Meziměstí

Sborník, jaro 2017

Tonda Češík
Anička Doležalová
David Hruška
Bára Kociánová
Honza Krejčí
Jakub Löwit
Viki Němeček
Marian Poljak
Martin Sýkora
Lucien Šíma
Štěpán Šimsa
Rado van Švarc
Martin Töpfer

Autoři: Tonda Češík, Anička Doležalová, David Hruška, Bára Kociánová, Honza Krejčí, Jakub Löwit, Viki Němeček, Marian Poljak, Martin Sýkora, Lucien Šíma, Štěpán Šimsa, Rado van Švarc, Martin Töpfer
Editoři: Tonda Češík, Viki Němeček
vydání první, náklad 45 výtisků
duben 2017
Díky za pomoc všem, kterým je za co děkovat.

Nekonečně malá čísla

Tonda Češík

Abstrakt. Ukážeme si tzv. nestandardní model reálných čísel. Ten umožňuje mluvit o nekonečně malých a nekonečně velkých číslech, pomocí kterých lze definovat pojmy jako limita a spojitost přímočařeji a intuitivněji. Standardně se tento model nepoužívá, protože ačkoli je v jistých pohledech intuitivní, může svádět k nekorektnímu zacházení. Tomuto nestandardnímu modelu se říká *hyperreálná čísla*.

Pokud ses již setkal(a) např. s definicí spojitosti funkce, možná Tě napadla následující myšlenka: „Vždyť jde vlastně jen o to, že když jsme blízko bodu a, tak funkční hodnota je blízko funkční hodnotě v a. Není tedy ta definice *Pro každé ε existuje δ atd.* zbytečně kostrbatá? Nešlo by to říct nějak jednodušeji?“ Odpověď je, že šlo, ale člověk si musí dávat pozor.

Trocha historie

V dobách počátku infinitezimálního počtu, tedy za dob Newtona a Leibnize, se zaujímal vcelku intuitivní přístup k problematice: *Když chci být hodně blízko, tak prostě budu nekonečně blízko.* Od začátku však tento přístup vypadal trochu podezřele. Časem si matematici uvědomili, že existenci *infinitezimálních veličin*[1], nemají nijak logicky odůvodněnou. Proto se namísto toho začala rozvíjet moderní teorie využívající epsilon-delta definice, a na tomto základu se matematická analýza staví dodnes. Od používání nekonečně malých čísel se tak na dlouhou dobu upustilo a byly považovány za nefungující slepou uličku. V šedesátých letech minulého století si však Abraham Robinson uvědomil, že nekonečně malá čísla vskutku lze zavést rigorózně. Dal tak vzniknout novému oboru pod názvem *Nestandardní analýza.*

Jdeme na to

Základní myšlenkou je, že začneme s nám známým *standardním* univerzem $\mathcal{U}$, obsahujícím reálná čísla $\mathbb{R}$, množiny v $\mathbb{R}$, funkce a relace v $\mathbb{R}$. Toto univerzum obohatíme o nekonečně malá a nekonečně velká čísla tím, že ho rozšíříme na univerzum $\mathcal{U}'$ pomocí operace $^*\colon \mathcal{U} \to \mathcal{U}'$, přiřazující objektu $\alpha \in \mathcal{U}$ odpovídající objekt $^*\alpha \in \mathcal{U}'$. Zvětšit ho pochopitelně nechceme nějak libovolně, ale tak, aby se zachovaly jeho

[1] Neboli nekonečně malých čísel.

původní vlastnosti, a tedy platila stejná tvrzení. To nám zařídí Princip transferu, ale abychom ho mohli formulovat, potřebujeme nejprve (pro naše potřeby ne úplně formálně) říci, co vlastně myslíme tím „tvrzením“.

Definice. *Formule* je konečný syntakticky korektní zápis tvořící logický celek v tom smyslu, že je možné uvažovat o jeho pravdivosti. Tedy je možné jednotlivé formule spojovat logickými spojkami. Formule může obsahovat:

(1) konstanty (označující objekty z $\mathcal{U}$),
(2) logické operátory (& , $\vee$, $\Rightarrow$, $=$, $\ldots$),
(3) množinové symboly $\in$, $\mathcal{P}$,
(4) proměnné (zastupující objekty v $\mathcal{U}$),
(5) kvantifikátory, pro naše účely výlučně ve tvaru $(\forall x \in \tau)$ nebo $(\exists x \in \tau)$, kde τ je konstanta nebo proměnná.

Sentence je formule, kde jsou všechny proměnné vázány kvantifikátory.

Příklad. Zápis $1+1$ není formule. Například $x = 5$ či $(\exists z \in \mathbb{R})(w \cdot z = 7)$ jsou formule, ale ne sentence. Sentence jsou například $1 + 1 = 2$ či $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x + y = 0)$.

Za sentence můžeme pokládat i věty v běžném jazyce, pokud víme, že je lze přepsat do požadovaného tvaru. Takže například větu „Každá konečná množina reálných čísel má minimum.“ lze považovat za sentenci.

Definice. Pro formuli φ definujeme formuli ${}^*\varphi$ tak, že v ní každou konstantu α nahradíme ${}^*\alpha$. Vše ostatní zůstává.

Axiom. (Princip transferu) *Sentence φ platí v $\mathcal{U}$, právě když sentence ${}^*\varphi$ platí v $\mathcal{U}'$.*

Příklad. Použijeme-li Princip transferu na dvě sentence platné v $\mathcal{U}$, dostaneme tak sentence platné v $\mathcal{U}'$:

$$\begin{aligned}
\varphi\colon &\quad (\forall x \in \mathbb{R})(\forall y \in \mathbb{R})(x + y = y + x),\\
\text{Transfer} \to {}^*\varphi\colon &\quad (\forall x \in {}^*\mathbb{R})(\forall y \in {}^*\mathbb{R})(x \,{}^*\!+ y = y \,{}^*\!+ x).\\
\psi\colon &\quad (\forall x \in \mathbb{R})(x \neq 0 \Rightarrow (\exists y \in \mathbb{R})(x \cdot y = 1)),\\
\text{Transfer} \to {}^*\psi\colon &\quad (\forall x \in {}^*\mathbb{R})(x \neq {}^*0 \Rightarrow (\exists y \in {}^*\mathbb{R})(x \,{}^*\!\cdot y = {}^*1)).
\end{aligned}$$

Tímto axiomem jsme zařídili, že rozšíření $\mathcal{U}'$ neporuší vlastnosti $\mathcal{U}$. Jak je vidět v příkladu, hvězdičkování všeho může vypadat trochu krkolomně, a tak přijmeme úmluvu, že hvězdičku budeme vynechávat u konstant z $\mathbb{R}$, funkcí a relací na $\mathbb{R}$. Tedy například budeme psát 1 místo ^{*1}, sin místo ${}^*\sin$, $<$ místo ${}^*<$, ale hvězdičku u ${}^*\mathbb{R}$ pochopitelně psát budeme. V tomto smyslu tedy můžeme uvažovat $\mathbb{R} \subset {}^*\mathbb{R}$.

Zatím jsme ale vůbec nezaručili, že nám operace * něco přidá. To zařídíme druhým axiomem, díky kterému nám * každou nekonečnou množinu zvětší.

Axiom. (Princip rozepnutí) *Pro každou nekonečnou množinu A v $\mathcal{U}$ platí $A \subsetneq {}^*A$.*

Množinu ${}^*\mathbb{R}$ budeme nazývat množinou *hyperreálných čísel*, množina ${}^*\mathbb{N}$ je množina *hyperpřirozených čísel.*

Důsledek. *Existují nekonečně malá a nekonečně velká hyperreálná čísla.*

Definice. Číslo $x \in {}^*\mathbb{R}$ se nazve

(1) *nekonečně malé*, pokud pro každé standardní kladné reálné ε (tj. $\varepsilon \in \mathbb{R}_+$) platí $|x| < \varepsilon$,
(2) *omezené*, pokud existuje $C \in \mathbb{R}_+$ takové, že $|x| \leq C$,
(3) *nekonečně velké*, pokud $|x| > C$ pro každé $C \in \mathbb{R}_+$.

Řekneme, že x je *nekonečně blízko* k y, pokud $x - y$ je nekonečně malé. Zapisujeme $x \approx y$.

Tvrzení. (vlastnosti $\approx$) *Pro hyperreálná čísla $a, b, c, d \in {}^*\mathbb{R}$ platí:*

(1) $a \approx b \ \& \ b \approx c \Rightarrow a \approx c$,
(2) $a \approx c \ \& \ b \approx d \Rightarrow a + b \approx c + d$,
(3) $a \approx 0 \ \&$ *b je omezené* $\Rightarrow a \cdot b \approx 0$.

Trocha nestandardní analýzy

Definice. Pro omezené hyperčíslo $x \in {}^*\mathbb{R}$ definujeme *standardní část* $\operatorname{st} x = x_0$, kde $x_0 \in \mathbb{R}$ je to jediné (standardní) reálné číslo splňující $x \approx x_0$. (Takové číslo existuje, protože reálná čísla jsou *úplná*.)

Definice. Řekneme, že posloupnost relaných čísel $(a_n)_{n=1}^{\infty}$ má *limitu* $a \in \mathbb{R}$, pokud pro všechny nekonečně velké indexy N platí $a_N \approx a$.

Definice. Říkáme, že funkce $f\colon \mathbb{R} \to \mathbb{R}$ je *spojitá*, pokud pro libovolné $x \in \mathbb{R}$ a $y \in {}^*\mathbb{R}$ takové, že $y \approx x$, platí i $f(y) \approx f(x)$.

Definice. Říkáme, že funkce $f\colon \mathbb{R} \to \mathbb{R}$ je *stejnoměrně spojitá*, pokud pro libovolnou dvojici reálných hyperčísel $x, y \in {}^*\mathbb{R}$ platí $x \approx y \Rightarrow f(x) \approx f(y)$.

Úloha. (Bolzanova věta) Spojitá funkce f někde nabývá záporné hodnoty, někde jinde kladné. Dokažte, že pak někde nabývá nuly.

Úloha. (Weierstrassova věta) Dokažte, že spojitá funkce na uzavřeném intervalu nabývá maximální hodnoty.

Úloha. Jsou dány dvě funkce $f, g\colon \mathbb{R}^2 \to \mathbb{R}$ splňující pro libovolné reálné x z intervalu $\langle 0, 1\rangle$

$$f(x, 0) < 0, \quad g(0, x) < 0, \quad f(x, 1) > 0, \quad g(1, x) > 0.$$

Dokažte, že pak existují reálná čísla x, y taková, že $f(x, y) = g(x, y) = 0$.

Konstrukce hyperreálných čísel

Doposud jsme zaujímali axiomatický přístup – tedy zavedli jsme si dva axiomy, které mají hyperreálná čísla splňovat. Je ale možné k tomu přistoupit i konstrukčně a hyperreálná čísla si „vyrobit“ z reálných. Myšlenka je následující: Nekonečně malé nenulové číslo budeme reprezentovat posloupností nenulových reálných čísel blížících se k nule.

Tedy hyperreálné číslo a pro nás bude posloupnost $(a_i)_{i=1}^{\infty}$, kde $a_i \in \mathbb{R}$. Operace budeme definovat po složkách, tedy

$$a + b = (a_1, a_2, a_3, \dots) + (b_1, b_2, b_3, \dots) = (a_1 + b_1, a_2 + b_2, a_3 + b_3, \dots)$$

a podobně pro násobení. Reálná čísla ztotožníme s konstantními posloupnostmi, tedy $x \in \mathbb{R}$ ztotožníme s posloupností $(x, x, x, \dots)$.

Aby tato myšlenka fungovala, je potřeba se ještě zbavit technického úskalí, kvůli kterému se posloupnosti nechovají jako reálná čísla (není splněn princip transferu). Například, v reálných číslech platí: pro $x \neq 0$, $y \neq 0$ je $x \cdot y \neq 0$. To pro naše posloupnosti neplatí, protože

$$(1, 0, 1, 0, \dots) \cdot (0, 1, 0, 1, \dots) = (0, 0, 0, 0, \dots).$$

Také není vůbec jasné, jak posloupnosti porovnávat, tedy jak rozhodnout, která z dvou posloupností je větší. Problém vyřešíme tak, že nás budou zajímat prvky jen na některých pozicích. Přesněji řečeno, budou nás zajímat prvky na velké množině indexů. Proto všechny množiny přirozených čísel rozdělíme na *malé* a *velké* tak, aby platilo následující.

(1) Každá jednoprvková množina $\{n\}$ je malá, prázdná množina je malá.
(2) Pokud $A, B \subset \mathbb{N}$ jsou obě velké, pak $A \cap B$ je velká.
(3) Pokud $A \subset \mathbb{N}$ je velká a $A \subset B \subset \mathbb{N}$, pak B je velká.
(4) Pro každou $A \subset \mathbb{N}$ je jedna z dvou množin A, $\mathbb{N} \setminus A$ velká (a tedy ta druhá je malá).

Fakt. (existence netriviálního ultrafiltru na $\mathbb{N}$) *Podmnožiny $\mathbb{N}$ takto rozdělit lze.*

Nyní tedy dvě hyperčísla $a = (a_i)_{i=1}^{\infty}$, $b = (b_i)_{i=1}^{\infty}$ prohlásíme za totožná, pokud $\{i \in \mathbb{N} : a_i = b_i\}$ je velká množina. Tím se vyřeší náš problém s násobením, protože pokud $a \cdot b$ je 0, pak nutně a nebo b má nuly na velké množině indexů.

Dále nám to umožní každá dvě hyperčísla porovnat. Máme totiž rozklad $\mathbb{N}$ na tři disjunktní množiny

$$\{i \in \mathbb{N} : a_i < b_i\}, \quad \{i \in \mathbb{N} : a_i = b_i\}, \quad \{i \in \mathbb{N} : a_i > b_i\},$$

z nichž je (díky vlastnostem velkých množin) právě jedna velká. Podle toho, která je velká, rozhodneme, jestli $a < b$, $a = b$, nebo $a > b$.

Ve skutečnosti jsme touto konstrukcí zařídili, že oba požadované axiomy jsou splněny, a opravdu jsme tak zkonstruovali hyperreálná čísla.

Literatura a zdroje

[1] Abraham Robinson: *Non–Standard Analysis*, 1966.
[2] Dalibor Pražák: *NMMA574 Vybrané kapitoly z teorie dynamických systémů*, přednáška MFF UK, letní semestr 2016/2017.
[3] Mirek Olšák: *Hyperčísla*, Oldřichov, 2012.

Přehýbání

Tonda Češík

Při této přednášce budeš mít za úkol sestrojit všechno možné jen pomocí ohýbání papíru, podobně jako při origami. Ovšem protože je přednáška matematická a ne umělecká, raději se dohodneme, jaké ohýbání bude dovolené. Určíme si šest axiomů přehýbací geometrie, tedy šest akcí, které můžeme provádět.

(A1) Máme-li dány na papíře body A a B, umíme udělat přehyb, který jimi prochází (papír přehneme v přímce procházející oběma body).

(A2) Máme-li dány body A a B, umíme udělat přehyb, aby bod A ležel na bodu B (body dáme prostě na sebe a přehneme, vytvoříme tak vlastně osu úsečky AB).

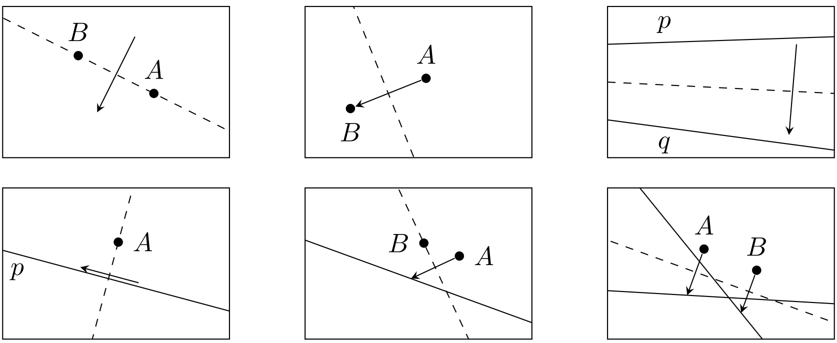
(A3) Máme-li dány dvě přímky p a q, umíme udělat přehyb takový, že p bude ležet na q.

(A4) Máme-li dán bod A a přímku p, umíme udělat přehyb kolmý na p procházející A.

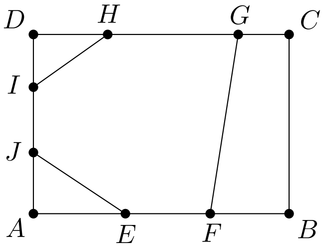
(A5) Máme-li dány body A a B a přímku p, umíme udělat přehyb procházející B takový, že A bude ležet na p (to už vyžaduje jistou dávku šikovnosti, přesto to proveditelné je).

(A6) Máme-li dány body A, B a přímky p, q, umíme udělat přehyb takový, že A bude ležet na p a B na q.

Pro názornost ještě axiomy v obrázcích:



Příklad 1. Na stranách obdélníkového papíru $ABCD$ formátu A4 jsou nakreslené body E, F, G, H, I, J jako na obrázku. Poskládejte střed kružnice vepsané trojúhelníku určenému přímkami EJ, FG a HI.



Příklad 2. Obarvěme jednu stranu papíru bíle a druhou černě. Poskládání papíru nazveme *vyvážené*, pokud pro každý bod při pohledu shora vidíme (i skrz) stejně bílých i černých stran (příklad: přehneme-li obdélník napůl, máme vyvážené poskládání, přehneme-li ho na třetiny, pak nikoliv).

Ukažte, že máme-li obdélník takový, že poměr délek jeho stran je racionální číslo, potom z tohoto obdélníku je možné poskládat čtverec tak, že toto poskládání bude vyvážené.

Příklad 3. Nechť $v_d > 2v_b$. Dokažte, že existuje nekonvexní čtyřúhelník $ABCD$ takový, že úhel u vrcholu B je větší než $180°$, výška trojúhelníku ABC z vrcholu B je rovna v_b, výška trojúhelníku ADC z vrcholu D je rovna v_d a ze čtyřúhelníku $ABCD$ lze poskládat čtyřstěn (pozor, ať neposkládáte „placku“).

Příklad 4. Poskládejte rovnostranný trojúhelník, máte-li dány dva jeho vrcholy. Je-li více možností, stačí nám jedna z nich.

Příklad 5. Je dán obdélníkový list papíru, obdélník tvořící papír označme R. Napřehýbejte **pouze pomocí axiomu (A2)** vrcholy obdélníku O takového, že O je podobný R a delší strana O má stejnou délku jako kratší strana R.

Příklad 6. Je dán čtvercový list papíru s vrcholy čtverce A, B, C, D (v tomto pořadí). Na straně AB je dán bod X_1. Napřehýbejte všechny body X_2 na straně BC takové, aby $X_1 = X_5$ při následujícím postupu skládání: Bod X_3 je bod na straně CD takový, že když přeložíme papír podél úseček X_1X_2 a X_2X_3, potom (přeložené) přímky BX_2 a CX_2 splývají (bod X_4 na straně DA a bod X_5 na AB získáme podobně).

Příklad 7. Mějme na papíře tři body, které tvoří trojúhelník. Poskládejte čtverec o stejném obsahu, jako má trojúhelník.

Příklad 8. Rozdělte zadaný úhel na třetiny.

Literatura

Přednáška je převzatá od *Monči Pospíšilové* z roku 2012, potažmo z 6. série 24. ročníku MKS:
http://mks.mff.cuni.cz/archive/24/6.pdf.

Velké prostory

Anička Doležalová

Abstrakt. Budeme si hrát s vektorovými prostory, které mají nekonečnou dimenzi. Cílem je si je trochu osahat a získat základní intuici. K tomu nám poslouží hlavně prostory posloupností.

Prerekvizity

Pokud byste rádi přišli na přednášku, ale nemáte potřebné znalosti z vektorových a metrických prostorů, odchyťte si mě v průběhu sousu a probereme to. Porozumění pojmům zde uvedeným je nezbytné[1] pro pochopení přednášky.

Úmluva. Píšeme-li „$\|x\|$ má vlastnost $\|x\| \geq 0$", máme tím na mysli, že tato nerovnost platí pro všechna x z příslušné množiny X.

Definice. *Vektorovým prostorem nad tělesem* T (zkráceně v. p. nad T) nazveme neprázdnou množinu V spolu s operacemi $+ : V \times V \to V$ a $\cdot : T \times V \to V$, pokud splňuje následující axiomy (kde $x, y, \dots \in V, \lambda, \vartheta \in T$):

(1) $x + y = y + x$, $(x + y) + z = x + (y + z)$,
(2) existuje x_0 takové, že $x_0 + x = x$ (typicky značíme 0),
(3) pro každé x existuje opačný prvek y: $x + y = 0$ (značíme $-x$),
(4) $\lambda \cdot (\vartheta \cdot x)) = (\lambda\vartheta) \cdot x$, $1 \cdot x = x$,
(5) $(\lambda + \vartheta) \cdot x = \lambda \cdot x + \vartheta \cdot x$, $\lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y$.

Znak pro násobení často vynecháváme. V přednášce budeme uvažovat pouze v. p. nad $\mathbb{R}$.

Lineárním obalem vektorů z množiny M rozumíme množinu všech (konečných!) lineárních kombinací těchto prvků, tj. $\{\sum_{i=1}^{n} \lambda_i x_i, \lambda_i \in T, x_i \in M\}$. Množinu vektorů nazveme lineárně nezávislou, pokud se žádný z nich nedá vyjádřit jako lineární kombinace ostatních.

Příklad. $\mathbb{R}^n$, kde n je přirozené číslo. Operace se provádějí po složkách, na nich se chovají jako standardní součet a součin. Nulový vektor je vektor $(0, \dots, 0)$.

[1] Ale nikoliv postačující.

Příklad. Prostor všech matic 2×2 nad $\mathbb{R}$. Sčítání i násobení se provádějí po složkách. Nulový vektor je nulová matice (všechny složky jsou nula).

Příklad. Prostor všech funkcí $\mathbb{R} \to \mathbb{R}$ s operacemi prováděnými bodově.

Definice. Dvojici $(X, \|\cdot\|)$ nazveme *normovaný vektorový prostor*, pokud X je vektorový prostor a zobrazení $\|\cdot\| : X \to \mathbb{R}$ splňuje

(1) $\|x\| \geq 0$, $\|x\| = 0 \iff x = 0$,
(2) $\|\lambda x\| = |\lambda| \cdot \|x\|$ $(\lambda \in \mathbb{R})$,
(3) $\|x + y\| \leq \|x\| + \|y\|$.

Zobrazení $\|\cdot\|$ nazveme norma.

Příklad. $X = \mathbb{R}$ s $\|x\| = |x|$ je normovaný v. p.

Příklad. Pro přirozené číslo n uvažujme $X = \mathbb{R}^n$ (tj. $x \in X$ je tvaru $(x_1, \ldots, x_n)$, kde $x_i \in \mathbb{R}$) s $\|x\|_1 = |x_1| + \ldots |x_n|$, $\|x\|_2 = \sqrt{|x_1|^2 + \cdots + |x_n|^2}$ nebo $\|x\|_\infty = \max\{|x_1|, \ldots, |x_n|\}$. V každém z těchto případů se jedná o normovaný v. p. Tyto prostory pro nás budou důležité, neboť z nich budeme v přednášce vycházet. Příslušné normy se nazývají postupně *součtová*, *eukleidovská* a *supremová*.

