Blansko – Obůrka

Sborník, jaro 2011

Háňa Bendová
Peter „πtr“ Korcsok
Jakub „Roman“ Klemsa
Vít „Vejtek“ Musil
Miroslav Olšák
Jakub „šnEk“ Opršal
Tomáš „Šavlík“ Pavlík
Michal „Kenny“ Rolínek
Petr Ryšavý
Alča Skálová
Alexandr „Olin“ Slávik
Miško Szabados
Pepa Tkadlec
Martina Vaváčková

AUTOŘI: Háňa Bendová, Peter „πtr“ Korcsok, Jakub „Roman“ Klemsa, Vít „Vejtek“ Musil, Miroslav Olšák, Jakub „šnEk“ Opršal, Tomáš „Šavlík“ Pavlík, Michal „Kenny“ Rolínek, Petr Ryšavý, Alča Skálová, Alexandr „Olin“ Slávik, Miško Szabados, Pepa Tkadlec, Martina Vaváčková
EDITOR: Jakub „šnEk“ Opršal
vydání první, náklad 45 výtisků
duben 2011
Díky za pomoc všem, kterým je za co děkovat.

Factoring lemma

Háňa Bendová

Abstrakt. Factoring lemma je jednoduché, ale užitečné lemma, s jehož pomocí se dají snadno vyřešit některé diofantické rovnice i jiné číselně teoretické úlohy. Příspěvek obsahuje lemma samotné, několik řešených úloh a několik úloh na procvičení.

Motivační příklad. Buďte a, b, c, d přirozená čísla taková, že $ab = cd$. Dokažte, že $a + b + c + d$ je složené.

Lemma. (Factoring lemma) *Nechť a, b, c, d jsou přirozená čísla taková, že platí $ab = cd$. Pak existují přirozená čísla m, n, p, q taková, že* $\gcd(n, p) = 1$ a

$$a = mn, \quad b = pq, \quad c = mp, \quad d = nq.$$

Důkaz. Podmínku $ab = cd$ můžeme přepsat jako

$$\frac{a}{c} = \frac{d}{b}.$$

Oba zlomky se dají reprezentovat stejným zlomkem $\frac{n}{p}$ v základním tvaru. Položme

$$m = \frac{a}{n} = \frac{c}{p}, \quad q = \frac{b}{p} = \frac{d}{n}.$$

Zřejmě m a q jsou přirozená a čísla m, n, p, q mají požadované vlastnosti.

Řešení příkladu. Najdeme přirozená čísla m, n, p, q jako v lemmatu. Pak

$$a + b + c + d = mn + pq + mp + nq = (m + q)(n + p),$$

z čehož vidíme, že $a + b + c + d$ je složené číslo.

Klíčová slova. factoring lemma, nesoudělnost, pythagorejské trojice, diofantické rovnice

Diofantické rovnice

Příklad 1. Po dvou nesoudělná celá čísla splňují $a^2 + b^2 = c^2$. Jestliže a je liché, existují celá čísla u, v tak, že $a = u^2 - v^2$ a $b = 2uv$.

Řešení. Přepíšeme podmínku jako

$$b^2 = (c - a)(c + a).$$

Podle lemmatu existují m, n, p, q tak, že $b = mn = pq$, $c - a = mp$, $c + a = nq$. Opět podle lemmatu existují x, y, z, w tak, že $m = xy$, $n = zw$, $p = xz$, $q = yw$. Tedy

$$b = xzyw, \quad a = \frac{nq - mp}{2} = \frac{yz}{2}(w^2 - x^2).$$

Protože w^2 a x^2 dávají po dělení čtyřmi pouze zbytky 0 nebo 1 a a je liché, musí platit $2 \mid yz$. Na druhou stranu číslo yz dělí jak b, tak $2a$, tedy $yz = 2$. Tím je důkaz hotov.

Příklad 2. Po dvou nesoudělná přirozená čísla a, b, c splňují $a^2+b^2 = 2c^2$. Dokažte, že existují celá čísla t, u, v tak, že

$$\begin{aligned} a &= \frac{t}{4}(u^2 - v^2 + 2uv), \\ b &= \frac{t}{4}(v^2 - u^2 + 2uv), \\ c &= \frac{t}{4}(u^2 + v^2). \end{aligned}$$

Řešení. Protože $(a - c)(a + c) = (c - b)(c + b)$, existují podle lemmatu celá čísla m, n, p, q tak, že

$$a - c = mn, \quad a + c = pq, \quad c - b = mp, \quad c + b = nq.$$

Odtud $pq - mn = mp + nq$, tedy $p(q - m) = n(q + m)$. Opět podle lemmatu existují celá čísla x, y, z, w taková, že

$$p = xy, \quad q - m = zw, \quad n = xz, \quad q + m = yw.$$

Platí

$$\begin{aligned} a &= \frac{1}{2}(mn + pq) = \frac{1}{2}\left(\frac{yw - zw}{2}xz + \frac{zw + yw}{2}xy\right) = \frac{xw}{4}(y^2 + 2yz - z^2), \\ b &= \frac{1}{2}(nq - mp) = \frac{1}{2}\left(\frac{zw + yw}{2}xz + \frac{yw - zw}{2}xy\right) = \frac{xw}{4}(-y^2 + 2yz + z^2). \end{aligned}$$

Nyní stačí položit $t = uv$, $u = y$, $v = z$.

Příklad 3. Buďte (a, b) a (c, d) dvě různé neuspořádané dvojice celých čísel takové, že $a^2 + b^2 = c^2 + d^2 = k$. Dokažte, že k je složené.

Řešení. Bez újmy na obecnosti $a > c$ (kdyby $a = c$, pak $b = d$ a dvojice by nebyly různé). Úpravou dostaneme

$$(a - c)(a + c) = (d - b)(d + b).$$

Vidíme, že $d > b$, tedy $a + c$, $a - c$, $d + b$, $d - b$ jsou přirozená čísla a podle lemmatu najdeme přirozená čísla m, n, p, q tak, že

$$a + c = mn, \quad a - c = pq, \quad d + b = mp, \quad d - b = nq.$$

Potom

$$a = \frac{mn + pq}{2}, \quad b = \frac{mp - nq}{2}$$

a platí

$$\begin{aligned} 4k = 4(a^2 + b^2) &= (mn + pq)^2 + (nq - mp)^2 \\ &= m^2n^2 + p^2q^2 + n^2q^2 + m^2p^2 = (m^2 + q^2)(n^2 + p^2). \end{aligned}$$

Předpokládejme, že k je prvočíslo. Pak bez újmy na obecnosti $k \mid m^2 + q^2$. Tedy buď $n^2 + p^2 = 4$, nebo $n^2 + p^2 = 2$. První případ nemůže nastat, neboť číslo 4 se nedá napsat jako součet dvou čtverců. Ve druhém případě $n = p = 1$, z čehož plyne $a = c$, $b = d$, což jsme v zadání zamítli. Číslo k tedy musí být složené.

V řešení posledního příkladu jsme po cestě dokázali i následující lemma.

Lemma. *Jsou-li a, b, c, d celá čísla a $a^2 + b^2 = c^2 + d^2$, pak existují celá čísla m, n, p, q taková, že*

$$2a = mn + pq, \quad 2b = mp - nq, \quad 2c = mp + nq, \quad 2d = mn - pq.$$

Další příklady

Příklad 1. Najdi všechna celočíselná řešení rovnice $x^2 + 3y^2 = z^2$.

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

Příklad 3. Dokažte, že je-li $N = a^2 + 2b^2 = c^2 + 2d^2$ a $\{a, b\} \neq \{c, d\}$, pak N je složené.

Příklad 4. Dokažte, že jsou-li a, b, c, d přirozená čísla a $ab = cd$, pak $a^n + b^n + c^n + d^n$ je složené.

Literatura a zdroje

[1] Iurie Boreico, Roman Teleuca, *A Factoring Lemma*, Mathematical reflections, 2007.
[2] Herman, Šimša, Kučera, *Metody řešení matematických úloh I*, Brno, 2001

Grafové algoritmy

Peter „πtr“ Korcsok

Abstrakt. Viacero matematických problémov je možné previesť na niektorú z grafových úloh, pre ktorú už existuje mnoho spôsobov, ako ju úspešne vyriešiť. Tento príspevok predstavuje 4 základné grafové algoritmy v ich najzákladnejších podobách, aby boli zrozumiteľné aj pre ľudí, ktorí sa nepohybujú v informatickej oblasti.

Pri skúmaní matematiky môžeme naraziť na množstvo problémov z úplne odlišných oblastí. Často ale stačí trochu abstrakcie a vieme ich previesť na niektorú z grafových úloh, ktoré potom podstatne jednoduchšie vyriešime, ak vieme ako na to. Cieľom tohto príspevku je predviesť niekoľko základných metód, ako tieto zadania úspešne zdolať.

Na začiatok by asi bolo vhodné vysvetliť, čo vlastne slová z názvu znamenajú:

Definícia. *Grafom* G nazveme dvojicu (V, E), kde $E \subseteq \binom{V}{2}$.[1] Prvky množín V a E potom budeme nazývať *vrcholmi* prípadne *hranami* grafu G.

Definícia. *Algoritmus* je konečná postupnosť dobre definovaných inštrukcií na splnenie určitej úlohy.

Ďalej sa nám bude hodiť poznať niekoľko pojmov zo sveta grafov, preto si ich radšej hneď pripomeňme:

Definícia. *Cestou* v grafe $G = (V, E)$ rozumieme postupnosť v_1, e_1, v_2, …, v_{n-1}, e_{n-1}, v_n, kde $e_i = (v_i, v_{i+1}) \in E$ $(\forall i = 1, \ldots, n-1)$ a jednotlivé vrcholy v_i ani hrany e_i sa neopakujú.

Definícia. *Kružnicou* v grafe $G = (V, E)$ budeme rozumieť postupnosť v_1, e_1, v_2, …, v_{n-1}, e_{n-1}, v_n, e_n, v_1, kde $e_i = (v_i, v_{i+1}) \in E$ $(\forall i = 1, \ldots, n-1)$, $e_n = (v_n, v_1) \in E$ a jednotlivé vrcholy v_i ani hrany e_i sa neopakujú.

Definícia. Graf $G = (V, E)$ nazveme *súvislým*, pokiaľ medzi každými dvoma vrcholmi $u, v \in V$ vedie cesta.

Kľúčové slová. graf, algoritmus, prehľadávanie do hĺbky, prehľadávanie do šírky, najkratšia cesta, hľadanie kružníc, Dijkstrov algoritmus, minimálna kostra, Jarníkov algoritmus

[1] Symbolom $\binom{X}{k}$ značíme množinu všetkých k-prvkových podmnožín množiny X.

Definícia. Pre súvislý graf $G = (V, E)$ definujeme jeho *kostru* ako súvislý graf $K = (V, E')$, ktorý neobsahuje žiadnu kružnicu a zároveň $E' \subseteq E$.

Definícia. *Ohodnotenie* grafu $G = (V, E)$ je ľubovoľné zobrazenie $c\colon E \to \mathbb{R}$, takto ohodnotený graf budeme značiť (V, E, c).

Ešte si zaveďme niekoľko značiek, ktoré nám potom sprehľadnia a skrátia zápis algoritmov:

Značenie.

- Symbol $x := y$ označuje priradenie hodnoty y do premennej x.
- Symbolom $x \to F$ budeme značiť pridanie hodnoty x na koniec zoznamu F.
- A nakoniec $F \to x$ bude predstavovať výber prvej hodnoty zo zoznamu F a jej dosadenie do premennej x.

Pretože už vieme všetky potrebné pojmy, nič nám nestojí v ceste k našim algoritmom. Začnime dvoma spôsobmi, ako môžeme taký graf vôbec prejsť, aby sme zbytočne neprechádzali ten istý vrchol viackrát.

Prehľadávanie grafu do hĺbky

Prvá možnosť je tzv. *prehľadávanie do hĺbky* (angl. *Depth First Search*, skrátene *DFS*). Hlavnou ideou tohto algoritmu je začať v jednom vrchole, z neho prejsť na nenavštíveného suseda, odtiaľ na ďalšieho suseda, ... a to celé až dovtedy, kým sa nám neprejdení susedia „neminú“. Vtedy sa vrátime k niektorému z predchádzajúcich vrcholov a skúšame ďalej.

Vstupom do tohto algoritmu by mal byť súvislý graf (V, E) a nejaký jeho vrchol $v \in V$, z ktorého chceme prehľadávanie spustiť. Výstupom potom bude napríklad usporiadanie množiny V v poradí, v akom boli prvky navštívené.

Algoritmus. (DFS)

1. označ v za navštívený, ostatné vrcholy za nenavštívené, $R := \{v\}$
2. ak $|R| = |V|$, vráť R a skonči
3. ak existuje nenavštívený sused v, označ ho ako u a navštívený, $u \to R$, $r(u) := v$, $v := u$ a prejdi na 2. krok
4. ak všetci susedia v sú už navštívení, $v := r(v)$ a prejdi na 3. krok

Pomocou DFS vieme napríklad nájsť nejakú kostru zadaného hrafu, nájsť v ňom kružnice a ak vynecháme podmienku súvislosti vstupného grafu (a mierne upravíme 2. krok), preskúmané vrcholy budú tvoriť práve tzv. *komponentu súvislosti* obsahujúcu vrchol v, teda najväčšiu súvislú časť grafu, v ktorej sa vrchol v nachádza.

Miernymi úpravami tohto algoritmu dostaneme pomerne efektívny spôsob na hľadanie cesty v labyrinte, prípadne dokonca vytváranie rôzne komplikovaných bludísk.

Prehľadávanie grafu do šírky

Druhou možnosťou je potom tzv. *prehľadávanie do šírky* (angl. *Breadth First Se-*

arch, skrátene *BFS*). Podobne ako pri DFS, aj tu začíname v jednom vrchole, akurát z neho prejdeme najprv všetkých jeho susedov, potom susedov susedov a takto pokračujeme, kým nemáme prejdený celý graf (alebo jeho komponentu).

Vstupom algoritmu je opäť súvislý graf (V, E) a štartovací bod $v \in V$, výstupom je znovu poradie prechodu vrcholov.

Algoritmus. (BFS)

1. označ v za navštívený, ostatné vrcholy za nenavštívené, $F := \{v\}$, $R := \emptyset$
2. ak $|R| = |V|$, vráť R a skonči
3. ak F nie je prázdne, $F \to v$, $v \to R$
4. ak existuje nenavštívený sused v, označ ho ako u a navštívený, $u \to F$ a prejdi znovu na 4. krok, inak prejdi na 3. krok

BFS prechádza vrcholy podľa vzrastajúcej vzdialenosti (na počet hrán) od počiatku v, takže ho môžeme použiť napríklad, keď potrebujeme nájsť najkratšiu cestu medzi dvoma bodmi. Podobne ako DFS, aj tento algoritmus môžeme upraviť tak, aby bol schopný bežať na nesúvislých grafoch – opäť preskúma práve vrcholy z jednej komponenty.

Hľadanie najkratšej cesty

Základnú myšlienku BFS môžeme rozšíriť aj na ohodnotené grafy a vzdialenosť počítanú ako minimálny súčet hodnôt hrán na ceste medzi dvoma bodmi. Na nájdenie tej najkratšej máme hneď niekoľko možných spôsobov, najjednoduchší z nich je asi *Dijkstrov algoritmus*. Znovu vyjdeme z jedného vrcholu v, ktorého vzdialenosť od seba samého je 0, vzdialenosti ostatných bodov ale zatiaľ nepoznáme. V každom kroku si potom zvolíme najbližší nespracovaný vrchol a všetkým jeho susedom upravíme vzdialenosť od v.

Tu si už s obyčajným grafom nevystačíme, budeme potrebovať, aby bol ohodnotený a dokonca všetky hrany musia mať nezápornú hodnotu (inak si v grafe narobíme neporiadok a to predsa nechceme :-)), po úspešnom priebehu ale budeme poznať najkratšiu vzdialenosť z počiatočného vrcholu v do všetkých ostatných.

Algoritmus. (Dijkstrov)

1. označ všetky vrcholy za nenavštívené, $d(v) := 0$, $d(u) := \infty$ $(\forall u \neq v)$
2. ak neexistuje vrchol v s $d(v) < \infty$, vráť d a skonči
3. za v označ nenavštívený vrchol s minimálnou hodnotou $d(v)$, označ v za navštívený
4. všetkým nenavštíveným susedom u vrcholu v nastav $d(u) := \min\{d(v) + c(v, u),\ d(u)\}$ a prejdi na 2. krok

Pomocou Dijkstrovho algoritmu vieme riešiť množstvo úloh, ktoré je možné previesť na problém najkratšej cesty (konkrétne príklady si spomenieme na prednáške). Na riešenie tohto problému samozrejme existujú aj iné algoritmy, viaceré si dokonca

vedia poradiť aj so zápornými hranami, vo väčšine prípadov nám ale ten Dijkstrov dostatočne poslúži.

Minimálna kostra

Poslednou oblasťou grafových úloh, ktorej sa budeme venovať, je problematika kostier. Už sme si uviedli jeden spôsob, ako ľubovoľnú z nich nájsť – DFS. Pretože ale v dnešnom svete je všetko príliš drahé, skúsme rovno nájsť kostru, ktorej celková cena za všetky vybrané hrany bude najnižšia možná. Aj na toto máme viacero možných algoritmov – napríklad *Jarníkov*[2], *Borůvkov* alebo *Kruskalov*, všetky tri sa radia medzi tzv. „pažravé“[3] algoritmy.

Pozrime sa teraz podrobnejšie na Jarníkov postup: jeho základnou ideou je budovanie jednej komponenty súvislosti (definícia je pri DFS), ku ktorej v každom kroku pridáme jeden vrchol a niektorú hranu z tohto bodu do už vytvorenej komponenty, pričom sa snažíme, aby pridaná hrana mala vždy najmenšiu váhu. Vstupom je opäť ohodnotený súvislý graf (V, E, c), výstupom niektorá z jeho minimálnych kostier.

Algoritmus. (Jarníkov)

1. zvoľ si niektorý vrchol v, $V' := \{v\}$, $E' := \emptyset$
2. ak $|V'| = |V|$, vráť (V', E') a skonči
3. z množiny hrán $\{(u, v); u \in V', v \in V \setminus V'\}$ vyber hranu $e = (u, v)$, že hodnota $c(e)$ je minimálna
4. $v \to V'$, $e \to E'$ a prejdi na 2. krok

Podmienku súvislosti vstupného grafu potrebujeme k tomu, aby sme nakoniec do kostry mohli pridať všetky vrcholy, v opačnom prípade by sme našli iba kostru komponenty, do ktorej patrí náhodne zvolený prvý vrchol. Tento algoritmus síce inde ako pri hľadaní kostry minimálnej váhy veľmi nevyužijeme, ale už len tým nám dokáže značne uľahčiť ďalšiu prácu na pôvodnom probléme. Obecne sú totiž stromy[4] (čo kostra je) na skúmanie jednoduchšie ako grafy s kružnicami.

Tým sa pomaly dostávame na koniec príspevku. Spomenuté algoritmy samozrejme nie sú jediné, často sa v praxi upravujú a kombinujú s ďalšími, aby sa prispôsobili špecifickým podmienkam zadania. Keby sme chceli aspoň okrajovo popísať všetky, tento text by musel byť podstatne dlhší.

Literatúra a zdroje

[1] Knižnica PraSiatka, *http://mks.mff.cuni.cz/library/*

[2] V anglickej literatúre je známy skôr ako *Primov*, ale pretože Jarník ho popísal 27 rokov pred Primom, myslím, že toto označenie si zaslúži.

[3] Po česky „hladové“, po anglicky „greedy“.

[4] *Strom* je súvislý graf bez kružníc.

O hranici neporiadku

Peter „πtr“ Korcsok

Motto. *Akokoľvek sa budeš snažiť, absolútny neporiadok neurobíš ;)*

Abstrakt. Dirichletov princíp je silný dôkazový nástroj, ktorý má široké využitie v najrôznejších oblastiach matematiky. V príspevku je metóda predvedená na dvoch riešených úlohách a čitateľovi je ďalej ponúknutá možnosť vyskúšať si jej použitie na sade 20 príkladov, ktoré sú usporiadané podľa zložitosti. Druhú časť príspevku tvorí aplikácia princípu vo svete grafov – úvod do Ramseyovej teórie.

