Zásada

Sborník, podzim 2014

Martin Čech
Anička Doležalová
Filip Hlásek
David Hruška
Marta Kossaczká
Mirek Olšák
Anička Steinhauserová
Kuba Svoboda
Pepa Svoboda
Martin „E.T.“ Sýkora
Štěpán Šimsa
Martin Töpfer
Martina Vaváčková

Autoři: Martin Čech, Anička Doležalová, Filip Hlásek, David Hruška, Marta Kossaczká, Mirek Olšák, Anička Steinhauserová, Kuba Svoboda, Pepa Svoboda, Martin „E.T.“ Sýkora, Štěpán Šimsa, Martin Töpfer, Martina Vaváčková
Editor: Martina Vaváčková
vydání první, náklad 50 výtisků
říjen 2014
Díky za pomoc všem, kterým je za co děkovat.

Kolik existuje prvočísel?

Martin Čech

V tomto příspěvku můžete najít několik těžších vět zabývajících se vlastnostmi prvočísel, které si včetně důkazů ukážeme na přednášce.

Kolik máme prvočísel?

Spousta čtenářů jistě tuší, že prvočísel je opravdu hodně, dokonce nekonečno. Někteří dokonce znají i tradiční Eukleidův důkaz – kdyby jich bylo konečně, všechny vynásobíme, k výsledku přičteme jedničku a dojdeme ke sporu. Ukážeme si méně tradiční, ale neméně krásný důkaz, který objevil maďarský matematik Paul Erdős. Celý důkaz uvidíte na přednášce, zde je pouze ve stručném znění:

Důkaz. (Pouze stručný) Označme $\pi(N)$ počet prvočísel menších nebo rovných N. Každé přirozené číslo n se dá vyjádřit (dokonce jednoznačně) jako součin $r^2 s$, kde s je bezčtvercové. Je-li $n \leq N$, může r nabývat nejvýše $\sqrt{N}$ hodnot a s nejvýše $2^{\pi(N)}$ hodnot, přitom celkový počet možností musí být alespoň N, aby každé číslo mohlo mít svou reprezentaci. Z toho dostáváme nerovnost $\sqrt{N} \cdot 2^{\pi(N)} \geq N$, po zlogaritmování a úpravách máme $\pi(N) \geq \frac{1}{2} \log_2 N$.

Trochu víc než nekonečno...

Sama skutečnost, že prvočísel máme nekonečně mnoho, nám nic neříká o tom, jak hustě jsou rozmístěna. Mocnin dvojky máme také nekonečno, přesto se „v blízkosti nekonečna“ objevují velmi zřídka. Následující věta nám říká něco trochu víc než pouze to, že jich je nekonečno.

Věta. *Řada převrácených hodnot prvočísel diverguje, neboli*

$$\sum_{p \text{ prvočíslo}} \frac{1}{p} = \infty.$$

Pokud máš problém s nekonečným součtem či s nekonečnem v této větě, nezoufej! Věta pouze říká, že když sčítáme převrácené hodnoty dalších a dalších prvočísel, výsledek časem přeroste libovolně obrovské číslo. Všimni si, že toto například pro zmiňované mocniny dvojky neplatí, je tedy vidět, že tento výsledek je ještě silnější než pouze to, že je prvočísel nekonečno.

Důkaz této věty si předvedeme na přednášce.

Ještě přesnější odhad

Jeden z největších matematiků Friedrich Gauss vyslovil domněnku, že funkce $\pi(x)$, která udává počet prvočísel menších nebo rovných x, roste přibližně jako $\frac{x}{\log x}$. Tento výsledek je nyní známý jako prvočíselná věta, na její důkaz se však čekalo mnoho let, než jej objevili nezávisle na sobě matematici Jacques Hadamard a Charles-Jean de la Vallée-Poussin. Jejich důkazy využívaly složitých metod komplexní analýzy a sahají daleko za rámec této přednášky, dokážeme si však pár lemmátek a s jejich pomocí méně přesné odhady, se kterými přišel ruský matematik P. L. Čebyšev.

Lemma 1. *Pro přirozené číslo n platí nerovnosti*

$$\frac{4^n}{2n+1} \leq \binom{2n}{n} \leq 4^n.$$

Lemma 2. *Pro všechna přirozená čísla n platí*

$$\prod_{\substack{n<p\leq 2n \\ p \text{ prvočíslo}}} p \leq \binom{2n}{n} \leq (2n)^{\pi(2n)}.$$

Kombinací těchto odhadů můžeme dokázat kýženou větu:

Věta. *Existují konstanty $0 < c_1 < c_2$ takové, že pro všechna $x \geq 2$ platí*

$$c_1 \cdot \frac{x}{\log x} \leq \pi(x) \leq c_2 \cdot \frac{x}{\log x}.$$

Důkaz této věty si necháme na přednášku.

Poděkování

Děkuji docentu Martinu Klazarovi, z jehož přednášky Úvod do teorie čísel jsem čerpal. Poznámky k této přednášce je možné najít v uvedené literatuře.

Zdroje a literatura

[1] *http://kam.mff.cuni.cz/~klazar/ln_utc.pdf*
[2] Křížek, M., Somer, L. a Šolcová, A.; *Kouzlo čísel*

Základní věty z teorie čísel

Martin Čech

Úmluva. Nebude-li řečeno jinak, všechny níže uvedené proměnné jsou z oboru celých čísel.

Na přednášce si ukážeme základní metody používané při řešení úloh z teorie čísel, které se vyskytují v různých olympiádách a dalších matematických soutěžích. Neobejdeme se však bez nejnutnější teorie.

Trocha teorie

Definice. Řekneme, že číslo a je *dělitelem* čísla b, pokud existuje číslo k takové, že platí $k \cdot a = b$. Tuto skutečnost zapisujeme $a \mid b$.

Cvičení. Rozmyslete si, že pro nenulová čísla a, b, c, d platí:

(1) $1 \mid a$,
(2) $a \mid a$,
(3) $a \mid 0$,
(4) pokud $a \mid b$ a $b \mid c$, potom $a \mid c$,
(5) pokud $a \mid b$ a $a \mid c$, potom $a \mid kb + lc$ pro libovolná čísla k, l,
(6) pokud $a \mid b$ a $c \mid d$, potom $ac \mid bd$,
(7) pokud $a \mid b$, potom $|a| \leq |b|$ (speciálně pokud navíc $b \mid a$, potom $|a| = |b|$).

Tvrzení. (Dělení se zbytkem) *Pro každá dvě čísla m a n existuje právě jedna dvojice nezáporných celých čísel k a r takových, že $r < m$ a $n = km + r$. Říkáme, že číslo n dává po dělení m zbytek r.*

Definice. (Kongruence) Říkáme, že čísla a, b jsou *kongruentní modulo d*, pokud dávají po dělení číslem d stejný zbytek (tj. pokud $d \mid a - b$). Tuto skutečnost zapisujeme $a \equiv b \pmod{d}$.

Cvičení. Rozmyslete si, že platí následující základní vlastnosti kongruencí:

(1) $a \equiv 0 \pmod{m}$ právě tehdy, když $m \mid a$,
(2) pokud $a \equiv b \pmod{m}$, potom $a + k \equiv b + k \pmod{m}$ a $ak \equiv bk \pmod{m}$ pro libovolné k,
(3) pokud $a \equiv b \pmod{m}$ a $b \equiv c \pmod{m}$, potom $a \equiv c \pmod{m}$,

(4) pokud $a \equiv b \pmod{m}$ a $c \equiv d \pmod{m}$, potom $a + c \equiv b + d \pmod{m}$ a $ac \equiv bd \pmod{m}$.

Definice. Přirozená čísla, která mají právě dva kladné dělitele, nazýváme *prvočísla.*

Definice. Je-li p prvočíslo, množinu čísel $0, 1, ..., p-1$ nazýváme *množinou zbytků modulo p.*

Prvočísla hrají zásadní roli v teorii čísel, hlavně díky následujícím tvrzením:

Tvrzení. *Jestliže $p \mid ab$, kde p je prvočíslo, potom $p \mid a$ nebo $p \mid b$.*

Tvrzení. (Prvočíselný rozklad) *Každé přirozené číslo lze jednoznačně až na pořadí činitelů vyjádřit jako součin prvočísel.*

Tvrzení. *Prvočísel je nekonečně mnoho.*

Před slibovanými větami přichází důležité tvrzení, které bude hrát zásadní roli v jejich důkazech.

Tvrzení. (Stěžejní) *Je-li p prvočíslo a a číslo, které není dělitelné p, potom*

$$\{a \pmod{p}, 2a \pmod{p}, ..., (p-1)a \pmod{p}, pa \pmod{p}\},$$

kde zápis $b \pmod{p}$ znamená zbytek b po dělení p, je množinou zbytků modulo p.

Předchozí tvrzení říká, že když počítáme modulo prvočíslo p, můžeme dělit libovolným nenulovým číslem (kde nenulovým myslíme nenulovým modulo p, tedy nedělitelným p).

Nyní přicházejí slibované věty:

Věta. (Malá Fermatova věta) *Je-li p prvočíslo a a číslo nedělitelné p, potom*

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

Pro její důkaz stačí vynásobit všech $p-1$ kongruencí z předchozího tvrzení.

Věta. (Wilsonova věta) *Číslo p je prvočíslo právě tehdy, když*

$$1 \cdot 2 \cdots (p-2) \cdot (p-1) = (p-1)! \equiv -1 \pmod{p}.$$

Vyzbrojeni těmito větami se už můžeme vrhnout na řešení úloh!

Úlohy

Úloha 1. Je-li p prvočíslo, dokažte, že $p \mid ab^p - ba^p$ pro všechna čísla a, b.

Úloha 2. Buď p prvočíslo a n takové číslo, že $p \mid 4n^2 + 1$. Dokažte, že potom $p \equiv 1 \pmod 4$.

Výsledek předchozí úlohy se dá použít k dokázání existence nekonečně mnoha prvočísel tvaru $4k + 1$. Stačí pro spor předpokládat jejich konečné množství a vzít za n jejich součin.

Úloha 3. Buďte $A = \{a_1, a_2, \ldots, a_{101}\}$ a $B = \{b_1, b_2, \ldots, b_{101}\}$ množiny všech přirozených čísel od 0 do 100 (v libovolném pořadí). Může i $C = \{a_1 b_1 \pmod{101}, a_2 b_2 \pmod{101}, \ldots, a_{101} b_{101} \pmod{101}\}$ obsahovat všechna přirozená čísla od 0 do 100?

Úloha 4. Mějme danou posloupnost $a_n = 2^n + 3^n + 6^n - 1$. Najděte všechna přirozená čísla, která jsou nesoudělná s každým členem této posloupnosti.

(IMO 2005)

Zobecnění Malé Fermatovy věty

Malá Fermatova věta se dá použít, pouze pokud počítáme modulo prvočísla. V této kapitolce si ukážeme, že se dá zobecnit i pro složená čísla.

Definice. Čísla a, b nazýváme *nesoudělná*, pokud žádné prvočíslo nedělí obě z nich (tj. pokud jediný jejich společný dělitel je 1). Pro přirozené číslo n značí $\varphi(n)$ počet nezáporných čísel menších než n, která jsou s n nesoudělná.

Všimněte si, že je-li n prvočíslo, potom $\varphi(n) = n - 1$. Budeme nyní postupovat podobně jako při důkazu Malé Fermatovy věty. Nejprve si ukážeme tvrzení obdobné stěžejnímu tvrzení z předchozí kapitoly, ze kterého potom obdobně dokážeme zobecnění Malé Fermatovy věty.

Tvrzení. *Je-li n přirozené číslo, $A = \{a_1, \ldots, a_{\varphi(n)}\}$ je množina nezáporných čísel menších než n, která jsou s n nesoudělná, a $a \in A$, potom $\{aa_1 \pmod n, aa_2 \pmod n, \ldots, aa_{\varphi(n)} \pmod n\} = A$.*

Po vynásobení $\varphi(n)$ kongruencí z předchozího tvrzení dostaneme:

Věta. (Eulerova věta) *Je-li n přirozené číslo a a přirozené číslo nesoudělné s n, potom*

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

Nyní přicházejí další úlohy na procvičení:

Úloha 5. Najděte všechna přirozená čísla n taková, že $n \mid 3^{n!} - 2^{n!}$.

(MKS, 17. ročník)

Úloha 6. Ukažte, že pro každá dvě nesoudělná přirozená čísla a, b existují přirozená čísla m, n taková, že $a^n + b^m \equiv 1 \pmod{ab}$.

Úloha 7. Mějme dánu posloupnost $a_n = na+b$, kde a, b jsou nesoudělná přirozená čísla. Dokažte, že kdykoliv dostanete nekonečnou podmnožinu členů posloupnosti a_n a přirozené číslo N, umíte najít alespoň N prvků této podmnožiny, jejichž součin je člen posloupnosti a_n.

Zdroje a literatura

[1] *http://www.artofproblemsolving.com/Resources/Papers/SatoNT.pdf*
[2] Andreescu, T., Andrica, D. a Feng, Z.; *104 Number Theory Problems*

Fibonacciho posloupnost

Anička Doležalová

Fibonacciho posloupnost je posloupnost $(F_n)_{n=0}^{\infty}$ celých čísel splňující rekurentní vztah $F_{n+2} = F_{n+1} + F_n$ pro všechna $n = 0, 1, 2, \ldots$ s počáteční podmínkou $F_0 = 0$ a $F_1 = 1$. Jejími prvními členy jsou tedy $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots$

Příklad 1. (O králících) Mějme tyto specifické podmínky: Předpokládejme, že máme na začátku jeden pár králíků, králíci dospívají (a tedy se mohou pářit) právě měsíc po narození, každý dospělý pár zplodí každý měsíc právě jeden nový pár a žádní králíci neumírají. Ukažte, že počet králíků po n-tém dni je n-tý člen Fibonacciho posloupnosti.

Příklad 2. (Schodiště) Představme si, že vystupujeme po schodišti tak, že jedním krokem můžeme postoupit vždy buď o jeden, nebo o dva schody. Dokažte, že počet možností, jak vystoupat na n-tý schod, je F_{n+1}.

Příklad 3. (Cassiniho identita) Dokažte, že $F_{n-1} \cdot F_{n+1} - F_n^2 = (-1)^n$.

Příklad 4. Dokažte, že $\sum_{i=1}^{n} F_i^2 = F_n \cdot F_{n+1}$.

Příklad 5. (Vzorec pro n-tý člen) Dokažte, že pro n-tý člen Fibonacciho posloupnosti platí

$$F_n = \frac{\varphi^n - \psi^n}{\varphi - \psi},$$

kde φ a ψ jsou kořeny rovnice $x^2 - x - 1 = 0$, tedy $\varphi = \frac{1}{2}\big(1 + \sqrt{5}\big)$, $\psi = \frac{1}{2}\big(1 - \sqrt{5}\big)$.

Příklad 6. Dokažte, že $F_1 + F_2 + \cdots + F_n = F_{n+2} - 1$.

Příklad 7. Dokažte, že $F_1 \cdot F_2 + F_2 \cdot F_3 + \cdots + F_{2n-1} \cdot F_{2n} = F_{2n}^2$.

Příklad 8. Dokažte, že

$$F_1 + F_3 + \cdots + F_{2n+1} = F_{2n+2},$$
$$1 + F_2 + F_4 + \cdots + F_{2n} = F_{2n+1}.$$

Příklad 9. Mějme posloupnost čísel, kde první dva členy jsou rovny jedné a každý další člen je součet předchozích dvou členů zvýšený o jedna. Nalezněte všechny dvojice přirozených čísel m, n takových, že n-tý člen posloupnosti je roven $2^m - 1$.

(KMS 2012/2013, 1. zimní série, úloha 10)

Zdroje

Přednáška čerpá převážně ze staršího příspěvku Helči Svobodové, které bych tímto ráda poděkovala.

Sto vězňů a žárovka

Filip Hlásek

Budeme se zabývat známou a tradiční 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 problému

Do nejmenované věznice právě nastoupilo sto nových vězňů. Bachař jim dá šanci vymanit se ze svého 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.

Řešení úlohy

V této sekci navrhneme několik různých postupů, jak spolu mohou vězni pomocí žárovky komunikovat. Ke každému uvedeme navíc střední počet dní, po nichž budou vězni propuštěni. Předpokládáme, že každý den má každý vězeň se stejnou pravděpodobnost, že bude vyslechnut.

Zkusíme štěstí

Rozdělíme dny na bloky po 100 dnech. Během každého bloku budou vězni komunikovat podle následujících pravidel:

(i) Pokud je první den bloku a žárovka je zhasnutá, rozsviť ji.
(ii) Je-li žárovka rozsvícená a jsi v tomto bloku vyslechnut podruhé, zhasni ji.
(iii) Pokud je první den bloku a žárovka je rozsvícená, ohlaš, že již byli všichni vyslechnuti.
(iv) Ve všech ostatních případech ponechej stav žárovky nezměněný.

Když některý vězeň ohlásí, že byli všichni vyslechnuti, musel být každý vyslechnut právě jednou v předcházejících 100 dnech. Pokud by tam byl v posledním bloku někdo dvakrát, žárovku by zhasnul. Ona ale zůstala rozsvícená, takže tam byl každý jenom jednou.

Střední doba trvání: $\frac{n^{n+1}}{n!} \sim \sqrt{\frac{n}{2\pi}} e^n \doteq 1{,}072 \cdot 10^{44}$ dní.

Počtář

Následující protokol nespoléhá na počítání dní, ale dává speciální funkci jednomu vězni. Před začátkem si všichni zúčastnění určí jednoho, který bude mít roli *počtáře*. Počtář si bude pamatovat jedno celé číslo – počet spoluvězňů, u kterých si je jist, že již byli vyslechnuti.

Všichni ostatní vězni si budou pamatovat také jednu hodnotu – to, zda již počtáři sdělili, že byli vyslechnuti. Pro lepší představu uvážíme, že má každý na začátku jeden *token* (= virtuální předmět, který se snaží předat počtáři).