Příklad. Prostor všech spojitých funkcí $[0, 1] \to \mathbb{R}$ se supremovou normou definovanou jako $\|f\| = \max_{x \in [0,1]} |f(x)|$ tvoří normovaný v. p.

Poznámka. Spojitá funkce na uzavřeném intervalu nabývá maxima, norma je tedy dobře definovaná.

Definice. Mějme dva normované v. p. X, Y (nad $\mathbb{R}$). Zobrazení $L : X \to Y$ nazveme *lineární*, pokud splňuje

(1) $L(x + \tilde{x}) = L(x) + L(\tilde{x})$,
(2) $L(\lambda x) = \lambda L(x)$.

Příklad. Vynásobení konstantou je lineární zobrazení. Přičtení nenulové konstanty ne.

Definice. Dvojici (X, ρ) nazveme *metrický prostor*, pokud X je neprázdná množina a ρ je zobrazení $X \times X \to \mathbb{R}$ splňující

(1) $\rho(x, y) \geq 0$, $\rho(x, y) = 0 \iff x = y$,
(2) $\rho(x, y) = \rho(y, x)$,
(3) $\rho(x, z) \leq \rho(x, y) + \rho(y, z)$.

Zobrazení ρ se nazývá metrika. *Okolím bodu* $x_0 \in X$ *o poloměru* ε nazveme množinu $U(x_0, \varepsilon) = \{x \in X : \rho(x_0, x) < \varepsilon\}$. Množinu nazveme *otevřenou*, pokud pro každý její bod leží v množině i nějaké jeho okolí.

Příklad. Každý normovaný v. p., kde za $\rho(x, y)$ vezmeme $\|x - y\|$. Této metrice říkáme metrika indukovaná normou. Například tedy $\mathbb{R}$ se vzdáleností $|x - y|$.

Dále se nám bude hodit (alespoň) intuitivní představa limity posloupnosti v metrickém prostoru. Pro úplnost tedy uveďme její formální definici:

Definice. Mějme v metrickém prostoru (X, ρ) posloupnost jeho prvků $(x_n)_1^\infty$. Řekneme, že tato posloupnost *konverguje k bodu* $x \in X$ (bod x je její limitou), pokud pro každé $\varepsilon > 0$ existuje index n_0 takový, že všechny prvky posloupnosti $(x_n)_{n_0}^\infty$ už leží v $U(x, \varepsilon)$. Řekneme, že posloupnost je *cauchyovská*, pokud pro každé $\varepsilon > 0$ existuje index n_0 takový, že pro všechny indexy m, n větší než n_0 už platí $\rho(x_m, x_n) < \varepsilon$.

Tvrzení. *Každá konvergentní posloupnost je cauchyovská. Opačná implikace neplatí.*

Důkaz. Náznak:

Pokud už jsou všechny členy $(x_n)_{n_0}^\infty$ v $U(x, \varepsilon)$, pak pro členy této posloupnosti platí $\rho(x_m, x_n) < 2\varepsilon$.

Naopak budeme-li uvažovat jako metrický prostor $\mathbb{Q}$ s absolutní hodnotou, pak (z hustoty racionálních čísel v reálných) umíme najít cauchyovskou posloupnost, která nemá limitu (v $\mathbb{Q}$).

Přednáška!

Definice. Mějme normovaný v. p., na kterém uvažujeme metriku indukovanou normou. Pokud platí, že každá cauchyovská posloupnost je konvergentní (tedy má v daném prostoru limitu), nazveme tento prostor *Banachův*.

Poznámka. Obecně metrický prostor, ve kterém platí, že každá cauchyovská posloupnost je konvergentní, nazveme *úplný*. Budeme brát jako fakt, že reálná čísla s absolutní hodnotou jsou Banachův prostor.

Příklad. Prostor $\mathbb{R}^n$ s libovolnou z výše uvedených tří norem je Banachův.

Příklad. Prostor $\mathbb{R}^n$ s libovolnou p-normou je Banachův, kde

$$\|x\|_p = (|x_1|^p + \cdots + |x_n|^p)^{1/p}, p \in [1, \infty).$$

(Pro $p = \infty$ se jedná o supremovou normu.)

Příklad. Prostor všech spojitých funkcí $[0, 1] \to \mathbb{R}$ se supremovou normou je Banachův.

Poznámka. Pojem „supremová norma“ se zdá být nadužívaný, v jistém smyslu se ale jedná o stále tutéž normu – vezme se (v absolutní hodnotě) největší hodnota z nějaké množiny. V případě konečného vektoru je to jeho největší složka, v případě funkce největší funkční hodnota.

Definice. Označme $X = \mathbb{R}^\mathbb{N}$ (tedy prostor nekonečných – spočetných – posloupností se složkami z $\mathbb{R}$). Jedná se o vektorový prostor. Pro $p \in [1, \infty)$ definujeme

$$\ell^p = \left\{ x \in X : \|x\|_p = \left(\sum_{n \in \mathbb{N}} |x_n|^p \right)^{1/p} < \infty \right\}.$$

Podobně definujeme prostor omezených posloupností

$$\ell^\infty = \{x \in X : \|x\|_\infty = \sup_{n\in\mathbb{N}} |x_n| < \infty\}$$

a prostor posloupností konvergujících k nule

$$c_0 = \{x \in X : (x_n)_1^\infty \text{ konverguje k } 0\}$$

se supremovou normou (tj. toutéž jako v ℓ^∞).

Posloupnosti, které mají n-tou složku rovnou jedné a všechny ostatní nulové, značíme e_n.

Poznámka. Všechny tyto prostory jsou Banachovy.

Úloha 1. Zkuste si představit c_0 a ℓ^p. :)

Úloha 2. Jak se intuitivně liší c_0, ℓ^p $(p \in [1, \infty))$ a ℓ^∞?

Úloha 3. Jak vypadá $U(0, \varepsilon)$ v c_0, ℓ^1, ℓ^2, ℓ^∞?

Úloha 4. Najděte co největší množinu lineárně nezávislých vektorů v ℓ^p.

Úloha 5. Jak vypadá lineární obal množiny $\{e_n, n \in \mathbb{N}\}$ v těchto prostorech?

Úloha 6. Dokažte, že ℓ^1 je separabilní[2] (obecně to platí pro $p \in [1, \infty)$).

Úloha 7. Najděte nějaké lineární zobrazení $\ell^p \to \ell^p$, $\ell^p \to \ell^1$, $\ell^1 \to \mathbb{R}$.

Věta. (Riesz, neformálně) *Nechť $p \in (1, \infty)$. Každé lineární zobrazení $\ell^p \to \mathbb{R}$ se dá jednoznačně ztotožnit s prvkem ℓ^q, kde $\frac{1}{p} + \frac{1}{q} = 1$. Toto ztotožnění je prosté a na.*

Poznámka. Obecně množina všech lineárních zobrazení z jednoho Banachova prostoru do druhého tvoří také Banachův prostor. Prostoru lineárních zobrazení z Banachova prostoru X do $\mathbb{R}$ se říká *duální prostor* a značí se X^*. Příslušná norma je odvozená z norem obou prostorů.

Úloha 8. Najděte lineární zobrazení $\ell^1 \to \mathbb{R}$, které není dobře definované jako $\ell^2 \to \mathbb{R}$.

Definice. Na prostoru ℓ^2 definujeme skalární součin jako

$$\langle x, y\rangle = \sum_{n\in\mathbb{N}} x_n y_n.$$

Kolmost a ortogonální doplněk definujeme analogicky jako v konečném případě (např. u $\mathbb{R}^2$), tedy dva prvky jsou na sebe kolmé, pokud je jejich skalární součin nula, ortogonální doplněk množiny M jsou všechny prvky, které jsou kolmé na každý prvek M.

[2] Tj. najděte spočetnou hustou podmnožinu.

Úloha 9. Jak vypadá ortogonální doplněk posloupnosti e_1?

Úloha 10. Najděte dva různé podprostory ℓ^2, jejichž ortogonální doplněk je stejný.

Další směry, kterými se můžeme ubírat, jsou Banachovy algebry (můžeme „násobit“ vektory mezi sebou!), duály a slabé topologie (pro silnější nátury, které znají alespoň základy topologie) nebo svět L^p prostorů (kde žijí Lebesgueovsky integrovatelné funkce).

Literatura a zdroje

[1] O. Kalenda: *Úvod do funkcionální analýzy, Funkcionální analýza 1*, MFF.

IMO 1 (mod 3)

David Hruška

Abstrakt. Příspěvek obsahuje zadání nejjednoduších úloh z IMO (mezinárodní matematické olympiády) a návody k jejich řešení.

V obou soutěžních dnech jsou účastníkům IMO předloženy k řešení tři úlohy, které by měly být seřazené vzestupně podle obtížnosti. I když jsou všechny nepochybně na úrovni, vyřešení nejjednodušších dvou z nich (tedy první a čtvrté) často stojí na jednom dobrém nápadu a základních znalostech[1], a přitom již většinou zajišťuje dostatečně vysoké umístění na bronzovou medaili.

Cílem této přednášky je se tyto úlohy „naučit řešit". Neděláme si samozřejmě ambice na nalezení nějakého obecného návodu, ale pokusíme se zvyknout si na jejich styl, obtížnost a další zákonitosti. Hlavně se jich ale naučíme nebát tak, že jich během přednášky co nejvíc vyřešíme, nebo se alespoň necháme k řešení dovést.

Úloha 1. Trojúhelník BCF má pravý úhel u vrcholu B. Nechť A je bod na přímce CF takový, že $|FA| = |FB|$, a bod F leží mezi body A a C. Nechť D je bod takový, že $|DA| = |DC|$ a přímka AC je osou úhlu DAB. Dále nechť E je takový bod, že $|EA| = |ED|$ a přímka AD je osou úhlu EAC, a nechť bod M je středem úsečky CF. Konečně nechť je X bod takový, že $AMXE$ je rovnoběžník. Dokažte, že přímky BD, FX a ME se protínají v jednom bodě. (IMO 2016 – 1)

Úloha 2. Množinu kladných celých čísel nazveme *voňavou*, jestliže obsahuje alespoň dva prvky a libovolný její prvek má nějakého (i více) společného prvočíselného dělitele s alespoň jedním jiným jejím prvkem. Uvažme polynom $P(n) = n^2 + n + 1$. Určete nejmenší celé kladné b, pro které existuje celé nezáporné a tak, že množnina

$$P(a+1), P(a+2), \ldots, P(a+b)$$

je voňavá. (IMO 2016 – 4)

Úloha 3. Konečnou množinu $\mathcal{S}$ bodů v rovině nazveme *vyváženou*, jestliže pro libovolné dva různé body A a B z $\mathcal{S}$ existuje v $\mathcal{S}$ takový bod C, že $|AC| = |BC|$.

[1] Které člověk získá třeba ročním poctivým řešením nějakého dobrého m/Matematického korespondenčního semináře.

Množinu $\mathcal{S}$ nazveme *středuprostou*, jestliže pro žádné tři různé body A, B a C z $\mathcal{S}$ neexistuje v $\mathcal{S}$ bod P takový, že $|PA| = |PB| = |PC|$.

(i) Dokažte, že pro každé přirozené číslo $n \geq 3$ existuje vyvážená množina obsahující právě n bodů.

(ii) Určete všechna přirozená čísla $n \geq 3$, pro něž existuje vyvážená středuprostá množina obsahující právě n bodů.

(IMO 2015 – 1)

Úloha 4. Trojúhelníku ABC je opsána kružnice Ω se středem O. Přitom kružnice Γ se středem A protne úsečku BC v bodech D a E takových, že body B, D, E a C jsou různé a leží na přímce BC v tomto pořadí. Kružnice Γ a Ω se protínají v bodech F a G, přičemž body A, F, B, C a G leží na kružnici v tomto pořadí. Označme K další průsečík kružnice opsané trojúhelníku BDF s úsečkou AB a L další průsečík kružnice opsané trojúhelníku CGE s úsečkou CA. Předpokládejme dále, že přímky FK a GL jsou různé a protínají se v bodě X. Dokažte, že bod X leží na přímce AO. (IMO 2015 – 4)

Úloha 5. Je dána rostoucí posloupnost přirozených čísel $a_0 < a_1 < a_2 \ldots$ Dokažte, že existuje právě jedno $n \geq 1$ splňující

$$a_n < \frac{a_0 + a_1 + a_2 + \cdots + a_n}{n} \leq a_{n+1}.$$

(IMO 2014 – 1)

Úloha 6. Na straně BC daného ostroúhlého trojúhelníku ABC leží body P a Q tak, že $|\sphericalangle PAB| = |\sphericalangle BCA|$ a $|\sphericalangle CAQ| = |\sphericalangle ABC|$. Body M a N leží po řadě na přímkách AP a AQ, přičemž bod P je středem úsečky AM a bod Q je středem úsečky AN. Dokažte, že přímky BM a CN se protínají na kružnici opsané trojúhelníku ABC. (IMO 2014 – 4)

Úloha 7. Dokažte, že pro libovolnou dvojici kladných celých čísel k a n existuje k kladných celých čísel $m_1, m_2, \ldots, m_k$ (ne nutně různých) takových, že

$$1 + \frac{2^k - 1}{n} = \left(1 + \frac{1}{m_1}\right) \cdots \left(1 + \frac{1}{m_k}\right).$$

(IMO 2013 – 1)

Úloha 8. Buď ABC ostroúhlý trojúhelník s průsečíkem výšek H a nechť W je bod na straně BC ($W \neq B$, $W \neq C$). Označme M, resp. N patu výšky z bodu B, resp. z bodu C. Označme dále ω_1 kružnici opsanou trojúhelníku BWN a nechť X je bod na této kružnici takový, že úsečka WX je průměrem kružnice ω_1. Analogicky definujeme kružnici ω_2 opsanou trojúhelníku CWM a bod Y na ní, aby WY byl průměr ω_2. Dokažte, že body X, Y a H leží na přímce. (IMO 2013 – 4)

Úloha 9. Je dán trojúhelník ABC. Nechť J je střed kružnice připsané ke straně BC a nechť M je bod jejího dotyku s touto stranou. Dále nechť K a L značí po řadě body dotyku této kružnice s přímkami AB a AC. Průsečík přímek LM a BJ označme F a průsečík přímek KM a CJ pak G. Dále nechť S je průsečík přímek AF a BC a konečně nechť T je průsečík přímek AG a BC. Dokažte, že M je středem úsečky ST. (IMO 2012 – 1)

Úloha 10. Najděte všechny funkce $f : \mathbb{Z} \to \mathbb{Z}$, pro které platí rovnost

$$f(a)^2 + f(b)^2 + f(c)^2 = 2f(a)f(b) + 2f(b)f(c) + 2f(c)f(a)$$

pro libovolná celá a, b, c splňující $a + b + c = 0$. (IMO 2012 – 4)

Úloha 11. Pro libovolnou množinu $A = \{a_1, a_2, a_3, a_4\}$ čtyř (po dvou různých) přirozených čísel označme s_A součet $a_1 + a_2 + a_3 + a_4$. Dále nechť n_A znací počet dvojic (i, j), kde $1 \leq i < j \leq 4$ a $a_i + a_j$ dělí s_A. Určete všechny čtyřprvkové množiny A přirozených čísel, pro které je hodnota n_A největší možná. (IMO 2011 – 1)

Úloha 12. Nechť n je celé kladné číslo. Máme dány rovnoramenné váhy a $n + 1$ závaží o hmotnostech $2^0, 2^1, \ldots, 2^n$. V n krocích máme na váhy postupně po jednom umístit všechna závaží. Každý z kroků spočívá ve výběru jednoho ze závaží, které ještě není na vahách, a jeho umístění buď na levou, nebo na pravou misku vah tak, aby obsah pravé misky nebyl nikdy těžší než obsah levé. Kolik různých posloupností takovýchto n kroků existuje? (IMO 2011 – 4)

Úloha 13. Určete všechny funkce $f : \mathbb{R} \to \mathbb{R}$ splňující $f(\lfloor x \rfloor y) = f(x) \lfloor f(y) \rfloor$ pro libovolná reálná x, y. (IMO 2010 – 1)

Úloha 14. Nechť bod P leží uvnitř trojúhelníku ABC. Přímky AP, BP a CP protínají kružnici Γ opsanou trojúhelníku ABC po řadě v bodech K, L a M (různých od A, B, C). Tečna ke kružnici Γ v bodě C protíná přímku AB v bodě S. Dokažte, že pokud mají úsečky SC a SP stejnou délku, pak jsou stejně dlouhé i úsečky MK a ML. (IMO 2010 – 4)

Co jsme se o nejlehčích úlohách z IMO tedy dozvěděli? Autora napadá například toto:

(i) Jedna z úloh 1 (mod 3) bývá geometrie řešitelná úhlením (případně mocností, což je ale skoro to samé), které ale může být trochu záludné,
(ii) pokud se na těchto pozicích objeví funkcionální rovnice, mělo by stačil přemýšlet a dosazovat,
(iii) je-li v zadání přirozené číslo, je dobré zvážit indukci,
(iv) pokud se na těchto pozicích objeví nějaká teorie čísel, měli bychom si vystačit s dělitelností a odhodláním to dopočítat.

A nakonec rada působící v tomto kontextu možná zvláštně, rada obecně platná pro matematické (a podobné) soutěže: ať už se zadavatelé snaží seřadit úlohy podle obtížnosti jakkoliv, nikdy se toto pořadí nemusí přesně shodovat s vašimi zkušenostmi a schopnostmi, takže se nikdy nesnažte vyřešit první úlohu za každou cenu, pokud jste ostatním věnovali zatím jen minimum času.

Návody

1. Lépe popište divně definované body D, E a X. Podívejte se místo přímek jen na úsečky BD, FX a ME a zjistěte, co o nich platí. Jak se dá dokázat, že tři přímky prochází jedním bodem?

2. Jaká prvočísla mohou „soudělit" daná čísla? Použijte Euklidův algoritmus. Najděte nejmenší b, pro které jdou dělitelnosti vůči zmíněným prvočíslům nakombinovat? Jaké tvrzení umožňuje předepisovat zbytky?

3. Konstrukce v i) i v ii) je snadná. Pro zbytek ii) vyrobte úplný graf na S a každou hranu obarvěte barvou odpovídající „středu" jejích krajních vrcholů. Co musí pro toto obarvení platit?

4. Vyúhlete, že XFG je rovnoramenný.

5. Prostřední člen je průměr a něco málo navíc. Zkuste v nerovnostech toto něco málo osamostatnit a uvažte posloupnost $b_n := (a_n - a_1) + (a_n - a_2) + \cdots + (a_n - a_n)$.

6. Dokreslete středy AB a AC a těžnicemi vyrobte podobné trojúhelníky.

7. Indukce podle k s rozebráním podle parity n.

8. Dokreslete druhý průsečík P (existuje?) kružnic ω_1 a ω_2 a dokažte, že A leží na jejich chordále PW. Dále dokreslete kružnici nad průměrem AH.

9. Dokažte, že čtyřúhelník $AFJL$ je tětivový.

10. Vypočítejte $f(0)$, zvolte $f(1)$ a indukcí dopočítejte všechny zbylé hodnoty.

11. Ukažte, že musí být $n_A \leq 4$ a najděte řešení.

12. Hodil by se rekurentní vztah. Použijte vztahu $2^k > 1 + 2 + \cdots + 2^{k-1}$.

13. Stačí dosazovat.

14. Z mocnosti je SP tečna opsané ABP. Z toho pomocí úsekových úhlů máme $KL \parallel SP$. Dokreslete střed O kružnice Γ a z $OC \perp CS$ vyvoďte $SP \perp OM$.

Literatura a zdroje

[1] Oficiální stránky IMO, *https://www.imo-official.org/problems.aspx*
[2] web Art of Problem Solving, *https://artofproblemsolving.com*

Řády a mocniny

DAVID HRUŠKA

ABSTRAKT. Olympiádní teorie čísel se často zabývá úlohami o zbytcích a mocninách. K této oblasti existuje poměrně bohatá teorie, která nám jednak dává dobrou představu, jak zbytky fungují, a jednak se hodí v matematických soutěžích. Příspěvek obsahuje shrnutí jejích přístupnějších partií a přes dvacet různě obtížných úloh k procvičení.

V rámci úloh z teorie čísel můžeme často místo s danými čísly pracovat jen s jejich zbytky po dělení vhodným n (říká se také „modulo n"). Podíváme se podrobně na to, co se děje se zbytky modulo pevné n, když je násobíme a mocníme.

Zbytky, zejména ty nesoudělné s n

Definice. *Úplnou sadou zbytků* myslíme množinu $\{0, 1, 2, \ldots, n-1\}$ zbytků modulo n. Značíme ji $\mathbb{Z}_n$. Když v ní sčítáme nebo násobíme, tak myslíme automaticky sčítání a násobení modulo n. *Redukovaná sada zbytků* je podmnožina $\mathbb{Z}_n$ obsahující všechna čísla nesoudělná s n. Značíme ji $\mathbb{Z}_n^*$ a má $\phi(n)$ prvků, kde ϕ nazýváme *Eulerova funkce*.

Věta. *Pokud $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, kde p_i jsou po dvou různá prvočísla, pak platí*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right).$$

Kvadratické zbytky

Definice. Číslo $a \in \mathbb{Z}_n^*$ je *kvadratický zbytek*, pokud $x^2 \equiv a \pmod{n}$ pro nějaké $x \in \mathbb{Z}_n$. Pokud takové x neexistuje, říkáme, že a je *kvadratický nezbytek*.

Tvrzení. *Pro liché prvočíslo p je kvadratických zbytků $\frac{p-1}{2}$.*

Definice. Nechť p je liché prvočíslo a $a \in \mathbb{Z}$, pak definujeme *Legendreův symbol*

$\left(\frac{a}{p}\right)$ následovně:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{pro } p \mid a \\ 1 & \text{pokud } a \text{ je kvadratickým zbytkem a } p \nmid a \\ -1 & \text{pokud } a \text{ není kvadratickym zbytkem} \end{cases}$$

Úloha 1. Dokaž, že liché číslo, které se dá zapsat jako součet dvou čtverců, je nutně ve tvaru $4k+1$.

Úloha 2. Dokaž, že pokud $7 \mid a^2 + b^2$, pak $7 \mid a$ a $7 \mid b$. Dokaž, že obdobné tvrzení pro pětku neplatí.

Úloha 3. Bětka si myslí třísetciferné číslo, které se skládá ze sta nul, sta jediček a sta dvojek, přičemž první cifra není nula. Může být Bětčino číslo čtverec?

(MKS 29–2–4)

Řády a mocnění

Definice. Pro každé číslo $a \in \mathbb{Z}_n^*$ existuje právě jedna *inverze* modulo n, tj. prvek $a' \in \mathbb{Z}_n^*$ takový, že $aa' \equiv 1 \pmod{n}$. Obvykle inverzi značíme a^{-1}.