Dirichletov princíp

Keby sme sa opýtali náhodného okoloidúceho, pravdepodobne by nám povedal, že svetu (a hlavne tomu matematickému) vládne chaos a neporiadok. Cieľom tohto príspevku je ukázať, že aj keď sa to na prvý pohľad nezdá, skutočnosť je úplne iná. Aj v zdanlivo neusporiadaných systémoch totiž platia určité pravidlá, o ktorých si tu niečo povieme.

Pri našom boji budeme mať pomerne silnú zbraň, ktorá je aj napriek svojmu vznešenému názvu *Dirichletov princíp* naozaj jednoduché tvrdenie. Toto označenie nie je jediné, často sa naň odkazuje ako na *priehradkový princíp* alebo *princíp holubníka* (angl. *pigeonhole pricinple*).

Veta. (Dirichletov princíp) *Ak máme rozdeliť $n+1$ guličiek do n košíkov, určite vieme nájsť košík, v ktorom sú aspoň 2 guličky.*

V mnohých prípadoch sa nám viac bude hodiť jeho obecnejšia formulácia:

Veta. (Dirichletov princíp, obecne) *Majme prirodzené čísla $n_1, n_2, \ldots, n_t$, množinu X s aspoň $1+\sum_{i=1}^{t}(n_i-1)$ prvkami a jej rozklad na množiny $X_1, X_2, \ldots, X_t$. Potom určite existuje i také, že X_i má aspoň n_i prvkov.*

Pre lepšiu predstavu si ho hneď vyskúšame použiť:

Kľúčové slová. Dirichletov princíp, princíp holubníku, pigeonhole principle, Erdős-Szekeres, Ramseyove vety, Ramseyovo číslo, graf, ofarbenie hrán, podgraf

Úloha 1. V šuflíku máme pomiešaných 10 čiernych, 12 modrých a 8 sivých ponožiek. Koľko ich musíme vybrať, aby sme s istotou mali aspoň jeden pár rovnakej farby?

Riešenie. Každá vytiahnutá ponožka má jednu z troch farieb, teda $n = 3$. Na konci chceme mať aspoň dva kusy spadajúce do rovnakej skupiny, preto nám podľa prvej verzie princípu stačí vybrať $n + 1 = 4$ ponožky.

Úloha 2. Ukážte, že z ľubovoľnej postupnosti $n + 1$ rôznych prirodzených čísel $a_0, a_1, \ldots, a_n$ vieme vybrať skupinu za sebou idúcich prvkov tak, aby ich súčet bol násobkom n.

Riešenie. Na začiatok sa pozrime na to, aké zvyšky dávajú súčty prvých členov našej postupnosti (teda $a_0 + \cdots + a_k$ postupne pre $k = 0, \ldots, n$) po delení číslom n. Pretože rôznych zvyškov je maximálne n, ale máme $n + 1$ súčtov, určite existujú $i < j$ také, že pre nejaké celé čísla x, y a z platia rovnosti:

$$a_0 + \cdots + a_i = nx + z$$
$$a_0 + \cdots + a_j = ny + z$$

Potom ale $a_{i+1}+\cdots+a_j = (a_0+\cdots+a_j)-(a_0+\cdots+a_i) = (ny+z)-(nx+z) = n(y-x)$, čo sme chceli dokázať. □

Dirichletov princíp sa môže s prehľadom využiť aj pri dôkaze nasledujúceho tvrdenia.

Tvrdenie. (Erdős-Szekeres) *Z každej postupnosti n^2+1 rôznych čísel vieme vybrať rastúcu alebo klesajúcu podpostupnosť dĺžky $n + 1$.*

Ľahké príklady

Príklad 3. Ukážte, že medzi 25 učastníkmi sústredenia existujú traja takí, že oslavujú narodeniny v rovnakom mesiaci.

Príklad 4. Dokážte, že v každej skupine 101 aspoň dvojciferných čísel vieme nájsť dvojicu takú, že majú posledné dve cifry rovnaké.

Príklad 5. V štvorci 6×6 cm je náhodne rozmiestnených 37 bodov. Dokážte, že vždy existuje štvorec 2×2 cm, v ktorom sa nachádza aspoň päť z nich.

(PraSe 94/95)

Príklad 6. V štvorci 10×10 cm je náhodne rozmiestnených 101 bodov. Dokážte, že vždy vieme vybrať trojuholník s obsahom 1 cm^2, ktorý obsahuje aspoň dva z nich.

Stredne ťažké príklady

Príklad 7. Po stole 1×1 m lezie 51 múch. Ukážte, že s pomocou kruhového hrnca

s polomerom $\frac{1}{7}$ m (a trochou šikovnosti **:)**) môžeme chytiť aspoň 3 muchy jednou ranou.

Príklad 8. Nájdite čo najdlhšiu aritmetickú postupnosť s diferenciou 60, ktorej všetky prvky sú prvočísla. (PraSe 98/99, 1. séria)

Príklad 9. Na šachovnici 8×8 políčok máme rozostavených 33 veží. Vieme medzi nimi nájsť 5 takých, že sa navzájom neohrozujú? (PraSe 00/01, 3. séria)

Príklad 10. Hrací plán hry „Človeče, nehnevaj sa“ obsahuje 36 políčok usporiadaných do kruhu. Koľko najmenej figúrok musí byť v hre, aby sme vždy mohli niektorú z nich vyradiť pomocou inej nezávisle na ich rozložení a výsledku hodu kockou? (PraSe 00/01, 3. séria)

Príklad 11. Dokážte, že pre všetky nesúdeliteľné čísla a a b je desatinný rozvoj $\frac{a}{b}$ konečný, alebo má periódu maximálne $b - 1$.

Príklad 12. Majme dvadsaťprvkovú množinu A po dvoch nesúdeliteľných prirodzených čísel a množinu B definovanú ako $B = \{x^y; x, y \in A\}$. Dokážte, že existujú dva prvky množiny B, ktorých rozdiel je deliteľný číslom 379.

Príklad 13. Dokážte, že z ľubovoľnej pätice vrcholov pravidelného deväťuholníku vieme jeden odstrániť tak, aby zvyšné štyri tvorili vrcholy lichobežníka.

Ťažké príklady

Príklad 14. New York je okrem iného známy aj pravidelnosťou svojich ulíc – má 151 severojužných a 151 východozápadných ulíc, ktoré sa vždy po 100 metroch krížia. V meste je rozmiestnených spolu 11401 telefónnych automatov. Vieme tam nájsť dva automaty, ktoré sú vzdialené maximálne 200 metrov chôdze po chodníku? (PraSe 00/01, 3. séria)

Príklad 15. Dokážte, že medzi ľubovoľnými ôsmimi zloženými prirodzenými číslami menšími než 360 existujú vždy dve čísla, ktoré majú spoločného deliteľa väčšieho ako 1. (PraSe 94/95)

Príklad 16. Dokážte, že pre každé $n \in \mathbb{N}$ vieme z ľubovoľnej $(n + 1)$-prvkovej podmnožiny $\{1, 2. \ldots, 2n\}$ vybrať dve rôzne čísla, z ktorých jedno delí druhé. (PraSe 00/01, 3. séria)

Príklad 17. Dokážte, že pre ľubovoľné prirodzené číslo n existuje jeho prirodzený násobok zložený iba z cifier 0 a 1.

Príklad 18. Na priamke p leží postupne 6 úsekov $u_1, u_2, \ldots, u_6$ s dĺžkami po rade $d_1, d_2, \ldots, d_6$, ktoré sú po dvoch disjunktné. V jednej polrovine určenej priamkou p zostrojíme body $S_1, S_2, \ldots, S_6$ tak, že vrchol S_i tvorí spolu s úsečkou u_i rovnostranný trojuholník $(i = 1, 2, \ldots, 6)$. Nakoniec vytvorme kruhy so stredmi v bodoch

$S_1, S_2, \ldots, S_6$ a polomermi $d_1, d_2, \ldots, d_6$. Dokážte, že neexistuje bod, ktorý by ležal vo všetkých šiestich kruhoch. (PraSe 08/09, 5. séria)

Pre borcov

Príklad 19. Dokážte, že z ľubovoľného šestnásťciferného čísla vieme vybrať neprázdnu skupinu za sebou idúcich cifier, ktorej ciferný súčin je druhou mocninou celého čísla. (PraSe 08/09, 5. séria)

Príklad 20. Majme v rovine n bodov $x_1, \ldots, x_n$ v obecnej polohe[5], pričom niektoré z týchto bodov sú spojené úsečkami. *Stupňom* bodu x_k budeme nazývať počet spojníc, ktoré z neho vedú. Dokážte, že ak pre žiadne body rovnakého stupňa neexistuje ich spoločný „sused“ a navyše aspoň jedna dvojica bodov je spojená úsečkou, potom nutne existuje bod, ktorého stupeň je 1. (PraSe 94/95)

Príklad 21. Ukážte, že existuje prirodzené číslo N také, že každé prirodzené číslo $a > N$ vieme „osekať“ z okrajov na prirodzený násobok čísla 2011.
(Kanadská MO 2011)

Príklad 22. Majme v priestore n bodov ($n \geq 3$), pričom ich spojnice sú rôzne dlhé a r z týchto úsečiek je zafarbených. Dokážte, že potom z týchto zafarbených spojníc vieme vytvoriť ťah[6] dĺžky aspoň $\lceil \frac{2r}{n} \rceil$, v ktorom dĺžka úsečiek narastá.[7]
(PraSe 97/98, 2. séria)

Ramseyove vety

Doteraz sme sa zaoberali ohraničovaním neporiadku v najrôznejších situáciách. Zamerajme sa preto v druhej časti príspevku už iba na jednu pomerne rozsiahlu časť matematiky – grafy. S ich pomocou vieme naznačiť rôznorodé vzťahy (priateľstvá, cesty medzi mestami, výmenné kurzy v bankách, ...) do jednoduchého modelu, pre ktorý už máme viaceré nástroje, ako s ním pracovať.

Aby sme však mohli pokračovať, potrebujeme si nadefinovať niekoľko pojmov:

Definícia. *Grafom* G nazveme dvojicu (V, E), kde $E \subseteq \binom{V}{2}$.[8] Prvky množín V a E budeme potom nazývať *vrcholmi* prípadne *hranami* grafu G.

Definícia. *Úplným grafom* $K_n = (V, E)$ budeme nazývať graf, v ktorom $|V| = n$ a $E = \binom{V}{2}$.

[5] Množina bodov je v *obecnej polohe*, pokiaľ žiadne tri z nich neležia na priamke.
[6] *Ťah* je postupnosť na seba nadväzujúcich hrán, ktoré sa neopakujú.
[7] Symbol $\lceil x \rceil$ označuje *hornú celú časť* čísla x, teda najbližšie celé číslo y, že $x \leq y$.
[8] Symbolom $\binom{X}{k}$ značíme množinu všetkých k-prvkových podmnožín množiny X.

Definícia. *Podgrafom* grafu $G = (V, E)$ budeme označovať graf $G' = (V', E')$, pre ktorý platí, že $V' \subseteq V$ a $E' \subseteq \binom{V'}{2} \cap E$.

Definícia. *Ofarbením hrán* grafu $G = (V, E)$ k farbami rozumieme ľubovoľné zobrazenie $f\colon E \to \{1, 2, \ldots, k\}$.

Na začiatok si uveďme motivačný príklad, s ktorým ste sa už pravdepodobne stretli.

Tvrdenie. (Večierok so šiestimi) *Na každom večierku s aspoň šiestimi hosťami vieme nájsť trojicu ľudí, kde sa všetci traja navzájom poznajú, alebo trojicu vzájomne neznámych hostí.*

Tvrdenie, ktoré sme práve vyslovili je špeciálnym prípadom rozsiahlejšej teórie pomenovanej po britskom matematikovi F. P. Ramseyovi. Nasledujúca veta má viacero variant, my si uvedieme len jej obecné znenie pre konečné grafy.

Veta. (Ramseyova) *Pre každé $t \in \mathbb{N}$ a skupinu čísel $n_1, n_2, \ldots, n_t$ existuje také číslo N, že ľubovoľné ofarbenie grafu K_N pomocou t farieb obsahuje ako podgraf K_{n_i}, kde všetky hrany sú i-tej farby (pre nejaké $1 \leq i \leq t$).*

Poznámka. Pozornejším čitateľom určite neuniklo, že tvrdenie o večierku je naozaj len špeciálnym prípadom pre $t = 2$ a $n_1 = n_2 = 3$. Týmto parametrom odpovedá napr. $N = 6$.

Definícia. Najmenšiu hodnotu N vyhovujúcu Ramseyovej vete s parametrami $t, n_1, n_2, \ldots, n_t$ často označujeme $R(n_1, n_2, \ldots, n_t)$ a nazývame *Ramseyovým číslom*.

Poznámka. Z definície Ramseyových čísel je jasné, že pre každú dvojicu čísel a, b platí $R(a, b) = R(b, a)$ (v nájdenom grafe len zmeníme farby hrán na opačné), podobná vlastnosť platí aj pre prípad $t \geq 3$.

Odhad Ramseyových čísel

Ramseyove čísla majú síce pekné vlastnosti, ale bez toho, aby sme poznali ich (približnú) hodnotu, je ich využitie dosť obmedzené. Tým sa postupne dostávame k menej príjemnej záležitosti – v skutočnosti je známa len malá časť týchto hodnôt, napr.:

- $R(3, 3) = 6$,
- $R(3, 4) = 9$,
- $R(3, 5) = 14$,
- $R(3, 6) = 18$,
- $R(4, 4) = 18$,
- $R(4, 5) = 25$,
- a niektoré ďalšie

Pri viacerých je ďalej známy aspoň interval, v ktorom sa nachádzajú, napr.:

- $35 \leq R(4, 6) \leq 41$,
- $43 \leq R(5, 5) \leq 49$,

- $58 \leq R(5,6) \leq 87$,
- $102 \leq R(6,6) \leq 165$,
- ...

Z „viacfarebných“ Ramseyových čísel spomeniem napríklad, že $R(3,3,3) = 17$, dôkaz tejto rovnosti už ale nie je úplne triviálny.

Veta. (Horný odhad) *Pre ľubovoľnú dvojicu čísel $k, l \in \mathbb{N}$ platí: $R(k,l) \leq \binom{k+l-2}{k-1}$.*

Veta. (Dolný odhad) *Pokiaľ čísla n a k spĺňajú nerovnosť $\binom{n}{k} \cdot 2^{1-\binom{k}{2}} < 1$, potom platí $R(k,k) > n$.*

Dôsledok. Pre každé $k \geq 3$ platí $R(k,k) > 2^{k/2}$.

Kam ďalej?

To, čo sme si tu uviedli, je jedna z najzákladnejších variant Ramseyovej vety. V skutočnosti je možné ju rozšíriť a zobecniť viacerými spôsobmi, za zmienku stoja hlavne nasledujúce dve možnosti:

(1) Doteraz sme ofarbovali hrany, teda dvojprvkové množiny vrcholov, rovnako ale môžeme ofarbovať aj väčšie skupiny (veľkosti n). Potom opäť hľadáme určitú podmnožinu vrcholov spĺňajúcu podmienku, že všetky n-tice v nej obsiahnuté sú rovnakej farby.

(2) Druhou možnosťou je zabudnúť na konečné grafy a prejsť rovno k tým nekonečným. Tu už ale musíme byť opatrnejšími, pretože bez podmienky konečnosti grafov vieme napáchať oveľa viac šarapaty :)

Ani jednému z možných rozšírení sa už venovať nebudeme.

Literatúra a zdroje

[1] Knižnica PraSiatka, *http://mks.mff.cuni.cz/library/*
[2] Archív PraSiatka, *http://mks.mff.cuni.cz/archive/*
[3] Internetové fórum *Mathlinks*, *http://www.mathlinks.ro*
[4] Jiří Matoušek, Jaroslav Nešetřil, *Kapitoly z diskrétní matematiky*, Karolinum, Praha, 2009.

Pri písaní príspevku som sa inšpiroval príspevkom Davida Stanovského *Dirichletův princip*, za čo sa mu chcem poďakovať.

RSA pro začátečníky

Jakub „Roman“ Klemsa

Abstrakt. RSA je moderní (1977) asymetrická šifrovací metoda, na které je postavena většina dnešních šifrovacích systémů. Cílem přednášky bude ukázat princip fungování na základě Eulerovy věty a ukázka na konkrétním příkladě. Předvedeme si i některé způsoby zlomení této šifry, taktéž na příkladech.

Tvrzení. *Pro libovolná dvě celá čísla a, b, kde alespoň jedno je nenulové, platí*

$$\mathrm{NSD}(a,b) = \mathrm{NSD}(a-b,b).$$

My toto tvrzení budeme používat pouze pro dvě přirozená čísla.

Pozorování. *Pro každé přirozené číslo a platí:*[9] $\mathrm{NSD}(a,1) = 1$, $\mathrm{NSD}(a,0) = a$.

Eukleidův algoritmus

Eukleidův algoritmus převádí hledání NSD dvou přirozených čísel na hledání NSD, kde jedno číslo je ostře menší. BÚNO předpokládejme $a > b$ a postupujme takto, dokud jsou oba členy NSD nezáporné:

$$\mathrm{NSD}(a,b) = \mathrm{NSD}(a-b,b) = \ldots = \mathrm{NSD}(a-k_1 b, b).$$

Označíme $r_1 := a - k_1 b = a \bmod b$ a víme, že $0 \leq r_1 < b$. Pokud $r_1 = 0$, algoritmus končí s hodnotou b, pokud ne, opakujeme algoritmus pro dvojici b, r_1:

$$\mathrm{NSD}(a,b) = \mathrm{NSD}(r_1,b) = \mathrm{NSD}(r_1, b-k_2 r_1) = \mathrm{NSD}(r_1,r_2),$$

kde $r_2 = b \bmod r_1$. Rekurzivně opakujeme, dokud nedojdeme k $\mathrm{NSD}(r_k,0) = r_k$.

Tvrzení. *Eukleidův algoritmus skončí po konečném počtu kroků ve stavu, kdy* $\mathrm{NSD}(a,b) = \mathrm{NSD}(r_k,0) = r_k$.

Klíčová slova. Eukleidův algoritmus, Malá Fermatova věta, Eulerova funkce, Eulerova věta, RSA, Fermatova a Pollardova metoda.

[9] $(\forall k \in \mathbb{N})(k \mid 0)$

Tvrzení. *Zpětným postupem dokážeme z Eukleidova algoritmu najít celá čísla x_0, y_0 taková, že* $\mathrm{NSD}(a,b) = ax_0 + by_0$. *Protože $k(ab - ba) = 0$ a každé z čísel a, b je dělitelné* $\mathrm{NSD}(a,b)$, *najdeme zbývající řešení pomocí*

$$\mathrm{NSD}(a,b) = k\left(a\frac{b}{\mathrm{NSD}(a,b)} - b\frac{a}{\mathrm{NSD}(a,b)}\right) + ax_0 + by_0$$

ve tvaru $x = x_0 + k(b/\mathrm{NSD}(a,b))$, $y = y_0 - k(a/\mathrm{NSD}(a,b))$, kde $k \in \mathbb{Z}$. Ukazuje se, že toto jsou již všechna řešení rovnice $ax + by = \mathrm{NSD}(a,b)$.

Cvičení. Pomocí Eukleidova algoritmu najděte $\mathrm{NSD}(432, 234)$ a dvě „nejbližší“ dvojice celých čísel x, y, aby $\mathrm{NSD}(432, 234) = 432x - 234y$.

Základní aritmetické věty

Tvrzení. (Malá Fermatova věta) *Pro libovolné prvočíslo p a přirozené číslo a nesoudělné s p platí*

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

Definice. (Eulerova funkce) Hodnotu Eulerovy funkce $\varphi\colon \mathbb{N} \to \mathbb{N}$ definujeme pro n jako počet přirozených čísel nepřevyšujících n, která jsou s n nesoudělná, tedy

$$\varphi(n) := \#\{k \in \mathbb{N} : k \leq n,\ k \perp n\}.$$

Cvičení. Spočítejte hodnotu Eulerovy funkce, kde p, q prvočísla, $k \in \mathbb{N}$: $\varphi(1)$, $\varphi(p)$, $\varphi(p^k)$, $\varphi(pq)$.

Tvrzení. (Eulerova věta) *Pro libovolná dvě přirozená čísla a, n, $a \perp n$, platí*

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

Poznámka. Eulerova věta pro n prvočíslo přechází v Malou Fermatovu větu.