Dále detailněji popíšeme systém, kterým si vězni budou předávat tokeny:

(i) Pokud nejsi počtář, máš ještě token a je zhasnuto, rozsviť a uber si jeden token.
(ii) Jsi-li jsi počtář a je-li rozsvíceno, zhasni a připočti si jeden token.
(iii) Pokud jsi počtář a nasbíral jsi všech 100 tokenů (včetně svého), ohlaš úspěch.
(iv) Ve všech ostatních případech ponechej stav žárovky nezměněný.

Střední doba trvání: $O(n^2) \sim 10417{,}74$ dní $\doteq 28{,}54$ let.

Dynamická volba počtáře

Trochu vylepšíme předcházející protokol tím, že zvolíme počtáře až v průběhu, nikoliv dopředu. Počtářem se stane ten, kdo bude během prvních n dní jako první vyslechnut podruhé. Celý protokol se tedy skládá ze dvou fází:

(i) prvních n dní – Pokud budeš vyslechnut podruhé a je v místnosti zhasnuto, rozsviť a staň se počtářem. Ostatní poté vidí rozsvíceno a ví tedy, že funkci počtáře si už někdo vzal. Kdyby nikdo nepřišel do místnosti podruhé, bude v n-tém dni pořád zhasnuto a vězeň vyslýchaný ten den bude vědět, že všichni byli jednou vyslechnuti. Může tedy ohlásit úspěch.

(ii) dny $n+1$, $n+2$, ... – Uvažme, že počtář byl vyslechnut podruhé v k-tém dni. Předtím bylo vyslechnuto $k-1$ různých lidí. Jsou to právě ti, kteří viděli v první fázi zhasnutou žárovku. Můžeme tedy postupovat podle předcházejícího protokolu s tím rozdílem, že oněch $k-1$ různých lidí již své tokeny počtáři předalo (vědí to oni i počtář).

Pomocní počtáři

Zásadní nevýhodou jednoho počtáře je to, že vždy poměrně dlouho trvá (průměrně 100 dní), než přijde a vezme si token. Navrhneme protokol, který používá deset *pomocných počtářů* a jednoho *hlavního počtáře* (může jím být dokonce jeden z pomocných počtářů). Každý pomocný počtář bude sbírat tokeny, dokud jich nebude mít deset, a poté je pošle hlavnímu počtáři, který je posbírá po desítkách. Teoreticky tedy stačí, aby byl každý z počtářů vyslechnut přibližně dvacetkrát namísto předchozích minimálně 100 výslechů počtáře.

Na první pohled to může vypadat přímočaře, ale zůstává otázkou, jak předávat tokeny. Samozřejmě, že pomocí žárovky (žádný jiný prostředek totiž nemáme). Problém je ale v tom, že není jasné, zda rozsvícená žárovka znamená poslání jednoho tokenu od *nepočtáře* nebo jednoho *desítkového* tokenu od pomocného počtáře tomu hlavnímu. Tyto dvě situace musíme nějak odlišit, nicméně žárovka může být bohužel pouze rozsvícená, nebo zhasnutá. Problém vyřešíme úskokem. Rozdělíme dny do jednotlivých fází. V první fázi (například 100 dní) budou posílat nepočtáři svoje jednotkové tokeny a pomocní počtáři je budou sbírat. Poté bude následovat druhá fáze (opět například 100 dní), kdy budou moct pomocní počtáři poslat své desítkové tokeny (pokud již nasbírali deset jednotkových) a hlavní počtář je bude sbírat. Po druhé fázi bude následovat opět první fáze a takto dále, dokud hlavní počtář neposbírá všech 100 tokenů. Každý vězeň si tedy musí důkladně počítat dny a vědět, která fáze právě probíhá.

Ani teď ještě nemáme vyhráno. Může se totiž stát, že nepočtář vyšle v první fázi token, ale do konce fáze už nebude vyslechnut žádný počtář. Když bude poté ve druhé fázi vyslechnut hlavní počtář, může si myslet, že rozsvícená žárovka symbolizuje desítkový token poslaný od pomocného počtáře. Takto může velmi snadno dojít k nedorozumění, které povede k neúspěchu. Bude tedy potřeba důsledně hlídat, aby tokeny „nepřetékaly“ mezi fázemi. Opravíme to tak, že během posledního dne každé

fáze sebere vyslýchaný vězeň token, pokud je žárovka rozsvícená, a to nezávisle na tom, zda je to počtář. I nepočtář tak může mít u sebe několik jednotkových či desítkových tokenů. Tyto tokeny se pokusí při nejbližší vhodné příležitosti doručit správným příjemcům. Když má nějaké tokeny, které mu nenáleží, je správná fáze a zhasnutá žárovka, vyšle jeden z nich rozsvícením žárovky.

Tento poměrně komplikovaný doručovací mechanizmus již funguje. Nyní ho popíšeme přesněji – každý vězeň začíná s jednotkovým tokenem a každý si bude pamatovat počet jednotkových a desítkových tokenů, které vlastní.

Hlavní počtář

(i) Pokud máš 10 desítkových tokenů, ohlaš vítězství.
(ii) Pokud je druhá fáze a žárovka je rozsvícená, zhasni a připočti si desítkový token.
(iii) Pokud je první fáze, máš jednotkový token a žárovka je zhasnutá, rozsviť a odeber si jeden token.
(iv) Je-li poslední den první fáze a je rozsvíceno, zhasni a připočti si jednotkový token.

Pomocný počtář

(i) Pokud máš 10 jednotkových tokenů, zahoď je a vyrob z nich jeden desítkový token. Přestáváš být pomocným počtářem a stáváš se nepočtářem.
(ii) Pokud je první fáze, žárovka je rozsvícená, zhasni a připočti si jednotkový token.
(iii) Pokud je druhá fáze, máš desítkový token a žárovka je zhasnutá, rozsviť a odeber si desítkový token.
(iv) Je-li poslední den druhé fáze a je rozsvíceno, zhasni a připočti si desítkový token.

Nepočtář

(i) Pokud je první fáze, máš jednotkový token a žárovka je zhasnutá, rozsviť a odeber si jeden token.
(ii) Je-li poslední den první fáze a je rozsvíceno, zhasni a připočti si jednotkový token.
(iii) Pokud je druhá fáze, máš desítkový token a žárovka je zhasnutá, rozsviť a odeber si desítkový token.
(iv) Je-li poslední den druhé fáze a je rozsvíceno, zhasni a připočti si desítkový token.

Střední doba trvání: $3\,500 - 4\,000$ dní $\doteq 9{,}5 - 11$ let.

Binární tokeny

Myšlenku uvedenou v předcházejícím řešení se nyní pokusíme ještě zobecnit, a dosáhnout tak téměř nejlepšího dosud známého postupu. Jak již název napovídá, nebudou počtáři shlukovat tokeny po deseti, ale po mocninách dvojky. Budeme potřebovat,

aby počet všech tokenů byla mocnina čísla dvě. Když počet vězňů není mocnina dvojky, dáme na začátku některému vězni tokenů více.

Předpokládejme tedy, že všichni vězni dohromady mají 2^k tokenů. Jejich počáteční rozdělení si domluví před začátkem, přičemž jediná podmínka je, aby měl každý alespoň jeden. Jakmile někdo získá všechny, může ohlásit úspěch. Podobně jako v minulém případě budou i tentokrát jednotlivé tokeny různě cenné. Konkrétně máme $k+1$ druhů tokenů o hodnotách $2^0, 2^1, \ldots, 2^k$. Jakmile někdo získá dva tokeny stejné hodnoty 2^i, udělá z nich jeden hodnoty 2^{i+1}.

Jak si budou vězni tokeny mezi sebou předávat? Opět nás nezklame myšlenka rozdělení dnů na fáze. Tentokrát bude ovšem fází k a bude mnohem více záviset na jejich velikosti. Jako nejlepší se ukazují stejně dlouhé fáze o zhruba 613 dnech. Nyní již máme vše potřebné k tomu, abychom řádně popsali, jak budou vězni komunikovat v i-té fázi:

(i) Pokud máš token hodnoty 2^k, ohlaš úspěch.
(ii) Pokud máš dva tokeny hodnoty 2^j pro nějaké celé j, udělej z nich jeden token hodnoty 2^{j+1}.
(iii) Je-li žárovka rozsvícená, zhasni ji a připočti si token hodnoty 2^i.
(iv) Je-li žárovka zhasnutá a máš-li token hodnoty 2^i, rozsviť a odeber si token.

Střední doba trvání: $O(n(\ln n)^2) \sim 3\,500$ dní $\doteq 9$ let.

Varianty úlohy

(1) **Zákeřný bachař** – Je dáno předem známé přirozené číslo k. Bachař může k-krát během celého procesu změnit stav žárovky (rozsvítit nebo zhasnout).
(2) **Všichni musí ohlásit** – Vězni budou propuštěni jedině tehdy, pokud všichni ohlásí, že již všichni byli vyslechnuti.
(3) **Propuštěný po ohlášení** – Všichni vězni musejí ohlásit, ale pokud někdo ohlásí, je okamžitě propuštěn a už nikdy nebude vyslýchán.
(4) **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.
(5) A **pošle zprávu** B – Předem určený vězeň A musí poslat zprávu (přirozené číslo) vězni B.
(6) **Čísla v celách** – V každé cele je napsáno jedno celé číslo. Vězeň, který ohlašuje, musí nahlásit také všechna tato čísla.
(7) **Všichni posílají zprávy všem** – Navrhněte obecný protokol, pomocí kterého si budou moci navzájem posílat jakékoliv zprávy.
(8) **Všichni musí 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.
(9) **Náhodné časy** – Řešte všechny předcházející úlohy bez předpokladu (c). Vězni jsou vyslýcháni v náhodné časy a nemohou tedy počítat dny.

Návody na řešení jednotlivých variant

(1) **Zákeřný bachař** – Každý vězeň bude mít $2k+1$ tokenů (méně nestačí!), a když počtář napočítá do $100(2k+1)-k$, může ohlásit, že již všichni byli vyslechnuti.

(2) **Všichni musí ohlásit** – Použijeme strategii *počtář* s tokeny n druhů (tedy n fází). Každý vězeň bude mít na začátku token určený pro každého dalšího. Každý vězeň je počtářem svého druhu tokenů.

(3) **Propuštění po ohlášení** – Funguje předcházející strategie: vězeň ohlásí až tehdy, když nasbírá svých sto tokenů a zbaví se všech ostatních.

(4) **Červené a modré cely** – Použijeme jednoho *počtáře*, který bude sbírat dva druhy tokenů – červené a modré (dvě fáze). Nasbírá-li dohromady 100 tokenů, ohlásí, kolik z nich bylo červených a kolik modrých.

(5) A **pošle zprávu** B – Vězeň A zakóduje zprávu do binární soustavy. Chce-li používat jiné znaky než jedničky a nuly, mohou se domluvit na posílání například po pěti bitech, kde každá pětice bude vyjadřovat jedno písmeno. Pět nul pak může znamenat konec zprávy.

Jak ale posílat jedničky a nuly? Použijeme opět dva druhy tokenů: *nulový* a *jedničkový*. Vězeň A bude postupně posílat věznì B jednotlivé bity zprávy. Přenos ale bohužel nezachovává pořadí, takže vězeň B pravděpodobně dostane bity přeházené. Abychom tomu zabránili, přidáme ještě potvrzovací token, který pošle vězeň B věznì A po přijetí jednoho bitu (nulového nebo jedničkového tokenu). Vězeň A vždy po vyslání bitu čeká na potvrzovací token a další bit vyšle až po jeho obdržení. Potřebujeme tedy celkem tři fáze a jim odpovídající tři typy tokenů. Všichni ostatní věznì si musí pamatovat, kolik mají kterých tokenů. Naštěstí však mohou mít všichni dohromady v každém okamžiku nejvýše jeden token (buď se posílá bit, nebo se čeká na potvrzení přijetí).

(6) **Čísla v celách** – Komunikační kanál popsaný v předchozí pasáži realizujeme mezi počtářem a každým vězněm. Celkem tak bude potřeba $3 \cdot 99$ různých tokenů. Tedy bude také $3 \cdot 99$ fází a každý vězeň si bude muset pamatovat, kolik kterých tokenů drží.

(7) **Všichni posílají zprávy všem** – Opět použijeme stejný mechanizmus, ale tentokrát budeme potřebovat dokonce $\frac{3n(n-1)}{2}$ druhů tokenů. Každý vězeň takto může komukoliv poslat jakoukoliv zprávu. To vše realizují věznì pomocí jediné žárovky.

(8) **Všichni musí ohlásit ve stejný den** – Vzhledem k předchozím výsledkům to může znít poměrně překvapivě, ale skutečně není možné navrhnout spolehlivý postup, pomocí kterého by věznì ohlásili, že již všichni byli vyslechnuti, ve stejný den. Pro spor předpokládejme, že taková strategie existuje, a uvažme nějakou posloupnost vyslýchání vězňů, při které všichni věznì ohlásí, že již byli vyslechnuti. Každý vězeň se musí někdy rozhodnout, že i pokud by už nebyl vyslechnut, tak v nějaký den D ohlásí. Podívejme se na toho vězně, který se rozhodne jako první. Od dne jeho rozhodnutí jej už nebudeme vyslýchat a jako zákeřný bachař budeme až do dne

D stále vyslýchat jednoho jiného vězně. Žádný vězeň kromě těchto dvou se tedy nerozhodne ohlásit, což je spor s existencí strategie.

Přestože si vězni mohou vyměnit jakékoliv zprávy, nemohou se domluvit na jednom konkrétním dni tak, aby se to všichni stihli dozvědět. Schopnost vyměňovat si zprávy je sice silný nástroj, ale vězni nemají žádný odhad na to, jak dlouho bude posílání zprávy trvat.

(9) **A co bez počítání dní?** – Navrhneme protokol, pomocí něhož si vězni mohou posílat zprávy bez toho, aby počítali dny. Ve všech předchozích řešeních bylo naprosto klíčové, aby vězni přesně věděli, která fáze právě probíhá. Není tedy možné přímo aplikovat výše uvedené postupy.

Zprávu budeme reprezentovat jako nezáporné celé číslo N (například ve dvojkové soustavě). Vězeň A bude vězni B postupně posílat N tokenů. Jelikož A je jediným odesílatelem (jediný, kdo rozsvěcuje žárovku) a B jediným příjemcem (jediný, kdo žárovku zhasíná), nemohou se tokeny nikde ztratit a po určité době dojde jistě celá zpráva k B. Poté A přestane vysílat tokeny. Problém je ale v tom, že B neví, jestli má ještě čekat, že mu něco přijde.

Na první pohled to opět vypadá jako neřešitelný problém, my ale přesto ukážeme postup, jak se s ním vypořádat. Vězeň B občas pošle jeden token zpátky, aby vyzkoušel, jestli už A poslal všechno. Pokud A již poslal všechno a viděl zhasnuto (tj. ví, že B vše přijal), je potom ochoten přijmout jeden token. Když se potvrzení podaří, uvidí poté B opět zhasnuto a bude si jist, že dostal celou zprávu. Pokud potvrzení nedostane (buď proto, že A bude ještě posílat, nebo proto, že mezitím nebyl vyslechnut), zkusí to po nějaké době znovu.

Uvedeným způsobem může předem zvolený vězeň poslat jakoukoliv zprávu jinému předem určenému vězni. Tentokrát ovšem není vůbec jasné, jak protokol rozšířit pro komunikaci každé dvojice vězňů. Je možné navrhnout systém, jak se budou vězni dorozumívat každý s každým, i pokud nemohou počítat dny. Je ale poměrně náročný a zdlouhavý, a proto ho nebudeme uvádět. Jeho kompletní popis společně s detailním rozborem většiny uvedených metod naleznete v článku [4].

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*

Harmonické čtveřice

David Hruška

Úmluva. Symbolem AB budeme značit tradičně přímku procházející body A, B a někdy navíc i délku *orientované úsečky* s krajními body A a B.

Dvojpoměr a promítání na přímky

Mějme přímku AB a na ní bod X. Polohu bodu X vzhledem k A a B můžeme vyjádřit tzv. *dělicím poměrem*.

Definice. Nechť X je bod na přímce AB různý od bodů A, B. Dělicí poměr bodu X vzhledem k bodům A a B je číslo $(AB, X) = \frac{AX}{BX}$.

Cvičení. Rozmyslete si, že pro dané body A, B je poloha bodu X hodnotou (AB, X) jednoznačně určena. Kdy je $(AB, X) > 0$?

Vzájemnou polohu čtyř bodů na přímce můžeme popsat podobnou veličinou.

Definice. *Dvojpoměr* bodů A, B, C, D (v tomto pořadí) ležících na jedné přímce je číslo

$$(AB, CD) = \frac{(AB, C)}{(AB, D)} = \frac{AC \cdot BD}{AD \cdot BC}.$$

Cvičení. Dokažte, že

$$(AB, CD) = (CD, AB) = (BA, DC) = \frac{1}{(AB, DC)} = \frac{1}{(DC, AB)} = \frac{1}{(BA, CD)}.$$

Poslední cvičení nám říká, že význačné hodnoty dvojpoměru jsou 1 a -1. Z rovnosti $(AB, CD) = 1$ ovšem plyne, že $A = B$ nebo $C = D$, takže nás bude více zajímat hodnota -1.

Definice. Body A, B, C, D ležící na přímce tvoří *harmonickou čtveřici*, pokud $(AB, CD) = -1$.

Cvičení. Rozmyslete si, jak zhruba harmonické čtveřice vypadají. V jakém pořadí mohou na přímce ležet jejich body?

Tvrzení. *Jsou dány přímky p, q a bod X mimo ně. Bodem X procházejí čtyři přímky, které protínají přímku p postupně v bodech A, B, C, D a přímku q postupně v bodech A', B', C', D'. Potom platí $(AB, CD) = (A'B', C'D')$.*

My budeme toto tvrzení používat hlavně pro promítání harmonických čtveřic. Příslušné čtyři přímky tvoří v tom případě *harmonický svazek*.

