Paseky

Sborník, podzim 2018

Filip Bialas
Tonda Češík
Petr Gebauer
Verča Hladíková
Honza Kadlec
Daniil Koževnikov
Jakub Löwit
Viki Němeček
Tomáš Novotný
Hedvika Ranošová
Lucien Šíma
Jáchym Solecký
Rado van Švarc
Michal Töpfer
Pavel Turek

Autoři: Filip Bialas, Tonda Češík, Petr Gebauer, Verča Hladíková, Honza Kadlec, Danil Koževnikov, Jakub Löwit, Viki Němeček, Tomáš Novotný, Hedvika Ranošová, Lucien Šíma, Jáchym Solecký, Rado van Švarc, Michal Töpfer, Pavel Turek
Editoři: Viki Němeček a Michal Töpfer
vydání první, náklad 45 výtisků
září 2018
Díky za pomoc všem, kterým je za co děkovat.

Pravděpodobnostní metoda

Filip Bialas

Abstrakt. Pravděpodobnostní metoda je způsob důkazu existence kombinatorických objektů „počítáním“. Navíc pro mnoho důležitých objektů je to jediný známý důkaz. Použití pravděpodobnosti nám oproti počítání možností nejen výpočet zjednoduší, ale poskytne nám i pokročilejší techniky, jak potřebné odhady dokázat.

Pravděpodobnostní metodu používáme hlavně pro důkaz existence nějakých matematických objektů. Místo snahy o jejich konstrukci (která mnohdy ani není známá) se pokusíme zjistit, s jakou pravděpodobností daný objekt najdeme – a pokud je nenulová, už z toho plyne jeho existence.

Definice. *Elementárním jevem* nazýváme kompletní situaci, která nastala po náhodném procesu, tedy například: „Na první kostce padla trojka, na druhé dvojka a na třetí trojka.“ *Jevem* pak nazýváme nějakou vlastnost takové situace, například: „Na první kostce padlo sudé číslo.“ Pravděpodobnost, že jev A nastal, značíme $P(A)$. Symbolem $A \cap B$ značíme, že nastal jev A a současně nastal jev B, a $A \cup B$ značí, že nastal jev A nebo nastal jev B. *Nezávislé jevy* jsou takové, pro které platí $P(A \cap B) = P(A) \cdot P(B)$.

Tvrzení. (Union bound) *Nechť $A_1, A_2, \dots A_n$ jsou jevy (nemusí být nezávislé). Pak*

$$P\left(\bigcup_{i=1}^{n} A_i\right) \leq \sum_{i=1}^{n} P(A_i).$$

Příklad 1. V jazykové škole se vyučuje $2n$ jazyků. Každý z 500 místních učitelů umí mluvit alespoň n jazyky. Dokažte, že najdeme 14 nebo méně jazyků tak, aby každý učitel mluvil alespoň jedním z nich.

Řešení. Zvolme si náhodnou 14-tici jazyků (uspořádanou, jazyky se můžou opakovat) a pevného učitele. Pravděpodobnost, že tento učitel nezná první jazyk, je nejvýše $1/2$, stejně tak u druhého jazyku atd. Celkem je tedy pravděpodobnost, že tento učitel nezná ani jeden ze 14 jazyků, rovna 2^{-14}. Za pomoci tvrzení výše získáváme, že pravděpodobnost, že alespoň jeden učitel nezná ani jeden z těchto 14 jazyků, je nejvýše $500 \cdot 2^{-14}$. Tedy pravděpodobnost, že všichni učitelé znají alespoň jeden z těchto 14 jazyků, je $1 - (500 \cdot 2^{-14}) > 0$. A nyní přichází klíčová myšlenka pravděpodobnostní metody: Má-li jev nenulovou pravděpodobnost, může

nastat. Tedy opravdu existuje 14-tice jazyků taková, že každý učitel mluví alespoň jedním z nich.

Příklad 2. Jsou dána nesoudělná přirozená čísla m, n. Jaký je počet cest po mřížce v obdélníku $m \times n$ z levého dolního rohu do pravého horního, které vedou jen doprava a nahoru a jsou celé pod úhlopříčkou? (MKS 26–5)

Příklad 3. Ve skupině 90 dětí má každé alespoň 30 kamarádů (kamarádství je vzájemné). Dokažte, že lze děti rozdělit do tří 30členných skupin tak, aby každé dítě mělo ve své skupince alespoň jednoho kamaráda. (MO 61–III)

Příklad 4. Matematické soutěže se účastnilo 200 studentů, každý z nich řešil šest úloh. Je známo, že každou úlohu správně vyřešilo alespoň 120 studentů. Dokažte, že můžeme najít dva studenty, kteří dohromady vyřešili všechny úlohy. (IMC 2002)

Příklad 5. Ukažte, že je možné obarvit prvky množiny $\{1, 2, \ldots, 1987\}$ čtyřmi barvami tak, aby neexistovala jednobarevná desetiprvková aritmetická posloupnost. (IMO 1987)

Příklad 6. V rovině je dáno 100 bodů v obecné poloze. Dokažte, že počet ostroúhlých trojúhelníků nepřekračuje 70 % počtu všech trojúhelníků. (IMO 1970)

Příklad 7. (Dolní odhad na Ramseyova čísla) Dokažte, že hrany úplného grafu na $2^{k/2}$ vrcholech je možné obarvit dvěma barvami tak, aby v nich nebyl žádný úplný jednobarevný podgraf na k vrcholech.

Příklad 8. V tabulce 100×100 jsou napsaná čísla $1, 2, \ldots, 5000$, každé právě dvakrát. Dokažte, že je možné vybrat 100 čísel tak, že z každého sloupce a z každého řádku vybereme právě jedno číslo, a navíc budou tato čísla různá.

Střední hodnota

Definice. *Náhodná veličina* je reálné číslo, které spočteme na základě elementárního jevu, tedy například: „Číslo, které padlo na první kostce.“ nebo: „Počet kostek, na kterých padla trojka.“

Definice. *Střední hodnota* náhodné veličiny X je její průměrná hodnota a značí se $E(X)$. Přesněji je $E(X)$ vážený aritmetický průměr přes všechny hodnoty X na elementárních jevech, kde váhy jsou pravděpodobnosti těchto jevů.

Tvrzení. (Počítání střední hodnoty)

(1) *Buď A jev a I_A náhodná veličina, která dává nulu resp. jedničku, pokud A nastal resp. nenastal. Pak $E(I_A) = P(A)$.*

(2) *Nechť X, Y jsou náhodné veličiny, pak $E(X + Y) = E(X) + E(Y)$.*

(3) *Nechť X je náhodná veličina a r reálné číslo, pak $E(r \cdot X) = r \cdot E(X)$.*

Pozor! Další zobecnění tohoto tvrzení, jako například $E(X \cdot Y) = E(X) \cdot E(Y)$, již obecně neplatí.

Tvrzení 9. (Použití střední hodnoty) *Buď X náhodná veličina. Pak existuje elementární jev, pro který platí $X \leq E(X)$, a také jiný elementární jev, pro který platí $X \geq E(X)$.*

Příklad 10. Nechť F je množina všech n-tic $(A_1, A_2, \ldots, A_n)$, kde každé A_i je podmnožinou $\{1, 2, \ldots, 1998\}$. Označme $|A|$ počet prvků množiny A. Najděte hodnotu

$$\sum_{(A_1,A_2,\ldots,A_n)\in F} |A_1 \cup A_2 \cup \cdots \cup A_n|.$$

(APMO 1998)

Příklad 11. V šachovém turnaji, kterého se zúčastnilo 40 hráčů, se odehrálo celkem 80 partií, přičemž žádná dvojice spolu nehrála víckrát. Ukažte pro co největší n, že existuje n hráčů, kteří mezi sebou nesehráli žádný zápas.

Příklad 12. V soutěži je a soutěžících a b porotců, kde $b \geq 3$ je liché číslo. Každý porotce hodnotí každého soutěžícího buď jako „dobrý“, nebo jako „špatný“. Předpokládejme, že k je takové číslo, že pro libovolnou dvojici porotců se jejich hlasy shodovaly u nejvýše k soutěžících. Dokažte nerovnost $k/a \geq (b-1)/(2b)$.

(IMO 1998)

Příklad 13. V turnaji n hráčů hrál každý s každým právě jednou. Hamiltonovská cesta je takové uspořádání n hráčů, že první porazil druhého, druhý třetího atd. Dokažte, že turnaj mohl dopadnout tak, že existovalo alespoň $n!/2^{n-1}$ hamiltonovských cest.

Příklad 14. Na večírku je $n \geq 2$ lidí, někteří se znají (vztah znát se je vzájemný). Dokažte, že existují dva lidé A, B takoví, že mezi zbylými $n-2$ najdeme $\left\lfloor \frac{n}{2} \right\rfloor - 1$ lidí, z nichž každý buď zná A i B, nebo oba nezná.

Příklad 15. Mějme graf G s n vrcholy a $m \geq 4n$ hranami. Dokažte, že kdykoli takový graf nakreslíme do roviny, bude obsahovat alespoň $m^3/(64n^2)$ průsečíků.

Návody

3. Spočítejte s jakou maximální pravděpodobnostní se stane, že dané dítě nemá ve své skupince žádného kamaráda.

4. Zvolte náhodně dvojici studentů a spočítejte, s jakou pravděpodobnostní ani jeden z této dvojice nevyřeší danou úlohu.

5. Zvolte náhodně obarvení. S jakou pravděpodobností bude jedna vybraná aritmetická posloupnost jednobarevná?

6. Mezi pěti body v obecné poloze vždy existují alespoň 3 tupoúhlé trojúhelníky.

7. Vyberte náhodný graf. Jaká je pravděpodobnost, že na daných k vrcholech je jednobarevný podgraf?

8. Vyberte náhodně z každého sloupce a řádku právě jedno číslo. Jaká je pravděpodobnost toho, že vyberete číslo i dvakrát?

10. Vyberte náhodnou n-tici podmnožin. S jakou pravděpodobností se objeví číslo i ve sjednocení?

12. S jakou minimální pravděpodobností se dva porotci shodují na jednom určeném soutěžícím?

13. Vyberte náhodný graf a následně náhodnou permutaci hráčů. Jaká je pravděpodobnost, že v této permutaci tvoří hamiltonovskou cestu?

14. Řešte podobně jako příklad 12.

15. Použijte Eulerův vzorec, vyberte libovolné nakreslení a následně s pevně zvolenou pravděpodobností smažte každý z vrcholů.

Literatura a zdroje

Tento příspěvek je beze změn převzat od Martina Töpfera, který jej vytvořil na soustředění ve Skleném (2015) a kterému tímto děkuji.

[1] Mirek Olšák: *Od Dirichleta k pravděpodobnosti*, sborník *i*KS 2012
[2] Law Ka Ho: *Probabilistic Method*, Mathematical Excalibur, 2009
[3] Sourav Chakraborty: *Probabilistic method*, lecture notes

Vieta Jumping

Filip Bialas

Abstrakt. Příspěvek se zabývá metodou řešení diofantických rovnic využívající nekonečný sestup v kombinaci s Viètovými vztahy.

Viètovy vztahy

Kvadratickou rovnicí rozumíme rovnici tvaru

$$ax^2 + bx + c = 0.$$

Jsou-li x_1 a x_2 řešení výše uvedené rovnice, pak můžeme rovnici vyjádřit následujícím způsobem:

$$a(x - x_1)(x - x_2) = 0.$$

Po roznásobení dostaneme vztahy mezi koeficienty a, b, c a kořeny x_1, x_2, které nazýváme Viètovy vztahy:

$$x_1 + x_2 = -b/a,$$

$$x_1 x_2 = c/a.$$

Nekonečný sestup

V přirozených číslech neexistuje nekonečná klesající posloupnost. Toto tvrzení se dá používat k důkazům neexistence řešení diofantických rovnic pomocí následující úvahy: Pokud by řešení existovalo, pak existuje i menší řešení, a kvůli němu i další menší řešení, atd. A když tímto způsobem sestrojíme nekonečnou klesající posloupnost přirozených čísel, dojdeme ke sporu.

Ekvivalentně můžeme tuto myšlenku formulovat tak, že si pro spor vezmeme „nejmenší“ řešení a dokážeme, že existuje ještě menší.

Příklad. Ukaž, že rovnice

$$x^3 + 2y^3 = 4z^3$$

nemá žádné řešení v oboru přirozených čísel.

Příklady

Příklad 1. Pro přirozená čísla a, b platí, že a^2+b^2 je dělitelné $ab+1$. Dokaž, že

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

je čtverec. (IMO 1988, př. 6)

Příklad 2. Přirozená čísla x, y, z splňují

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

Dokaž, že $z=3$.

Příklad 3. Buďte a, b přirozená čísla. Ukaž, že pokud $(4a^2-1)^2$ je dělitelné $4ab-1$, pak $a=b$. (IMO 2007, př. 5)

Příklad 4. Najdi všechny dvojice přirozených čísel m, n splňující

$$\frac{m}{n}+\frac{n}{m}\in\mathbb{N}.$$

Příklad 5. Ukaž, že ke každému přirozenému číslu m lze najít nekonečně mnoho dvojic celých čísel (x,y) takových, že

(i) x, y jsou nesoudělná,
(ii) $x \mid y^2+m$,
(iii) $y \mid x^2+m$. (IMO shortlist 1992)

Příklad 6. Najděte všechny dvojice monických komplexních polynomů $P(x), Q(x)$ takové, že

(i) $P(x) \mid Q(x)^2+1$,
(ii) $Q(x) \mid P(x)^2+1$. (IMC 2018)

Příklad 7. Přirozená čísla a, b, c splňují

$$0<a^2+b^2-abc\leq c.$$

Dokaž, že a^2+b^2-abc je čtverec. (CRUX)

Příklad 8. Zjisti, pro která $n\in\mathbb{N}$ má rovnice

$$w+x+y+z=n\sqrt{wxyz}$$

řešení v přirozených číslech. (Vietnam 2002)

Příklad 9. Zjisti, pro která $n\in\mathbb{N}$ má rovnice

$$x^2+y^2+x+y=nxy$$

řešení v přirozených číslech. (Vietnam 2002)

Literatura a zdroje

Tento příspěvek je s pouze malými změnami převzat od Tondy Le, který jej vytvořil na soustředění ve Starém Městě (2015) a kterému tímto děkuji.

[1] Yimin Ge: *The Method of Vieta-Jumping*, *www.yimin-ge.com/doc/VietaJumping.pdf*
[2] *www.mathlinks.ro/viewtopic.php?p=2192633#p2192633*
[3] Alča Skálová, *Vieta jumping*, 2011 Hojsova Stráž.

Banachův–Tarského paradox

Tonda Češík

Abstrakt. Banachův–Tarského paradox je na první pohled zcela neintuitivní tvrzení: Kouli lze rozdělit na konečně mnoho dílů, tyto díly přeskládat a získat tak dvě koule, stejně velké jako ta původní. V příspěvku se nejprve podíváme na to, kde naše intuice selhala. Poté si v sérii několika kroků paradox dokážeme.

V roce 1924 dokázali Stefan Banach a Alfred Tarski větu říkající, že kouli lze „rozřezat“ a „přeskládat“ na dvě koule shodné s tou původní. Tato věta je tradičně označována jako „paradox“, protože zcela odporuje naší geometrické intuici ve starém známém Eukleidovském prostoru $\mathbb{R}^3$. Opírá se totiž o existenci množin, které si jen těžko umíme představit.

Nyní si tuto větu korektně zformulujme.

Definice. Dvě množiny $A, B \subset \mathbb{R}^3$ jsou *ekvirozložitelné*, pokud existují disjunktní množiny $A_1, \ldots, A_n$ splňující $A_1 \cup \cdots \cup A_n = A$ a disjunktní množiny $B_1, \ldots, B_n$ splňující $B_1 \cup \cdots \cup B_n = B$ takové, že A_i je shodná s B_i, $i = 1, \ldots, n$.

Věta. (Banach–Tarski) *Jednotková koule v $\mathbb{R}^3$ je ekvirozložitelná se dvěma jednotkovými koulemi.*

Existuje i silnější verze věty, která pokrývá mnohem více různých množin, než jsou jen koule.

Věta. (Banach–Tarski, silnější verze) *Každé dvě množiny $A, B \subset \mathbb{R}^3$, které jsou omezené*[1] *a mají neprázdný vnitřek*[2]*, jsou ekvirozložitelné.*

Co je na tom tak divného? Zřejmě to, že na začátku máme množinu s nějakým objemem, provedeme s ní pár operací a získáme množinu s dvojnásobným objemem. Přitom shodná zobrazení objem zachovávají. Ve skutečnosti Banachův–Tarského paradox ukazuje, že ne všechny množiny v $\mathbb{R}^3$ mají objem. Přesněji:

Důsledek. *V $\mathbb{R}^3$ neexistuje „univerzální objem“, tedy funkce μ, která by každé množině přiřadila nezáporné reálné číslo či ∞, jednotkové krychli by přiřadila* 1,

[1] Množina je *omezená*, pokud je obsažena v nějaké kouli.

[2] Množina má *neprázdný vnitřek*, pokud obsahuje nějakou kouli.

při shodných zobrazeních by neměnila hodnotu a pro každé dvě disjunktní množiny $A, B \subseteq \mathbb{R}^3$ *by platilo* $\mu(A \cup B) = \mu(A) + \mu(B)$.[3]

Na rozehřátí si ukážeme jednodušší tvrzení, které se bude i při důkazu samotného Banachova–Tarského paradoxu hodit.

Tvrzení. *Kružnice je ekvirozložitelná s kružnicí bez jednoho bodu.*

Schéma důkazu

Samotný důkaz Banachova–Tarského paradoxu povedeme v několika krocích:

(1) Vezmeme si tzv. *volnou grupu generovanou dvěma prvky* a rozdělíme ji na čtyři části tak, že z dvojic částí dokážeme „posunutím“ sestavit dvě kopie původní grupy. (V tom to celé věží!)
(2) Prvky grupy interpretujeme jako rotace v prostoru. Díky tomu provedeme na sféře (tzn. povrchu koule), ze které vyhodíme některé body, rozklad na čtyři části analogický tomu na grupě.
(3) Ukážeme, že vyhození bodů ze sféry nám nevadí, a dokážeme tak Banacha–Tarského pro sféru.
(4) Kouli rozdělíme na sféry a se středem koule se vypořádáme zvlášť.

Krok (1): rozklad volné grupy F_2

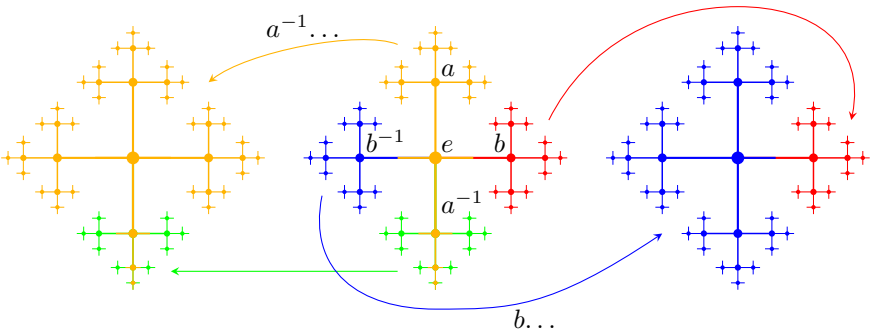
Definice. *Volná grupa generovaná dvěma prvky* je množina všech (konečných) slov skládajících se z „písmen“ a, b, a^{-1}, b^{-1}, přičemž a a a^{-1}, resp. b a b^{-1}, se v těchto slovech nesmí vyskytovat za sebou; navíc obsahuje prázdné slovo e. Tuto grupu značíme F_2. Prvky F_2 lze skládat tak, že příslušná slova napíšeme za sebe[4] a případná zakázaná podslova vyškrtneme[5].

Grupu si lze nakreslit jako uprostřed na obrázku jako větvící se strom. Uprostřed je prázdné slovo, přidáním a, resp. b, resp. a^{-1}, resp. b^{-1}, se posuneme nahoru, resp. doprava, resp. dolů, resp. doleva. Na obrázku je vyznačený náš rozklad F_2.

[3] Tento problém naštěstí není až tak palčivý, jak by se mohlo zdát – s uvedenými patologickými případy se v „praxi“ téměř nikdy nesetkáváme, takže pokud se smíříme s jistými nepříliš striktními omezeními na množiny, u kterých chceme měřit objem (tzv. měřitelné množiny), můžeme takovouto μ sestrojit.

[4] Pokud je jedním z těchto slov e, jednoduše místo něj nic nenapíšeme.

[5] Pokud po vyškrtnutí vzniknou nová zakázaná podslova, pokračujeme ve škrtání. Pokud po vyškrtání nic nezbyde, jde o prázdné slovo e.



Náš rozklad jsou tedy množiny
$F_b = \{\text{slova začínající symbolem } b\}$,
$F_{b^{-1}} = \{\text{slova začínající symbolem } b^{-1}\}$,
$F_a = \{\text{slova začínající symbolem } a\} \cup \{e, a^{-1}, a^{-1}a^{-1}, a^{-1}a^{-1}a^{-1}, \dots\}$,
$F_{a^{-1}} = F_2 \setminus (F_b \cup F_{b^{-1}} \cup F_a)$.
Potom $a^{-1}F_a \cup F_{a^{-1}} = F_2$, a zároveň i $b^{-1}F_b \cup F_{b^{-1}} = F_2$.

Krok (2): F_2 jako grupa rotací a rozklad sféry bez pár bodů

Definice. Označme jako[6] $SO(3)$ množinu všech rotací v $\mathbb{R}^3$ okolo počátku.

Tvrzení. *$SO(3)$ je grupa. Neboli obsahuje identitu, každá rotace ρ má inverzní rotaci ρ^{-1} a složení dvou rotací ρ, σ je opět rotace $\sigma \circ \rho$.*

Tvrzení. *$SO(3)$ obsahuje volnou grupu generovanou dvěma prvky. Neboli existují dvě nezávislé rotace $a, b \in SO(3)$, tedy takové, že pokud složením rotací a, b, a^{-1}, b^{-1} dostaneme identitu, pak slovo odpovídající tomuto složení dá po zkrácení prázdné slovo.*

Je mnoho různých pro naše účely vyhovujících dvojic a a b. Například můžeme zvolit a jako otočení o úhel $\alpha = \arccos \frac{3}{5}$ kolem osy y , b jako otočení o úhel α kolem osy z.

Jednotkovou sféru (tj. povrch jednotkové koule) se středem v počátku budeme značit symbolem S.

Nyní chceme náš „paradoxní“ rozklad grupy F_2 přenést na rozklad sféry. Body, které nějaká rotace nechá na místě, nám v tom však budou dělat nepořádek. Proto na ně prozatím zapomeneme: označme $D = \{x \in S; \exists \varphi \in F_2 : \varphi(x) = x\}$.

Definice. Pro bod $x \in S \setminus D$ definujeme jeho *orbitu* $O_x = \{y \in S; \exists \varphi \in F_2 : \varphi(x) = y\}$ (Tj. všechny body, do kterých se z x dá dostat pomocí rotace z F_2. Všimněme si, že do bodů z D se dostat nedá.)

[6] K označení: S značí speciální, O ortogonální, 3 je dimenze prostoru.

Pozorování. *Orbity tvoří rozklad $S \setminus D$. Neboli pro $x, y \in S \setminus D$ je buď $O_x = O_y$, nebo $O_x \cap O_y = \emptyset$.*

Nyní zvolme T jako *výběrovou množinu* pro $\{O_x : x \in S \setminus D\}$, neboli z každé orbity dáme do T právě jeden bod. (Zde jsme použili axiom výběru!)