Asymetrická šifra RSA

Šifrovací metodu RSA navrhli roku 1977 matematici Rivest, Shamir a Adleman. Jedná se o šifru s jedním veřejným šifrovacím klíčem a jedním soukromým, dešifrovacím, odtud asymetrická.

Pro šifrování pomocí RSA budeme potřebovat dvě velká (ale opravdu velká) prvočísla p a q, jejich vynásobením dostáváme tzv. modulus $n = pq$. Odtud známe i hodnotu Eulerovy funkce $\varphi(n) = (p-1)(q-1)$. Dále vygenerujeme veřejný exponent e takový, aby $e \perp \varphi(n)$, $1 < e < \varphi(n)$. Nesoudělnost ověříme Eukleidovým algoritmem, odkud zjistíme i koeficienty d a k takové, že $ed - k\varphi(n) = 1$. Najdeme d takové, že $1 < d < \varphi(n)$. Toto d pak bude náš soukromý exponent.

Shrňme si, co uveřejníme a co naopak přísně utajíme: dvojici (n, e) uveřejníme jako veřejný klíč, dvojici (n, d) uchováme jako soukromý klíč a prvočísel p, q společně s hodnotou $\varphi(n)$ se bezpečně zbavíme.
Postup šifrování:

(i) od příjemce naší zprávy si necháme poslat veřejný klíč (n, e)
(ii) zprávu reprezentovanou číslem $m < n$ zašifrujeme do $c = m^e \bmod n$
(iii) příjemce naši šifrovanou zprávu c rozšifruje pomocí soukromého klíče (n, d) stejným způsobem: $m = c^d \bmod n$

Tvrzení. *Pro m, e, d, n splňující požadavky RSA platí*

$$c^d = m^{ed} \equiv m \pmod{n}.$$

Na tomto tvrzení stojí funkčnost RSA. Její bezpečnost jsme však tímto neukázali.

Příklad. Kelišová chce poslat Cecilce nový drb podléhající vysokému utajení. Cecilka proto vygeneruje dvě „velká“ prvočísla 11 a 13, spočítá $n = 143$, $\varphi(n) = 120$ a vygeneruje $e = 13$. Eukleidovým algoritmem dostane

$$\begin{aligned} 120 &= 9 \cdot 13 + 3, \\ 13 &= 4 \cdot 3 + 1, \\ 3 &= 3 \cdot 1 + 0. \end{aligned}$$

Odtud $120 \perp 13$ a zná rozklad $1 = 13 - 4 \cdot 3 = 13 - 4 \cdot (120 - 9 \cdot 13) = 37 \cdot 13 - 4 \cdot 120$ neboli $d = 37$. Dvojici $(143, 13)$ pošle Kelišce jako veřejný klíč. Kelišová bude chtít, jak jinak, poslat šifrovanou zprávu 42, postupovat bude takto:

(i) z důvodu zjednodušení výpočtu rozepíše $13 = 2^3 + 2^2 + 2^0$
(ii) $42^{13} = ((42^2)^2)^2 \cdot (42^2)^2 \cdot 42$
(iii) $42 \bmod 143 = 42$
(iv) $42^2 \bmod 143 = 1764 \bmod 143 = 48$
(v) $(42^2)^2 \bmod 143 = 48^2 \bmod 143 = 2304 \bmod 143 = 16$
(vi) $((42^2)^2)^2 \bmod 143 = 16^2 \bmod 143 = 256 \bmod 143 = 113$
(vii) $42^{13} \bmod 143 = (113 \cdot 16 \cdot 42) \bmod 143 = 75936 \bmod 143 = 3$

Kelišová odešle zpět Cecilce zašifrovanou zprávu 3. Cecilka ji stejným způsobem dešifruje svým soukromým klíčem $d = 37$ a vyjde jí dychtivě očekávaná 42.

Jak RSA rozlousknout?

(i) faktorizace n, výpočet $\varphi(n)$, pomocí e pak dopočteme i d
(ii) využití chyby při šifrování (více exponentů k jednomu modulu apod.)
(iii) využití některé slabiny prvočíselné dvojice p, q – viz dále

Faktorizace malých n problém není, problém je ve složitosti algoritmu. Neznáme algoritmus se složitostí nižší než exponencielní (v závislosti na délce modulu), proto

nám stačí číslo n o několik cifer prodloužit a nepříteli bude trvat několikanásobně déle rozklad najít. To činí RSA tak bezpečnou.

Fermatova metoda

Tato metoda předpokládá malý rozdíl p a q, označíme $D := \frac{p-q}{2}$. Všimneme si, že

$$n = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2,$$

odtud $n + D^2 = \left(\frac{p+q}{2}\right)^2$. Zkoušíme tedy pro malá D, jestli číslo $n + D^2$ je čtverec. Jakmile takové D najdeme, dopočteme snadno p a q ze soustavy rovnic jako

$$p, q = \sqrt{n + D^2} \pm D.$$

Pollardova $p - 1$ metoda

Pollardova $p - 1$ metoda předpokládá, že alespoň pro jeden faktor n (ozn. p) má číslo $p - 1$ všechny své faktory relativně malé (omezené nějakým b). Nyní můžeme odhadnout[10] například $k = b!$ jako násobek $p - 1$, neboli $p - 1 \mid k$. Dle Fermatovy věty pro dané a nesoudělné s p (což není vůbec problém, např. $a = 2$) platí

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

Protože $p - 1 \mid k$, můžeme tuto kongruenci umocnit do tvaru

$$a^k \equiv 1 \pmod{p}.$$

Odtud $p \mid \mathrm{NSD}(a^k - 1, n)$, neboli můžeme předpokládat, že $p = \mathrm{NSD}(a^k - 1, n)$. Pokud vyjde 1, náš odhad k nebyl násobkem $p - 1$ ani $q - 1$, pokud vyjde n, odhad k byl násobkem obou. Tímto se dále řídíme a zlepšujeme odhad k. Pro silná p, q je toto hádání velmi obtížné, protože dokud nenatipujeme všechny faktory $p - 1$ (BÚNO), dostáváme jako NSD 1 a o $p - 1$ nadále nic nevíme. A pokud ano, je dost pravděpodobné, že máme i všechny faktory $q - 1$ a dostaneme jako NSD n.

Cvičení. (Za čokoládu) „Kapříci připluli!“ ozvalo se z telefonu. Spolu s tím i dvě čísla, 6901 a 725. Z druhé strany zaznělo 42. Otázkou pro vás je, kolik „kapříků“ letos vylovíme?

Literatura a zdroje

[1] Z. Masáková, *Diskrétní matematika I*, FJFI ČVUT, Praha, 2010.
[2] Wang Baocang, Liu Shuanggen, Hu Yupu, *New weak keys in RSA*, WUJNS, Wuhan, 2006.
[3] Ľ. Balková, *RSA (Úvod do kryptologie)*, FJFI ČVUT, Praha, 2011.

[10] Lze provést i jiný odhad čísla, které by mohlo být násobkem $p - 1$.

Soustavy rovnic

Vít „Vejtek“ Musil

Abstrakt. Příspěvek se věnuje vybraným partiím ze soustav nelineárních rovnic – cyklickým soustavám a soustavám se symetrickými polynomy. Některé příklady vyžadují užití nějaké známé nerovnosti. U vybraných úloh jsou uvedeny zdroje, kde lze nalézt řešení.

Během řešení mnoha problémů často narážíme na problém řešení rovnic a jejich soustav. Jde-li o soustavy rovnic lineárních, nalezení řešení nepředstavuje žádný problém, lze jej algoritmicky popsat, a tak tyto soustavy za nás může snadno a rychle louskat počítač. V obecném případě však máme smůlu, žádný magický univerzální algoritmus nemáme. Nad každým takovým případem se musíme zamyslet zvlášť, někdy se nám však může podařit vyřešit naráz celou škálu příkladů v jistém smyslu „podobných“.

Cyklické soustavy

Jedna ze zajímavých tříd takových soustav jsou soustavy cyklické. Vyznačují se tím, že jednotlivé rovnice se od sebe liší pouze cyklickou záměnnou proměnných.

Úmluva. Domluvíme se, že v celém textu, nebude-li řečeno jinak, všechny neznámé jsou z oboru reálných čísel.

Pozorování. *Buďte $x_1, x_2, \ldots x_n$ reálná čísla. Potom*

$$x_1^2 + x_2^2 + \cdots + x_n^2 = 0,$$

právě když $x_1 = x_2 = \cdots = x_n = 0$.

Toto banální pozorování se hodí nejen na cyklické soustavy. V případě cyklických většinou všechny rovnice sečteme a správně „učtvercujeme“. Podle tohoto návodu si každý snadno rozřeší následující úlohy.

Klíčová slova. soustavy rovnic, rovnice, symetrické polynomy

Příklad 1. Řešte cyklickou soustavu ve třech proměnných

$$x^2 + 1 = 2y.$$

Příklad 2. Řešte cyklickou soustavu ve třech proměnných

$$x^2 = yz.$$

Nyní přichází něco více obecného. Následující lemma se nám hodí pro některé cyklické soustavy, kde se v každé rovnici vyskytují pouze dvě neznámé.

Lemma. *Buďte $f, g\colon I \to \mathbb{R}$ funkce rostoucí na intervalu I. Potom pro řešení soustavy*

$$\begin{cases} f(x_1) = g(x_2) \\ f(x_2) = g(x_3) \\ \qquad \vdots \\ f(x_n) = g(x_1) \end{cases}$$

platí $x_1 = x_2 = \cdots = x_n$.

Z nastalé rovnosti již většinou snadno dopočítáme všechna řešení. Zkusme si to na následujících příkladech. U některých bude možná trošku obtížnější ukázat monotonii.

Příklad 3. Řešte cyklickou soustavu v proměnných a až z

$$a^5 = b + b^5. \qquad \text{(MKS-29-2-4)}$$

Příklad 4. Řešte cyklickou soustavu ve třech proměnných

$$x^3 = 2y^3 + y - 2.$$

Příklad 5. Řešte cyklickou soustavu ve třech proměnných

$$x = y^3 + y - 8.$$

Ne vždy však dostaneme soustavu nachystanou, jak bychom si přáli. Někdy je třeba provést drobné úpravy, nebo najít interval I, kde lze lemma aplikovat.

Příklad 6. Řešte cyklickou soustavu ve třech proměnných

$$x = \frac{4y^2}{1 + 4y^2}. \qquad \text{(MKS-27-1-7)}$$

Příklad 7. Řešte cyklickou soustavu ve třech proměnných

$$x + \frac{1}{x} = \frac{2}{y^2}.$$

Na některé soustavy je však toto lemma příliš krátké, zkusme třeba tento příklad:

Příklad 8. Řešte cyklickou soustavu ve třech proměnných

$$x + 2y = \sqrt{6z - 1}.$$

Zde se v každé rovnici vyskytují všechny tři proměnné, zachrání nás však lemma o trošku silnější.

Lemma. *Buďte $f, g, h\colon I \to \mathbb{R}$ funkce neklesající na intervalu I. Potom pro řešení soustavy*

$$\begin{cases} f(x) + g(y) = h(z) \\ f(y) + g(z) = h(x) \\ f(z) + g(x) = h(y) \end{cases}$$

platí $h(x) = h(y) = h(z)$. Je-li navíc h rostoucí, je $x = y = z$.

Příklad 9. Řešte cyklickou soustavu ve třech proměnných

$$x = y^3 + 1.$$

Příklad 10. Řešte cyklickou soustavu ve třech proměnných

$$x^5 = 5y^3 - 4z. \qquad \text{(Polská MO)}$$

Jak bylo předestřeno dříve, ani toto lemma není všemocné, na další úlohy musíme hledat trik jim šitý na míru.[11]

Příklad 11. Řešte cyklickou soustavu ve třech proměnných

$$x^2 = y + z + 2.$$

Příklad 12. Řešte cyklickou soustavu ve třech proměnných

$$(x + y)(y^3 - z^3) = 3(z - x)(z^3 + x^3).$$

(MR-6-J179)

Použití nerovností

Další třída rovnic se na první pohled nápadně liší od té předchozí. S použitím nějaké nerovnosti (nebo nerovností) buď ukážeme, že n musí být nějak omezené, nebo dokážeme, že rovnice platí, právě když nastává rovnost v nerovnosti. Pro tyto případy se tedy hodí nerovnosti znát a vědět, za jakých podmínek platí rovnost.

[11] A taky by bylo trochu divné, že by pro každou cyklickou soustavu platila rovnost všech neznámých.

Následující tři příklady řeště v kladných reálných číslech.

Příklad 13. Vyřešte soustavu

$$\begin{cases} x_1 + x_2 + \cdots + x_n = \dfrac{1}{4} \\ \dfrac{1}{x_1} + \dfrac{4}{x_2} + \cdots + \dfrac{n^2}{x_n} = n^2(n+1)^2 \end{cases}$$

Příklad 14. Vyřešte soustavu

$$\begin{cases} x_1 + x_2 + \cdots + x_n = 1 \\ \dfrac{1}{x_1} + \dfrac{1}{x_2} + \cdots + \dfrac{1}{x_n} + \dfrac{1}{x_1 x_2 \cdots x_n} = n^3 + 1 \end{cases}$$

(MR-6-J172)

Příklad 15. Vyřešte soustavu

$$\begin{cases} x_1 + x_2^2 + \cdots + x_n^n = n \\ x_1 + 2x_2 + \cdots + nx_n = \dfrac{1}{2}n(n+1) \end{cases}$$

Symetrické polynomy

Symetrické polynomy jsou speciální případy polynomů více proměnných. Věnovat se jim budeme právě kvůli jejich pěkným vlastnostem, které si záhy ukážeme. Není třeba se obávat, nejde o žádnou novinku, snad každý se s nimi setkal v takzvaných Viètových vztazích.

Definice. Polynom $P(x_1, \ldots, x_n)$ proměnných x_1 až x_n nazveme symetrickým, pokud pro každou bijekci $\pi\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$ platí

$$P(x_1, x_2, \ldots, x_n) = P(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}).$$

Definice vlastně neříká nic jiného než to, že polynom se nezmění, pokud libovolným způsobem přeznačíme proměnné. Mezi všemi symetrickými polynomy vynikají tzv. elementární polynomy.

Definice. Buď $1 \leq i \leq n$. Symetrický polynom proměnných x_1 až x_n

$$\sum_{1 \leq j_1 < j_2 < \cdots < j_i \leq n} x_{j_1} x_{j_2} \cdots x_{j_i}$$

nazveme i-tým elementárním symetrickým polynomem, označíme jej δ_{in}.

Definice možná působí děsivě, avšak jde jen o jinak zapsanou známou věc.

Tvrzení. (Viètovy vztahy) *Buďte x_1 až x_n kořeny polynomu $t^n + a_1 t^{n-1} + \cdots + a_{n-1}t + a_n$. Potom platí*

$$\begin{aligned} a_1 &= -\delta_{1n} \\ a_2 &= \delta_{2n} \\ a_3 &= -\delta_{3n} \\ &\vdots \\ a_n &= (-1)^n \delta_{nn}. \end{aligned}$$

Nyní můžeme vyslovit důležitou větu z algebry o symetrických polynomech.

Věta. *Každý symetrický polynom proměnných x_1 až x_n lze napsat jako polynom v proměnných δ_{1n} až δ_{nn}.*

Věta jinak řečeno tvrdí, že každý symetrický polynom lze v jistém smyslu napsat pomocí elementárních symetrických polynomů, a to tak, že je můžeme sčítat, násobit konstantou a násobit navzájem. Co věta neříká, je, jak to udělat, musíme se spokojit s tím, že to lze. Dost už ale teorie, pojďme si to vyzkoušet na příkladech.

Příklad 16. Řešte soustavu

$$\begin{cases} x + y + z = 0 \\ xy + yz + xz = 0 \end{cases}$$

(MKS-27-1-4)

Příklad 17. Najděte hodnotu $1/x + 1/y + 1/z$ za předpokladu, že

$$\begin{cases} x + y + z = 5 \\ x^2 + y^2 + z^2 = 15 \\ xy = z^2 \end{cases}$$

Příklad 18. Řešte soustavu

$$\begin{cases} xy + yz + xz = 4 \\ (xy)^2 + (yz)^2 + (xz)^2 = 6 \\ (xy)^3 + (yz)^3 + (xz)^3 = 10 \end{cases}$$

Literatura a zdroje

[MŘ] J. Herman, R. Kučera, J. Šimša, *Metody řešení matematických úloh I*, MU, Brno, 2001.
[ML] *Mathlinks*, *http://www.mathlinks.ro*
[MR] *Mathematical Reflections*, *http://awesomemath.org/mathematical-reflections*

Everze sféry

Miroslav Olšák

Abstrakt. Dostanete sféru (míč) z materiálu, který umí procházet sám sebou a chcete ji obrátit naruby. Zdá se vám to triviální? Zdá se vám, že to nejde? Ani jedno není správný odhad.

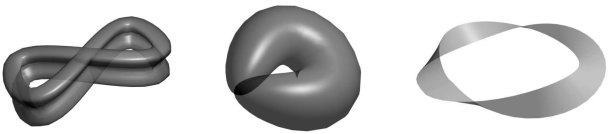
S objekty v našem světě se budeme seznamovat pěkně od nejjednoduššího po nejsložitější.

Materiál

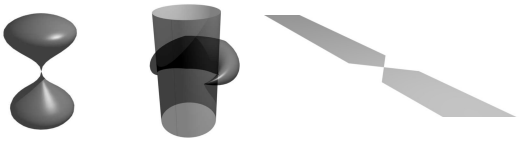
Naše objekty budou převážně z kouzelného materiálu, který:

(i) je dokonale placatý.
(ii) je dokonale pružný a natahovací.
(iii) umí procházet sám sebou.
(iv) nemůžeme neomezeně smrsknout.
(v) nemůžeme neomezeně ohnout.
(vi) nemůžeme dělit, trhat, dělat v něm díry atd.

Například z něho může být vyrobeno:

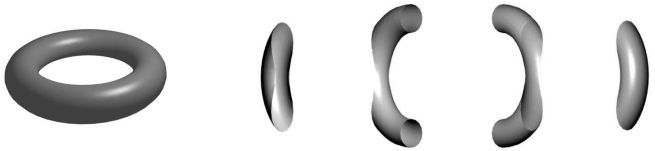


Ale již nikoliv:



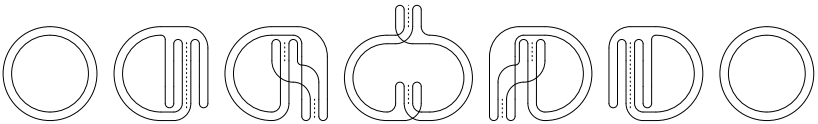
Klíčová slova. algebraická topologie, nepředstavitelnost, sféra, torus, naruby

Torus



Někomu připomíná pneumatiku, někomu koblihu, vznikne tak, že spojíme levou stranu obdélníka s pravou a horní s dolní.

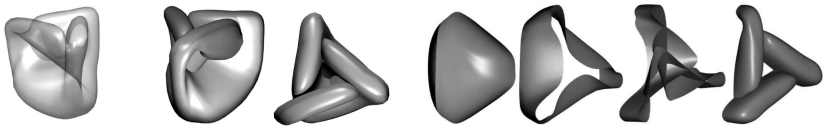
Torus je možné jednoduše evertovat (převrátit naruby).



Kleinova láhev

Vcelku jednoduchý objekt, vznikne podobně jako torus s tím rozdílem, že vzniklý válec slepíme zevnitř. Tato plocha je (stejně jako Möbiova páska) neorientovatelná. A že prochází sama sebou? Na to si zvyknete.

Boyova plocha



Tři kopečky nahoře, jeden dole. Reprezentuje reálnou projektivní rovinu. To znamená, že Boyovu plochu dostanete, pokud slepíte kruh tak, že spojíte každý hraniční bod s protějším.

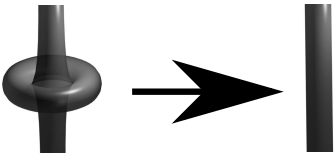
Sféra (povrch koule)

Nevinně vyhlížející plocha: neprochází sama sebou, všechny křivky na ní jdou stáhnout do bodu, je orientovatelná – a v tom je ta potíž.