Definice. Pro $a \in \mathbb{Z}_n^*$ nazveme *řád prvku a modulo n* nejmenší $k \in \mathbb{N}$ takové, že $a^k \equiv 1 \pmod{n}$. Značíme ho $\mathrm{ord}_n(a)$.

Tvrzení. *Pro $a \in \mathbb{Z}_n^*, x, y \in \mathbb{N}_0$ platí*

$$a^x \equiv a^y \pmod{n} \iff x \equiv y \pmod{ord_n(a)}.$$

Důsledek. *Nechť $a \in \mathbb{Z}_n^*, x \in \mathbb{N}_0$. Pak $a^x \equiv 1 \pmod{n}$ právě, když $ord_n(a) \mid x$.*

Důsledek. *Pokud $a^x \equiv 1 \pmod{p}$ a zároveň $a^y \equiv 1 \pmod{p}$, pak též $a^{(x,y)} \equiv 1 \pmod{p}$.*

Věta. (Wilsonova) *Platí, že p je prvočíslo právě tehdy, když $(p-1)! \equiv -1 \pmod{p}$.*

Věta. (Eulerova) *Pro $a \in \mathbb{Z}_n^*$ platí $a^{\phi(n)} \equiv 1 \pmod{n}$.*

Speciálnímu případu této věty, kdy n je prvočíslo (a tedy $\phi(n) = n-1$), se říká *malá Fermatova věta.*

Tvrzení. (Eulerovo kritérium) *Nechť p je liché prvočíslo a a je číslo nesoudělné s p, potom $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.*

Tvrzení. *Buď p liché prvočíslo a a, b celá čísla. Pak $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.*

Úloha 4. Ukaž, že kdykoliv je p prvočíslo a a, b přirozená čísla, pak $p \mid ab^p - ba^p$.

Úloha 5. Ukaž, že pro různá prvočísla p, q platí

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

Úloha 6. Nechť p je prvočíslo a b je celé číslo. Dokažte, že $b^{p^2-1} \equiv 1 \pmod{p^2}$, právě když $b^{p-1} \equiv 1 \pmod{p^2}$. (MKS 28–9–4)

Úloha 7. Ukaž, že -1 je kvadratický zbytek modulo p, právě když p je ve tvaru $4k+1$.

Úloha 8. Nechť p je prvočíslo a q je prvočíslo, které dělí $2^p - 1$. Dokaž, že pak $p \mid q-1$.

Úloha 9. Pokud prvočíslo p dělí n-té Fermatovo číslo $2^{2^n} + 1$, pak $2^{n+1} \mid p-1$.

Úloha 10. Najdi všechna kladná celá čísla nesoudělná se všemi členy nekonečné posloupnosti

$$a_n = 2^n + 3^n + 6^n - 1.$$

(IMO 2005, 4)

Úloha 11. Buď p prvočíslo ve tvaru $3k+2$. Platí, že $p \mid a^2 + ab + b^2$, kde $a, b \in \mathbb{N}$. Ukaž, že pak i $p \mid a$, $p \mid b$.

Úloha 12. Nechť $p \geq 5$ je prvočíslo a $n = \frac{2^{2p}-1}{3}$. Ukaž, že $n \mid 2^n - 2$. (iKS 1, N4)

Úloha 13. Dokaž, že pro $n > 1$ nemůže nastat $n \mid 2^{n-1} + 1$. (Schinzel)

Úloha 14. Nalezni všechny trojice prvočísel p, q, r splňující soustavu dělitelností

$$p \mid q^r + 1,\ q \mid r^p + 1,\ r \mid p^q + 1.$$

(USA TST 2003)

Úloha 15. Najdi všechna $n > 1$, pro která existuje právě jedno $0 < a \leq n!$ takové, že $a^n + 1$ je dělitelné $n!$. (ISLS 2005, N4)

Úloha 16. Nechť $p \geq 5$ je prvočíslo. Dokaž, že existuje $1 \leq a \leq p-2$ takové, že ani $a^{p-1} - 1$, ani $(a+1)^{p-1} - 1$ není dělitelné p^2. (ISLS 2001, N4)

Úloha 17. Nechť p je prvočíslo. Dokaž, že existuje prvočíslo q takové, že pro žádné přirozené číslo n není $n^p - p$ dělitelné q. (IMO 2003, 6)

Primitivní prvek

Asi nejzajímavější tvrzení o zbytcích modulo p je existence primitivního prvku. Nebudeme ji dokazovat, ale krátce si ukážeme, jak funguje.

Definice. Číslo $a \in \mathbb{Z}_n^*$ nazveme *primitivní prvek*, pokud $\operatorname{ord}_n(a) = \phi(n)$.

Poznámka. Primitivní prvek g je tedy číslo, které „generuje" celou $\mathbb{Z}_n^*$, neboli

$$\{g^0 \pmod n, g^1 \pmod n, g^2 \pmod n, \dots\} = \mathbb{Z}_n^*.$$

Věta. *Primitivní prvek existuje právě pro modula ve tvaru* $2, 4, p^k, 2p^k$, *kde* p *je liché prvočíslo a* $k \in \mathbb{N}$.

Úloha 18. Nechť p je liché prvočíslo. Najdi všechna taková k, že

$$p \mid 1^k + 2^k + \cdots + (p-1)^k.$$

(Hungary-Israel Math Competition 2009)

Úloha 19. Pro prvočíslo p urči, jaký je součet všech kvadratických zbytků modulo p. Jak je to s kvadratickými nezbytky?

Úloha 20. Dokaž, že součin všech primitivních prvků modulo p je kongruentní 1 mod p.

Úloha 21. Ukaž, že 2 je primitivní prvek mod 3^n.

Úloha 22. Dokaž, že pokud je p Fermatovo prvočíslo (tedy je ve tvaru $2^{2^k}+1$ pro nějaké $k \in \mathbb{N}$), pak je každý kvadratický nezbytek modulo p současně primitivním prvkem.

Návody

1. Modulo 4.

2. Rozeberte možnosti na zbytky modulo 7.

3. Modulo 9.

4. Rozeber zvlášť případ, kdy je jedno z čísel dělitelné p, pak využij malou Fermatovu větu.

5. Podívej se na kongruenci zvlášť modulo p a q, použij malou Fermatovu větu.

6. Využij Eulerovu větu.

7. První implikaci sporem s malou Fermatovou větou. Druhou implikaci Eulerovým kritériem.

8. $\operatorname{ord}_q(2) = p$.

9. Umocni kongruenci na druhou, abys dostal řád prvku 2 modulo p.

10. Pro prvočísla $p > 3$ uvaž člen a_{p-2} a využij malou Fermatovu větu.

11. Platí také $a^3 \equiv b^3 \pmod{p}$. Umocni na vhodnou mocninu, aby šla využít malá Fermatova věta.

12. Dokaž $2p \mid n - 1$.

13. Vyluč sudá čísla, rozlož na součin a uvaž takové prvočíslo p v rozkladu, že $p-1$ je dělitelné nejmenší mocninou r čísla 2. Dokaž $n \equiv 1 \pmod{2^r}$.

14. BÚNO p je nejmenší. Pokud je p liché, dokaž $p \mid q - 1$ nebo $p \mid q + 1$ a vyluč první možnost a následně dokaž $q \mid r + 1$ a $r \mid p + 1$.

15. Platí pro prvočísla. Pro lichá složená uvaž $a = \frac{n!}{d} - 1$, kde $d \mid n$. Pro lichá prvočísla dokaž, že $\frac{a^n+1}{a+1}$ je nesoudělné s $(n-1)!$.

16. Označ C množinu těch a, pro které $a^{p-1} \equiv 1 \pmod{p^2}$. Dokaž $|C| \leq \frac{p-1}{2}$. Dále sporem dostaň $1, 3, \ldots, p-2 \in C$ a spor vyvoď z $p-4, p-2 \in C$.

17. Vezmi libovolné prvočíslo $q \mid \frac{p^p-1}{p-1}$. Dokaž $q \equiv 1 \pmod{p}$ a $q \mid p^k - 1$, kde $q = kp + 1$. Potom dokaž $p \mid k$ a $q \equiv 1 \pmod{p^2}$. To nemůže nastat pro všechny prvočíselné dělitele $\frac{p^p-1}{p-1}$.

18. Zapiš čísla $1, \ldots, p-1$ pomocí jednoho primitivního prvku a využij vzoreček pro součet geometrické řady.

19. Kvadratické zbytky jsou přesně ty prvky $\mathbb{Z}_p^*$, u kterých má primitivní prvek sudý exponent.

20. Inverzní prvek k primitivnímu prvku je opět primitivní.

21. Indukcí podle n. Musí platit $\phi(3^n) = \operatorname{ord}_{3^n}(2) \mid \operatorname{ord}_{3^{n+1}}(2) \mid \phi(3^{n+1})$. Další indukcí vyluč případ $\operatorname{ord}_{3^{n+1}} = 2 \cdot 3^{n-1}$.

22. Kvadratické zbytky nemohou být primitivními prvky. Kolik má p primitivních prvků?

Literatura a zdroje

Tento příspěvek je téměř podmnožinou příspěvku *Štěpána Šimsy* z pátého soustředění *i*KS s názvem *Řády a primitivní prvek*, kterému tímto děkuji.

Úvod do kombinatoriky

Bára Kociánová

Abstrakt. Příspěvek vysvětluje základní kombinatorické pojmy a obsahuje mnoho lehčích příkladů i s výsledky, spíše mimochodem také zmiňuje, co je to pravděpodobnost. Neobsahuje žádnou hlubší teorii.

Kolik různých pořadí může mít závod s pěti účastníky? Kolika způsoby si můžeme ze skříně vybrat oblečení pro dnešní den? Jaká je pravděpodobnost, že v kostkách hodíme samé jedničky? A že správně tipneme čísla, která si někdo myslí?

Na tyto a další otázky spolu budeme hledat odpovědi.

Jak různě můžeme vybírat

Máme-li vybrat jednoho dobrovolníka ze skupiny pěti lidí, máme zjevně pět možností, koho zvolit. Pokud máme vybrat dva, dělí se nám příklad na různé případy, podle toho, jestli nám záleží na jejich pořadí, nebo ne.

Pokud dostanou oba dobrovolníci stejný úkol ve stejný čas, nezajímá nás, koho jsme zvolili prvního a koho druhého. Hledáme tedy počet dvojic mezi pěti lidmi, přičemž dvojice Žibřida a Zdislavy je stejná jako dvojice Zdislavy a Žibřida. To zvládneme spočítat třeba výčtem všech možností: k Žibřidovi můžeme přidat postupně Zdislavu, Yvonnu, Xaveria a Waldemara, ke Zdislavě už jen Yvonnu, Xaveria a Waldemara, Yvonna pak s Xaveriem a Waldemarem vytvoří dvě dvojice a Xaverius s Waldemarem nakonec jednu. Dohromady máme $4 + 3 + 2 + 1 = 10$ možných dvojic. Ke stejnému výsledku dojdeme, pokud uvažujeme, že každý má čtyři různé kamarády, s nimiž může utvořit dvojici. To by bylo $5 \cdot 4 = 20$. Jenže, jak již bylo řečeno, je dvojice Žibřida a Zdislavy totožná s dvojicí Zdislavy a Žibřida, a tak jsme tuto (a každou další také) dvojici započítali dvakrát. Vydělením dvěma dostaneme $20/2 = 10$. Můžeme říct, že jsme právě spočítali počet dvoučlenných *kombinací* z pěti prvků.

Pokud začneme dobrovolníky mezi sebou rozlišovat, situace se výrazně změní. Nejprve předpokládejme, že prvnímu dobrovolníkovi zavážeme oči a druhý ho pak povede po předem vyznačené trase. Kolik máme možností provedení? Pro vybrání prvního pět, pro druhého zbývají jen čtyři, neboť ten vybraný už má zavázané oči a nemůže dělat obojí. Jenže co s těmi čísly teď, sečíst, vynásobit, umocnit? Pokud náš slepý dobrovolník bude Žibřid a povede ho Zdislava, je to úplně jiný příběh, než pokud Zdislavě bude ukazovat cestu Žibřid. Tedy pro každého prvního dobrovolníka existují čtyři druzí dobrovolníci. Máme proto $5 \cdot 4$ různých dvojic slepec – vodič, což je počet dvoučlenných *variací* z pěti prvků.

Ještě jiný výpočet použijeme, představíme-li si, že vybraný dobrovolník skupince zatančí čardáš a vrátí se mezi ostatní. Následně vybereme dalšího dobrovolníka, který bude chvíli stepovat. Kolika způsoby se tohle mohlo stát? Jako prvního tanečníka můžeme vybrat pět různých lidí. A jako druhého také pět, protože po Žibřidovi můžeme tentokrát vybrat znovu Žibřida. A poučeni z předchozího případu tato čísla vynásobíme, protože pro každého z pěti prvních dobrovolníků existuje pět možných následovníků. Dostaneme $5 \cdot 5 = 25$, neboli počet dvoučlenných *variací s opakováním* z pěti prvků.

Několik matematických pojmů

Ujasníme si názvosloví a pravidlo součtu a součinu mimochodem zmíněné v předchozím odstavci, definujeme si faktoriál a kombinační číslo, řekneme si něco málo o pravděpodobnosti a zjistíme, k čemu je to dobré.

Tvrzení 1. (Pravidlo součtu) *Mějme konečné množiny $A_1, A_2, \dots A_n$, které jsou po dvou disjunktní. Potom počet prvků množiny $A_1 \cup A_2 \cup \dots \cup A_n$ je roven součtu počtů prvků množin $A_1, A_2, \dots A_n$.*

Toto pravidlo používáme zcela intuitivně, jak je vidět v následujícím příkladu:

Příklad 2. Na soustředění jelo jedním vlakem pět účastníků z Prahy, dva z Liberce, čtyři z Karlových Varů a jeden z Plzně. Kolik jich jelo celkem?

Tvrzení 3. (Pravidlo součinu) *Počet všech uspořádaných n-tic takových, že první složku můžeme vybrat k_1 způsoby, druhou k_2 způsoby, ... až n-tou k_n způsoby, je roven $k_1 \cdot k_2 \cdot \ldots \cdot k_n$.*

Toto pravidlo jsme už využili při vybírání slepého a vodiče v předchozím textu. Slepého jsme mohli vybrat pěti způsoby, vodiče čtyřmi, dohromady tedy $5 \cdot 4$ způsoby.

Příklad 4. Kolik je čtyřciferných čísel dělitelných pěti?

Řešení. Na místo tisíců můžeme vybrat devět cifer (nulu ne), na místo stovek deset, na místo desítek také deset a na místo jednotek jen dvě, nulu nebo pětku. Dohromady máme $9 \cdot 10 \cdot 10 \cdot 2 = 1800$.

Definice 5. Pojem *k-členná kombinace z n prvků* vyjadřuje počet možností, kterými můžeme vybrat k prvků z n-prvkové množiny, aniž by nám záleželo na pořadí výběru.

Pojem *k-členná variace z n prvků* značí také počet možností, kterými můžeme vybrat k prvků z n-prvkové množiny, ale pokud pořadí výběru zohledníme.

Pojem *permutace na n prvcích* značí počet možných uspořádání n prvků.

Definice 6. Faktoriál n definujeme jako $n! = n \cdot (n-1) \cdot (n-2) \dots 2 \cdot 1$. Speciálně definujeme $0! = 1$.

Tvrzení 7. *Počet permutací na n prvcích se rovná $n!$.*

Definice 8. Kombinační číslo [en nad ká] definujeme jako $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Tvrzení 9. *Počet k-členných kombinací z n prvků vyjadřuje kombinační číslo $\binom{n}{k}$.*

Tvrzení 10. (Binomická věta) *Platí*

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{(n-1)}b + \cdots + \binom{n}{k}a^{(n-k)}b^k + \cdots + \binom{n}{1}ab^{(n-1)} + \binom{n}{0}b^n.$$

Definice 11. Množinu všech možných výsledků náhodného pokusu označme Ω, přičemž předpokládejme, že všechny její prvky ω nastanou se stejnou pravděpodobností. Podmnožinu A množiny Ω nazveme *jevem*, pro $A = \Omega$ *jistým jevem*, pro $A = \emptyset$ *nemožným jevem*. Pravděpodobnost, že nastane daný jev A, vyjádříme jako $P(A) = |A|/|\Omega|$.

Příklad 12. Jaká je pravděpodobnost, že při hodu kostkou padne jednička nebo šestka?

Řešení. Možné výsledky hodu kostkou tvoří množinu $\Omega = \{1, 2, 3, 4, 5, 6\}$. Jev „padne jednička nebo šestka“ je množina $A = \{1, 6\}$, čili pravděpodobnost, že padne jednička nebo šestka, je $2/6 = 1/3$.

Tvrzení 13. *Ω je množina možných výsledků náhodného pokusu, $A, B \subset \Omega$.*

(1) $P(\Omega) = 1$, $P(\emptyset) = 0$
(2) $0 \le P(A) \le 1$
(3) $P(\Omega \setminus A) = 1 - P(A)$
(4) $P(A \cup B) = P(A) + P(B) - P(A \cap B)$

Nejtypičtější příklady

Na konci příspěvku jsou k příkladům uvedeny návody, které mnohdy přímo prozrazují výsledek.

Příklad 14. Kolik existuje sudých čtyřciferných čísel, která nejsou dělitelná pěti? Kolik je pěticiferných čísel, která jsou dělitelná čtyřmi? Kolik je trojciferných čísel, v jejichž desítkovém zápise je každá číslice nejvýš jednou? Kolik je čtyřciferných čísel, v nichž se sudé a liché číslice střídají?

Příklad 15. Kolik úhlopříček má n-úhelník?

Příklad 16. Jakou nejdelší abecedu bychom mohli zakódovat pomocí nejvýše čtyř teček či čárek? A co v Braillově písmu (nejvýše šest vystouplých teček)? Nebo v semaforu (ukazuje se rukama do osmi různých směrů, přičemž ruce nejsou rozlišitelné a nemohou splývat)?

Příklad 17. K pětadvacátým narozeninám dostala princezna bonboniéru ve tvaru čtverce, kde v každém řádku i sloupci bylo pět bonbonů. Chtěla si jich hned pět sníst, ale tak, aby nevyjedla žádný celý řádek ani sloupec. Kolika způsoby si mohla bonbony vybrat? A co kdyby chtěla z každého řádku i sloupce sníst právě jeden?

Příklad 18. V královské radě tradičně zasedá pět lidí. Do voleb se přihlásilo dvanáct lidí, z toho sedm šlechticů a pět šlechtičen. Protože je království moderní a podporuje rovnost mužů a žen, vyžaduje se, aby v radě byli aspoň dva muži a aspoň dvě ženy. Kolika způsoby může volba dopadnout?

Příklad 19. V jiném královském poradním orgánu zasedá předem neurčený nenulový počet lidí. O tuto funkci mají zájem čtyři muži a tři ženy a tentokrát je jedinou podmínkou pro volbu, aby v radě bylo stejně mužů jako žen. Kolik je možných výsledků?

Příklad 20. Kroketového turnaje se účastní šestnáct lidí. Hrají vždy dvě dvojice proti sobě. Kolika způsoby můžeme všechny hráče rozdělit?

Příklad 21. Vrháme obyčejnou šestistěnnou kostkou. Jaká je pravděpodobnost, že ve třech hodech hodíme aspoň jednu jedničku, že v pěti hodech nepadne žádné sudé číslo a že součet čísel po dvou hodech bude pět?

Příklad 22. Elsa každé ráno bezradně kouká do skříně a neví, co si obléct. Vždyť je tak těžké si vybrat! Má patery šaty, troje punčochy, čtyři páry střevíčků, dvě spony do vlasů a dva a půl páru náušnic (jednu ztratila). Z kolika možností každé ráno vybírá, když na sobě podle dvorního protokolu musí mít šaty, punčochy, dva střevíčky, sponu do vlasů a dvě náušnice? S jakou pravděpodobností na sobě bude mít spárované střevíčky a náušnice? (Střevíčky jsou levé a pravé, kdežto dvě náušnice z páru jsou identické.)

Příklad 23. Dvanáct měsíčků se z nudy stavělo do řady podle stáří, teploty, množství uzrálých jahod a podobných vlastností, až je napadlo: kolika různými způsoby se za sebe můžou postavit? Jaká je pravděpodobnost, že při náhodném seřazení (kde jsou všechny možnosti stejně pravděpodobné) budou stát vedle sebe měsíce ročního období (tj. mezi měsíci nějakého ročního období nebude stát žádný měsíc jiného ročního období)? A jak se můžou seřadit, pokud se červen pohádal s prosincem a odmítají stát vedle sebe?

Příklad 24. Zákazník si chce u věštkyně ověřit, že přišel k té pravé, a tak si pětkrát myslí nějakou cifru a nechává věštkyni hádat. Určete postupně pravděpodobnost, že se podvodnice ani jednou netrefí, že právě dvakrát tipne správné číslo a že se aspoň jednou splete.

Další příklady

Příklad 25. Určete počet obarvení šachovnice $1 \times n$ pěti barvami tak, aby žádná dvě sousední políčka neměla stejnou barvu. Pokud máme všechny správně obarvené šachovnice schované v pytli, s jakou pravděpodobností z něj vytáhneme nějakou dvoubarevnou nebo nějakou, na které je aspoň jedno políčko červené?

Příklad 26. Výrobce hodin se rozzlobil na svůj nudný sortiment a rozhodl se vyrábět nové dokonale kulaté ciferníky, na nichž budou čísla od jedné do dvanácti uspořádána v kruhu libovolně a napsaná tak, aby nebylo poznat, kde je nahoře. Kolikery hodiny bude mít nově v nabídce?

Příklad 27. Milion obyvatel země hlasovalo v zemských volbách o tom, které roční období je nejlepší. Výsledky se udávají ve tvaru uspořádané čtveřice získaných počtů hlasů v pořadí [jaro, léto, podzim, zima]. Kolik možných výsledků volby mají?

Příklad 28. Na dostihových závodech běží pět koní. Pokud jejich čas měříme na celé vteřiny (tedy pokud dva koně doběhnou v jednu vteřinu, doběhli na stejném místě), kolika různých pořadí koní se můžeme dočkat?

Pokud si na svého oblíbeného koně vsadíme, že doběhne nejhůř třetí (tj. bude mít nejhůř třetí čas), jakou máme šanci vyhrát? Předpokládejme, že všechny možné výsledky jsou stejně pravděpodobné.

Příklad 29. Čísla $1, 2, \ldots, 2017$ dáme do tří barevných kyblíčků: bílého, modrého a červeného. Kolika způsoby můžeme čísla rozházet, pokud žádný z nich není prázdný a dvě po sobě jdoucí čísla nikdy nejsou v témže kyblíčku? (PraSe 30–4–4)

Příklad 30. Ve vězení je pět mužů a sedm žen. Domluvili se, že každý den vylosují jednoho z nich, kdo se zeptá strážce, jestli je nechce pustit ven. Jaká je pravděpodobnost, že první dva vylosovaní byli muži?

Strážce to po roce omrzelo a slíbil jim, že pokud se ho desetkrát po sobě zeptá žena, opravdu jim celu odemkne. S jakou pravděpodobností bude vězení do dvou týdnů prázdné?

