nelze. Nicméně nemusíme zoufat, neboť platí:

Tvrzení. *Každý graf lze nakreslit na sféru s přidáním dostatečného počtu uší.*

Důkaz. Důkaz je velmi snadný, stačí zadaný graf „skoro-nakreslit“ (povolíme protínání jeho hran) na sféru a poté na každé místo, kde se nějaké dvě hrany kříží, přidáme ucho jako „most“, přes který jednu z nich převedeme. Takto sice můžeme přidat velké množství uší, ale na vzniklou plochu již zadaný graf nakreslit lze. □

Cvičení. Ukažte, že každý graf lze nakreslit na sféru s přidáním dostatečného počtu křižítek.

Problémem předchozího tvrzení je fakt, že uší (či křižítek) je někdy třeba přidat mnoho. Pokud ovšem dostaneme zadanou plochu, tak si ukážeme, že grafy nakreslitelné na tuto plochu jsou poměrně omezené. Konkrétně si postupně dokážeme následující „magické“ tvrzení:

Tvrzení. (magické) *V každém grafu nakresleném na plochu charakteristiky χ různou od sféry existuje vrchol stupně nejvýše*

$$\left\lfloor \frac{5 + \sqrt{49 - 24\chi}}{2} \right\rfloor .$$

Byť toto tvrzení může vypadat velmi pokročile, uvidíme, že s využitím znalosti *zobecněné Eulerovy formule* není její důkaz příliš obtížný.

Věta. (Eulerova formule) *Pro každý rovinný graf obsahující s stěn platí*

$$|V| - |E| + s \geq 2,$$

přičemž pokud je graf souvislý, platí rovnost.

Můžete si zkusit tuto větu dokázat[1]. Pro nás je ovšem důležitá její zobecněná verze:

Věta. (zobecněná Eulerova formule) *Pro každý graf nakreslený na plochu s charakteristikou χ obsahující s stěn platí nerovnost*

$$|V| - |E| + s \geq \chi.$$

Byť to tak na první pohled nevypadá, s touto znalostí už lze „magické“ tvrzení pomocí několika lehčích úvah dokázat. Nejprve si uvědomme, že každá stěna má na svém obvodu alespoň tři hrany a také každá hrana sousedí s nejvýše dvěma stěnami. Tudíž

$$s \leq \frac{2|E|}{3}.$$

Když tuto nerovnost dosadíme do zobecněné Eulerovy formule, dostaneme

$$\begin{aligned} |V| - \frac{|E|}{3} &\geq \chi, \\ \frac{6|V|}{|V|} - \frac{2|E|}{|V|} &\geq \frac{6\chi}{|V|}, \\ \frac{2|E|}{|V|} &\leq 6 - \frac{6\chi}{|V|}. \end{aligned}$$

Jelikož $\frac{2|E|}{|V|}$ je průměrný stupeň vrcholu grafu, víme, že minimální stupeň grafu musí být nejvýš takový, tedy že existuje vrchol stupně nejvýše $6 - \frac{6\chi}{|V|}$. Tudíž pro každý graf na ploše s kladnou charakteristikou (tj. sféra a projektivní rovina) existuje vrchol stupně nejvýše pět, takže projektivní rovina splňuje „magické“ tvrzení.

Jiný horní odhad na minimální stupeň grafu s n vrcholy je $n - 1$, neboť zřejmě všechny jeho vrcholy mají stupeň nejvýše $n - 1$.

Nyní si stačí všimnout, že pro $\chi \leq 0$ je funkce $f(x) = 6 - \frac{6\chi}{x}$ pro $x > 0$ nerostoucí, naopak $g(x) = x - 1$ je zjevně rostoucí. Tudíž pokud nalezneme průsečík těchto funkcí, zjistíme maximální možný minimální stupeň grafu, který lze na odpovídající plochu nakreslit:

$$\begin{aligned} 6 - \frac{6\chi}{x} &= x - 1, \\ x^2 - 7x + 6\chi &= 0, \\ \left(x - \frac{7 - \sqrt{49 - 24\chi}}{2}\right)\left(x - \frac{7 + \sqrt{49 - 24\chi}}{2}\right) &= 0. \end{aligned}$$

[1] Nápověda: Uvědomte si, že věta platí pro stromy, a pak použijte indukci podle hran.