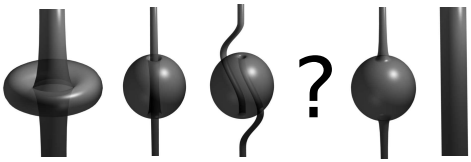
V roce 1958 přišel Stephen Smale s důkazem, že je možné obrátit sféru naruby. Everze podle jeho důkazu ale byla prakticky nezobrazitelná, tedy vědělo se, že to jde, ale již ne jak. Nyní jsou známy postupy, jak everzi provést, ale než se do nich pustíme, podíváme se, proč je převrácení sféry tak složité na představu:

Věta 1. *V rovině není možné převrátit kružnici naruby.*

Odstranění smyčky z válce

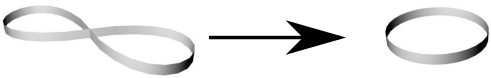


Tento problém je ekvivalentní obrácení sféry naruby. Pokud umíme odstranit smyčku z válce, je everze sféry triviální. Obráceně to provedeme tak, že smyčku nafoukneme, čímž vyrobíme sféru, do které vedou zevnitř dvě hadičky. Po převrácení sféry povedou hadičky do sféry zvenčí, takže získáme válec bez smyčky.



Vezmeme si před odstraněním smyčky a po odstranění smyčky jen levý proužek válce. Líbilo by se nám, kdybychom tyto proužky mohli převést na sebe, ale ...

Věta 2. *Není možné rozmotat osmičku na nepřekroucený proužek.*



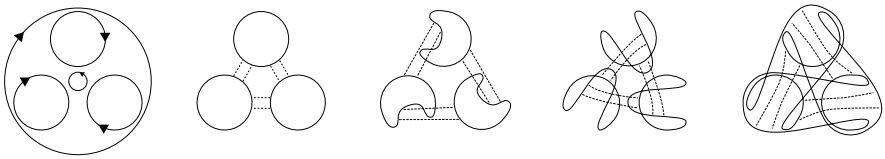
Samozřejmě tato věta možnost everze nevyvrací, jen tvrdí, že se nám při odstraňování smyčky válec překroutí.

A pak je ještě jeden důvod, proč je everze sféry nepředstavitelná.

Věta 3. *V každé everzi sféry existuje okamžik, kdy prochází čtyři roviny jedním bodem.*

Everze přes Boyovu plochu

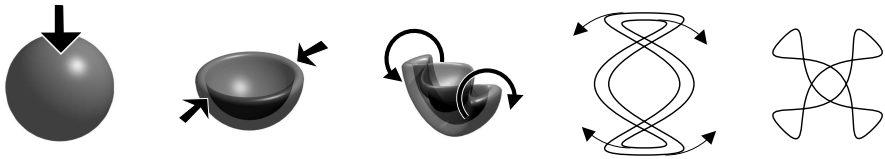
Namotáme sféru dvakrát na Boyovu plochu. Začneme tedy tak, že si nahoře vyrobíme tři kopečky. A pak s tím začneme kroutit:



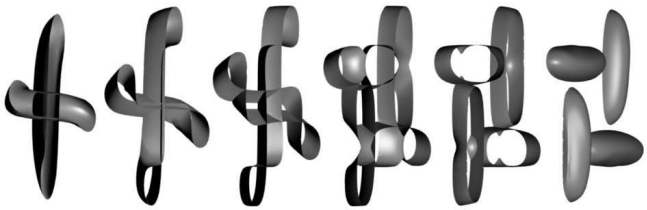
Čárkovaná čára značí sedla mezi jednotlivými kopečky.
Když to šlo tam, musí to jít i zpátky, rozmotáme a máme sféru naruby.

Everze přes Morinovu plochu

Začneme tak, že jižní pól protlačíme dolů (zatím ne skrz sféru), takže dostaneme něco jako povrch misky. Vzápětí tuto misku nahoře protlačíme samu sebou. A teď s tím začneme kroutit.



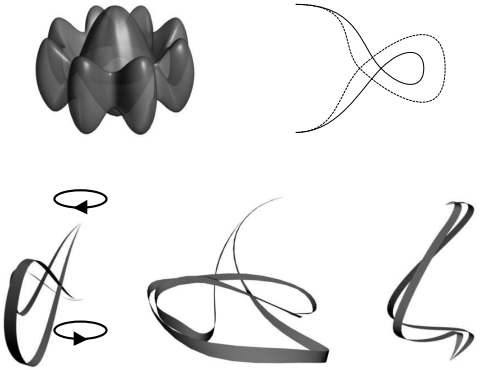
Když uši otočíme o 90° a spodní části na sebe budou kolmé, získáváme Morinovu plochu.



Nyní stačí otočit o 90° a aplikovat zpětný postup.

Everze Thurstonovým zvlněním

Sféru si poledníky rozdělíme na několik (například 8) proužků a každý z nich převrátíme zvlášť. Protlačíme sebou severní a jižní pól. Dále sféru uchopíme v několika polednících a každý druhý poledník zvětšíme.



Když už jsme s oběma póly otočili o 180°, stačí protlačit středem sféry ještě prostřední části proužků a everze je dokončena.

Odkazy a zdroje

[1] Video *Outside In* (Thurstonovo zvlnění),
http://video.google.com/videoplay?docid=-6626464599825291409#
[2] Software zobrazující *The Optiverse*, podobné Morinově everzi,
http://new.math.uiuc.edu/optiverse/
[3] Software zobrazující Thurstonovo zvlnění,
http://www.dgp.utoronto.ca/~mjmcguff/eversion/
[4] *A History of Sphere Eversions*,
http://torus.math.uiuc.edu/jms/Papers/isama/color/opt1.htm
[6] *Wikipedia: Smale's paradox*, *http://en.wikipedia.org/wiki/Smale's_paradox*

Kombinatorická geometrie

Miroslav Olšák

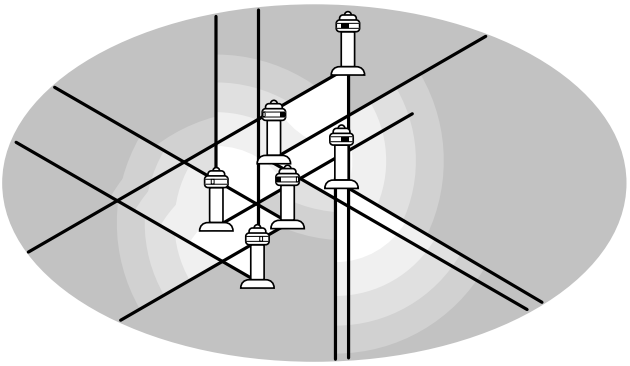
Abstrakt. Postupy v řešení geometrických a kombinatorických úloh se značně liší. Přesto u některých úloh není jasné, z kterého směru je uchopit, což může vést k mylnému pocitu, že nejdou uchopit vůbec. Někdy je možné převést úlohu na čistě geometrickou či čistě kombinatorickou (například grafovou). Jindy se třeba dá nalézt chytrá geometrická neměnka.

Příklad 1. Uvnitř $2n$-úhelníku se nachází liška. Ze všech vrcholů najednou po této lišce vystřelíme. Žádná střela nezasáhla vrchol. Dokažte, že některá hrana musela být zasažena dvakrát.

Příklad 2. Rozřezali jsme obdélník na menší obdélníky a shledáváme, že každý má alespoň jednu stranu celočíselnou. Dokažte, že i původní obdélník měl jednu stranu celočíselnou.

Příklad 3. Je dán bod A a několik mnohoúhelníků v rovině takových, že každé dva mají neprázdný průnik. Dokažte, že existuje kružnice se středem v A, která protíná všechny tyto mnohoúhelníky nebo se jich alespoň dotýká. (PraSe 2008/2009)

Příklad 4. V zátoce je postaveno 18 majáků, každý dokáže osvítit úhel 20°. Dokažte, že umíme natočit majáky tak, aby byla světly majáků pokryta celá zátoka.



Klíčová slova. Kombinatorická geometrie

Příklad 5. Kruhový terč o poloměru 12cm zasáhlo 19 střel. Dokažte, že vzdálenost dvou zásahů je menší než 7cm. (MO 2009/2010)

Příklad 6. V rovině je dáno několik bodů tak, že neleží všechny na jedné přímce. Dokažte, že je možné najít přímku, na které leží právě dva tyto body.

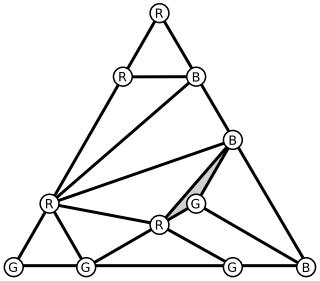
Příklad 7. V rovině jsou dány body P, A_1, A_2, ... , A_{2010} v obecné poloze. Dokažte, že počet všech trojúhelníků $A_iA_jA_k$, uvnitř kterých leží bod P, je sudý.

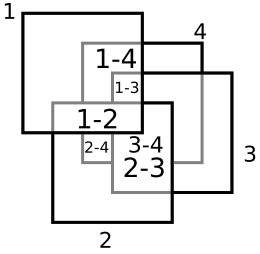
Příklad 8. Máme v rovině 100 bodů v obecné poloze. Dokažte, že mezi všemi trojúhelníky tvořenými těmito body není více než 70% ostroúhlých. (IMO 1970)

Příklad 9. Je dán mnohoúhelník o obsahu n. Dokažte, že je možné jej vložit do roviny tak, aby pokrýval (hranice se počítá) alespoň $n + 1$ mřížových bodů.

Příklad 10. Máme daných 60 bodů v jednotkovém kruhu. Dokažte, že je možné zvolit na okraji tohoto kruhu bod (nemusí být jedním ze zadaných), jehož součet vzdáleností od zadaných bodů nepřevyšuje 80. (ČPS 2009/2010)

Příklad 11. Kolik nejvýše je možné umístit čtverců 1×1 do prostoru tak, aby měly navzájem rovnoběžné strany a každé dva se viděly? Říkáme, že dva čtverce se vidí, pokud existuje úsečka spojující tyto dva čtverce, která je kolmá na jejich roviny a přitom vede mimo všechny ostatní čtverce. A co kdyby to byly kruhy?





Příklad 12. Nakreslíme do roviny trojúhelník RGB. Rozdělíme jej na několik menších trojúhelníčků tak, aby žádný trojúhelníček neměl vrchol uvnitř strany jiného trojúhelníčku. Nyní obarvíme vrcholy trojúhelníčků červeně, zeleně a modře tak, aby vrcholy velkého trojúhelníku dostaly příslušné barvy. Dále vrcholy na stranách musí dostat barvu jednoho z přilehlých vrcholů velkého trojúhelníka. Dokažte, že má pak jeden z malých trojúhelníčků všechny vrcholy různě barevné.

(Spernerovo lemma)

Příklad 13. Půdorys galerie má tvar n-úhelníku. Kolik strážníků v závislosti na n (opravdu to závisí ;)) potřebujeme, abychom je mohli rozestavit tak, aby dohromady viděli na (hlídali) celou galerii? Strážník na rozdíl od majáku vidí všemi směry.

(Art gallery problem)

Příklad 14. Dokažte, že z lichého počtu trojúhelníku stejného obsahu neposkládáme čtverec. (Monskyho věta)

Celá čísla p-naruby

Jakub „šnEk“ Opršal

Abstrakt. Příspěvek obsahuje základy teorie p-adických čísel, ukazuje jeden z intuitivnějších a méně formálních způsobů zavedení. Obsahuje také mnohá cvičení na osvětlení struktury p-adických celých čísel.

Prvočísla vždy hrála velkou roli v teorii čísel, už jen z toho důvodu, že když počítáme modulo prvočíslo, můžeme všemi nenulovými zbytky dělit. Na vlastnostech prvočísel také velmi stojí koncept p-adické valuace, která počítá nejvyšší mocninu prvočísla p, která dělí dané číslo. Tato myšlenka sama o sobě umí řešit mnohé diofantické rovnice.

p-adická čísla jen posouvají valuaci dále, definují pomocí ní normu a tak převádějí otázky (jako dělitelnost) dříve řešené jen algebraickou teorií čísel do analýzy a diferenciálního počtu. Dnes jsou p-adická čísla prakticky základem moderní teorie čísel, používají se například pro zlomení některých šifrovacích algoritmů postavených na eliptických křivkách či k aproximaci Riemannovy zeta funkce.

p-adická valuace a norma

Nechť p je prvočíslo. Definujeme *p-adickou valuaci* $v_p(n)$ nenulového celého čísla n jako nejvyšší exponent x takový, že $p^x \mid n$. Definujeme navíc $v_p(0) = \infty$. Ekvivalentně je-li $n = p^\alpha q$, kde $p \nmid q$, pak $v_p(n) = \alpha$.

p-adickou valuaci můžeme rozšířit i na racionální čísla, je-li $q = a/b$ zlomek (v základním tvaru), pak $v_p(q) = v_p(a) - v_p(b)$.

Cvičení. Ukažte, že v definici p-adické valuace na racionálních číslech nezáleží na tom, jestli je zlomek a/b v základním tvaru.

Tvrzení. *p-adická valuace na $\mathbb{Q}$ je zobrazení $v_p\colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ a splňuje pro všechna racionální čísla a a b*

(i) $v_p(a) = \infty$, *právě když* $a = 0$,
(ii) $v_p(ab) = v_p(a) + v_p(b)$,
(iii) $v_p(a + b) \geq \min\{v_p(a), v_p(b)\}$.

Klíčová slova. p-adická čísla, valuace, celá čísla, dělitelnost, teorie čísel

Přitom v poslední situaci může ostrá nerovnost nastat pouze pro $v_p(a) = v_p(b)$.

Cvičení. Buď p prvočíslo a n přirozené. Ukažte, že platí

$$v_p\big((p^n)!\big) = 1 + p + p^2 + \cdots + p^{n-1}.$$

Cvičení. Nechť $S(n)$ značí ciferný součet čísla n v soustavě o základu p. Dokažte, že

$$v_p(n!) = \frac{n - S(n)}{p - 1}.$$

Z p-adické valuace je odvozena tzv. *p-adická norma* racionálního čísla q jako

$$|q|_p = \frac{1}{p^{v_p(q)}},$$

speciálně $|0|_p = 0$.

Tvrzení. *p-adická norma $|\cdot|_p \colon \mathbb{Q} \to \mathbb{R}_0^+$ je zobrazení splňující*

(i) $|q|_p \geq 0$ *a přitom* $|q|_p = 0$, *právě když* $q = 0$,
(ii) $|ab|_p = |a|_p \cdot |b|_p$,
(iii) $|a + b|_p \leq \max\{|a|_p, |b|_p\}$.

Metrika na množině (prostoru) X je binární zobrazení $\rho : X^2 \to \mathbb{R}_0^+$, které dvěma bodům přiřadí jejich vzdálenost. Po metrice chceme, aby měla nějaké docela intuitivní vlastnosti, například aby splňovala trojúhelníkovou nerovnost. Nás přesná definice moc zajímat nebude, stačit bude představa, že metrika nám dovoluje měřit vzdálenosti.

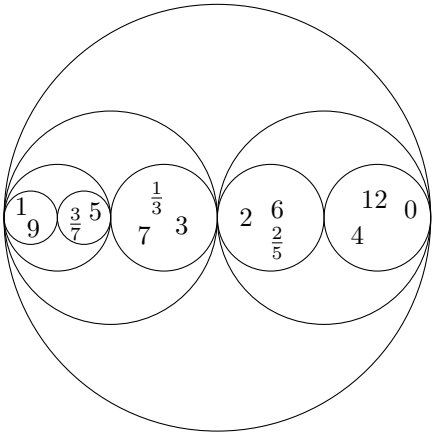
Z p-adické valuace můžeme definovat p-adickou metriku následovně

$$\rho_p(x, y) = |x - y|_p.$$

Tvrzení. *V p-adické metrice je každý trojúhelník rovnoramenný a každý kruh má střed v libovolném vnitřním bodě.*

Následující obrázek ukazuje topologii 2-adických čísel. Největší kružnice vyjadřuje kružnici s poloměrem 1, dvě menší pak mají každá poloměr $1/2$, ty ještě menší mají poloměr $1/4$ a nejmenší kružnice má poloměr $1/8$. Všechna celá čísla leží v tomto největším kruhu, spolu s některými racionálními čísly. Ostatní racionální čísla, jako

například $1/2$, $1/6$, $1/100$, leží vně tohoto největšího kruhu.



Cvičení. Buď x racionální číslo. Ukažte, že x je celé, právě když pro všechna prvočísla p platí $|x|_p \leq 1$.

Ještě se na chvíli zamyslíme, co znamená, že dvě čísla jsou od sebe vzdálena $1/p^n$ v p-adické metrice. Nechť a a b jsou dvě taková čísla, pak

$$|a-b|_p = \frac{1}{p^n} \quad \longleftrightarrow \quad v_p(a-b) = n.$$

Tedy existuje q nesoudělné s p, že $a - b = p^n q$. Stejnou úvahou můžeme odvodit, že

$$|a-b|_p \leq \frac{1}{p^n} \quad \longleftrightarrow \quad a \equiv b \pmod{p^n}.$$

Zápis racionálních čísel v p-adické soustavě a p-adická čísla

Zopakujeme si nejdříve, co znamená zápis celého čísla k v soustavě o základu p. Je to zápis ve tvaru

$$(k)_p = (a_n \cdots a_1 a_0)_p,$$

kde a_0, a_1, … , a_n jsou cifry, tj. celá čísla od 0 do $p-1$, který vyjadřuje rovnost

$$k = a_n p^n + \cdots + a_1 p + a_0.$$

Podobně chápeme i zápis s desetinnou[12] čárkou

$$(a_n \cdots a_0, a_{-1} a_{-2} \cdots a_{-m})_p = a_n p^n + \cdots + a_0 + a_{-1}\frac{1}{p} + a_{-2}\frac{1}{p^2} + \cdots + a_{-m}\frac{1}{p^m}.$$

[12]Pojmenování „desetinná čárka“ je dost zavádějící, když je to vlastně p-tinná čárka.

Normálně je zvykem racionální čísla zapisovat s nekonečným zápisem doprava, za desetinnou čárku. V p-adických číslech je tomu však naopak, tedy zajímají nás čísla s nekonečným zápisem doleva. Důvod k tomu je ten, že $1/p^\alpha$ mají čím dál větší p-adickou absolutní hodnotu, tedy například součet $1+1/p+1/p^2+\dots$ nedává smysl, protože když sčítáme postupně, tak každým dalším číslem uděláme větší a větší skok. Je to podobná situace jako kdybychom chtěli sečíst $1+p+p^2+\dots$ v reálných číslech. Na druhou stranu tento druhý součet má velmi dobrý smysl v p-adických číslech.

Množinu všech *p-adických čísel* definujeme následovně: p-adická čísla jsou množinou všech řad tvaru

$$a_{-m}p^{-m} + a_{-m+1}p^{-m+1} + \cdots + a_0 + a_1 p + \cdots,$$

kde $a_i = 0, 1, \dots, p-1$. Tedy všech čísel, která mají v p-kové soustavě nekonečný (nebo i konečný) zápis

$$\dots a_2 a_1 a_0, a_{-1} \dots a_{-m}.$$

Všimni si, že p-adická čísla nemají, na rozdíl od reálných čísel, znaménko. To proto, že ho prostě nepotřebujeme, „záporná čísla“ umíme vyjádřit i bez něj.

Cvičení. Spočtěte $1 + 2 + 2^2 + \dots$ a $1 - 2 + 2^2 - 2^3 + \dots$ v $\mathbb{Q}_2$.

Cvičení. Máme-li dané p-adické číslo a s rozvojem

$$\dots a_1 a_0, a_{-1} \dots a_{-m},$$

jak vypadá p-adický rozvoj čísla $-a$?

Cvičení. Vyjádřete rozvoj $1/5$ v 2-adických číslech.

Cvičení. Spočtěte rozvoj $1/3!$ v $\mathbb{Q}_3$.

Můžeme velmi snadno definovat p-adickou valuaci na p-adických číslech. Důležité je, že p z indexu valuace se shoduje s prvočíslem p v p-adické soustavě. Definujeme

$$v_p(\dots a_1 a_0, a_{-1} \dots a_{-m}) = -m,$$

pro a_{-m} nenulové, tedy $v_p(a)$ udává, na které pozici je poslední nenulová cifra čísla a. Všimni si, že toto rozšiřuje p-adickou valuaci definovanou na celých číslech. Z toho už snadno rozšíříme i p-adickou normu – zadefinujeme ji stejně, jako v racionálních číslech, tj. $|a|_p = p^{-v_p(a)}$.