Každá orbita teď „vypadá stejně“ jako F_2 (díky tomu, že jsme vynechali D), proto sféru můžeme rozložit takto:

$$\begin{aligned} S_a &= \{\varphi(t) : t \in T, \varphi \in F_a\}, \\ S_{a^{-1}} &= \{\varphi(t) : t \in T, \varphi \in F_{a^{-1}}\}, \\ S_b &= \{\varphi(t) : t \in T, \varphi \in F_b\}, \\ S_{b^{-1}} &= \{\varphi(t) : t \in T, \varphi \in F_{b^{-1}}\}. \end{aligned}$$

Dokázali jsme tak

Tvrzení. *$S \setminus D$ je ekvirozložitelná se dvěma kopiemi $S \setminus D$.*

Krok (3): přidání bodů z D zpět

Připomeňme, že množina M je *spočetná*, pokud existuje prosté zobrazení $f\colon M \to \mathbb{N}$ (tzn. M lze očíslovat přirozenými čísly).

Pozorování. *Grupa F_2 je spočetná, a tedy i množina D.*

Naproti tomu sféra je nespočetná, což nám umožní dokázat

Tvrzení. *Pokud je $M \subset S$ spočetná, pak $S \setminus M$ je ekvirozložitelná s S.*

Důsledek. *Sféra je ekvirozložitelná se dvěma kopiemi sféry.*

Krok (4): ze sféry na kouli

Jelikož na kouli můžeme pohlížet „po vrstvách“ jako na sjednocení sfér a středu, dostáváme, že koule bez středu je ekvirozložitelná se dvěma koulemi bez středu. Jednoduše si však rozmyslíme, že

Tvrzení. *Koule bez středu je ekvirozložitelná s koulí.*

Tím jsme dokázali Banachův–Tarského paradox!

Poznámka. Konstrukci je možné udělat s rozkladem na pouze 5 částí a je dokázáno, že méně nestačí.

Důkaz silnější verze

K důkazu silnější verze Banachova–Tarského paradoxu postačí chytře využít následující větu.

Věta. (Cantor–Bernstein–Schröder–Banach) *Pokud jsou X, Y množiny a $f\colon X \to Y$, $g\colon Y \to X$ prostá zobrazení, pak existují disjunktní množiny X_1, X_2, kde $X_1 \cup X_2 = X$, a disjunktní množiny Y_1, Y_2, kde $Y_1 \cup Y_2 = Y$, splňující $f(X_1) = Y_1$, $g(Y_2) = X_2$.*

Důsledek. *Mějme množiny $A, A_1, B, B_1 \subset \mathbb{R}^3$, kde $A_1 \subset A$ a $B_1 \subset B$. Pokud A je ekvirozložitelná s B_1 a B je ekvirozložitelná s A_1, pak je A ekvirozložitelná s B.*

Důsledek. (Banach–Tarski, silnější verze) *Každé dvě množiny $A, B \subset \mathbb{R}^3$, které jsou omezené a mají neprázdný vnitřek, jsou ekvirozložitelné.*

Literatura a zdroje

[1] Francis Edward Su: *The Banach–Tarski paradox*, *https://www.math.hmc.edu/∼su/papers.dir/banachtarski.pdf*

[2] Márton Elekés: *Banach–Tarski paradox*, ELTE Summer School in Mathematics, Budapešť, 2017.

[3] Alexander „Olin“ Slávik: *Banachův–Tarského paradox*, sborník Oldřichov, 2012.

Úvod do nekonečna

Petr Gebauer

Abstrakt. V přednášce se seznámíme se základy porovnávání nekonečných množin, řekneme si o velikostech některých známých množin a ke konci si zavedeme ordinální čísla a zkonstruujeme si množinu přirozených čísel.

Základy

Nejprve by bylo dobré si říct, co vlastně pod pojmem nekonečno míníme. Pro nás se nebude jednat o žádný objekt, se kterým bychom pracovali, ale o vlastnost, konkrétně vlastnost množin. Pro začátek budeme slovo množina vnímat ve standardním intuitivním smyslu, jak se asi učí na většině středních škol.

Definice 1. Množinu prohlásíme za *nekonečnou* právě tehdy, když nebude existovat žádné přirozené číslo, které se rovná počtu jejích prvků (za přirozené číslo budeme považovat i nulu). Ostatní množiny označíme slovem *konečné*.

Nabízí se otázka, zda některé nekonečné množiny jsou menší než jiné a jak vlastně tyto vztahy větší, menší, stejně velká definovat, aby přibližně odpovídaly našim intuitivním představám. Budeme postupovat jako malé dítě, které chce rozdělit bonbony na dvě stejně velké hromádky, ale nezná čísla, která by vyjádřila jejich počet (bonbonů je moc), a bonbony, resp. prvky množiny, spárujeme. Protože jsme ale už velké děti, provedeme to trochu formálněji přes zobrazení.

Definice 2. Zobrazení $z : A \to B$ nazveme *prosté* právě tehdy, když pro všechna $x, y \in A$, $x \neq y$ platí $z(x) \neq z(y)$. Nazveme jej *na* právě tehdy, když pro každé $y \in B$ existuje $x \in A$ takové, že platí $z(x) = y$. Pokud je zobrazení prosté a na, nazveme jej *bijekcí*.

Bijekce tedy odpovídá našemu spárování, každý prvek A má svůj protějšek v B a žádné dva svůj protějšek nesdílejí, stejně tak prvky B.

Definice 3. O dvou množinách A, B řekneme, že jsou *stejně velké* (mají *stejnou mohutnost*), což budeme značit $A \approx B$, právě tehdy, když mezi nimi existuje bijekce. Podobně existenci prostého zobrazení z A do B označíme $A \preceq B$. Konečně pokud $A \preceq B$, ale tyto množiny nejsou stejně velké, budeme psát $A \prec B$. Analogicky definujeme $\succeq, \succ$.

Nyní se nabízí pár otázek:

(1) Musí vždy nastat $A \preceq B$ nebo $B \preceq A$?
(2) Pokud $A \approx B$ a $B \subsetneq C$, je nutně $A \prec C$?
(3) Pokud $A \preceq B$ a $B \preceq A$, musí už platit $A \approx B$?

Cvičení 4. Rozmyslete si, že

(1) pokud $A \approx B$, pak $B \approx A$;
(2) pokud $A \approx B$ a $B \approx C$, pak $A \approx C$;
(3) pokud $A \preceq B$ a $B \preceq C$, pak také $A \preceq C$.

Cvičení 5. Porovnejte velikosti množin $\mathbb{N}^+, \mathbb{N}, \mathbb{Z}, \mathbb{Q}$.

Definice 6. Pro množinu A označíme $P(A) = \{B : B \subseteq A\}$, tedy množinu všech podmnožin množiny A.

Věta 7. *Pro každou množinu A platí $P(A) \succ A$.*

Důkaz. Zjevně platí $A \preceq P(A)$, tudíž stačí dokázat, že nejsou stejně velké. Mějme pro spor nějakou bijekci $b : A \to P(A)$. Vezměme množinu $M = \{x \in A : x \notin b(x)\}$. Platí $M \in P(A)$, tudíž existuje nějaké $m \in A$ takové, že $b(m) = M$. Tím jsme ovšem ve sporu, neboť $m \in M \Leftrightarrow m \notin M$.

Předchozí tvrzení nám tedy říká, že některé nekonečné množiny jsou skutečně menší než jiné. Pokud však uvážíme libovolnou nekonečnou množinu A, musí pro každé přirozené číslo n platit, že obsahuje více prvků než n, což nám přímočaře určuje prosté zobrazení $z : \mathbb{N}^+ \to A$: postupujeme od 1 a každému číslu přiřadíme libovolný prvek A, který jsme ještě nepřiřadili. Takový prvek musí pro každé kladné přirozené n existovat, protože jinak by měla A maximálně n prvků. To znamená, že $\mathbb{N}$ je nejmenší nekonečná množina. Tak si její velikost rovnou pojmenujeme.

Definice 8. Množinu A označíme za *spočetnou* právě tehdy, když $A \preceq \mathbb{N}$. V opačném případě ji označíme za *nespočetnou*.

Tvrzení 9. $(0;1) \succ \mathbb{N}$.

Cvičení 10. Kolik se do roviny vejde (spočetně, nebo nespočetně) disjunktních (podobných):

a) kružnic,
b) kruhů,
c) osmiček,
d) osmiček s vynechaným středem?

Věta 11. (Cantor–Bernstein) *Pokud $A \preceq B$ a $B \preceq A$, pak $A \approx B$.*

Věta 12. *Pro všechna $a, b \in \mathbb{R}$, pro která je $a < b$, platí $(0;1) \approx \langle 0;1\rangle \approx (a;b) \approx \mathbb{R}$.*

Věta 13. $\mathbb{R} \approx P(\mathbb{N})$.

Věta 14. *Mějme nekonečnou množinu A. Poté $(P(A))^2 \preceq P(A^2)$.*[1]

[1] Platí rovnost, ale tu nebudeme dokazovat.

Důkaz. Protože $P(A) \approx P(A) \setminus \{\emptyset\}$, a tedy $(P(A))^2 \approx (P(A) \setminus \{\emptyset\})^2$, stačí najít prosté zobrazení $z : (P(A) \setminus \{\emptyset\})^2 \to P(A^2)$. To lze definovat jako $z([B,C]) = B \times C$ pro B, C neprázdné, $B, C \subseteq A$. Toto zobrazení je prosté, neboť z kartézského součinu $B \times C$ různého od $\emptyset$ lze opět jednoznačně určit množiny B, C.

Důsledek: $\mathbb{C} \approx \mathbb{R}^2 \approx \mathbb{R}$.

Russellův paradox a axiomy

Nyní se seznámíme s takzvaným Russellovým paradoxem. Množinu jsme do nynějška považovali prostě za jakýsi pytel, kam můžeme naházet cokoliv. Takže můžeme vzít pytel a naházet do něj úplně všechny ostatní pytle, neboli uvažme množinu všech množin. Teď z ní vyházíme všechny množiny, které obsahují sebe sama (ty se nám nelíbí, protože jsou divné), čímž jsme získali množinu všech množin, které nejsou prvky sebe sama. Jenže ouha, když nás napadne otázka, zda je takto vytvořená množina prvkem sebe sama, zjistíme, že jsme ve sporu. Zřejmě je potřeba pro množiny zavést nějaká pravidla a pořádnou teorii s axiomy. My se s nimi spíše jen zběžně seznámíme:

(1) **axiom existence:** $(\exists x)(\forall y)(y \notin x)$
(2) **extensionality:** $((\forall z)(z \in x \Leftrightarrow z \in y)) \Rightarrow (x = y)$
(3) **dvojice:** $(\forall x, y)(\exists z)(z = \{x, y\})$
(4) **schéma vydělení:** Pokud $\varphi(z)$ je formule neobsahující y, pak $(\forall x)(\exists y)(\forall z)$ $(z \in y \Leftrightarrow (z \in x \wedge \varphi(z)))$.
(5) **sjednocení:** $(\forall x)(\exists s)(\forall z)(z \in s \Leftrightarrow (\exists y \in x)(z \in y))$
(6) **potence:** $(\forall x)(\exists y)(y = P(x))$
(7) **schéma nahrazení:** Mějme formuli $\psi(x, y)$, která neobsahuje b, y_0, y_1. Budeme ji vnímat jako zobrazení, tedy značíme $\psi(x, y)$ jako $f(x) = y$. Potom $(\forall x, y_0, y_1)(((f(x) = y_0) \wedge (f(x) = y_1)) \Rightarrow y_0 = y_1) \Rightarrow (\forall a)(\exists b)(b = \{f(x) : x \in a\}))$.
(8) **fundovanosti neboli regularity:** $(\forall x \neq \emptyset)(\exists y \in x)(\forall z \in y)(z \notin x)$
(9) **nekonečna:** $(\exists m)(\emptyset \in m \wedge (\forall x \in m)(x \cup \{x\} \in m))$
(10) **výběru:** $(\forall a)((\forall x \in a, y \in a)(x \neq y \Leftrightarrow x \cap y = \emptyset) \Rightarrow (\exists b)(\forall x \in a)(\exists y)(x \cap b = \{y\}))$

Tyto axiomy nám tedy zaručují existenci některých množin a existenci jiných vylučují (jako těch z Russellova paradoxu). Občas se ale hodí používat množinu v dřívějším intuitivním smyslu, v tom případě použijeme slovo *třída*. Třída je určená nějakou formulí a za její prvky považujeme vše, co splňuje tuto formuli. Třídu, která není zároveň množinou, nazýváme *vlastní*. Abychom se vyhnuli Russellovu paradoxu, zavedeme pravidla:

(1) Vlastní třída nemůže být prvkem žádné třídy ani množiny.
(2) Třídy nelze ve výrocích kvantifikovat (např. ptát se, zda existuje třída splňující nějaké požadavky).

Standardně se na středních školách definuje zobrazení jako množina, občas se ale v teorii množin používá zobrazení, které množinou být nemůže, popř. se nechceme zabývat tím, jestli může být množinou. Proto si dovolíme, aby zobrazení byl prostě nějaký předpis, který přiřazuje jednoznačně. Pokud to chcete formálněji:

Definice 15. (pro fajnšmekry) *Třídové zobrazení* je formule $\psi(x,y)$ neobsahující proměnné x_0, y_0 taková, že pro každé x_0 existuje maximálně jedno y_0, pro které je formule $\psi(x_0,y_y)$ splněna. Jeho *definičním oborem* potom nazýváme třídu všech x_0, pro která existuje y_0 takové, že formule $\psi(x_0,y_0)$ je splněna.

A zobrazení podle klasické definice budeme říkat množinové.

Definice 16. *Množinové zobrazení* $z : A \to B$ je podmnožina $A \times B$ taková, že $(\forall x_1, x_1 \in A)(z(x_1) = z(x_2) \Rightarrow x_1 = x_2)$.

Nyní se pokusíme dokázat o některých množinách (konkrétně $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$), že skutečně existují. U toho si zároveň vytvoříme užitečný nástroj pro vyjadřování velikostí (nekonečných) množin.

Věta 17. *Pokud existují A, B, pak existuje i $A \times B$.*

DUM a ordinály

Definice 18. *Dobře uspořádanou množinou* (zkráceně *DUMou*) nazveme uspořádanou dvojici [D,U], kde D,U jsou množiny splňující

(1) $U \subseteq D \times D \setminus \{[x,x] : x \in D\}$ (neboli U je ireflexivní relace na D; kde pro $a, b \in D$ vnímáme $[a,b] \in U$ jako $a < b$);
(2) $(\forall a, b \in D)((a \neq b) \Rightarrow (([a,b] \in U \wedge [b,a] \notin U) \vee ([b,a] \in U \wedge [a,b] \notin U)))$ (neboli vždy nastane právě jedna z možností $a < b, b < a, a = b$);
(3) $([a,b] \in U \wedge [b,c] \in U) \Rightarrow ([a,c] \in U)$ (neboli U je tranzitivní, tj. pokud $a < b$ a také $b < c$, pak i $a < c$);
(4) $(\forall A \subseteq D)(\exists m \in A)(\forall x \in A)(x = m \vee [m,x] \in A)$ (neboli každá podmnožina D má svůj nejmenší prvek, z bodu (2) plyne, že je jediný).

Matematickým objektům, které splňují body (1) až (3) říkáme obecně *lineárně uspořádané*. Za prvky DUMy $[D,U]$ budeme označovat prvky D a často budeme množinu U značit znaménkem, kterým je určená, tedy např. budeme mluvit o DUMě $[A,<]$.

Definice 19. Pro DUMu D a její prvek x označíme jako $D \leftarrow x$ množinu $\{x \in D : y < x\}$ uspořádanou podle uspořádání D (ale jen na této menší množině).

Definice 20. Mějme zobrazení $z : A \to B$, kde A, B jsou DUMy[2]. Toto zobrazení nazveme *rostoucí* právě tehdy, když zachovává uspořádání, neboli $(\forall a, b \in A)(a < b \Rightarrow z(a) < z(b))$. DUMy A, B nazveme *stejně velké*, značíme $\simeq$, právě tehdy, když mezi nimi existuje rostoucí bijekce. Řekneme, že A *je menší než* B, značíme $A < B$,

[2]Striktně vzato tím míníme zobrazení $D_A \to D_B$, kde $A = [D_A, U_A], B = [D_B, U_B]$.

právě tehdy, když existuje rostoucí bijekce mezi A a $B \leftarrow x$ pro nějaké $x \in B$. Intuitivně pak definujeme $A \leq B, A \geq B, A > B$.

Věta 21. *Pro každé dvě DUMy A, B platí právě jedna z možností $A < B, A \simeq B, A > B$.*

Definice 22. Mějme nějakou DUMu $[D, U]$ a k ní zobrazení f definované předpisem $f(x) = \{f(d) : d < x\}$, potom *typem* $[D, U]$ nazveme množinu $\{f(x) : x \in D\}$. Množiny, které jsou typem nějaké DUMy nazveme *ordinální čísla*, nebo zkráceně *ordinály*.

Existence jednotlivých obrazů prvků DUMy plyne z axiomů vydělení (pro existenci $D \leftarrow x$) a nahrazení. Dalším použitím axiomu nahrazení získáme, že existuje samotný typ DUMy. Zároveň lze (transfinitní) indukcí dokázat, že je určen jednoznačně.

Věta 23. *Každé ordinální číslo je dobře uspořádáno znaménkem $\in$.*

Důkaz. Mějme nějaký ordinál α. Z definice se jedná o typ nějaké DUMy, kterou si označíme A a vybereme z ní libovolné dva různé prvky a_1, a_2 (ono jich bude víc, takže vybereme libovolnou z nich). Z definice rovněž platí $a_1 < a_2 \Rightarrow f(a_1) \in f(a_2)$, kde f je zobrazení z definice ordinálů. Pokud by však zároveň platilo $f(a_2) \in f(a_1)$, dostali bychom spor s axiomem fundovanosti (resp. jeho konjunkcí s axiomem dvojice). To znamená, že také $f(a_1) \in f(a_2) \Rightarrow a_1 < a_2$. Zároveň žádné $f(a)$ pro $a \in A$ neobsahuje sebe sama, tudíž $a_1 < a_2 \Leftrightarrow f(a_1) \in f(a_2)$, což znamená, že $[\alpha, \in]$ je také DUM (dokonce stejně velká jako A).

Cvičení 24. Dokažte, že každé dvě stejně velké DUMy mají stejný typ; a pokud pro dva ordinály α, β platí $\alpha \simeq \beta$, pak $\alpha = \beta$.

Věta 25. *Pro libovolná ordinální čísla α, β, γ platí $\alpha \in \beta \vee \alpha = \beta \vee \beta \in \alpha$ a zároveň $(\alpha \in \beta \wedge \beta \in \gamma) \Rightarrow \alpha \in \gamma$. Navíc libovolná množina ordinálů má prvek, který je zároveň prvkem všech ostatních.*

Definice 26. Ordinály si rozdělíme do tří skupin:

(1) *Nulový*, tj. $\emptyset$ (uvědomte si, proč je to ordinál),
(2) *Izolované* jsou takové, které mají přímého předchůdce (tj. mají největší prvek),
(3) *Limitní* jsou všechny ostatní.

Přirozená a další čísla

Definice 27. *Konečnými* nazveme právě ty izolované a nulové ordinály, pro které jsou všechny menší ordinály také izolované či nulové.

Nyní uvažme nějakou (existující) množinu zkonstruovanou způsobem určeným v axiomu nekonečna a pomocí axiomu vydělení z ní vyberme pouze ty prvky, které

jsou konečnými ordinály. Takto zkonstruovanou množinu označíme $\mathbb{N}$ a jejím prvkům budeme říkat přirozená čísla (množinou $\mathbb{N}^+$ pak rozumíme $\mathbb{N} \setminus \{\emptyset\}$).

Věta 28. *$\mathbb{N}$ obsahuje všechna konečná ordinální čísla.*

Důkaz. Vezměme pro spor nejmenší konečný ordinál $n \notin \mathbb{N}$.[3] Protože je konečný, má největší prvek n', který obsahuje všechny ostatní prvky n, tedy $n = n' \cup \{n'\}$. Protože n' je menší než n, je prvkem $\mathbb{N}$. V tom případě ale z konstrukce $\mathbb{N}$ plyne, že $n \in \mathbb{N}$ právě tehdy, když je konečným ordinálem, čímž dostáváme spor.

Jako $\mathbb{Z}$ potom označíme množinu $(\{0,1\} \times \mathbb{N}) \setminus \{[0,0]\}$, kde $[0;n]$ chápeme jako $-n$, a vynechaná dvojice tedy je „-0“. Jako $\mathbb{Q}$ dále označíme množinu $\{[p,q] \in \mathbb{Z} \times \mathbb{N}^+ : nsd(|p|,q) = 1\}$, kde $[p,q]$ chápeme jako $\frac{p}{q}$ (můžete si rozmyslet, jak na ní definovat uspořádání). Poté definujeme $\mathbb{R} = \{x \in P(\mathbb{Q}) : (\forall [a,b] \in \mathbb{Q}^2)((a < b \wedge b \in x) \Rightarrow a \in x)\}$. Reálné číslo x je pro nás tedy množina všech racionálních čísel, která jsou menší nebo rovna x. A nakonec definujeme $\mathbb{C} = \mathbb{R}^2$.

Všimněte si, že při tomto zavedení striktně vzato neplatí $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$. Mohli bychom ale předchozí množiny přirozených a jiných čísel označit jen za pomocné a vydělit odpovídající čísla zpět z $\mathbb{C}$. Tím by se ale porušilo hezké tvrzení, že přirozená čísla jsou konečnými ordinály, a tedy trochu představa, že ordinály jsou jakási 'nekonečně velká přirozená čísla'. Ony totiž celkem hezky vyjadřují nejen typ DUM, ale některé z nich (nazýváme je kardinály) také velikost množin obecně.

Literatura a zdroje

[1] PraSečí seriál 35. ročníku
[2] David Hruška: *Nekonečno*, Staré Město, 2015.

Ke studiu mohu také doporučit videa Mirka Olšáka „Esence teorie množin“.

[3] Zde předpokládám, že i podtřída ordinálů, která není množinou, musí mít nejmenší prvek. Můžete si to zkusit rozmyslet, ale je to jen taková technikálie.

Matematická indukce

Verča Hladíková

Abstrakt. Příspěvek slouží jako sbírka úloh na procvičení matematické indukce. V úvodu uvádím princip MI s pár motivačními příklady a dále zde najdete příklady nejen z PraSátka.

Matematická indukce je jedna ze základních důkazových metod, která se obvykle používá, chceme-li dokázat, že nějaké tvrzení či matematická věta platí pro všechna přirozená čísla.

Tvrzení. (Princip matematické indukce) *Buď $V(n)$ výrok závislý na přirozeném čísle n. Předpokládejme, že jsou splněny následující dvě podmínky:*

(i) *$V(1)$ je pravdivý výrok.*
(ii) *Pro každé $k \in \mathbb{N}$ platí implikace $V(k) \Rightarrow V(k+1)$.*

Pak výrok $V(n)$ je pravdivý pro každé n přirozené.

Poznámka. Řešení využívající matematickou indukci zpravidla sestává ze dvou kroků. Nejprve ověříme první podmínku (to jde většinou snadno). Potom provedeme tzv. indukční krok, důkaz druhé podmínky. Ten obvykle vedeme tak, že předpokládáme platnost $V(k)$ a odvodíme $V(k+1)$.

Vzorový příklad

Příklad. Zapiš výraz $1 + 3 + 5 + \cdots + (2k-1)$ v jednodušší formě.

Řešení: Ukážeme, že pro každé $k \in \mathbb{N}$ platí

$$1 + 3 + 5 + \cdots + (2k-1) = k^2.$$

Toto tvrzení dokážeme indukcí. Pro $k = 1$ skutečně nastává rovnost $(2 \cdot 1 - 1 = 1^2)$. Dále buď $t \in \mathbb{N}$ libovolné.