Jelikož je $\chi \leq 0$, tak $\sqrt{49-24\chi} \geq 7$, tudíž první závorka součinu nesplňuje $x > 0$. Ovšem z druhé závorky přímo plyne, že pro minimální stupeň d libovolného grafu platí

$$d \leq \left\lfloor \frac{5+\sqrt{49-24\chi}}{2} \right\rfloor,$$

což je ovšem přesně naše „magické“ tvrzení!

Cvičení.

(1) Zkuste nakreslit co největší úplný graf na torus.

(2) Zkuste nakreslit co největší úplný graf na projektivní rovinu.

(3) Zkuste nakreslit co největší úplný graf na Kleinovu láhev.

Ve skutečnosti lze na každou plochu nakreslit úplný graf s právě $\left\lfloor \frac{5+\sqrt{49-24\chi}}{2} \right\rfloor + 1$ vrcholy, ovšem s výjimkou Kleinovy láhve. Předchozí cvičení bylo tedy trochu chyták, neboť byť mají torus i Kleinova láhev stejnou charakteristiku, na torus lze nakreslit K_7, ovšem na Kleinovu láhev bohužel ne.

Literatura a zdroje

Příspěvek je upravenou verzí příspěvku od *Tomáše Novotného*, který ho přednášel v Hojsově Stráži na jaře 2016 a kterému tímto děkuji.

[1] Tomáš Novotný, *Kreslení grafů na plochy*, Hojsova Stráž, 2016.
[2] Zápisky z předmětu *Kombinatorika a grafy II* na MFF UK.
[3] Peter „πtr“ Korcsok, *Grafity v metre*, Mentaurov, 2013.

Apolloniova kružnice

Adéla Karolína Žáčková

Abstrakt. Příspěvek se zaměřuje na zajímavou geometrickou množinu bodů, Apolloniovu kružnici. Podíváme se na její využití v konstrukčních a důkazových úlohách a na další pěkné aplikace.

Ještě než se pustíme do samotné Apolloniovy kružnice, ukažme si pár vlastností os úhlů, které se nám budou dále velice hodit.

Tvrzení. (o ose vnitřního úhlu) *V trojúhelníku ABC označme průsečík osy vnitřního úhlu BAC a strany BC jako D. Pak platí*

$$\frac{|BD|}{|DC|} = \frac{|AB|}{|AC|}.$$

Tvrzení. (o ose vnějšího úhlu) *V trojúhelníku ABC, kde $|AB| \neq |AC|$, označme průsečík osy vnějšího úhlu BAC a přímky BC jako E. Pak platí*

$$\frac{|BE|}{|CE|} = \frac{|AB|}{|AC|}.$$

Příklad 1. V kartézské soustavě souřadnic jsou dány body $A = [5, 0]$ a $B = [20, 0]$. Najděte na přímce AB dva body, které jsou dvakrát blíže k A než k B. Zkuste najít další body mimo přímku AB. Dokázali byste je nějak popsat všechny?

A konečně k Apolloniově kružnici

Tvrzení. (o Apolloniově kružnice) *V rovině jsou dány body A, B. Množina těch bodů X, pro které je poměr $|XA| : |XB|$ roven dané kladné konstantě $\lambda \neq 1$, je kružnice se středem na přímce AB.*

Příklad 2. Na přímce jsou dány po řadě body A, B, C. Určete množinu bodů X, ze kterých jsou úsečky AB a BC vidět pod stejnými úhly.

Příklad 3. V rovině jsou dány čtyři různé body A, B, C, D neležící na stejné přímce. Sestrojte všechny body X, pro něž platí $\triangle ABX \sim \triangle CDX$.

Příklad 4. Na přímce jsou dány po řadě body A, B, C, D, které jsou vzájemně různé. Sestrojte všechny body X ležící v rovině, pro něž platí

$$|\sphericalangle AXB| = |\sphericalangle BXC| = |\sphericalangle CXD|.$$

Příklad 5. Je dána úsečka BC. Sestrojte všechny trojúhelníky ABC takové, že velikosti výšek v_b, v_c z bodů B, C jsou v poměru $1 : 2$.

Příklad 6. V trojúhelníku ABC označme S_a, S_b, S_c postupně středy jeho stran BC, CA, AB. Dokažte, že pro libovolný bod X různý od bodů S_a, S_b, S_c platí

$$\min\left\{\frac{|XA|}{|XS_a|}, \frac{|XB|}{|XS_b|}, \frac{|XC|}{|XS_c|}\right\} \leq 2.$$

(MO 70-A-I-5)

Příklad 7. Je dán trojúhelník ABC a dva různé body X, Y takové, že platí $|AX| : |BX| : |CX| = |AY| : |BY| : |CY|$. Dokažte, že přímka XY prochází středem O kružnice opsané trojúhelníka ABC.