Můžeme také psát

$$a \equiv b \pmod{p^k}$$

pro $a, b \in \mathbb{Q}_p$ a $k \in \mathbb{N}$, což znamená, že $|a-b|_p \leq 1/p^k$. Jinými slovy že zápisy a a b se shodují zprava až do cifry na místě p^k.

Celým p-adickým číslem rozumíme každé takové číslo z, že z nemá žádné cifry za desetinnou čárkou. Jinými slovy jsou to právě taková p-adická čísla z, že $|z|_p \leq 1$.

Například každé celé číslo je p-adické celé a racionální čísla a/b taková, že $p \nmid b$ jsou p-adická celá. Kromě těchto čísel i všechna s nekonečným neperiodickým zápisem.

Cvičení. Ukažte, že je-li p prvočíslo a q libovolné celé číslo takové, že $p \nmid q$, pak $1/q \in Z_p$, a ukažte, jak lze nalézt p-adický rozvoj takových čísel.

Cvičení. Ukažte, že pro libovolné číslo $a \in \mathbb{Q}_p$, $|a|_p = 1$, existuje $b \in \mathbb{Z}_p$, že platí $ba = 1$, neboli pro taková a platí $1/a \in \mathbb{Z}_p$. Jaká je pak p-adická norma čísla $1/a$?

Cvičení. Spočtěte $\sqrt{-3}$ a $\sqrt{2}$ v $\mathbb{Q}_7$ s přesností na 4 cifry. Existuje v $\mathbb{Q}_7$ odmocnina z 3?

Cvičení. Nalezněte rozvoj $\sqrt{7}$ v $\mathbb{Q}_2$ s přesností na 5 cifer.

Cvičení. Jak poznáme, že v $\mathbb{Q}_p$ existuje odmocnina z n, kde $p \nmid n$?

Věta. (Henzelovo lemma) *Nechť $F(x) = c_0 + c_1x + \cdots + c_nx^n$ je polynom, jehož koeficienty jsou p-adická celá čísla, a buď $F'(x) = c_1 + 2c_2x + 3c_3x^2 + \cdots + nc_nx^{n-1}$. Je-li $a_0 \in \mathbb{Z}_p$ takové, že $F(a_0) \equiv 0 \pmod p$ a $F'(a_0) \not\equiv 0 \pmod p$, pak existuje jednoznačné p-adické číslo a takové, že*

$$F(a) = 0 \quad \text{a} \quad a \equiv a_0 \pmod p.$$

Drsná teorie čísel

Nearchimédovskou normou na $\mathbb{Q}$ myslíme zobrazení $||\cdot||\colon \mathbb{Q} \to \mathbb{R}$ takové, které splňuje

(i) $||a|| \geq 0$ a $||a|| = 0$, právě když $a = 0$,
(ii) $||ab|| = ||a|| \cdot ||b||$,
(iii) $||a + b|| \leq \max\{||a||, ||b||\}$.

Příkladem takových norem jsou všechny p-adické normy. To, že žádné jiné příklady fakticky neexistují, nám říká Ostrovského věta.

Věta. (Ostrovski) *Pro každou nearchimédovskou normu $||\cdot||\colon \mathbb{Q} \to \mathbb{R}_0^+$ existuje prvočíslo p a reálné číslo α, že platí*

$$||q|| = |q|_p^\alpha$$

pro každé racionální $\mathbb{Q}$.

V teorii kolem valuací a norem je docela důležité následující tvrzení, které nám jinými slovy také říká, že jsme na žádnou normu nezapomněli a že se kruh do sebe uzavírá. Toto tvrzení si můžeš zkusit dokázat, je to docela jednoduché.

Věta. (Součinová formule) *Pro každé racionální číslo q platí*

$$|q| \cdot \prod\nolimits_p |q|_p = 1,$$

kde $\prod_p$ značí součin přes všechna prvočísla p.

Literatura

[K] Neal Koblitz, *p-adic Numbers, p-adic analysis, and Zeta-Functions*, Springer-Verlag, New York, 1984.

[KHŠ] R. Kučera, J. Herman, J. Šimša, *Metody řešení matematických úloh I.*, Masarykova Univerzita, Brno, 2002.

Hmotné body

Tomáš „Šavlík“ Pavlík

Abstrakt. Přednáška pojednává o specifické metodě v geometrii, která je odvozená z jednoduchých fyzikálních vlastností.

Definice. *Hmotným bodem* rozumíme dvojici (A, m), kde A je bod a $m \in \mathbb{R}$ je jeho hmotnost.

Základní axiomy

(i) Existence těžiště: Každá hmotná soustava má právě jedno těžiště.
(ii) Zákon páky: Těžiště T bodů A, B s hmotnostmi a, b leží na přímce AB a platí $|AT| \cdot a = |TB| \cdot b$.
(iii) Redukční princip: Těžiště soustavy se nezmění, pokud zaměníme libovolnou podsoustavu s jedním hmotným bodem splývajícím s těžištěm této podsoustavy a majícím stejnou celkovou hmotnost.

Příklad 1. Dokažte, že se těžnice protínají v jednom bodě. Dokažte, že se protínají v poměru $1 : 2$.

Příklad 2. Najděte váhy vrcholů trojúhelníka tak, aby jeho těžištěm bylo
(i) ortocentrum,
(ii) střed kružnice vepsané,
(iii) střed kružnice opsané.

Příklad 3. Dokažte, že se v trojúhelníku spojnice vrcholů s body dotyku kružnice a) vepsané b) připsané s protilehlou stranou protínají v jednom bodě.

Příklad 4.
(i) Najděte těžiště hmotné destičky ve tvaru trojúhelníka.
(ii) Najděte těžiště hmotného drátku, který tvoří obvod trojúhelníka.

Příklad 5. Nechť $ABCD$ je konvexní čtyřúhelník a středy úseček AB, BC, CD, DA, AC, BD pojmenujme postupně E, F, G, H, I, J. Dokažte, že se přímky EG, FH a IJ protínají v jednom bodě.

Klíčová slova. goemetrie, planimetrie, hmotné body, barycentrická soustava souřadnic

Úmluva. Budeme používat standardní značení: ABC je trojúhelník, $D \in BC$, $E \in AC$, $F \in AB$.

Příklad 6. Bod F je střed strany AB, P je střed úsečky CF a zároveň $P \in AD$. Spočítejte $\frac{|BD|}{|DF|}$.

Příklad 7. $\frac{|AF|}{|FB|} = 2:1$, $\frac{|BD|}{|DC|} = 3:1$, $P = AD \cap CF$, spočítejte $\frac{|CP|}{|PF|}$.

Příklad 8. Bod D leží na ose vnitřního úhlu u vrcholu A, bod E je střed strany AC, $P = AD \cap BE$. Dále víme, že $|AB| = 6$, $|BC| = 7$, $|CA| = 8$, spočítejte $\frac{|AP|}{|PD|}$.

Příklad 9. Nechť se AD, BE, CF protínají v bodě P. Víme, že $\frac{|AP|}{|PD|} = 1$ a $\frac{|BP|}{|PE|} = 2$. Určete $\frac{|CP|}{|PF|}$. (Náboj 2011)

Příklad 10. Je dán trojúhelník ABC. Dokažte, že střední příčka rovnoběžná s AC, osa vnitřního úhlu u vrcholu C a spojnice bodů dotyku kružnice vepsané se stranami AB a AC prochází jedním bodem.

Příklad 11. (Van Aubelova věta) Mějme trojúhelník ABC a v něm ceviány AD, BE a CF, které se protínají v bodě P. Dokažte, že

$$\frac{|AP|}{|PD|} = \frac{|EA|}{|CE|} + \frac{|AF|}{|FB|}$$

Příklad 12. Nechť $\frac{|BD|}{|DC|} = 3:1$, $\frac{|CE|}{|EA|} = 2:1$ a P je střed úsečky ED. Určete $\frac{|CP|}{|PF|}$.

Příklad 13. Máme dáno $\frac{|AF|}{|FB|} = 3:2$ a $\frac{|BE|}{|EC|} = 3:2$. Nechť se polopřímky AC a FE protnou v bodě P. Zjistěte poměr $\frac{|FE|}{|EP|}$.

Příklad 14. Dokažte, že každá přímka, která dělí obsah i obvod trojúhelníka ve stejném poměru, prochází středem kružnice vepsané.

Příklad 15. $ABCD$ je konvexní čtyřúhelník, E, F jsou postupně středy stran AB, CD.

(i) Dokažte, že AC dělí usečky BD a EF ve stejném poměru.
(ii) Dokažte, že EF dělí úsečky AC a BD ve stejném poměru.

Příklad 16. Nechť $\frac{|AF|}{|FB|} = 3:7$, $\frac{|BD|}{|DC|} = 2:5$, $\frac{|CE|}{|EA|} = 3:4$ a $P = ED \cap CF$. Určete $\frac{|CP|}{|PF|}$.

Příklad 17. $ABCD$ je konvexní čtyřúhelník. Na stranách AB, BC, CD, DA leží postupně body E, F, G, H tak, aby

$$\frac{|AE|}{|EB|} = \frac{|CF|}{|FB|} = \frac{|CG|}{|GD|} = \frac{|AH|}{|HD|}$$

Dokažte, že $EFGH$ je rovnoběžník.

Příklad 18. Dokažte Cevovu a Menelaovu větu pomocí hmotných bodů.

Příklad 19. Mějme trojúhelník, kde $\frac{|AF|}{|FB|} = 2 : 1$, $\frac{|BD|}{|DC|} = 2 : 1$, $\frac{|CE|}{|EA|} = 2 : 1$. Spočítejte obsah trojúhelníku, tvořeného přímkami AD, BE, CF když víte, že obsah ABC je 1. (pro borce: určete obsah, když jsou poměry obecné)

Příklad 20. Nechť se AD, BE, CF protínají v bodě P. Zjistěte vztah mezi poměry $\frac{|DP|}{|AD|}$, $\frac{|EP|}{|BE|}$ a $\frac{|FP|}{|CF|}$.

Příklad 21. Je dán trojúhelník ABC, středem jeho kružnice vepsané vedeme přímku, která protne přímky AB, AC, BC postupně v M, N, O. Dokažte vztah

$$\frac{a}{|BO| \cdot |OC|} + \frac{b}{|CN| \cdot |NA|} + \frac{c}{|AM| \cdot |MB|} = \frac{(a+b+c)^2}{a \cdot b \cdot c}.$$

(BRKOS XVII 1.6)

Literatura a zdroje

[1] Jaromír Šimša, *Archimédova statika v geometrii*.
[2] Paul Yiu, *Introduction ot the Geometry of the Triangle*.
[3] Tom Rike, *Mass Point Geometry*.

Algebraické legrácky

Michal „Kenny“ Rolínek

Abstrakt. Sbírka příkladů, jež lze řešit vtipnou algebraickou manipulací.

Každý z následujících příkladů má řešení založené na nějaké vtipné a trikové úpravě. Přijdete na ně?

Příklad 1. Označme $m \circ n = \frac{mn+4}{m+n}$. Určete

$$((((2011 \circ 2010) \circ 2009) \circ \cdots \circ 2) \circ 1) \circ 0.$$

(Náboj 2009)

Příklad 2. Součin reálných čísel x, y, z je 1. Určete všechny možné hodnoty výrazu

$$\frac{1}{1+x+xy} + \frac{1}{1+y+yz} + \frac{1}{1+z+zx}.$$

Příklad 3. Nalezněte všechna prvočísla tvaru $n^4 + 4m^4$, kde $m, n \in \mathbb{N}$.

Příklad 4. Najděte všechna reálná x splňující

$$(x^2+3x+2)(x^2-2x-1)(x^2-7x+12)+24 = 0.$$

Příklad 5. Pro nenulová reálná čísla a, b, c platí

$$a^2 - b^2 = bc, \qquad b^2 - c^2 = ca.$$

Ukažte, že pak platí i $a^2 - c^2 = ab$.

Příklad 6. Nechť existuje $n > 0$ reálných čísel $x_1, x_2, \ldots, x_n$, která pro každé $i = 1, \ldots, n$ splňují

$$x_i = \frac{1}{x_i - x_1} + \frac{1}{x_i - x_2} + \cdots + \frac{1}{x_i - x_{i-1}} + \frac{1}{x_i - x_{i+1}} + \cdots + \frac{1}{x_i - x_n}.$$

Navíc platí $x_1^2 + x_2^2 + \cdots + x_n^2 = 45$. Určete n. (PraSe 27/1/8)

Klíčová slova. úprava výrazu, triky, algebra

Příklad 7. Jsou dána reálná čísla x, y, z, která splňují

$$x + y + z = 12, \qquad x^2 + y^2 + z^2 = 54.$$

(i) Ukažte, že výrazy xy, yz, zx jsou nejvýše rovny 25 a alespoň rovny 9.
(ii) Ukažte, že alespoň jedno z čísel x, y, z je nejvýše rovno 3 a alespoň jedno je větší nebo rovno 5. (Celostátní kolo MO 2011)

Příklad 8. Buďte a, b, c nezáporná reálná čísla taková, že

$$(a + b)(b + c)(c + a) = 2.$$

Dokažte, že

$$(a^2 + bc)(b^2 + ca)(c^2 + ab) \leq 1.$$

(Vasile Cirtoaje)

Příklad 9. Nechť a, b, c, d, e, f jsou přirozená čísla. Označme $S = a+b+c+d+e+f$. Platí, že S dělí výrazy $abc + def$ a $ab + bc + ca - de - ef - fd$. Dokažte, že S je složené. (IMO shortlist 2005)

Literatura a zdroje

[1] Vo Quoc Ba Can, Cirtoaje Vasile, Phuong Tran, *Inequalities with beautiful solutions*, GIL, 2010.

Nerovnosti

Petr Ryšavý

Abstrakt. Příspěvek seznamuje s dvojicí nejjednodušších postupů při důkazech nerovností, a to úpravou na čtverec a AG nerovností. Kromě toho se na příkladech zastavíme u několika nejobvyklejších triků, které se mohou hodit.

Důkazy nerovností jsou jedním z oblíbených témat nejen v PraSátku, ale třeba i v Matematické olympiádě. Pokud se pokoušíme nějakou nerovnost dokázat, musíme si nejprve ujasnit, jakým směrem chceme postupovat a jestli náhodou nedokazujeme něco, co z nerovnosti vyplývá. Rozdíl mezi tím, jak na řešení nerovnosti přicházíme a jak řešení nakonec sepíšeme, je zde ohromný (narozdíl třeba od geometrie).

Příklad. Dokažte, že pro libovolná čísla $a, b \in \mathbb{R}$ platí nerovnost

$$a^2 + b^2 \geq 2ab.$$

Než se ale pustíme do příkladů, ujasníme si dva pojmy, které se u nerovností často používají. Jde o cykličnost a symetrii. Platí, že symterické nebo cyklické nerovnosti se dokazují mnohem lépe, protože cykličnost nám umožňuje pro proměnné a, b, c předpokládat, že $a = \max(a, b, c)$. Symetrie umožňuje předpokládat dokonce $a \geq b \geq c$. Většina ze známých nerovností je symetrická nebo přinejmenším cyklická.

Definice. (Symetrie) Výraz V nazveme *symeterický*, pokud se nezmění při libobolné záměně proměnných.

Definice. (Cykličnost) Výraz $V(a, b, c)$ nazveme *cyklický*, pokud se nezmění při provedení libovolné cyklické záměny, tj.

$$V(a, b, c) = V(b, c, a) = V(c, a, b).$$

Úprava na čtverec

První oblíbená metoda je úprava na čtverec. Při ní se snažíme nerovnost ekvivalentně upravovat, až ji převedeme do tvaru, který říká, že součet několika čtverců je alespoň

Klíčová slova. nerovnosti, AG nerovnost, úprava na čtverec

nula. To určitě platí, a protože jsme nerovnost upravovali *ekvivalentně*, lze postup obrátit, a tím máme dokázanou i zadanou nerovnost.

Tvrzení. *Nechť x je libovolné reálné číslo. Pak platí*

$$x^2 \geq 0.$$

Příklad 1. Dokažte, že pro libobolná reálná čísla a, b, c platí

$$a^2 + b^2 + c^2 \geq ab + bc + ca.$$

Příklad 2. Dokažte, že pro reálná čísla a, b splňující $a + b > 0$ platí

$$\frac{a}{b^2} + \frac{b}{a^2} \geq \frac{1}{a} + \frac{1}{b}.$$

(MKS 24-3-3)

AG nerovnost

Druhou metodou, kterou si předvedeme, je používání AG nerovnosti. Je to silná nerovnost s jejíž pomocí lze dokazovat hlavně nerovnosti, které mají na obou stranách členy ve stejných mocninách.

Tvrzení. (AG nerovnost) *Pro libovolná nezáporná reálná čísla $x_1, x_2, \ldots, x_n$ ($n \in \mathbb{N}$) platí*

$$x_1 + x_2 + \cdots + x_n \geq n \sqrt[n]{x_1 \cdot x_2 \cdots x_n}.$$

Rovnost nastává tehdy a jen tehdy, když $x_1 = x_2 = \cdots = x_n$.

Příklad 3. Dokažte, že pro libovolná kladná čísla a, b, c platí nerovnost

$$\left(a + \frac{1}{b}\right)\left(b + \frac{1}{c}\right)\left(c + \frac{1}{a}\right) \geq 8.$$

Zjistěte, kdy nastane rovnost. (Školní kolo kat. B MO 55r.)

Příklad 4. Dokažte, že pro každou trojici x, y, z nezáporných čísel platí nerovnost

$$x(x - \sqrt{yz}) + y(y - \sqrt{zx}) + z(z - \sqrt{xy}) \geq 0.$$

(Krajské kolo kat. A MO 17r.)

Příklad 5. Dokažte, že pro libovolná kladná čísla a, b, c platí

$$\frac{a}{b + c} + \frac{b}{c + a} + \frac{c}{a + b} \geq \frac{3}{2}.$$

(Nesbittova nerovnost)

Příklad 6. Nechť a, b, c jsou kladná čísla. Dokažte nerovnost

$$\frac{a^3}{bc} + \frac{b^3}{ca} + \frac{c^3}{ab} \geq a + b + c.$$

Příklad 7. Dokažte, že pro každou trojici x, y, z kladných čísel platí nerovnost

$$\sqrt{xyz}\left(\frac{2}{x+y} + \frac{2}{y+z} + \frac{2}{z+x}\right) \leq \sqrt{x} + \sqrt{y} + \sqrt{z}.$$

(Školní kolo kat. B MO 47r.)

Příklad 8. Pro libovolná kladná a, b, c dokažte

$$\frac{a}{b} + \sqrt{\frac{b}{c}} + \sqrt[3]{\frac{c}{a}} > \frac{5}{2}.$$

Příklad 9. Dokažte, že pro každá tři nezáporná reálná čísla x, y, z platí

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

Těžší příklady

Příklad 10. Nechť a, b jsou kladná reálná čísla. Dokažte, že

$$\frac{1}{a^2} + \frac{1}{b^2} + \frac{4}{a^2 + b^2} \geq \frac{32(a^2 + b^2)}{(a+b)^4}.$$

Příklad 11. Dokažte, že pro libovolná reálná čísla a, b, c platí

$$\frac{a^2}{3a^2 + (b+c)^2} + \frac{b^2}{3b^2 + (c+a)^2} + \frac{c^2}{3c^2 + (a+b)^2} \geq \frac{1}{3}.$$

Příklad 12. Nechť a, b, c jsou kladná reálná čísla. Dokažte, že platí

$$\frac{a}{b} + \frac{b}{c} + \frac{c}{a} \geq \frac{a+b}{b+c} + \frac{b+c}{a+b} + 1.$$

(Běloruská MO 1998)

Literatura

[1] Vo Quoc Ba Can, Cirtoaje Vasile, Phuong Tran, *Inequalities with beautiful solutions*, GIL, 2010.

[2] M. Rolínek, P. Šalom, *Seriál o nerovnostech*, archiv MKS, 2010.

Extremální princip

Alča Skálová

Abstrakt. Příklady na extremální princip – důkazovou metodu, kterou lze použít v mnoha oblastech matematiky

Extremální princip je důležitá důkazová metoda, která se dá použít v mnoha oblastech matematiky, od teorie čísel po geometrii, od teorie grafů po řešení rovnic. Hlavní myšlenkou je najít v úloze nějaké uspořádání a podívat se na uvažované objekty podle velikosti, vyplatí se často přemýšlet o největších či nejmenších prvcích. Ukažme si to hned na příkladě:

Příklady

Příklad 1. Každý mřížový bod[13] v rovině označíme cedulkou s přirozeným číslem tak, aby platilo, že číslo na cedulce je aritmetickým průměrem čtyř „sousedních" cedulek (té nahoře, dole, vlevo a vpravo). Ukaž, že čísla na cedulkách musejí být všechna stejná.