Příklad 31. Na zámku je úschovna zavazadel, v níž je n skříněk, ke kterým patří n různých klíčů. Zlý trpaslík do každé skříňky dal nějaký klíč a pak všechny zavřel. Hodný trpaslík má kouzelnou hůlku, která umí otevřít skříňku vlevo nahoře. Z ní může vyzvednout klíč a odemknout k němu příslušnou skříňku a pokračovat dále. Určete pravděpodobnost, že se mu podaří otevřít všechny skříňky.

(PraSe 26–5–3)

Příklad 32. Kolik vět můžeme vytvořit z šestadvaceti písmen abecedy, pokud každé použijeme právě jednou a za větu považujeme libovolnou posloupnost písmen rozdělenou mezerami (přičemž mezer může být libovolně, ale nikdy ne dvě vedle sebe)?

Příklad 33. Anna dělala zasedací pořádek na svatbu. Pozvala dvacet čtyři hostů, z nichž bylo osmnáct mužů a šest dam. Chtěla vybrat nejlepší posazení hostů tak, aby u každého kulatého stolu pro čtyři lidi seděla jedna dáma. Z kolika takových vybírala? Když zasedání u stolu jen otočíme, považujeme ho za stejné, podobně nezáleží na tom, u jakého přesně stolu kdo sedí.

Jaká je pravděpodobnost, že při náhodně vylosovaném zasedacím pořádku bude Anna vedle svého ženicha?

Příklad 34. Šnek se chce dostat z jednoho rohu krychle do protějšího, avšak plazit se chce pouze po hranách, a to nejvýše po pěti. Kolik takových cest má? Počítáme i ty, během nichž navštíví cíl vícekrát. (PraSe 29–3–4)

Příklad 35. V cukrárně měli n sladkostí, ale každou bohužel jen jednou. Přišli dva mlsouni a nakoupili několik sladkostí, každý aspoň jednu. Kolika způsoby to mohli udělat? (PraSe 25–5–4)

Příklad 36. Mějme čtverečkovaný papír $m \times n$. Kolika způsoby můžeme strany všech čtverečků obarvit pomocí tří barev tak, aby každý čtvereček měl právě dvě strany obarvené jednou barvou a zbývající dvě nějakou jinou jednou barvou? Strany, kterými se sousedící čtverečky dotýkají, považujeme za totožné. (PraSe 33–1–4)

Příklad 37. Kolika způsoby se může posadit deset chlapců a dvanáct děvčat na kolotoč s dvaceti čtyřmi sedadly tak, aby mezi každými dvěma chlapci sedělo aspoň jedno děvče? Posazení, která se liší jen otočením kolotoče, považujeme za totožná. (PraSe 3–6–4)

Návody

14. $9 \cdot 10 \cdot 10 \cdot 4$; $9 \cdot 10 \cdot 10 \cdot 25$; $9 \cdot 9 \cdot 8$; $5 \cdot 5 \cdot 5 \cdot 5 + 4 \cdot 5 \cdot 5 \cdot 5$

15. $\frac{n(n-3)}{2}$

16. $2 + 4 + 8 + 16$; 2^6; $8 \cdot 7/2$

17. $\binom{25}{5} - 10$; $5!$

18. $\binom{5}{3} \cdot \binom{7}{2} + \binom{5}{2} \cdot \binom{7}{3}$

19. $4 \cdot 3 + \binom{4}{2} \cdot \binom{3}{2} + \binom{4}{3} \cdot \binom{3}{3}$

20. Do čtveřic: $16!/(4!)^5$, ve čtveřici do dvojic: 3, celkem: $\frac{16! \cdot (3)^4}{(4!)^5}$.

21. $1 - \left(\frac{5}{6}\right)^3$; $\left(\frac{1}{2}\right)^5$; $\frac{4}{36}$

22. $5 \cdot 3 \cdot 4 \cdot 4 \cdot 2 \cdot 8$ (střevíčky jsou levé a pravé, náušnice výčtem možností); $\frac{1}{16}$

23. $12!$; $4! \cdot (3!)^4$; $12! - 11! \cdot 2$

24. $\left(\frac{9}{10}\right)^5$; $\left(\frac{9}{10}\right)^3 \cdot \left(\frac{1}{10}\right)^2 \cdot \binom{5}{2}$; $1 - \left(\frac{1}{10}\right)^5$

25. $5 \cdot 4^{n-1}$; $\left(\frac{5 \cdot 4}{5 \cdot 4^{n-1}}\right) + \left(\frac{5 \cdot 4^{n-1} - 4 \cdot 3^{n-1}}{5 \cdot 4^{n-1}}\right) - \left(\frac{2 \cdot 4}{5 \cdot 4^{n-1}}\right)$ (dvoubarevné + červené − dvoubarevné červené)

26. $12!/12 = 11!$

27. Chceme seřadit milion hlasů a tři přepážky, což je $\frac{1000003!}{1000000!3!}$.

28. $n = 5! + 4!\binom{5}{2} + 3!\binom{5}{3} + 2!\binom{5}{4} + 1 + 3! \cdot 5 \cdot \frac{\binom{4}{2}}{2} + 2!\binom{5}{2}$; $1 - \frac{2 \cdot 4! + 4 \cdot 3! + 3! \cdot \binom{4}{2}}{n}$

29. $3 \cdot 2^{2016} - 6$

30. $\frac{5 \cdot 5}{12 \cdot 12}$; $\frac{(7^{10} \cdot 12^4 + 5 \cdot 7^{10} \cdot 12^3 + 12 \cdot 5 \cdot 7^{10} \cdot 12^2 + 12^2 \cdot 5 \cdot 7^{10} \cdot 12 + 12^3 \cdot 5 \cdot 7^{10})}{12^{14}}$

31. $\frac{29}{30} \cdot \frac{28}{29} \cdot \ldots \cdot \frac{2}{3} \cdot \frac{1}{2} = \frac{1}{30}$

32. $26! \cdot 2^{25}$ (Mezery se můžou nebo nemusí dát na pětadvacet míst v posloupnosti.)

33. $18!$; $\frac{2}{18}$

34. $3 \cdot \frac{5!}{3!} + 6$

35. $3^n - 2 \cdot 2^n + 1$

36. $3^{m+n} \cdot 2^{mn}$

37. $\binom{12}{2} \cdot \binom{24}{2} \cdot 9! \cdot 12!$

Literatura a zdroje

[1] Poznámky ze školy a soustředění, zmíněné série PraSete.
[2] *PraSečí seriál o kombinatorice*, *http://mks.mff.cuni.cz/archive/27/9.pdf*

Komplexní čísla

HONZA KREJČÍ

ABSTRAKT. Co jsou to komplexní čísla? K čemu se používají? Dá se s nimi dělat něco cool? Na tyto a další otázky se na přednášce/v příspěvku pokusíme odpovědět.

Proč vznikla komplexní čísla? Podívejme se na polynomy s reálnými koeficienty. Ty jsou super, ale mají jednu nepříjemnou vlastnost – ne všechny jsme schopni zapsat jako součin polynomů stupně nejvýše jedna. To znamená, že dopředu třeba nevíme, kolik má polynom $x^8 + 5x^6 + 17x^2 + 349x + 5$ kořenů. Nebo neumíme rozložit tak jednoduchý polynom jako $x^2 + 1$. Co s tím?

První případ vypadá dost komplikovaně, ve druhém by nám stačilo mít *číslo*, jehož druhá mocnina dává -1. Označme si takové číslo i, tj. $i^2 = -1$. (Zřejmě, pokud takové číslo máme, pak číslo k němu opačné má stejnou vlastnost.) Nyní, abychom měli uzavřenost na operace sčítání a násobení, tak uvažujme všechna čísla tvaru $a + bi$, kde a, b jsou reálná, a označme tuto množinu $\mathbb{C}$. Pak se zmiňovaný polynom nad touto množinou rozkládá na součin $x^2 + 1 = (x + i)(x - i)$. To není všechno – lze dokonce dokázat, že každý polynom nad $\mathbb{C}$ se rozkládá na součin polynomů stupně nejvýše jedna. Ukazuje se, že toto není jediná hezká vlastnost komplexních čísel. Mimo jiné se s nimi dají intuitivně odvodit zajímavé vzorce a (dokonce) mají praktické uplatnění v popisu geometrických zobrazení nebo také ve fyzice.

Úmluva 1. Dále v tomto textu předpokládáme, že a, b, c a d jsou reálná čísla a z je číslo komplexní.

Definice 2. (Komplexní číslo) Číslo $z = a+bi$, kde $i^2 = -1$, budeme nazývat *komplexní číslo*, a nazveme *reálnou částí* komplexního čísla a b nazveme jeho *imaginární částí*. Značíme $\Re(z) = a$ a $\Im(z) = b$.

Věta 3. (Základní věta algebry) *Každý polynom nad komplexními čísly má kořen.*

Úloha 4. Jaký tvar má součin a součet čísel $a + bi$, $c + di$?

Různé tvary komplexních čísel

S komplexními čísly se dají provádět stejné věci jako s čísly reálnými, ale k některým z nich je právě definovaný tvar nevhodný.

Zřejmě, abychom jednoznačně zadali komplexní číslo, stačí nám uspořádaná dvojice reálných čísel. Dvojice se rovněž používají pro zadávání bodů v rovině – nebylo by možné si komplexní čísla představit jako body v rovině?

Definice 5. (Komplexní čísla podruhé) Komplexnímu číslu $a + bi$ přiřadíme v rovině bod se souřadnicemi $[a, b]$. Ose x budeme říkat *reálná osa* a ose y *imaginární.* Pro libovolné dva body v rovině se souřadnicemi $[a, b]$ a $[c, d]$ definujeme operace sčítání a násobení následovně:

- $[a, b] + [c, d] = [a + b, c + d]$,
- $[a, b] \cdot [c, d] = [ac - bd, ad + bc]$.

Nyní definujeme třetí tvar, tzn. *goniometrický.* Pro dané nenulové komplexní číslo $z = a + bi$ existuje právě jeden průsečík jednotkové kružnice se středem v počátku a polopřímky vycházející z počátku, která prochází bodem z. Bod na jednotkové kružnici jsme schopni reprezentovat dvojicí $[\cos\varphi, \sin\varphi]$ a délka úsečky spojující počátek se z je $\sqrt{a^2 + b^2}$. Proto můžeme psát $a + bi = \sqrt{a^2 + b^2} \cdot (\cos\varphi + i \cdot \sin\varphi)$.

Definice 6. (Absolutní hodnota a argument komplexního čísla) Pro komplexní číslo $z = a + bi$ definujeme:

- *Absolutní hodnota* komplexního čísla z je $|z| = \sqrt{a^2 + b^2}$.
- *Argument* komplexního čísla z je číslo φ z rozmezí $[0, 2\pi)$ takové, že platí $z = |z| \cdot (cos\varphi + i \cdot \sin\varphi)$.

Z hlediska geometrického si lze absolutní hodnotu představit jako délku úsečky spojující počátek s vybraným komplexním číslem. Argument je potom úhel, který tato úsečka svírá s kladnou částí reálné osy.

Úloha 7. Je přechod mezi základním tvarem komplexního čísla a goniometrickým tvarem jednoznačný, tj. je jednoznačné zobrazení, které komplexnímu číslu přiřadí dvojici absolutní hodnota a argument?

Úloha 8. Převeďte čísla $-2 - 2i$, $3 - i\sqrt{3}$, $-7 + 7i$ do goniometrického tvaru.

Je-li absolutní hodnota komplexního čísla rovna jedné, nazveme takové číslo *komplexní jednotka.*

Věta 9. (Součtové vzorce) *Pro a, b platí:*

- $\sin(a + b) = \sin a \cos b + \cos a \sin b$,
- $\cos(a + b) = \cos a \cos b - \sin a \sin b$.

Z poslední definice a znalosti součtových vzorců si lze konečně představit, jak vypadá násobení komplexních čísel.

Mějme čísla $z_1 = |z_1|(\cos\varphi_1 + i\sin\varphi_1)$ a $z_2 = |z_2|(\cos\varphi_2 + i\sin\varphi_2)$. Potom $z_1 \cdot z_2 = |z_1||z_2|(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2))$. Tj. dostaneme číslo, které má argument roven součtu argumentů násobených čísel a jeho vzdálenost od počátku je rovna součinu vzdáleností násobených čísel.

Úloha 10. Jaká geometrická zobrazení jsou reprezentována:

- přenásobením $\pm i$?
- přenásobením komplexní jednotkou?
- přenásobením reálným číslem?
- přenásobením komplexním číslem?

Úloha 11. Popište zobrazení, které komplexnímu číslu přiřadí jeho absolutní hodnotu.

Věta 12. (Moivreova věta) *Pro a a celé číslo n platí následující rovnost:*

$$(\cos a + i \sin a)^n = \cos na + i \sin na$$

Důkaz. Pro $n \geq 0$ tvrzení dokážeme matematickou indukcí podle n za pomoci součtových vzorců. Je-li $n < 0$, pak z již dokázaného platí, že $(\cos a + i \sin a)^n = \frac{1}{(\cos a + i \sin a)^{-n}} = \frac{1}{\cos(-na) + i \sin(-na)}$. Dále přenásobíme zlomkem $\frac{\cos(-na) - i \sin(-na)}{\cos(-na) - i \sin(-na)}$. Tímto přenásobením nám stále zůstává zachována rovnost, neboť násobíme jedničkou. Nakonec si uvědomíme, že sinus je lichá funkce, kosinus sudá funkce a dostaneme $(\cos a + i \sin a)^n = \cos(-na) - i \sin(-na) = \cos na + i \sin na$. $\square$

Základní operace s komplexními čísly

S reálnými čísly toho děláme spoustu, mimo jiné třeba dělíme, mocníme a odmocňujeme. Mocnit číslo $(-2-2i)^{42}$ nevypadá jako příjemná činnost, nicméně na mocnění (s celočíselným koeficientem) máme goniometrický tvar a Moivreovu větu. Vyjde-li nám čas, ukážeme si, jak umocnit nebo odmocnit (skoro) všechno za použití komplexní exponenciály a logaritmu.

Komplexní čísla jsou zákeřnější co se zlomků týče – jakou hodnotu má výraz $\frac{1+i}{1-i}$? Zkusme zlomek usměrnit tak, aby ve jmenovateli nebylo komplexní číslo (usměrníme číslem komplexně sdruženým k číslu ve jmenovateli zlomku): $\frac{1+i}{1-i} = \frac{1+i}{1-i} \cdot \frac{1+i}{1+i} = i$.

Definice 13. (komplexně sdružené číslo) Mějme $z = a + bi$, potom číslo *komplexně sdružené* je $\overline{z} = a - bi$.

Věta 14. (Vlastnosti komplexního sdružování) *Nechť z_1, z_2 jsou komplexní čísla a P polynom s reálnými koeficienty, potom:*

- $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$,
- $\overline{z_1 z_2} = \overline{z_1} \cdot \overline{z_2}$,
- $\overline{P(z_1)} = P(\overline{z_1})$.

Další problém, který s komplexními čísly máme, je, že neumíme spočítat druhou odmocninu. Zkusme (cvičně) spočítat odmocninu z čísla $5 + i\sqrt{11}$. Tato odmocnina bude komplexní číslo $a + bi$ pro vhodné konstanty a, b. Umocníme-li rovnici a porovnáme reálné a imaginární části, dostaneme pro ně tuto soustavu rovnic:

$$5 = a^2 - b^2$$

$$\sqrt{11} = 2ab$$

Soustavu můžeme vyřešit vyjádřením a z druhé rovnice, dosazením do první a následným dopočítáním a. Dostaneme čísla $\pm(\frac{\sqrt{22}}{2} + i\frac{\sqrt{2}}{2})$.

Nyní ověříme, že kvadratická rovnice $-\frac{1}{4}x^2 + 2x + 1 + i\sqrt{11} = 0$ má skutečně dva kořeny.

Krátkou úpravou kvadratického polynomu se můžeme přesvědčit, že „vzoreček“ pro výpočet kořenů kvadratické rovnice funguje pořád stejně:

$$\begin{aligned}
px^2 + qx + r &= p\left(\left(x^2 + \frac{q}{p}x + \frac{q^2}{4p^2}\right) - \left(\frac{q^2}{4p^2} - \frac{r}{p}\right)\right) \\
&= p\left(\left(x + \frac{q}{2p}\right)^2 - \left(\sqrt{\frac{q^2 - 4pr}{4p^2}}\right)^2\right) \\
&= p\left(x + \frac{q}{2p} - \sqrt{\frac{q^2 - 4pr}{4p^2}}\right)\left(x + \frac{q}{2p} + \sqrt{\frac{q^2 - 4pr}{4p^2}}\right).
\end{aligned}$$

Položíme-li poslední součin roven nule a vyjádříme x, dostaneme požadované.

Co ale dělat, když umocňujeme na něco komplexního?

Komplexní exponenciála a logaritmus

Pro nedostatek prostoru zavedeme komplexní exponenciálu a její vlastnosti uvedeme bez důkazu.

Definice 15. Funkci $\exp : \mathbb{C} \to \mathbb{C}\setminus\{0\}$, která komplexnímu číslu $z = a + bi$ přiřadí hodnotu $e^a(\cos b + i \sin b)$, nazýváme komplexní exponenciála.

Věta 16. (Vlastnosti komplexní exponenciály) *Komplexní exponenciála je spojitá $2\pi i$ periodická funkce, která splňuje následující vlastnosti:*

- $\exp'(z) = \exp(z)$,
- $\exp(z_1 + z_2) = \exp(z_1)\exp(z_2)$,
- $\exp(z) = \sum_{j=0}^{\infty} \frac{z^n}{n!}$.

Úloha 17. Jaký je obraz přímky rovnoběžné s osou x při zobrazení exp?

Idea, jak definovat komplexní logaritmus, je vcelku jednoduchá – chceme funkci, která nám pro zvolené z vrátí takovou hodnotu w, že $\exp(w) = z$. Takových hodnot může být hodně, nicméně když budeme požadovat w takové, že $\Im(w) \in [0, 2\pi)$, dostaneme právě jednu. Lze si rozmyslet, že $w = \log|z| + i \arg z$.

Definice 18. (Komplexní mocnina) Pro $z \neq 0$ a $\alpha \in \mathbb{C}$ definujeme $z^\alpha = \exp(\alpha \cdot \log(z))$.

Pokud se zbavíme požadavku, že logaritmus musí být jednoznačný, můžeme uvažovat množinu komplexních mocnin, která je pro $\alpha \in \mathbb{C}\setminus\mathbb{R}$ dokonce nekonečná.

Co se s tím dá dělat

Zkusme si s pomocí komplexní exponenciály spočítat řešení rovnice $x^n = -1$. Postupně budeme upravovat $x^n = \exp(n \cdot \log x) = \exp(\pi i) = -1$. Protože je exponenciála $2\pi i$ periodická, $n \log x = \pi i + 2k\pi i$. Nakonec dostaneme $x = \exp(\frac{\pi i + 2k\pi i}{n})$. Z definice exponenciály a absolutní hodnoty si lze všimnout, že všechna řešení jsou komplexní jednotky, a ty navíc tvoří pravidelný n-úhelník.

Úloha 19. Co se změní, pokud budeme uvažovat rovnice $x^n = 1$, $x^n = c$, kde $c \in \mathbb{R}$?

Úloha 20. Jakou hodnotu má výraz i^i?

Několik příkladů na závěr

Příklad 21. Nechť P je reálný polynom lichého stupně. Dokažte, že má kořen v reálných číslech.

Příklad 22. Nechť $z \neq 1$ je komplexní jednotka. Dokažte, že zlomek $\frac{z+1}{z-1}$ je ryze imaginární (tj. že má nulovou reálnou část a nenulovou imaginární část).

Příklad 23. Najděte všechna z, pro která $z^2 + \overline{z}^2 \in \mathbb{R}$.

Příklad 24. Sečtěte:

- $\sin a + \sin 2a + ... + \sin ka$,
- $\cos a + \cos 2a + ... + \cos ka$.

Příklad 25. Pro dané $n \in \mathbb{N}$ sečtěte:

- $\binom{n}{0} - \binom{n}{2} + \binom{n}{4} - \dots,$
- $\binom{n}{0} + \binom{n}{3} + \binom{n}{6} - \dots.$

Literatura a zdroje

[1] Roman Lávička: *Úvod do komplexní analýzy*, Praha, 2017.
[2] Pavel Podbrdský: *Komplexní čísla*, neznámé, 2001.
[3] Martin Tancer: *Komplexní čísla a jejich geometrické aplikace*, Olšanka, 2006.

Permutace

Jakub Löwit

Abstrakt. Jak v olympiádní, tak ve vysokoškolské matetamice se nám často stane, že mám někdo něco zamíchá nebo přeuspořádá. Všechny takové příklady ale spojuje jeden algebraicko-kombinatorický princip - permutace. V přednášce si ukážeme jejich základní vlastnosti, které posléze použijeme k řešení mnoha různorodých příkladů. Na závěr si blíže ukážeme sílu permutací v teorii čísel.

Permutace!

Permutace je jedním ze základních algebraických a kombinatorických objektů. Jde zkrátka o přečíslování či zamíchání nějaké množiny objektů. Přesto nás ale často může překvapit. Je dobré mít na paměti, že permutace jsou snad ty nejsymetričtější objekty, co si můžeme představit.

Definice 1. (Permutace) *Permutace* σ na množině X je zobrazení, které každému prvku X přiřadí nějaký (ne nutně jiný) prvek X. Přitom obrazy různých prvků musí být různé a každý prvek má nějaký vzor.

Definice 2.

(1) Skutečnost, že σ je permutace na množině X, často značíme $\sigma \in S_X$.
(2) Permutaci, která zobrazuje všechny prvky z X na sebe samotné nazýváme *identita*.
(3) Ke každé permutaci σ existuje právě jedna *inverzní* permutace σ^{-1}, která přiřazuje obrazům jejich vzory.
(4) Složením permutací σ, π myslíme zobrazení, které vznikne provedením postupně zobrazení σ a následně π. Toto zobrazení je opět permutace a značíme jej $\pi \circ \sigma$.
(5) Řádem permutace σ myslíme nejmenší $n \in \mathbb{N}_0$ takové, že pokud složíme σ samu se sebou k-krát, dostaneme identickou permutaci.

Lemma 3. *Existuje přesně $n! = n \cdot (n-1) \ldots 3 \cdot 2 \cdot 1$ permutací n-prvkové množiny.*

Lemma 4. *Každé přirozené číslo lze jednoznačně zapsat jako $a_1 \cdot 1! + a_2 \cdot 2! + a_3 \cdot 3! + \ldots$, kde $0 \le a_i \le i$.*

Definice. *Cyklus* je permutace, která cyklicky posouvá nějakých k prvků, přičemž ostatní nechává na místě.

Lemma 5. *Každou permutaci na konečné množině lze (až na pořadí) jednoznačně rozložit na součin disjunktních cyklů.*

Definice. *Transpozice* je permutace, která prohazuje pouze dva prvky (a všechny ostatní nechává na místě).

Lemma 6. *Každou permutaci na konečné množině lze získat jako složení několika transpozic.*

Lemma 7. *Každá permutace má nějaký řád (tedy existuje přirozené k takové, že složení této permutace k-krát je identická permutace).*

Na úvod...