Příklad 8. V rovině jsou dány body A, B, C neležící na jedné přímce. Zkonstruujte kružnici k procházející skrz body A, B takovou, že tečny z bodu C na ni svírají úhel $60°$.

Příklad 9. Na průměru kružnice k jsou dány body A, B. Vepište do kružnice k rovnoramenný trojúhelník tak, aby body A, B ležely na jeho různých ramenech.

Příklad 10. V rovině jsou dány dvě kružnice $k_1(S_1, r_1)$ a $k_2(S_2, r_2)$, kde $|S_1S_2| > r_1 + r_2$. Najděte množinu všech bodů X, které neleží na přímce S_1S_2 a mají tu vlastnost, že úsečky S_1X, S_2X protínají po řadě kružnice k_1, k_2 v bodech, jejichž vzdálenosti od přímky S_1S_2 se rovnají. (MO 63-A-II-2)

Příklad 11. V rovině jsou dány body A, B, C neležící na jedné přímce a je dána kladná konstanta $k \neq 1$. Nechť m je Apolloniova kružnice definovaná jako množina bodů X, pro něž $|XA| : |XB| = k$, a nechť n je kružnice opsaná trojúhelníku ABC. Označme T, U body, kde se m a n protínají. Dokažte, že tečny na m a n v bodě T, resp. U jsou na sebe kolmé.

Pro náročné

Apolloniova kružnice je těsně spjata s kruhovou inverzí, ale i se středy v trojúhelnících. Pojďme se podívat, kam se nám schovala tentokrát.

Definice. (kruhová inverze) Zobrazení určené kružnicí k se středem S a poloměrem r, které bodu $A \neq S$ přiřadí bod A' ležící na polopřímce SA tak, že

$$|SA'| \cdot |SA| = r^2,$$

se nazývá *kruhová inverze určená kružnicí k*.

Příklad 12. V rovině je dána kružnice k a bod A mimo ni a různý od jejího středu. Nechť A' je obraz bodu A přes kruhovou inverzi podle k. Ukažte, že kružnice k je Apolloniovou kružnicí kolem bodů A a A'.

Příklad 13. (izodynamické body) V rovině je dán trojúhelník ABC. Nechť k_a je Apolloniova kružnice kolem bodů B a C procházející bodem A, tj. množina bodů X takových, že $|XB| : |XC| = |AB| : |AC|$. Této kružnici se říká *A-Apolloniova kružnice*. Obdobně definujme k_b a k_c jako B-Apolloniovu kružnici a C-Apolloniovu kružnici. Ukažte, že k_a, k_b a k_c se potkávají ve dvou bodech.

S izodynamickými body se váže spousta dalších zajímavostí. Jsou si například navzájem obrazy při kruhové inverzi podle kružnice opsané trojúhelníku ABC nebo leží na stejné přímce (Brocardově), na níž leží také opsiště a Lemoinův bod.[1]

[1] Víc se můžete dočíst ve 3. dílu seriálu *Geometrie trojúhelníka*: *https://prase.cz/archive/36/uvod3s.pdf*.

Návody

2. Využij tvrzení o ose úhlu.

3. Znáš poměr stran finálních trojúhelníků?

4. Použij dvakrát úlohu 2.

5. V jakém poměru jsou pak strany AB a AC?

6. Najdi vhodné Apolloniovy kružnice a ukaž, že body uvnitř kružnice mají poměr vzdáleností větší.

7. Sleduj obrázek z pohledu bodů X a Y.

8. Ke konstrukci kružnice se hodí zkonstruovat její střed.

9. Čím bude spojnice středu kružnice k a hlavního vrcholu rovnoramenného trojúhelníku?

10. Označ si Y_1 a Y_2 průsečíky kružnic s úsečkami S_1X a S_2X. Využij podobnost trojúhelníků XY_1Y_2 a XS_1S_2.

11. Dokaž, že trojúhelníky OTA a OBT, kde O je střed kružnice m, jsou podobné.

12. Využij definici kruhové inverze.

13. Ukaž, že průsečík dvou kružnic leží i na té třetí.

Literatura a zdroje

Chtěla bych poděkovat *Jáchymu Soleckému*, jehož přednáška mě už jako účastnici zaujala a z níž jsem nyní notně čerpala pro svůj příspěvek.