Řešení. Označme si nejmenší číslo vyskytující se na nějaké cedulce jako m. Čísla na sousedních cedulkách označíme a, b, c, d. Podle zadání je

$$a + b + c + d = 4m \qquad (\heartsuit)$$

a z volby m jakožto nejmenšího čísla máme $a \geq m$, $b \geq m$, $c \geq m$, $d \geq m$. Pokud by některé z čísel a, b, c, d bylo ostře větší než m, dojdeme ke sporu s $(\heartsuit)$, takže $a = b = c = d = m$. Odtud již plyne, že všechna čísla na cedulkách jsou rovna m.

Příklad 2. Dokaž, že existuje nekonečně mnoho prvočísel.

Příklad 3. V rovině je dáno n bodů takových, že každé tři body tvoří trojúhelník, jehož plocha je menší než 1. Ukaž, že všech n bodů leží v trojúhelníku o obsahu menším než 4.

Klíčová slova. extremální princip, minimální, maximální

[13] Mřížový bod v rovině je bod, který má obě souřadnice celočíselné.

Příklad 4. Nechť B a C jsou dvě konečné množiny bílých a černých bodů v rovině takových, že každá úsečka spojující dva body stejné barvy obsahuje navíc bod barvy druhé. Dokažte, že všechny body leží na přímce.

Příklad 5. V rovině je dáno n přímek ($n > 3$), žádné dvě z nich nejsou rovnoběžné, navíc průsečíkem každých dvou přímek prochází nějaká třetí přímka. Ukaž, že všechny přímky procházejí jedním bodem.

Příklad 6. Najdi všechna celočíselná řešení rovnice

$$a^2 + b^2 = 3(c^2 + d^2).$$

Příklad 7. Najdi všechna celočíselná řešení rovnice

$$8w^4 + 4x^4 + 2y^4 = z^4.$$

Příklad 8. Všechny silnice v Novosibiřské oblasti jsou jednosměrné. Každé dvě osady v oblasti jsou propojeny právě jednou přímou silnicí. Ukaž, že existuje osada, do které se lze z kterékoli jiné osady dostat přímo nebo nejvýš přes jednu jinou osadu.

Příklad 9. Kolem stolu sedí 7 trpaslíků, každý má před sebou pohár a v něm mléko. Mléka mají dohromady 3 litry. První trpaslík rozdělí své mléko rovnoměrně do zbývajících pohárů. Pak postupně, proti směru hodinových ručiček, udělají totéž všichni ostatní. Když sedmý trpaslík skončí, má každý tolik mléka, kolik měl na začátku. Urči, kolik to je.

Příklad 10. Na dvourozměrnou šachovnici $n \times n$ lze umístit n věží tak, že ohrožují všechna pole. Kolik nejméně věží je potřeba pro třírozměrnou šachovnici $n \times n \times n$?

Příklad 11. V rovině je dán konečný počet bodů takových, že všechny neleží na jedné přímce. Dokaž, že existuje přímka, která prochází právě přes dva z nich.

Musí to platit i pro nekonečnou množinu?

Příklad 12. Každý člen parlamentu má nejvýše tři nepřátele[14] mezi zbývajícími členy. Je možné členy parlamentu rozdělit do dvou skupin tak, aby každý měl nejvýše jednoho nepřítele ve své skupině?

Příklad 13. Dokaž, že existuje nekonečně mnoho prvočísel tvaru $6n - 1$.

Příklad 14. Mějme $2n$ bodů v rovině takových, že žádné tři neleží na přímce. Víme, že n z nich jsou farmy a zbývajících n jsou studny. Dokaž nebo vyvraťte: Lze postavit n přímých neprotínajících se cest (úseček) tak, že z každé farmy vede cesta k právě jedné studni.

Literatura a zdroje

[1] Arthur Engel, *Problem-Solving Strategies*, Springer, UK, 1998.

[14] Nepřátelství je symetrické, je-li A nepřítelem B, je i B nepřítelem A.

Koulítko a rovinítko

Alča Skálová

Abstrakt. Konstrukční úlohy trochu jinak – místo roviny prostor, místo pravítka rovinítko, místo kružítka koulítko.

Na přednášce si procvičíme prostorovou představivost řešením konstrukčních úloh ve třech dimenzích. Oproti klasickým nástrojům rovinné geometrie budeme mít k dispozici rovinítko (umožní nám proložit rovinu třemi body, které neleží v jedné přímce) a koulítko (z daného bodu opíše sféru s určeným poloměrem).

Při řešení mnohých úloh napoví, představíš-li si podobnou konstrukci v rovině. Například hned první úloha je „stejná“ jako konstrukce rovnostranného trojúhelníka. Jen má o dimenzi víc.

Příklady

Příklad 1. Sestroj pravidelný čtyřstěn.

Řešení. Zvolíme si v prostoru dva libovolné body A a B. Úsečka AB (její délku označíme a) bude hranou našeho čtyřstěnu. Zabodneme koulítko postupně do bodů A a B a z obou opíšeme sféru o poloměru a. Průnik těchto sfér je kružnice, říkejme jí k. Kdekoliv na k si zvolíme další bod – C.[15] Z bodu C opět nakreslíme sféru o poloměru a, ta protne k ve dvou bodech. Libovolný z těchto bodů je čtvrtý vrchol našeho čtyřstěnu.

Příklad 2. Je dána přímka p a bod B, který na ní neleží. Sestroj rovinu kolmou na p a procházející bodem B.

Příklad 3. Je dána rovina σ a přímka p. Sestroj rovinu τ, která je kolmá na σ a současně v ní leží přímka p.

Příklad 4. Mějme rovinu σ a bod B mimo σ. Sestroj přímku p procházející bodem B a kolmou na σ.

Příklad 5. Sestroj přímku q rovnoběžnou s danou přímkou p a procházející daným bodem B nenáležejícím p.

Klíčová slova. stereometrie, konstrukční úlohy, koulítko, rovinítko

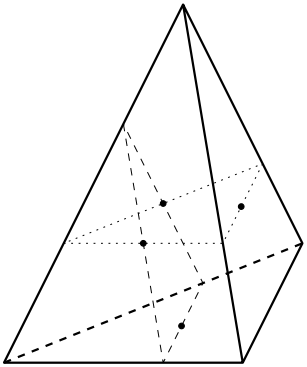
[15] Jistě sis všiml/a, že body A, B, C tvoří rovnostranný trojúhelník.

Příklad 6. Sestroj kouli opsanou danému čtyřstěnu.

Příklad 7. Sestroj rovinu, která prochází daným bodem a je rovnoběžná k dané rovině.

Příklad 8. Sestroj čtyřstěn, jsou-li zadána těžiště jeho stěn.

Návodný obrázek:



Příklad 9. Sestroj kouli vepsanou danému čtyřstěnu.

Příklad 10. Nechť jsou dány body $S, S_{AB}, S_{BD}, S_{CD}$, které neleží v jedné rovině. Sestroj čtyřstěn $ABCD$ takový, že S je střed koule jemu opsané a S_{AB}, S_{BD}, S_{CD} jsou po řadě středy hran AB, BD, CD.

Příklad 11. Sestroj kouli, která prochází danými dvěma body a dotýká se daných dvou koulí.

Příklad 12. Nechť jsou dány nekolineární[16] body T_A, V_A, T_C, přímka p mimoběžná s přímkou T_AV_A a úsečka délky d. Sestroj čtyřstěn $ABCD$ takový, že T_A, resp. T_C je těžiště stěny BCD, resp. ABD, V_A je pata výšky spuštěné z vrcholu A na stěnu BCD, bod B leží na přímce p a vzdálenost $|CV_A|$ je rovna d.

Příklad 13. Sestroj krychli **pouze koulítkem**, jsou-li dány délky stěnové a tělesové úhlopříčky.

Literatura a zdroje

Úlohy 6 až 13 jsou převzaty ze 6. série 19. ročníku našeho semináře. Najdeš je i se vzorovým řešením v archivu (*mks.mff.cuni.cz/archive/archive.php*).

[16] Tedy takové, že neleží na společné přímce.

Prostory metrické a jiné

Alexander „Olin“ Slávik

Abstrakt. V příspěvku jsou rozebrány základní vlastnosti metrických prostorů a jejich vztah k dalším důležitým prostorům. Uvedeny jsou rozličné příklady metrických prostorů.

V matematice i v praktických aplikacích jsme často postaveni do situace, kdy bychom o nějakých objektech chtěli říct, že jsou nějak „blízko“ či „daleko“, přičemž bychom byli rádi, aby tato vzdálenost měla „rozumné“ vlastnosti. Metrika je asi nejpřirozenější konstrukcí, která tyto myšlenky formalizuje.

Definice. *Metrikou* na množině X rozumíme funkci $\varrho\colon X \times X \to \langle 0, \infty)$ splňující

(i) $\varrho(x, y) = 0$, právě když $x = y$,
(ii) $\varrho(x, y) = \varrho(y, x)$ pro všechna $x, y \in X$,
(iii) $\varrho(x, y) \leq \varrho(x, z) + \varrho(z, y)$ pro všechna $x, y, z \in X$ (trojúheníková nerovnost).

Dvojici (X, ϱ) pak nazveme *metrickým prostorem*.

Příklady.

(i) Asi nejběžnější metrikou na $\mathbb{R}^n$ je *euklidovská*, která odpovídá vzdálnosti, na kterou jsme zvyklí:

$$\varrho_2(x, y) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + \cdots + (x_n - y_n)^2}.$$

Jinou možnou metrikou je *manhattanská* či *newyorská*:

$$\varrho_1(x, y) = |x_1 - y_1| + |x_2 - y_2| + \cdots + |x_n - y_n|.$$

Konečně je zde i *maximová* metrika:

$$\varrho_\infty(x, y) = \max\{|x_1 - y_1|, |x_2 - y_2|, \ldots, |x_n - y_n|\}.$$

(ii) Na množině[17] $\mathcal{C}(\langle 0, 1\rangle)$ máme taky maximovou metriku,

$$\varrho_{\max}(f, g) = \max_{x \in \langle 0,1\rangle} |f(x) - g(x)|,$$

Klíčová slova. Metrický prostor, metrika, norma, skalární součin, vektorový prostor, topologický prostor

[17] $\mathcal{C}(\langle 0, 1\rangle)$ značí množinu všech spojitých reálných funkcí na intervalu $\langle 0, 1\rangle$.

navíc zde máme i *integrální* metriku

$$\varrho_{\mathrm{int}}(f,g) = \int_0^1 |f(x) - g(x)| \,\mathrm{d}x$$

a mnohé další.

(iii) Na úplně každé množině můžeme definovat *diskrétní metriku* předpisem

$$\varrho(x,y) = \begin{cases} 0 & \text{pokud } x = y, \\ 1 & \text{jinak.} \end{cases}$$

(iv) Nechť X je množina všech (konečných) slov nad nějakou abecedou Σ. Na slovech si povolíme operace přidání libovolného písmene ze Σ kamkoliv do slova, odstranění kteréhokoliv písmene ve slově a nahrazení kteréhokoliv písmene libovolným jiným. Pro $a, b \in X$ definujeme metriku[18] $\varrho(a,b)$ jako nejmenší počet těchto operací, které potřebujeme k tomu, abychom slovo a transformovali na slovo b.

(v) Buď G (konečný jednoduchý) souvislý graf, V množina jeho vrcholů. Pro $u, v \in V$ můžeme definovat metriku $\varrho(u,v)$ jako délku nejkratší cesty z u do v v G.

(vi) Označme ještě E množinu hran grafu G. Každou hranu $e \in E$ „ohodnotíme“ nějakým kladným reálným číslem $f(e)$. Je-li C cesta v G používající hrany $e_1, e_2, \ldots, e_n$, pak její ohodnocenou délkou nazveme číslo $f(e_1)+f(e_2)+\cdots+f(e_n)$. Pro $u, v \in V$ pak můžeme definovat metriku $\varrho(u,v)$ jako nejmenší možnou ohodnocenou délku cesty z u do v.

Cvičení 1. Jaké problémy mohou nastat, pokud u grafů v bodech (v) a (vi) vynecháme předpoklad souvislosti nebo předpoklad konečnosti? Musí být ohodnocení hran kladné? Jak se situace změní, pokud budeme uvažovat multigrafy (tj. povolíme více hran mezi dvěma vrcholy), nebo naopak orientované grafy, ve kterých budeme brát v potaz pouze orientované cesty?

Cvičení 2. Na políčkách šachovnice 8×8 uvažme pro každá dvě pole nejmenší počet tahů, kterou musíme udělat králem, resp. věží, resp. koněm, resp. střelcem, abychom figuru přemístili z jednoho pole do druhého. Ve kterých případech jde o metriku? Jak tato metrika souvisí s metrikami uvedenými výše?

Cvičení 3. Ukažte, že ke každému metrickému prostoru (X, ϱ) existuje (nekonečný, je-li to zapotřebí) graf s ohodnocenými hranami, jehož vrcholy jsou prvky X a konstrukce metriky dle bodu (vi) výše dá přesně metriku ϱ.

Cvičení 4. Uvažme graf G, který získáme z $(\mathbb{R}^2, \varrho_2)$ podle řešení cvičení 3. Lze z tohoto grafu některé hrany odstranit tak, abychom podle postupu (vi) získali metrický prostor $(\mathbb{R}^2, \varrho_1)$ nebo $(\mathbb{R}^2, \varrho_\infty)$? Co se stane, pokud v G ponecháme pouze hrany spojující body $x = (x_1, x_2)$, $y = (y_1, y_2)$ takové, že $x_1 y_2 = x_2 y_1$?

[18] Tato metrika se obvykle nazývá *Levenshteinova vzdálenost*.

Definice. Buď (X, ϱ) metrický prostor, $x \in X$ a $r \in (0, \infty)$. Množinu

$$B_\varrho(x, r) = \{y \in X : \varrho(x, y) < r\}$$

nazveme *(otevřenou) koulí* se středem v x a poloměrem r.

Definice. Buď (X, ϱ) metrický prostor. Řekneme, že množina $G \subseteq X$ je *otevřená*, pokud pro každý bod $x \in G$ existuje $r \in (0, \infty)$ takové, že $B_\varrho(x, r) \subseteq G$. Řekneme, že množina $F \subseteq X$ je *uzavřená*, pokud je $X \setminus F$ otevřená.

Příklad. Jak lze vytušit z terminologie, v $\mathbb{R}$ s běžnou metrikou jsou otevřené intervaly otevřené, analogicky uzavřené intervaly jsou uzavřené. Nejde ovšem o všechny otevřené/uzavřené množiny!

Příklad. V metrických prostorech $(\mathbb{R}^n, \varrho_1)$, $(\mathbb{R}^n, \varrho_2)$ a $(\mathbb{R}^n, \varrho_\infty)$ jsou tytéž množiny otevřené – to platí díky nerovnosti

$$\varrho_\infty(x, y) \leq \varrho_2(x, y) \leq \varrho_1(x, y) \leq n \cdot \varrho_\infty(x, y).$$

Cvičení 5. Popište všechny otevřené množiny v prostoru s diskrétní metrikou.

Cvičení 6. Dokažte, že pokud je množina otevřená v prostoru $\big(\mathcal{C}(\langle 0, 1\rangle), \varrho_{\text{int}}\big)$, tak je otevřená i v $\big(\mathcal{C}(\langle 0, 1\rangle), \varrho_{\max}\big)$, ale opačná implikace obecně neplatí.

Věta. (Vlastnosti otevřených množin)

(O1) *Celý prostor a prázdná množina jsou otevřené množiny.*
(O2) *Sjednocení (libovolně velkého) systému otevřených množin je otevřená množina.*
(O3) *Průnik dvou otevřených množin je otevřená množina.*[19]

Cvičení 7. Ukažte, že průnik nekonečně mnoha otevřených množin již nemusí být otevřenou množinou.

Konvergence a spojitost v metrických prostorech

Jakmile máme vybudován aparát limit a spojitých funkcí v reálných číslech, velmi snadno tyto pojmy přeneseme do metrických prostorů.

Definice. Řekneme, že posloupnost $\{x_n\}_{n=1}^\infty$ bodů z metrického prostoru (X, ϱ) má *limitu* x (značíme $\lim_{n\to\infty} x_n = x$), pokud platí $\lim_{n\to\infty} \varrho(x_n, x) = 0$. Má-li posloupnost limitu, nazývá se *konvergentní*.

Lemma. *Množina F v metrickém prostoru (X, ϱ) je uzavřená, právě když pro každou konvergentní posloupnost $\{x_n\}_{n=1}^\infty$ bodů z F je $\lim_{n\to\infty} x_n \in F$ (neformálně, z uzavřené množiny nelze „vykonvergovat ven“).*

[19] Odtud snadno plyne, že průnik konečně mnoha otevřených množin je otevřená množina.

Věta. (Weierstrassova) *Pro každou funkci $f \in \mathcal{C}(\langle 0,1\rangle)$ existuje posloupnost polynomů $\{p_n\}_{n=1}^{\infty}$ taková, že $f = \lim_{n\to\infty} p_n$, kde limitu uvažujeme v maximové metrice.*

Definice. Nechť (X,ϱ), (Y,σ) jsou metrické prostory. Řekneme, že funkce $f\colon X \to Y$ je *spojitá*, pokud pro každou konvergentní posloupnost $\{x_n\}_{n=1}^{\infty}$ bodů z X platí

$$f\left(\lim_{n\to\infty} x_n\right) = \lim_{n\to\infty} f(x_n).$$

Řečeno méně formálně, funkce je spojitá, pokud „zachovává limity posloupností“.

Věta. *Nechť (X,ϱ), (Y,σ) jsou metrické prostory. Funkce $f\colon X \to Y$ je spojitá právě tehdy, když pro každou otevřenou množinu $G \subseteq Y$ je vzor této množiny v f, tj. množina*

$$f^{-1}(G) = \{x \in X : f(x) \in G\}$$

otevřená (v X).

Poznámka. Uvedená věta naznačuje, že pojem spojitosti funkcí není nijak hluboce závislý na konkrétních metrikách, které na množinách máme, rozhodující je pouze informace, které množiny jsou v daných prostorech otevřené. Tato skutečnost je motivací pro pojem struktury obecnější, než je metrický prostor, tzv. *topologického prostoru*. Uvedeme pouze formální definici.

Definice. Buď X množina a $\mathcal{G}$ nějaký systém jejích podmnožin. $\mathcal{G}$ nazveme *topologií na X*, pokud jeho množiny splňují podmínky (O1), (O2) a (O3). Množiny z $\mathcal{G}$ pak nazveme *otevřené* množiny a dvojici $(X,\mathcal{G})$ *topologický prostor*.

Prostory s normou či skalárním součinem

Množiny, na kterých zavádíme metriky, zpravidla nebývají nějaké úplně abstraktní – často na nich již máme nějakou jinou strukturu. U takových množin bychom „byli rádi“, kdyby námi definovaná metrika nějak „souhlasila“ s již existující strukturou. Běžným příkladem takové struktury je vektorový prostor, na který se nyní trochu blíže podíváme.

Definice. Nechť V je libovolná množina, $+\colon V \times V \to V$ a $\cdot\colon \mathbb{R} \times V \to V$ binární operace takové, že

(i) existuje prvek $\mathbf{o} \in V$ takový, že pro všechna $\mathbf{v} \in V$ je $\mathbf{v} + \mathbf{o} = \mathbf{v}$,
(ii) pro všechna $\mathbf{v} \in V$ existuje $\mathbf{w} \in V$ takový, že $\mathbf{v} + \mathbf{w} = \mathbf{o}$, značíme $\mathbf{w} = -\mathbf{v}$,
(iii) pro všechna $\mathbf{v}, \mathbf{w} \in V$ je $\mathbf{v} + \mathbf{w} = \mathbf{w} + \mathbf{v}$,
(iv) pro všechna $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ je $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$,
(v) pro všechna $a, b \in \mathbb{R}$, $\mathbf{v} \in V$ je $a \cdot (b \cdot \mathbf{v}) = (a \cdot b) \cdot \mathbf{v}$,
(vi) pro všechna $\mathbf{v} \in V$ je $1 \cdot \mathbf{v} = \mathbf{v}$,

(vii) pro všechna $a \in \mathbb{R}$, $\mathbf{v}, \mathbf{w} \in V$ je $a \cdot (\mathbf{v} + \mathbf{w}) = a \cdot \mathbf{v} + a \cdot \mathbf{w}$,
(viii) pro všechna $a, b \in \mathbb{R}$, $\mathbf{v} \in V$ je $(a + b) \cdot \mathbf{v} = a \cdot \mathbf{v} + b \cdot \mathbf{v}$.