Dokážeme, že pokud tvrzení platí pro t, platí i pro $t+1$. Jelikož jsme výše ukázali, že platí pro jedničku, bude pak muset platit také pro všechna přirozená k. Chceme tedy dokázat, že

$$1 + 3 + 5 + \cdots + (2t-1) + (2t+1) = (t+1)^2,$$

přičemž můžeme využít toho, že

$$1 + 3 + 5 + \cdots + (2t - 1) = t^2. \tag{1}$$

Dosaďme nyní do levé strany dokazovaného tvrzení vztah (1) a upravme

$$[1 + 3 + 5 + \cdots + (2t - 1)] + (2t + 1) = t^2 + (2t + 1) = (t + 1)^2.$$

Jsme hotovi.

Tvrzení. (Princip silné matematické indukce) *Buď $V(n)$ výrok závislý na přirozeném čísle n. Předpokládejme, že jsou splněny následující dvě podmínky:*

(i) *$V(1)$ je pravdivý výrok.*
(ii) *Pro každé $k \in \mathbb{N}$ platí implikace: pro každé $m \leq k$ je $V(m)$ pravdivé $\Rightarrow$ $V(k + 1)$ je pravdivé.*

Pak výrok $V(n)$ je pravdivý pro každé n přirozené.

Příklad. Ukaž, že každé $n \in \mathbb{N}, n \geq 2$ lze zapsat jako součin prvočísel.

Na rozjezd

Příklad 1. Mějme v rovině n kružnic, které ji dělí rovinu na několik oblastí. Ukaž, že je možné každou z těchto oblastí vybarvit jednou ze dvou barev tak, že žádné dvě oblasti se stejnou barvou spolu nesousedí.

Příklad 2. Mějme n přímek v rovině, z nichž žádné dvě nejsou rovnoběžné a žádné tři se neprotínají v jednom bodě. Dokaž, že dělí rovinu na $\frac{1}{2}n(n + 1) + 1$ částí.

Příklad 3. Dokaž, že pro všechna $n \in \mathbb{N}$ můžeme trojkostičkami tvaru L pokrýt šachovnici $2^n \times 2^n$, ze které jsme odstranili jedno políčko.

Příklad 4. Dokaž, že každé přirozené $n \geq 12$ jde zapsat jako součet několika čtyřek a pětek.

Příklad 5. Nechť funkce f splňuje pro každé $n \geq -1$ vztah

$$f(n + 2) = 2f(n + 1) - f(n).$$

Dokaž, že pokud platí $f(0) = 1$ a zároveň $f(1) = 2$, pak $f(n) = n + 1$ pro všechna celá $n \geq -1$.

Příklad 6. Dokaž, že všechna čísla ve tvaru $12008, 120308, 1203308, \ldots$ jsou dělitelná číslem 19.

Příklad 7. Tabulka čokolády má n řad a m sloupců. Kolikrát musíš čokoládu přelomit, abys získal(a) jednotlivé čtverečky?

Příklad 8. Dokaž, že pro každé $n \in \mathbb{N}$ existuje n-ciferné přirozené číslo dělitelné číslem 2^n, které má za cifry pouze jedničky a dvojky. (MKS 26–4–6)

Další úlohy

Příklad 9. Mějme reálné číslo x takové, že $x + \frac{1}{x}$ je celé číslo. Dokaž, že pak je i $x^n + \dfrac{1}{x^n}$ celé číslo pro libovolné $n \in \mathbb{N}$. (MKS 26–4–3)

Příklad 10. V PraSestánu je n měst. Mezi každými dvěma městy vede jednosměrná cesta. Dokaž, že existuje cesta vedoucí přes všechna města právě jednou.

Příklad 11. V rovině je dáno $2n$ bodů, $n \geq 2$, v obecné poloze[1]. Dále je mezi těmito body sestrojeno $n^2 + 1$ úseček. Dokaž, že existuje trojice bodů, ve které jsou každé dva spojeny úsečkou.

Příklad 12. Mějme $n = 2^k$, $k \geq 0$. Dokaž, že z libovolných $(2n - 1)$ přirozených čísel lze vybrat n takových, že jejich součet je dělitelný číslem n.

Příklad 13. Mějme $f(1) = f(2) = 1, f(n) = 3(f(n-1) + f(n-2)) + 1$ pro $n \geq 3$. Dokaž, že pro všechna $n \in \mathbb{N}$ je $(f(3n) + f(3n+1))$ dělitelné číslem 32.

Příklad 14. Dokaž, že pro libovolné $n \geq 0$ přirozené platí $3^{n+1} \mid 2^{3^n} + 1$.

Součty a součiny

Příklad 15. Dokaž, že pro libovolné $n \in \mathbb{N}$ platí

(i) $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$.
(ii) $1^3 + 2^3 + 3^3 + \cdots + n^3 = (1 + 2 + 3 + \cdots + n)^2$.
(iii) $1^2 + 4^2 + 7^2 + \cdots + (3n-2)^2 = \frac{1}{2}n(6n^2 - 3n - 1)$.

Příklad 16. Dokaž, že pro všechna $n \in \mathbb{N}$ platí

$$(n+1)(n+2)\cdots 2n = 2^n \cdot 1 \cdot 3 \cdots (2n-1).$$

Příklad 17. Dokaž, že pro všechna $n \in \mathbb{N}$ platí

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n(n+1)} < 1.$$

Příklad 18. Dokaž, že pro libovolné $n \geq 2$ platí nerovnost

$$\frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n} > \frac{1}{2}.$$

Příklad 19. Buď $n \geq 2$ přirozené číslo, pak platí

$$\left(1 - \frac{1}{\sqrt{2}}\right)\left(1 - \frac{1}{\sqrt{3}}\right)\cdots\left(1 - \frac{1}{\sqrt{n}}\right) < \frac{2}{n^2}.$$

[1] tj. žádné tři neleží na přímce

Návody

1. Indukce, přebarvi rovinu po přidání jedné kružnice.

2. Kolik nových oblastí se vytvoří při přidání jedné přímky?

3. Rozděl pole $2^{n+1} \cdot 2^{n+1}$ na 4 čtverce.

4. MI $n \to n+4$

5. Vyjádři $f(n+1)$ pomocí $f(n)$ a $f(n-1)$ a ověř všechny podmínky.

6. Jaký je rozdíl mezi dvěma po sobě jdoucími čísly?

7. Silná indukce (nebo invariant ;).

8. Jaký zbytek dává 10^{n-1} resp. $2 \cdot 10^{n-1} \pmod{2^n}$?

9. $(x + \frac{1}{x}) \cdot (x^n + \frac{1}{x^n})$

10. Silná indukce.

11. Odeber dva spojené vrcholy a použij předpoklad.

12. Najdi dostatek podmnožin čísel o velikosti 2^{k-1}, jejichž součet je dělitelný 2^{k-1}.

13. Vyjádři $f(3(n+1))$ a $f(3(n+1)+1)$ pomocí $f(3n)$ a $f(3n+1)$.

14. Vyděl výraz pro $n+1$ výrazem pro n.

15. (i) $2n^2 + 7n + 6 = (n+2)(2n+1)$
(ii) $(a+b)^2 = a^2 + 2ab + b^2$
(iii) $(n+1)(6(n+1)^2 - 3(n+1) - 1) = 6n^3 + 15n^2 + 11n + 2$

16. Dosaď pravou stranu pro n do levé strany pro $n+1$.

17. Vymysli, čemu se rovná levá strana, a ověř MI.

18. Jaký je rozdíl výrazu pro n a $n+1$?

19. Ukaž, že $\frac{2}{n^2} \cdot \left(1 - \frac{1}{\sqrt{n+1}}\right) < \frac{2}{(n+1)^2}$.

Literatura a zdroje

[1] Jarda Hančl, *Indukce bez králíků*, Dobrá Voda 2010.
[2] Anička Doležalová *Indukce*, Staré Město 2015

Tětivové čtyřúhelníky

Honza Kadlec

Abstrakt. Jednoduchá a základní přednáška o tětivových čtyřúhelnících. Hlavní důraz je kladen na počítání úhlů a hledání tětivových čtyřúhelníků. Příspěvek obsahuje znění vět o obvodových, středových a úsekových úhlech a několik úloh, včetně mnoha úloh olympiádních.

Základní pojmy

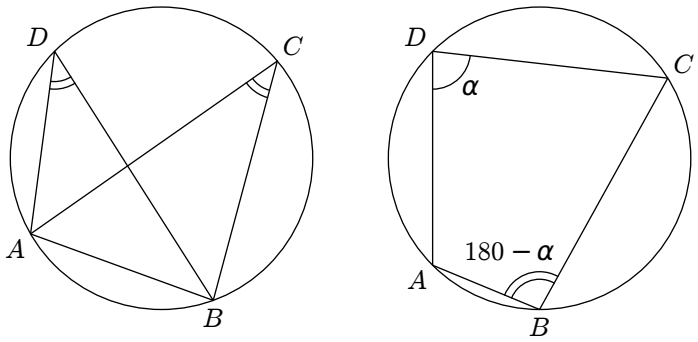
Věta. (o obvodových a středových úhlech) *Mějme kružnici se středem S, její tětivu AB a libovolný bod M na větším oblouku AB. Úhel ASB nazýváme středovým a úhel AMB obvodovým k příslušné tětivě AB. Platí, že $|\sphericalangle ASB| = 2|\sphericalangle AMB|$.*

Věta. (o úsekových úhlech) *Mějme kružnici a na ní tětivu AB. Veďme přímku t, která se dotýká kružnice v bodě A. Odchylku AB od t nazveme úsekovým úhlem k tětivě AB. Úsekový úhel má stejnou velikost jako příslušný obvodový úhel.*

Definice. Čtyřúhelník je *tětivový*, když mu lze opsat kružnici.

K důkazu tětivovosti čtyřúhelníka nám mohou pomoci dvě jeho základní vlastnosti (plynoucí triviálně z věty o obvodovém a středovém úhlu). Čtyřúhelník je tětivový právě tehdy, když je splněna jedna z podmínek:

(i) součet protějších úhlů je 180°,
(ii) jedna z jeho stran je vidět ze zbylých vrcholů pod stejným úhlem.



Lehké příklady

Příklad 1. Mějme trojúhelník ABC. Osa úhlu BCA protíná kružnici opsanou $\triangle ABC$ v bodě $\check{S} \neq C$. Dokažte, že $\check{S}$ je střed oblouku AB (který neobsahuje bod C).

Příklad 2. Mějme trojúhelník ABC s průsečíkem výšek H. Dokažte, že obrazy H v osových souměrnostech podle stran $\triangle ABC$ leží na kružnici opsané ABC.

Příklad 3. Označme D, E a F paty výšek ostroúhlého trojúhelníka ABC. Dokažte, že výšky $\triangle ABC$ jsou osami úhlů $\triangle DEF$.

Příklad 4. Nechť M je libovolný vnitřní bod přepony AB pravoúhlého trojúhelníka ABC. Označme S, S_1 a S_2 středy kružnic opsaných postupně trojúhelníkům ABC, AMC a BMC. Dokažte, že body M, C, S_1, S_2 a S leží na jedné kružnici.
(MO 56–A–II–3a)

Příklad 5. Rovnostrannému trojúhelníku KLM opíšeme kružnici. Na kratším oblouku KL této kružnice si zvolíme bod Q. Pak z bodu M spustíme kolmice na přímky QK a QL a jejich paty označíme E a F. Ukažte, že trojúhelník MEF je rovnostranný. (MKS 28–2–3)

Další příklady

Příklad 6. (Simsonova přímka) Je dán trojúhelník ABC a bod D na jeho kružnici opsané. Z bodu D spustíme kolmice na strany BC, CA, AB a jejich paty označíme P, Q, R. Dokažte, že P, Q, R leží v přímce.

Příklad 7. Na kratším oblouku AB kružnice opsané čtverci $ABCD$ je bod P. Nechť $PD \cap AB = X$ a $PC \cap BD = Y$. Dokažte, že $|\sphericalangle XYB| = 90°$.

Věta 8. (Japonský teorém) *Nechť je $ABCD$ libovolný tětivový čtyřúhelník a nechť jsou M_1, M_2, M_3, M_4 středy trojúhelníků $\triangle ABD$, $\triangle ABC$, $\triangle BCD$, $\triangle ACD$. Pak je čtyřúhelník $M_1M_2M_3M_4$ pravoúhlý.*

Důkaz. Dokaž za pomoci znalostí o tětivových čtyřúhelnících a úhlech. □

Příklad 9. Uvnitř základny AB rovnoramenného trojúhelníku ABC leží bod D. Zvolme bod E tak, aby $ADEC$ byl rovnoběžník. Na polopřímce opačné k ED leží bod F takový, že $|EB| = |EF|$. Dokažte, že délka tětivy, kterou vytíná přímka BE v kružnici opsané trojúhelníku ABF, je dvojnásobkem délky úsečky AC.
(MO 66–A–I–5)

Příklad 10. V konvexním čtyřúhelníku $ABCD$ platí $|\sphericalangle ABC| = |\sphericalangle ACD|$ a $|\sphericalangle ACB| = |\sphericalangle ADC|$. Předpokládejme, že střed O kružnice opsané trojúhelníku BCD je různý od bodu A. Dokažte, že úhel $\sphericalangle OAC$ je pravý. (MO 67–A–I–5)

Příklad 11. Je dán ostroúhlý trojúhelník ABC s průsečíkem výšek H. Osa úhlu $\sphericalangle BHC$ protíná stranu BC v bodě D. Označme postupně E a F obrazy bodu D

v osových souměrnostech podle přímek AB a AC. Dokažte, že kružnice opsaná trojúhelníku AEF prochází středem G kružnicového oblouku BAC.

(MO 66–A–III–5)

Příklad 12. Je dán rovnoramenný lichoběžník $ABCD$ s delší základnou AB. Označme I střed kružnice vepsané trojúhelníku ABC a J střed kružnice připsané straně AD trojúhelníku ACD. Dokažte, že přímky IJ a AB jsou rovnoběžné.

(MO 67–A–III–5)

Příklad 13. Je dána kružnice nad průměrem UV a její tětiva AB se středem S taková, že bod B neleží na UV. Patu kolmice z B na UV označme C. Ukažte, že úhel BCS se nezmění, pokud s tětivou AB začneme pohybovat po celé kružnici.

(MKS 28–2–6)

Příklad 14. Je dán rovnoběžník $ABCD$ s tupým úhlem ABC. Na jeho úhlopříčce AC v polorovině BDC zvolme bod P tak, aby platilo $|\sphericalangle BPD| = |\sphericalangle ABC|$. Dokažte, že přímka CD je tečnou ke kružnici opsané trojúhelníku BCP, právě když úsečky AB a BD jsou shodné. (MO 59–A–II–2)

Literatura a zdroje

[1] Martin Töpfer: *Tětivové čtyřúhelníky*, Mentaurov, 2013.

Cyklotomické polynomy

Daniil Koževnikov

Abstrakt. Na přednášce si ukážeme některé základní vlastnosti cyklotomických polynomů, které mají řadu aplikací ve vysokoškolské i pokročilé olympiádní matematice. Nabyté znalosti využijeme v elegantních důkazech speciálního případu Dirichletovy věty a Zsigmondyho věty.

Cyklotomické polynomy jsou objektem, se kterým se přirozeně setkáme, koukáme-li se na rozklady polynomů tvaru $x^n - 1$ pro přirozená n. Pojďme si ale nejdříve představit několik pojmů a tvrzení, bez nichž se neobejdeme:

Definice. O polynomu řekneme, že je *monický*, pokud je jeho vedoucí koeficient roven 1.

Definice. Je-li $\mathbb{K}$ okruh, tak *okruh polynomů nad* $\mathbb{K}$ (značíme $\mathbb{K}[x]$) je množinou polynomů jedné proměnné, jejichž koeficienty leží v $\mathbb{K}$. Budeme pracovat s okruhy $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}[x]$ a $\mathbb{Z}_p[x]$.

Definice. O polynomu $P \in \mathbb{K}[x]$ řekneme, že je *ireducibilní nad* $\mathbb{K}$, pokud neexistují nekonstantní polynomy $Q, R \in \mathbb{K}[x]$ takové, že $P = QR$.

Věta. *Pro libovolné těleso* $\mathbb{K}$ *má nenulový polynom* $P(x) \in \mathbb{K}[x]$ *stupně* n *nejvýše* n *kořenů v* $\mathbb{K}$.

Věta. (Základní věta algebry) *Nenulový polynom* $P(x) \in \mathbb{C}[x]$ *stupně* n *má (včetně násobnosti) právě* n *kořenů v* $\mathbb{C}$.

Věta. (Dělení se zbytkem) *Pro libovolné nenulové polynomy* $P(x), Q(x) \in \mathbb{K}[x]$ *existují jednoznačně dané polynomy* $A(x), B(x) \in \mathbb{K}[x]$, *pro které platí* $P(x) = A(x)Q(x) + B(x)$ *a* $\deg(B) < \deg(Q)$.

Věta. (Gaussova) *Je-li monický polynom ireducibilní nad* $\mathbb{Z}[x]$, *pak je ireducibilní i nad* $\mathbb{Q}[x]$.

Definice. O čísle $\alpha \in \mathbb{C}$ řekneme, že je *algebraické*, pokud existuje monický polynom $P \in \mathbb{Q}[x]$, jehož je α kořenem. Má-li navíc P ze všech takových polynomů nejnižší možný stupeň, tak ho nazýváme *minimálním polynomem* α; $\deg(P)$ pak nazýváme *stupněm* α.

Definice. O komplexním čísle z řekneme, že je *odmocninou z jedné*, pokud je kořenem polynomu $z^n - 1$ pro nějaké přirozené n. Pokud navíc pro všechna čísla menší než n platí $z^n \neq 1$, tak je z *primitivní n-tou odmocninou z jedné*. Dále budeme značit $\omega_n = e^{\frac{2\pi i}{n}}$.

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

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

Cvičení. Spočtěte si několik prvních cyklotomických polynomů. Jaký je řád polynomu $\Phi_n(x)$?

Cvičení. Rozmyslete si, že Φ_n je monický polynom, jehož kořeny jsou právě primitivní n-té odmocniny jedné.

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

Věta. *Pro libovolné přirozené n má polynom $\Phi_n(x)$ celočíselné koeficienty.*

Cvičení. Dokažte, že $\Phi_n(x)$ je reciproký pro $n \geq 2$, tj. že pro jeho koeficienty a_i platí $a_{\varphi(n)-i} = a_i$.

Cvičení. Ukažte, že součet primitivních n-tých odmocnin z jedné je roven $\mu(n)$, kde μ je Möbiova funkce.

Věta. *Je-li p prvočíslo a n jeho násobek, pak platí $\Phi_{np}(x) = \Phi_n(x^p)$. Pokud n není dělitelné p, pak platí $\Phi_{np}(x)\Phi_n(x) = \Phi_n(x^p)$.*

Cvičení. Spočtěte si několik dalších cyklotomických polynomů pomocí minulé věty.

Cvičení. Rozmyslete si, že pro lichá $n \geq 3$ platí $\Phi_{2n}(x) = \Phi_n(-x)$.

Cvičení. Ukažte, že pro nesoudělná n, a platí $\Phi_n(x^a) = \prod_{d|a} \Phi_{nd}(x)$.

Věta. (MFV pro polynomy) *Buď p prvočíslo, x celé číslo a $f(x)$ polynom s celočíselnými koeficienty. Potom platí $f(x^p) \equiv f(x)^p \pmod p$.*

Věta. *$\Phi_n(x)$ je ireducibilní v $\mathbb{Z}[x]$ pro libovolné přirozené n.*

Řády a nesoudělnost

Věta. *Pro přirozené číslo n a prvočíslo p takové, že $gcd(n, p) = 1$, neexistuje žádný nekonstantní polynom $m \in \mathbb{Z}_p[x]$ takový, že $m^2(x)|x^n - 1$.*

Věta. *Není-li mn dělitelné prvočíslem p, pak jsou v $\mathbb{Z}_p[x]$ polynomy $\Phi_m(x)$ a $\Phi_n(x)$ nesoudělné.*

Věta. *Buď p prvočíslo. Potom pro libovolné celé t a libovolné přirozené n, nesoudělné s p, platí $p|\Phi_n(t) \iff ord_p(t) = n$.*

Cvičení. Rozmyslete si, že z minulého cvičení vyplývá existence primitivního prvku modulo p.

Věta. *Buďte m, n různá přirozená čísla. Jsou-li hodnoty $\Phi_m(t)$ a $\Phi_n(t)$ soudělné pro nějaké celé t, pak existuje prvočíslo p a celá čísla k, l, pro něž $\frac{m}{n} = p^k$ a $\gcd(\Phi_m(t), \Phi_n(t)) = p^l$.*

Věta. (Schurova věta) *Množina hodnot libovolného nekonstantního polynomu $P \in \mathbb{Z}[x]$ v přirozených číslech má nekonečně mnoho prvočíselných dělitelů.*

Věta. (slabší Dirichletova věta) *Aritmetická posloupnost $\{an + 1\}_{n=1}^{\infty}$ obsahuje nekonečně mnoho prvočísel pro libovolné přirozené a.*

Zsigmondyho věta

Věta. (Zsigmondy) *Jsou-li $a > b$ nesoudělná přirozená čísla, tak pro libovolné přirozené n (tedy až na níže uvedené výjimky) existuje prvočíslo p, jež dělí $a^n - b^n$, ale nikoliv $a^i - b^i$ pro $1 \leq i < n$ (tzv. primitivní prvočíselný dělitel). Jediné výjimky tvoří následující případy:*

(1) $n = 1$ a $a - b = 1$
(2) $n = 2$ a $a + b = 2^k$ pro $k \in \mathbb{Z}$
(3) $a = 2$, $b = 1$, $n = 6$

Analogické tvrzení platí i pro $a^n + b^n$, až na výjimku $a = 2$, $b = 1$, $n = 3$.

Cvičení. Existence primitivního prvočíselného dělitele $a^n - 1$ je ekvivalentní s tím, že $\Phi_n(a)$ má prvočíselného dělitele nesoudělného s n.

Cvičení. Rozmyslete si, že stačí dokázat Zsigmondyho větu jen pro rozdíl a pouze v případě $b = 1$.

Věta. *Předpokládejme, že pro přirozená a, $n > 1$ jsou všechny dělitele $\Phi_n(a)$ zároveň děliteli n. Potom buď $n = 2$ nebo $\Phi_n(a)$ je prvočíslo.*

Věta. *Buďte $a, n > 1$ přirozená čísla. Nechť $n = p^k r$ pro prvočíslo p a r nesoudělné s p. Potom $\Phi_n(a) > (b^p - b^{p-2})^{\varphi(r)}$ pro $b = a^{p^{k-1}}$.*

Příklady

Příklad 1. Dokažte, že žádné z čísel $10001, 100010001, \ldots$ není prvočíslo.
(Britská MO)

Příklad 2. Najděte všechny dvojice celých čísel (x, y) splňující $\frac{x^7-1}{x-1} = y^5 - 1$.
(IMO 2006 SL)

Příklad 3. Buď $n > 2$ liché číslo a $S \subset \{1, \ldots, n\}$. Označme dále t_i počet neprázdných podmnožin S, které mají součet prvků kongruentní s i modulo n. O množině S řekneme, že je n-vyvážená, pokud platí $t_0 = t_1 = \cdots = t_{n-1}$.

(1) Ukažte, že existuje n-vyvážená množina pro libovolné liché n. (CPS 2016)

(2) Ukažte, že $\mathbb{Z}_n^*$ je n-vyvážená.

Příklad 4. Dokažte, že $\cos\left(\frac{2\pi}{n}\right)$ je algebraické číslo. Jaký je jeho stupeň?

Příklad 5. Buď X neprázdná podmnožina vrcholů pravidelného n-úhelníka. O X řekneme, že je *křupavoučká*, pokud její těžiště splývá s těžištěm celého n-úhelníku. Charakterizujte všechny křupavoučké množiny pro:

(1) n rovné mocnině prvočísla;
(2) n rovné součinu dvou prvočísel;
(3) co nejobecnější možné n.