[1] Jáchym Solecký: *Apolloniova kružnice*, Branná, 2019.
[2] *Archiv příkladů Matematické olympiády*, *http://www.matematickaolympiada.cz/*.

Švrčkův bod

Adéla Karolína Žáčková

Abstrakt. Přednáška uvádí do problematiky Švrčkova bodu, který je klíčový mimo jiné pro řešení olympiádních geometrických úloh, a ukazuje jeho užitečné vlastnosti. Nuže, pojďme se ponořit do hlubin krásné, syntetické geometrie!

Tvrzení. (Švrčkův bod) *V trojúhelníku ABC se osa vnitřního úhlu BAC, osa strany BC a kružnice opsaná protínají v jednom bodě. Tento bod nazýváme Švrčkův bod příslušející vrcholu A a značíme $\check{S}_A$.*

Tvrzení. *Střed kružnice vepsané $\triangle ABC$, střed kružnice připsané straně BC a body B a C leží na jedné kružnici se středem v $\check{S}_A$.*

Tvrzení. *Nechť se kružnice k, l vnitřně dotýkají v bodě T, tětiva AB kružnice k se dotýká l v bodě U. Pak UT je osa úhlu ATB.*

Tvrzení. (Shooting lemma) *Nechť M je střed oblouku PQ na kružnici ω a přímka p procházející bodem M protíná přímku PQ v X a ω v Y. Pak platí:*

(1) $|MX| \cdot |MY| = |MP|^2$.
(2) *Nechť I je vepsiště $\triangle PYQ$, pak $|MX| \cdot |MY| = |MI|^2$.*
(3) *Nechť p' je další přímka procházející M, která protíná přímku PQ v X' a ω v Y', pak X, Y, X' a Y' leží na jedné kružnici.*

Úmluva. V přednášce budeme používat následující značení (pokud nebude řečeno jinak): I je střed kružnice vepsané (vepsiště), O střed kružnice opsané (opsiště), J_A střed kružnice připsané k BC (připsiště) (obdobně J_B, J_C). Dále nechť AD je osa úhlu CAB, kde D leží na BC, obdobně BE a EF.

A jde se řešit

Příklad 1. Je dán trojúhelník ABC. Označme O střed kružnice opsané trojúhelníku BCI. Dokažte, že $|\sphericalangle OKB| = |\sphericalangle OLC|$, kde K, L jsou body dotyku kružnice vepsané ABC po řadě se stranami AB, AC. (China girls 2012/5)

Příklad 2. Čtyřúhelník $ABCD$ je vepsán do kružnice ω. Středy sousedních oblouků AB, BC, CD, DA označme postupně $\check{S}_A$, $\check{S}_B$, $\check{S}_C$, $\check{S}_D$. Dokažte, že přímky $\check{S}_A\check{S}_C$ a $\check{S}_B\check{S}_D$ jsou na sebe kolmé.

Příklad 3. V trojúhelníku ABC s běžným značením ukažte, že I je ortocentrem trojúhelníka $\check{S}_A\check{S}_B\check{S}_C$.

Příklad 4. Dokažte, že body J_A, J_B, A, B leží na jedné kružnici.

Příklad 5. Označme $\check{N}_A$ průsečík osy vnějšího úhlu u vrcholu A a osy protější strany. Ukažte, že tento „antišvrk“

(i) leží na kružnici opsané trojúhelníku ABC,
(ii) leží ve středu J_BJ_C
(iii) a jeho vzdálenost od přímky BC je $\frac{r_B+r_C}{2}$, kde r_B a r_C značí poloměry kružnic připsaných naproti vrcholům B a C.