Pak čtveřici $(V, +, \cdot, \mathbf{o})$ nazveme *vektorovým* (či *lineárním*) *prostorem nad* $\mathbb{R}$.

Definice. Buď $(V, +, \cdot, \mathbf{o})$ vektorový prostor nad $\mathbb{R}$. Funkci $\|\cdot\|\colon V \to \langle 0, \infty)$ nazveme *normou* na V, pokud platí

(i) $\|\mathbf{v}\| = 0$, právě když $\mathbf{v} = \mathbf{o}$,
(ii) pro všechna $a \in \mathbb{R}$, $\mathbf{v} \in V$ je $\|a \cdot \mathbf{v}\| = |a| \cdot \|\mathbf{v}\|$,
(iii) pro všechna $\mathbf{v}, \mathbf{w} \in V$ je $\|\mathbf{v} + \mathbf{w}\| \leq \|\mathbf{v}\| + \|\mathbf{w}\|$.

Poznámka. Každá norma na vektorovém prostoru přirozeně definuje metriku na tomto prostoru předpisem $\varrho(\mathbf{v}, \mathbf{w}) = \|\mathbf{v} - \mathbf{w}\|$. Normu tedy můžeme chápat jednak jako „velikost“, jednak jako „vzdálenost od nuly“.

Příklady. Na vektorovém prostoru $\mathbb{R}^n$ s běžnými operacemi můžeme definovat normy

$$\|x\|_2 = \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2},$$
$$\|x\|_1 = |x_1| + |x_2| + \cdots + |x_n|,$$
$$\|x\|_\infty = \max\{|x_1|, |x_2|, \ldots, |x_n|\},$$

na prostoru $\mathcal{C}(\langle 0, 1\rangle)$ zase

$$\|f\|_{\max} = \max_{x \in \langle 0,1\rangle} |f(x)|, \qquad \|f\|_{\mathrm{int}} = \int_0^1 |f(x)| \, \mathrm{d}x.$$

Metriky uvedené na začátku příspěvku jsou generovány právě těmito normami.

Definice. Binární operaci $\cdot\colon V \times V \to \mathbb{R}$ nazveme *skalárním součinem* na prostoru V, pokud platí

(i) pro všechna $\mathbf{v} \in V$ je $\mathbf{v} \cdot \mathbf{v} \geq 0$, přičemž $\mathbf{v} \cdot \mathbf{v} = 0$, právě když $\mathbf{v} = \mathbf{o}$,
(ii) pro všechna $\mathbf{v}, \mathbf{w} \in V$ je $\mathbf{v} \cdot \mathbf{w} = \mathbf{w} \cdot \mathbf{v}$,
(iii) pro všechna $a \in \mathbb{R}$, $\mathbf{v}, \mathbf{w} \in V$ je $(a \cdot \mathbf{v}) \cdot \mathbf{w} = a \cdot (\mathbf{v} \cdot \mathbf{w})$,
(iv) pro všechna $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ je $(\mathbf{u} + \mathbf{v}) \cdot \mathbf{w} = \mathbf{u} \cdot \mathbf{w} + \mathbf{v} \cdot \mathbf{w}$.

Poznámka. Pomocí skalárního součinu lze na vektorovém prostoru definovat normu předpisem $\|\mathbf{v}\| = \sqrt{\mathbf{v} \cdot \mathbf{v}}$. Ne každá norma ale odpovídá nějakému skalárnímu součinu – takové normy musí splňovat rovnoběžníkové pravidlo, tj. pro každé $\mathbf{v}, \mathbf{w} \in V$ musí platit

$$2\|\mathbf{v}\|^2 + 2\|\mathbf{w}\|^2 = \|\mathbf{v} + \mathbf{w}\| + \|\mathbf{v} - \mathbf{w}\|.$$

Příklad. Běžný skalární součin na $\mathbb{R}^n$ se definuje jako

$$x \cdot y = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n.$$

Cvičení 8. Najděte nějaký skalární součin na prostoru $\mathcal{C}(\langle 0, 1\rangle)$. Jaká norma (metrika) tomuto skalárnímu součinu odpovídá?

Věta. (Cauchy-Schwarz-Buňakovského nerovnost) *Je-li* $\|\cdot\|$ *norma generovaná příslušným skalárním součinem, pak pro libovolné* $\mathbf{v}, \mathbf{w} \in V$ *platí*

$$|\mathbf{v} \cdot \mathbf{w}| \leq \|\mathbf{v}\| \cdot \|\mathbf{w}\|.$$

Literatura a zdroje

[1] P. Simon, V. Musil, *Poznámky k přednášce Základy teorie metrických prostorů*, dostupné z *http://atrey.karlin.mff.cuni.cz/˜vejtek/studium/files/metrprs/metrSpc.pdf*

Teória čísel

Michal „Miško“ Szabados

Abstrakt. V príspevku sú formulované základné tvrdenia z oblasti teórie čísel spolu s niekoľkými príkladmi. Jedná sa okrem iného o deliteľnosť a kongruencie, Malú Fermatovu a Eulerovu vetu, Čínsku zvyškovú vetu či kvadratické zvyšky.

Úvod

Tento zborníčkový príspevok začnem netradične tým, že vás odkážem na literatúru. Je to z toho dôvodu, že na tému teória čísel bolo napísaných mnoho dobrých knižiek. Pred pár rokmi dokonca vychádzal v PraSe seriál a len pred rokom mal Kenny prednášku na túto istú tému. Tieto materiály môžete nájsť v PraSačej knižnici, zoznam knižiek nájdete v literatúre nižšie.

Takže nie je dôvod písať ďalší obšírny text. Nájdete tu akurát definície potrebných pojmov a niekoľko príkladov. Všetko vysvetľovanie si nechám na prednášku a nechám niečo vymyslieť aj vás. Bude to zaujímavé, určite príďte!

Deliteľnosť a kongruencie

Všetky neznáme v tomto príspevku sú celé čísla.

Definícia. Zápis $a \mid b$ čítame „a delí b“ a vyjadruje fakt, že existuje číslo n také, že $b = na$.

Definícia. Zápis $a \equiv b \pmod{p}$ čítame „a je kongruentné s b modulo p“ alebo „a dáva rovnaký zvyšok ako b po delení p“. Povieme tak vtedy, keď platí $p \mid a - b$. Veľmi často budeme skúmať kongruencie modulo nejaké prvočíslo.

Príklad 1. Nech n je prirodzené číslo. Dokážte, že číslo $3^{2^n} + 1$ je párne, ale nie je deliteľné 4.

Príklad 2. Ak $3 \mid a^2 + b^2$, tak potom $3 \mid a$ a $3 \mid b$. Dokážte.

Kľúčové slová. teorie čísel, kongruence, Malá Fermatova věta, Eulerova věta, Čínska zbytková věta, kvadratické zbytky

Príklad 3.

(i) Dokážte, že čísla tvaru $4k+3$ sa nedajú zapísať ako súčet dvoch štvorcov.[20]
(ii) Nájdite nekonečne veľa čísel, ktoré sa nedajú zapísať ako súčet troch štvorcov.

Príklad 4. Dané je racionálne číslo x z intervalu $(0,1)$. Nech y je také číslo z intervalu $(0,1)$, ktorého n-tá cifra za desatinnou čiarkou sa rovná 2^n-tej cifre za desatinnou čiarkou čísla x. Dokážte, že aj y je racionálne.

Príklad 5. Dokážte, že pre každé n existuje n-ciferné číslo skladajúce sa iba z nepárnych cifier a zároveň deliteľné 5^n.

Príklad 6. Dokážte, že je nekonečne veľa prvočísel tvaru $4k-1$.

Užitočné vety

Definícia. (Eulerova funkcia) Zápis $\varphi(m)$ označuje počet prirodzených čísel, ktoré sú menšie ako m a sú s m nesúdeliteľné.[21] Eulerovu funkciu vieme vyjadriť so znalosťou prvočíselného rozkladu $m = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ ako

$$\varphi(m) = (p_1-1)\cdots(p_k-1)\cdot p_1^{\alpha_1-1}\cdots p_k^{\alpha_k-1} = m\cdot\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right).$$

Veta. (Malá Fermatova) *Pre prvočíslo p a číslo a také, že $p\nmid a$, platí $a^{p-1}\equiv 1 \pmod p$.*

Veta. (Eulerova) *Pre nesúdeliteľné čísla m a a platí $a^{\varphi(m)}\equiv 1 \pmod m$.*

Veta. (Wilsonova) *Pre prvočíslo p platí $(p-1)! = 1\cdot 2\cdots(p-1)\equiv -1 \pmod p$.*

Veta. (Bézoutova) *Nech a, b sú celé čísla. Potom existujú m, n také, že $ma+nb = \mathrm{NSD}(a,b)$.*

Veta. (Čínska zvyšková) *Nech $m_1,\ldots,m_k$ sú po dvoch nesúdeliteľné čísla. Potom sústava kongruencií s neznámou x*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}\\ x &\equiv a_2 \pmod{m_2}\\ &\vdots\\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

má práve jedno riešenie modulo $m_1\cdots m_k$.

[20] Štvorec je v tomto význame druhá mocnina celého čísla.
[21] Čísla a a b sú nesúdeliteľné, ak ich najväčší spoločný deliteľ je 1.

Príklad 7. Dokážte, že pre každé prvočíslo $p > 5$ existuje nejaký jeho násobok, ktorý má tvar $11\ldots11$.

Príklad 8. Dokážte, že vo Fibonacciho postupnosti $1, 1, 2, 3, 5, 8, \ldots$ existuje člen deliteľný každým prvočíslom.

Príklad 9. Nech p je prvočíslo. Dokážte, že dĺžka najkratšej periódy čísla $1/p$ v desiatkovom zápise delí $p - 1$.

Príklad 10. Nájdite najväčší spoločný deliteľ všetkých čísel tvaru $n^{13} - n$ pre n prirodzené.

Príklad 11. Nájdite poslednú cifru čísel $77^{77^{77}}$ a 4^{4^4}.

Príklad 12. Dokážte, že číslo $2^{2^{4n+1}} + 7$ je zložené.

Príklad 13. Rozhodnite, či existuje nekonečne veľa párnych čísel k takých, že číslo $p^2 + k$ je zložené pre každé prvočíslo p.

Kvadratické zvyšky

Definícia. Číslo a také, že $m \nmid a$, je kvadratický zvyšok modulo m, ak existuje b také, že $a \equiv b^2$. V opačnom prípade povieme, že je kvadratický nezvyšok.

Definícia. (Legenderov symbol) Pre nepárne prvočíslo p definujeme

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ak } a \text{ je kvadratický zvyšok mod } p, \\ 0, & \text{ak } p \mid a, \\ -1, & \text{ináč.} \end{cases}$$

Tvrdenie. *Pre Legenderov symbol platí*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Veta. (Zákon kvadratickej reciprocity) *Pre rôzne nepárne prvočísla p, q platí*

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

Príklad 14. Pre ktoré prvočísla je -1 kvadratický zvyšok?

Príklad 15. Dokážte, že pre prvočíslo $p = 4k + 3$ platí $\left(\frac{p-1}{2}\right)! \equiv \pm 1$.

Príklad 16. Dokážte, že rovnica $a^2 + b^2 + 1 \equiv 0 \pmod{p}$ má riešenie pre každé prvočíslo p.

Príklad 17. Dokážte, že pre bezštvorcové[22] číslo m má rovnica $a^2 + b^2 \equiv k \pmod{m}$ riešenie pre každé k.

Príklad 18. Nájdite nekonečne veľa navzájom nesúdeliteľných čísel m takých, že rovnica $a^2 + b^2 \equiv k \pmod{m}$ nemá riešenie pre každé k.

Magické tabuľky

mod 11	0	1	2	3	4	5	6	7	8	9	10
2	0	1	4	9	5	3	3	5	9	4	1
3	0	1	8	5	9	4	7	2	6	3	10
4	0	1	5	4	3	9	9	3	4	5	1
5	0	1	10	1	1	1	10	10	10	1	10
6	0	1	9	3	4	5	5	4	3	9	1
7	0	1	7	9	5	3	8	6	2	4	10
8	0	1	3	5	9	4	4	9	5	3	1
9	0	1	6	4	3	9	2	8	7	5	10
10	0	1	1	1	1	1	1	1	1	1	1

mod 13	0	1	2	3	4	5	6	7	8	9	10	11	12
2	0	1	4	9	3	12	10	10	12	3	9	4	1
3	0	1	8	1	12	8	8	5	5	1	12	5	12
4	0	1	3	3	9	1	9	9	1	9	3	3	1
5	0	1	6	9	10	5	2	11	8	3	4	7	12
6	0	1	12	1	1	12	12	12	12	1	1	12	1
7	0	1	11	3	4	8	7	6	5	9	10	2	12
8	0	1	9	9	3	1	3	3	1	3	9	9	1
9	0	1	5	1	12	5	5	8	8	1	12	8	12
10	0	1	10	3	9	12	4	4	12	9	3	10	1
11	0	1	7	9	10	8	11	2	5	3	4	6	12
12	0	1	1	1	1	1	1	1	1	1	1	1	1

[22] To je také, ktoré nie je deliteľné žiadnym štvorcom, okrem 1.

Literatúra a zdroje

[1] Titu Andreescu, Dorin Andrica, Zuming Feng, *104 Number Theory Problems from USA IMO Training*, BirkHauser, Boston, 2007.
[2] Víťa a šnEk, Seriál z teórie čísel, *http://mks.mff.cuni.cz/archive/28/9.pdf*
[3] PraSačia knižnica, kategória Teória čísel, *http://mks.mff.cuni.cz/library/library.php*
[4] Kenny pozná dobré knižky, spýtajte sa jeho :)

Kruhová inverze

Pepa Tkadlec

Abstrakt. Příspěvek seznamuje se základními vlastnostmi kruhové inverze a na úlohách ze světových soutěží ilustruje, kdy je vhodné inverzi při řešení použít. Obsahuje jeden řešený příklad a stručné návody ke všem ostatním.

Kruhová inverze je jedno z nejexotičtějších geometrických zobrazení. Přestože nezachovává ani tak jednoduché objekty jako jsou přímky, má řadu překvapujících a užitečných vlastností, díky nimž je velmi silným nástrojem při řešení jinak obtížných geometrických úloh.

Definice

Úmluva. Rovinu rozšíříme o (jediný) bod ∞, o němž prohlásíme, že leží na všech přímkách.

Definice. *Kruhová inverze* je geometrické zobrazení určené kružnicí k se středem I a poloměrem r, které bodu A přiřadí bod A' podle následujícího pravidla:

(i) Je-li $A = I$, pak $A' = \infty$.
(ii) Je-li $A = \infty$, pak $A' = I$.
(iii) Jinak je A' ten bod polopřímky IA, pro nějž platí

$$|IA'| \cdot |IA| = r^2.$$

Vlastnosti

Takto definované zobrazení má triviálně následující vlastnosti:

(i) Body kružnice k jsou samodružné.
(ii) Leží-li bod A uvnitř kružnice k, leží obraz A' venku a naopak.
(iii) Inverze provedená dvakrát podle téže kružnice je identita.

Klíčová slova. kruhová inverze, planimetrie, geometrie, geometrická zobrazení

Tvrzení. (Konstrukce obrazu) *Je dána kružnice k a bod A vně této kružnice. Tečny ke kružnici k vedené bodem A se jí dotýkají v bodech T, U. Pak obraz A' bodu A v kruhové inverzi podle kružnice k je střed úsečky TU.*

Lemma. (Přepočítávací lemma) *Je dána kružnice $k(I,r)$ a body X, Y. Označme X', Y' obrazy bodů X, Y v inverzi podle kružnice k. Pak*

(i) $|\sphericalangle IX'Y'| = |\sphericalangle XYI|$,
(ii) $|X'Y'| = |XY| \cdot \frac{r^2}{|IX|\cdot|IY|}$,
(iii) $|XY| = |X'Y'| \cdot \frac{r^2}{|IX'|\cdot|IY'|}$.

Cvičení. (Tětivové čtyřúhelníky) Je dána kružnice k se středem I a body A, B takové, že neleží na jedné přímce s I. Označme A', B' obrazy bodů A, B v inverzi podle k. Ukažte, že body A, B, A', B' leží na jedné kružnici.

Tvrzení. (Stěžejní) *Uvažme kruhovou inverzi určenou kružnicí k se středem I. Pak*

(i) *Obrazem přímky procházející bodem I je ona sama.*
(ii) *Obrazem přímky* **ne***procházející bodem I je kružnice.*
(iii) *Obrazem kružnice procházející bodem I je přímka.*
(iv) *Obrazem kružnice* **ne***procházející bodem I je kružnice.*

Cvičení. (Středy kružnic) Podle předchozího tvrzení je obrazem kružnice k se středem O nějaká kružnice k' se středem S (neprochází-li k středem inverze I). Ukažte, že ačkoliv bod S leží na polopřímce IO, není to obraz bodu O (kruhová inverze na sebe tedy nezobrazuje středy kružnic).

Cvičení. (Samodružné kružnice) Podle předchozího tvrzení se přímka zobrazí na sebe sama právě tehdy, když prochází středem inverze. Které kružnice mají tuto vlastnost také?

Záhadou zůstává, jak rozpoznat, že na úlohu lze zaútočit inverzí. Několik rysů nás může k použití inverze navést. Proberme je postupně.

Máme vzor i obraz

Umíme-li v obrázku interpretovat některou přímku nebo kružnici jako obraz jiné přímky či kružnice ve vhodné inverzi, může pouhé uvážení této inverze vnést do úlohy zcela nové světlo.

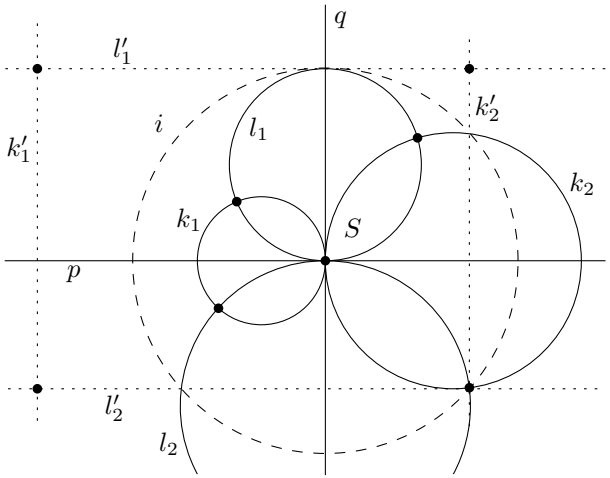
Příklad 1. Přímka p protne kružnici k v bodech X, Y. Označme $\check{S}$ střed jednoho oblouku XY. Bodem $\check{S}$ vedeme dvě přímky, které protnou kružnici k v bodech A, B a přímku p v bodech C, D. Ukažte, že body A, B, C, D leží na jedné kružnici.

Příklad 2. Kružnice k_1, k_2, k_3 mají po dvou vnější dotyk. Kružnice l má se všemi třemi vnější dotyk postupně v bodech L_1, L_2, L_3. Kružnice m má se všemi třemi vnitřní dotyk postupně v bodech M_1, M_2, M_3. Ukažte, že přímky L_1M_1, L_2M_2, L_3M_3 procházejí jedním bodem. (PraSe)

Typické použití kruhové inverze je ale jiné. Kruhová inverze nám totiž umožňuje řešit místo zadané úlohy jinou (ale ekvivalentní) úlohu v jiném (zinvertovaném) obrázku. Tento princip objasňuje následující řešený příklad.

Příklad 3. Kolmé přímky p, q se protínají v bodě S. Kružnice k_1, k_2 se středy na přímce p a procházející bodem S protínají kružnice l_1, l_2 se středy na přímce q a rovněž procházející bodem S podruhé ve čtyřech různých bodech. Ukažte, že tyto čtyři body leží na jedné kružnici.