Příklad 6. Dokažte, že pro různá lichá prvočísla $p_1, \ldots, p_n$ má $2^{p_1 \cdots p_n} + 1$ alespoň $2^{2^{n-1}}$ dělitelů. (silnější IMO 2002 SL)

Příklad 7. Najděte všechna přirozená n, pro která je $\frac{2^n+1}{n^2}$ celé číslo. (IMO 1990)

Příklad 8. Dokažte, že pokud všechny kořeny $p \in \mathbb{Z}[x]$ leží na jednotkové kružnici, pak už jsou to nutně odmocniny z jedné. (Kroneckerova věta)

Příklad 9. Pro dané přirozené číslo k charakterizujte všechny polynomy $p \in \mathbb{Z}[x]$, pro které je $p(x^k)$ dělitelné $p(x)$.

Příklad 10. Ukažte, že $\sum_{1 \le i \le n,\, \gcd(n,i)=1} \omega_n^{ki}$ je celé číslo pro libovolná přirozená k, n. Obecněji: je-li p symetrický polynom $\varphi(n)$ proměnných s celočíselnými koeficienty, tak jeho hodnota v kořenech $\Phi_n(x)$ je celé číslo.

Příklad 11. Jsou-li ω odmocnina z jedničky a $f \in \mathbb{Z}[x]$, pro které platí $|f(\omega)| = 1$, pak je $f(\omega)$ rovněž odmocnina z jedničky.

Příklad 12. Ukažte, že pro nekonečně mnoho přirozených čísel n jsou všechny prvočíselné dělitele $n^2 + n + 1$ menší než $\sqrt{n}$.

Příklad 13. (pro odvážné) Ukažte, že se každé celé číslo objeví jako koeficient některého cyklotomického polynomu.

Příklad 14. (dávka abstraktní algebry) Nechť a, b, c, d jsou primitivní n-té odmocniny z jedné. Určete hodnotu n, platí-li $a + b + c + d = 1$.

Návody

1. Rozložte na cyklotomické polynomy.

2. Pracujte modulo 7.

3. Pro první část použijte binárku. Ve druhé využijte toho, že pro $p \in \mathbb{C}[x]$ je $\frac{1}{n}\sum_{i=0}^{n-1} p(\omega_n^i)$ součet koeficientů p, u kterých je exponent x dělitelný n.

4. $\cos(x) = \frac{e^{ix}+e^{-ix}}{2}$; stupeň vyjde $\frac{\varphi(n)}{2}$ pro $n > 2$

5. Použijte analytiku v Gaussově rovině a dělitelnost cyklotomickými polynomy. Jo, a třetí část je open :D

6. Rozložte na cyklotomické polynomy.

7. Nejprve pomocí MFV ukažte, že nejmenší prvočíselný dělitel n je trojka. Pak pomocí rozkladu na CP ukažte, že devítka nedělí n; dokončete zase přes prvočíselné dělitele.

8. Jsou-li kořeny p $z_1, \ldots, z_n$, tak se dívejte na polynomy p_k s kořeny $z_1^k, \ldots, z_n^k$. Ukažte, že existuje takové k, pro které platí $p_k(x) = p(x)$.

9. Použijte minulý příklad a zapojte do toho cyklotomické polynomy.

10. Celočíselnost koeficientů $\Phi_n(x)$ a Newtonovy vztahy/základní věta symetrických polynomů.

11. Ukažte, že je-li $\Phi_n(\omega) = 0$, pak $\Phi_n(x) | f(x)f(x^{n-1}) - 1$; z toho odvoďte $|f(\omega^k)| = 1$ pro $(k, n) = 1$ a z minulého cvičení $\prod_{(k,n)=1}(x - f(\omega^k) \in \mathbb{Z}[x]$, pak je to jen Kronecker.

12. Zvolte $n = k^m$ a rozložte $\Phi_3(k^m)$ na součin, pak využijte toho, že $\frac{\varphi(n)}{n}$ může být libovolně blízko nule.

13. Je to dost kencr; kdo to dá, dostane lízátko ;)

14. Pro $(k, n) = 1$ uvažte automorfismy f_k z $\mathbb{Q}[\omega_n]$, které zobrazí ω_n na ω_n^k. Po sečtení $f_k(L) = f_k(P)$ přes všechna k dostaneme, že musí platit $4\mu(n) = \varphi(n)$.

Literatura a zdroje

[1] *https://imosuisse.ch/smo/skripte/imovorbereitung/rootsofunity/en-rootsofunity.pdf*

[2] *http://yufeizhao.com/olympiad/exponent-lifting-sol.pdf*

[3] Lawrence Sun: Cyclotomic polynomials in olympiad number theory

Úvod do nerovností

Danil Koževnikov

Abstrakt. Během přednášky si ukážeme nejdůležitější metody řešení nerovností, a to především na známých úlohách a příkladech ze všemožných soutěží.

Nerovnosti jsou velmi oblíbeným tématem úloh nejen ve středoškolské a vysokoškolské matematice, ale i ve všemožných matematických soutěžích. Proto patří základní návyky k jejich řešení k takřka povinné výbavě řešitele jakékoliv z nich, ať už se jedná o MO nebo o PraSe. Pojďme se tedy seznámit s nejběžnějšími metodami, pomocí nichž lze však s dostatkem trpělivosti a kreativity vyřešit naprostou většinu olympiádních nerovností!

Čtverce

Úplně nejzákladnější nerovnost, kterou budeme používat, je $x^2 \geq 0$, která platí pro libovolné reálné x. Snadné, že? Typicky může její využití vypadat například takto:

Úloha. Pro libovolná reálná x, y, z dokažte nerovnost $x^2+y^2+z^2 \geq xy+yz+zx$. Kdy nastane rovnost?

Řešení. Po vynásobení dvěma a převedení všech členů na levou stranu je dokazovaná nerovnost ekvivalentní s $(x-y)^2+(y-z)^2+(z-x)^2 \geq 0$, což dostaneme sečtením tří platných nerovností. Aby nastala rovnost, musí nastat rovnost ve všech dílčích nerovnostech, neboli musí platit $x=y=z$.

No dobře, jak ale na takovýto tvar vůbec přijít? Tomu se člověk učí především praxí a zkoušením různých způsobů, jak by takový zápis mohl vypadat. Méně trikovou, ovšem často také méně elegantní, cestou je využití diskriminantu, jehož podstata by se dala shrnout v následujícím tvrzení:

Věta. (Diskriminant) *Platí-li pro reálná čísla a, b, c zároveň nerovnosti $a \geq 0$ a $b^2-4ac \leq 0$, tak platí i nerovnost $ax^2+bx+c \geq 0$ pro všechna reálná x. Pokud se omezíme pouze na nenulová a, jedná se dokonce o ekvivalenci.*

Úloha. Dokažte nerovnost $x^2+y^2+2y+4 \geq xy+2x$.

Řešení. Na danou nerovnost se můžeme dívat jako na kvadratickou funkci v proměnné x s parametrem y, přepíšeme ji proto do vhodnějšího tvaru $x^2-(y+2)x+y^2+2y+4 \geq 0$. Diskriminant tohoto výrazu vyjde roven $(y+2)^2-4(y^2+2y+4) = -3y^2-4y-12$, což je nekladné pro libovolné y (to dokážeme opět pomocí diskriminantu), takže můžeme použít výše uvedené tvrzení a máme hotovo.

Vlastnosti výrazů

Definice. O výrazu ve třech proměnných $V(a,b,c)$ řekneme, že je (kde a,b,c jsou libovolná čísla z jeho definičního oboru):

(i) *symetrický*, pokud jeho hodnota nezávisí na pořadí čísel a,b,c; symetrickými výrazy tak jsou například $a+b+c$, abc nebo $\frac{a+b}{c}+\frac{b+c}{a}+\frac{c+a}{b}$,

(ii) *cyklický*, pokud platí $V(a,b,c)=V(b,c,a)=V(c,a,b)$; cyklické jsou tak všechny symetrické výrazy, nebo například $\frac{a}{b}+\frac{b}{c}+\frac{c}{a}$,

(iii) *homogenní stupně* α, pokud platí $V(ta,tb,tc)=t^\alpha V(a,b,c)$; homogenní jsou tak výrazy $a+b+c$, $\frac{a^2}{bc}$, $\frac{1}{\sqrt{abc}}$ (se stupni 1, 0 a $-\frac{3}{2}$).

K čemu jsou tyto vlastnosti dobré? Chceme-li dokázat nerovnost $V(a,b,c)\geq 0$ pro symetrický výraz V, můžeme díky přeuspořádávání BÚNO předpokládat $a\geq b\geq c$; pro cyklický výraz pouze $a=\max\{a,b,c\}$. Je-li V homogenní, tak si zase můžeme přenásobením všech tří proměnných vhodnou konstantou zavést nějakou podmínku, například $a=42$, $ab+bc+ca=3$, nebo $abc=1$.

Poslední zmíněná podmínka se občas vyskytuje přímo v zadání různých nerovností. Chceme-li se této podmínky zbavit, můžeme od proměnných a,b,c přejít k novým proměnným x,y,z, které splňují $a=\frac{x}{y}, b=\frac{y}{z}, c=\frac{z}{x}$. Může se stát, že se v zadání objeví i nějaká ošklivější podmínka, například $\frac{1}{a}+\frac{2}{b}+\frac{3}{c}=\sqrt{2}$. Potom se můžeme dané podmínky zbavit přenásobením vhodných členů tak, abychom nerovnost homogenizovali.

Věta. (Schurova nerovnost) *Pro nezáporná čísla a, b, c platí*

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

Důkaz. Díky symetrii můžeme předpokládat $a\geq b\geq c$. Potom zřejmě platí $c(c-b)(c-a)\geq 0$, takže zbývá dokázat pouze nerovnost $a(a-b)(a-c)-b(a-b)(b-c)\geq 0$. Ta je ekvivalentní s $(a-b)(a^2-b^2+bc-ac)\geq 0$, neboli $(a-b)^2(a+b-c)\geq 0$, což je zjevné z uspořádání. Rovnost tentokráte nastává nejen při rovnosti všech tří proměnných, ale i v případě $b=c=0$.

Úloha. Pro kladná reálná a, b a $r\geq s\geq 0$ dokažte nerovnost $(a^r+b^r)^{\frac{1}{r}}\leq (a^s+b^s)^{\frac{1}{s}}$.

Řešení. Obě strany jsou homogenní stupně jedna, takže můžeme BÚNO předpokládat $a^r+b^r=1$ a stačí nám dokázat $a^s+b^s\geq 1$. Snadno nahlédneme, že z dané podmínky vyplývá $1\geq a,b\geq 0$, takže zároveň $1\geq a^{r-s},b^{r-s}\geq 0$, což můžeme vyžít k odhadu $1=a^r+b^r=a^sa^{r-s}+b^sb^{r-s}\leq a^s+b^s$.

Úloha. Pro reálná a, b, c se součtem 3 dokažte nerovnost $a+b+c\geq ab+bc+ca$.

Řešení. Levou stranu dané nerovnosti můžeme ekvivalentně vynásobit jedničkou, neboli výrazem $\frac{1}{3}(a+b+c)$, čímž dostaneme, že nám stačí dokázat (homogenní!) nerovnost $\frac{1}{3}(a+b+c)^2\geq ab+bc+ca$, která je po roznásobení ekvivalentní prvnímu cvičení z minulé sekce.

Cauchyho–Schwarzova nerovnost

Představíme si nyní první ze dvou, pro olympiádu nejdůležitějších, nerovností, kterou můžeme s využitím předchozích poznatků dokázat hned několika způsoby:

Věta. (Cauchyho–Schwarzova nerovnost) *Pro dvě libovolné posloupnosti reálných čísel $a_1, \dots, a_n, b_1, \dots, b_n$ platí nerovnost*

$$(a_1^2 + \cdots + a_n^2)(b_1^2 + \cdots + b_n^2) \geq (a_1 b_1 + \cdots + a_n b_n)^2.$$

Pojďme si nyní ukázat několik různě trikových způsobů, kterými jde Cauchyho nerovnost aplikovat:

Úloha. Pro reálná $a_1, \dots, a_n$ dokažte nerovnost $n(a_1^2 + \cdots + a_n^2) \geq (a_1 + \cdots + a_n)^2$.

Řešení. n si můžeme představit jako součet n jedniček, takže stačí v CS zvolit $b_i = 1$.

Úloha. (CS a odmocniny) Pro všechna x, pro něž dávají všechny výrazy v zadání smysl, dokažte nerovnost $\sqrt{x+1} + \sqrt{2x-3} + \sqrt{50-3x} \leq 12$.

Řešení. Nerovnost je ekvivalentní $144 = ((x+1)+(2x-3)+(50-3x))(1+1+1) \geq (\sqrt{x+1} + \sqrt{2x-3} + \sqrt{50-3x})^2$, což plyne z CS.

Věta. (Odmocninový tvar CS) *Pro posloupnosti kladných reálných čísel $a_1, \dots, a_n$ a $b_1, \dots, b_n$ platí nerovnost* $\sqrt{(a_1 + \cdots + a_n)(b_1 + \cdots + b_n)} \geq \sqrt{a_1 b_1} + \cdots + \sqrt{a_n b_n}$.

Úloha. (CS a zlomky) Pro kladná reálná x, y, z dokažte nerovnost $\frac{x^2}{y+z} + \frac{y^2}{z+x} + \frac{z^2}{x+y} \geq \frac{x+y+z}{2}$.

Řešení. Po přenásobení obou stran kladným výrazem $2(x+y+z)$ je nerovnost ekvivalentní $\left(\frac{x^2}{y+z} + \frac{y^2}{z+x} + \frac{z^2}{x+y}\right)((y+z)+(z+x)+(x+y)) \geq (x+y+z)^2$, což plyne z CS.

Věta. (CS–zlomkobijec) *Pro posloupnosti kladných reálných čísel $a_1, \dots, a_n$ a $b_1, \dots, b_n$ platí nerovnost* $\frac{a_1}{b_1} + \cdots + \frac{a_n}{b_n} \geq \frac{(\sqrt{a_1} + \cdots + \sqrt{a_n})^2}{b_1 + \cdots + b_n}$.

AG nerovnost

Nyní přichází na řadu druhá z již zmíněných nerovností, k jejíž důkazu už také máme dostatek znalostí:

Věta. (AG nerovnost) *Pro n-tici kladných reálných čísel $x_1, \dots, x_n$ platí nerovnost*

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

I tady existuje řada triků běžně používaných spolu s AG nerovností. K jejich ilustraci slouží následující příklady:

Úloha. Pro kladná reálná x dokažte nerovnost $2x^3 + \frac{3}{x^2} \geq 5$.

Řešení. Stačí pouze aplikovat AG nerovnost pro pět členů: $x^3+x^3+\frac{1}{x^2}+\frac{1}{x^2}+\frac{1}{x^2} \geq 5$.

Úloha. (sčítání AG) Pro kladná reálná a, b, c dokažte nerovnost $a^3 + b^3 + c^3 \geq a^2b + b^2c + c^2a$.

Řešení. Přímočarým použitím AG dostaneme nerovnost $2a^3 + b^3 \geq 3a^2b$. Můžeme ale analogicky obdržet i nerovnosti $2b^3 + c^3 \geq 3b^2c$, $2c^3 + a^3 \geq 3c^2a$, které stačí pouze sečíst a vydělit 3.

Úloha. (AG a zlomky) Pro kladná reálná a, b, c dokažte nerovnost $\frac{a^3}{bc} + \frac{b^3}{ca} + \frac{c^3}{ab} \geq a + b + c$.

Řešení. Úlohu bychom se mohli pokusit řešit podobně jako tu minulou, sčítáním vhodně navážených AG, ale existuje i méně pracné řešení. Vyjdeme z nerovnosti $\frac{a^3}{bc}+b+c \geq 3a$. Teď už stačí pouze sečíst tuto nerovnost s jejími cyklickými záměnami a odečíst $2(a + b + c)$ (náš postup si můžeme představit taky tak, že ke každému zlomku přičteme jeho jmenovatele).

Příklady

Jelikož cvik, jak známo, dělá mistra, tak si můžete vyzkoušet pomocí nerovností, které jsme si na přednášce ukázali, vyřešit některé z následujících příkladů (nejsou řazeny dle obtížnosti). Před nimi ještě následuje krátký seznam obecných rad:

(1) nelekejte se, pokud vás hned první odhad nedovede k řešení, často bude zapotřebí udělat více kroků,
(2) rozmyslete si, kdy nastává rovnost; dává smysl používat pouze takové odhady, které zachovávají tento případ rovnosti,
(3) zkuste si nerovnost napsat v co „nejhezčím“ tvaru; když vás ale nenapadá nic lepšího, tak se to vždycky dá se zatnutými zuby roznásobit. ;)

Příklad 1. Pro $x \in \mathbb{R}^+$ dokažte nerovnost $x^{2018} + 1 \geq x^{2000} + x^{18}$.

Příklad 2. Dokažte, že pro kladná reálná x, y, z platí $(x+y)(y+z)(z+x) \geq 8xyz$.

Příklad 3. Pro a, b, $c > 0$ dokažte nerovnost $\frac{2}{3}(a+b+c) \geq \sqrt[3]{ab}+\sqrt[3]{bc}+\sqrt[3]{ca}-1$.

Příklad 4. Pro a, b, $c \in \mathbb{R}^+$ dokažte nerovnost $\frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} \geq \frac{3}{2}$.
(Nesbittova nerovnost)

Příklad 5. Nechť $n > 2$ a $a_2, a_3, \ldots, a_n$ jsou kladná reálná čísla splňující podmínku $a_2a_3 \cdots a_n = 1$. Dokažte, že platí $(1 + a_2)^2(1 + a_3)^3 \cdots (1 + a_n)^n > n^n$.
(IMO 2, 2012)

Příklad 6. Pro kladná reálná čísla a, b, c platí $ab + bc + ca = 16$ a $a \geq 3$. Najděte nejmenší možnou hodnotu výrazu $2a + b + c$. (KKMO A, 2015)

Příklad 7. Pro kladná reálná čísla a, b, c platí $(a+c)(b^2+ac)=4a$. Určete, pro které trojice (a,b,c) nabývá výraz $b+c$ největší možné hodnoty.
(CKMO A, 2016)

Příklad 8. Pro kladná reálná a, b dokažte nerovnost $\frac{a}{\sqrt{b^2+1}}+\frac{b}{\sqrt{a^2+1}}\geq\frac{a+b}{\sqrt{ab+1}}$.
(CKMO A, 2014)

Příklad 9. Kladná čísla x, y, $z\geq 1$ splňují $\frac{1}{x}+\frac{1}{y}+\frac{1}{z}=2$. Dokažte $\sqrt{x-1}+\sqrt{y-1}+\sqrt{z-1}\leq\sqrt{x+y+z}$.

Příklad 10. Dokažte, že pro každá a, b, $c>0$ platí $\frac{a^3}{(a+b)(a+c)}+\frac{b^3}{(b+c)(b+a)}+\frac{c^3}{(c+a)(c+b)}\geq\frac{a+b+c}{4}$.
(IMO SL, 19něco)

Příklad 11. Pro kladná reálná a, b, c se součinem 1 dokažte nerovnost $(a+\frac{1}{b}-1)(b+\frac{1}{c}-1)(c+\frac{1}{a}-1)\leq 1$.
(IMO 1, 2000)

Příklad 12. Nechť a, b, c jsou kladná čísla, jejichž součin je roven jedné. Dokažte, že platí $\frac{1}{a^3(b+c)}+\frac{1}{b^3(a+c)}+\frac{1}{c^3(b+a)}\geq\frac{3}{2}$.
(IMO 2, 1995)

Příklad 13. Pro kladná reálná a, b, c, která splňují $a+b+c=\frac{1}{a}+\frac{1}{b}+\frac{1}{c}$, dokažte nerovnost $\frac{1}{(2a+b+c)^2}+\frac{1}{(2a+b+c)^2}+\frac{1}{(2a+b+c)^2}\leq\frac{3}{16}$.
(IMO SL, 2009)

Příklad 14. Pro kladná reálná a, b, c, která splňují $a+b+c=\frac{1}{a^2}+\frac{1}{b^2}+\frac{1}{c^2}$, dokažte nerovnost $2(a+b+c)\geq(7a^2b+1)^{\frac{1}{3}}+(7b^2c+1)^{\frac{1}{3}}+(7c^2a+1)^{\frac{1}{3}}$.
(MEMO 2013)

Literatura a zdroje

[1] M. Rolínek, P. Šalom: *Zdolávání nerovností*, PraSečí seriál, 29. ročník.
[2] David Hruška: *Diskriminant a Cauchyho–Schwarzova nerovnost*, Hojsova Stráž, 2016
[3] Marian Poljak: *AG nerovnost*, Meziměstí, 2017

p-adická čísla

Jakub Löwit

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

Značení

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

Lepší modulení

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

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

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

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

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

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

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

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

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

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

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

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

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

Důkaz. K jednoznačnému zakódovaní konzistentní posloupnosti nám stačí nekonečná posloupnost $(d_i)_{i=1}^{\infty}$, kde $d_i \in \mathbb{Z}_p$. Pokud totiž známe prvních i členů, máme přesně p možností na volbu členu a_{i+1}, při kterých bude výsledná posloupnost konzistentní – a_{i+1} je zbytek modulo p^{i+1}, přitom už známe jeho zbytek modulo p^i. Mocninné řadě $\sum_{i=0}^{\infty} d_i p^i$ naopak v této korespondenci odpovídá konzistentní posloupnost jejích částečných součtů. Že sčítání a násobení funguje správně, je dost jasné.

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

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

Henselovo lemma

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

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

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

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

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

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

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

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

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

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

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

„Olympiádní“ úlohy

Pojďme se nyní podívat na několik celkem těžkých olympiádních úloh, kde lze výhodně použít některé, právě nabyté, znalosti. Z teorie p-adických čísel pro nás bude stěžejní Henselovo lemma. Z elementární teorie čísel je dobré znát Čínskou zbytkovou větu a Bezoutovu větu. K duhu nám také přijde následující Schurovo lemma:

Lemma 8. (Schurovo) *Ať f je celočíselný nekonstantní polynom. Potom existuje nekonečně mnoho prvočísel p, která dělí nějaké nenulové číslo z množiny $\{f(1), f(2), f(3), \dots\}$.*

Úloha 9. Ať f je nekonstantní celočíselný polynom. Ukažte, že pro libovolné $k \in \mathbb{N}$ existuje nekonečně mnoho prvočísel p takových, že p^k dělí nějaké nenulové číslo z množiny $\{f(1), f(2), f(3), \dots\}$.

Úloha 10. Najděte všechny celočíselné polynomy f, které pro všechna $m, n \in \mathbb{N}$ splňují implikaci $f(m)|f(n) \implies m|n$.

(Irán TST)

Úloha 11. Existuje celočíselný polynom, který nemá žádný racionální kořen, ale má kořen modulo libovolné přirozené číslo?

(Kömal)

Valuace

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

Definice. Prvek $u \in O_p$ nazveme *jednotkou*, jestliže existuje nějaké $v \in O_p$ splňující $uv = 1$.

Všimněme si, že součin jednotek je vždy jednotka.

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

Důkaz. Pokud je a_1 rovno nule, žádným přenásobením z něj 1 vyrobit nelze. Pokud je naopak a_1 nenulové, žádné a_i není dělitelné p, tedy má inverz modulo p^i. Seřazení těchto inverzů do posloupnosti dá konzistentní posloupnost, čímž jsme hotovi.

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

Důkaz. Pro $a \in \mathcal{O}_p$ označme $k+1$ index prvního nenulového prvku příslušné konzistentní posloupnosti. Potom platí $a = \sum_{i=0}^{\infty} d_i p^i = p^k \cdot \sum_{i=k}^{\infty} d_i p^{i-k}$, což je hledaný rozklad.