Příklad 6. Je dán trojúhelník ABC se středem kružnice vepsané I a vnitřním bodem P. Dále platí

$$|\sphericalangle PBA| + |\sphericalangle PCA| = |\sphericalangle PBC| + |\sphericalangle PCB|.$$

Ukažte, že $|AP| \geq |AI|$, přičemž rovnost nastává, právě když $P = I$. (IMO 2006)

Příklad 7. Nechť jsou AL a BK osy úhlů nerovnoramenného trojúhelníku ABC (L leží na straně BC, K leží na straně AC). Osa úsečky BK protne přímku AL v bodě M. Bod N leží na přímce BK a platí, že LN je rovnoběžná s MK. Dokažte, že $|LN| = |NA|$. (Junior Balkan 2010)

Příklad 8. Kružnice ω_1 a ω_2 mají vnější dotyk v bodě T a obě se vnitřně dotýkají kružnice ω postupně v bodech R a S. Buď Q druhý průsečík RT a ω. Ukažte, že $|\sphericalangle QST| = 90°$. (KMS)

Příklad 9. Nechť BC je průměr kružnice k se středem O. Dále buď A bod na k takový, že $|\sphericalangle AOB| < 120°$, a D buď střed toho oblouku AB, který neobsahuje C. Rovnoběžka s DA vedená bodem O protne AC v bodě I. Osa úsečky OA protne k v bodech E a F. Ukažte, že I je středem kružnice vepsané trojúhelníku CEF. (IMO 2002)

Příklad 10. Mějme trojúhelník ABC. Označme I střed kružnice vepsané a průsečíky osy úhlu z vrcholu A se stranou BC a s kružnicí opsanou postupně D a M. Dokažte, že platí $|AM| \cdot |ID| = |MI| \cdot |AI|$.

Příklad 11. Nechť ABC je ostroúhlý trojúhelník s $|AB| \neq |AC|$. Kružnice nad průměrem BC protne strany AB a AC postupně v bodech M a N. Označme O střed strany BC a R průsečík os úhlů BAC a MON. Dokažte, že kružnice opsané trojúhelníkům BMR a CNR se protínají na straně BC. (IMO 2004)

Příklad 12. Trojúhelník ABC splňuje vztah $|AC| + |BC| = 3 \cdot |AB|$. Kružnice jemu vepsaná se středem I se dotýká stran BC a CA postupně v bodech D a E. Nechť K, L jsou obrazy bodů D, E ve středové souměrnosti podle I. Ukažte, že body A, B, K a L leží na jedné kružnici. (IMO shortlist 2005)

Příklad 13. Je dán trojúhelník ABC se středem I kružnice vepsané a kružnicí opsanou Γ. Přímka AI protne kružnici Γ podruhé v bodě D. Buď E bod na oblouku BDC a F bod na úsečce BC takový, že $|\sphericalangle BAF| = |\sphericalangle CAE| < \frac{1}{2}|\sphericalangle BAC|$. Dále buď G střed úsečky IF. Dokažte, že přímky EI a DG se protínají na kružnici Γ.
(IMO 2010)

Příklad 14. Přímka ℓ protíná kružnici Γ v bodech A, B. Kružnice Γ_1 a Γ_2 jsou vepsané do stejné úseče určené přímkou ℓ a mají vnější dotyk. Dokažte, že jejich vnitřní společná tečna prochází pevným bodem, pohybují-li se Γ_1, Γ_2 ve vymezené úseči. (Prasolov)

Příklad 15. Je dán rovnoramenný lichoběžník $ABCD$ s delší základnou AB. Označme I střed kružnice vepsané trojúhelníku ABC a J střed kružnice připsané straně AD trojúhelníku ACD. Dokažte, že přímky IJ a AB jsou rovnoběžné.

Příklad 16. V trojúhelníku ABC platí $|AB| < |BC|$. Označme M střed AC. Dokažte, že $|\sphericalangle IMA| = |\sphericalangle I\check{N}_B B|$.

Příklad 17. Kružnice ω_1 a ω_2 se obě zevnitř dotýkají kružnice ω postupně v bodech A a B. Společná tečna ω_1 a ω_2 se jich dotýká postupně v bodech C a D. Ukažte, že $ABDC$ je tětivový čtyřúhelník

Příklad 18. Nechť kružnice Ω a ω mají vnitřní dotyk v bodě P, přičemž ω leží uvnitř Ω. Buď AB tětiva Ω, která se dotýká ω v bodě C. Průsečík PC s Ω různý od P si označme Q. Nechť tečny z bodu Q ke kružnici ω protínají kružnici Ω v bodech R a S. Vepsiště trojúhelníků APB, ARB a ASB si postupně označíme jako I, X a Y. Ukažte, že $|\sphericalangle PXI| + |\sphericalangle PYI| = 90°$. (Rumunsko TST 2013)