Řešení. Invertujme podle kružnice i se středem S a libovolným poloměrem. Tvrzení bude dokázáno, pokud se nám podaří ukázat, že *obrazy* zmíněných čtyř průsečíků leží na kružnici neprocházející bodem S, protože původní čtyři druhé průsečíky budou potom muset ležet na obrazu této kružnice v inverzi podle i, což je podle *Stěžejního tvrzení* kružnice.



Přímky p, q se v inverzi podle i zobrazí samy na sebe. Kružnice k_1, k_2 se zobrazí na nějaké přímky k_1', k_2' obě kolmé na p. Obdobně se kružnice l_1, l_2 zobrazí na přímky l_1', l_2' obě kolmé na q. Obrazy zmíněných čtyř druhých průsečíků jsou proto vrcholy obdélníka. Vrcholy obdélníka leží na kružnici, tato kružnice neprochází bodem S a my jsme hotovi. □

Zbývá umět rozpoznat, podle kterého bodu a s jakým poloměrem invertovat.

„Přetížený“ bod

V úlohách, které překypují kružnicemi, volíme za střed inverze bod, jímž prochází hodně kružnic či přímek (tzv. „přetížený“ bod). Po inverzi pak dostaneme podstatně jednodušší obrázek, v němž již bývá snadné ekvivalent dokazovaného tvrzení dokázat. Na poloměru inverzní kružnice při tom zpravidla vůbec nezáleží.

Příklad 4. Kružnice k, l mají vnější dotyk v bodě T a obě mají vnitřní dotyk s kružnicí m po řadě v bodech U, V. Přímka UT protne kružnici m podruhé v bodě X. Ukažte, že $|\sphericalangle TVX| = 90°$. (KMS)

Příklad 5. Je dán pravoúhlý trojúhelník ABC s pravým úhlem při vrcholu C a uvnitř jeho stran AC, BC po řadě body D, E. Dokažte, že paty výšek z bodu C na přímky AB, AE, BD, DE leží na jedné kružnici.

Příklad 6. Kružnice vepsaná trojúhelníku ABC se dotýká jeho stran BC, CA, AB postupně v bodech D, E, F. Bod X leží uvnitř trojúhelníka ABC tak, že kružnice vepsaná trojúhelníku BCX se dotýká jeho stran BC, CX, XB postupně v bodech D, Y, Z. Ukažte, že body E, F, Y, Z leží na jedné kružnici. (IMO shortlist 1995)

Příklad 7. Je dána půlkružnice t nad průměrem AB. Přímka p kolmá na AB protíná úsečku AB v bodě C a půlkružnici t v bodě D. Kružnice k se dotýká úsečky AC v bodě E, půlkružnice t v bodě T a navíc přímky p. Dokažte, že DE půlí úhel ADC. (Izrael 1995)

Příklad 8. Dvojice kružnic k_1 a k_2, k_2 a k_3 a k_3 a k_1 mají postupně vnější dotyk v bodech K_3, K_1, K_2. Navíc mají k_1, k_2, k_3 postupně vnitřní dotyk z kružnicí m v bodech M_1, M_2, M_3. Dokažte, že přímky K_1M_1, K_2M_2, K_3M_3 procházejí jedním bodem.

Příklad 9. Kružnice k, l se protínají v bodech A, D. Jejich společná tečna bližší bodu A se dotýká k v E a l v F. Rovnoběžka s touto tečnou procházející bodem D protne kružnice k, l podruhé v bodech C, B. Kružnice opsané trojúhelníkům CDF a BDE se podruhé protínají v bodě P. Ukažte, že body D, A, P leží v přímce. (Brkos 2011)

Divné podmínky

Indikátorem toho, že budeme chtít invertovat, jsou i divné podmínky. Často se totiž do „rozumného“ tvaru přeloží v současném zadání nepřirozeně vyhlížející vztah o velikostech úhlů nebo délkách (máme na paměti *Přepočítávací lemma*), nebo vyjdou najevo významy některých umělých konstrukcí.

Příklad 10. Kružnice k_1 a k_3 stejně jako k_2 a k_4 mají vnější dotyk v P. Označme druhé průsečíky $k_1 \cap k_2 = A$, $k_2 \cap k_3 = B$, $k_3 \cap k_4 = C$ a $k_4 \cap k_1 = D$. Dokažte, že

$$\frac{|AB| \cdot |BC|}{|AD| \cdot |DC|} = \frac{|PB|^2}{|PD|^2}.$$

(IMO shortlist 2003)

Příklad 11. Bod P uvnitř trojúhelníka ABC splňuje

$$|\sphericalangle APB| - |\sphericalangle ACB| = |\sphericalangle APC| - |\sphericalangle ABC|.$$

Označme D, E středy kružnic vepsaných trojúhelníkům APB, APC. Dokažte, že přímky AP, BD, CE procházejí jedním bodem. (IMO 1996)

Příklad 12. (Ptolemaiova věta) Dokažte, že ve čtyřúhelníku $ABCD$ se standardně značnými délkami stran a úhlopříček platí

$$ac + bd \geq ef,$$

přičemž rovnost nastává právě tehdy, když je čtyřúhelník $ABCD$ tětivový.

Příklad 13. Je dán trojúhelník ABC. Označme polovinu jeho obvodu s. Na přímce AB nalezneme body E, F tak, že $|CE| = |CF| = s$. Dokažte, že kružnice opsaná trojúhelníku CEF se dotýká kružnice připsané trojúhelníku ABC vzhledem k vrcholu C.

Příklad 14. Nechť je dán trojúhelník ABC. Označme S střed jemu vepsané kružnice l a označme P, Q, R dotykové body kružnice l po řadě se stranami BC, AC, AB. Buď k kružnice opsaná středům stran trojúhelníku PQR. Buď $X \neq C$ průsečík přímky CS a kružnice opsané trojúhelníku ABC, buď Y průsečík úsečky SX a kružnice k. Buď Z jeden z průsečíků kružnice l a kolmice k přímce CX vedené bodem Y. Dokažte, že přímka XZ se dotýká kružnice l. (PraSe)

Dominantní úhel

Mnohdy je užitečné invertovat podle vrcholu dominantního úhlu, pokud úloha takový má.

Příklad 15. Je dán trojúhelník ABC. Uvažme kružnici l, která se dotýká stran AB, AC a navíc jeho kružnice opsané v bodě T. Označme ještě D bod dotyku kružnice připsané trojúhelníku ABC vzhledem k vrcholu A se stranou BC. Ukažte, že $|\sphericalangle BAD| = |\sphericalangle CAT|$.

Příklad 16. Na stranách AB, AC trojúhelníka ABC zvolme body K, L tak, aby $KL \| BC$ a buď $P = AL \cap BK$. Označme Q druhý průsečík kružnic opsaných trojúhelníkům BPK a CPL. Dokažte, že $|\sphericalangle BAP| = |\sphericalangle CAQ|$.

(Balkan MO 2009)

Zvol si poloměr!

V předchozích úlohách stačilo odhalit střed inverze a aplikovat inverzi s libovolným poloměrem. U následujících úloh je již potřeba zvolit i vhodný poloměr – tedy invertovat podle nějaké konkrétní kružnice.

Příklad 17. Na půlkružnici nad průměrem AB a se středem O zvolíme body C, D. Předpokládejme, že se polopřímky AB a DC protnou v bodě M. Označme K druhý průsečík kružnic opsaných trojúhelníkům AOD a BOC. Ukažte, že $|\sphericalangle MKO| = 90°$.

(Rusko 1995)

Příklad 18. Ukažte, že Feuerbachova kružnice[23] trojúhelníka ABC se dotýká jeho kružnice vepsané i všech jeho kružnic připsaných.

Příklad 19. Označme M, N, P body dotyku kružnice vepsané trojúhelníka ABC postupně se stranami BC, CA, AB. Dokažte, že ortocentrum trojúhelníka MNP, střed I kružnice vepsané trojúhelníku ABC a střed O kružnice trojúhelníku ABC opsané leží v přímce. (Írán 1995)

Příklad 20. (Steinerův porismus) Uvnitř kružnice k je dána kružnice l. Předpokládejme, že existuje n-prvkový řetěz kružnic $m_1, \ldots, m_n$ takový, že každá kružnice v řetězu má vnější dotyk se svými dvěma sousedními kružnicemi a s l a vnitřní dotyk s k. Potom každá kružnice mající vnější dotyk s l a vnitřní dotyk s k je částí nějakého n-prvkového řetězu.

Příklad 21. Je dán trojúhelník ABC. Body D, E leží na přímce AB v pořadí D, A, B, E tak, že $|AD| = |AC|$ a $|BE| = |BC|$. Osy úhlů u vrcholů A a B protnou strany BC a AC po řadě v bodech P, Q a kružnici opsanou trojúhelníku ABC v bodech M, N. Označme U, V středy kružnic opsaných trojúhelníkům BME, AND. Konečně buď $X = AU \cap BV$. Dokažte, že $CX \perp PQ$. (Srbsko TST 2008)

Stručné návody

Návod k příkladu 1. Uvažte inverzi se středem $\check{S}$, která zobrazí p na k a všimněte si, že body C, D přejdou na body A, B.

Návod k příkladu 2. Uvažte inverzi podle kružnice opsané trojúhelníku tvořenému body dotyku kružnic k_1, k_2, k_3 a všimněte si, že tyto kružnice se v inverzi zachovají. Kružnice l, m se tedy prohodí. Společným průsečíkem je střed inverze.

Návod k příkladu 4. Invertujte podle T a dokazujte $|uhelV'X'T| = 90°$.

Návod k příkladu 5. Invertujte podle C. Obrazy pat výšek interpretujte jako průsečíky kružnic nad průměry CA, CB, CD, CE; tyto tvoří obdélník.

Návod k příkladu 6. Invertujte podle D. Zobrazte nejdříve body A a B a obě kružnice. Rozmyslete si, že obraz $EFYZ$ je obdélník.

Návod k příkladu 7. Invertujte podle E. Dokazované tvrzení přejde v to, že je jistý trojúhelník rovnoramenný.

Návod k příkladu 8. Invertujte podle některého z bodů dotyku. Dva ze tří bodů, které budou mět ležet v přímce, určují chordálu jistých dvou kružnic. Ukažte, že třetí bod má k oběma stejnou mocnost.

Návod k příkladu 9. Invertujte podle D a rozpoznejte trojúhelník s Gergonnovým bodem.

[23] Feuerbachova kružnice je kružnice procházející středy stran a patami výšek trojúhelníka.

Návod k příkladu 10. Invertujte podle P. Přepočtěte dokazovaný vztah a využijte tho, že v rovnoběžníku mají protější strany shodnou délku.

Návod k příkladu 11. Invertujte podle A nebo P. Využijte, že osa úhlu dělí protější stranu ve známém poměru, tyto poměry dejte do rovnosti a přepočtěte. Vyjde, že jistý trojúhelník má být rovnoramenný, což je díky přepočtení zadané úhlové podmínky.

Návod k příkladu 12. Invertujte podle jednoho z vrcholů. Ptolemaiova nerovnost je „obrazem“ trojúhelníkové nerovnosti.

Návod k příkladu 13. Invertujte podle C s poloměrem s. Všimněte si, že na této kružnici leží i body dotyku kružnice připsané s prodlouženími stran CA, CB.

Návod k příkladu 14. Invertujte podle kružnice vepsané torjúhelníku ABC.

Návod k příkladu 15. Invertujte podle A. Kružnice l přejde v přímku antirovnoběžnou se stranou BC. Dokončete uvážením osové souměrnosti podle osy úhlu BAC.

Návod k příkladu 16. Rozpoznejte Q jako Miquelův bod čtyřúhelníka $AKPL$ a dokreslete kružnice $ABQL$ a $AKQC$. Invertujte podle A.

Návod k příkladu 17. Invertujte podle zadané půlkružnice a rozpoznejte obrázek s ortocentrem a Feuerbachovou kružnicí.

Návod k příkladu 18. Invertujte podle kružnice se středem ve středu strany a poloměrem po body dotyku s vepsanou a připsanou kružnicí. Uvědomte si, že vepsaná i připsaná se zachovají a ukažte, že obrazem Feuerbachovy kružnice bude jejich druhá společně vnitřní tečna (spočtěte jednak její úhel se stranou, druhak pozici průsečíku).

Návod k příkladu 19. Invertujte podle vepsané kružnice. Uvědomte si, že obrazem kružnice opsané $\triangle ABC$ je Feuerbachova kružnice $\triangle MNP$ a vzpomeňte na Eulerovu přímku.

Návod k příkladu 20. Invertujte tak, aby kružnice k, l přešly v soustředné kružnice. Pak je tvrzení zřejmé.

Návod k příkladu 21. Invertujte podle A s poloměrem $\sqrt{bc}$ a interpretujte přímku AU jako obraz přímky AO (kde O je střed opsané trojúhelníku CPQ) v osové souměrnosti podle osy úhlu u vrcholu A. Totéž proveďte s B a vzpomeňte na to, že střed opsané a ortocentrum jsou isogonal conjugates.

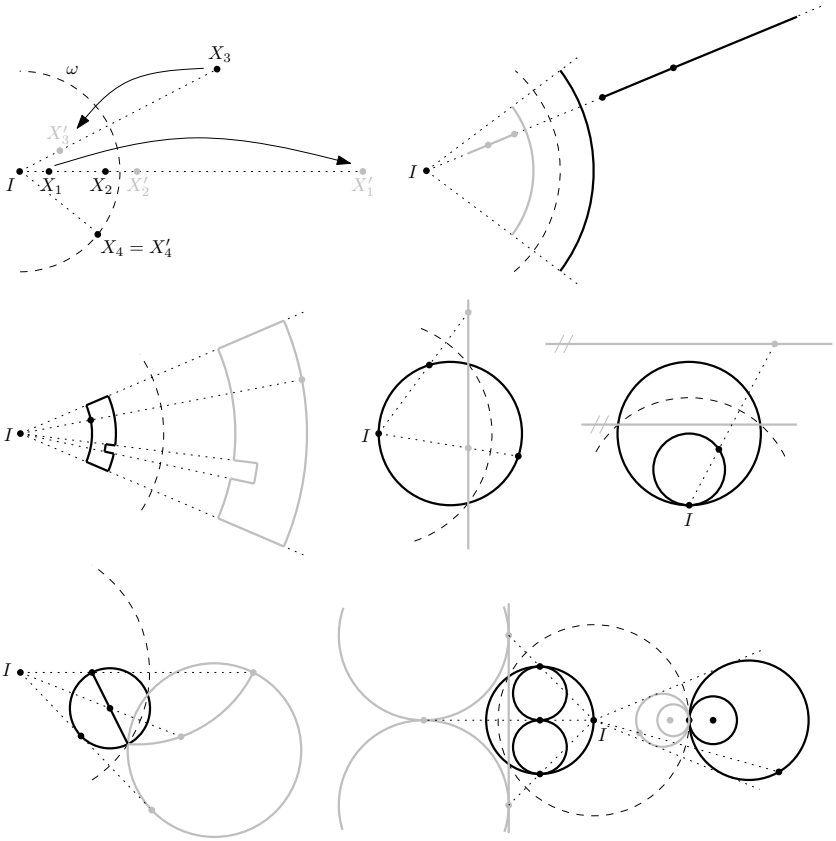
Literatura

Při tvorbě příspěvku jsem čerpal ze starších příspěvků Michala „Kennyho“ Rolínka a Martina Tancera, jimž bych tímto rád poděkoval, a z

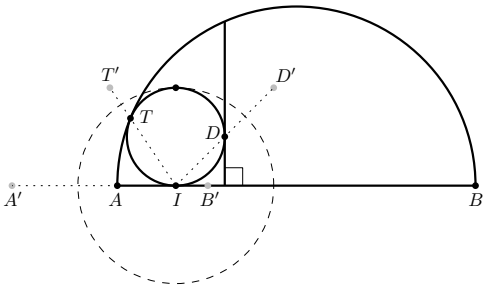
[1] *Mathlinks*, *http://www.mathlinks.ro*
[2] *Zadači*, *problems.ru*
[3] Archiv MKS, *http://mks.mff.cuni.cz/archive*

Obrázková příloha

Na ukázku:



A na procvičení:



Švrčkův bod

Martina Vaváčková

Abstrakt. Přednáška shrnuje základní vlastnosti středu oblouku, tzv. Švrčkova bodu. Tento bod figuruje v mnoha geometrických úlohách, a jeho dobrá znalost je tedy pro úspěch při řešení velmi užitečná. To vše ilustruje řada příkladů.

Středem pozornosti naší přednášky bude Švrčkův bod. Podíváme se na něj zblízka a všimneme si některých jeho zajímavých vlastností. Zformulujeme a dokážeme pár užitečných tvrzení, která pak prakticky využijeme při řešení úloh.

Definice a značení

Definice. Nechť je trojúhelník ABC vepsaný do kružnice ω. Střed oblouku BC, který neobsahuje A, označme $\check{S}_a$ a říkejme mu *Švrčkův bod* trojúhelníka ABC vzhledem k A. Body $\check{S}_b$, $\check{S}_c$ definujme analogicky.

Značení. V trojúhelníku ABC označme ω kružnici opsanou, I střed kružnice vepsané, $\check{S}_a$, $\check{S}_b$, $\check{S}_c$ odpovídající Švrčkovy body, E_a, E_b, E_c odpovídající středy kružnic připsaných a konečně AD, BE, CF osy úhlů v $\triangle ABC$, kde $D \in BC$, $E \in AC$, $F \in AB$.

Základní vlastnosti

Tvrzení 1. *V trojúhelníku ABC se osa úhlu BAC a osa strany BC protínají na kružnici ω. Jejich průsečíkem je $\check{S}_a$.*

Tvrzení 2. *Body B, C, I, E_a leží na jedné kružnici se středem $\check{S}_a$. Platí tedy $|\check{S}_a I| = |\check{S}_a B| = |\check{S}_a C| = |\check{S}_a E_a|$.*

Tvrzení 3. *Bodem $\check{S}_a$ veďme polopřímky p a q, které protnou stranu BC postupně v bodech X a Y a kružnici ω protnou podruhé postupně v Z a W. Pak body X, Y, Z, W leží na jedné kružnici.*

Tvrzení 4. *V trojúhelníku ABC platí $|\check{S}_a D| \cdot |\check{S}_a A| = |\check{S}_a I|^2 = |\check{S}_a C|^2 = |\check{S}_a B|^2$.*

Klíčová slova. planimetrie, trojúhelník, geometrie, Švrčkův bod, osa úhlu, kružnice opsaná

Tvrzení 5. *Nechť X je bod na úsečce AD. Pak jsou následující tvrzení ekvivalentní:*

(i) $X = I$.
(ii) $|\check{S}_a X| = |\check{S}_a I|$.
(iii) $|\check{S}_a D| \cdot |\check{S}_a A| = |\check{S}_a X|^2$.

Tvrzení 6. *Je dán trojúhelník ABC a kružnice ω_1, která má vnitřní dotyk s kružnicí ω v bodě A a se stranou BC v bodě D'. Pak $D = D'$.*

Příklady

Příklad 1. Je dán trojúhelník ABC se středem kružnice vepsané I a vnitřním bodem P. Platí

$$\sphericalangle PBA + \sphericalangle PCA = \sphericalangle PBC + \sphericalangle PCB.$$

Ukažte, že $|AP| \geq |AI|$, přičemž rovnost nastává, právě když $P = I$. (IMO 2006)

Příklad 2. 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 3. 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 4. Nechť jsou AL a BK osy úhlů nerovnoramenného trojúhelníka 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 5. V trojúhelníku ABC dokažte při zavedeném značení následující metrické vztahy:

(i) $|A\check{S}_a| \cdot |ID| = |\check{S}_a I| \cdot |AI|$,
(ii) $|A\check{S}_a| \cdot |AD| = |AI| \cdot |AE_a| = |AB| \cdot |AC|$,
(iii) $|IA| \cdot |E_a D| = |E_a A| \cdot |ID|$.

Příklad 6. Nechť ABC je ostroúhlý trojúhelník ($|AB| \neq |AC|$). 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 7. Trojúhelník ABC splňuje vztah $|AC| + |BC| = 3|AB|$. 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 8. 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 9. 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 10. Je dán trojúhelník ABC, jeho kružnice ospaná ω a bod D na straně BC. Buď ω_1 kružnice dotýkající se úsečky AD v bodě F, strany BC 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)

Literatura a zdroje

[1] Michal Rolínek, Josef Tkadlec: *The Š point*, *www.onlinemathcircle.com*.

Obsah