Úloha 8. Kolika způsoby lze na šachovnici 8×8 rozmístit 8 věží tak, aby se žádné dvě neohrožovaly?

Úloha 9. Do tabulky $n \times n$ napíšeme čísla $1, 2, \ldots, n^2$ popořadě tak, že nejprve vyplníme zleva doprava první řádek, potom druhý atd. Nyní v tabulce vybereme n políček tak, abychom z každého řádku i každého sloupce vybrali právě jedno, a čísla na vybraných pozicích sečteme. Jaké výsledky můžeme dostat?

Nahlížíme

Jak už se nám doneslo, počet permutací n-prvkové množiny je $n!$. Když se proto někde faktoriál objeví, permutace určitě nejsou daleko a často se k řešení úlohy přímo vybízí vhodná kombinatorická interpretace.

Úloha 10. Pro přirozená k, n nahlédněte rovnost

$$\frac{(kn)!}{(k!)^n} = \binom{k}{k} \cdot \binom{2k}{k} \cdots \binom{nk}{k}.$$

Úloha 11. Je dáno přirozené k a $n \geq k$. Uvažme náhodnou permutaci na $1, 2, \ldots, n$. Nahlédněte, že pravděpodobnost, že prvky $1, \ldots, k$ leží v jednom cyklu, nezávisí na volbě n.

Úloha 12. Uvažme nějakou permutaci α množiny $1, 2, \ldots, n$. Postupně za sebe napišme všechny prvky $\alpha(1)$, $\alpha(2)$, $\ldots$, $\alpha(n)$. Jejich čtením zleva doprava získáme postupně $f(\alpha)$ rostoucích úseků. Jaká je průměrná hodnota $f(\alpha)$ přes všechny permutace zadané množiny?

Úloha 13. Permutacím σ na množině $1, 2, \ldots, 2n$, pro něž existuje $1 \leq i < 2n$ takové, že $|\sigma(i) - \sigma(i+1)| = n$, říkejme dobré. Ostatní nazývejme špatné. Nahlédněte, že dobrých permutací je víc, než špatných.

(IMO 1989)

Úloha 14. Je dáno $n \geq 2$ bodů očíslovaných $1, 2, \ldots, n$, přičemž mezi každými dvěma vede šipka směrem od nižšího čísla k vyššímu. Obarvení šipek červenou a modrou nazveme *jednobarevné*, jestliže mezi žádnými dvěma vrcholy nevede zároveň červená a modrá cesta. Uvědomte si, že počet *jednobarevných* obarvení je $n!$.

(ARO 2005)

Úloha 15. Označme $D(n)$ počet permutací na n prvcích, které nenechávají na místě ani jeden prvek. Nahlédněte, že

$$D(n) = \sum_{i=0}^{n} (-1)^i \binom{n}{i} (n-i)!.$$

Úloha 16. Jako *plné* n-tici přirozených čísel budeme označovat ty, ve kterých pro každé číslo $i \geq 2$, jež se v n-tici vyskytuje, platí, že číslo $i-1$ se v ní vyskytuje také, přičemž první výskyt $i-1$ je před posledním výskytem i. Nahlédněte, že *plných* n-tic je $n!$.

(IMO Shortlist 2002)

Úloha 17. Pro přirozená $n \geq 1$ dokažte identitu

$$n! = \sum_{i=1}^{n} (-1)^{n-i} \cdot \binom{n}{i} \cdot i^n$$

.

Hrajeme si…

Nejčastěji je zkrátka potřeba si s úlohou chvíli hrát a pochopit, jak funguje. Občas nám sice nějaká znalost navíc může pomoct, cesta k řešení je ale většinou o dost zajímavější.

Úloha 18. Kolik existuje permutací π množiny $1, 2, \ldots, n$, které splňují

$$1 \cdot \pi(1) \leq 2 \cdot \pi(2) \leq \cdots \leq n \cdot \pi(n)?$$

Úloha 19. Na slavnostní večeři je n účastníků. Někteří z nich jsou přitom přátelé. Před každým účastníkem leží jedno jídlo, přičemž na stole nejsou žádná dvě jídla stejná. Každý z účastníků ale má chuť na něco jiného. Pokud se dva lidé přátelí, mohou si vyměnit svá jídla. Kolik dvojic účastníků musí být přátelé, aby každý mohl dostat své vysněné jídlo?

Úloha 20. Ve vězení sedí 100 vězňů. Ředitel věznice se rozhodl, že jim dá šanci na svobodu. Do 100 očíslovaných šuplíků ve své kanceláři proto náhodně umístil jména vězňů, do každého šuplíku právě jedno. Vězni budou jeden po druhém chodit do kanceláře. Každý z nich se může postupně podívat do 50-ti šuplíků. Pokud se všem vězňům povede nalézt svá jména, jsou propuštěni, jinak je ředitel nechá popravit.

Před začátkem hry se navíc mohou domluvit. Vymyslete pro vězně takovou strategii, aby jejich šance na propuštění byla alespoň $1-(\frac{1}{51}+\frac{1}{52}+\cdots+\frac{1}{100})>\frac{3}{10}$.

(folklor)

Úloha 21. Uvažme strom na n vrcholech označených čísly 1, 2, …, n. Postupně zvolíme všechny hrany (každou právě jednou), přičemž vždy prohodíme čísla na koncích zvolené hrany. Tím dostaneme nějakou permutaci čísel ve vrcholech. Kolik cyklů může tato permutace obsahovat?

(Irán TST 2014)

Úloha 22. Na severní straně ulice je $n \geq 2$ domů. Ze západu k východu, domy nají čísla postupně od 1 do n, přičemž na každém domě visí jeho číslo. Jednou si obyvatelé chtěli vystřelit z pošťáka. Během jednoho dne tak postupně prohodili čísla všem $n-1$ dvojicím sousedních domů. Kolik různých posloupností čísel může být večer v na domech v ulici?

(MEMO 2013)

Úloha 23. Je dáno n přirozené. Určete (v závislosti na n) počet permutací p na množině $1,\ldots,n$, pro něž $p\cdot p$ obrací pořadí čísel (tj. posílá číslo i na $n+1-i$ pro všechna $1 \leq i \leq n$).

Úloha 24. V řadě stojí n studentů. Když se učitel nedívá, někteří změní svá místa. Pokud student změnil pozici v řadě z i na j, pohnul se o $|j-i|$ míst. Určete maximální součet míst, o která se mohli pohnout všichni studenti dohromady.

(MEMO 2015)

Úloha 25. Stroj na vyměňování myslí funguje tak, že vždy vymění mysl zvolené dvojici lidí. Tato dvojice těl si už ale nikdy znovu nemůže pomocí stroje znovu vyměnit mysli. Jednoho dne si n lidí hrálo se strojem. Nyní by každý rád získal zpět své tělo. Dokažte, že pokud si na pomoc seženou alespoň dva další kamarády (kteří ještě stroj nikdy nezkoušeli), tak se jim to podaří.

(Futurama)

Úloha 26. Pro sudé $n \geq 4$ mějme tabulku $n \times n$ vyplněnou čísly 1, 2, …, $\frac{n^2}{2}$, přičemž každé je použito právě dvakrát. Dokažte, že lze vybrat n políček takovým způsobem, aby bylo zvoleno právě jedno políčko z každého řádku i sloupce, a navíc žádná dvě vybraná políčka neobsahovala stejné číslo.

Úloha 27. O Velikonocích hrálo n hráčů turnaj. Každý hrál s každým a nenastaly žádné remízy. Permutací n hráčů je *pomlázková*, pokud se poráželi cyklicky dokola. Dokažte, že se mohlo hrát tak, aby vzniklo alespoň $\frac{n!}{2^n}$ pomlázkových permutací.

Úloha 28. Dokažte, že každý konvexní mnohostěn P v $\mathbb{R}^d$ lze získat jako projekci nějakého k rozměrného simplexu v $\mathbb{R}^n$ pro vhodné n, k (k-rozměrný simplex je mnohostěn, který má $k+1$ vrcholů, jejichž vzájemné vzdálenosti jsou stejné).

Úloha 29. Dokažte rovnost polynomů

$$\sum_{\pi \in S_n} x^{I(\pi)} = 1 \cdot (1+x) \cdot (1+x+x^2) \dots (1+x+\dots+x^{n-1}),$$

kde $I(\pi)$ značí počet inverzí v pemutaci π, tedy dvojic $1 \le i < j \le n$, pro která je $\pi(i) > \pi(j)$.

Nejsou čísla jako čísla...

Většina úloh o permutacích moc nezávisí na tom, jak velkou množinu vlastně permutujeme. Občas je ale potřeba využít i její velikosti, popřípadě se zajímat i o jiné teoriečíselné vlastnosti, které po nás vyžaduje zadání.

Úloha 30. Při večeři sedí $2n$ lidí kolem otočného stolu. Každý si objednal jiné jídlo, ale zmatený číšník rozdal jídla náhodně. Dokažte, že lze stůl otočit tak, aby alespoň dva lidé měli jídlo, které si objednali.

(Brkos)

Úloha 31. Máme balíček $2n$ karet. Zamíchání balíčku změní pořadí karet z a_1, a_2, $\dots$, a_n, b_1, b_2, $\dots$, b_n na a_1, b_1, a_2, b_2, $\dots$, a_n, b_n. Určete všechna n taková, že po 8 zamícháních má balíček karet původní pořadí.

(VJIMC 2014)

Úloha 32. Nechť $p > 2$ je prvočíslo. Pro každou permutaci $\pi = (\pi(1), \pi(2), ..., \pi(p))$ prvků množiny $S = 1, 2, ..., p$ nechť $f(\pi)$ značí počet všech násobků prvočísla p, které se vyskytují mezi následujícími p čísly: $\pi(1), \pi(1)+\pi(2), ..., \pi(1)+\pi(2)+...+\pi(p)$. Určete průměrnou hodnotu $f(\pi)$ uvažovanou pro všechny permutace π prvků množiny S. (MEMO 2012)

Úloha 33. Pro $n \ge 2$ označíme permutaci σ množiny $1, 2, \dots, n$ jako *kvadratickou* (respektive *kubickou*), jestliže jsou čísla $\sigma_i \cdot \sigma_{i+1} + 1$ druhé (respektive třetí) mocniny přirozených čísel pro všechna i od 1 do $n-1$. Dokažte, že pro nekonečně mnoho n existuje kvadratické permutace, ale pro žádné n neexistuje kubická.

(Irán TST 2014)

Úloha 34. Permutaci $(a_1, a_2, ..., a_n)$ množiny $(1, 2, ..., n)$ nazveme *čtvercovou*, pokud je mezi čísly a_1, $a_1 + a_2$, $\dots$, $a_1 + a_2 + ... + a_n$ alespoň jedna druhá mocnina přirozeného čísla. Najděte všechna přirozená n taková, že jsou všechny permutace množiny $(1, 2, ..., n)$ čtvercové.

(Irán TST 2002)

Parita!

Nyní si ukážeme trikový invariant, který je zachováván při různých zápisech nějaké permutace, zvaný parita permutace. Hezké na něm je to, že jde zjistit hned několika různými způsoby. Tato na první pohled hravá tvrzení mají poměrně hluboké důsledky.

Lemma 35. (Parita transpozic) *Mějme pevnou permutaci σ rozepsanou jako složení n transpozic. Potom parita n nezávisí na konkrétním rozepsání.*

Definice. (Znaménko) Pro permutaci σ uvažme její libovolný rozklad na n transpozic. Pak definujeme její *znaménko* (neboli *paritu*) jako $\operatorname{sgn}(\sigma) = (-1)^n$.

Lemma 36. *Pro libovolné permutace σ, π na stejné množině platí*

$$\operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\pi) = \operatorname{sgn}(\sigma \circ \pi).$$

Lemma 37. *Pro permutaci σ uvažme její rozklad na disjunktní cykly, dále označme k počet těchto cyklů, které mají sudou délku. Potom $\operatorname{sgn}(\sigma) = (-1)^k$.*

Lemma 38. *Inverzí v permutaci σ na množině $1, 2, \ldots, n$ označíme libovolnou dvojici prvků této množiny i, j, které splňují $i < j$ a zároveň $\sigma(i) > \sigma(j)$. Počet různých inverzí v permutaci σ označme l. Potom $\operatorname{sgn}(\sigma) = (-1)^l$.*

Lemma 39. *Uvažme funkci f, které každé permutaci z S_X přiřadí 1 nebo -1. Navíc pro libovolnou dvojici takových permutací σ, τ platí $f(\sigma \circ \tau) = f(\sigma) \cdot f(\tau)$. Potom buď f je konstantně 1, nebo $f = \operatorname{sgn}$.*

Úloha 40. Pro přirozené $n \geq 2$ spočtěte počet sudých permutací n-prvkové množiny.

Úloha 41. Je dán čtverečkovaný hrací plán 4×4. Na čtvercích plánu jsou náhodně rozmístěna čísla $1, 2, \ldots, 15$, každé právě jednou. Poslední pole je volné. V každém tahu můžeme zvolit jedno z polí, která sousedí stranou s volným polem a přesunout číslo, které obsahuje, do volného pole. Hru vyhrajeme právě tehdy, když se nám po konečném počtu kroků povede seřadit všechna čísla postupně po řádcích (a pravý dolní čtvereček zůstane prázdný). Rozhodněte, zda vždy umíme vyhrát.

Úloha 42. Jaká je pravděpodobnost, že hru z předešlého příkladu umíme vyhrát, dostaneme-li na začátku náhodné rozmístění čísel 1, 2, …, 15?

Úloha 43. Pro přirozené číslo n uvažme množinu S všech permutací na n prvcích. Elsa a Anna hrají následující hru. Každá z nich ve svém tahu vybere jednu permutaci z S, která doteď nebyla zvolena. Pokud lze pomocí skládání a invertování vybraných permutací vyrobit všechny permutace z S, hra končí a hráč, který hrál poslední, prohrává. Elsa přitom hraje první. Pro která n má Elsa vyhrávající strategii?

(IMC 2012)

Úloha 44. Dokažte, že pro libovolnou n-tici reálných čísel a_1, a_2, …, a_n platí identita

$$\sum_{\pi \in S_n} sgn(\pi) \prod_{i=1}^{n} a_{\pi(i)}^{i-1} = \prod_{1 \le i < j \le n} (a_j - a_i).$$

A co na to teorie čísel?

Pojďme si na závěr jště lépe demonstrovat sílu permutací v teorii čísel. Od snadných tvrzení se kouzelně dostaneme až k samotné reciprocitě.

Lemma 45. (Malá Fermatova věta) *Pro prvočíslo p a číslo a, které není dělitelné p, platí $a^{p-1} \equiv 1 \pmod{p}$.*

Lemma 46. (Eulerova věta) *Pro přirozené n označme $\varphi(n)$ počet přirozených čísel $m \le n$, která jsou s ním nesoudělná. Potom pro libovolné a, která je nesoudělné s n, platí $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Lemma 47. (Čínská zbytková věta) *Pro n-tici po dvou nesoudělných čísel a_1, a_2, …, a_k a libovolná celá b_1, b_2, …, b_k existuje právě jedno číslo $0 \le x < a_1 a_2 \dots a_k$, které dává po dělení číslem a_i zbytek b_i pro všechna $i \in 1, 2, \dots, k$.*

Definice. (Legendreův symbol) Ať p je prvočíslo, a celé číslo. Potom definujeme Legendreův symbol jako

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{pokud } p \mid a, \\ 1, & \text{pokud a je kvadratický zbytek modulo p,} \\ -1, & \text{pokud a je kvadratický nezbytek modulo p.} \end{cases}$$

Nyní si ještě rozmyslíme jedno lemma bez použití permutací, potom už permutace budou všude.

Lemma 48. (Eulerovo kritérium) *Pro prvočíslo $p \ge 3$ a a celé platí $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$.*

Lemma 49. (Gaussovo lemma) *Mějme prvočíslo $p \ge 3$ a a libovolné celé. Označme m počet čísel a, $2a$, …, $\frac{p-1}{2}a$, jejichž zbytek modulo p je ostře větší než $\frac{p-1}{2}$. Potom $\left(\frac{a}{p}\right) = (-1)^m$.*

Lemma 50. (Zolotarevovo lemma) *Pro prvočíslo $p \ge 3$ a a nesoudělné s p platí $\left(\frac{a}{p}\right) = \operatorname{sgn}(\pi_a)$, kde π_a značí permutaci indukovanou na zbytcích modulo p násobením číslem a.*

Lemma 51. (Kvadratická reciprocita) *Pro prvočísla p, $q \ge 3$ platí vztah*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Návody

3. První prvek lze vybrat n způsoby, druhý $n-1$ způsoby atd., až poslední jedním způsobem.

4. Indukcí podle počtu členů je to zřejmé.

5. Vyjděte na procházku z nějakého prvku, časem se nutně musíte vrátit. Tím jste našli jeden cyklus.

6. Rozmyslete si, že libovolný cyklus umíte zapsat jako složení transpozic.

7. Stačí vzít nejmenší společný násobek délek všech jejích cyklů.

8. Přesně 8! způsoby, protože pozice věží postupně ve sloupcích zleva doprava odpovídají permutaci osmiprvkové množiny.

9. Rozepište si čísla na součet řádkové a sloupcové části, každou z nich můžete nasčítat zvlášť.

10. Mějme kn různých míčků k barev a n tvarů. Kolik různých posloupností všech míčků můžeme vytvořit, pokud nás zajímají pouze jejich tvary?

11. Sestrojte všechny permutace na n prvcích takovým způsobem, aby pravděpodobnost skutečně nezávisela na k. Co třeba přidávat čísla postupně?

12. Je to $\frac{n+1}{n}$. Spárujte permutace do dvojic podle směru čtení.

13. Permutace si představujte jako posloupnosti kuliček n barev, přičemž každá barva je použita dvakrát. Dvě kuličky stejné bary vedle sebe lze splácnout do jedné. Špatných posloupností je stejně jako dobrých, ve kterých došlo k jednomu splácnutí.

14. Rozmyslete si, že každé takové obarvení odpovídá nějakému seřazení čísel 1, 2, …, n, které jednoznačně určuje barvy šipek a naopak. Barvy jsou směry.

15. Použijte princip inkluze a exkluze podle počtu.

16. $(2,1,2,1,2,1,3,3) \equiv (6,3,5,2,4,1,8,7)$

17. Použije princip inkluze a exkluze, i-tý člen odpovídá počtu možností, jak udělat nepermutaci pouze s využitím i prvků z n-prvkové množiny.

18. Induktivně dokažte, že takové permutace mohou nanejvýš prohazovat některá sousedící čísla. Posléze si uvědomte, jak se množí králíci.

19. Stačí vzít $n-1$ transpozic vedlejších účastníků. Ukažte, že z nich už lze vygenerovat všechny transpozice, méně triviálně nestačí.

20. Vězni si mohou označit šuplíky svými jmény. Jména v šuplících jsou permutací jmen na nich. Vězeň se vždy otevře ten šuplík, na který ukazuje jméno z předchozího. Rozmyslete si, že neuspějí právě tehdy, když zmíněná permutace obsahuje cyklus délky alespoň $n+1$. pravděpodobnost takového jevu je ale celkem malá.

21. Takové permutace musí mít jeden cyklus délky n. Nějakým prohozením se začít musí, dál už stačí indukce.

22. Vezměte to indukcí ze správného konce, vyjde 2^{n-1}.

23. Rozmyslete si, jakým způsobem se permutace mohou skládat na jednotlivých prvcích. Posléze si permutaci rozložte na nezávislé cykly a v závislosti na n modulo 4 dopočtěte, jak to dopadne.

24. Dokažte, že optimum nastává, třeba když se pořadí studentů otočí. Vhodným přepojování cyklů stačí ukázat, že se při optimální konstrukci prohodil první a poslední student (popř. můžete sumu přepsat s užitím minim původních a nových pozic).

25. Postupujte po cyklech, rozmyslete si, jak přejdete z jednoho na jiný a jak ten poslední dokončíte. Prohození dvou nových lidí si šetřete na konec.

26. Každá taková volba odpovídá nějaké permutaci. Odhadněte shora počet permutací, které obsahují nějaká dvě políčka se stejnými čísla a ukažte, že je ostře menší než $n!$.

27. Vezměte všechny takové turnaje a shora odhadněte počet nepomlázkových permutací ve všech dohromady. Z toho vyplyne, že pomlázkových je v průměru alespoň tolik, jako zadaný zlomek.

28. Dívejte se na souřadnice bodů. Prvních d složek vyplňte souřadnicemi vrcholů P (P pak bude nutně projekcí našeho simplexu). Zbývá přidat libovolný konečný počet souřadnic tak, aby byly vzdálenosti všech vrcholů stejné. Co je na světě nejsymetričtější? Permutace!

29. Postupně přidávejte čísla $1, 2, \ldots, n$. U i-tého máte i možností, ty přidají nějaký pořet inverzí.

30. Předpokládejte, že každé jídlo je posunuté o jiný počet míst ve zvoleném směru modulo $2n$. Dojděte ke sporu porovnáním součtu pozic míst a jídel modulo $2n$.

31. Očíslujte si všechny karty kromě poslední čísly modulo $2n-1$ a lépe popište definované zobrazování.

32. Sčítejte počet vyhovujících k-tic přes k. Pro $k \neq p$ si permutace rozdělte do vhodných skupinek po p permutacích tak, aby v každé skupince vyhovovala právě jedna. Znalost Čínské zbytkové věty výhodou.

33. Pro kvadratické permutace stačí využít identitu $(i-1) \times (i+1) = i^2 - 1$ a zkonstruovat je. Pro kubické uvažujte největší mocninu dvojky menší rovnou n, ta by musela dělit $x^3 - 1$ pro nějaké x, rozkladem polynomu a snadnými odhady dojděte ke sporu s existencí dostatečně malého souseda.

34. Řešením jsou vskutku pouze ta špatná n, pro které je $\frac{n(n+1)}{2}$ čtverec. Pro ostatní čísla si posloupnost $(1, 2, ..., n)$ rozstříhejte na úseky mezi špatnými čísly a vymyslete, jak je na rozstříhnutých místech pozměnit.

35. Jak se změní počet cyklů permutace, vynásobíme-li ji libovolnou permutací?

36. Počet transpozic se sčítá, stejně jako parita.

37. Rozmyslete si, jak rozložit cyklus délky n na $n-1$ transpozic.

38. Každou permutaci na $1, 2, \ldots, n$ jde rozepsat jako složení transpozic sousedních prvků. Parita počtu prohození dvou konkrétních čísel odpovídá tomu, jaké je potom jejich vzájemné pořadí.

39. Ukažte, že f je jednoznačně určena hodnotou na jediné transpozici π. Rozmyslete si tedy, jak napsat libovolnou jinou transpozici tak, aby její znaménko záviselo pouze $\mathrm{sgn}(\pi)$. Je nutné rozebrat dva případy podle toho, kolik má hledaná transpozice společného s π.

40. Je jich přesně polovina. Stačí popárovat sudé a liché permutace do dvojic, třeba složením s pevnou transpozicí.

41. Neumíme. Každému stavu hry odpovídá jedna permutace 16-prvkové množiny. Obarvěte plán šachovnicově a dívejte se, jak souvisí barva volného políčka s paritou permutace.