Příklad 19. Je dán trojúhelník ABC, jeho kružnice opsaná ω a bod D na straně BC. Buď ω_1 kružnice dotýkající se úsečky AD v bodě F, strany BC v bodě E a kružnice ω v bodě K. Dokažte, že střed I kružnice vepsané $\triangle ABC$ leží na přímce EF. (Sawayama-Thebault theorem, PraSe 29/myšmaš)

Návody

1. Všimni si, že na poloze bodů B, C příliš nezáleží, úloha je symetrická podle osy úhlu.

2. Úhel mezi $\check{S}_A\check{S}_C$ a $\check{S}_B\check{S}_D$ je součet velikostí oblouků nad $\check{S}_A\check{S}_B$ a nad $\check{S}_C\check{S}_D$. Jakou část kružnice tyto oblouky dohromady zabírají?

3. Úhel mezi $\check{S}_B\check{S}_C$ a $A\check{S}_A$ je součet velikostí oblouků nad $A\check{S}_C$ a nad $\check{S}_A\check{S}_B$. Jakou část kružnice tyto oblouky dohromady zabírají?

4. Využij vlastnosti os vnitřního a vnějšího úhlu.

5. (ii) Všimni si, že kružnice opsaná $\triangle ABC$ je kružnice devíti bodů $\triangle J_AJ_BJ_C$. Alternativně využij výsledek předchozího příkladu a dokaž, že $\check{N}_A$ je střed kružnice J_BJ_CBC.

6. Dokaž, že P leží na kružnici opsané trojúhelníku BIC, a využij trojúhelníkovou nerovnost.

7. Ukaž, že M je Švrčkův bod nějakého trojúhelníku. A pak to ukaž i pro N.

8. Dokresli si společnou tečnu ω_1 a ω_2. Pak dokaž, že Q je antišvrk.

9. Všimni si, že A je švrk trojúhelníku CEF. Potom dokaž, že I leží na kružnici se středem v A a poloměrem AE.

10. Trojúhelníky MCD a BAD jsou podobné, využij Shooting lemma.

11. Ukaž, že R je Švrčkův bod trojúhelníku AMN.

12. Tipni si, kde leží střed kružnice, a převeď úlohu na počítání vzdáleností.

13. Dokresli J_A, aby ses zbavil bodu G.

14. Využij Shooting lemma a mocnost bodu ke kružnici.

15. Dokresli si vepsiště trojúhelníku ABC, přidej Švrčkův bod $\triangle ADC$ a doúhli.

16. Dokresli si J_A, J_B a podívej se na podobnost trojúhelníků AIC a J_CIJ_A.

17. Využij tvrzení o dotýkajících se kružnicích a dokaž, že střed oblouku určeného společnou tečnou kružnic leží na BD i AC. Shooting lemma.

18. Uvědom si, že Q je švrk všech tří trojúhelníků a dokaž, že X, Y jsou body dotyku tečen z něj ke kružnici ω. Doúhli.

19. Protni osu úhlu u vrcholu A s EF (dokresli i Švrčkův bod) a využij Shooting lemma.

Literatura a zdroje

Příspěvek je převzatý z přednášky *Verči Hladíkové* a také inspirovaný seriálem na téma *Geometrie trojúhelníka*. Tímto jeho dvěma autorům a také Verče děkuji.

[1] Verča Hladíková: *Švrčkův bod*, Branná, 2019.

[2] David Hruška, Radovan Švarc: *Geometrie trojúhelníka*, seriál MKS, 2016/17.

Obsah

Největší společný dělitel (Fíla Čermák) 3
Pravděpodobnostní paradoxy (Fíla Čermák) 8
Kvadratické zbytky (Matěj Doležálek) 11
Konečné projektivní roviny (Klárka Grinerová) 18
Konstrukční úlohy (Verča Hladíková) 22
Odmocniny z jedničky (Lenka Kopfová) 25
Derivace (Terka Kučerová) 29
Fibonacciho čísla (Anna Mlezivová) 32
Toky v sítích (Honza Nekarda) 34
Chinese dumbass notation a SOS (Radek Olšák) 39
Hilbertovský kalkulus (Daniel Perout) 49
Náhodné procházky (Hedvika Ranošová) 53
Izogonály a kamarádi (Martin Raška) 58
p-adická čísla (Martin Raška) 62
Konečné automaty (Michal Töpfer) 71
Kreslení grafů na plochy (Michal Töpfer) 76
Apolloniova kružnice (Adéla Karolína Žáčková) 81
Švrčkův bod (Adéla Karolína Žáčková) 85