Jak poznat harmonickou čtveřici?

To nám velmi usnadní následující tvrzení.

Tvrzení. *V následujících běžných konfiguracích se vyskytují harmonické čtveřice:*

(i) *Pokud M je střed AB, pak $(AB, M\infty) = -1$.*
(ii) *Ceviány AD, BE, CF se protínají v P. Označme $D' = EF \cap BC$. Pak $(BC, DD') = -1$.*
(iii) *Na průměru AB kružnice k se středem O je dán bod X. Je-li X' jeho obraz v kruhové inverzi podle k (tj. platí-li $|OX| \cdot |OX'| = |OA|^2 = |OB|^2$), pak $(AB, XX') = -1$.*

Tvrzení. („Dvě ze tří“) *Nechť A, B, C, D leží na přímce a P mimo ni. Pak z libovolných dvou následujících bodů plyne třetí:*

(i) $(AC, BD) = -1$,
(ii) $|\sphericalangle APC| = 90°$,
(iii) $|\sphericalangle BPC| = |\sphericalangle CPD|$, *kde úhly chápeme orientovaně.*

A konečně jsou tady…

Úlohy I

Úloha 1. Mějme trojúhelník ABC, bod I je jeho vepsiště, bod I_a jeho A-připsiště, D je průsečík osy úhlu u A a strany BC. Dokažte, že $(AD, II_a) = -1$.

Úloha 2. Ceviány AD, BE, CF se protínají v P. Označme $Q = BC \cap EF$, $R = AD \cap EF$, $S = CF \cap BR$ a $T = DF \cap BR$. Ukažte, že

$$(QR, EF) = (AP, DR) = (CS, PF) = (BS, RT) = -1.$$

Úloha 3. Body D, E, F jsou zvoleny postupně na stranách BC, CA, AB trojúhelníku ABC tak, že $AD \cap BE \cap CF = K$. Přímka FD protíná přímku BE v bodě X, P je střed úsečky AK a EP protíná přímku AB v bodě Y. Dokažte $XY \parallel AD$.

Úloha 4. Na přímce p jsou dány body B, D, C v tomto pořadí. Dokažte, že všechny body A takové, že AD je osa úhlu BAC, leží na pevné kružnici (tzv. *Apolloniově kružnici*).

Úloha 5. (Blanchet Theorem) Na A-výšce AD trojúhelníka ABC je dán bod P. Označme $X = BP \cap AC$, $Y = CP \cap AB$. Dokažte $|\sphericalangle XDA| = |\sphericalangle YDA|$.

Úloha 6. Je dán trojúhelník ABC, body dotyku kružnice vepsané se stranami BC, CA, AB označme postupně D, E, F. Bod X leží uvnitř trojúhelníku ABC tak, že kružnice vepsaná trojúhelníku XBC se dotýká jeho stran v bodech D, Y a Z. Dokažte, že E, F, Y, Z leží na jedné kružnici. (IMO Shorlist 1995)

Úloha 7. V trojúhelníku ABC označme D patu osy úhlu u A a I_b, I_c vepsiště trojúhelníků ABD, ACD.

(1) (Sharygin 2013) Je-li $Q = BC \cap I_bI_c$, dokažte $|\sphericalangle DAQ| = 90°$.
(2) Označíme-li průsečíky I_bI_c s AB, AC postupně M, N, dokažte, že MC a NB se protnou na AD.

Úloha 8. Je dána kružnice ω se středem O a tětivou AB ($O \notin AB$). Bod C leží na ω tak, že AC půlí úsečku OB. Označme $D = AB \cap OC$ a $F = BC \cap AO$. Dokažte, že $|AF| = |CD|$.

Harmonické čtyřúhelníky

Užitečným nástrojům není zdaleka konec. Co zkusit promítat na kružnice?

Tvrzení. *Je dán bod P ležící na kružnici k a mimo přímku p. Přímky a, b, c, d protnou p v A', B', C', D' a k v A, B, C, D. Pak platí*

$$|(A'B', C'D')| = \frac{|AC| \cdot |BD|}{|AD| \cdot |BC|}.$$ [1]

Definice. Řekneme, že tětivový čtyřúhelník $ABCD$ je *harmonický*, pokud pro délky jeho stran platí $ac = bd$.

Pozorování. *S použitím předchozího tvrzení si snadno rozmyslíme, že čtyřúhelník $ABCD$ vepsaný do kružnice ω je harmonický právě tehdy, když pro libovolný bod $P \in \omega$ tvoří přímky PA, PB, PC, PD harmonický svazek.*[2]

Tvrzení. (O harmonických čtyřúhelnících) *Buď D bod na oblouku BC kružnice k opsané trojúhelníku ABC, který neobsahuje bod A. Pak následující tvrzení jsou ekvivalentní:*

(i) *Čtyřúhelník $ABDC$ je harmonický.*
(ii) *Přímka AD je A-symediána v $\triangle ABC$ (tedy čára symetrická s A-těžnicí podle osy úhlu u A).*
(iii) *Přímka AD a tečny ke k skrz B a C procházejí jedním bodem.*

[1] Obecnější tvrzení bez absolutních hodnot také platí, ale potřebovali bychom k jeho formulaci komplexní čísla.

[2] Pokud například $P = A$, uvažujeme místo PA tečnu k ω v bodě A.

Cvičení. Úhlopříčky tětivového čtyřúhelníku $ABCD$ se protínají v P. Dokažte, že pokud je BP symediána v ABC, pak AP je symediána v ABD.

(Rumunsko TST 2006)

Pojďme to vyzkoušet!

Úlohy II

Úloha 9. Kružnice vepsaná rovnoramennému trojúhelníku ABC ($|AB| = |AC|$) se dotýká AC v E. Přímka různá od BE vedená bodem B protíná kružnici vepsanou v bodech F, G. Přímky EF, EG protnou BC v K, L. Dokažte $|BK| = |CL|$.

(MEMO 2008)

Úloha 10. V trojúhelníku ABC platí $|AC| = 2|AB|$. Označme P průsečík tečen k jemu opsané kružnici ω vedených body A a C. Dokažte, že průsečík přímky BP a osy strany BC leží na kružnici ω. (ČR TST 2012)

Úloha 11. Nechť $ABCD$ je konvexní čtyřúhelník. Označme $F = AB \cap CD$, $E = AD \cap BC$ a $T = AC \cap BD$. Předpokládejme, že A, B, T, E leží na kružnici, která protíná přímku EF v bodě P. Označme M střed úsečky AB. Dokažte, že $|\sphericalangle APM| = |\sphericalangle BPT|$. (Írán TST 2004)

Úloha 12. Paty kolmic z bodu D tětivového čtyřúhelníku $ABCD$ na přímky BC, CA, AB označme postupně P, Q, R. Dokažte, že $|PQ| = |QR|$ právě tehdy, když se osy úhlů $\sphericalangle ABC$ a $\sphericalangle ADC$ protínají na úhlopříčce AC. (IMO 2003)

Úloha 13. V tětivovém pětiúhelníku $ABCDE$ platí $AC \parallel DE$ a střed M tětivy BD splňuje $|\sphericalangle AMB| = |\sphericalangle BMC|$. Dokažte, že BE půlí tětivu AC.

Poláry

Posledním objektem, který si ukážeme, budou *poláry*. Motivací pro jejich zkoumání je následující tvrzení.

Tvrzení. *Tečny ke kružnici k vedené bodem A se jí dotýkají v bodech T, U. Přímka p procházející bodem A protne přímku TU v B a kružnici k v X, Y. Pak $(AB, XY) = -1$.*

Definice. Buď k kružnice se středem O a $X \neq O$. Přímku, která prochází obrazem X' bodu X v kruhové inverzi podle k a je kolmá na OX, nazýváme *polárou* bodu X (vzhledem ke k). Bod X je *pól* přímky p (vzhledem ke k).

Tvrzení. *Ať P, Q jsou body a p, q jejich poláry (vzhledem k nějaké kružnici k). Pak platí, že pokud P leží na q, pak Q leží na p.*

Tvrzení. *Čtyřúhelník $ABCD$ je vepsaný do kružnice k. Označme $P = AC \cap BD$, $Q = AB \cap CD$ a $R = AD \cap BC$. Pak trojúhelník PQR je selfpolar, tedy PQ je polára bodu R, PR je polára bodu Q a QR je polára bodu P.*

Teď už to musí jít samo, ne?

Úlohy III

Úloha 14. Je dána kružnice k a přímka p, která ji neprotíná. Po přímce p se pohybuje bod P. Tečny z P ke k se jí dotýkají v T a U. Dokažte, že přímka TU prochází pevným bodem.

Úloha 15. Je dána půlkružnice γ s průměrem UV. Její body P, Q splňují $UP < UQ$. Tečny k γ v bodech P a Q se protínají v bodě R. Označme $S = UP \cap VQ$. Dokažte $RS \perp UV$.

Úloha 16. Je dán trojúhelník ABC s vepsištěm I. Body dotyku kružnice vepsané s odpovídajícími stranami označme A_1, B_1, C_1. Dále označme $D = BC \cap B_1C_1$ a $F = DI \cap AA_1$. Dokažte $|\sphericalangle AFB| = |\sphericalangle AFC|$.

Úloha 17. Kružnice vepsaná trojúhelníku ABC se středem I se dotýká jeho stran AB, AC v F, E. Označme N průsečík EF a A-těžnice AM. Dokažte $NI \perp BC$.

Obtížnější úlohy

Úloha 18. Je dán ostroúhlý trojúhelník ABC s ortocentrem H. Kružnice s průměrem AB protne CH v bodech X a Y, kružnice s průměrem AC protne BH v bodech Z a W. Dokažte, že (nezávisle na označení) se XZ a YW protínají na BC.
(Brazílie 2013)

Úloha 19. Kružnice vepsaná trojúhelníku ABC se dotýká jeho stran BC, CA, AB v D, E, F. Úsečka AD protne vepsanou podruhé v J a přímky BJ, CJ protnou vepsanou podruhé v K, L. Dokažte, že KC, LB a AD procházejí jedním bodem.

Úloha 20. Je dán ostroúhlý trojúhelník ABC s patou A-výšky D a kolmištěm H. Kružnice skrz B a C protne kružnici nad průměrem AH v X a Y. Označíme-li P projekci D na XY, dokažte $|\sphericalangle BPD| = |\sphericalangle CPD|$. (Japonsko 2013)

Úloha 21. Je dán konvexní čtyřúhelník $ABCD$. Přímky AB a CD se protnou v bodě E, přímky BC, AD v bodě F. Průsečík úhlopříček označme P a projekci P na EF označme O. Dokažte, že $|\sphericalangle BOC| = |\sphericalangle AOD|$. (China TST 2002)

Návody

1. Využijte tvrzení „dvě ze tří“.

2. Vždy najděte správný bod, z nějž promítat.

3. Najděte harmonický svazek vycházející z Y.

4. Dokreslete čtvrtého do party k B, D, C a využijte tvrzení „dvě ze tří“.

5. Zkombinujte konfiguraci „Ceva–Mene“ a tvrzení „dvě ze tří“.

6. Čtvrtý do party k B, D, C a mocnost.

7. (1) Kde je čtvrtý do party k I_bI_c a $X = AD \cap I_bI_c$? (2) Pokud mají dvě harmonické čtveřice společný bod, pak spojnice zbylých tří odpovídajících si dvojic procházejí jedním bodem.

8. Dokažte sporem(!), že $OB \parallel FD$.

9. Označte zbylé body dotyku, najděte harmonický čtyřúhelník a promítněte ho.

10. Dokažte, že BX, kde X je průnik osy BC a ω, je symediána v ABC.

11. Dokažte, že $PATB$ je harmonický.

12. Dokažte, že oba výroky jsou ekvivalentní s tím, že $ABCD$ je harmonický.

13. Začněte tím, že AC je symediána v ABD.

14. Kterým zajímavým bodem prochází polára bodu na přímce p?

15. Dokažte, že RS je polára bodu K.

16. Dokažte a využijte, že AA_1 je polára D.

17. Dokazujte, že N je pól rovnoběžky s BC bodem A.

18. Pokud mají dvě harmonické čtveřice společný bod, pak zbylé tři spojnice procházejí jedním bodem.

19. Ukažte, že $JKDL$ je harmonický.

20. Chordály tří kružnic procházejí jedním bodem.

21. Dokažte, že OP je společná osa jistých dvou úhlů.

Literatura a zdroje

[1] Pepa Tkadlec; *Dvoupoměr a poláry*, Sborník *i*KS, 2013
[2] *http://www.artofproblemsolving.com*

Extremálny princíp

Marta Kossaczká

Extremálny princíp je jedna z dôkazových metód, ktorá má využitie v rôznych oblastiach matematiky. Základom tejto metódy je nájsť vhodné usporiadanie určitých objektov a zaoberať sa najmenším alebo najväčším prvkom.

Príklad. Na nekonečnej šachovnici je v každom políčku umiestnené prirodzené číslo tak, aby bolo rovné aritmetickému priemeru svojich štyroch susedov. Ukážte, že všetky políčka majú rovnaké číslo.

Riešenie. Najmenšie číslo si označme m a jeho susedné čísla a, b, c, d. Potom platí

$$a + b + c + d = 4m.$$

Všetky čísla sú prirodzené, a teda platí aj $a \geq m$ $b \geq m$ $c \geq m$ $d \geq m$. Zrejme teda $a = b = c = d = m$. Z toho je už jasné, že všetky čísla musia byť m.

Príklad 1. Dokážte, že existuje nekonečne veľa prvočísel.

Príklad 2. V rovine je n bodov takých, že ľubovolné tri tvoria trojuholník s obsahom menším ako 1. Dokažte, že všetky ležia v trojuhoníku s obsahom menším ako 4.

Príklad 3. V rovine máme útvar s obsahom S. Ukážte, že vieme nájsť aspoň $\frac{S}{\pi}$ bodov v našom útvare tak, aby každé dva boli vzdialené aspoň 1.

Príklad 4. Nájdite všetky a, b, c, d celé, pre ktoré platí

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

Príklad 5. Nájdite všetky x, y, z, w celé, pre ktoré platí

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

Príklad 6. V rovine je n bodov ofarbených na červeno a modro, každá úsečka spojujúca dva body rovnakej farby obsahuje ešte aspoň jeden bod druhej farby. Dokážte, že všetky body ležia na jednej priamke.

Príklad 7. V okolí Pork Townu je n dedín, medzi ktorými vedú jednosmerné vlakové trate, medzi každými dvoma dedinami práve 1. Ukážte, že existuje aspoň jedna dedina, z ktorej sa dá dostať do ľubovolnej inej maximálne cez jednu ďalšiu dedinu.

Príklad 8. V rovine je zelených n bodov. Dokážte, že existuje priamka, ktorá prechádza práve dvoma zelenými bodmi.

Príklad 9. Dokážte, že n banditov sa dá rozdeliť na dve skupiny tak, aby každý mal vo svojej skupine maximálne polovicu úhlavných nepriateľov (úhlavné nepriateľstvo je vzájomné).

Príklad 10. Dokážte, že existuje nekonečne veľa prvočísel tvaru $6n - 1$.

Príklad 11. V rovine je n fialových a n zelených bodov takých, že žiadne tri neležia na jednej priamke. Ukážte, že existuje n úsečiek s rôznofarebnými koncovými vrcholmi tak, že žiadne dve nemajú spoločný bod.

Príklad 12. Do tabulky $n \times n$ sme vpísali čísla $1, 2, \ldots, n^2$, do každého políčka práve jedno. Dokážte, že existujú dve (stranou alebo aj rohom) susediace políčka, ktorých rozdiel je aspoň $n + 1$.

Príklad 13. Máme n kariet, očíslovaných $1, 2, \ldots, n$. Zamiešame ich a potom v každom ťahu otočíme vrchnú kartu. Na nej je číslo k, následne vezmeme vrchných k kariet, obrátime ich poradie, vrátime ich späť a pokračujeme. Dokážte, že raz bude na vrchu 1.

Literatura a zdroje

[1] Engel, A.; *Problem-Solving Strategies*, Springer, UK, 1998
[2] Derksen, H.; *Mathematical Problem Solving*

Burnsideovo lemma

Mirek Olšák

Úmluva. Není-li řečeno jinak, zanedbáváme pouze otáčení s předmětem – nikoli překlápění či jiné úpravy.

Netřeba jít s kanónem na vrabce

Ne ve všech případech je vhodné lemma třeba použít – někdy je jednodušší si rozmyslet všechny možnosti a situaci šikovně zjednodušit.

Úloha 1. Kolika způsoby můžeme přiřadit stěnám krychle čísla 1 až 6 (každé právě jednou) tak, aby součet hodnot protilehlých stěn byl vždy roven sedmi?

Úloha 2. Kolik je možností, jak obarvit stěny krychle dvěma barvami?

Úloha 3. Kolik existuje neizomorfních grafů na čtyřech vrcholech?

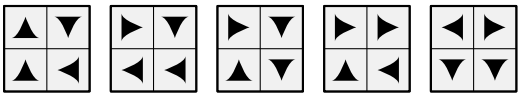
Úloha 4. Kolik existuje různých sítí krychle?

Úloha 5. Má více sítí krychle, nebo pravidelný osmistěn?

Úloha 6. Kolik je možností, jak obarvit vrcholy krychle dvěma barvami?

Terminologie

Definice. Obrázek[1] je jedna „kombinace“, u které zatím nic nezanedbáváme. Tedy pět různých obrázků může vypadat například takto:



[1] V odborné literatuře se typicky jedná o prvek množiny X.