42. Opravdu je to $\frac{1}{2}$, ale je to mírně technické. Nakreslete přes hrací plán hada, permutace posuzujte podle pořadí neprázdných polí na něm (pohyb prázdného políčka po hadovi toto pořadí nemění). Zbývá dokázat, že všechny pohyby prázdného políčka mimo směr hada už nagenerují všechny sudé permutace.

43. Případy $n \in 2, 3$ rozeberte zvlášť. Pro $n \geq 4$ vhodně použijte paritu a symetrii, které hrají ve prospěch Anně. Je opravdu nutné dávat pozor, abyste nenagenerovali celou S moc brzy.

44. Suma na levé straně je determinant vhodné matice a platí pro něj hodně pěkných vztahů. Pro přehlednost je dobré napsat si do n řádků šachovnice $n \times n$ vzestupně mocniny jednotlivých čísel a_i.

45. Vynásobením všech nenulových zbytků jedním (pevným) dostaneme jejich permutaci. Okamžitě proto $(p-1)! \equiv a^{p-1}(p-1)!$ modulo p.

46. Udělejte to samé, jako při důkazu Malé Fermatovy věty, uvažujte ale pouze zbytky nesoudělné s n.

47. Tvrzení stačí dokázat pro dvě nesoudělná čísla a_1, a_2. Násobení čísel modulo a_1 číslem a_2 je pouze propermutuje. Vezměte správný zbytek modulo a_1 a zkuste k němu násobky a_1 přičítat.

48. Pro kvadratické zbytky tvrzen plyne z Malé Fermatovy věty. Pro nezbytky se zamyslete, kolik nejvýše kořenů může mít polynom stupně $\frac{p-1}{2}$ nad zbytky modulo p.

49. Násobení a zbytky permutuje, převeďte problém na Eulerovo kritérium.

50. Rozmyslete si, že obě funkce dávají pro pevné p oba výsledky $-1, 1$ a navíc jsou obě multiplikativní. Že pro každé p dává permutace indukovaná nějakým $a$výsledek -1 plyne z existence primitivního prvku. S pomocí primitivního prvku si snadno rozmyslíme, že jsou obě funkce stejné.

51. Uvažujte tabulku $m \times n$ a permutaci odpovídající rozdání karet po řádcích a jejich následné sesbírání po sloupcích. Speciálně se dívejte na její znaménko (které odpovídá znaménku ze vztahu pro kvadratickou reciprocitu). Tuto permutaci lze navíc z Čínské zbytkové věty elegantně rozložit na součin dvou permutací, jejichž znaménka budou odpovídat současně permutování prvků modulo m násobením n (a naopak). Dokončete Zolotarevovým lematem.

Literatura a zdroje

[1] *Art of Problem Solving*, https://artofproblemsolving.com/
[2] Mirek Olšák: *Kombinatorické nepočítáni*, iKS
[3] Matt Baker: *Zolotarev's magical proof of the Law of Quadratic Reciprocity*
[4] Matoušek, Nešetřil: *Kapitoly z diskrétní matematiky*

A další zdroje napříč internetem.

Burnsideovo lemma

VIKI NĚMEČEK

ABSTRAKT. Kombinatorická úloha často žádá spočítat množství různých obarvení, uspořádání a podobně. Takové kalkulace jsou předmětem běžné středoškolské výuky. Potíž však nastane, jakmile je k úloze dodatek: „Obarvení lišící se pouze otočením/překlopením/posunutím považujeme za identická.“ A právě Burnsideovo lemma dává nástroj, jak se s tímto vypořádat. Na rozdíl od běžných přednášek o Burnsideově lemmatu se tento příspěvek snaží minimalizovat používání pojmů z teorie grup a nahradit je pojmy pokud možno přirozenými.

Úmluva 1. 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 použít – někdy je jednodušší si rozmyslet všechny možnosti a situaci šikovně zjednodušit.

Úloha 2. Kolika způsoby můžeme přiřadit stěnám krychle čísla 1 až 6 (každé právě jednou) tak, aby součet hodnot protilehlých stěn byl vždy roven sedmi?

Úloha 3. Kolik je možností, jak obarvit stěny krychle dvěma barvami?

Úloha 4. Kolik existuje neizomorfních grafů na čtyřech vrcholech?

Úloha 5. Kolik existuje různých sítí krychle?

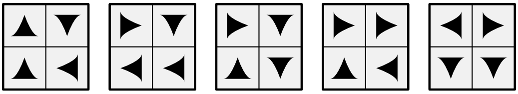
Úloha 6. Má více sítí krychle, nebo pravidelný osmistěn?

Úloha 7. 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:

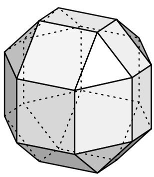
(i) Kdykoli složíme (provedeme po sobě) dva pohyby z G, dostaneme opět pohyb z G.
(ii) V G musí existovat nepohyb – pohyb, který vše nechá na místě.
(iii) Pro každý pohyb $p \in G$ existuje opačný pohyb p^{-1}, který při složení (v kterémkoli pořadí) s původním pohybem p dá nepohyb.

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

Úloha 9. Kolika způsoby můžeme nakreslit šipku směrem k jedné hraně na každou z 26 stěn následujícího tělesa (krychle se seříznutými hranami a vrcholy)?



Úloha 10. Na špíz můžeme napíchnout vždy maso, slaninu, nebo cibuli – celkem napíchneme deset kousků. Kolik existuje různých špízů (konce špejle jsou nerozlišitelné)?

Úloha 11. Kolik bude náhrdelníků z úlohy 8, 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 12. Kolik náhrdelníků vyjde v úloze 8, budeme-li mít k dispozici dvanáct černých a dvanáct bílých korálků?

Úloha 13. 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 14. O kolik se zvětší výsledek úlohy 9, pokud budeme

(i) trojúhelníkové stěny barvit jednou ze tří barev namísto kreslení šipky,
(ii) čtyřúhelníkové stěny sousedící s trojúhelníkovými barvit čtyřmi barvami namísto kreslení šipky,
(iii) čtyřúhelníkové stěny nesousedící s trojúhelníkovými barvit čtyřmi barvami namísto kreslení šipky?

Úloha 15. Kolik je možností, jak obarvit právě patnáct z třiceti hran dvacetistěnu?

Úloha 16. 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

2. 2

3. 10

4. 11

5. 20

6. Stějně (dá se popsat bijekce).

7. 30

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

9. $2^{33}\cdot 3^{7}$

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

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

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

13. $(2^{81} + 8 \cdot 2^{27} + 72 \cdot 2^{9})/81$

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

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

Literatura a zdroje

Tento příspěvek je takřka beze změn převzat od *Mirka Olšáka*, který jej vytvořil na soustředění v Zásadě (2014) a kterému tímto děkuji (a toto poděkování je zkopírované zpod jednoho Davidova příspěvku).

AG nerovnost

MARIAN POLJAK

ABSTRAKT. V příspěvku jsou obsažena základní i pokročilá užití AG nerovnosti.

Účinné používání nerovností patří k základním dovednostem člověka účastnícího se matematických soutěží. Přestože je tento text zaměřen primárně na řešení nerovností, soustavy rovnic jsou s jejich pomocí také často hračka a silné odhady nezřídka vyřeší i nealgebraickou úlohu. Jednou ze (dvou) stěžejních nerovností, je nerovnost mezi aritmetickým a geometrickým průměrem (zkráceně AG nerovnost). V této dvojpřednášce se s ní seznámíme a ukážeme si všechny možné nekalé triky, které s ní můžeme provádět.

Věta 1. (AG nerovnost) *Pro libovolná nezáporná čísla $x_1, x_2, \ldots, x_n$ platí*

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

Poznámka 2. Rovnost nastává právě tehdy, když existuje $x > 0$, že $x_1 = x_2 = \cdots = x_n$.

Příklad 3.

(1) $a^2 + b^2 \geq 2ab$,
(2) $(a + b + c)(\frac{1}{a} + \frac{1}{b} + \frac{1}{c}) \geq 9$,
(3) $2x^3 + y^3 \geq 3x^2 y$.

Cvičení 4. (Základní fígle.) Pro x, y, z kladná dokažte:

(1) $\frac{a}{b} + \frac{b}{a} \geq 2$,
(2) $x^3 + y^3 + z^3 \geq 3xyz$,
(3) $x^2 + \frac{2}{x} \geq 3$,
(4) $\frac{x^3}{yz} + y + z \geq 3x$,
(5) $\frac{x}{y} + \frac{y}{z} + \frac{z}{x} \geq 3$,
(6) $2(x + y + z)(x^2 + y^2 + z^2) \geq x^3 + y^3 + z^3 + 15xyz$,
(7) $\frac{z}{x} + \frac{x}{y+z} + \frac{y}{z} \geq 2$.

Příklad 5. Nechť a, b jsou kladná reálná čísla taková, že $a > b$. Najděte minimum výrazu

$$a + \frac{1}{b(a-b)}.$$

Příklad 6. Najděte všechna kladná reálná řešení (a, b, c, d) splňující $a+b+c+d = 12$ a $abcd = 27 + ab + ac + ad + bc + bd + cd$.

Sčítání AG nerovností a míchání členů

Jak jste si možná všimli, většina dosud dokazovaných nerovností měla společnou jednu věc – členů na jedné straně nerovnosti bylo hodně, zatímco na druhé straně jeden. To samozřejmě (při letmém pohledu na AG nerovnost) není náhoda. Co kdybychom ale chtěli AG utilizovat i pro boj s následující nerovností?

$$x^3 + y^3 + z^3 \geq x^2y + y^2z + z^2x$$

Není těžké ověřit, že nerovnost (konkrétně její trojnásobek) můžeme "namíchat" součtem nerovnosti $2x^3 + y^3 \geq 3x^2y$ a jejích cyklických záměn.

Ukažme si, jak na správné namíchání přijít!

Příklad 7. Dokažte, že pro kladná reálná x, y, z platí

$$x^3y + y^3z + z^3x \geq x^2yz + y^2zx + z^2xy.$$

Cvičení 8. (Míchací.) Pro x, y, z kladná dokažte (a určete, kdy nastává rovnost):

(1) $x^2 + y^2 + z^2 \geq xy + yz + zx$,
(2) $x^4 + y^4 + z^4 \geq x^3y + y^3z + z^3x$,
(3) $x^4y + y^4z + z^4x \geq x^2y^2z + y^2z^2x + z^2x^2y$,
(4) $\frac{x^2}{y} + \frac{y^2}{z} + \frac{z^2}{x} \geq x + y + z$,
(5) $x^7 + 1 \geq x^4 + x^3$,
(6) $\frac{x^3}{y} + \frac{y^3}{z} + \frac{z^3}{x} \geq xy + yz + zx$.

Poslední cvičení ukázala, že rozložit nepříjemnou nerovnost na součet několika lehčích nerovností může často vést k řešení. Musíme si však dát pozor na to, aby tyto lehčí nerovnosti platily. Pojďme si techniku "Rozděl a panuj!" ukázat na různorodějších příkladech!

Příklad 9. Dokažte, že pro kladná reálná x, y, z platí

$$a^3 + b^3 + c^3 + 6 \geq 3(a + b + c).$$

Příklad 10. Dokažte, že pro kladná reálná x, y, z platí

$$(x + y)(y + z)(z + x) \geq 8xyz.$$

Příklad 11. Pro $a, b, c > 0$ dokažte nerovnost

$$\frac{2}{3}(a+b+c) \geq \sqrt[3]{ab} + \sqrt[3]{bc} + \sqrt[3]{ca} - 1.$$

Poznámka 12. Pomaličku začíná přituhovat a budeme bojovat se složitějšími výrazy. Abychom se v úpravách neztratili, vyzbrojíme se znakem tzv. *cyklické sumy*. Funguje to nějak takto: $\sum_{cyc} a = a + b + c$, $\sum_{cyc} xy^2 = xy^2 + yz^2 + zx^2$. Například jedno z prvních cvičení lze zapsat následovně:

$$2\left(\sum_{cyc} x\right)\left(\sum_{cyc} x^2\right) \geq \sum_{cyc} x^3 + 15xyz.$$

Lehké odhady na těžké nerovnosti

Asi největší využití AG nerovnosti spočívá v tvorbě odhadů, "mezivýrazů", které vypadají rozumněji než levá a pravá strana a které se mezi ně proto pokoušíme vklínit. Mnohdy je vztah mezi levou a pravou stranou nerovnosti natolik slabý, že i ne moc dobrý odhad úlohu vyřeší. U těžších nerovností jsou silné odhady často nutností (jejich používání vyžaduje notnou dávku praxe). Obojí si ukážeme.

Příklad 13. Pro $a, b, c > 0$ dokažte nerovnost

$$\sum_{cyc} \frac{1}{a^3 + b^3 + abc} \leq \frac{1}{abc}.$$

Poznámka 14. (Nenápadná, ale důležitá.) Při dokazování neostrých nerovností má smysl používat pouze takové odhady, u kterých se zachovají případy rovnosti.

Příklad 15. Pro $a, b, c > 0$ dokažte nerovnost

$$(a^5 - a^2 + 3)(b^5 - b^2 + 3)(c^5 - c^2 + 3) \geq (a+b+c)^3.$$

(USAMO, 2004)

AG vs. zlomky

Na úlohy se zlomky je většinou silnou zbraní Cauchyho-Schwarzova nerovnost (druhá ze stěžejních nerovností). Nicméně i AG lze na zlomky použít překvapivě dobře – stačí sečíst zlomek s jeho jmenovatelem (funguje zejména u slabších nerovností). Při řešení nezapomeňme na poznámku o rovnosti!

Příklad 16. Pro $a, b, c > 0$ dokažte nerovnost

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

Příklad 17. Dokažte, že pro každá $a, b, c > 0$ platí

$$\sum_{cyc} \frac{a^3}{(a+b)(a+c)} \geq \frac{a+b+c}{4}.$$

Příklad 18. Pro a, b, c kladná dokažte

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

Úlohy na procvičení (triviální až středně obtížné)

Úloha 19. Určete všechna kladná reálná x, y, z splňující $x + y + z = 6$ a $xyz = 8$.

Úloha 20. Dokažte, že pro každé přirozené $n > 1$ platí

$$\left(\frac{1}{2} + \frac{2}{3} + \cdots + \frac{n}{n+1}\right)^n > \frac{n^n}{n+1}.$$

Úloha 21. Dokažte, že pro $0 \leq a \leq b \leq c$ platí $(a+3b)(b+4c)(c+2a) \geq 60abc$.

Úloha 22. Dokažte, že pro kladná reálná x, y, z platí

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

Úloha 23. Ukažte, že pro každou trojici kladných čísel a, b, c splňující $abc = 1$ platí

$$\sum_{cyc} \frac{ab}{a^5 + b^5 + ab} \leq 1.$$

(IMO shortlist, 1996)

Úloha 24. Dokažte, že pro kladná reálná a, b, c splňující $a + b + c = 3$ platí

$$a^b b^c c^a \leq 1.$$

Úloha 25. Dokažte, že pro $a, b, c > 0$ splňující $abc = 1$ platí

$$\sum_{cyc} \frac{a^3}{(1+a)(1+b)} \geq \frac{3}{4}.$$

Úloha 26. Na každé straně čtverce o straně 1 zvolíme bod. Tyto body vytvoří čtyřúhelník o stranách a, b, c, d. Dokažte, že platí $2 \leq a^2 + b^2 + c^2 + d^2 \leq 4$ a $2\sqrt{2} \leq a + b + c + d \leq 4$.

Úloha 27. Dokažte, že pro $a, b, c > 0$ platí

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

Těžší úlohy

Úloha 28. Pro a, b, c kladná platí $a + b + c = 1$. Dokažte, že

$$\sqrt{a^{1-a}b^{1-b}c^{1-c}} \leq \frac{1}{3}.$$

(Rakousko, 2008)

Úloha 29. Nechť a, b, c jsou kladná reálná a platí $a+b+c \geq 6$. Najděte minimum výrazu

$$\sum_{cyc} a^2 + \sum_{cyc} \frac{a}{b^2 + c + 1}.$$

(Uzbekistán NMO)

Úloha 30. Ukažte, že pro každé přirozené n a každou n-tici kladných reálných čísel $x_1, x_2, \ldots, x_n$ platí

$$(1 + x_1)(1 + x_1 + x_2) \cdots (1 + x_1 + x_2 + \cdots + x_n) \geq \sqrt{(n + 1)^{n+1} x_1 x_2 \ldots x_n}.$$

(35. ročník MKS, finální myšmaš)

Úloha 31. Nechť $a, b, c > 0$ a $a + b + c = 1$. Dokažte, že platí

$$\sum_{cyc} \frac{a^3 + bc}{a^2 + bc} \geq 2.$$

Úloha 32. Nechť $n > 2$ a $a_2, a_3, \ldots, a_n$ jsou kladná reálná čísla splňující podmínku $a_2 a_3 \cdots a_n = 1$. Dokažte, že platí

$$(1 + a_2)^2 (1 + a_3)^3 \cdots (1 + a_n)^n > n^n.$$

(IMO 2, 2012)

Úloha 33. Nechť $a, b, c > 0$ a $abc = 1$. Dokažte, že platí

$$a^4 + b^4 + c^4 + a + b + c + \frac{2a}{b^2 + c^2} + \frac{2b}{a^2 + c^2} + \frac{2c}{a^2 + b^2} \geq 9.$$

Úloha 34. Mějme ostroúhlý trojúhelník ABC a jemu opsanou kružnici se středem O a poloměrem R. Označme D druhý průsečík přímky AO s kružnicí opsanou BOC, E druhý průsečík přímky BO s kružnicí opsanou AOC a F druhý průsečík přímky CO s kružnicí opsanou AOB. Dokažte

$$|OD| \cdot |OE| \cdot |OF| \geq 8R^3.$$

Úloha 35. Nechť $a, b, c > 0$ a $abc = 1$. Dokažte, že platí

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

Úloha 36. Nechť $a, b, c > 0$ a platí

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

Dokažte, že platí

$$2(a+b+c) \geq \sqrt[3]{7a^2b+1} + \sqrt[3]{7b^2c+1} + \sqrt[3]{7c^2a+1},$$

a určete, pro které trojice (a, b, c) nastává rovnost.

Úloha 37. Nechť $a, b, c > 0$ a $a+b+c = 1$. Dokažte, že platí

$$\sum_{cyc} \frac{\sqrt{a^2+abc}}{c+ab} \leq \frac{1}{2\sqrt{abc}}.$$

Literatura a zdroje

[1] Michal Rolínek, Pavel Šalom: *Zdolávání nerovností*, Univerzita J.E. Purkyně, 2012.

[2] Samin Riasat: *Basics of Olympiad Inequalities*.

Extremální princip

Martin Sýkora

Abstrakt. Příspěvek obsahuje několik příkladů vhodných na procvičení jedné ze základních důkazových metod – extremálního principu.

Extremální princip je základní důkazovou metodou. Spočívá v tom, že nalezneme něco, co je v nějakém slova smyslu maximální (nebo minimální) a zamyslíme se, co z toho vyplývá. Velmi často kombinujeme extremální princip s důkazem sporem. Například uvážíme nejdelší úsečku a ukážeme, že pak by musela existovat i nějaká delší, čímž získáme spor. Pojďme si ukázat použití extremálního principu na úloze.

Úloha. V nekonečných rovinatých tajgách severního Arendellu rostou v pravidelné čtvercové síti zakrslé smrky, přičemž výška každého je průměrem výšek všech čtyř kolem stojících stromů. Pokud výšky nabývají přirozených hodnot, ukažte, že jsou stromy stejně vysoké.

Řešení. (Náznak) Protože výšky stromů jsou přirozené, existuje (ne nutně jeden) strom s nejmenší výškou. Nějaký takový si vyberme a označme S. Všichni čtyři jeho sousedi musí mít výšku stejnou nebo vyšší. Kdyby byl ale nějaký vyšší, výška stromu S by nebyla průměrem výšek okolních stromů. Proto všichni jeho sousedi mají stejnou výšku jako S. Indukcí pak snadno ukážeme, že všechny stromy jsou stejně vysoké.

Nyní se můžeme pustit do samostatného počítání.

Příklady

Příklad 1. Olaf dokázal, že prvočísel je konečně mnoho. Ukažte, že se spletl.

Příklad 2. Města na Jižních ostrovech jsou vystavena v takových rozestupech, že trojúhelník s vrcholy v libovolných třech městech má rozlohu menší než 19 000 km^2. Ukažte, že všechna města se vejdou na plochu menší, než má Česká republika.[1]

Příklad 3. Na Jižních ostrovech je konečně mnoho věží, přičemž každá přímka, která prochází skrz dvě věže, prochází i nějakou třetí věží. Ukažte, že věže leží v jedné přímce.

[1] Dokonce se vejdou na trojúhelníkovou plochu menší než 76000 km^2.

Příklad 4. Hans dal služebné za úkol najít aspoň jedno celočíselné řešení rovnice $a^2 + b^2 = 3(c^2 + d^2)$. Pomozte jí a najděte dokonce všechna taková řešení.

Příklad 5. V Arendellu jsou všechny silnice jednosměrné a každá dvě města jsou spojena právě jednou silnicí. Ukažte, že existuje město, do kterého se dá dostat z každého jiného buď přímo, nebo po dvou silnicích.[2]

Příklad 6. Na Elsině korunovaci se každý pohádal nejvýše se třemi lidmi. Je možné účastníky slavnosti rozdělit do dvou skupin tak, aby každý měl ve své skupině nejvýše jednoho jiného člověka, se kterým se pohádal?

Příklad 7. Sedm konšelů z Jižních ostrovů sedí kolem kruhového stolu. Každý před sebou má pohár s mlékem. Dohromady mají mléka tři litry. Nejdřív první z nich vstane a rozdělí své mléko rovnoměrně mezi ostatní. Pak postupně, proti směru hodinových ručiček, totéž udělají i zbývající konšelé. Když skončí, má každý z nich tolik mléka, kolik měl na začátku. Kolik to je?

Příklad 8. Anna s Kristoffem hráli 3D šachy a přitom je napadla otázka, kolik nejméně věží je potřeba, aby ohrožovaly všechna políčka šachovnice $n \times n \times n$. Kolik to je?

Příklad 9. Města v Arendellu neleží na jedné přímce. Ukažte, že pak existuje přímka, která prochází jen přes dvě z těchto měst. Platilo by to, i kdyby bylo měst nekonečně mnoho?

Příklad 10. Olaf dokázal, že prvočísel ve tvaru $6n - 1$ je konečně mnoho. Ukažte, že se spletl.

Příklad 11. V Arendellu je n hradů a n studen. Vojenský analytik rozhodl, že by bylo vhodné každý hrad spojit s jednou studnou přímou cestou aniž by se cesty křížily. Je možné toto provést?

Příklad 12. Po drtivém útoku Jižních ostrovů na americký Pentagon byla podstava této budovy zdeformována do tvaru obecného konvexního pětiúhelníku. Ukažte, že i tak z ní lze vybrat tři úhlopříčky, z nichž lze vytvořit trojúhelník.

Příklad 13. Ukažte, že každý mnohostěn má alespoň dvě stěny se stejným počtem hran.