Tento rozklad je navíc skutečně jednoznačný – jsou-li $p^k u$, $p^l v$ dva takové rozklady, pro přirozená $k \geq l$, můžeme upravovat $p^k u = p^l v$ na $p^l \cdot (p^{k-l} u - v) = 0$. Přitom $p^l \neq 0$ a součin dvou nenulových prvků je vždy nenulový – dostáváme tedy $p^{k-l} u = v$. Protože jsou u, v jednotky, lze rovnost přepsat na $p^{k-l} w = 1$ pro nějakou jednotku w. Tím pádem je ale p^{k-l} také jednotka, takže dle předešlého tvrzení dostáváme $k = l$; dosazením do rovnosti $p^{k-l} u = v$ pak dostáváme také $u = v$.

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

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

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

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

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

Důkaz. První vlastnost je jasná, $p^k u \cdot p^l v = p^{k+l} uv$, kde uv je jednotka. Nerovnost z druhé vlastnosti je také jednoduchá: pokud jsou konzistentní posloupnosti příslušné číslům a, b na nějaké pozici obě nulové, je na této pozici nulová i posloupnost příslušející jejich součtu. Pokud je navíc jedna ze sčítaných posloupností na nějaké pozici nulová a druhá nenulová, jejich součet je na této pozici opět nenulový.

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

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

Zlomky

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

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

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

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

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

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

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

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

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

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

Cvičení 12. Rozhodněte, zda rovnice $x^2 = p$ má řešení v $\mathbb{Q}_p$.

Cvičení 13. Je-li $a = d_j p^j + d_{j+1} p^{j+1} + d_{j+2} p^{j+2} + \dots$ mocninná řada příslušná číslu $a \in \mathbb{Q}_p$, potom číslo $-a$ odpovídá mocninné řadě:

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

Cvičení 14. Upravte číslo $1 + 2 + 2^2 + 2^3 + \dots$ v $\mathbb{Q}_2$ na co nejhezčí tvar.

Cvičení 15. Vyjádřete $\frac{1}{5}$ v $\mathbb{Q}_2$ jako mocninnou řadu.

Cvičení 16. Vyjádřete $\frac{1}{6}$ v $\mathbb{Q}_3$ jako mocninnou řadu.

Cvičení 17. Dokažte, že v $\mathbb{Q}_p$ platí vzorec pro součet geometrické řady:

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

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

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

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

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

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

Úloha 18. Ať $p > 5$ je prvočíslo. Ukažte, že p^4 dělí čitatel čísla

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

Vzdálenost

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

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

Z vlastností valuace hned vyplývají analogické vlastnosti normy.

Tvrzení. (Vlastnosti normy)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Cvičení 19. Každá trojice různých čísel $a, b, c \in \mathbb{Q}_p$ určuje rovnoramenný trojúhelník.

Cvičení 20. Každý kruh v $\mathbb{Q}_p$ má střed v libovolném svém vnitřním bodě.

Cvičení 21. Spočtěte součet řady $1 - 2 + 2^2 - 2^3 + \ldots$ v $\mathbb{Q}_2$.

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

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

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

Úloha 22. Ukažte, že každé prvočíslo, které dělí jmenovatel čísla $\binom{r}{k}$, musí dělit i jmenovatel čísla r.

Úloha 23. Každé prvočíslo, které dělí jmenovatel čísla r, dělí i jmenovatel čísla $\binom{r}{k}$.

Drsnější verze Henselova lemmatu

Zformulujeme si nyní Henselovo lemma v mírně silnější podobě a jinými slovy. Oproti předchozímu zde dovolujeme, aby koeficienty zadaného polynomu byla libovolná čísla z $\mathcal{O}_p$, jinak je tvrzení do puntíku stejné.

Tvrzení. (Henselovo lemma) *Ať f je polynom nad $\mathcal{O}_p$, $a \in \mathcal{O}_p$ splňující $f(a) \equiv 0 \pmod p$, $f'(a) \not\equiv 0 \pmod p$. Potom existuje právě jedno $b \in \mathcal{O}_p$ splňující $f(b) = 0$, $a - b \equiv 0 \pmod p$.*

Poznamenejme ještě, že z definice kongruence a normy lze lemma ekvivalentně zformulovat takto: „Ať f je polynom nad $\mathcal{O}_p$, $a \in \mathcal{O}_p$ splňující $|f(a)|_p < 1$, $|f'(a)|_p = 1$. Potom existuje právě jedno $b \in \mathcal{O}_p$ splňující $f(b) = 0$, $|a - b|_p < 1$.“ Dříve než půjdeme dál zobecňovat toto tvrzení, podíváme se, co umí už teď.

Cvičení 24. Ať $n \in \mathbb{N}$ a p je prvočíslo, které nedělí n. Dále ať $u \in \mathcal{O}_p$ splňuje $u \equiv 1 \pmod p$. Ukažte, že u je n-tá mocnina nějakého prvku z $\mathcal{O}_p$.

Cvičení 25. Je dáno prvočíslo $p \geq 3$ a jednotka $u \in \mathcal{O}_p$. Dokažte, že u je čtverec právě tehdy, když je první složka jeho konzistentní posloupnosti u_1 čtverec modulo p.

Cvičení 26. Mějme prvočíslo p. Ukažte, že se polynom $x^p - x$ rozkládá na lineární činitele v $\mathbb{Q}_p$.

Definice. Číslo $a \in \mathcal{O}_p$ nazveme odmocninou z jedné, jestliže existuje $n \in \mathbb{N}$, pro které je $a^n = 1$.

V racionálních číslech jsou tedy odmocniny z jedné dvě, 1 a -1. Naproti tomu v komplexních číslech už jich je nekonečně. Kolik jich bude v našem $\mathbb{Q}_p$?

Tvrzení. (Odmocniny z jedné) *Pro prvočíslo $p \geq 3$ existuje v $\mathbb{Q}_p$ právě $p - 1$ různých odmocnin z jedné. V $\mathbb{Q}_2$ existují právě dvě odmocniny z jedné.*

Nyní si zformulujeme slíbenou drsnější verzi Henselova lemmatu. Podmínka na $f'(a)$ je v ní mnohem slabší – i když má polynom f v nějakém čísle „násobný kořen“, pořád se něco dovíme.

Tvrzení. (drsnější Henselovo lemma) *Ať f je polynom nad $\mathcal{O}_p$, $a \in \mathcal{O}_p$ splňující*

$$|f(a)|p < |f'(a)|_p^2.$$

Potom existuje jednoznačně určené $b \in \mathcal{O}_p$ splňující $|a - b|_p < |f'(a)|_p$. Dokonce platí

(1) $|a - b|_p = |\frac{f(a)}{f'(a)}|_p < |f'(a)|_p$,
(2) $|f(a)|_p = |f'(a)|_p$.

Něco na závěr

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

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

Návody

1. Přímočaré.

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

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

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

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

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

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

8. Pro $f(0) = 1$ to není těžké, případ $f(0) = 0$ se dá zvesela ignorovat. Je-li $f(0) = m \neq 0$, uvažte polynom $g(x) = \frac{f(0)\cdot x}{f(0)}$.

9. Na Schurovo lemma použijte Henselovo lemma. Aby šlo použít, je potřeba vzít f ireducibilní nad $\mathbb{Z}$ a dostatečně velká prvočísla p.

10. Fungují právě polynomy tvaru ax^k pro $a \in \mathbb{Z}$, $k \in \mathbb{N}_0$. Použijte předchozí úlohu.

11. Volte $f = (x^2 + 3)(x^2 - 13)(x^2 + 39)$. Z Čínské zbytkové věty stačí tvrzení dokazovat pro mocniny prvočísel, z Henselova lemmatu v podstatě jen pro prvočísla.

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

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

14. Vyjde -1.

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

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

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

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

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

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

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

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

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

24. Henselovo lemma na polynom $f = x^n - u$ s počáteční hodnotou 1.

25. Vezměte polynom $f = x^2 - u$, začněte dosazením u_1. Druhá implikace je jasná.

26. Použijte Malou Fermatovu větu.

Zdroje

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

Náboj

Úloha. Může být hodnota polynomu $f(x) = x^{11} + x^2 + 11x + 3$ v nějakém přirozeném čísle dělitelná 11^{2018}?

Řešení. S pomocí Malé Fermatovy věty máme $f(5) \equiv 0 \pmod{11}$, přitom $f'(5) \not\equiv 0 \pmod{11}$. Z Henselova lemmatu tedy takové číslo existuje.

Úloha. Může být hodnota polynomu $f(x) = x^{11} + x^2 + 11x + 1$ v nějakém přirozeném čísle dělitelná 11^{2018}?

Řešení. Ne, tento polynom nemá kořen dokonce ani modulo 11 (neboť polynom $x^{11} + x^2 + 11x \equiv x(x+1) \pmod{11}$ dává pouze zbytky 0, 1 2, 6, 8, 9).

Úloha. Kolik existuje přirozených čísel n menších než 100^{100}, že $10^{10} \mid n^5 + n^2 + 4$?

Řešení. Označme $f(n) = n^5 + n^2 + 4$. Platí $f(1) \equiv 0 \pmod{2}$ a $f'(1) \equiv 1 \pmod{2}$, z Henselova lemmatu proto existuje právě jeden (nutně nenlový) kořen f modulo 2^{10}. Obdobně $f(2) \equiv 0 \pmod{5}$ a $f'(1) \equiv 4 \pmod{5}$, tedy existuje právě jeden (nenulový) kořen modulo 5^{10}. Z čínské zbytkové věty pak existuje jednoznačný kořen modulo 10^{10}. Vyjde proto $\frac{100^{100}}{10^{10}} = 10^{190}$.

Úloha. Rozepište $\frac{1}{5}$ v $\mathcal{O}_3$ jako mocninnou řadu. *(Zlomkem $\frac{1}{5}$ myslíme takový prvek, který splňuje rovnost $\frac{1}{5} \cdot 5 = 1$)*

Řešení. V soustavě o základu 3 rozepíšeme $5 = 2 + 3$. Postupně dopočítáme

$$\frac{1}{5} = 2 + 2 \cdot 3 + 0 \cdot 3^2 + 1 \cdot 3^3 + 2 \cdot 3^4 + 0 \cdot 3^5 + 1 \cdot 3^3 + 2 \cdot 3^4 + 0 \cdot 3^5 + \dots,$$

tj. koeficienty tvoří periodickou posloupnost $2\overline{201}$. (Obecněji na to jde trikově přijít pomocí Malé Fermatovy věty a sčítání geometrických řad v $\mathcal{O}_p$.)

Poloměnky

Viki Němeček

Abstrakt. Ukázka využití poloměnek (tj. monovariantů) na příkladu mnoha úloh. Složitost úloh od triviální až po starší IMO.

Úlohy, ve kterých se objevují invarianty (neboli česky neměnky), jsou celkem časté. Občas se ale stane, že žádný takový invariant neexistuje (nebo ho alespoň neumíme najít). V takových případech může pomoci právě monovariant (neboli poloměnka). Jde o veličinu, která se sice mění, ale pouze jedním směrem - tj. buď jen klesá nebo jen stoupá.

Je to vidět!

V některých úlohách nám zdravý rozum může říkat, že tvrzení úlohy je zřejmé. Exaktní sepsání takových úloh ale nebývá úplně snadné a monovarianty v něm mohou velmi pomoct.

Příklad 1. V řadě vedle sebe je 100 mincí. V jednom tahu můžeme otočit kolik chceme sousedních mincí, pokud na té nejlevější z nich byl orel. Ukažte, že po konečném počtu kroků se dostaneme do stavu, kdy budou na všech mincích panny.

Příklad 2. 2013 lidí je rozmístěno ve 100 pokojích. Každou minutu někdo přejde z jednoho pokoje do pokoje, kde je alespoň tolik lidí jako v pokoji, odkud vycházel. Ukažte, že po konečně mnoha krocích budou všichni v jedné místnosti.

Příklad 3. V každém políčku tabulky $m \times n$ je napsáno reálné číslo. V jednom kroku můžeme změnit znaménka u všech čísel v jednom řádku nebo v jednom sloupci. Ukažte, že lze dosáhnout stavu, kdy bude součet v každém řádku i v každém sloupci nezáporný.

Příklad 4. Na několika políčkách nekonečného pásku je dohromady konečné množství žetonů. V jednom tahu můžeme vzít dva žetony z téhož políčka, jeden posunout o 1 směrem doprava a druhý o 1 směrem doleva. Můžeme se po konečně mnoha krocích vrátit do původního stavu?

Přeskupování

Pokud máme ukázat, že lze vytvořit nějaký stav (např. rozdělení lidí), občas jde postupovat tak, že vyjdeme z obecného stavu a popíšeme takovou operaci (přeskupení lidí), že se při ní nějaká veličina (poloměnka) vždy sníží. Pak se už jednoduše ukáže, že až operace nepůjde provést, budeme v požadovaném stavu.

Příklad 5. Na zájezdu má každý turista nejvýše tři nepřátele. Dokažte, že je možno turisty rozdělit do dvou autobusů tak, že nikdo nejede v autobuse s více než jedním svým nepřítelem.

Příklad 6. V rovině je dáno n modrých a n červených bodů tak, že žádné tři neleží v přímce. Dokažte, že lze nakreslit n úseček tak, aby každý z $2n$ bodů byl spojený s právě jedním bodem jiné barvy a žádné dvě úsečky se nekřížily.

Ukončení procesu

V úlohách, které se nás ptají, zda nějaký proces skončí, můžeme hledat klesající poloměnku přirozených čísel a poté využít triviálního tvrzení:

Tvrzení. *Neexistuje nekonečná klesající posloupnost přirozených čísel.*

Příklad 7. Vrcholy n-úhelníka jsou očíslované reálnými čísly. Buďte a, b, c, d čtyři sousední čísla. Je-li $(a-d)(b-c) < 0$, můžeme vyměnit b a c. Může být tato operace prováděna nekonečně dlouho?

Příklad 8. Na tabuli je několik přirozených čísel. V jednom kroku můžeme dvě čísla taková, že žádné z nich není násobkem druhého, nahradit jejich největším společným dělitelem a nejmenším společným násobkem. Ukažte, že tento proces nemůže pokračovat do nekonečna. (St. Petersburg, 1996)

Příklad 9. Ke každému vrcholu pětiúhelníku napíšeme celé číslo, součet všech pěti čísel je kladný. Pokud na obvodu pětiúhelníku jsou x, y a z (v tomto poradí) a $y < 0$, můžeme tuto trojici nahradit trojicí $x + y$, $-y$, $y + z$. Může tento proces probíhat nekonečně dlouho? (IMO 1986–3)

Příklad 10. Ve 123 místnostech je rozmístěno 1000 mužů a 1000 žen. Pro pohyb mezi místnostmi platí, že buď muž jde z místnosti s více muži než ženami do místnosti s více ženami než muži (počítáno před jeho pohybem), nebo naopak žena jde z místnosti s více ženami než muži do místnosti s více s více muži než ženami (počítáno před jejím pohybem). Ukažte, že nastane situace, kdy se nebude moci nikdo pohnout.

Příklad 11. Mějme k přepínačů v řadě. Každý přepínač ukazuje nahoru, doprava, dolů nebo doleva. Pokud tři sousední přepínače ukazují různými směry, jsou všechny přepnuty do čtvrtého směru. Ukažte, že se proces zastaví. (BAMO 2006–5)

Hledané monovarianty

Zde jsou příklady monovariantů, které v jednotlivých úlohách fungují. Rozhodně se však nejedná o jediná řešení.

1. Posloupnost orlů a pan interpretovaná jako číslo ve dvojkové soustavě.

2. Součet čtverců lidí v jednotlivých pokojích.

3. Součet čísel v celé tabulce.

4. Součet vzdáleností všech dvojic žetonů.

5. Počet nepřátelství v rámci téhož autobusu.

6. Součet délek všech úseček.

7. Součet čtverců rozdílů sousedních čísel.

8. Součet čísel na tabuli.

9. Součet absolutních hodnot součtů všech podmnožin čísel ve vrcholech takových, že jsou tato čísla v pětiúhelníku vedle sebe.

10. Součet rozdílů počtů mužů a žen v jednotlivých místnostech.

11. Součet odmocnin i takových, že vypínač na i-té a $i+1$-ní pozici je v téže pozici. Jednodušší rozbor množiny možných hodnot nabízí dvousložkový monovariant, kde primárně maximalizujeme počet sousedních stejně orientovaných vypínačů a sekundárně minimalizujeme součet čtverců pozic, kde jsou.

Poděkování

Rád bych tímto poděkoval Martinu Töpferovi, z jehož příspěvku na soustředění v Mentaurově jsem přebral téměř všechny úlohy.

Literatura a zdroje

Z anglické literatury Martin čerpal z

[1] Arthur Engel: *Problem-Solving Strategies*, Springer, 1998
[2] Zvezdelina Stankova, Tom Rike: *A Decade of the Berkley Math Circle*, AMS MSRI, 2008

Z českých zdrojů využil materiálů k *Umění vidět v matematice* a také několika příspěvku v PraSečí knihovničce o invariantech.

(Ne)rozhodnutelné problémy

Tomáš Novotný

Abstrakt. Často narazíme na nějaký problém, jehož cílem je něco spočítat nebo rozhodnout, zda má být odpověď ano či ne. Obvykle očekáváme, že k odpovědi lze určitým způsobem dojít. V tomto příspěvku si však ukážeme, že existuje řada teoretických i praktických otázek, na které odpověď algoritmicky nalézt nelze.

Zavedení nezbytných pojmů

Abychom mohli říci, co to znamená „být (ne)rozhodnutelný“, musíme nejprve zavést řadu základních pojmů – bez dostatečně přesného pochopení, co to vlastně je rozhodování, se prostě neobejdeme.

Definice. *Abecedou* Σ budeme nazývat konečnou množinu symbolů, například $\{P, r, a, S, e\}$ či $\{0, 1\}$.

Definice. *Slovo* w nad danou abecedou je konečná posloupnost znaků z této abecedy.

Definice. *Jazyk* L je množina slov nad danou abecedou.

Definice. *Pravidlo* (neboli instrukce) má dvě části:

(1) Požadavky – znak a_1 z abecedy a libovolný stav s_1
(2) Důsledky – rovněž znak a_2 z abecedy a libovolný stav s_2, ne nutně různé od a_1 a s_1. Dále posun p, který může být buďto „jdi vlevo“ ($\leftarrow$), „jdi vpravo“ ($\rightarrow$), nebo „zůstaň stát“ ($\times$).

Pravidlo budeme značit $(a_1, s_1) \rightarrow (a_2, s_2, p)$, například $(P, \triangle) \rightarrow (r, \triangle, \rightarrow)$. Předpokládejme, že pro konkrétní požadavky vždy existuje nejvýše jedno pravidlo.

Hlavní pojmy bychom měli, tak si definujme počítač!

Definice. (Turingův stroj) Nechť Σ je abeceda, S konečná množina stavů a δ množina pravidel nad touto abecedou a stavy. Pro jednoduchost předpokládejme, že $\square \in \Sigma$ a $s, c \in S$. *Turingovým strojem* (dále TS) pak bude uspořádaná trojice (Σ, S, δ).

Definice. (Výpočet TS) Mějme (potenciálně) nekonečnou řadu přihrádek. Na nějakém místě vyplníme po sobě jdoucí přihrádky zadaným slovem, rozděleným po

znacích. Ostatní přihrádky vyplníme znakem □. Do přihrádky s prvním písmenem zadaného slova umístíme TS, jehož stav je nastavený na s.

Výpočet pak probíhá po krocích, kde jeden *krok* probíhá následovně:

(1) TS se podívá, jestli má pravidlo pro svůj aktuální stav a znak, který se nachází v jeho přihrádce.
(2) Pokud ne, skončí.
(3) Jinak použije toto pravidlo – nahradí znak v jeho přihrádce, změní svůj stav na nový a případně se posune v určeném směru o jednu přihrádku.

Pokud se TS po skončení nachází ve stavu c (tzv. přijímající stav), řekneme, že TS přijímá dané slovo. Jinak (tj. buďto skončí v jiném stavu nebo počítá do nekonečna) ho nepřijímá.

Pro jednoduchost budeme používat pojem „jazyk“ i pro TS – budeme tak označovat množinu všech slov, které TS přijímá.

Příklad. Vytvořte pravidla pro TS, který přijme právě tehdy, když má zadané slovo (tvořené pouze nulami) lichou délku.

Příklad. Vytvořte pravidla pro TS, který přijme právě tehdy, když je prostřední znak vstupního slova 0. Můžete předpokládat, že zadané slovo má lichou délku a je složeno jen ze znaků 0 a 1. Smíte si libovolně rozšířit abecedu a zvolit množinu stavů.

Jdeme se rozhodovat

Již máme všechny důležité součásti, které potřebujeme pro pojem rozhodnutelnost. Ukážeme si také první problémy, které rozhodovat nelze.

Definice. Řekneme, že jazyk L je rozhodnutelný, pokud existuje TS, který ho přijímá a vždy se zastaví. Jinak řekneme, že L je nerozhodnutelný.

Mohlo by se zdát, že přeci vždy můžeme zjistit, zda určité slovo v daném jazyce je či není. Bohužel, není tomu tak, a to dokonce ve „většině“ případů (pro znalé pojmu mohutnost: množina rozhodnutelných jazyků je spočetná, zatímco nerozhodnutelných nespočetná).

Pro konstrukci nerozhodnutelného jazyka se nám bude velmi hodit následující pozorování.

Pozorování. *Každý TS lze „zakódovat“ do posloupnosti dvouznakové abecedy.*

Toto pozorování má dva důležité důsledky – jednak můžeme každému TS přiřadit unikátní číslo, a také můžeme zakódovaný TS dát jako vstup jinému TS. Stroj, který je schopný simulovat libovolný jiný stroj s libovolným vstupním slovem skutečně existuje a lze zkonstruovat (tzv. Univerzální TS) – na přednášce si tuto konstrukci naznačíme.

Základní nerozhodnutelné problémy

Nyní si již můžeme ukázat první jazyk, pro který nemůže existovat TS, který by ho příjímal. Tento jazyk budeme označovat jako $DIAG$, podle své diagonální konstrukce.

Vyplňme nekonečnou tabulku tak, že řádky i sloupce odpovídají vzestupně seřazeným kódům všech TS. Na políčko (i, j) napíšeme jedničku právě tehdy, když stroj odpovídající řádku i přijme kód odpovídající sloupci j, jinak nulu. Do jazyka $DIAG$ pak dáme právě ty kódy řádků i, pro které je na pozici (i, i) nula.

Jelikož jsme do řádků vypsali všechny TS a $DIAG$ se od každého z jejich jazyků liší na alespoň jedné pozici, hledaný TS pro $DIAG$ neexistuje a jazyk je tedy nerozhodnutelný.

Tento jazyk je poměrně umělý a v praxi nepříliš použitelný. Nicméně je základem pro důkaz nerozhodnutelnosti mnoha dalších jazyků – rozhodnutelnost takových jazyků by totiž implikovala rozhodnutelnost $DIAG$. Nejznámější je tzv. Problém zastavení.

Věta. (Halting problem) *Nechť dvojice (M, w) je kód TS a nějaké slovo. Jazyk obsahující právě ty dvojice, pro které se stroj M zastaví na slově w, je nerozhodnutelný.*

Tato věta vlastně říká, že nelze obecně rozpoznat, co nějaký program dělá. To je samozřejmě velký problém při kontrole korektnosti programů a jejich optimalizaci. Ve skutečnosti je jejím důsledkem ještě problematičtější skutečnost:

Věta. (Riceova) *Pro jakoukoli jinou než triviální vlastnost (tj. takovou, která je vždy splněna či naopak nikdy nesplněna) nelze rozhodnout, zda ji má jazyk příjímaný daným TS.*

Poznámka. Vlastnost „množina příjímaných slov je prázdná“ **není** triviální, neboli nelze rozhodnout, zda daný TS přijme alespoň jedno slovo. Totéž platí pro množinu všech slov.

Tedy nejenom, že nejsme schopni rozhodovat Halting problem, ale pro jakoukoli užitečnou vlastnost (například zda program přijme všechna sudá čísla) nedokážeme obecně říci, zda ji zadaný program má.

Další zajímavé nerozhodnutelné problémy

Jak bylo zmíněno, nerozhodnutelných problémů je mnohem více než rozhodnutelných. Níže ukážeme pár z nich, které jsou více či méně zajímavé.