Definice. Pohyb vezme obrázek a udělá z něj (typicky jiný) obrázek – je to tedy funkce, která zobrazí množinu obrázků do množiny obrázků. Například první čtveřice obrázků z předchozího příkladu vzniká postupně aplikováním pohybu „Otoč o 90° proti směru hodinových ručiček.“ Množina G všech uvažovaných pohybů (těch, které chceme zanedbat) musí tvořit grupu, což znamená:

(i) Kdykoli složíme (provedeme po sobě) dva pohyby z G, dostaneme opět pohyb z G.
(ii) V G musí existovat nepohyb – pohyb, který vše nechá na místě.
(iii) Pro každý pohyb $p \in G$ existuje opačný pohyb p^{-1}, který při složení (v kterémkoli pořadí) s původním pohybem p dá nepohyb.

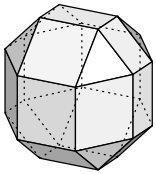
Poznámka. V úlohách je pohyb obvykle nejen zobrazením na množině obrázků, ale současně na bodech v rovině, respektive v prostoru. Může se tedy hypoteticky stát, že dva pohyby dávají tutéž permutaci na množině obrázků, ale jsou různé.

Definice. Předmět[2] je typicky to, co chceme spočítat – v podstatě totéž co obrázek až na to, že předměty lišící se jen nějakým pohybem považujeme za identické. Například první čtyři obrázky z příkladu odpovídají tomu samému předmětu.

Jdeme zanedbávat pohyby

Úloha 7. Kolik různých náhrdelníků (v rovině) je možné vytvořit z šesti černých a sedmi bílých korálků?

Úloha 8. Kolika způsoby můžeme nakreslit šipku směrem k jedné hraně na každou z 26 stěn následujícího tělesa (krychle se seřízlými hranami a vrcholy)?



Úloha 9. Na špíz můžeme napíchnout vždy maso, slaninu, nebo cibuli – celkem napíchneme deset kousků. Kolik existuje různých špízů (konce špejle jsou nerozlišitelné)?

Úloha 10. Kolik bude náhrdelníků z úlohy 7, pokud zanedbáme i překlápění?

[2] V odborné literatuře se používá pojem orbita.

S kanónem na draka

Taky vám vychází…?

Lemma. (Burnside) *Pro pohyb p označme S_p množinu všech obrázků odolných vůči p (tedy pevných bodů p). Pak počet předmětů spočteme jako*

$$\frac{1}{|G|}\sum_{p\in G}|S_p|.$$

Úloha 11. Kolik náhrdelníků vyjde v úloze 7, budeme-li mít k dispozici dvanáct černých a dvanáct bílých korálků?

Úloha 12. Kolika způsoby můžeme obarvit políčka nekonečného čtverečkovaného papíru dvěma barvami tak, aby políčko $[x, y]$ mělo vždy stejnou barvu jako políčka $[x \pm 9, y]$ a $[x, y \pm 9]$? Obarvení lišící se pouze posunutím (avšak **nikoli** otočením či překlopením) považujeme za totožná.

Úloha 13. O kolik se zvětší výsledek úlohy 8, pokud budeme

(1) trojúhelníkové stěny barvit jednou ze tří barev namísto kreslení šipky,
(2) čtyřúhelníkové stěny sousedící s trojúhelníkovými barvit čtyřmi barvami namísto kreslení šipky,
(3) čtyřúhelníkové stěny nesousedící s trojúhelníkovými barvit čtyřmi barvami namísto kreslení šipky?

Úloha 14. Kolik je možností, jak obarvit právě patnáct z třiceti hran dvacetistěnu?

Úloha 15. Pro všechna přirozená čísla N a n dokažte, že n dělí $\sum_{k=1}^{n} N^{\gcd(n,k)}$, kde $\gcd(a, b)$ značí největší společný dělitel a a b.

Návody

1. 2

2. 10

3. 11

4. 20

5. Stějně (dá se popsat bijekce).

6. 30

7. $\binom{13}{6}/13$

8. $2^{33}\cdot 3^7$

9. $\left(3^9+3^5\right)/2$

10. $\left(\binom{13}{6}+13\binom{6}{3}\right)/26$

11. $\left(\binom{24}{12} + \binom{12}{6} + 2\binom{8}{4} + 2\binom{6}{3} + 2\binom{4}{2} + 8\right)/24$

12. $(2^{81} + 8 \cdot 2^{27} + 72 \cdot 2^9)/81$

13. (i) $2^{12} \cdot 3^3$, (ii) $2^{14} \cdot 3^4$, (iii) $2^6 \cdot 3^2 + 2^{13} \cdot 3^4$

14. $\left(\binom{30}{15} + 20\binom{10}{5} + 24\binom{6}{3} + 30\binom{14}{7}\right)/60$

Diskrétní kalkulus

Mirek Olšák

Diference posloupnosti

Definice. Uvažujme posloupnost a_n (definovanou na přirozených nebo celých číslech). Definujeme její *posuv* Ea a *diferenci*[1] Δa vztahy

$$(Ea)_n = a_{n+1}, \quad (\Delta a)_n = a_{n+1} - a_n = (Ea - a)_n.$$

Cvičení. Popište všechny posloupnosti a splňující $\Delta a = a$. Která slavná posloupnost splňuje $a = E\Delta a$?

Diference k-té mocniny vyžaduje roznásobování binomickou větou – proto zavádíme pojem klesající mocniny, která se s diferencí kamarádí více.

Definice. *Klesající mocninu* $x^{\underline{k}}$ definujeme pro reálné číslo x a nezáporné celé číslo k jako

$$x^{\underline{k}} = x \cdot (x-1) \cdots (x-(k-1)), \quad x^{\underline{0}} = 1.$$

Pozorování. *K posloupnosti a_n můžeme najít diferenci následujícími vzorci:*

a_n	$n^{\underline{k}}$	c^n	$\binom{n}{k}$	cx_n	$x_n + y_n$	$x_n y_n$
(Δa_n)	$kn^{\underline{k-1}}$	$(c-1)c^n$	$\binom{n}{k-1}$	$c(\Delta x_n)$	$(\Delta x + \Delta y)_n$	$((\Delta x)y + (Ex)(\Delta y))_n$

Cvičení. Spočtěte diferenci posloupnosti $n^{\underline{3}} \cdot 3^n + \binom{n}{k}$.

Cvičení. Roznásobte $(x+y)^{\underline{2}}$ a upravte na tvar obsahující pouze klesající mocniny. Dokážete výsledek zobecnit?

Cvičení. Jaká je k-tá diference posloupnosti $n^{\underline{k}}$, respektive n^k?

Cvičení. Pomocí předchozího cvičení spočtěte $\sum_{k=0}^{n} \binom{n}{k}(-1)^k k^n$.

Cvičení. Dodefinujte klesající mocninu pro záporná čísla tak, aby $n^{\underline{-1}} = n^{-1}$ a platil vzorec pro diferenci.

[1] Obdoba derivace.

Opak diference – suma

Pozorování. *Pro danou posloupnost A_n lze najít posloupnost a_n takovou, že platí $\Delta A = a$. Tato posloupnost a_n je určena jednoznačně až na přičtení stejné konstanty ke všem členům a_n.*

Definice. Nějakou posloupnost A_n z předchozího pozorování značíme symbolem[2] $\sum a$. Pro celá čísla x, y dále definujeme $\sum_x^y a = A_y - A_x$.

Pozorování. *Číslo $\sum_x^y a$ nezávisí na volbě posloupnosti A, a je-li navíc $x < y$, platí rovnost (pozor!, a_y se nezapočítá)*

$$(\text{naše}) \sum_x^y a = (\text{klasická}) \sum_{n=x}^{y-1} a_n.$$

Obrácením vztahů z diference můžeme dostat vztahy pro sumu – například:

$$\sum n^{\underline{k}} = \frac{n^{\underline{k+1}}}{k+1} + C, \quad \sum (a+b) = \sum a + \sum b.$$

Cvičení. Pomocí klesajících mocnin zapište polynom p čtvrtého stupně splňující $p(0) = 1$, $p(1) = 4$, $p(2) = 57$, $p(3) = 232$, $p(4) = 625$.

Cvičení. Odvoďte vzorec pro součet $1^2 + 2^2 + \cdots + n^2$.

Počítání sumy již však není tak přímočaré jako u diference, protože chybí explicitní vzorec pro součin dvou posloupností. Namísto toho můžeme použít takzvanou sumaci *per partes* – ta součin zcela nezabije, ale při vhodném použití jej může zjednodušit. Je-li $\Delta A = a$, pak můžeme psát

$$\sum ab = Ab - \sum (EA)(\Delta b).$$

Cvičení. Spočtěte $\sum n \cdot 2^n$.

Cvičení. Součet $H_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$ se nazývá n-té harmonické číslo a odpovídá přirozenému logaritmu ve standardním kalkulu. Vyjádřete $\sum H_n$ a $\sum nH_n$.

Poděkování

Chtěl bych poděkovat Miškovi Szabadosovi, jehož příspěvek na totéž téma byl tak úžasný, že jsem jej jen s malými úpravami v podstatě převzal.

[2]Obdoba integrálu. Formálně si pod $\sum a$ můžeme představovat například množinu všech takových posloupností, proto se k vypočtené posloupnosti připisuje $+C$.

Tětivové čtyřúhelníky a mocnost

Anička Steinhauserová

Tětivové čtyřúhelníky

Věřte nebo ne, na následujícím jednoduchém tvrzení stojí velká část veškeré syntetické (tedy ne analytické) geometrie.

Tvrzení. (O obvodovém a středovém úhlu) *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 $|\sphericalangle ASB| = 2|\sphericalangle AMB|$.*

Tvrzení. (O úsekovém úhlu) *Mějme kružnici a její tětivu AB. V bodě A k ní sestrojíme tečnu t. Odchylku přímek AB a t nazveme úsekovým úhlem tětivy AB. Úsekový úhel má stejnou velikost jako příslušný obvodový úhel.*

Přikročme k tomu hlavnímu.

Definice. Čtyřúhelník nazýváme *tětivový*, pokud mu lze opsat kružnici.

Tvrzení. *Čtyřúhelník je tětivový právě tehdy, když je součet jeho protějších vnitřních úhlů roven* $180°$.

Příklady

Příklad 1. Máme zadané dvě kružnice k a l s průsečíky X a Y. Bodem X veďme přímku, která protíná k v bodě A a l v bodě C. Bodem Y veďme přímku, která protíná k v bodě B a l v bodě D. Dokažte $AB \parallel CD$.

Příklad 2. Máme zadané tři kružnice k, l a m procházející bodem P. Další průsečíky kružnic k, l, kružnic l, m a kružnic k, m označme postupně A, B, C. Nyní zvolme na kružnici k bod K různý od A, P, C. Přímka KA protne l v bodě L a přímka LB protne m v bodě M. Dokažte, že bod C leží na přímce KM.

Příklad 3. Buď D bod na přeponě AB pravoúhlého trojúhelníka ABC. Označme X střed kružnice opsané $\triangle ACD$ a Y střed kružnice opsané $\triangle BDC$. Dokažte, že body C, D, X a Y leží na jedné kružnici.

Příklad 4. Čtyřúhelník $ABCD$ je tětivový a má kolmé úhlopříčky. Označme po řadě p, q kolmice z bodů D, C na přímku AB. Dále označme X průsečík přímek AC a p, obdobně Y průsečík přímek BD a q. Dokažte, že $XYCD$ je kosočtverec nebo čtverec.

Příklad 5. Na kratším oblouku AB kružnice opsané čtverci $ABCD$ je dán bod P. Nechť $PD \cap AB = X$ a $PC \cap BD = Y$. Dokažte, že $|\sphericalangle XYB| = 90°$.

Příklad 6. Nechť $ABCD$ je pravoúhlý lichoběžník ($AB \parallel CD$, $AB \perp AD$). Sestrojme kružnici k, která se dotýká přímky AB v bodě A a přímky CD v bodě D. Dále sestrojme kružnici l, která se dotýká přímky AB v bodě B a prochází bodem C. Nechť kružnice k a l mají vnější dotyk v bodě P. Dokažte $|\sphericalangle PDC| = |\sphericalangle PCB|$.

Mocnost bodu ke kružnici

Definice. Je dán bod M a kružnice k se středem O a poloměrem r. *Mocností* bodu M ke kružnici k rozumíme číslo $p(M,k) = |MO|^2 - r^2$.

Tvrzení. (Základní vlastnosti) *Nechť M je bod a $k(O;r)$ kružnice.*

(i) *Číslo $p(M,k)$ je nulové právě tehdy, když bod M leží na kružnici k. Číslo $p(M,k)$ je kladné/záporné právě tehdy, když M leží vně/uvnitř kružnice k.*
(ii) *Buď N další bod. Je-li $p(M,k) = p(N,k)$, pak $|MO| = |NO|$.*
(iii) *Pokud M leží vně k, označme T ten bod kružnice k, pro který je přímka MT ke kružnici k tečnou. Pak platí $p(M,k) = |MT|^2$.*
(iv) *(zásadní!) Nechť přímka p vedená bodem M protne k v bodech A, B. Pak $MA \cdot MB = p(M,k)$, kde úsečky MA, MB nahlížíme jako orientované.*

Tvrzení. *Nechť $ABCD$ je čtyřúhelník a $Q = AD \cap BC$. Pak $ABCD$ je tětivový právě tehdy, když $|QA| \cdot |QD| = |QB| \cdot |QC|$.*

Příklady

Příklad 7. Na prodloužení tětivy KL kružnice k se středem O leží bod A. Tečny z bodu A ke kružnici k se jí dotýkají v bodech T, U. Označme M střed úsečky TU. Ukažte, že čtyřúhelník $KLMO$ je tětivový.

Příklad 8. Nechť $ABCD$ je čtyřúhelník vepsaný do kružnice k takový, že přímky AD a BC se protínají v bodě Q. Označme M průsečík přímky BD a rovnoběžky s přímkou AC vedenou bodem Q. Zvolme $T \in k$ tak, aby MT byla tečnou kružnice k. Dokažte, že $|MT| = |MQ|$. (PraSe 2005)

Příklad 9. Je dána kružnice k se středem S, mimo ni bod A. Na kružnici k je pohyblivý průměr XY. Trojúhelníku AXY je opsána kružnice se středem O. Určete množinu všech bodů O.

Příklad 10. Mějme rovnostranný trojúhelník ABC a jemu opsanou kružnici k. Nechť D, resp. E je střed strany AB, resp. AC. Polopřímka DE protíná k v bodě P. Dokažte: $|DE|^2 = |DP| \cdot |PE|$.

Příklad 11. Na úsečce AB je bod M. Ve stejné polorovině od AB jsou čtverce $ACDM$ a $MEFB$, kterým jsou opsány kružnice, jež se protnou v bodech M a N. Dokažte, že přímka MN prochází jedním bodem, bez ohledu na polohu bodu M.

Příklad 12. Je dán trojúhelník ABC a uvnitř něho bod P. Označme X průsečík přímky AP se stranou BC a Y průsečík přímky BP se stranou AC. Dokažte, že čtyřúhelník $ABXY$ je tětivový, právě když druhý průsečík (různý od bodu C) kružnic opsaných trojúhelníkům ACX a BCY leží na přímce CP.

Literatura a zdroje

Čerpala jsem z PraSečí knihovny, zejména z těchto příspěvků:

[1] Josef Tkadlec; *Mocnost a chordály*, Sborník MKS, 2010
[2] Tomáš „Šavlík“ Pavlík; *Tětivové čtyřúhelníky*, Sborník MKS, 2009

Diofantické rovnice

Kuba Svoboda

Diofantické rovnice je souhrnný název pro rovnice, kde nás zajímá přirozené, celočíselné, případně racionální řešení. Na diofantické rovnice neexistuje žádný obecný trik, ale kolem jejich řešení je rozvinutá zajímavá teorie. Z množiny existujících diofantických rovnic si vybereme ty, které se spíše objevují v olympiádách a mají hezké a pochopitelné řešení.

Rozklad na součin

Při rozkládání na součin využíváme faktu, že každé číslo lze rozložit na prvočísla nebo že některá čísla jsou nesoudělná. Potom už stačí jen výraz vhodně upravit, aby součin byl vidět, poté spočítáme jen triviální soustavu rovnic.

Úloha 1. Buďte p a q dvě prvočísla. Vyřešte tuto rovnici v přirozených číslech:

$$\frac{1}{x}+\frac{1}{y}=\frac{1}{pq}.$$

Úloha 2. Najděte všechna celočíselná řešení rovnice $x^2+3x=y^3-2$.

Úloha 3. Najděte všechna nezáporná řešení rovnice

$$(xy-7)^2=x^2+y^2.$$

Úloha 4. Najděte všechny trojice přirozených čísel x, y, z takové, že platí

$$x^3+y^3+z^3-3xyz=17.$$

Bonus: Řešte rovnici $x^3+y^3+z^3-3xyz=p$, kde p je libovolné prvočíslo větší než 3.

Úloha 5. Vyřešte v $\mathbb{N}$ rovnici $p-y^4=4$, kde p je prvočíslo.

Úloha 6. Najděte všechny dvojice celých čísel x, y splňujících $x^6+3x^3+1=y^4$.

Počítání modulo

Pokud zvládnete zjistit, jaký dává neznámá zbytek po dělení dvěma, už vám stačí vyzkoušet jen polovinu toho, co jste museli předtím. Někdy je tato metoda ještě silnější a výsledek vypadne po několika úvahách.

Úloha 7. F_n je n-té Fibonacciho číslo ($F_1 = 1, F_2 = 1, F_{n+2} = F_{n+1} + F_n$). Najděte všechny dvojice $a, n \in \mathbb{N}$ takové, že

$$F_n + F_{2n} + F_{3n} = a! + 43.$$

Úloha 8. Najděte všechna $m, n \in \mathbb{N}$ taková, že platí $1! + 2! + 3! + \cdots + n! = m^2$.

Úloha 9. Dokažte, že rovnice

$$x^2 = 3 - 8z + 2y^2$$

nemá řešení v celých číslech.