Příklad 14. Elsa namalovala na rovinné plátno $n > 3$ přímek takových, že žádné dvě z nich nejsou rovnoběžné a průsečíkem každých dvou prochází i třetí přímka. Ukažte, že se pak všechny protínají v jednom bodě.

Literatura a zdroje

[1] Arthur Engel: *Problem-Solving Strategies*, Springer, 1997.
[2] Alča Skálová: *Extremální princip*, Blansko-Obůrka, 2011.

[2] Navíc, pokud se do žádného města nedá dostat přímo, taková města jsou aspoň tři.

Goniometrické substituce

Martin Sýkora

Abstrakt. V příspěvku jsou uvedeny základní vlastnosti geometrických funkcí a příklady vhodné na nácvik techniky goniometrických substitucí.

Na přednášce si ukážeme, jak je možné řešit některé nepříjemné algebraické úlohy pomocí goniometrických substitucí. Základní ideou je nahrazení neznámých goniometrickými funkcemi a následné využití známých goniometrických identit. Ještě než se ale pustíme do počítání příkladů, zopakujme si, co bychom o goniometrických funkcích měli vědět.

Nejběžněji využívané goniometrické funkce jsou sinus, kosinus, tangens a kotangens a platí pro ně (mimo jiné) následující:

Tvrzení. *Pro funkce sinus a kosinus platí:*

(i) *Definiční obor obou funkcí jsou všechna reálná čísla.*
(ii) *Jejich obor hodnot je interval $\langle -1, 1\rangle$.*
(iii) *Obě dvě funkce jsou 2π-periodické.*
(iv) *Sinus je na intervalu $\left\langle -\frac{\pi}{2}, \frac{\pi}{2}\right\rangle$ rostoucí a na $\left\langle \frac{\pi}{2}, \frac{3\pi}{2}\right\rangle$ klesající.*
(v) *Kosinus je na $\langle -\pi, 0\rangle$ rostoucí a na $\langle 0, \pi\rangle$ klesající.*

Funkce *tangens* a *kotangens* jsou na svých definičních oborech definované po řadě jako

$$\operatorname{tg} a = \frac{\sin a}{\cos a}, \operatorname{cotg} a = \frac{\cos a}{\sin a}.$$

Tvrzení. *Pro funkce tangens a kotangens platí:*

(i) *Definiční obor funkce tangens je $\mathbb{R} \setminus \left\{k\frac{\pi}{2}; k \in \mathbb{Z}\right\}$ a funkce kotangens $\mathbb{R} \setminus \left\{k\pi; k \in \mathbb{Z}\right\}$.*
(ii) *Obor hodnot obou funkcí jsou všechna reálná čísla.*
(iii) *Obě dvě funkce jsou π-periodické.*
(iv) *Tangens je na intervalu $(-\frac{\pi}{2}, \frac{\pi}{2})$ rostoucí.*
(v) *Kotangens je na intervalu $(0, \pi)$ klesající.*

Dále pro goniometrické funkce platí následující vztahy:

Tvrzení. *Pro všechna $a, b \in \mathbb{R}$, pro která mají dané výrazy smysl (tj. nedělíme* *nulou) platí:*

$$\sin\left(\tfrac{\pi}{2}-a\right)=\cos a, \qquad \cos\left(\tfrac{\pi}{2}-a\right)=\sin a,$$
$$\sin(-a)=-\sin a, \qquad \cos(-a)=\cos a,$$
$$\operatorname{tg}(-a)=-\operatorname{tg} a, \qquad \operatorname{cotg}(-a)=-\operatorname{cotg} a,$$
$$\sin^2 a+\cos^2 a=1,$$
$$\sin(a\pm b)=\sin a\cdot\cos b\pm\sin b\cdot\cos a,$$
$$\cos(a\pm b)=\cos a\cdot\cos b\mp\sin a\cdot\sin b,$$
$$\operatorname{tg}(a\pm b)=\frac{\operatorname{tg} a\pm\operatorname{tg} b}{1\mp\operatorname{tg} a\cdot\operatorname{tg} b},$$
$$\operatorname{cotg}(a\pm b)=\frac{\operatorname{cotg} a\cdot\operatorname{cotg} b\mp 1}{\operatorname{cotg} b\pm\operatorname{cotg} a},$$
$$\sin a\pm\sin b=2\sin\left(\frac{a\pm b}{2}\right)\cdot\cos\left(\frac{a\mp b}{2}\right),$$
$$\cos a+\cos b=2\cos\left(\frac{a+b}{2}\right)\cdot\cos\left(\frac{a-b}{2}\right),$$
$$\cos a-\cos b=-2\sin\left(\frac{a+b}{2}\right)\cdot\sin\left(\frac{a-b}{2}\right).$$

Příklady na rozjezd

Následující příklady jsou poměrně jednoduché a přímočaré – stačí najít vhodnou substituci a úloha se vzdává.

Příklad 1. Kristoff dostal jako svatební dar reálné číslo K a Anna zase A, přičemž platilo, že $K^2+A^2=1$. Samou láskou svá čísla vynásobili. Jakého nejvyššího a nejnižšího výsledku mohli dosáhnout?

Příklad 2. Elsa si vymyslela čtyři navzájem různá reálná čísla z intervalu $(0,1)$. Ukažte, že Anna si z nich mohla vybrat dvě čísla x, y taková, že

$$0<x\sqrt{1-y^2}-y\sqrt{1-x^2}<\frac{1}{2}.$$

Příklad 3. Lars chtěl dát své mamince jako dárek 100-prvkovou množinu reálných čísel S s tou vlastností, že když x patří do S, tak i číslo $2x^2-1$ patří do S. Mohl ji na jarmarku sehnat, nebo takové množiny neexistují?

Příklad 4. Hans se rozhodl pro libovolné reálné číslo a definovat posloupnost vztahem $x_1=a$ a $x_{n+1}=1/(1-x_n)-1/(1+x_n)$. Posloupnost vytvářel až do chvíle, kdy pro nějaké k poprvé nastalo $x_k=\pm1$. Číslo k potom nazval délkou posloupnosti. Kolik existuje posloupností délky osm?

Příklad 5. Dokažte, že rekurentně zadaná posloupnost splňující vztah

$$x_{n+1} = \frac{\sqrt{3}x_n - 1}{x_n + \sqrt{3}}$$

je – stejně jako roční období na jižních ostrovech – periodická.

Příklad 6. Astrologové zjistili, že průměrné roční teploty v Arendellu se řídí rekurentní posloupností danou předpisem

$$x_{n+1} = \frac{1 + x_n}{1 - x_n}.$$

Historikové také vzpomínají, že ve středověku v roce 1323 za ohnivé královny Asly byla teplota 2013 °C. Jaké oblečení byste pro návštěvu Arendellu zvolili letos?

Příklad 7. Elsa se pohádala s Larsem o to, jestli mezi každými pěti reálnými čísly existují dvě taková čísla a, b, pro která platí

$$|ab + 1| > |a - b|.$$

Existují, nebo ne?

Příklad 8. Kristoff hledal nějakou posloupnost splňující pro všechna přirozená n vztah $a_{n+1} = \frac{c+a_n}{1-ca_n}$. Mohl najít takovou, která by měla prvních 2016 členů kladných a 2017. člen záporný?

Nerovnosti

Goniometrické substituce lze využít i při dokazování některých typů nerovností. Substituce ale bývá ale jen začátkem a následně bývá potřeba využít nějakou další zbraň, typicky AG nerovnost, nebo Jensenovu nerovnost, kterou budeme na přednášce používat v následujícím znění bez důkazu.

Tvrzení. (Jensenova nerovnost) *Buď f konvexní funkce na intervalu I, $x_1, x_2, \dots, x_n \in I$ a $\lambda_1, \lambda_2, \dots, \lambda_n \in \langle 0, 1\rangle$ tak, že $\lambda_1 + \lambda_2 + \cdots + \lambda_n = 1$. Pak platí*

$$\lambda_1 f(x_1) + \lambda_2 f(x_2) + \cdots + \lambda_n f(x_n) \geq f(\lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n).$$

Je-li f na I konkávní, pak

$$\lambda_1 f(x_1) + \lambda_2 f(x_2) + \cdots + \lambda_n f(x_n) \leq f(\lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n).$$

Následující tvrzení nám – jak uvidíme z příkladů – pomohou využít goniometrické substituce a zbavit se někdy neintuitivních podmínek.

Tvrzení. *Mějme trojúhelník s vnitřními úhly a, b, c, potom platí:*

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

Tvrzení. *Mějme ostroúhlý trojúhelník s vnitřními úhly a, b, c, potom platí:*

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

Poznámka. Tvrzení platí i pro obecný trojúhelník.

Tvrzení. *Nechť jsou čísla $a, b, c \in (0, \frac{\pi}{2})$, pak a, b, c jsou úhly trojúhelníka právě tehdy, když platí následující rovnost:*

$$\operatorname{tg} a+\operatorname{tg} b+\operatorname{tg} c=\operatorname{tg} a\operatorname{tg} b\operatorname{tg} c.$$

Tvrzení. *Uvažme čísla $a, b, c \in (0, \pi)$, pak a, b, c jsou úhly trojúhelníka právě tehdy, když platí následující rovnost:*

$$\operatorname{tg}\frac{a}{2}\operatorname{tg}\frac{b}{2}+\operatorname{tg}\frac{b}{2}\operatorname{tg}\frac{c}{2}+\operatorname{tg}\frac{c}{2}\operatorname{tg}\frac{a}{2}=1.$$

Další příklady, se kterými potřebuje Olaf pomoci

Příklad 9. Buďte x, y, z kladná reálná čísla taková, že $x+y+z=xyz$. Dokažte:

$$\frac{1}{\sqrt{1+x^2}}+\frac{1}{\sqrt{1+y^2}}+\frac{1}{\sqrt{1+z^2}}\leq\frac{3}{2}.$$

(Korea 1998)

Příklad 10. Mějme kladná reálná čísla x, y, z taková, že platí $x+y+z=xyz$. Ukažte:

$$xy+yz+xz\geq 3+\sqrt{1+x^2}+\sqrt{1+y^2}+\sqrt{1+z^2}.$$

Příklad 11. Nechť a, b, c, d jsou kladná reálná čísla taková, že

$$\frac{1}{1+a^4}+\frac{1}{1+b^4}+\frac{1}{1+c^4}+\frac{1}{1+d^4}=1.$$

Dokažte, že $abcd\geq 3$. (Lotyšsko 2002)

Příklad 12. V oboru reálných čísel řešte soustavu rovnic:

$$3(x^2+1)yz=4(y^2+1)xz=5(z^2+1)xy,$$

kde platí $xy+yz+xz=1$.

Příklad 13. Mějme kladná reálná čísla x, y, z splňující $x+y+z=xyz$. Dokažte, že potom platí:

$$\frac{x}{\sqrt{1+x^2}}+\frac{y}{\sqrt{1+y^2}}+\frac{z}{\sqrt{1+z^2}}\leq\frac{3\sqrt{3}}{2}.$$

Literatura a zdroje

[1] Marta Kossaczká: *Goniometrické Substitúcie*, Uhelná Příbram, 2014.

Čínská zbytková věta

Lucien Šíma

Abstrakt. Na přednášce si ukážeme Čínskou zbytkovou větou a demonstrujeme její využití na několika olympiádních příkladech.

Pohádka

Generál Koňadra by rád zjistil, kolik má vojáků. Svým bystrým okem odhadne, že jich zřejmě nebude více než 210. Jelikož je líný vojáky počítat, nařídí jim, aby se rozdělili do skupin. Když je rozdělil do skupin po dvou či po třech, zbyl jeden osamocený voják. Když je rozdělil do skupin po pěti či po sedmi, zbyli nerozdělení tři vojáci. Po snadných úvahách mu došlo, kolik vojáků má.

Soustava kongruencí

Označme si x počet vojáků. Generál se vlastně snažil vyřešit následující soustavu kongruencí:

$$\begin{aligned} x &\equiv 1 \pmod 2,\\ x &\equiv 1 \pmod 3,\\ x &\equiv 3 \pmod 5,\\ x &\equiv 3 \pmod 7. \end{aligned}$$

Je možné vždy najít nějaké řešení pro libovolný počet kongruencí? Kolik takových řešení bude? Odpovědí na tyto otázky je následující věta.

Věta. (Čínská zbytková věta) *Nechť $n_1, \dots, n_k \in \mathbb{N}$ jsou po dvou nesoudělná čísla a $r_1, \dots, r_k \in \mathbb{N}$. Pak soustava kongruencí*

$$\begin{aligned} x &\equiv r_1 \pmod{n_1},\\ x &\equiv r_2 \pmod{n_2},\\ &\dots\\ x &\equiv r_k \pmod{n_k}, \end{aligned}$$

má právě jedno řešení x takové, že 0 $\leq x < n_1 \cdot \ldots \cdot n_k$.

Příklady

Příklad 1. Zjistěte poslední tři číslice čísla 249^{19}.

Příklad 2. Dokažte, že pro každé $n \in \mathbb{N}$ existuje n-tice po sobě jdoucích čísel takových, že pro každé z nich existuje prvočíslo $p \in \mathbb{N}$, že $p^2 \mid n$.

Příklad 3. Dokažte, že pro každé $n \in \mathbb{N}$ existuje n-tice po sobě jdoucích složených čísel.

Příklad 4. Jsou dána čísla $a_1, \dots, a_n$. Dokažte, že existuje K $\in \mathbb{N}$ takové, že $K \cdot a_i$ je mocnina pro každé $i \in (1, \dots, n)$.

Příklad 5. Dokažte, že pro každé $n \in \mathbb{N}$ existuje n-tice přirozených čísel takových, že součet libovolného počtu z nich je mocnina.

Příklad 6. Zkonstruujte nekonečnou rostoucí posloupnost a_n takovou, že pro každé $k \in \mathbb{N}$ obsahuje posloupnost $a_n + k$ pouze konečně mnoho prvočísel.

(Česká MO 1997)

Příklad 7. Dokažte, že pro každé $n \in \mathbb{N}$ existuje n-tice po dvou nesoudělných čísel $k_1, \dots, k_n > 1$ taková, že $k_1 \cdot k_2 \cdot \dots \cdot k_n - 1$ je součin dvou po sobě jdoucích přirozených čísel. (USAMO 2008)

Příklad 8. Dokažte, že pro každé $n \in \mathbb{N}$ existují $a, b \in \mathbb{N}$ takové, že $n \mid 4a^2+9b^2-1$.

Příklad 9. Mřížový bod v rovině nazveme *neviditelný*, pokud se na úsečce spojující jej s počátkem nachází další mřížový bod. Dokažte, že pro každé $n \in \mathbb{N}$ existuje čtverec o rozměrech $n \times n$ se stranami rovnoběžnými s osami, jehož n^2 mřížových bodů je neviditelných. (Taiwan 2012)

Příklad 10. Rozhodněte, zda existuje posloupnost, která obsahuje každé přirozené číslo právě jednou, a pro každé k $\in \mathbb{N}$ platí, že $k \mid a_1 + a_2 + \cdots + a_k$.

(Ruská MO 1995)

Příklad 11. Dokažte, že pro každá dvě různá prvočísla p, q platí, že: $p^{q-1}+q^{p-1} \equiv 1 \pmod{pq}$.

Příklad 12. Nechť $f : \mathbb{N} \to \mathbb{N}$ je funkce splňující:

(1) $\mathrm{NSD}(f(m), f(n)) = 1 \Leftrightarrow \mathrm{NSD}(m, n) = 1$,
(2) $n \leq f(n) \leq n + 2017$ pro každé $n \in \mathbb{N}$.

Dokažte, že pro každé $n \in \mathbb{N}$ a prvočíslo p platí, že $p \mid f(n)$ implikuje $p \mid n$.

(TSTST 2012/3)

Návody

1. $1000 = 8 \cdot 125$

2. Zvolte si libovolných n prvočísel.

3. Zvolte si libovolných $2n$ prvočísel.

4. Koukněte se na prvočíselné rozklady čísel v n-tici a doplňte je na mocninu.

5. Uvědomte si, že se jedná o důsledek příkladu 4.

6. Pro každé k zvolte prvočíslo p_k, které bude dělit všechny členy $a_n + k$ až na konečně mnoho.

8. Použijte rozklad n na prvočinitele.

9. Chceme, aby souřadnice všech těchto bodů byly soudělné. Zvolme n^2 prvočísel a nalezněme souřadnice levého dolního bodu $[x, y]$, aby tomu tak bylo.

10. Zkonstruujte jí rekurzivně. Přidávejte členy po dvou.

11. Použijte Malou Fermatovu větu.

12. Hint není. Přece jenom to má být nejtěžší úloha, ne?

Literatura a zdroje

[1] Titu Andrescu, Dorin Andrica: *Number Theory*, Springer, 2009.
[2] David Hruška: *Čínská zbytková věta*, Uhelná Příbram, 2014.
[3] Evan Chen: *The Chinese Remainder Theorem*, *web.evanchen.cc/handouts/CRT/CRT.pdf*

Minimální kostry

Štěpán Šimsa

Abstrakt. Cílem příspěvku je seznámit s tématem minimálních koster, konkrétně s teoretickými základy, algoritmy a jejich analýzou.

Problém. (Minimální kostra) Je zadaný graf G s množinou vrcholů V a hranami E ohodnocený vahami $w : E \to \mathbb{R}$. Naším cílem je najít souvislý podgraf grafu G (na stejné množině vrcholů), který má ze všech takových grafů minimální součet vah vybraných hran.

Cvičení. Minimální kostra nemusí existovat jedna. Víme-li ale navíc, že jsou váhy hran po dvou různé, už jednoznačná je.

Teorie

Definice. Buď $T \subseteq G$ nějaká kostra grafu G. Pak:

- $T[x, y]$ bude značit cestu v T, která spojuje x a y. (Cestou opět míníme množinu hran.)
- $T[e] := T[x, y]$ pro hranu $e = xy$. Této cestě budeme říkat *cesta pokrytá hranou* e.
- Hrana $e' \in E \setminus T$ je *lehká vzhledem k* $T \equiv \exists e \in T[e'] : w(e') < w(e)$. Ostatním hranám neležícím v kostře budeme říkat *těžké.*

Věta. *Kostra T je minimální $\Leftrightarrow$ neexistuje hrana lehká vzhledem k T.*

Definice. Pro kostru T a hrany $e \in T, e' \notin T$ zaveďme $swap(T, e, e') := T - e + e'$.

Pozorování. Pokud $e' \notin T$ a $e \in T[e']$, je $swap(T, e, e')$ opět kostra. Stačí si uvědomit, že přidáním e' do T vznikne kružnice a vynecháním libovolné hrany z této kružnice získáme opět kostru.

Lemma. (O swapování) *Máme-li libovolné kostry T a T', pak lze z T dostat T' konečným počtem operací ($swap$).*

Lemma. (Monotónní o swapování) *Je-li T kostra, k níž neexistují žádné lehké hrany, a T' libovolná kostra, pak lze od T k T' přejít posloupností swapů, při které váha kostry neklesá.*

Všechny tradiční algoritmy na hledání minimální kostry lze popsat jako speciální případy následujícího meta-algoritmu. Formulujeme ho pro případ, kdy jsou všechny váhy hran navzájem různé.

Algoritmus. (Červenomodrý meta-algoritmus)

1. Na počátku jsou všechny hrany bezbarvé.
2. Dokud to lze, použijeme jedno z následujících pravidel:
   Modré pravidlo: Vyber řez (podmnožinu hran, jejichž odebráním graf přestane být souvislý) takový, že jeho nejlehčí hrana není modrá, a obarvi ji na modro.
   Červené pravidlo: Vyber cyklus takový, že jeho nejtěžší hrana není červená, a obarvi ji na červeno.

Lemma. (Modré lemma) *Je-li libovolná hrana e algoritmem kdykoliv obarvena na modro, pak $e \in T_{\min}$.*

Lemma. (Červené lemma) *Je-li libovolná hrana e algoritmem kdykoliv obarvena na červeno, pak $e \notin T_{\min}$.*

Lemma. (Bezbarvé lemma) *Pokud existuje nějaká neobarvená hrana, lze ještě použít některé z pravidel.*

Věta. *Pro Červenomodrý meta-algoritmus spuštěný na libovolném grafu s hranami lineárně uspořádanými podle vah platí:*

1. *Vždy se zastaví.*
2. *Po zastavení jsou všechny hrany obarvené.*
3. *Modře obarvené hrany tvoří minimální kostru.*

Klasické algoritmy

Algoritmus. (Kruskalův neboli Hladový)

1. Setřídíme hrany podle vah vzestupně.
2. Začneme s prázdnou kostrou (každý vrchol je v samostatné komponentě souvislosti).
3. Bereme hrany ve vzestupném pořadí. Pro každou hranu e se podíváme, zda spojuje dvě různé komponenty – pokud ano, přidáme ji do kostry (obarvíme ji na modro), jinak ji zahodíme (obarvíme ji na červeno).

Tvrzení. *Algoritmus má časovou složitost $O(m \log n)$. Máme-li hrany předem setřízené nebo můžeme-li je setřídit v lineárním čase, algoritmus lze implementovat v čase $O(m\alpha(m,n))$, kde $\alpha(m,n)$ je obdoba inverzní Ackermannovy funkce.*

Algoritmus. (Borůvkův) Opět si budeme pěstovat modrý les, avšak tentokrát jej budeme rozšiřovat ve fázích. V jedné fázi nalezneme ke každému stromečku nejlevnější incidentní hranu (hranu sdílející právě jeden vrchol s tímto stromečkem) a všechny tyto nalezené hrany naráz přidáme (aplikujeme několik modrých pravidel najednou). Pokud jsou všechny váhy různé, cyklus tím nevznikne.

Tvrzení. *Algoritmus má časovou složitost $O(m \log n)$.*

Algoritmus. (Jarníkův) Jarníkův algoritmus je podobný Borůvkovi, ale s tím rozdílem, že nenecháme růst celý les, ale jen jeden modrý strom. V každém okamžiku nalezneme nejlevnější hranu vedoucí mezi stromem a zbytkem grafu a přidáme ji ke stromu (modré pravidlo); hrany vedoucí uvnitř stromu průběžně zahazujeme (červené pravidlo). Kroky opakujeme, dokud se strom nerozroste přes všechny vrcholy.

Tvrzení. *Algoritmus má časovou složitost $O(m \log n)$. S Fibonacciho haldou se dá naimplementovat v $O(m + n \log n)$.*

Důsledek. *Máme lineární algoritmus pro grafy s $m \geq c \cdot n \log(n)$ pro libovolnou konstantu c.*

Příklady

Příklad 1. Nechť úplný graf K_n na množině vrcholů $\{1, 2, \ldots, n\}$ má hranu $\{i, j\}$ ohodnocenou číslem

(i) $\max(i, j)$,
(ii) $i + j$.

Nalezněte minimální kostru a spočtěte její váhu.

Příklad 2. Nalezněte jednoduchý algoritmus pro výpočet minimální kostry v grafech ohodnocených vahami $\{1, \ldots k\}$ se složitostí $\mathrm{O}(mk)$ nebo dokonce $\mathrm{O}(m + nk)$.