Příklad. (Domino – Postův korespondenční problém) Mějme sadu svislých dominových kostek takovou, že v horní i dolní části je libovolná (i prázdná) posloupnost znaků. Lze vybrat posloupnost kostek (můžeme brát neomezeně kusů od každého typu) takovou, že výsledné sekvence v horní a dolní části budou stejné?

Příklad. (Busy biever) Kolik nejvýše kroků může udělat TS s n stavy, abecedou $\Sigma = \{\square, \triangle\}$ a prázdným vstupním slovem, pokud se zastaví?

Poznámka. Předchozí problém hledá číslo, takže nejde přímo o rozhodnutelnost (této funkci se říká nevyčíslitelná). Nicméně problém lze snadno upravit na rozhodovací – můžeme se ptát, zda je ta hodnota menší než zadané x a opakovaným ptaním pro různá x bychom tuto hodnotu nalezli.

Příklad. (MRDP theorem) Má daný polynom více proměnných s celočíselnými koeficienty celočíselný kořen?

Příklad. (Conwayova hra života) Dostane se pro dva dané stavy simulace Conwayovy hry života začínající prvním stavem někdy do druhého stavu?

Následující příklad souvisí s oblíbeným paradoxem typu „Nejmenší přirozené číslo, které nelze vyjádřit méně než dvanácti slovy“.

Příklad. (Kolmogorovská složitost) Mějme pevný „programovací jazyk“. Jaká je délka nejkratšího programu v tomto programovacím jazyce, který vygeneruje dané slovo?

Literatura a zdroje

[1] P. Kučera: *Základy složitosti a vyčíslitelnosti*, *http://ktiml.mff.cuni.cz/ kucerap/NTIN090/NTIN090-slajdy.pdf*
[2] *Nerozhodnutelné problémy*, *https://en.wikipedia.org/wiki/List_of_undecidable_problems*
[3] *Kolmogorovská složitost*, *https://en.wikipedia.org/wiki/Kolmogorov_complexity*

Dělitelnost

Tomáš Novotný

Abstrakt. Nejen v olympiádách často narazíme na úlohy, v nichž potřebujeme rozhodnout, zda jedno číslo dělí jiné či jaký dává po dělení zbytek. V příspěvku nejprve probereme základní vlastnosti, později se podíváme i na pokročilé metody, které lze při řešení takových úloh využít.

Základní pojmy a vlastnosti

Nejprve si zavedeme dva klíčové pojmy:

Definice 1. Řekneme, že a *dělí* b (značíme $a \mid b$), pokud $b = k \cdot a$ pro nějaké celé číslo k. V opačném případě budeme říkat a *nedělí* b a používat značení $a \nmid b$.

Definice 2. Řekneme, že a je *kongruentní* s b modulo n (značíme $a \equiv b \pmod{n}$), pokud $n \mid (a - b)$.

Pomocí tohoto značení můžeme snadno popsat řadu vlastností, které jsou sice triviální, nicméně jsou využity (občas implicitně) v celé řadě úloh.

Pozorování 3. *Pro libovolná nenulová celá čísla* a, b, c, d, n *platí*

(1) $1 \mid a$,
(2) $a \mid 0$,
(3) $a \mid a$,
(4) $a \mid b \wedge a \mid c \implies a \mid b + c$,
(5) $a \mid b \wedge c \mid d \implies ac \mid bd$,
(6) $n \mid b + c \implies b \equiv -c \pmod{n}$,
(7) $a + b \cdot n \equiv a \pmod{n}$,
(8) $a \equiv b \pmod{n} \wedge c \equiv d \pmod{n} \implies a + c \equiv b + d \pmod{n}$,
(9) $a \equiv b \pmod{n} \wedge c \equiv d \pmod{n} \implies ac \equiv bd \pmod{n}$.
(10) *Pokud je* c *nesoudělné s* n, *pak* $ac \equiv bc \pmod{n} \implies a \equiv b \pmod{n}$.

Příklad 4. Najděte zbytek po dělení čísla $2 \cdot 3 \cdot 10 \cdot 11 \cdot 13$ číslem 28.

Příklad 5. Ukažte, že $\frac{n^3 - n}{6}$ je pro každé celé číslo n rovněž celé.

Příklad 6. Najděte největší přirozené číslo a takové, že $a \mid 3^{2n+1} + 1$ pro každé přirozené číslo n.

Příklad 7. Ukažte, že pro každé přirozené číslo n platí $133 \mid 11^{n+1} + 12^{2n-1}$.

Příklad 8. (AIME 1999) Najděte největší celé číslo n takové, že

$$\frac{(n-2)^2 (n+1)}{n-1}$$

je celé číslo.

Malá Fermatova věta a Eulerova věta

Dosud jsme se moc nezabývali vlastnostmi zbytků při mocnění, které se chovají mnohem složitěji. Nicméně máme k dispozici dvě klíčová tvrzení, která nám mohou pomoci.

Věta 9. (Malá Fermatova) *Nechť p je prvočíslo a a celé číslo takové, že $p \nmid a$. Pak*

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

Věta 10. (Eulerova) *Nechť a a n jsou nesoudělná přirozená čísla. Označme $\varphi(n)$ počet přirozených čísel menších než n, která jsou s n nesoudělná. Pak*

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

Můžeme si povšimnout, že Malá Fermatova věta je speciálním případem Eulerovy, neboť pro každé prvočíslo jsou s ním všechna menší přirozená čísla nesoudělná. Jelikož se ale v úlohách často dělí prvočíslem, je vhodné tento případ zmiňovat zvlášť.

Příklad 11. Ukažte, že $13 | 2^{35} + 3^{36} + 5^{37}$.

Příklad 12. Dokažte, že pro lichá přirozená čísla n platí

$$n \mid 2^{(n-1)!} - 1.$$

Příklad 13. (Putnam 1972) Najděte všechna přirozená n, pro která

$$n \mid 2^n - 1.$$

Hledání čísel dávajících dané zbytky

Zatím jsme se zabývali především dokazováním, zda nějaké číslo dělí jiné. Občas by se nám ale naopak hodilo najít nějaké číslo, které by dávalo požadované zbytky při dělení více různými čísly.

Věta 14. (Čínská o zbytcích) *Nechť $m_1, m_2, \ldots, m_n$ jsou po dvou nesoudělná, přirozená čísla. Pak soustava rovnic*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_n \pmod{m_n}, \end{aligned}$$

má pro libovolná celá čísla $a_1, a_2, \ldots, a_n$ právě jedno řešení mezi 0 a $m_1 \cdot m_2 \ldots m_n - 1$.

Tato věta nám říká, že hledání nebude marné (pokud zrovna nechceme mít zbytek 1 po dělení třemi a 2 po dělení šesti), nicméně návod, jak takové číslo najít, už nedává. Naštěstí existuje jednoduchý postup, jak taková čísla nalézt, navíc má řadu dalších využití.

Definice 15. (Euklidův algoritmus) Mějme celočíselnou rovnici $ax + by = 1$, kde a a b jsou nesoudělná a BÚNO $a > b$. Řešení pak můžeme nalézt následujícím způsobem:

(1) Připravíme si tabulku se třemi sloupečky, do prvního řádku napíšeme po řadě $a, 1, 0$ a do druhého $b, 0, 1$.
(2) Dokud nemáme v prvním sloupci jedničku, opakujeme následující kroky:
(3) Označme k_1, k_2, k_3 a l_1, l_2, l_3 hodnoty v posledních dvou vyplněných řádcích tabulky.
(4) Spočteme dělením se zbytkem $k_1 : l_1 = d$ (zb. z).
(5) Do nového řádku napíšeme po řadě čísla z, $k_2 - l_2 \cdot d$ a $k_3 - l_3 \cdot d$.

Poslední dvě hodnoty posledního řádku pak udávají hledaná x a y.

Pozorování 16. *Pokud si vezmeme libovolný řádek tabulky a dosadíme poslední dvě čísla do zadané rovnice za x a y, dostaneme jeho první číslo.*

Cvičení 17.

(1) Jak najdeme řešení $ax + by = c$ pro $c \neq 1$?
(2) Jak vypadají všechna řešení takové rovnice?

Euklidův algoritmus má ještě jednu pěknou vlastnost: pokud by nebyla čísla a a b nesoudělná, tak jako poslední nenulové číslo v prvním sloupci dostaneme jejich největší společný dělitel – rozklad na prvočísla tedy vůbec není nutný!

Jak nám však tento algoritmus pomůže najít řešení garantované Čínskou větou o zbytcích? Pokud chceme, aby takové číslo dávalo zbytek a_1 po dělení m_1 a zbytek

a_2 po dělení m_2, řešíme vlastně rovnici

$$x = a_1 + m_1 \cdot y = a_2 + m_2 \cdot z,$$

pro neznámá y, z, což již umíme vyřešit. Pro více podmínek je pak stačí přidávat postupně po jedné.

Příklad 18. Kolik přirozených čísel menších než 1050 dává po dělení pěti zbytek 1, po dělení šesti zbytek 3 a po dělení sedmi zbytek 5?

Příklad 19. (IMO 1959) Dokažte, že zlomek $\frac{21n+4}{14n+3}$ nelze pro žádné přirozené číslo n zkrátit.

Návody

4. Použijte sedmé pravidlo.

5. Roznásobte pravou stranu.

6. Zjistěte, co lze vytknout, a pak ukažte, že zbylý dělitel pro $n = 1$ dané číslo pro jiná n nedělí.

7. Postupujte indukcí.

11. Použijte Malou Fermatovu větu na jednotlivé členy.

12. Rozmyslete si, že $\varphi(n) \mid n!$.

13. Je jen jediné. Pak zkuste využít Malou Fermatovu větu.

18. Nehledejte je.

19. Použijte Euklidův algoritmus na nalezení největšího společného dělitele.

Literatura a zdroje

[1] Kuba Krásenský: *Dělitelnost pro začátečníky*, Domašov, 2012.
[2] Pavel Paták: *Dělitelnost v praxi*, Ramzová, 2006.
[3] *Mathematical Excalibur*, *https://www.math.ust.hk/excalibur/v20_n2.pdf*

Spirální podobnost

Hedvika Ranošová

Abstrakt. Přednáška seznamuje s vlastnostmi spirální podobnosti a ukazuje její využití v olympiádní geometrii.

Úvod

Spirální podobnost je nejobecnější přímé podobné zobrazení roviny, které řeší některé, jinak velmi složité, úlohy. Cílem tohoto příspěvku je shrnutí poznatků o spirální podobnosti a ukázání jejich použití na lehkých až středně těžkých příkladech.

Definice. *Spirální podobnost* je složení otočení a stejnolehlosti podle téhož středu. Je určena středem spirální podobnosti O, orientovaným úhlem otočení $\overrightarrow{\omega}$ a koeficientem stejnolehlosti $k > 0$. Značíme ji $\mathcal{S}(O, \overrightarrow{\omega}, k)$.

Motivační příklady

Příklad 1. V rovině jsou dány různě velké, stejně orientované, podobné trojúhelníky ABC a $A'B'C'$. Středy úseček AA', BB', CC' označme po řadě A'', B'', C''. Ukažte, že i trojúhelník $A''B''C''$ je podobný předchozím trojúhelníkům.

Příklad 2. Je dán čtyřúhelník $ABCD$ s různoběžnými protějšími stranami. Průsečík přímek AB a CD označme Q a průsečík přímek AD a BC označme R. Ukažte, že kružnice opsané trojúhelníkům BCQ, ADQ, ABR a CDR procházejí jedním bodem.

Vlastnosti spirální podobnosti

Tvrzení 1. (Základní vlastnosti) *Pro spirální podobnost platí:*

(i) *Spirální podobnost je podobné zobrazení – obrazem přímky je přímka, obrazem čtverce je čtverec, obrazem středu úsečky je střed obrazu úsečky, obecně obrazem útvaru je jemu podobný útvar.*
(ii) *Úhel mezi přímkou a jejím obrazem je úhel otočení.*
(iii) *Poměr délky úsečky a jejího obrazu je roven koeficientu stejnolehlosti.*

Tvrzení 2. (Speciální případy) *Spirální podobnost $\mathcal{S}(O, \overrightarrow{\omega}, k)$ se při speciálních hodnotách $\overrightarrow{\omega}$, k redukuje následovně:*

(i) *Pro $\overrightarrow{\omega} = 0$ dostáváme stejnolehlost se středem O a koeficientem k.*
(ii) *Pro $\overrightarrow{\omega} = 180°$ dostáváme stejnolehlost se středem O a koeficientem $-k$.*
(iii) *Pro $k = 1$ dostáváme otočení kolem O o úhel $\overrightarrow{\omega}$.*
(iv) *Pro $k = 1$ a $\overrightarrow{\omega} = 180°$ dostáváme středovou souměrnost se středem O.*
(v) *Žádná kombinace O, $\overrightarrow{\omega}$, k nám nedá posunutí nebo nepřímé zobrazení.*

Tvrzení 3. (Spirální podobnosti chodí po dvou) *Nechť spirální podobnost se středem O převádí $A \to C$ a $B \to D$. Pak jednoznačně určená spirální podobnost, která převádí $A \to B$ a $C \to D$, má též střed v O. Úhel otočení a koeficient se může lišit.*

Tvrzení 4. (Existence a jednoznačnost) *V rovině jsou dány body A, B, C, D takové, že $ABDC$ (v tomto pořadí!) není rovnoběžník. Pak existuje právě jedna spirální podobnost, která převádí $A \to C$, $B \to D$.*

Lemma 5. (S. p. jednoznačně určena trojúhelníkem OAA') *Buď $\mathcal{S}(O, \overrightarrow{\omega}, k)$ spirální podobnost zobrazující bod A na A'. Potom platí následující.*

(i) *Pro různé body A jsou všechny trojúhelníky OAA' podobné.*
(ii) *Libovolný trojúhelník OAA' zpětně jednoznačně určuje spirální podobnost $\mathcal{S}(O, \overrightarrow{\omega}, k)$.*

Tvrzení 6. (Konstrukce středu; existence) *Buď $ABB'A'$ čtyřúhelník takový, že se přímky AB a $A'B'$ protínají v bodě Q. Potom druhý průsečík O kružnic opsaných trojúhelníkům QAA' a QBB' je střed spirální podobnosti*

$$\mathcal{S}\Big(O, \sphericalangle\overrightarrow{AOA'}, \tfrac{|AB|}{|A'B'|}\Big),$$

která zobrazuje $A \to A'$, $B \to B'$.

Tvrzení 7. (Průsečík čtyř kružnic) *Buď $ABB'A'$ čtyřúhelník s různoběžnými protějšími stranami. Průsečík přímek AB a $A'B'$ označme Q, průsečík přímek AA' a BB' označme R. Potom střed spirální podobnosti O, která zobrazuje $A \to A'$ a $B \to B'$, je průsečíkem kružnic opsaných trojúhelníkům $AA'Q$, $BB'Q$, ABR a $A'B'R$.*

Příklady

Příklad 3. (Simsonova přímka) Buď $ABCD$ tětivový čtyřúhelník. Ukažte, že paty kolmic z D postupně na přímky AB, AC, BC leží na jedné přímce.

Příklad 4. Nechť $ABCD$ je čtyřúhelník a nechť E, F jsou body postupně na stranách AD, BC takové, že dělí strany ve stejném poměru $|AE| : |ED| = |BF| : |FC|$. Přímka EF protíná přímky BA a CD postupně v bodech S a T. Dokažte, že kružnice opsané trojúhelníkům SAE, SBF, TCF a TDE mají společný bod.

(USAMO 2006)

Příklad 5. ABC je ostroúhlý trojúhelník s výškou AD. Body X a Y leží po řadě na kružnicích opsaných trojúhelníkům ABD a ACD tak, že X, D, Y leží na jedné přímce a body X, D, Y, B jsou po dvou různé. Označme dále M střed strany BC a M' střed úsečky XY. Dokažte, že přímky MM' a AM' jsou kolmé.
(MKS 27–3–8)

Příklad 6. Stranám AB a BC trojúhelníka ABC připíšeme zvenčí podobné pravoúhelníky[1] $BKLC$ a $MNBA$. Ukažte, že přímky NC, ML a AK procházejí jedním bodem.

Příklad 7. Úhlopříčky čtyřúhelníku $ABCD$ se protínají v P. Označme O_1 a O_2 středy kružnic opsaných trojúhelníkům ADP a CBP. Body M, N a O jsou postupně středy úseček AC, BD a O_1O_2. Ukažte, že O je střed kružnice opsané PMN.

Příklad 8. Je dán pětiúhelník $ABCDE$ takový, že jsou si trojúhelníky ABC, ACD, ADE podobné. Označme T průsečík BD a CE. Ukažte, že přímka AT je kolmá na spojnici středů S_1 a S_2 kružnic opsaných trojúhelníkům ABC a ADE.

Příklad 9. Buď $ABCDE$ konvexní pětiúhelník takový, že jsou si trojúhelníky ABC, ACD, ADE podobné. Úhlopříčky BD a CE se protínají v P. Ukažte, že přímka AP půlí stranu CD. (IMO Shortlist 2006)

Příklad 10. Je dán pravoúhlý trojúhelník ABC s pravým úhlem u C. Označme M střed přepony a D takový bod odvěsny BC, že platí $|CD| = |CM|$. Nechť dále P značí průsečík kružnic opsaných trojúhelníkům CMB a BDA, $P \neq B$. Ukažte, že přímka BP je osou úhlu ABC. (iKS 7–1G)

Příklad 11. Nechť $ABCD$ je tětivový čtyřúhelník, P je průsečík jeho úhlopříček a body E, F jsou po řadě paty kolmic z bodu P na strany AB, CD. Nechť bod K je střed strany BC a L střed AD. Dokažte, že přímky EF a KL jsou kolmé.
(USA TST 2000)

Příklad 12. Střed kružnice opsané tětivovému čtyřúhelníku $ABCD$ označme O. Úhlopříčky AC a BD se protínají v P. Kružnice opsané trojúhelníkům ABP a CDP se protínají v P a Q. Předpokládejme, že jsou body O, P a Q různé. Dokažte, že $|\sphericalangle OQP| = 90°$. (Čína 1992)

Příklad 13. Na straně BC daného ostroúhlého trojúhelníku ABC leží body P a Q tak, že $|\sphericalangle PAB| = |\sphericalangle BCA|$ a $|\sphericalangle CAQ| = |\sphericalangle ABC|$. Body M a N leží po řadě na přímkách AP a AQ, přičemž bod P je středem úsečky AM a bod Q je středem úsečky AN. Dokažte, že přímky BM a CN se protínají na kružnici opsané trojúhelníku ABC. (IMO 2014/4)

Příklad 14. Na stranách a, b, c trojúhelníka ABC zvolíme postupně body A_1, B_1, C_1. Kružnice opsané trojúhelníkům AB_1C_1, BC_1A_1, CA_1B_1 protnou kružnici opsanou podruhé v bodech A_2, B_2, C_2. Body A_3, B_3, C_3 jsou středovými obrazy

[1] Pravoúhelník je obdélník nebo čtverec.

bodů A_1, B_1, C_1 postupně podle středů stran a, b, c. Ukažte, že trojúhelník $A_2B_2C_2$ je podobný trojúhelníku $A_3B_3C_3$. (IMO Shortlist 2006)

Návody

3. Najděte spirální podobnost se středem v D, která zobrazí paty kolmic na body A a C.

4. Najděte spirální podobnost zobrazující $A \to B$ a $D \to C$ a využijte tvrzení o konstrukci středu.

5. Najděte spirální podobnost svazující tři Thaletovy kružnice.

6. Vezměte vhodnou spirální podobnost a zobrazte na sebe kružnice opsané našim pravoúhelníkům.

7. Vzpomeňte si na první motivační příklad.

8. Vezměte spirální podobnost, která zobrazuje $\triangle ABC$ na $\triangle ADE$.

9. Označme Q průsečík BD a AC, R průsečík DA a EC. Díky *Cèvově větě* stačí ukázat $|AQ| : |QC| = |AR| : |RD|$. Čtyřúhelníky $ABCD$ a $ACDE$ si odpovídají ve spirální podobnosti, tedy i jejich průsečíky úhlopříček, a jsou tak zachovány potřebné poměry.

10. Ukažte shodnost $\triangle CPD$ a $\triangle MPA$.

11. Zobrazíme bod P v osové souměrnosti podle CD a určíme vhodnou spirální podobnost. Z vlastností podobných zobrazení můžeme uvažovat vhodný deltoid.

12. Dokreslete body S_1 a S_2, středy úhlopříček AC a BD.

13. Uvažujme trojúhelník AB_1C_1 takový, že strana BC je jeho střední příčkou. Trojúhelník ANC je spirálně podobný s BB_1M s úhlem otočení $\sphericalangle BAC - 180°$.

14. (i) Pomocí znalosti průniku kružnic jako středu s.p. ukažte, že $\triangle A_2BC \sim \sim \triangle A_2C_1B_1$.
(ii) Označme středy úseček b, c, AA_2 postupně S_b, S_c, S_{AA_2}. Ukažte $\triangle S_{AA_2} S_cS_b \sim \triangle A_2BC$.
(iii) Pomocí tvrzení odůvodněte $\triangle A_2C_1B_1 \sim \triangle S_{AA_2}S_cS_b \sim \triangle AC_3B_3$.
(iv) Ukažte shodnost odpovídajících úhlů v $\triangle A_2B_2C_2$ a $\triangle A_3B_3C_3$.

Literatura a zdroje

[1] Franta Konopecký: *Spirální podobnost*, Domaslav, 2010.
[2] Tomáš Pavlík: *Spirální podobnost*, Uhelná příbram, 2014.
[3] Yufei Zhao: *Three Lemmas in Geometry*, *http://yufeizhao.com/olympiad/three_geometry_lemmas.pdf*

Polynomy

Lucien Šíma

Abstrakt. Příspěvek seznámí čtenáře s polynomy a jejich základními vlastnostmi. Dále uvádí několik příkladů k procvičení.

Naši cestu do světa polynomů zahájíme formální definicí a několika teoretickými poznatky.

Teorie

Definice. *Polynomem stupně n* rozumíme výraz tvaru

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

kde $a_n \neq 0$. Čísla a_i nazýváme *koeficienty polynomu* a x *proměnnou*.

Poznámka. Zpravidla bývají koeficienty polynomu reálná čísla. Obecně však můžeme polynomy definovat nad libovolným komutativním okruhem.

Poznámka. K polynomům si přidáme jeden speciální případ a to *nulový polynom*, který má všechny koeficienty rovny nule. Jeho stupeň klademe roven -1.

Polynomy můžeme intuitivně (člen po členu) sčítat, odčítat i násobit. Jak je to ale s dělením?

Definice. Řekneme, že polynom g dělí polynom f (píšeme $g \mid f$), pokud existuje polynom h takový, že $f = g \cdot h$.

Tvrzení. (Dělení se zbytkem) *Nechť f je polynom a g nenulový polynom. Pak existuje právě jedna dvojice polynomů h, r taková, že $f = g \cdot h + r$ a deg[1] $(r) < deg(g)$.*

Další část teorie věnujeme pojmu kořen polynomu.

Definice. Číslo a je *kořenem* polynomu f, pokud $f(a) = 0$.

Tvrzení. *Polynom f má kořen a právě tehdy, když $(x - a) \mid f$.*

[1] stupeň polynomu

Důsledek. *Nenulový polynom stupně n má nejvýše n kořenů.*

Základní věta algebry říká, že každý polynom nad komplexními čísly (s komplexními koeficienty) má alespoň jeden (komplexní) kořen. Z toho již plyne, že každý komplexní polynom stupně n lze zapsat ve tvaru $a_0(x-x_1)(x-x_2)\dots(x-x_n)$, kde x_i jsou jednotlivá komplexní čísla. Nalezení kořenů polynomu nám tedy umožňuje jej dostat do součinového tvaru, v němž se nám s ním bude lépe pracovat. Důkaz této věty je složitý a přesahuje rámec přednášky. Platí ale, že každý reálný polynom lichého stupně má alespoň jeden reálný kořen.