Úloha 10. Řešte v přirozených číslech rovnici $a^6 + b^4 + c^2 = 1234567$.

Úloha 11. Dokažte, že rovnice

$$(x+1)^2 + (x+2)^2 + \cdots + (x+2001)^2 = y^2$$

nemá řešení v celých číslech.

Úloha 12. Dokažte, že rovnice

$$x^5 - y^2 = 4$$

nemá řešení v celých číslech.

Úloha 13. Najděte všechny páry přirozených čísel x, y, pro které platí

$$x^2 - a! = 1996.$$

Nerovnosti

Využijeme jednoduché tvrzení, a to, že neexistují x, y a n přirozená tak, že

$$y^n < x^n < (y+1)^n.$$

Také můžeme použít faktu, že některé nejmenší číslo může být hodně malé, což celou úlohu zjednoduší.

Úloha 14. V $\mathbb{N}$ řešte rovnici $4^a + 4a^2 + 4 = b^2$.

Úloha 15. Najděte všechny trojice (x, y, z) přirozených čísel takových, že

$$\left(1+\frac{1}{x}\right)\left(1+\frac{1}{y}\right)\left(1+\frac{1}{z}\right)=2.$$

Úloha 16. Vyřešte v přirozených číslech rovnici $3(xy+yz+zx)=4xyz$.

Úloha 17. Najděte všechny dvojice $x, y \in \mathbb{Z}$, pro něž platí $x^3+y^3=(x+y)^2$.

Úloha 18. Najděte všechna celočíselná řešení rovnice

$$x^3+(x+1)^3+(x+2)^3+\cdots+(x+7)^3=y^3.$$

Úloha 19. Najděte všechny trojice přirozených čísel x, y, z, která splňují rovnici

$$(x+y)^2+3x+y+1=z^2.$$

Úloha 20. Najděte přirozená čísla n a $k_1, k_2, \ldots, k_n$ taková, že

$$k_1+k_2+k_3+\cdots+k_n=5n-4,$$

$$\frac{1}{k_1}+\frac{1}{k_2}+\frac{1}{k_3}+\cdots+\frac{1}{k_n}=1.$$

Fermatova metoda nekonečného sestupu

Tvrzení. *Neexistuje nekonečná klesající posloupnost přirozených čísel.*

Tato metoda funguje jednoduše. Místo toho, abychom hledali řešení, si představíme, že řešení už máme. Pomocí tohoto řešení nalezneme jedno menší. A pomocí toho zase další, které je menší... No a tak dále.

Úloha 21. Najděte všechna řešení v nezáporných celých číslech rovnice

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

Úloha 22. Najděte všechny trojice $x, y, z \in \mathbb{N}$, které splňují rovnici

$$x^3+3y^3+9z^3-3xyz=0.$$

Úloha 23. Najděte všechna celočíselná řešení rovnice $x^2+y^2=7z^2$.

Úloha 24. Najděte všechna celočíselná řešení rovnice $\frac{x-y^2}{y}+\frac{y-x^2}{x}=(x-1)(y-1)$.

Úloha 25. Vyřešte v celých číslech rovnici $x^4+y^4+z^4=9u^4$.

Úloha 26. Řešte v přirozených číslech následující rovnici: $x^2-y^2=2xyz$.

Další úlohy

Pokud se vám chce řešit, můžete, pokud ne, tak to máte na doma.

Úloha 27. Pro každé přirozené $n \geq 3$ dokažte, že existují různá čísla $x_1, x_2, \ldots x_n$ splňující rovnici $\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n} = 1$.

Úloha 28. Dokažte, že pro každé $n \in \mathbb{N}$ je rovnice $x^2 + y^2 + z^2 = 59^n$ řešitelná v $\mathbb{N}$.

Úloha 29. (Velká Fermatova věta pro $n = 4$) Dokažte, že rovnice $x^4 + y^4 = z^4$ nemá řešení v přirozených číslech.

Návody k úlohám

1. Co kdybychom po roznásobení na každou stranu přidali p^2q^2?

2. Znáte dvě po sobě následující čísla, které jsou třetí mocninou?

3. Co kdyby bylo vlevo jen $(xy - 6)^2$?

4. Vyzkoušejte, čemu se rovná $(x + y + z)(x^2 + y^2 + z^2 - xy - zy - xz)$.

5. Co nám zbude, když dáme $(y^4 + 2)^2$?

6. $(x^3 + 1)^2 + x^3 + 1 = y^4 + 1$ a potom vynásobte 4.

7. Něco je liché a něco je sudé...

8. Stačí najít správné číslo, kterým modulit.

9. Je jen pár možností, jaké zbytky může dávat druhá mocnina.

10. Zase modulte správným číslem.

11. Substituujte $x = y - 1001$.

12. Se znalostí Fermatovy věty je příklad jednodušší.

13. Zase najděte správné číslo.

14. $4^a = 2^{2a} = (2^a)^2$. Kolik je potom $(2^a + 1)^2$?

15. Jaké může být nejmenší číslo, jaké největší?

16. Vydělte to tak, aby na jedné straně byly jen neznámé a na druhé čísla, a potom se zase zeptejte, jaké může být nejmenší a jaké největší.

17. Co roste rychleji?

18. Kolik je tam x? Sevřete to mezi dvě třetí mocniny.

19. Zase sevřete mezi dvě druhé mocniny.

20. Tady použijte slavné nerovnosti. Buď harmonický-aritmetický průměr nebo Cauchyho-Schwarzovu.

21. Nejjednodušeji, jak to jde.

22. Co třeba trojka, jaký zbytek po dělení třemi dává x?

23. Když je tam napsaná sedmička, co kdybych zkusil ji?

24. Nějaká úprava, třeba na $x^2 + xy + y^2 = x^2y^2$, a potom jsou tam dvě neznámé, tak co třeba dvěma?

25. Co třeba malý Fermat? Pomůže?

26. Tentokrát vyzkoušíme obecné p, co dělí v pravo, musí dělit vlevo.

27. Z náhodně nalezeného řešení pro $n = 3$ pak vyrobíme další.

28. Pokud už máme jeden výsledek, máme ho i pro $n + 2$.

29. Stačí si uvědomit, že $x^4 = (x^2)^2$, no a ještě pár dalších věcí.

Zdroje

Čerpal jsem zejména z knihy *Úvod do diofantických rovnic* od Titu Andreescu.

Kruhová inverze

Pepa Svoboda

Síla tohoto zobrazení spočívá v tom, že dokáže převést tvrzení o kružnicích na tvrzení o přímkách. Často se komplikovaná geometrická situace po vhodném zobrazení inverzí změní na jednoduchou a přístupnou klasickým metodám planimetrie.

Úmluva. Rovinu rozšíříme o jediný bod ∞, o kterém tvrdíme, že leží na všech přímkách.

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

(i) Když je $A = O$, potom $A' = \infty$.
(ii) Když je $A = \infty$, potom $A' = O$.
(iii) Jinak je A' bod polopřímky OA, pro který platí

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

Cvičení. Rozmyslete si následující jednoduchá pozorování.

(1) Kruhová inverze je bijekce, pokud ji navíc provedeme dvakrát podle stejné kružnice, dostaneme identitu.
(2) Pevné body inverze podle kružnice k jsou přesně body této kružnice.
(3) Pokud leží bod A „uvnitř“ kružnice k, leží obraz A' „vně“, a naopak.

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

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

Kruhová inverze není shodné ani podobné zobrazení. Přesto dokážeme vyjádřit vzdálenost obrazů dvou bodů následujícím způsobem.

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

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

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

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

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

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

Vyzbrojeni těmito poznatky se můžeme vrhnout na úlohy.

Příklady

Příklad. V rovině jsou dány dvě kružnice k, ℓ s průsečíky A, B. Vezměme přímku p procházející bodem B, její druhý průsečík s kružnicí k označme C, její druhý průsečík s kružnicí ℓ označme D. Dokažte, že velikost úhlu CAD nezávisí na poloze přímky p.

Řešení. Zajímá nás velikost úhlu sevřeného přímkami AC a AD. Obě tyto přímky procházejí bodem A, a navíc tímto bodem procházejí i obě kružnice k, ℓ. Zobrazme tedy celou situaci v inverzi se středem A a nějakým poloměrem r. Obrazy kružnic k, ℓ budou přímky k', ℓ' s průsečíkem B'. Obrazem přímky p je kružnice p', která prochází bodem A. Tato kružnice protíná přímku k' podruhé v bodě C' a přímku ℓ' podruhé v bodě D'.

Máme tři možná pořadí, jak můžou na kružnici p' ležet tyto body: A, C', B', D', nebo A, B', C', D', nebo A, C', D', B'. Ve všech třech případech je velikost úhlu $C'AD'$ rovna velikosti úhlu sevřeného přímkami k', ℓ' – toho, ve kterém neleží bod A. A to je přesně to, co jsme chtěli dokázat. □

Cvičení. (Švrčkův bod) Dokažte bez použití inverze. Je dán trojúhelník ABC s vepsištěm I. Dokažte, že osa strany AB, osa úhlu ACB a kružnice opsaná trojúhelníku ABC se protínají v jednom bodě. Označme tento bod Š. Dokažte, že Š je střed kružnice opsané trojúhelníku ABI.

Příklad 1. V rovině jsou dány tři shodné kružnice, které procházejí společným bodem H. Označme druhé průsečníky těchto kružnic A, B, C (různé od H). Dokažte, že H je ortocentrum trojúhelníka ABC.

Příklad 2. Přímka p protne kružnici k v bodech X, Y. Označme R střed oblouku XY. Bodem R vedeme dvě přímky, které protnou kružnici k v bodech A, B a přímku p v bodech C, D. Ukažte, že body A, B, C, D leží na jedné kružnici.

Příklad 3. (Ptolemaiova nerovnost) Pro čtyřúhelník $ABCD$ platí:

$$|AB| \cdot |CD| + |BC| \cdot |AD| \geq |AC| \cdot |BD|,$$

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

Příklad 4. Kružnice k_1, k_2 se protínají v bodech A, B. Kružnice k_3 se zvenku dotýká kružnic k_1, k_2 popořadě v bodech C, E. Kružnice k_4 se zvenku dotýká kružnic k_1, k_2 popořadě v bodech D, F. Dokažte, že kružnice opsaná trojúhelníku ACE se dotýká kružnice opsané trojúhelníku ADF. (Polská MO 2004)

Příklad 5. V rovině jsou dány dvě kružnice k, ℓ s průsečíky A, C. Z bodu A vedeme tečnu ke k, ta podruhé protne kružnici ℓ v bodě D. Bod B je průsečíkem kružnice k s tečnou ke kružnici ℓ v bodě A. Dokažte, že $|AB| \cdot |CD| = |AC| \cdot |AD|$.

Příklad 6. Kružnice ℓ se zvenku dotýká kružnice k v bodě A. Zvolíme bod B na kružnici ℓ. Tečna k ℓ v bodě B protne kružnici k v bodech D, E. Označme C střed toho oblouku DE kružnice k, který obsahuje bod A. Dokažte, že body A, B, C leží na přímce.

Příklad 7. Jsou dány kružnice k_1, k_2, k_3, k_4 tak, že k_i se zvenčí dotýká k_{i+1} pro $i = 1, 2, 3, 4$ ($k_5 = k_1$). Dokažte, že čtyři body dotyku těchto kružnic leží na jedné kružnici.

Příklad 8. Kružnice k_1, k_2 se zvenku dotýkají v bodě D. Přímka p se dotýká kružnic k_1, k_2 po řade v (různých) bodech A, B. Úsečka AC je průměrem kružnice k_1. Přímka q prochází přes bod C a dotýká se kružnice k_2 v bodě E. Dokažte, že trojúhelník ACE je rovnoramenný. (Polská MO 2004)

Další příklady

Příklad 9. Na půlkružnici nad průměrem AB a se středem O zvolíme body C, D. Předpokládejme, že se polopřímky AB a DC protnou v bodě M. Označme K druhý průsečík kružnic opsaných trojúhelníkům AOD a BOC. Ukažte, že $|\sphericalangle MKO| = 90°$. (Rusko 1995)

Příklad 10. (Steinerův porismus) Uvnitř kružnice k je dána kružnice l. Předpokládejme, že existuje n-prvkový řetěz kružnic $m_1, \ldots, m_n$ takový, že každá kružnice v řetězu má vnější dotyk se svými dvěma sousedními kružnicemi a s l a vnitřní dotyk s k. Potom každá kružnice mající vnější dotyk s l a vnitřní dotyk s k je částí nějakého n-prvkového řetězu.

Příklad 11. Kružnice k_1 a k_3 stejně jako k_2 a k_4 mají vnější dotyk v bodě P. Označme druhé průsečíky $k_1 \cap k_2 = A$, $k_2 \cap k_3 = B$, $k_3 \cap k_4 = C$ a $k_4 \cap k_1 = D$. Dokažte, že

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

(IMO shortlist 2003)

Návody k příkladům

1. Stačí ukázat, že AH je kolmé na BC, a využít předcházející cvičení.

2. Uvažte inverzi se středem R, která zobrazí p na k, a všimněte si, že body C, D přejdou na body A, B.

3. Co připomíná dokazovaný vztah?

4. Pryč s kružnicemi! Jak se změní dokazované tvrzení?

5. Umíme se vhodnou inverzí zbavit nějakých kružnic?

6. Dá se udělat inverze tak, aby se kružnice k zobrazila na přímku DE?

7. Za střed inverze zvolte libovolný bod dotyku a využijte stejnolehlost.

8. Zkuste použít inverzi se středem v bodě C a poloměrem $|CA|$.

9. Invertujte podle zadané půlkružnice a rozpoznejte obrázek s ortocentrem a Feuerbachovou kružnicí.

10. Invertujte tak, aby kružnice k, l přešly v soustředné kružnice. Pak je tvrzení zřejmé.

11. Invertujte podle P. Přepočtěte dokazovaný vztah a využijte toho, že v rovnoběžníku mají protější strany shodnou délku.

Literatura a zdroje:

Při tvorbě přednášky jsem čerpal ze starších příspěvků Viktora „Zaja“ Szabadose a Josefa „Pepy“ Tkadlece, kterým bych tímto velmi rád poděkoval.

[1] *http://www.artofproblemsolving.com*
[2] Archiv MKS, *http://mks.mff.cuni.cz/archiv*

Tropická geometrie

Pepa Svoboda

Tropické počítání

Tropickými čísly nazýváme obvyklá reálná čísla, ke kterým z formálních důvodů přidáme $-\infty$. Na těchto číslech zavedeme dvě operace: tropické sčítání "$+$" a tropické násobení "$\cdot$", za kterými se neskrývá nic jiného než obvyklé maximum a sčítání: "$x + y$" $= \max\{x, y\}$, "$x \cdot y$" $= x + y$.

Příklad. Platí "$1 + 1$" $= 1$, "$1 + 2$" $= 2$, "$1 \cdot 1$" $= 2$, "$0 \cdot 1$" $= 1$, "$-\infty + 5$" $= 5$.

Poznámka. Tropické operace se v jistém smyslu dohromady chovají podobně jako obvyklé sčítání s násobením. Platí například, že "$a + (b + c)$" $=$ "$(a + b) + c$" nebo "$a(b + c)$" $=$ "$ab + ac$". Prvek $-\infty$ hraje obvyklou roli nuly, zatímco nula hraje obvyklou roli jedničky. Základní odlišnost ale spočívá ve faktu, že v tropickém světě není žádné odčítání – pro žádné číslo $a \neq -\infty$ neexistuje číslo b tak, aby "$a + b$" $= -\infty$. Proto se tropickým číslům obvykle říká „semitěleso“[1].

Cvičení. (Školákův sen) "$(x + y)^n$" $=$ "$x^n + y^n$".

Tropické polynomy

Funkcím tvaru $f(x) =$ "$\sum_{i=0}^{n} a_i x^i$" říkáme tropické polynomy[2]. Pokud přepíšeme tropické operace podle definice, dostaneme $f(x) = \max\{a_i + n \cdot x\}$, což je maximum z několika lineárních funkcí – tedy konvexní, po částech lineární funkce.

Příklad. "$0 \cdot x$" $=$ "x" $= x$, "$1 \cdot x$" $= x + 1$, "$3x^3 - 2x^2 + x + 3$" $= \max\{3x + 3, 2x - 2, x, 3\}$.

Definice. Kořen tropického polynomu $f = \sum_0^n a_i x^i$ je takové číslo x_0, ve kterém se láme graf polynomu. Jinými slovy to je číslo, pro které platí $a_i + i x_0 = a_j + j x_0$ pro nějaká $0 \leq i, j \leq n$. Maximum výrazu $|i - j|$ pro taková i a j nazýváme násobnost kořene x_0. Násobnost kořenu tedy vyjadřuje, jak moc se graf zlomí.

[1] Zatímco reálná čísla tvoří tzv. těleso.

[2] Formálně správnější je říkat „tropické funkce“, neboť dva polynomy mohou odpovídat jedné funkci, např "$x^2 + x + 0$" $= \max\{2x, x, 0\} = \max\{2x, 0\} =$ "$x^2 + 0$".

Cvičení. Nakresli grafy polynomů "$x^3 + 2x^2 + 3x + (-1)$" a "$x^3 + (-2)x^2 + 2x + (-1)$" a urči jejich kořeny.

Cvičení. Tropické číslo x_0 je kořenem polynomu $p(x)$ s násobností aspoň k, právě když existuje polynom $q(x)$ tak, že "$p(x) = (x + x_0)^k q(x)$".

Cvičení. Tropický polynom stupně n má přesně n kořenů, pokud je počítáme s násobností.

Každý tropický polynom stupně n se tedy dá zapsat jako součin n lineárních polynomů, podobně jako komplexní polynomy. Naopak reálné polynomy tuto silnou vlastnost nemají.

Tropické křivky

Zajímavá situace nastane, pokud vezmeme tropické polynomy dvou proměnných x a y a díváme se na kořeny těchto polynomů (tím opět myslíme místa, kde se láme graf polynomu). Dostaneme tak „tropické křivky“, podobně jako v klasické geometrii dostaneme obvyklé rovinné křivky.

Příklad. Křivka zadaná polynomem $x+y+0$ je složena z tří polopřímek vedoucích z počátku soustavy souřadné v západním, jižním a severovýchodním směru.

Cvičení. Všechny křivky "$ax + by + c$" mají stejný tvar. Říkáme jim tropické přímky.

Cvičení. (Nakresli si koníka) Načrtni graf křivky "$x^2 + 1xy + (-3)y^2 + x + y + 0$".

Cvičení. Jak mohou obecně vypadat grafy polynomů stupně dva, tj. tropické kuželosečky?

Pro každý polynom "$P(x, y)$" vyznačme v rovině body (i, j) pro všechny jednočleny $x^i y^j$, které se vyskytují v polynomu $P(x, y)$, dále spojme hranou ty body, které odpovídají jednočlenům, jejichž oblasti (místa, kde tento jednočlen odpovídá maximu) se v grafu křivky dotýkají. Takto dostaneme duální mnohoúhelník (dále jen duálník) tropické křivky.

Cvičení. Nakresli duálník tropické přímky a koníka.

Cvičení. Jakým objektům v duálníku odpovídají vrcholy tropických křivek? Co platí pro hranu křivky a odpovídající hranu v mnohoúhelníku?

Cvičení. Zkus najít metodu, jak nakreslit tropickou křivku na základě znalosti jejího duálníku.

Věta. (tropická verze Bézoutovy věty) *Nechť C_1 a C_2 jsou křivky stupně d_1 a d_2, které se protínají jen v konečně mnoha bodech a v žádném z vrcholů. Potom je počet průsečíků C_1 a C_2 roven $d_1 \cdot d_2$.*

Důležitým pozorováním je, že sjednocením dvou tropických křivek je tropická křivka. Násobnost průsečíku se poté definuje jako obsah odpovídající oblasti mno-

hoúhelníka (což musí být rovnoběžník). S tímto uvědoměním se můžeš sám vrhnout na důkaz Bézoutovy věty.

Úloha. Dokaž Bézoutovu větu.

Z reality do tropů a zpět

Standardním semitělesem v matematice nejsou tropická, nýbrž nezáporná reálná čísla. Předvedeme si, jak spolu navzájem souvisejí: Pro každé $t > 1$ vezměme funkci z nezáporných reálných čísel do tropických čísel, která číslu x přiřadí $\log_t(x)$. Jde o bijekci, inverzní zobrazení přiřadí tropickému číslu a nezáporné číslo t^a. Zavedeme na tropických číslech operaci $\cdot_t$ takový, že vezmeme odpovídající nezáporná reálná čísla, ta normálně vynásobíme a podíváme se, kterému tropickému číslu odpovídá výsledek. Tyto funkce převádějí obvyklé násobení na tropické násobení:

$$a \cdot_t b = \log_t(t^a \cdot t^b)) = \log_t(t^a) + \log_t(t^b) = a + b = \text{"}a \cdot b\text{"}.$$

Nic podobného ale neplatí pro sčítání:

$$a +_t b = \log_t(t^a + t^b) \neq \max\{a, b\}.$$

Můžeme se nicméně podívat, co se stane, když pošleme t do nekonečna: BÚNO $a = \max\{a, b\}$. Platí nerovnosti

$$a = \log_t(t^a) \leq \log_t(t^a + t^b) \leq \log_t(2t^a) = a + \log_t(2).$$

Vidíme, že náš výraz je z obou stran sevřen výrazy, které jdou k a, sám proto také jde k $a = \max\{a, b\}$.

Podobnou metodou založenou na funkcích (z reálné roviny do tropických čísel) zadaných jako $(\log_t |x|, \log_t |y|)$ můžeme převádět klasické křivky na tropické. Zajímavé je, že se tento proces dá obrátit – díky tomu můžeme pomocí jednoduchých tropických křivek vytvářet a popisovat „opravdové“ algebraické křivky, což je jinak obtížný problém[3].

Literatura a zdroje:

Při tvorbě příspěvku jsem čerpal z přednášky profesora Iliy Itenberga, kterému bych tímto velmi rád poděkoval.

[1] *http://arxiv.org/pdf/1311.2360v3.pdf*
[2] *http://homepages.warwick.ac.uk/staff/D.Maclagan/papers/TropicalBook23.8.13.pdf*
[3] *http://math.jacobs-university.de/summerschool/2013/videos/index.php*

[3] V podstatě se jedná o šestnáctý Hilbertův problém, jenž zůstává stále otevřený pro křivky stupně osm a víc.

Pick v německém lesíku

Martin „E.T.“ Sýkora

Na přednášce si definujeme, co jsou mřížové body, a naučíme se s nimi lehce pracovat. Stěžejní částí přednášky bude Pickova formule, která umožňuje snadno počítat obsahy určitých mnohoúhelníků. Zbude-li čas, popovídáme si i o Minkowského větě a využijeme ji k řešení úlohy o německém lesíku.

Pickova formule

Definice. *Mřížovým bodem* nazveme bod X v rovině, jehož obě souřadnice jsou celočíselné. Jinak řečeno, mřížovým bodem nazveme bod X takový, že $X = \{a, b\}$, kde $a, b \in \mathbb{Z}$.

Tvrzení. (Pickova formule) *Mějme libovolný jednoduchý mnohoúhelník*[1] M *s vrcholy v mřížových bodech. Označme* V *počet těch mřížových bodů, které leží uvnitř* M*, a* H *počet těch, které leží na jeho obvodu. Pak obsah* M *je roven* $V + \frac{H}{2} - 1$.

Příklad 1. Mějme mřížku o hraně délky $\sqrt{2}$. Dokažte, že každý mnohoúhelník s vrcholy v bodech této mřížky má celočíselný obsah.

Příklad 2. Platí nějaká obdoba Pickovy formule i v prostoru? A co v trojúhelníkové mřížce?

Příklad 3. *Půlbodem* nazývejme libovolný bod o souřadnicích $(k/2, l/2)$, kde k a l jsou celá čísla. Každý půlbod určitě jde vyjádřit jako střed úsečky spojující dva mřížové body mnoha různými způsoby. Představte si, že máte půlbod ležící uvnitř nějakého mřížového mnohoúhelníku. Dokažte, že jej lze dostat jako střed úsečky spojující dva mřížové body, které samy leží uvnitř tohoto mnohoúhelníku.

Příklad 4. (Varianta Pickovy formule pro „mnohoúhelník s dírami“) Dokažte, že obsah mnohoúhelníku, který obsahuje D „děr“, je roven $V + \frac{H}{2} + D - 1$, kde H je počet mřížových bodů na všech $D+1$ uzavřených křivkách tvořících hrany mnohoúhelníku.

Příklad 5. Mějme mřížový trojúhelník ABC takový, že jedinými mřížovými body na jeho hranici jsou jeho vrcholy a uvnitř něj leží právě jeden mřížový bod. Dokažte, že tento bod je těžištěm trojúhelníku ABC.

[1] Jednoduchý mnohoúhelník je takový mnohoúhelník, jehož obvod neprotíná sám sebe.

Minkowského věta a německý lesík

Co by to bylo za přednášku s jednou jedinou definicí?

Definice. *Konvexní* množina obsahuje s každými dvěma svými body A, B celou úsečku AB.

Věta. (Minkowského) *Všechny konvexní množiny bodů v rovině, které jsou středově souměrné podle počátku a mají obsah ostře větší než* 4*, obsahují alespoň jeden mřížový bod různý od nuly.*

Poznámka. Větu lze zobecnit i pro vyšší dimenze. Pak objem porovnáváme s 2^d, kde d je dimenze prostoru.

Úloha. (O německém lesíku) Mějme čtverec o straně délky 50 m a ve vrcholech každého metru čtverečního vyjma středu strom s průměrem kmene 8 cm. Nazvěme toto seskupení německým lesíkem. Stojí-li pozorovatel ve středu německého lesíku, vidí z něho ven?

Překvapivě ale Minkowského věta nemá uplatnění jen v geometrii. Přesvědčit se o tom můžete v následujícím příkladu z teorie čísel.

Příklad. Ukažte, že pro každé kladné iracionální číslo α existuje nekonečně mnoho dvojic přirozených čísel m, n takových, že

$$\left|\alpha - \frac{m}{n}\right| < \frac{1}{n^2}.$$

Zdroje

[1] Míša Prokešová; *Německý lesík a teorie čísel*, Sborník MKS, 1998
[2] Jarda Hančl; *Pickova formule*, soustředění Sborník MKS, 2009
[3] Helča Svobodová; *Pickova formule*, Sborník MKS, 2012
[4] Náboj, soustředění Domašov 2012
[5] *http://math.jacobs-university.de/summerschool/2013/videos/index.php*

Částečná uspořádání

Martin „E.T.“ Sýkora

Částečná uspořádání se pohybují na hranici středoškolské olympiádní a vysokoškolské matematiky. Ve středoškolských úlohách se jejich aplikace vyskytují spíše výjimečně, a proto ani v tomto příspěvku nečekej smršť olympiádních úloh. Přesto se k nějakým dostaneme. Nejprve si ale musíme odbýt (nebo užít?) teorii.

Teoretické minimum

Definice. *Kartézským součinem množin X a Y* rozumíme množinu všech uspořádaných dvojic tvaru (x, y), kde $x \in X$ a $y \in Y$. Tento součin značíme $X \times Y$. V případě, že $X = Y$, značíme jej tradičně X^2.

Definice. O množině M řekneme, že je *binární relací mezi množinami X a Y*, pokud $M \subseteq X \times Y$. Binární relace obvykle značíme písmenem R.

Poznámka. Místo relativně zdlouhavého zápisu $(x, y) \in R$ většinou píšeme $R(x, y)$ nebo xRy.

Poznámka. Speciálním případem relací jsou funkce. Jedná se o takové relace R, v nichž pro každé $x \in X$ existuje nejvýše jedno $y \in Y$ splňující $(x, y) \in R$.

Nyní si představme, že máme množinu X a na ní relaci R.[1] Pak o R řekneme, že je *částečným uspořádáním*[2] *množiny M*, pokud má následující vlastnosti:

(a) (Tranzitivita) Pokud pro nějaké tři prvky $x, y, z \in X$ platí $R(x, y)$ a $R(y, z)$, pak pro ně platí i $R(x, z)$.
(b) (Slabá antisymetrie) Pokud pro nějaké dva prvky $x, y \in X$ platí $R(x, y)$ a $R(y, x)$, pak $x = y$.
(c) (Reflexivita) Pro všechna $x \in X$ platí $R(x, x)$.

Částečná uspořádání jsou tedy kvůli reflexivitě neostrá.

[1] Relací na množině M rozumíme relaci mezi množinami M a M.
[2] Místo pojmu částečné uspořádání často užíváme stručnější pojem uspořádání.

Poznámka. Částečná uspořádání se místo R tradičně značí symbolem $\leq$. Nejčastěji se pak setkáváne se zápisem $x \leq y$, zatímco zápis $\leq (x, y)$ se používá výjimečně. Symbolem $\leq$ tedy odteď nebudeme značit relaci „menší nebo rovno“, ale libovolné částečné uspořádání. I přesto budeme zápis $x \geq y$ číst „x je větší než y“.

Definice. Uspořádanou dvojici $(X, \leq)$, kde X je nějaká množina a $\leq$ je částečné uspořádání, nazveme *častečně uspořádanou množinou*, neboli *ČUM*.

Definice. *Řetězcem* na ČUM $(X, \leq)$ nazveme množinu Y takovou, že pro všechna $x, y \in Y$ buď $x \leq y$, nebo $y \leq x$. *Antiřetězcem* na $(X, \leq)$ pak nazveme množinu Z takovou, že pro všechny $u, v \in Z, u \neq v$ neplatí ani $u \leq v$, ani $v \leq u$.

Definice. Prvek x z ČUM $(X, \leq)$ se nazývá

(i) *maximální*, pokud „žádný prvek není ostře větší“, tedy pokud pro žádné $y \in X$, $y \neq x$, neplatí $x \leq y$,
(ii) *největší*, pokud „je větší než všechny ostatní“, tedy pokud pro každé $y \in X$ platí $y \leq x$,
(iii) *minimální*, pokud „žádný prvek není ostře menší“, tedy pokud pro žádné $y \in X$, $y \neq x$, neplatí $y \leq x$,
(iv) *nejmenší*, pokud „je menší než všechny ostatní“, tedy pokud pro každé $y \in X$ platí $x \leq y$.

Teoretické maximum (které stihneme probrat)

Po smršti definic ze začátku si ukážeme několik zajímavých vět a tvrzení.

Věta. (O dlouhém a širokém) *Nechť (X, R) je konečná ČUM, $X \neq \emptyset$. Potom $|X| \leq \alpha(X, R) \cdot \omega(X, R)$, kde*

(i) *$\alpha(X, R)$ je počet prvků v největším antiřetězci,*
(ii) *$\omega(X, R)$ je počet prvků v největším řetězci.*

Věta. (Dilworthova) *Nechť k je velikost největšího antiřetězce v $(X, \leq)$, kde množina X je konečná. Pak lze X pokrýt pomocí k řetězců.*

Dilworthova věta má i svou duální sestru, která říká, že pokud je k velikost největšího řetězce v $(X, \leq)$, kde množina X je konečná, lze X pokrýt pomocí k antiřetězců.

Věta. (Spernerova) *Mějme libovolný antiřetězec F na množině všech podmnožin množiny $X, |X| = n$, uspořádané inkluzí. Pak $|F| \leq \binom{n}{n/2}$.*

A konečně příklady

Konečně se dostáváme k příkladům a úlohám. Některé z nich se dají řešit elementárně, jiné jsou ušity na míru jedné z výše uvedených vět. Nejprve si vyzkoušíme vyřešit několik spíše teoretických úloh (seřazených přibližně od nejlehčí po nejtěžší).

Cvičení 1. Dokažte, že pokud je prvek x nejmenším prvkem nějaké ČUM, pak je i jejím minimálním prvkem.

Cvičení 2. Je relace *být dělitelem* na množině přirozených čísel částečným uspořádáním? Jinak řečeno, je relace $R = \{(x, y); x \mid y\}$ částečné uspořádání na $\mathbb{N}$? Pokud ano, má maximální, minimální, největší a nejmenší prvky? Pokud ano, pokuste se je chrarakterizovat.

Cvičení 3. Dokažte, že každá konečná ČUM má minimální a maximální prvek.

Úloha 4. (Věta o reprezentaci) Ukažte, že pro každou ČUM $(X, \leq)$ existuje prosté zobrazení $f : X \to \mathcal{P}(X)$ takové, že $f(x) \subseteq f(y)$ právě tehdy, když $x \leq y$.

Následují o něco „praktičtější“ úlohy, jimž podobné lze potkat v různých matematických soutěžích, třeba MO. Opět jsou uspořádány přibližně podle obtížnosti.

Úloha 5. Ukažte, že mezi $n + 1$ čísly z množiny $\{1, 2, \ldots, 2n\}$ jsou dvě taková, že jedno dělí druhé.

Úloha 6. Je dáno 1001 obdélníků s celočíselnými délkami stran nepřesahujícími 1000. Dokažte, že je možné najít tři obdélníky takové, že jeden se vejde do druhého a druhý do třetího. Obdélníky je možné otáčet a stejně velké obdélníky se do sebe vejdou.

Úloha 7. Test skládající se ze tří úloh řešilo 49 studentů. Za každou úlohu bylo možné získat 0 až 7 bodů. Dokažte, že existují dva studenti takoví, že jeden z nich získal z každé úlohy alespoň tolik bodů jako ten druhý.

Úloha 8. Nechť n je bezčtvercové přirozené číslo.[3] Uvažme množinu D nějakých jeho dělitelů takových, že žádný dělitel z D nedělí jiného dělitele z D. V závislosti na n určete největší možnou velikost množiny D.

Úloha 9. (Erdős, Szekeres) Jsou dána přirozená čísla a, b. Ukažte, že z každé posloupnosti, jejíž členy se neopakují a která má délku $ab + 1$, lze vybrat rostoucí posloupnost délky $a + 1$ nebo klesající posloupnost délky $b + 1$.

Úloha 10. Mějme 50 ne nutně různých intervalů. Dokažte, že alespoň osm z nich má společný neprázdný průnik, nebo alespoň osm z nich je po dvou disjunktních.
(AUO 1972)

Úloha 11. Buď n přirozené číslo. Množinu $S \subseteq \{1, 2, 3, \ldots, n\}$ nazveme *trojatou*, pokud neobsahuje tři členy a, b, c takové, že $a \mid b$ a zároveň $b \mid c$. Určete největší možný počet prvků trojaté množiny S. (MEMO 2012)

[3] Přirozené číslo je bezčtvercové, pokud jej nedělí čtverec žádného přirozeného čísla většího než jedna.

Literatura a zdroje

[1] Matoušek, J. a Nešetřil, J.; *Kapitoly z diskrétní matematiky*, Praha, 2002
[2] Mirek Olšák, *Od Dirichleta k pravděpodobnosti*, Sborník iKS, 2012

Rozklady

Štěpán Šimsa

Rozklady patří do netradiční části teorie čísel, kde místo s násobením budeme pracovat se sčítáním. Nejprve se seznámíme s tím, co to jsou kompozice, rozklady a jejich různé typy. Seznámíme se s Ferrerovými diagramy, které představují jednoduchý, ale užitečný nástroj, jak si rozklady reprezentovat. Pentagonální věta zase přináší užitečné poznatky o počtu rozkladů. Ve druhé části si ukážeme základní metody pro práci s vytvořujícími funkcemi, a to nám umožní snadno vyřešit velké množství identit. Ke konci se opět vrátíme ke kombinatorickému přístupu a dokážeme Cohen–Remmelovu větu.

Pro začátek několik základních pojmů.