Důsledek. *Pokud se dva polynomy stupně nejvýše n shodují v alespoň $n+1$ bodech, jsou identické.*

Důsledek. *Každými $n+1$ body lze proložit unikátní polynom stupně nejvýše n.*

Věta. *Má-li polynom f celočíselné koeficienty a $a, b \in \mathbb{Z}$, pak $a-b \mid f(a)-f(b)$.*

Věta. (Rational Root Theorem) *Má-li polynom $P(x)=a_nx^n+a_{n-1}x^{n-1}+\dots+a_0$ s celočíselnými koeficienty racionální kořen r/s (v základním tvaru), pak $r \mid a_0$ a $s \mid a_n$.*

Příklady

Příklad 1. Najděte polynom nabývající celočíselných hodnot ve všech celých číslech, který nemá všechny koeficienty celočíselné. (MKS 34–6–1)

Příklad 2. Najděte všechny polynomy f splňující: $x \cdot f(x-1) = (x+1) \cdot f(x)$ pro všechna reálná x. (MKS 34–6–3)

Příklad 3. Najděte všechny polynomy f splňující $f(0) = 0$ a $f(x^2+1) = (f(x))^2+1$ pro všechna reálná x.

Příklad 4. Najděte všechny polynomy f splňující $f(2) = 6$ a $f(x^2) = x^2(x^2+1)f(x)$ pro všechna reálná x.

Příklad 5. Ať f je polynom s celočíselnými koeficienty. Dokažte, že je-li $f(n)$ dělitelné třemi pro tři po sobě jdoucí přirozená čísla, pak je dělitelné třemi pro všechna přirozená čísla.

Příklad 6. Mějme polynom f s celočíselnými koeficienty a $a \in \mathbb{Z}$. Dále platí, že $f(-a) < f(a) < a$. Dokažte, že $f(-a) < -a$.

Příklad 7. Najděte všechny polynomy f splňující $f(x)f(2x^2) = f(2x^3+x^2)$ pro všechna reálná x.

Příklad 8. Existuje polynom sudého stupně s lichými celočíselnými koeficienty, který má racionální kořen? (MKS 34–6–4)

Příklad 9. Polynom f s celočíselnými koeficienty splňuje $f(0) = 1$. V kolika nejvíce různých celých číslech může nabývat hodnoty 2008? (MKS 28–3–5)

Příklad 10. Ať f je polynom s celočíselnými koeficienty splňující $f(0) = f(1) = 2011$. Ukažte, že $f(x)$ nemá celočíselný kořen.

Příklad 11. Koeficienty polynomu f jsou přirozená čísla. Pro každé přirozené číslo n označme a_n součet cifer v desítkovém zápisu čísla $f(n)$. Dokažte, že existuje číslo, které se v posloupnosti $a_1, a_2, \ldots$ vyskytuje nekonečněkrát. (MKS 21–6–6)

Příklad 12. Polynom $f(x)$ stupně 2015 pro $k = 1, \ldots, 2016$ splňuje $f(k) = \frac{1}{k}$. Určete $f(2017)$. (MKS 29–1–8)

Návody

1. Nápovědu k prvnímu příkladu nechceš.

2. Ukažte, že kořenem polynomu je každé celé číslo.

3. Postupně dosazujte za x hodnoty $0, 1, 2, \ldots$ a použijte důsledek o identičnosti polynomů.

4. Z druhé rovnosti určete stupeň polynomu f.

5. Z věty výše víme, že pokud je $a - b$ dělitelné třemi, pak i $f(a) - f(b)$ je dělitelné třemi.

6. Vhodně použijte větu o polynomech s celočíselnými koeficienty.

7. Porovnejte členy s nejnižším stupněm na pravé a levé straně.

8. Aplikujte Rational Root Theorem.

9. Uvažte $g(x) = f(x) - 2008$. Hledejte maximální počet kořenů g. Pro kořeny x_i platí $-2007 = a \cdot x_1 \cdot x_2 \cdot \ldots \cdot x_n$, tedy $n \leq 5$.

10. Kdyby a bylo celočíselným kořenem f, muselo by z věty platit $a \mid 2011$ i $a \pm 1 \mid 2011$, což není možné.

11. Dosaďte „vysokou“ mocninu 10.

12. Zkoumejte kořeny polynomu $g(x) = xf(x) - 1$.

Literatura a zdroje

[1] Martin Sýkora: *Polynomy bez Viètových vztahů*, Sborník MKS, Hojsova Stráž, 2016.

Cèvova a Menealova věta

Jáchym Solecký

Abstrakt. Občas se můžete setkat s geometrickou úlohou, kdy máte za úkol dokázat, že tři body leží na jedné přímce. Nebo že tři úsečky se protínají v jednom bodě. Na tento typ úloh můžeme velmi často použít Cèvovu nebo Menealovu větu, případně kombinaci obou. V této přednášce se seznámíme s tím, co tyto věty říkají, a jak je použít na některé typy geometrických úloh.

Cèvova věta

Lemma 1. (O obsazích) *Na straně BC trojúhelníka ABC je zvolen bod D. Na úsečce AD je zvolen bod D'. Dokažte, že*

$$\frac{S_{ABD'}}{S_{ACD'}} = \frac{|BD|}{|DC|}.$$

Věta 2. (Cèvova věta) *V trojúhelníku ABC jsou na stranách BC, CA, AB postupně zvoleny body D, E, F. Dokažte, že přímky AD, BE, CF se protínají v jednom bodě právě tehdy, když platí*

$$\frac{|BD|}{|DC|} \cdot \frac{|CE|}{|EA|} \cdot \frac{|AF|}{|FB|} = 1.$$

Cèvova věta platí, i když je jen jeden z bodů na straně trojúhelníka a zbylé dva jsou na prodloužení odpovídajících stran.

Úloha 3. Dokažte pomocí Cèvovy věty, že se

(i) těžnice,
(ii) osy úhlů,
(iii) výšky

v trojúhelníku protínají v jednom bodě.

Úloha 4. Na stranách BC, CA trojúhelníku ABC jsou dány body D, E tak, že $|BD| : |DC| = |CE| : |EA| = 2$. Označme X průsečík AD a BE a F průsečík CX a AB. Určete $|BF| : |FA|$.

Úloha 5. (Gergonnův bod) Kružnice vepsaná trojúhelníku ABC se dotýká jeho stran BC, CA, AB postupně v bodech D, E, F. Dokažte, že úsečky AD, BE, CF se protínají v jednom bodě.

Úloha 6. Rovnoběžka se stranou BC trojúhelníku ABC protíná strany AB, AC v bodech X, Y. Dokažte, že průsečík úseček BY, CX leží na A-těžnici.

Úloha 7. Dokažte, že přímky spojující středy stran se středy odpovídajících výšek (tj. střed strany BC se středem výšky na stranu BC apod.) procházejí jedním bodem.

Úloha 8. Kružnice připsané trojúhelníku ABC se dotýkají jeho stran BC, CA, AB v bodech T, U, V. Dokažte, že přímky AT, BU, CV procházejí jedním bodem.

Lemma 9. (O poměrech) *V trojúhelníku ABC je na straně BC zvolen bod D. Dokažte, že*

$$\frac{|BD|}{|DC|} = \frac{|AB| \sin \sphericalangle BAD}{|CA| \sin \sphericalangle CAD}.$$

Věta 10. (Cèvova věta, trigonometrická verze) *Na stranách BC, CA, AB trojúhelníku ABC jsou dány body D, E, F. Pak se přímky AD, BE, CF protínají v jednom bodě právě tehdy, když*

$$\frac{\sin \sphericalangle DAC}{\sin \sphericalangle BAD} \cdot \frac{\sin \sphericalangle EBA}{\sin \sphericalangle CBE} \cdot \frac{\sin \sphericalangle FCB}{\sin \sphericalangle ACF} = 1.$$

Úloha 11. (Isogonální kamarád) Na stranách BC, CA, AB trojúhelníku ABC jsou dány body D, E, F tak, že úsečky AD, BE, CF se protínají v jednom bodě. Přímky AD, BE, CF zobrazíme podle příslušných os vnitřních úhlů trojúhelníku ABC. Dokažte, že vzniklé přímky opět procházejí jedním bodem.

Úloha 12. Je dán trojúhelník ABC s výškami AD, BE, CF. Označme M, N, P středy úseček EF, FD, DE. Dokažte, že přímky AM, BN, CP procházejí jedním bodem.

Menealova věta

Věta 13. (Menealova věta) *Je dán trojúhelník ABC. Body D, E, F leží po řadě na přímkách BC, CA, AB tak, že buď jeden z nich, nebo všechny tři leží vně trojúhelníku ABC. Pak body D, E, F leží v přímce právě tehdy, když platí*

$$\frac{|AE|}{|EC|} \cdot \frac{|CD|}{|DB|} \cdot \frac{|BF|}{|FA|} = 1.$$

Úloha 14. V trojúhelníku ABC označme N střed těžnice AM a P bod na straně AC takový, že $|AC| = 3|AP|$. Rozhodněte, zda body B, N, P leží v přímce.

Úloha 15. Je dán trojúhelník ABC s vepsištěm I. Osa úhlu u vrcholu A protíná stranu BC v bodě D. Pomocí délek stran vyjádřete hodnotu poměru $|AI|/|ID|$.

Úloha 16. (Van Aubelova věta) V trojúhelníku ABC jsou na stranách BC, CA, AB postupně zvoleny body D, E, F tak, že přímky AD, BE, CF se protínají v jednom bodě X. Dokažte, že pak

$$\frac{|AX|}{|XD|} = \frac{|AE|}{|EC|} + \frac{|AF|}{|FB|}.$$

Úloha 17. Kružnice vepsaná různostrannému trojúhelníku ABC se dotýká jeho stran BC, CA, AB postupně v bodech D, E, F. Uvnitř trojúhelníku ABC je dán bod X tak, že kružnice vepsaná trojúhelníku BCX se dotýká BC i v D. Označme dále Y, Z její body dotyku se stranami XB, XC. Dokažte, že přímky EF, YZ a BC procházejí jedním bodem.

Úloha 18. (Newton-Gauss line) Je dán konvexní čtyřúhelník $ABCD$, jehož protilehlé strany nejsou rovnoběžné. Označme $Q = BC \cap DA$ a $R = AB \cap CD$. Dále označme X, Y, Z postupně středy úseček AC, BD, QR. Dokažte, že body X, Y, Z leží na jedné přímce.

Další úlohy

Nebojte se použít Cèvovu a Menealovu větu v jedné úloze víckrát. A nezapomeňte ani na podobnost, mocnost a sinovou větu. Všechny pracují s poměry, a tak se můžou hodit.

Úloha 19. Úhlopříčky konvexního čtyřúhelníku $ABCD$ se protínají v bodě P. Dokažte, že

$$\frac{\sin \sphericalangle DAP}{\sin \sphericalangle APB} \cdot \frac{\sin \sphericalangle ABP}{\sin \sphericalangle PCB} \cdot \frac{\sin \sphericalangle BCP}{\sin \sphericalangle PCD} \cdot \frac{\sin \sphericalangle CDP}{\sin \sphericalangle PDA} = 1.$$

Úloha 20. Na stranách BC, CA, AB trojúhelníku ABC jsou dány body D, E, F tak, že úsečky AD, BE, CF se protínají v jednom bodě. Kružnice opsaná trojúhelníku DEF protne strany podruhé v bodech D', E', F'. Dokažte, že AD', BE', CF' se také protnou v jednom bodě.

Úloha 21. Na přímce p jsou dány body A, Z, B v tomto pořadí, přičemž Z není středem AB. Zvolme libovolně bod $X \notin p$ a poté libovolně zvolme bod Y na úsečce XZ. Označme $D = AX \cap BY$ a $E = BX \cap AY$. Dostali jsme tak přímku DE, jejíž konstrukce závisí na zvolených bodech X, Y. Dokažte, že všechny takto zkonstruované přímky DE procházejí jedním pevným bodem.

Úloha 22. Je dán trojúhelník ABC a uvnitř něj bod P. Bodem P prochází přímka p. Bod A' dostaneme jako průsečík strany BC a obrazu přímky AP podle osy p. Analogicky dostaneme body B' a C'. Dokažte, že body A', B', C' leží na jedné přímce. (USAMO 2012)

Úloha 23. Je dán trojúhelník ABC. Přímka skrz jeho těžiště G protne strany AB, AC v bodech F, E. Dokažte, že

$$\frac{|BF|}{|FA|} + \frac{|CE|}{|EA|} = 1.$$

Úloha 24. Nechť ABC je rovnoramenný trojúhelník s $|AB| = |AC|$. Kružnice vepsaná se dotýká stran BC a CA postupně v bodech D a E. Bodem B vedeme přímku různou od BE, která protne kružnici vepsanou v bodech F a G. Nechť BC protíná přímky EF a EG postupně v bodech K a L. Dokažte, že $|DK| = |DL|$.
(MEMO 2008)

Úloha 25. (Pascalova věta) Body A, B, C, D, E, F leží na kružnici v libovolném pořadí. Nechť $L = AB \cap DE$, $M = BC \cap EF$, $N = CD \cap FA$. Dokažte, že L, M, N leží na jedné přímce.

Návody

1. Dokažte, že $\frac{S_{ABD}}{S_{ACD}} = \frac{|BD|}{|DC|}$.

6. Dokažte pomocí Cèvovy věty, že obě úsečky a A-těžnice se protínají v jednom bodě.

7. Použijte Cèvovu větu na trojúhelník ze středních příček.

8. Vyjádřete délky BT, ... pomocí délek stran trojúhelníka ABC.

12. Použijte lemma o poměrech pro trojúhelníky FAE, ECD, DBF. Pak Cèvovu větu pro výšky v ABC upravte na požadovanou goniometrickou verzi s body M, N a P.

15. Osa úhlu dělí protější stranu v poměru délek přilehlých stran. Menealovu větu použijte pro trojúhelník ADC.

16. Menealovu větu použijte pro trojúhelník ABD.

17. Zvlášť spočítejte, kde protnou přímku BC přímky EF a YZ.

18. Menealovu větu použijte pro trojúhelník ze středních příček trojúhelníku ABQ.

19. Použijte lemma o poměrech pro trojúhelníky ABC, BCD, CDA a DAB.

20. Použijte mocnost bodů A, B, C ke kružnici opsané trojúhelníku DEF.

21. Hlavní roli hraje trojúhelník ABC, pro který použijte Menealovu i Cèvovu větu.

22. Vyjádřete si poměry z Menealovy věty pomocí lemmatu o poměrech.

23. Vyjádřete si oba zlomky z Menealovy věty pro přímku EF a trojúhelníky ABM, resp. ACM, kde M je střed BC (označte si průsečík EF a BC).

24. Označte si $X = CG \cap AB$ a použijte Menealovu větu pro trojúhelník XBC dvakrát – s body E, G, L a s body E, F, K. Pak pomůže mocnost.

25. Prodlužte sudé strany šestiúhelníku $ABCDEF$, a tím vytvořte trojúhelník XYZ. Pro ten pak napište tři Menealovy věty pro tři různé přímky.

Literatura a zdroje

[1] Pavel Šalom, Pepa Tkadlec: Cèvova věta, seminář AoPS, 2014.
[2] Pavel Šalom, Pepa Tkadlec: Menealova věta, seminář AoPS, 2014.
[3] Tomáš Pavlík: Levely a Menealova věta, Mentaurov, 2013.
[4] Tomáš Pavlík: Cèvova a Menealova věta, Domaslav, 2010.

IMO dělitelné třemi

Rado van Švarc

Abstrakt. Na přednášce budeme procházet nejtěžší příklady z několika ročníků soutěže IMO.

Příklad 1. Ukažte, že pro každé přirozené číslo n platí

$$\left\lfloor \frac{n+2^0}{2^1} \right\rfloor + \left\lfloor \frac{n+2^1}{2^2} \right\rfloor + \cdots + \left\lfloor \frac{n+2^{n-1}}{2^n} \right\rfloor = n.$$

(IMO 1968 – 6)

Příklad 2. Mějme čtvercovou tabulku $n \times n$ nezáporných celých čísel. Předpokládejme, že kdykoli má nějaké políčko P nulovou hodnotu, pak součet hodnot na všech políčkách, která mají s P jednu společnou souřadnici, je vyšší nebo roven n. Dokažte, že součet hodnot na všech políčkách je roven alespoň $\frac{n^2}{2}$. (IMO 1971 – 6)

Příklad 3. Nalezněte všechny funkce $f : \mathbb{N} \to \mathbb{N}$ takové, že $f(n+1) > f(f(n))$. (IMO 1977 – 6)

Příklad 4. Jaká je nejvyšší možná hodnota výrazu $m^2 + n^2$, kde m a n leží mezi čísly $1, 2, \ldots, 1981$ a splňují $(n^2 - mn - m^2)^2 = 1$. (IMO 1981 – 3)

Příklad 5. Konečně mnoho bodů v rovině s celočíselnými souřadnicemi je vybráno. Je pro každou takovou množinu možné obarvit body červeně a modře tak, aby se na každé přímce rovnoběžné se souřadnicovou osou počet červených a modrých bodů lišil nanejvýš o jedna? (IMO 1986 – 6)

Příklad 6. Říkáme, že permutace $(x_1, x_2, \ldots, x_{2n})$ množiny $\{1, 2, \ldots, 2n\}$ má vlastnost P, pokud pro alespoň jedno $i \in \{1, 2, \ldots, 2n-1\}$ platí $|x_i - x_{i+1}| = n$. Ukažte, že pro každé n existuje více permutací s vlastností P než bez ní. (IMO 1989 – 6)

Příklad 7. Na nekonečné šachovnici hrajeme partii solitéru následujícím způsobem: Na začátku máme n^2 figurek rozestavených do čtverce o straně n. V každém kroku můžeme jednou figurkou skočit přes jinou na prázdné políčko a přeskočenou figurku odstranit. Pro která n je možné po několika krocích skončit s pouze jednou figurkou? (IMO 1993 – 3)

Příklad 8. Ukažte, že existuje množina A přirozených čísel taková, že pro libovolnou množinu prvočísel S existují přirozená čísla $k \geq 2$, $m \in A$ a $n \notin A$, pro které platí,že m i n jsou součinem k různých prvočísel z S. (IMO 1994 – 6)

Příklad 9. Nalezněte všechny dvojice přirozených čísel $m, n \geq 3$ takové, že pro nekonečně mnoho přirozených čísel a je

$$\frac{a^m + a - 1}{a^n + a^2 - 1}$$

přirozené číslo. (IMO 2002 – 3)

Příklad 10. V rovině leží n kružnic s jednotkovým poloměrem a středy $O_1, \ldots, O_n$. Pokud každá přímka má kontakt s nanejvýš dvěma z těchto kružnic, ukažte, že

$$\sum_{1 \leq i < j \leq n} \frac{1}{O_i O_j} \leq \frac{(n-1)\pi}{4}.$$

(IMO 2002 – 6)

Příklad 11. Nechť $a_1, a_2, \ldots, a_n$ jsou navzájem různá kladná celá čísla a M je množina $n-1$ kladných celých čísel neobsahující číslo $s = a_1 + a_2 + \cdots + a_n$. Luční kobylka skáče podél číselné osy, přičemž začíná v bodě 0 a provede doprava n skoků o délkách $a_1, a_2, \ldots, a_n$ v určitém pořadí. Dokažte, že pořadí skoků lze zvolit tak, že se kobylka neoctne na žádném čísle z množiny M. (IMO 2009 – 6)

Příklad 12. „Hra na chytrou horákyni“ je hrou mezi dvěma hráči A a B. Pravidla hry závisejí na dvou kladných celých číslech k a n, která jsou známa oběma hráčům. Na začátku hry zvolí hráč A celá čísla x a N, kde $1 \leq x \leq N$, a z nich prozradí (po pravdě) hráči B pouze číslo N, číslo x si nechá pro sebe. Hráč B se nyní snaží získat informace o čísle x kladením otázek hráči A. Může přitom klást pouze otázky následujícího typu: vybere libovolnou podmnožinu S kladných celých čísel (může vybrat i množinu, kterou již zvolil v některé z předchozích otázek) a zeptá se hráče A na to, zda číslo x leží v S. Hráč B může položit libovolně mnoho takovýchto otázek. Na každou otázku musí hráč A okamžitě odpovědět, a to buď „ano“, nebo „ne“. Při odpovědích však může hráč A lhát, dokonce libovolně mnohokrát; jediným omezením je pouze to, aby mezi každými jeho $k+1$ za sebou následujícími odpověďmi byla alespoň jedna pravdivá. Poté, co hráč B skončí s kladením všech svých otázek, zadá nějakou, nejvýše n-prvkovou, podmnožinu X kladných celých čísel. Pokud číslo x náleží do množiny X, tak hráč B vyhrál, jinak prohrál. Dokažte:

(1) Pro $n \geq 2^k$ má hráč B vyhrávající strategii.
(2) Pro každé dostatečně velké celé kladné k (tj. od jisté meze pro každé celé kladné číslo k) existuje číslo $n \geq 1,99^k$ takové, že neexistuje vyhrávající strategie za hráče B.

(IMO 2012 – 3)

Příklad 13. Mějme celé číslo $n \geq 3$ a $n+1$ bodů rovnoměrně rozložených na kružnici. Uvažujme taková označkování těchto bodů číselnými znaky 0, 1, ... n, ve kterých je použit každý z těchto znaků právě jednou. Dvě označkování považujeme za stejná, jestliže jedno přejde na druhé nějakou rotací kružnice. Označkování nazveme *krásným*, jestliže pro libovolné čtyři znaky $a < b < c < d$ takové, že $a + d = b + c$, tětiva spojující body označené znaky a a d neprotíná tětivu spojující body označené znaky b a c. Nechť M značí počet krásných označkování a N počet uspořádaných dvojic (x, y) kladných celých čísel takových, že $x + y \leq n$ a $\mathrm{NSD}(x, y) = 1$. Dokažte rovnost $M = N + 1$. (IMO 2013 – 6)

Příklad 14. Říkáme, že přímky v rovině jsou v obecné poloze, pokud žádné dvě nejsou rovnoběžné a žádné tři neprocházejí jedním bodem. Množina přímek v obecné poloze rozděluje rovinu na oblasti, z nichž některé mají konečný obsah. Nazýváme je konečné oblasti příslušné dané množině přímek. Pro každé dostatečně velké n dokažte, že v libovolné množině n přímek v obecné poloze je možné obarvit modře aspoň $\sqrt{n}$ přímek tak, že žádná z příslušných konečných oblastí nebude mít celou hranici modrou. (IMO 2014 – 6)

Příklad 15. V rovině je dáno n, $n > 2$, úseček tak, že se libovolné dvě z nich protínají ve vnitřním bodě obou, ale žádné tři se neprotínají v jednom bodě. Pepa vybere koncový bod každé úsečky a umístí do něj žábu, směrem k druhému koncovému bodu. Poté $(n-1)$-krát tleskne. Na každé tlesknutí každá žába neprodleně poskočí na následující průsečík na své úsečce. Žádná žába nemění směr svých skoků. Pepa by chtěl umístit žáby tak, aby žádné dvě z nich nebyly po žádném tlesknutí ve stejném průsečíku.

(1) Dokažte, že Pepa tak může učinit, je-li n liché.
(2) Dokažte, že Pepa tak nemůže učinit, je-li n sudé.

(IMO 2016 – 6)

Příklad 16. Lovec a neviditelný zajíc hrají hru v Euklidovské rovině. Zajícova počáteční poloha A_0 a lovcova počáteční poloha B_0 jsou stejné. Po $n-1$ kolech hry se zajíc nachází v bodě A_{n-1} a lovec v bodě B_{n-1}. V n-tém kole postupně proběhnou tři věci:

(1) Zajíc se neviděn přesune do bodu A_n takového, že vzdálenost mezi A_{n-1} a A_n je přesně 1.
(2) Sledovací zařízení nahlásí lovci bod P_n. Jediná záruka poskytnutá sledovacím zařízením je, že vzdálenost mezi P_n a A_n je nejvýše 1.
(3) Lovec se viditelně přesune do bodu B_n takového, že vzdálenost mezi B_{n-1} a B_n je přesně 1.