Definice. Mějme přirozené číslo n.

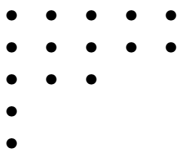
(i) *Kompozice* čísla n jsou výrazy $n = a_1 + a_2 + \cdots + a_r$, kde $a_1, \ldots, a_r$ jsou přirozená čísla. Jejich počet značíme $c(n)$.

(ii) Nechť $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_r$ jsou přirozená čísla. Pak $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_r)$ nazýváme *rozklad* a čísla λ_i jeho *části*. Pokud $\lambda_1 + \cdots + \lambda_r = n$, tak λ je rozklad čísla n. Často také píšeme $\lambda = (\lambda_1^{f_1}, \lambda_2^{f_2}, \ldots, \lambda_r^{f_r})$, kde exponent udává, kolikrát se v rozkladu daná část vyskytuje.

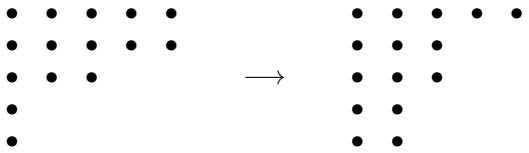
(iii) Označme $\mathcal{P}$ množinu všech rozkladů a $\mathcal{P}_n$ množinu všech rozkladů čísla n. Jejich počet značíme $p(n) = |\mathcal{P}_n|$.

Cvičení 1. Určete počet kompozic $c(n)$ a počet kompozic s právě k částmi $c(n, k)$.

Ferrerův diagram je vizualiazace rozkladu pomocí teček tak, že každý řádek obsahuje tolik teček jako jedna část rozkladu. Například $\lambda = (5^2, 3, 1^2)$ má Ferrerův diagram:



Definice. *Kamarádský rozklad* γ' je rozklad, který vznikne z rozkladu γ otočením Ferrerova diagramu podle diagonály. Například $\lambda = (5^2, 3, 1^2)$ má kamarádský rozklad $\lambda' = (5, 3^2, 2^2)$:



Cvičení 2. Počet rozkladů s maximálně k částmi je stejný jako počet rozkladů na části nepřesahující číslo k.

Cvičení 3. Nahlédněte, že počet rozkladů čísla n je roven počtu rozkladů čísla $2n$ na n částí.

Cvičení 4. Rozklad nazveme symetrický, pokud je sám svým kamarádským rozkladem. Uvědomte si, že symetrických rozkladů čísla n je stejně jako těch rozkladů čísla n, kde jsou jednotlivé části různé a současně liché.

Cvičení 5. Počet rozkladů čísla n, kde se mohou opakovat pouze části, které nejsou dělitelné 2^m, je stejný jako počet rozkladů čísla n, kde se každá část vyskytuje maximálně $\left(2^{m+1}-1\right)$-krát.

Cvičení 6. Počet rozkladů čísla n na po sobě jdoucí části (například $9 = 2{+}3{+}4 = 4+5 = 9$) je stejný jako počet lichých dělitelů čísla n.

Cvičení 7. Počet rozkladů čísla n s různými částmi je stejný jako počet rozkladů čísla n s lichými částmi.

Cvičení 8. Bijektivně ukažte, že počet rozkladů čísla n, které neobsahují druhou mocninu přirozeného čísla, je stejný jako počet rozkladů čísla n, ve kterých se každé číslo i vyskytuje nanejvýš $(i-1)$-krát.

Definice. *Pentagonální čísla* jsou čísla, která se dají zapsat ve tvaru $\frac{3m^2+m}{2}$ pro celé nenulové číslo m. Tedy jsou to postupně čísla (pro $m = -1, 1, \dots$):

$$1, 2, 5, 7, 12, 15, 22, 26, \dots$$

Věta. (Pentagonální) *Nechť $\omega(m) = (3m^2+m)/2$. Pak platí následující tři tvrzení:*

(1) $$\prod_{n=1}^{\infty}(1-x^n) = 1 + \sum_{m=1}^{\infty}(-1)^m\left(x^{\omega(m)} + x^{\omega(-m)}\right) = \sum_{m=-\infty}^{\infty}(-1)^m x^{\omega(m)}.$$

(2) *Nepentagonální číslo n má stejný počet rozkladů na sudý počet různých částí jako na lichý počet různých částí. Pro pentagonální číslo $n = \omega(\pm m)$ je rozdíl počtu rozkladů na sudý počet různých částí a počtu rozkladů na lichý počet různých částí rovný $(-1)^m$.*

(3) *Pro přirozené číslo n platí rekurence*

$$\begin{aligned} p(n) = {} & p(n-1) + p(n-2) - p(n-5) - p(n-7) + \\ & + p(n-12) + p(n-15) - \cdots, \end{aligned}$$

kde dodefinujeme $p(m) = 0$ pro $m < 0$ a $p(0) = 1$.

Definice. (Vytvořující funkce) Nechť $a_0, a_1, a_2, \dots$ je posloupnost přirozených čísel. Potom mocninná řada

$$f(x) = \sum_{n=0}^{\infty} a_n x^n,$$

kde $x \in \mathbb{C}$, se nazývá vytvořující funkcí posloupnosti $\{a_n\}_{n=0}^{\infty}$.

Tvrzení. *Nechť A je podmnožina přirozených čísel. Označme*

$$f(x) = \sum_{n=0}^{\infty} p_A(n) x^n \qquad \text{a} \qquad f_k(x) = \sum_{n=0}^{\infty} p_{A,k}(n) x^n,$$

kde $p_A(n)$ a $p_{A,k}(n)$ je postupně počet rozkladů čísla n na části z A a počet rozkladů čísla n na části z A, z nichž žádná se nevyskytuje více než k-krát. Pak

$$f(x) = \prod_{a \in A} \frac{1}{1 - x^a},$$

$$f_k(x) = \prod_{a \in A} (1 + x^a + \dots + x^{ka}) = \prod_{a \in A} \frac{1 - x^{(k+1)a}}{1 - x^a}.$$

Cvičení 9. Dokažte si cvičení 7, 8, 5a případně 2 pomocí vytvořujících funkcí.

Věta. (Sylvester) *Označme $A_k(n)$ počet rozkladů čísla n na liché části tak, že různých částí je právě k. Dále $B_k(n)$ označme počet rozkladů čísla n skládajících se z k úseků po sobě jdoucích částí. Pak $A_k(n) = B_k(n)$ pro každé k, n.*

Cvičení 10. Uvědomte si, že speciální případ této věty je cvičení číslo 6.

Věta. (Princip inkluze a exkluze) *Nechť $X_1, X_2, \dots, X_k$ jsou konečné množiny a všechny jsou podmnožinami množiny X. Pak platí*

$$\left| X \setminus \bigcup_{i=1}^{k} X_i \right| = |X| + \sum_{\emptyset \neq I \subseteq \{1,2,\dots,k\}} (-1)^{|I|} \left| \bigcap_{i \in I} X_i \right|.$$

Věta. (Cohen, Remmel) *Nechť $\Lambda = \{\lambda^1, \lambda^2, \dots\}$ a $\Gamma = \{\gamma^1, \gamma^2, \dots\}$ jsou (nekonečné) posloupnosti rozkladů takové, že pro každou konečnou podmnožinu I přirozených čísel platí*

$$\left| \bigcup_{i \in I} \lambda^i \right| = \left| \bigcup_{i \in I} \gamma^i \right|.$$

Pak pro každé přirozené číslo n je počet rozkladů čísla n neobsahujících žádný rozklad z Λ stejný jako počet rozkladů čísla n neobsahujících žádný rozklad z Γ.

Důsledek. (Glaisherova identita) *Počet rozkladů čísla n neobsahujících žádnou část, která je násobkem d, je stejný jako počet rozkladů čísla n, kde je každá část nejvýše $(d-1)$-krát.*

Důsledek. (Schurova identita) *Počet rozkladů čísla n, jejichž části dávají zbytky 1 a 5 po dělení šesti, je stejný jako počet rozkladů čísla n na různé části nedělitelné třemi.*

Návody

2. Navzájem popárujte kamarádské rozklady.

3. V rozkladu délky n snižte každý sčítanec o jedna.

4. Spojte tečky z i-tého řádku a i-tého sloupce symetrického rozkladu do jedné části nového rozkladu.

5. Opakovaně spojujte 2^{m+1} stejných částí ve dvě 2^m-krát větší části.

6. Dokažte, že počet rozkladů na lichý počet po sobě jdoucích částí je stejný jako počet lichých dělitelů čísla n menších než $\sqrt{2n}$.

7. Popárujte rozklady. Například $1+4+3+6 = 1+1+1+1+1+3+3+3$.

8. Nahrazujte v prvním typu rozkladů vždy k stejných čísel k za číslo k^2.

Literatura a zdroje

[1] Klazar, M.; *Introduction to Number Theory (lecture notes)*, 2006, *http://kam.mff.cuni.cz/~klazar/ln_utc.pdf*

[2] Hančl, J.; *Obecná enumerace číselných rozkladů*, 2011

[3] Andrews, G. E.; *The theory of partitions*, Cambridge University Press, 1998 (reprint originálu 1976)

[4] Mirek Olšák; *Kombinatorické (ne)počítání*, Sborník iKS, 2013, *http://iksko.org/files/sbornik2.pdf*

[5] Hirschhorn, M. D. a Hirschhorn, P. M.; *Partitions into Consecutive Parts*, Mathematics Magazine, 2003, Volume 76, Number 4, strany 306-308, *http://www.maa.org/sites/default/files/3004420056860.pdf.bannered.pdf*

[6] Bui, L.; *New Results in Partition Theory*, 1997

Cauchyho nerovnost

Martin Töpfer

Cauchy–Schwarz[1] (zkráceně CS) je po AG nerovnosti jednou z nejčastěji používaných nerovností. Ukážeme si několik jejích podob, které se hodí na různé druhy nerovností. Nejprve si ji ale dokážeme v jejím nejčastěji uváděném tvaru.

Věta. (Cauchyho–Schwarzova nerovnost) *Pro každé dvě n-tice* $u_1, u_2, \dots u_n \in \mathbb{R}$ a $v_1, v_2, \dots v_n \in \mathbb{R}$ *platí*

$$\big(u_1^2 + u_2^2 + \cdots + u_n^2\big)\big(v_1^2 + v_2^2 + \cdots + v_n^2\big) \geq (u_1v_1 + u_2v_2 + \cdots + u_nv_n)^2,$$

přičemž rovnost nastává právě tehdy, když existuje $\lambda \in \mathbb{R}$ *takové, že* $u_1 = \lambda v_1$, $u_2 = \lambda v_2, \dots, u_n = \lambda v_n$.

Klasický CS

Příklad 1. Buď ABC trojúhelník o stranách a, b, c a KLM trojúhelník o stranách délek k, l, m. Ukažte, že

$$(a^2 + b^2 + c^2)(k^2 + l^2 + m^2) = (ak + bl + cm)^2,$$

právě když $\triangle ABC \sim \triangle KLM$.

Příklad 2. Dokažte následující nerovnosti pro kladná čísla a_i, $i = 1, \dots, n \in \mathbb{N}$:

(1) $(a_1 + a_2 + \cdots + a_n)\left(\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}\right) \geq n^2$,

(2) $n\big(a_1^2 + a_2^2 + \cdots + a_n^2\big) \geq (a_1 + a_2 + \cdots + a_n)^2$.

Příklad 3. Dokažte nerovnost pro $x, y, z \in \mathbb{R}^+$:

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

[1] Krátce Cauchyho nerovnost, dlouze občas Cauchyho–Schwarzova–Bunjakowského nerovnost.

CS a zlomky

Tvrzení. (CS zlomkobijec) *Je-li* $n \in \mathbb{N}$ *a* $a_1, a_2, \ldots, a_n \in \mathbb{R}^+$, $b_1, b_2, \ldots, b_n \in \mathbb{R}^+$, *pak platí*

$$\left(\frac{a_1}{b_1} + \frac{a_2}{b_2} + \cdots + \frac{a_n}{b_n}\right) \geq \frac{\left(\sqrt{a_1} + \sqrt{a_2} + \cdots + \sqrt{a_n}\right)^2}{b_1 + b_2 + \cdots + b_n}.$$

Příklad 4. Pro $a, b, c \in \mathbb{R}^+$ dokažte

$$\frac{2}{a+b} + \frac{2}{b+c} + \frac{2}{c+a} \geq \frac{9}{a+b+c}.$$

Příklad 5. Pro $a, b, x, y, z \in \mathbb{R}^+$ dokažte

$$\frac{x}{ay+bz} + \frac{y}{az+bx} + \frac{z}{ax+by} \geq \frac{3}{a+b}.$$

Příklad 6. (Nesbittova nerovnost) Pro $a, b, c \in \mathbb{R}^+$ dokažte následující nerovnost

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

Příklad 7. Ukaž, že pro kladná a, b, c splňující $a + b + c = 1$ platí

$$\frac{a}{1+bc} + \frac{b}{1+ca} + \frac{c}{1+ab} \geq \frac{9}{10}.$$

(MKS 2009/2010, 1. seriálová série)

Příklad 8. 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 1995)

CS a odmocniny

Tvrzení. *Buď* n *přirozené číslo a* $a_1, a_2, \ldots, a_n$, $b_1, b_2, \ldots, b_n$ *čísla kladná. Pak platí*

$$\sqrt{a_1 b_1} + \sqrt{a_2 b_2} + \cdots + \sqrt{a_n b_n} \leq \sqrt{(a_1 + a_2 + \cdots + a_n)(b_1 + b_2 + \cdots + b_n)}.$$

Příklad 9. Dokažte následující nerovnosti pro $a, b, c \in \mathbb{R}^+$:

(1) $\sqrt{a^3} + \sqrt{b^3} + \sqrt{c^3} \leq \sqrt{(a+b+c)(a^2+b^2+c^2)}$,

(2) $\sqrt{a^3} + \sqrt{b^3} + \sqrt{c^3} \leq \sqrt{3(a^3+b^3+c^3)}$,

(3) $a\sqrt{b} + b\sqrt{c} + c\sqrt{a} \leq \sqrt{(a+b+c)(a^2+b^2+c^2)}$.

Příklad 10. Kladná čísla $x, y, z \geq 1$ splňují $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 2$. Dokažte, že

$$\sqrt{x-1} + \sqrt{y-1} + \sqrt{z-1} \leq \sqrt{x+y+z}.$$

(Iránská MO 1998)

Příklad 11. Pro kladná čísla a, b, c dokažte nerovnost

$$\frac{a}{\sqrt{a^2+8bc}} + \frac{b}{\sqrt{b^2+8ac}} + \frac{c}{\sqrt{c^2+8ab}} \geq 1.$$

(IMO 2001)

Příklad 12. Pro kladná čísla a, b, c, x, y, z taková, že $x^2 + y^2 + z^2 = 1$, dokažte

$$\sum_{cyc} \sqrt{a^2x^2 + b^2y^2 + c^2z^2} \geq a + b + c.$$

Literatura a zdroje

Přednáška vychází z příspěvku Alči Skálové z Oldřichova. Je doplněna některými příklady z *Mathematical Olympiad Treasures* (Titu Andreescu, Bogdan Enescu) a obsahuje upravený výběr lehčích příkladů z textu *Zdolávání nerovností* (Michal Rolínek, Pavel Šalom).

Ramseyova věta

Martin Töpfer

„Úplný nepořádek není možný.“ Tak by se dala shrnout všechna tvrzení, která si tu předvedeme. Abychom si zjednodušili představu našeho světa, budeme se pohybovat ve světě grafů.

Příklad. (Motivační) Mezi šesti lidmi jsou alespoň tři, kteří se navzájem znají, nebo alespoň tři, kteří se neznají.

Tvrzení. (Dirichletův princip) *Nechť k, n jsou přirozená čísla. Pak kdykoli umístíme $kn + 1$ předmětů do n přihrádek, tak alespoň v jedné přihrádce bude alespoň $k + 1$ předmětů.*

Grafové pojmy

Definice. *Graf* (V, E) je dvojice množiny vrcholů V a množiny hran E.

Definice. *Úplný graf* K_n je graf na vrcholech 1, 2, ..., n, který obsahuje všechny hrany.

Definice. *(Hranové) obarvení grafu* G pomocí k barev je funkce f, která každé hraně přiřadí jednu barvu. Matematicky bychom řekli, že f je zobrazení z E do $\{1, 2, \ldots, k\}$.

Definice. *(Indukovaný) podgraf* grafu (V, E) je takový graf, že jeho vrcholy V' jsou některé vrcholy z V a jeho hrany jsou všechny hrany původního grafu, které vedou mezi vrcholy z V'.

Definice. *Klika* v grafu je taková množina jeho vrcholů, že každé dva z nich jsou spojeny hranou.

Definice. *Nezávislá množina* v grafu je taková množina jeho vrcholů, že žádné dva z nich nejsou spojeny hranou.

A jdeme na to!

Věta. (Ramseyova věta – jednoduchá verze) *Pro každá n, m přirozená čísla existuje $N \in \mathbb{N}$ tak, že všechny grafy na N vrcholech obsahují buď kliku velikosti n nebo nezávislou množinu velikosti m. Nejmenší takové číslo N nazvěme Ramseyovým číslem $R(n, m)$.*

O velikosti Ramseyových čísel se toho obecně moc neví a neexistuje ani žádný příliš těsný odhad na jejich velikost. Například o hodnotě $R(5, 5)$ víme, že je mezi 43 a 49, ale ani v době výkonných počítačů přesnou hodnotu neznáme. My si ukážeme následující odhad na jejich velikost:

$$2^{\frac{k}{2}} < R(k, k) \leq \binom{2k-2}{k-1}.$$

Nyní si uvědomíme, že místo rozhodování je/není hrana bychom mohli úplný graf obarvovat pomocí dvou barev. Pak se už přirozeně nabízí zobecnění této věty.

Definice. Graf na vrcholech V je *jednobarevný* v obarvení f, pokud všechny hrany mají v f stejnou barvu.

Věta. (Ramseyova věta – vícebarevná verze) *Pro libovolná $b, n \in \mathbb{N}$ existuje $N \in \mathbb{N}$ tak, že když $|V| = N$ a množina barev $|B| = b$, tak pro každé obarvení $f : \binom{V}{2} \to B$ existuje jednobarevný úplný graf na n vrcholech.*

Věta. (Schurova věta) *Pro libovolný počet barev $b \in \mathbb{N}$ existuje $N \in \mathbb{N}$ tak, že když obarvíme čísla $\{1, 2, \ldots, N\}$ pomocí b barev, pak budou existovat tři čísla x, y, z stejné barvy splňující $x + y = z$.*

Věta. (van der Waerdenova věta) *Pro libovolný počet barev $b \in \mathbb{N}$ a číslo l existuje $N \in \mathbb{N}$ tak, že když obarvíme čísla $\{1, 2, \ldots, N\}$ pomocí b barev, pak bude existovat jednobarevná aritmetická posloupnost délky alespoň l.*

Věta. (Ramseyova věta – nekonečná) *Pro libovolné $b \in \mathbb{N}$ a množinu barev $|B| = b$ platí, že pro každé obarvení $f : \binom{V}{2} \to B$ existuje v nekonečném spočetném grafu jednobarevný úplný spočetný graf na n vrcholech.*

Konečně příklady

Příklad. Ukažte, že pro každé $m \geq 2$ existuje p_0 tak, že pro všechna prvočísla $p > p_0$ má kongruence

$$x_m + y_m \equiv z_m \pmod{p}$$

řešení.

Příklad. Spolupráce mezi sedmnácti vědci vypadá tak, že každí dva komunikují o jednom ze tří témat. Ukažte, že existují tři vědci, kteří se navzájem baví o stejném tématu.

Příklad. Mezinárodní společnost má celkem 1978 členů ze šesti zemí, kteří jsou očíslováni čísly $1, 2, \ldots, 1978$. Ukažte, že existuje člen, jehož číslo je součtem čísel dvou jeho krajanů nebo je dvakrát větší než číslo nějakého jeho krajana.

(IMO 1978)

Zdroje a literatura

[1] přednáška Kombinatorika a grafy II na MFF UK (Vít Jelínek)
[2] Mareš, M.; *Ramseyovy věty*, *http://mj.ucw.cz/papers/ramsey.pdf*
[3] Taylor, G.; *Ramsey Theory*,
http://web.mat.bham.ac.uk/D.Kuehn/RamseyGreg.pdf
[4] Hliněný, P.; *Graph Theory*, lecture 12,
http://www.fi.muni.cz/~hlineny/Vyuka/GT/Grafy-lect-en-12.pdf

Od grupoidů ke grupám

Martina Vaváčková

Grupoid je množina, na níž je zavedena jedna binární operace, tedy zobrazení, které každé dvojici prvků přiřazuje nějaký třetí prvek. Podle vlastností této operace lze grupoidy dále dělit – základní dělení si na přednášce představíme a osaháme.

Ačkoliv se nám (obzvlášť některé) grupoidy mohou na první pohled zdát podivné, uvidíme, že jsou vlastně docela přirozené a narážíme na ně i v běžném životě.

Formální definice a vlastnosti

Definice. (Grupoid) Množina G spolu s binární operací $\cdot : G \times G \to G$ se nazývá *grupoid* a značí se $(G, \cdot)$.

Cvičení. Určete, zda je a) $(\mathbb{N}, +)$, b) $(\mathbb{N}, -)$ grupoid.

Cvičení. Kolik existuje grupoidů na množině $\{1, 2\}$?

Má-li množina G konečně mnoho prvků, lze na ní zadat binární operaci pomocí tabulky výsledků – tzv. *Cayleyho tabulky.*

Příklad. Uvažujme množinu $\{0, 1, 2\}$ s operací sčítání modulo 3. Příslušná Cayleyho tabulka je:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Definice. (Některé základní vlastnosti grupoidů)

(i) Grupoid $(G, \cdot)$ je *asociativní*, jestliže pro všechna $a, b, c \in G$ platí $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(ii) Grupoid $(G, \cdot)$ má *latinskou vlastnost*, jestliže pro všechna $a, b \in G$ existuje právě jedno x takové, že $a \cdot x = b$, a právě jedno y takové, že $y \cdot a = b$. Ekvivalentně, Cayleho tabulka operace $\cdot$ tvoří latinský čtverec.

(iii) Grupoid $(G, \cdot)$ má *jednotku*, jestliže existuje $e \in G$ takové, že pro všechna $a \in G$ platí $a \cdot e = e \cdot a = a$.

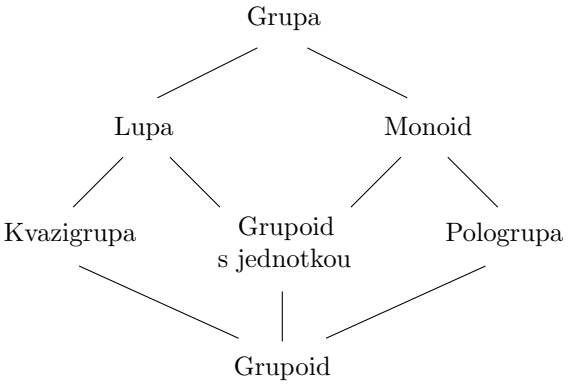
(iv) Grupoid $(G, \cdot)$ je *komutativní*, jestliže pro všechna $a, b, c \in G$ platí $a \cdot b = b \cdot a$.

(v) Prvek $a \in G$ je *idempotentní*, jestliže $a \cdot a = a$. Grupoid $(G, \cdot)$ je *idempotentní*, jestliže pro všechna $a \in G$ platí $a \cdot a = a$.

Cvičení. Ukažte, že každý grupoid má nejvýše jednu jednotku.

Hierarchie grupoidů

Asociativní grupoid se nazývá *pologrupa*. Pokud má navíc jednotku, jedná se o *monoid*. Grupoid s latinskou vlastností je *kvazigrupa*, a pokud má jednotku, nazývá se *lupa*. Asociativní grupoid s latinskou vlastností a jednotkou je *grupa*.[1]



Motivační příklady

Příklad. (Maximum) Množina $\mathbb{R}$ spolu s operací maxima, která každé dvojici čísel $a, b \in \mathbb{R}$ přiřadí to větší z nich, je komutativní idempotentní pologrupa.

Příklad. (Slova) Množina všech konečných posloupností znaků anglické abecedy spolu s operací „zřetězení“ je monoid. Jednotkou je prázdná posloupnost.

Příklad. (Relativistické sčítání rychlostí) Množina všech reálných čísel z intervalu $(-c, c)$ spolu s operací $\oplus$ definovanou jako

$$u \oplus v = \frac{u + v}{1 + \frac{uv}{c^2}}$$

je komutativní lupa s jednotkou 0.

Příklad. (Aritmetický průměr) Množina $\mathbb{R}$ spolu s operací $\circ$ definovanou jako $a \circ b = \frac{a+b}{2}$ tvoří komutativní idempotentní kvazigrupu.

[1] Obvykle se grupa definuje jako asociativní grupoid s jednotkou a inverzními prvky, nicméně tato definice je ekvivalentní a pro naše účely výhodnější.

Cvičení a příklady

Cvičení 1. Ukažte, že kdykoliv G je kvazigrupa a pro $a, b, c \in G$ platí $a \cdot b = a \cdot c$ nebo $b \cdot a = c \cdot a$, pak $b = c$.

Cvičení 2. Nechť G je asociativní grupoid s latinskou vlastností. Ukažte, že G je grupa.

Cvičení 3. Nechť G je grupa. Ukažte, že pak ke každému $x \in G$ existuje prvek x^{-1} takový, že $x \cdot x^{-1} = x^{-1} \cdot x = e$ (inverzní prvek).

Cvičení 4. Ukažte, že každá idempotentní grupa je už nutně jednoprvková.

V následujících příkladech určete, o jaké struktury se jedná.

Příklad 1. Množina a) $\mathbb{Z}$, b) $\mathbb{Z}\backslash\{0\}$ s násobením.

Příklad 2. Množina $\{e, x, y\}$ spolu s operací $\cdot$ danou následující tabulkou:

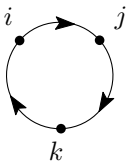
$\cdot$	e	x	y
e	e	x	y
x	y	e	x
y	x	y	e

Příklad 3. Permutace na množině $\{1, 2, 3, 4\}$ se skládáním.

Příklad 4. Komplexní čísla a jejich zobecnění – kvaterniony, oktoniony:

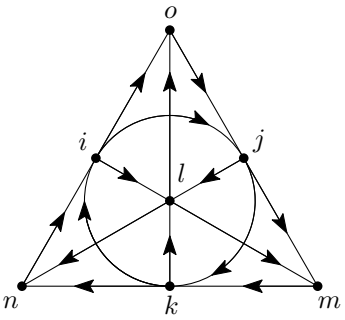
(1) Množina $\{\pm 1, \pm i\}$, kde i je komplexní jednotka splňující $i^2 = -1$, spolu s násobením komplexních čísel.

(2) Množina $\{\pm 1, \pm i, \pm j, \pm k\}$, kde i, j, k jsou komplexní jednotky splňující $i^2 = j^2 = k^2 = -1$, které se mezi sebou násobí dle následujícího schématu:



Kdykoliv $a \neq b$ a vede šipka od a k b, je $a \cdot b = c$ a $b \cdot a = -c$, kde c je třetí jednotka.

(3) Množina $\{\pm 1, \pm i, \pm j, \pm k, \pm l, \pm m, \pm n, \pm o\}$, kde i, j, k, l, m, n, o jsou komplexní jednotky splňující $i^2 = \cdots = o^2 = -1$, které se mezi sebou násobí dle následujícího schématu:



Kdykoliv $a \neq b$ a vede šipka od a k b, je $a \cdot b = c$ a $b \cdot a = -c$, kde c je třetí jednotka na úsečce spojující a a b.

Příklad 5. Množina funkcí $\alpha: X \to X$ s operací skládání $\circ$, definovanou jako $\alpha \circ \beta(x) = \alpha(\beta(x))$, $x \in X$.

Příklad 6. *Steinerův systém trojic* je množina X spolu se souborem neuspořádaných trojic T jejích prvků takovým, že pro každé $x, y \in X$ $(x \neq y)$ existuje právě jedno $z \in X$ splňující $\{x, y, z\} \in T$. Na X definujme operaci $\cdot$ následovně:

$$x \cdot y = \begin{cases} z, & \text{pokud } x \neq y \text{ a } \{x, y, z\} \in T, \\ x, & \text{pokud } x = y. \end{cases}$$

Příklad 7. Množina $\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix}; a, b, c, d \in \mathbb{Z} \right\}$ s maticovým násobením.

Příklad 8. Soubor podmnožin dané množiny s operací sjednocení.

Zdroje

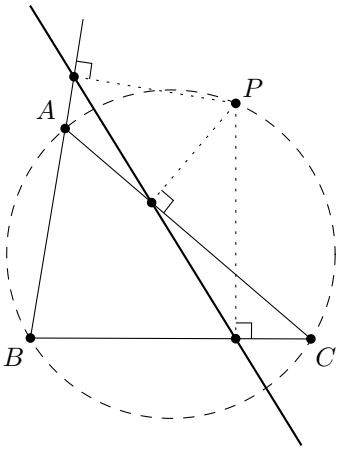
Čerpala jsem především z přednášky *Binární systémy* Davida Stanovského na MFF UK, kterému tímto děkuji.

Simsonova přímka

Martina Vaváčková

Simsonova přímka je užitečným nástrojem k řešení některých geometrických úloh, které se objevují v olympiádách a dalších soutěžích. Je tedy výhodné o ní vědět a naučit se ji používat – přesně to bude obsahem přednášky.

Věta. (Simsonova přímka) *Mějme trojúhelník ABC a bod P. Pak paty kolmic z bodu P na přímky BC, CA a AB leží na jedné přímce, právě když bod P leží na kružnici opsané trojúhelníku ABC. Tato přímka se nazývá Simsonova přímka bodu P vzhledem k trojúhelníku ABC.*



Užitečné vlastnosti

(a) Simsonovou přímkou vrcholu trojúhelníka je výška na protější stranu.
(b) Simsonovou přímkou obrazu vrcholu podle středu kružnice opsané je protější strana.
(c) Je-li S střed kružnice opsané, pak Simsonovy přímky bodů P a Q svírají úhel $\frac{1}{2}|\sphericalangle PSQ|$.
(d) Je-li H ortocentrum, pak Simsonova přímka bodu P půlí úsečku PH.

(e) Mají-li dva trojúhelníky společnou kružnici opsanou, pak úhel Simsonových přímek bodu P vzhledem k těmto trojúhelníkům nezávisí na volbě bodu P.

Cvičení. Ukažte, že Simsonovy přímky protějších bodů na kružnici opsané danému trojúhelníku se protínají na kružnici devíti bodů tohoto trojúhelníka.

Cvičení. Ukažte, že obrazy přímky procházející ortocentrem podle stran trojúhelníka se protínají v jednom bodě na kružnici opsané.

Sbírka příkladů

Příklad 1. V trojúhelníku ABC protne výška z vrcholu A kružnici opsanou podruhé v bodě P. Ukažte, že Simsonova přímka bodu P je rovnoběžná s tečnou ke kružnici opsané v bodě A.

Příklad 2. Mějme trojúhelník ABC a přímku, která protíná strany BC, AC a AB postupně v bodech R, S a T. Označme P průsečík kružnic opsaných trojúhelníkům ABC a RSC. Ukažte, že čtyřúhelník $APST$ je tětivový.

Příklad 3. Na přímce jsou dány body A, B, C a mimo ni bod P. Dokažte, že bod P leží na kružnici opsané trojúhelníku tvořenému středy kružnic opsaných trojúhelníkům ABP, BCP, ACP.

Příklad 4. V trojúhelníku ABC protíná osa úhlu BAC protější stranu v bodě D. Označme P, Q paty kolmic vedených bodem D na strany AB, AC. Kolmice na BC z bodu D protne PQ v bodě X. Ukažte, že X leží na těžnici z bodu A.

Příklad 5. Konvexní pětiúhelník $AXYZB$ je vepsán do půlkružnice se středem O a průměrem AB. Označme P, Q, R, S postupně paty kolmic z bodu Y na přímky AX, BX, AZ, BZ. Dokažte, že velikost ostrého úhlu, který svírají přímky PQ a RS, je rovna $\frac{1}{2}|\sphericalangle XOZ|$. (USAMO 2010)

Příklad 6. Nechť kružnice vepsaná trojúhelníku ABC má střed I a protíná strany BC, CA, AB postupně v bodech D, E, F. Nechť dále M je střed strany BC. Pak se přímky EF, DI a AM protínají v jednom bodě.

Příklad 7. Na kružnici opsané trojúhelníku ABC leží body P, Q tak, aby $PQ \parallel BC$. Paty kolmic z bodů P a Q na AB, respektive AC označme postupně X_1, Y_1, respektive X_2, Y_2. Dokažte, že přímky X_1X_2 a Y_1Y_2 se protínají na výšce na stranu BC.

Příklad 8. Uvažujme pět bodů A, B, C, D, E takových, že $ABCD$ je rovnoběžník a $BCED$ je tětivový čtyřúhelník. Přímka l prochází bodem A, protíná úsečku DC v jejím vnitřním bodě F a přímku BC v bodě G. Platí-li $|EF| = |EG| = |EC|$, ukažte, že l je osou úhlu DAB. (IMO 2007)

Příklad 9. Nechť $ABCD$ je tečnový čtyřúhelník a g je přímka procházející bodem A, která protíná stranu BC v bodě M a stranu CD v bodě N. Označme I_1, I_2, I_3 středy kružnic vepsaných trojúhelníkům ABM, MNC a NDA. Ukažte, že ortocentrum trojúhelníka $I_1I_2I_3$ leží na přímce g. (IMO Shortlist 2009)

Příklad 10. Označme H ortocentrum ostroúhlého trojúhelníka ABC a k jeho kružnici opsanou. Přímka procházející bodem H protne kratší oblouky AC, BC kružnice k postupně v bodech M, P. Rovnoběžka se Simsonovou přímkou bodu P vzhledem k trojúhelníku ABC vedená bodem M protne k v bodě K, rovnoběžka s BC vedená bodem P protne k podruhé v bodě Q. Označme J průsečík BC a KQ. Dokažte, že trojúhelník KJM je rovnoramenný. (China TST 2011)

Návody

1. Vyúhlete pomocí obvodového a úsekového úhlu.

2. Bodem P veďte kolmice na strany trojúhelníka ABC a přímku ST.

3. Interpretujte středy úseček AP, BP, CP jako paty kolmic.

4. Spusťte kolmici ze středu kratšího oblouku BC a použijte stejnolehlost.

5. Všimněte si, že PQ a RS se protínají na AB.

6. Za pomoci Simsonovy věty ukažte, že body A, M a průsečík DI a EF leží na jedné přímce.

7. Dokreslete kolmice z P, Q na BC a najděte rovnoběžníky.

8. Uvažte Simsonovu přímku bodu E vzhledem k trojúhelníku BCD a vyúhlete.

9. Využijte vlastnost (d) Simsonovy přímky bodu C vzhledem k trojúhelníku $I_1I_2I_3$.

10. Označte $S = MP \cap BC$ a uvědomte si, že stačí, aby $KSJM$ byl tětivový.

Literatura a zdroje

[1] Posamentier, A. a Salkin, C.; *Challenging Problems in Geometry*
[2] Altshiller-Court, N.; *An Introduction to the Modern Geometry of the Triangle and the Circle*
[3] *www.artofproblemsolving.com*

Na závěr bych chtěla poděkovat Pepovi Tkadlecovi, z jehož příspěvku jsem převzala část úloh.

Obsah