Může lovec vždy (tj. bez ohledu na to, jak se hýbe zajíc, a na to, jaké body hlásí sledovací zařízení) volit své pohyby tak, aby měl jistotu, že po 10^9 kolech bude vzdálenost mezi ním a zajícem nejvýše 100? (IMO 2017 – 3)

Návody

1. Binárka.

2. Uvažte sloupec/řádek s nejmenším součtem. BÚNO se jedná o řádek a součet jeho čísel je k. Pak umíte součty $n-k$ sloupců (z nul v daném řádku) zdola odhadnout jako $n-k$ a součet zbylých k sloupců (z minimality) pomocí k.

3. Indukcí podle m ukažte, že pokud $n \geq m$, pak $f(n) \geq m$.

4. Ukažte, že pokud (n, m) vyhovuje, vyhovuje i $(m-n, m)$, $(n+m, m)$ a $(-m, n)$ a odtud odvoďte tvar vyhovujících dvojic.

5. Ano! Odstraňujte cykly, a rozestavění bez cyklů obarvěte přímočaře.

6. V permutaci bez vlastnosti P dejte první prvek k jeho „kamarádovi“. Tím získáte prosté zobrazení z permutací bez P do permutací s P.

7. Protože kdykoliv máme tři figurky vedle sebe, které na jednom konci mají na jedné straně prázdno a na druhé figurku, umíme tuto trojici vyrušit, a tím udělat konstrukci pro n nedělitelné třemi. Pro n dělitelné třemi obarvíme šachovnici přirozeně třemi barvami a zkoumáme paritu.

8. Zvolte A tak, že $p_1 \cdot \ldots \cdot p_k \in A \Leftrightarrow p_1 \cdot \ldots \cdot p_k \equiv 1 \pmod{k+1}$.

9. Ukažte, že pokud tato dělitelnost skutečně nastává nekonečně často, pak nastává vždy a polynomiálně. Pak využijte, že $a^n + a^2 - 1$ má reálný kořen mezi 0 a 1.

10. Všechny kružnice ohraničte jednou velikou a zkoumejte, jak velké části této velké kružnice vytínají společné vnitřní tečny a kolikrát je tímto způsobem možné „pokrýt“ jednu část velké kružnice.

11. Dokazujte indukcí podle počtu skoků. Skákejte první skok nejdelším skokem a rozeberte na tři případy. Případ, kdy prvním skokem přeskočíte několik „min“ a na jednu spadnete, vyřešte posunutím všech přeskočených min o délku tohoto skoku a po použití indukčního předpokladu prohozením prvních dvou skoků.

12. Pro část jedna binárním vyhledáváním najděte v každých $k+1$ krocích jeden prvek, který určitě není x. Pro část dva se snažte minimalizovat součet $\sum_{i=1}^{n+1} \lambda^{m_i}$, kde m_i je počet odpovědí v každém kroku, které jsou nepravdivé o i a λ je dostatečně blízké dvojce.

13. Indukcí dokažte, že všechna krásná označkování vzniknou zvolením reálného čísla $r \in (0, 2\pi)$ a následným skákáním po jednotkové kružnici o r a postupným psaním čísel 1, 2, … n. Množinu N dvojic bijektivně zobrazte na takové skoky r, pro které se některé body překryjí. Zbytek nahlédněte.

14. Obarvěte co nejvíce přímek na modro. Pro každé zbylé přiřaďte jednu „krizovou oblast“ a v každé takové oblasti rovnoměrně rozdělte mezi průsečíky dvou modrých přímek hodnotu jednu. Ukažte, že žádný průsečík dvou modrých přímek nemá větší součet hodnot, než 2.

15. Kolem všech úseček nakreslete jednu velkou kružnici, úsečky protáhněte a zkoumejte dvojice „sousedících“ úseček.

16. Zajíc opakuje každých 200 kroků následující proces - ukáže lovci, kde přesně je, a následně utíká do bodu ve vzdálenosti 200 od jeho současné polohy a ve vzdálenosti jedno od polopřímky opačné k polopřímce spojující zajíce a lovce. Pokud sledovací zařízení vždy ukáže přímo na přímku, tak lovec neví, do kterého ze dvou takových možných bodů zajíc utíká a zajíc díky tomu umí vždy zvýšit svou vzdálenost o alespoň $\frac{1}{2}$.

Literatura a zdroje

[1] Mirek Olšák: *Kdopak by se IMO šestky bál?*, Uhelná Příbram, 2014.
[2] *mathlinks.ro*

Symediány

Rado van Švarc

Abstrakt. Symediány patří k velice zajímavým oblastem moderní geometrie trojúhelníka. Jedná se o pokročilejší, ale pro olympiádní matematiku velice důležité, téma, protože rozmanitých vlastností symedián se dá v úlohách často využít. Příspěvek obsahuje nejprve několik nejdůležitějších tvrzení a poté sbírku úloh. Na konci příspěvku najdete nápovědy ke zmíněným tvrzením i úlohám.

Než začneme se symediánami, připomeneme si některé související pojmy.

Definice. Mějme daný úhel XVY a jeho osu o. Přímky p a q nazveme *antirovnoběžné*, pokud osový obraz přímky p podle o je rovnoběžný s přímkou q. Pokud navíc $V \in p$ a $V \in q$, říkáme, že p a q jsou izogonální.

Jedna ze základních vlastností antirovnoběžek je, že jejich průsečíky s přímkami VX a VY leží na jedné kružnici.

Nyní si můžeme definovat, co jsou to symediány.

Definice. Symediány trojúhelníka jsou přímky izogonální s jeho těžnicemi.

Tvrzení 1. *Symediány se protínají v jednom bodě, který nazveme Lemoinovým bodem a budeme ho značit K.*

Ještě než začneme s důležitými tvrzeními a příklady, dohodneme se na značení. Symediánu skrz vrchol A nazveme A-symediána. Průsečíky symedián se stranami BC, CA, AB značíme postupně S_a, S_b, S_c.

Tvrzení 2. *Symediána je množina středů antirovnoběžek s protější stranou.*

To samé se dá říct ještě jiným způsobem. Protíná-li antirovnoběžka ke straně BC přímky AB, AC v bodech B', C', tak symediána v trojúhelníku ABC je těžnice v trojúhelníku $AB'C'$ a naopak těžnice v ABC je symediána v $AB'C'$.

Z následujícího tvrzení se dá snadno dokázat, že se symediány protínají v jednom bodě.

Tvrzení 3. *Symediána z vrcholu A je množina vnitřních bodů X úhlu BAC, pro něž je*

$$\frac{d(X, AB)}{d(X, AC)} = \frac{c}{b}.$$

Tvrzení 4. *A-symediána prochází průsečíkem tečen ke kružnici opsané v bodech B a C.*

Další vlastnosti symedián

Tvrzení 5. *S_a dělí stranu BC v poměru*

$$\frac{BS_a}{S_aC} = \frac{c^2}{b^2}.$$

Tvrzení 6. *Mějme bod X na symediáně a veďme jím antirovnoběžky ke stranám AC, AB. Ty protnou přímky AB, AC v bodech T, U. Pak platí $|XT| = |XU|$.*

Tvrzení 7. *Udělejme tečny ke kružnici opsané v bodech A, B, C. Ty ohraničují takzvaný Gergonnův trojúhelník $E_aE_bE_c$ (E_a je průsečík tečen z vrcholů B, C). Pak Lemoinův bod trojúhelníku ABC je Gergonnův bod trojúhelníku $E_aE_bE_c$ (to je průsečík přímek AD, BE, CF).*

Tvrzení 8. *Nechť X je bod na kružnici opsané různý od A, pro který platí*

$$\frac{|XB|}{|XC|} = \frac{c}{b}.$$

Pak AX je A-symediána. Navíc BC, XA, CB jsou symediány v trojúhelnících BXA, XBC, BAX.

Obtížnější tvrzení

Tvrzení 9. (Kosinová kružnice) *Bodem K vedeme antirovnoběžky se stranami. Ty na obvodu trojúhelníka vytnou šestici koncyklických bodů. Střed této kružnice je K.*

Tvrzení 10. (Lemoinova kružnice) *Bodem K vedeme rovnoběžky se stranami. Ty na obvodu trojúhelníka vytnou šestici koncyklických bodů. Střed kružnice, na níž leží, je střed úsečky OK.*

Tvrzení 11. *Nechť M je střed strany BC a X střed A-výšky. Pak na MX leží Lemoinův bod.*

Tvrzení 12. (Tuckerovy kružnice) *Strany trojúhelníka „přistejnolehlíme“ ke K s koeficientem menším než jedna. Obrazy na obvodu trojúhelníka vytnou šestici koncyklických bodů. Střed kružnice je na úsečce OK.*

Tvrzení 13. (Lemoinův teorém) *Lemoinův bod je jediný bod, který je těžištěm svého pedal triangle, tedy trojúhelníku, jehož vrcholy jsou projekce K na strany.*

Příklady

Příklad 14. Symediána leží vždy mezi osou úhlu a výškou.

Příklad 15. Nechť D, E, F jsou body dotyku kružnice vepsané postupně se stranami BC, CA, AB. Dokažte, že ABC je rovnostranný, pravě když je těžiště trojúhelníku ABC Lemoinovým bodem trojúhelníku DEF.

Příklad 16. Je dán trojúhelník ABC, v němž $|AC| = 2|AB|$. Ke kružnici k jemu opsané sestrojme tečny v bodech A a C a jejich průsečík označme P. Dokažte, že průsečík přímky BP a osy strany BC leží na kružnici k. (ČR TST 2013)

Příklad 17. Nechť ABC je rovnoramenný trojúhelník se základnou BC. Bod P leží uvnitř trojúhelníka tak, že $|\sphericalangle CBP| = |\sphericalangle ACP|$. Označme M střed strany BC. Ukažte, že $|\sphericalangle BPM| + |\sphericalangle CPA| = 180°$. (Poland 2000)

Příklad 18. V konvexním čtyřúhelníku $ABCD$ pro střed M úsečky AC platí $|\sphericalangle BMC| = |\sphericalangle CMD| = |\sphericalangle BAD|$. Dokažte, že $ABCD$ je tětivový.
(Poland 2005)

Příklad 19. Nechť MN je přímka rovnoběžná s BC, kde M, N leží na stranách AB, AC. Přímky BN a CM se protínají v bodě P. Kružnice opsané trojúhelníkům BMP a CNP se protínají ve dvou různých bodech P a Q. Dokažte $|\sphericalangle BAQ| = |\sphericalangle CAP|$. (Balkan MO 2009)

Příklad 20. Nechť ABC je ostroúhlý trojúhelník. Osa úhlu u vrcholu A protne stranu BC v bodě D a kružnici opsanou trojúhelníku ABC v bodě E (různém od A). Kružnice s průměrem DE protne podruhé kružnici opsanou v bodě F. Dokažte, že AF je symediána v trojúhelníku ABC. (ARO 2009)

Příklad 21. Trojúhelník ABC je vepsaný do kružnice ω. Tečny k ω v bodech B a C se protínají v T. Bod S leží na polopřímce BC tak, že $AS \perp AT$. Body B_1 a C_1 leží na polopřímce ST (s C_1 mezi B_1 a S) tak, že $|B_1T| = |BT| = |C_1T|$. Dokažte, že trojúhelníky ABC a AB_1C_1 jsou podobné. (USA TST 2007)

Literatura a zdroje

Tento příspěvek je beze změn převzat od Štěpána Šimsy, který jej vytvořil na soustředění v Uhelné Příbrami (2014) a kterému tímto děkuji (a toto poděkování je zkopírované zpod jednoho Vikiho příspěvku).

[1] Sborník *i*KS 1, příspěvek Michala Rolínka, *http://iksko.org/sous.php*
[2] PraSečí archiv, *http://mks.mff.cuni.cz/archive/archive.php*
[3] Cut The Knot, *http://cut-the-knot.org*
[4] Mathematical Reflections 4, 2013, *https://www.awesomemath.org/assets/PDFs/MR4_Symmedians.pdf*
[5] 107 Geometry Problems

Sto vězňů a žárovka

Michal Töpfer

Abstrakt. Příspěvek se zamýšlí nad známým komunikačním problémem, kde se agenti (vězni) pomocí jednoduchého média (žárovky) a lokálních změn systému (přepnutí žárovky) snaží předat globální informaci týkající se jich všech. Na první pohled je až neuvěřitelné, že lze úlohu vůbec vyřešit. Když vězeň vidí svítící žárovku, neví, kdo ji rozsvítil; pokud se rozhodne zhasnutou žárovku rozsvítit, neví zase, kdo ji poté uvidí svítit. Přesto ukážeme, že pomocí takto jednoduchého komunikačního prostředku lze navrhnout protokol k přenosu mnoha informací.

Budeme se zabývat dnes už docela známou komunikační úlohou. Nebyla vždy takto populární a do obecného povědomí se dostala až začátkem jednadvacátého století. Vše začalo v roce 2002, kdy americká technologická společnost IBM vypsala soutěž týkající se této úlohy. Poté se objevily nové varianty hádanky a vědecké články, které vedou k pozoruhodným aplikacím při návrhu komunikačních protokolů. Především teoreticky se jedná o velmi zajímavý problém a existuje mnoho dosud nezodpovězených otázek souvisejících s tímto tématem.

Zadání

Do nejmenované věznice právě nastoupilo sto nových vězňů. Bachař jim dá šanci vymanit se z jejich trestu. Počínaje zítřkem budou vězněni v oddělených celách a každý den bude vybrán jeden vězeň k výslechu. Jediným zajímavým předmětem ve výslechové místnosti je běžná žárovka, což je také jediný prostředek, pomocí kterého spolu mohou vězni komunikovat. Žárovku vidí pouze právě vyslýchaný vězeň a může ji dle svého uvážení zhasnout nebo rozsvítit. Kdykoliv může kterýkoliv vězeň ohlásit: „Všech sto vězňů již bylo alespoň jednou vyslechnuto.“ Pokud je to pravda, budou všichni okamžitě propuštěni, v opačném případě budou všichni popraveni. Pomozte vězňům domluvit si spolehlivou strategii, díky které se jim podaří dosáhnout svobody.

Předpoklady

(a) Každý vězeň bude vyslechnut nekonečněkrát. V některých případech budeme potřebovat dokonce, aby každý den byl vyslechnut náhodný vězeň.
(b) Žárovka je na začátku zhasnutá.
(c) Každý den je vyslechnut právě jeden vězeň.

Varianty úlohy

(1) **Více žárovek** – V místnosti není jen jedna žárovka, ale je jich více (jsou nezávislé).
(2) **Zákeřný bachař** – Je dáno předem známé přirozené číslo k. Bachař může k-krát během celého procesu změnit stav žárovky (rozsvítit nebo zhasnout).
(3) **Všichni musí ohlásit** – Vězni budou propuštěni jedině tehdy, pokud všichni ohlásí, že již všichni byli vyslechnuti.
(4) **Propuštěný po ohlášení** – Všichni vězni musejí ohlásit, ale pokud někdo ohlásí, je okamžitě propuštěn a už nikdy nebude vyslýchán.
(5) **Červené a modré cely** – Někteří vězni jsou ubytovaní v červených celách, zatímco ostatní v modrých. Při ohlášení musí vězeň také nahlásit, kolik jeho kolegů bydlí v červených a kolik v modrých celách.
(6) A **pošle zprávu** B – Předem určený vězeň A musí poslat zprávu (přirozené číslo) vězni B.
(7) **Čísla v celách** – V každé cele je napsáno jedno celé číslo. Vězeň, který ohlašuje, musí nahlásit také všechna tato čísla.
(8) **Všichni posílají zprávy všem** – Navrhněte obecný protokol, pomocí kterého si budou moci navzájem posílat jakékoliv zprávy.
(9) **Všichni musejí ohlásit ve stejný den** – Vězni mohou ohlásit, že již všichni byli vyslechnuti, také ve dny, kdy nejsou vyslýcháni. Budou propuštěni jedině tehdy, pokud to všichni ohlásili ve stejný den. Ohlásí-li to někdo dříve, budou všichni popraveni.
(10) **Náhodné časy** – Řešte všechny předcházející úlohy bez předpokladu (c). Vězni jsou vyslýcháni v náhodné časy a nemohou tedy počítat dny.

Poděkování

Na tomto místě bych rád poděkoval Filipu Hláskovi. Tento příspěvek je upravenou verzí jeho přednášky ze soustředění v Zásadě na podzim 2014.

Literatura a zdroje

[1] IBM Research, *100 prisoners and a lightbulb challenge*, 2002.
[2] *https://www.math.washington.edu/~morrow/336_11/papers/yisong.pdf*
[3] *http://www.ocf.berkeley.edu/~wwu/papers/100prisonersLightBulb.pdf*
[4] *http://www.segerman.org/prisoners.pdf*
[5] *http://personal.us.es/hvd/newpubs/FinalLightKR.pdf*

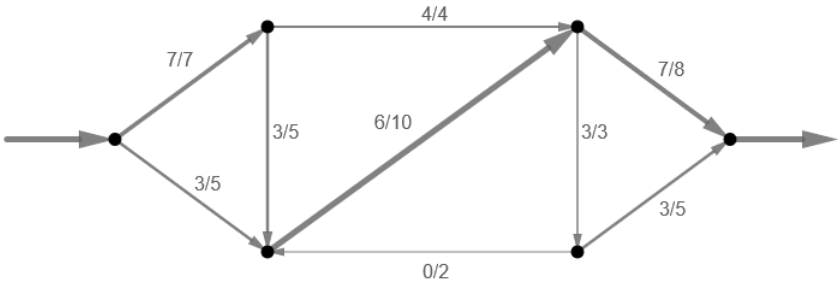
Toky v sítích

Pavel Turek

Abstrakt. Vysvětlíme si, co je myšleno pojmem tok v síti. Dokážeme základní větu o maximálním toku a popíšeme, jak takový tok najít. Nakonec se podíváme na pár olympiádních a grafových příkladů.

Úvod

Představme si systém orientovaných trubek s danými kapacitami s přívodem (nazývaným *zdroj*) a odtokem (nazývaným *stok*) a místy, kde se trubky kříží. Takový systém nazveme sítí. *Tok* pak bude situace, kdy sítí pustíme vodu ze zdroje do stoku. Množství vody vypuštěné ze zdroje/vpuštěné do stoku se nazývá *velikost toku*. Příkladem toku s velikostí 10 v síti je následující obrázek.



Definice pomocí grafů

Sítí nadále budeme rozumět orientovaný graf s (konečnou) množinou vrcholů V a s dvěma různými speciálními vrcholy – zdrojem a stokem. Navíc pro každou hranu z vrcholu i do j je dána její kapacita $c_{ij} \geq 0$. Tok pak získáme tím, že ke každé hraně (vedoucí z i do j) přiřadíme nezáporné číslo $x_{ij} \leq c_{ij}$.

Zároveň musí platit: $$\sum_{j \in V} x_{ij} - \sum_{j \in V} x_{ji} = \begin{cases} v & \text{pokud } i \text{ je zdroj,} \\ -v & \text{pokud } i \text{ je stok,} \\ 0 & \text{jinak.} \end{cases}$$

Velikost toku je výše zmíněné v.

Maximální velikost toku

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

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

Tvrzení. *Každá síť má tok maximální velikosti.*

Definice. *Řez* je množina vrcholů S obsahující zdroj a neobsahující stok. Jeho velikostí rozumíme $\sum_{i\in S}\sum_{j\in V\setminus S} c_{ij}$.

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

Definice. *Zlepšující cesta* mezi vrcholy u a v je posloupnost vrcholů v_1, v_2, ... , v_n s $v_1 = u$ a $v_n = v$ a navíc pro $i \in \{1, 2, ..., n-1\}$ buď $c_{v_iv_{i+1}} - x_{v_iv_{i+1}} > 0$ nebo $x_{v_{i+1}v_i} > 0$.

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

Fordův–Fulkersonův algoritmus

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

(i) Vezmeme vhodný tok s racionálními x_{ij}, třeba nulový.
(ii) Pokud neexistuje další zlepšující cesta ze zdroje do stoku, jsme hotovi.
(iii) Najdeme zlepšující cestu v_1, v_2, ... , v_n ze zdroje do stoku a zvýšíme průtok touto cestou o δ, kde $\delta = \min_i \max\{c_{v_iv_{i+1}} - x_{v_iv_{i+1}},\ x_{v_{i+1}v_i}\}$.
(iv) Vrátíme se k (ii).

Tvrzení. *Fordův–Fulkersonův algoritmus nalezne v konečném čase maximální velikost toku pro sítě s racionálními kapacitami.*

Důsledek. *Pro síť s kapacitami rovnými celým číslům existuje tok s maximální velikostí a s celočíselnými x_{ij}.*

Příklady

Příklad 1. Je dána obdélníková tabulka reálných čísel taková, že součet každého řádku i sloupce je celočíselný. Dokažte, že je možné každé číslo v tabulce nahradit jeho dolní nebo horní celou částí tak, aby hodnoty čísel zůstaly nezměněny.

(IMO Shortlist 1998)

Příklad 2. V tabulce $n \times n$ jsou v políčkách nezáporná celá čísla a v každém řádku i sloupci je stejný kladný součet. Dokažte, že je možné postavit n šachových věží na nenulová políčka tak, aby se vzájemně neohrožovaly.

Příklad 3. (Hallova věta) Máme takový systém množin, že kdykoli sjednotíme několik z nich, bude sjednocení vždy obsahovat alespoň tolik prvků, kolik množin jsme sjednotili. Dokažte, že je možné v každé množině zakroužkovat jeden prvek tak, aby zakroužkované prvky byly navzájem různé.

Příklad 4. Řekneme, že graf je hranově k-souvislý, když je souvislý a zůstane souvislý i po odebrání libovolných $k-1$ nebo méně hran. Dokažte, že graf je hranově k-souvislý právě tehdy, když mezi každými dvěma vrcholy vede alespoň k hranově disjunktních cest.

Příklad 5. Ukažte, že Fordův–Fulkersonův algoritmus nemusí fungovat pro obecné reálné kapacity.

Návody

1. BÚNO jsou v tabulce čísla mezi 0 a 1. Postavte síť s celočíselnými kapacitami tak, aby vyplnění tabulky byl jeho maximální tok a využijte skutečnosti, že je možné najít stejně velký celočíselný tok.

2. BÚNO součty jsou 1. Sestavte síť s kapacitami 0 a 1 s maximálním tokem daným tabulkou a užijte tvrzení pro tyto sítě.

3. Kapacita 1 přitéká do jednotlivých množin, z každé množiny pak do jejích prvků a z každého prvku pak kapacita 1 do stoku.

4. Každá hrana má kapacitu 1, přímá aplikace základní věty o tocích.

5. (i) Zkuste nejdříve ukázat, že vynecháme-li ve Fordově–Fulkersonově algoritmu podmínku, že x_{ij} mají být racionální, tak nemusí fungovat.
(ii) Uvažujte 4 vrcholy + stok + zdroj, kde ze zdroje vedou hrany do všech 4 a ze všech 4 vedou hrany do stoku a ještě další 4 hrany jsou mezi 4 vrcholy.
(iii) Dejte hranám velké kapacity. Mohlo by se hodit nějak využít vlastností zlatého řezu v prvním toku. Není třeba řešením nějaké pěkné kvadratické rovnice?

Literatura a zdroje

[1] Mirek Olšák: *Toky v sítích*, Staré Město, Jaro 2015
[2] Ravindra K. Ahuja, Thomas L. Magnanti, James B. Orlin: *Network Flows: Theory, Algorithms, and Applications*, Prentice-Hall, Inc., 1993.
[3] Michael Tehranchi: *IB Optimisation*, *http://www.statslab.cam.ac.uk/~mike/optimisation/*

Obsah