Příklad 3. Uvažme v rovině n-bodovou množinu V. Definujme ohodnocení hran úplného grafu na V: ohodnocením hrany $\{x, y\}$ bude vzdálenost bodů x a y.

(i) Ukažte, že maximální stupeň vrcholu v libovolné minimální kostře je nejvýš 6.
(ii) Ukažte, že existuje minimální kostra, jejíž hrany se navzájem nekříží.

Příklad 4. Nechť V je množina n bodů ve čtverci o straně 1. Dokažte, že existuje kostra na V s celkovou délkou hran nejvýš $10\sqrt{n}$ (uvažujeme všechny kostry úplného grafu na V a váha hrany $\{x, y\}$ je euklidovská vzdálenost bodů x a y). Konstantu 10 lze podstatně zlepšit, ale nejlepší možná hodnota není známa (jaký nejlepší odhad se podaří najít vám?).

Příklad 5. Buď $G = (V, E)$ graf, w nezáporné ohodnocení jeho hran.

(i) Každá množina $E' \subseteq E$ navzájem disjunktních hran se nazývá *párování* v grafu G. Označme $\nu_w(G)$ maximální možnou hodnotu $w(E')$ pro párování $E' \subseteq E$. Hladový algoritmus pro maximální párování funguje podobně jako Kruskalův algoritmus pro maximální kostru, jenže zamítá hrany protínající některou dříve vybranou hranu. Ukažte, že takový algoritmus vždy najde párování váhy nejméně $\nu_w(G)/2$.

(ii) Ukažte, že odhad v (i) nelze zlepšit, tj. že pro libovolné $\alpha > \frac{1}{2}$ existuje zadání, pro nějž hladový algoritmus najde párování váhy menší než $\alpha\nu_w(G)$.

Rychlejší algoritmy

Definice. Kontrakce hrany spojí dva konce hrany do jednoho vrcholu, tuto hranu smaže, ale ostatní zachová (přičemž mohou vznikat paralelní hrany a smyčky).

Cvičení. Rozmyslete si, že Červenomodrý meta-algoritmus funguje i pro multigrafy.

Pozorování. Pokud $F \subseteq \mathrm{M}ST(G)$ (kde $\mathrm{M}ST(G)$ je minimální kostra grafu G), G' je graf vzniklý z G kontrakcí podél hran z F, pak kostra grafu G, která vznikne z $\mathrm{M}ST(G')$ zpětným expandováním kontrahovaných vrcholů, je $\mathrm{M}ST(G)$. Pokud kontrakcí vzniknou smyčky, můžeme je ihned odstraňovat; pokud paralelní hrany, ponecháme z nich vždy tu nejlehčí. To nás vede k následujícímu algoritmu:

Algoritmus. (Kontrahující Borůvkův algoritmus)

1. Ke každému vrcholu najdeme nejlevnější incidentní hranu – dostaneme množinu hran $F \subseteq E$.
2. Graf kontrahujeme podle F následovně:
3. Prohledáme do šířky graf (V, F) a přiřadíme každému vrcholu číslo komponenty, v níž se nachází.
4. Přečíslujeme hrany v G podle čísel komponent.
5. Odstraníme násobné hrany:
6. Setřídíme hrany lexikograficky přihrádkovým tříděním (násobné hrany jsou nyní pospolu).
7. Projdeme posloupnost hran a z každého úseku multihran odstraníme všechny až na nejlevnější hranu. Také odstraníme smyčky.
8. Pokud stále máme netriviální graf, opakujeme předchozí kroky.
9. Vrátíme jako minimální kostru všechny hrany, které se v průběhu algoritmu dostaly do F.

Tvrzení. *Algoritmus má pro rovinné grafy*[1] *časovou složitost* $O(n)$.

Algoritmus. (Kombinace Jarníkova a Borůvkova algoritmu)

1. Provedeme $\log\log n$ cyklů upraveného Borůvkova algoritmu s kontrahováním hran popsaného výše.
2. Pokračujeme Jarníkovým algoritmem (implementovaným Fibonacciho haldou).

Tvrzení. *Algoritmus má časovou složitost* $O(m \log\log n)$.

[1] Platí i silnější tvrzení, že algoritmus je lineární pro třídy grafů uzavřené na *minory*, kde *minor* vznikne z původního grafu jako podgraf, kterému kromě odebírání hran a vrcholů zároveň povolujeme kontrahovat hrany.

Algoritmus. (Jarníkův s omezenou velikostí haldy)

1. Opakujeme, dokud máme netriviální G (s alespoň jednou hranou):
2. $\quad t \leftarrow |V(G)|$.
3. $\quad$ Zvolíme $k \leftarrow 2^{2m/t}$ (velikost haldy).
4. $\quad T \leftarrow \emptyset$.
5. $\quad$ Opakujeme, dokud existují vrcholy mimo T:
6. $\qquad$ Najdeme vrchol v_0 mimo T.
7. $\qquad$ Spustíme Jarníkův alg. (s Fib. haldou) pro celý graf od v_0. Zastavíme ho, pokud:
8. $\qquad\quad |H| \geq k$ (byla překročena velikost haldy) nebo
9. $\qquad\quad H = \emptyset$ (došli sousedé) nebo
10. $\qquad\quad$ do T jsme přidali hranu oboustranně incidentní s hranami v T (připojili jsme novou podkostru k nějaké už nalezené).
11. $\quad$ Kontrahujeme G podle podkoster nalezených v T.

Tvrzení. *Časová složitost tohoto algoritmu je $O(m\beta(m,n))$, kde*

$$\beta(m,n) = \min\{i : \log^{(i)} n < m/n\}.$$

Všimněte si, že $\beta(m,n)$ je méně než $\log^* n$, kde $\log^* n$ (*iterovaný logaritmus*) je definován jako 0 pro $n \leq 1$ a jako $1 + \log^*(\log n)$ pro $n > 1$.

Důsledek. *Algoritmus je lineární pro grafy s $m \geq n \log^{(k)} n$ pro libovolnou konstantu k.*

Další výsledky

- $O(m\alpha(m,n))$, kde $\alpha(m,n)$ je obdoba inverzní Ackermannovy funkce definovaná podobně, jako je $\beta(m,n)$ obdobou $\log^*$.
- $O(\mathcal{T}(m,n))$, kde $\mathcal{T}(m,n)$ je hloubka optimálního rozhodovacího stromu pro nalezení minimální kostry v grafech s patřičným počtem hran a vrcholů. Jelikož každý deterministický algoritmus založený na porovnávání vah lze popsat rozhodovacím stromem, je tento algoritmus zaručeně optimální. Jen bohužel nevíme, jak optimální stromy vypadají, takže je stále otevřeno, zda lze minimální kostru nalézt v lineárním čase. Nicméně tento algoritmus pracuje i na Pointer Machine, pročež víme, že pokud je lineární složitosti možné dosáhnout, není k tomu potřeba výpočetní síla RAMu.[2]
- $O(m)$ pro grafy s celočíselnými vahami (na RAMu).
- $O(m)$, pokud už máme hrany setříděné podle vah: jelikož víme, že záleží jen na uspořádání, můžeme váhy přečíslovat na $1, \ldots, m$ a použít předchozí algoritmus.
- $O(m)$ průměrně: randomizovaný algoritmus, který pro libovolný vstupní graf doběhne v očekávaném lineárním čase.

[2] V tomto modelu dovolujeme přístupy na libovolné místo v paměti v konstantním čase.

- Na zjištění, zda je zadaná kostra minimální, stačí O(m) porovnání a dokonce lze v lineárním čase zjistit, která to jsou. Z toho ostatně vychází předchozí randomizovaný algoritmus.

Návody

1.

(i) Sporem dokažte, že n-tý vrchol musí být spojený právě s jedním z předchozích vrcholů, pak indukce.
(ii) Analogicky, ale vrchol n musí být konkrétně spojený s vrcholem 1.

2. Dovolte si používat jen hrany s vahami $\leq k'$.

3.

(i) Pro vrchol v stupně ≥ 7 existují hrany $\{v, u_1\}, \{v, u_2\}$ svírající úhel $< 60°$. Jednu z nich lze nahradit hranou $\{u_1, u_2\}$.
(ii) Vezměte libovolné křížící se hrany $\{a, b\}$ a $\{c, d\}$. Odeberte je a uvědomte si, že po odebrání je právě jedna dvojice z vrcholů a, b, c, d ve stejné komponentě.

4. Jedno řešení: Rozdělte na síť $\sqrt{n} \times \sqrt{n}$.
Druhé řešení: Dokažte, že některé dva body jsou vzdálené $O(\sqrt{n})$, jeden vymažte a indukcí.

5.

(i) Buď E_M maximální párování, E_H párování nalezené hladovým algoritmem a každé hraně $e \in E_M$ přiřaďme první z hran E_H, která ji protíná.
(ii) Stačí graf na 4 vrcholech. Zařiďte, aby algoritmus kvůli vybrání největší hrany zahodil dvě jen o epsilon menší.

Literatura a zdroje

[1] Martin Mareš: *Krajinou grafových algoritmů*, *http://http://mj.ucw.cz/vyuka/ga/*
[2] Jiří Matoušek, Jaroslav Nešetřil: *Kapitoly z Diskrétní matematiky*, Nakladatelství Karolinum, 2009

Simsonova přímka

Štěpán Šimsa

Abstrakt. Příspěvek obsahuje některé vlastnosti Simsonovy přímky a řadu úloh, k jejichž řešení lze Simsonovu přímku využít.

Věta. (Simsonova přímka) *Označme K, L, M paty kolmic vedených z bodu P na strany trojúhelníka BC, CA, AB trojúhelníka ABC. Pak body K, L, M leží v přímce právě tehdy, když bod P leží na kružnici opsané trojúhelníku ABC. Této přímce se říká Simsonova přímka bodu P vzhledem k trojúhelníku ABC.*

Zajímavost. (Šikmá Simsonova přímka) *Body leží na přímce i pokud v předchozím tvrzení nahradíme kolmice přímkami, které svírají s příslušnými stranami stejný úhel (orientovaný).*

Cvičení. Simsonovou přímkou vrcholu trojúhelníka je výška na protější stranu.

Cvičení. Simsonovou přímkou obrazu vrcholu podle středu kružnice opsané je protější strana.

Tvrzení 1. *Je-li H ortocentrum, pak Simsonova přímka bodu P půlí úsečku PH.*

Tvrzení 2. *Je-li S střed kružnice opsané, pak Simsonovy přímky bodů P a Q svírají úhel $\frac{1}{2}|\sphericalangle PSQ|$.*

Důsledek. *Simsonovy přímky protějších bodů jsou na sebe kolmé a protínají se na Feuerbachově kružnici.*

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

Příklady

Příklad 1. (Kamarád bodu na kružnici) Pro bod P na kružnici opsané trojúhelníku ABC platí, že obrazy přímek PA, PB, PC v osových souměrnostech postupně podle os úhlů BAC, CBA, ACB jsou rovnoběžné a navíc svírají se Simsonovou přímkou pravý úhel.

Příklad 2. Na kratším z oblouků CD kružnice opsané pravoúhelníku $ABCD$ zvolme bod P. Paty kolmic z bodu P na přímky AB, AC a BD označme postupně

K, L, M. Ukažte, že úhel $\sphericalangle LKM$ má velikost $45°$, právě když $ABCD$ je čtverec. (MO 58-III-2)

Příklad 3. (Miquelův bod) Mějme čtyři přímky v obecné poloze (žádné dvě nejsou rovnoběžné a žádné tři se neprotínají v jednom bodě). Každá trojice z nich definuje trojúhelník a uvážíme-li kružnice opsané těmto čtyřem trojúhelníkům, protínají se v jednom bodě.

Zajímavost. (Cliffordův řetízek) *Pět Miquelových bodů definovaných čtveřicemi z pěti přímek v obecné poloze leží na kružnici, šest těchto kružnic daných všemi péticemi přímek ze šesti přímek v obecné poloze se protínají v jednom bodě atd.*

Příklad 4. 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 5. 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 6. 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 7. Nechť kružnice vepsaná trojúhelníku ABC má střed I a dotýká se stran 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 8. 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 9. 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 10. Nechť $ABCD$ je tečnový čtyřúhelník a g je přímka procházející bodem A, která protíná stranu BC v bodě M a přímku 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, G8)

Příklad 11. 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)

Příklad 12. Nechť ABC je ostroúhlý trojúhelník a ω kružnice jemu opsaná. Dále nechť t je tečna kružnice ω a t_a, t_b, t_c jsou po řadě obrazy přímky t v osové symetrii podle přímek BC, CA, AB. Ukažte, že kružnice opsaná trojúhelníku určenému přímkami t_a, t_b, t_c se dotýká kružnice ω. (IMO 2011, 6)

Návody

1. Pro kolmost obrazu přímky PC uvažte tětivový čtyřúhelník $PCKL$.

2. Dokreslete paty kolmic z P na AD a BC. Nalezněte Simsonovy přímky a uvědomte si, že $|\sphericalangle LKM| = |\sphericalangle APB|$.

3. Protněte dvě z kružnic v bodě P a uvědomte si, že paty kolmic v jednotlivých trojúhelnících definují stejné přímky.

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

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

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

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

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

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

10. Využijte Tvrzení 1 pro Simsonovu přímku bodu C vzhledem k trojúhelníku $I_1I_2I_3$.

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

12. Označme T dotyk t s ω, A' průsečík t_b s t_c a analogicky B' a C'.

(i) Body X, Y, Z definujeme jako obrazy T podle BC, CA, AB. Dokažte, že leží v přímce.
(ii) Dokažte $\sphericalangle(XC, XC') = \sphericalangle(YC, YC')$.
(iii) Označte K Miquelův bod pro přímky $A'B'$, $B'C'$, $C'A'$, XY.
(iv) Doúhlete, že K je hledaný bod dotyku.

Literatura a zdroje

[1] Pepa Tkadlec: *Simsonova Přímka*, Hojsova Stráž, 2011.
[2] Martina Vaváčková: *Simsonova Přímka*, Zásada, 2014.
[3] *www.artofproblemsolving.com*

Kombinatorická teorie čísel

Rado van Švarc

Abstrakt. Příspěvek obsahuje úlohy z kombinatorické teorie čísel.

Úloha 1. Vybrali jsme $n+1$ čísel z množiny $1, 2, \dots, 2n$. Dokažte, že některé z nich dělí některé jiné. (Paul Erdős)

Úloha 2. Dokažte, že každé přirozené číslo je možné vyjádřit jako součet přirozených čísel tvaru $2^a 3^b$ tak, aby žádné z nich nedělilo jiné.

Úloha 3. Alespoň dvouprvková množina M přirozených čísel je *kouzelná*, jestliže pro každá různá $a, b \in M$ platí také

$$\frac{a+b}{NSD(a,b)} \in M.$$

Najděte všechny konečné kouzelné množiny. (BAMO, 2009)

Úloha 4. Buď m přirozené číslo a označme

$$M = \{n \in \mathbb{N} \mid m^2 \le n < (m+1)^2\}.$$

Dokažte, že všechny součiny tvaru ab pro $a, b \in M$ jsou různé pro různé neuspořádané dvojice $\{a, b\}$. (Indie 1998)

Úloha 5. Buď A n-prvková množina zbytků modulo n^2. Dokažte, že existuje n-prvková množina B zbytků modulo n^2 taková, že součty $A + B$ pokrývají alespoň polovinu všech zbytků modulo n^2. (IMO Shortlist 1999)

Úloha 6. Buď p prvočíslo. Dokažte, že z tabulky $p^2 \times p^2$ je možné vybrat p^3 políček tak, aby žádná čtveřice vybraných políček netvořila vrcholy pravoúhelníku, jehož strany jsou rovnoběžné se stranami tabulky.

(Česko-slovensko-polské střetnutí 2010)

Úloha 7. Najděte všechna přirozená čísla $k \ge 2$, pro která platí: pro libovolný pár různých přirozených čísel m, n nepřevyšujících k není číslo $n^{n-1} - m^{m-1}$ dělitelné k. (MEMO 2009)

Úloha 8. Je dáno prvočíslo p. Najděte všechna k taková, že množinu $\{1, 2, \dots, k\}$ lze rozdělit na p částí se stejným součtem prvků. (IMO Long List 1985)

Nebojme se nekonečna

Úloha 9. Množina všech přirozených čísel je rozdělena na konečně mnoho podmnožin. Ukažte, že některá z nich (označme ji M) má následující vlastnost: s každým $n \in M$ leží v M nekonečně mnoho dalších násobků n.

(Berkeley Math Circle Monthly Contest 1999-2000)

Úloha 10. Rozhodněte, zda existuje nekonečná rostoucí posloupnost $a_1, a_2, \ldots$ taková, že pro každé k je pouze konečně mnoho z čísel $a_1 + k, a_2 + k, a_3 + k, \ldots$ prvočísly.

Úloha 11. Dokažte, že existuje libovolně velká množina přirozených čísel M taková, že $(a-b)^2 \mid ab$ pro libovolná různá $a, b \in M$. (USA 1998)

Úloha 12. Buďte a, b přirozená čísla větší než 2. Dokažte, že existuje konečná posloupnost $(n_i)_1^k$ taková, že $n_1 = a$, $n_k = b$, a navíc $n_i + n_{i+1} \mid n_i n_{i+1}$.

(Rumunsko 1998)

Úloha 13. Přirozené číslo n je *rozložitelné*, pokud existuje 2012 přirozených čísel a_i s následujícími vlastnostmi:

(i) $n = a_1 + a_2 + \cdots + a_{2012}$,
(ii) $1 \leq a_1 < a_2 < \cdots < a_{2012}$,
(iii) $a_i \mid a_{i+1}$ pro $i = 1, 2, \ldots, 2011$.

Dokažte, že přirozených čísel, která nejsou rozložitelná, je pouze konečně mnoho.

(iKS 2012)

Úloha 14. Dokažte, že existuje nekonečná množina přirozených čísel H taková, že pro každá dvě čísla $x, y \in H$ má číslo $x + y$ sudý počet různých prvočíselných dělitelů. (MKS 30-8-4b)

Úloha 15. Obarvíme-li všechna přirozená čísla konečně mnoha barvami, dokažte, že najdeme tři různá čísla a, b, c stejné barvy, která splňují $a + b = c$.

(Schurova věta)

Úloha 16. Nechť $a_1 < a_2 < \cdots$ je rostoucí posloupnost taková, že $a_{n+1} - a_n < 1\,000\,000$ pro všechna n. Dokažte, že pak existují indexy i, j takové, že $a_i \mid a_j$.

(Reid Barton)

Návody

1. Rozdělte množinu ze zadání na n částí tak, že kdykoli vezmeme dvě čísla z jedné části, tak jedno bude dělit druhé.

2. Je-li číslo sudé, vydělte dvěma, je-li liché, odečtěte největší možnou mocninu trojky.

3. Vezměte si jakožto a, b nejmenší čísla z M. Pak musí $(a+b)/NSD(a,b) = a$, z toho plyne $a \mid b$, a vyjádříme $b = a^2 - a$. Případ, kdy v množině je ještě třetí nejmenší číslo c dovedeme do sporu (opět $a \mid c$, vyjádříme c atd.). Jediné kouzelné množiny jsou tedy dvouprvkové $\{a, a^2 - a\}$.

4. Kdykoli $a_1 b_1 = a_2 b_2$, dají se tato čísla vyjádřit jako $a_1 = uv$, $b_1 = xy$, $a_2 = ux$, $b_2 = vy$. Dále pokud $u < x$ a $v < y$, tak $\lfloor\sqrt{uv}\rfloor < \lfloor\sqrt{xy}\rfloor$. Rozebráním možností uspořádání u, v, x, y dostáváme výsledek.

5. Postupně vybírejte prvky B. V každém kroku můžete pomocí Dirichletova principu pokrýt alespoň $n/2$ nových zbytků.

6. Rozsekejte na čtverce $p \times p$ a v každém vyberte jakožto p políček úhlopříčku posunutou v závislosti na součinu souřadnic příslušného čtverce.

7. Pouze 2, 3. Pro sudé $k \geq 4$ přímo najdete m, n. Pro lichá $k \geq 5$ existuje alespoň $(k+3)/2$ různých $n \leq k$, pro které n^{n-1} dává kvadratický zbytek, ale těch může být nanejvýš $(k+1)/2$.

8. Musí nutně platit $k > p$ a $p \mid \frac{k(k+1)}{2}$. A v takových situacích je skutečně možné rozdělení najít. Jakmile máte rozdělení pro k, najdete snadno rozdělení pro $k + 2p$ párováním dvojic se stejným prvkem. Takto ošetříte případ $p = 2$ a pro lichá prvočísla stačí najít rozdělení pro k rovno $2p$, $2p-1$, $3p$ a $3p-1$. Případ $2p$ je možné opět spárovat, pro $3p$ volte posloupnosti: $a_n = 3n$, $b_1 = 3p - 1$, b_{n+1} je největší číslo pod b_n nedělitelné třemi a c_n analogicky jako b_n, ovšem začínající na $(3p-1)/2$. Pak funguje rozdělení na trojice

$$\{a_n, b_n, c_n\} \text{ pro } n = 1, 2, \dots, p.$$

Jelikož mají tato rozdělení pro $2p$ a $3p$ stejně početné části, je možné je použít i na $2p - 1$ a $3p - 1$, když si do množiny přimyslíte nulu.

9. Sporem, předpokládejte, že každá množina má zástupce, jehož pouze konečně násobků leží v příslušné množině. Spor pak hledejte v násobcích součinu všech zástupců.

10. Ano, volíme ji tak, aby a_1 bylo složené, dále a_2 i $a_2 + 1$ byla složená, aby a_3, $a_3 + 1$ i $a_3 + 2$ byla složená, ...

11. Máme-li takovou množinu, můžeme ji celou posouvat o jistou konstantu tak, že vlastnost zůstane zachována. Současně, máme-li takovou množinu, můžeme do ní „beztrestně“ přidat nulu.

12. Uvědomíme si, že vztah ze zadání říká, že sousední čísla jsou tvaru xyz, $x(x-y)z$. Nejprve umíme převést číslo a na číslo $a!$, pak z něj můžeme postupně odbourávat nejvyšší prvočísla, až dostaneme mocninu dvojky. Nakonec stačí libovolné dvě mocniny dvojky na sebe umět převést.

13. Indukcí podle počtu sčítanců, na které to rozkládáme. Chceme-li rozložit obrovské liché číslo l, použijeme indukční přepoklad na $(n-1)/2$, příslušné rozložení vynásobíme dvěma a přičteme jedničku. Stejně rozložíme i násobky obrovských lichých čísel, zbývá rozložit obrovské mocniny dvojky $1 + 3 + 3 \cdot 4 + 3 \cdot 4^2 + \cdots$.

14. Podle Ramseyovy věty v grafu, jehož vrcholy jsou vhodná přirozená čísla a hrany jsou obarveny podle parity počtu různých prvočíselných dělitelů součtu, najdete nekonečnou kliku.

15. Podle Ramseyovy věty v grafu, jehož vrcholy jsou celá čísla a hrany jsou obarveny podle barvy své délky, najdete nekonečnou kliku.

16. Nazvěme posloupnost x_n k-skoro aritmetickou, pokud existuje aritmetická posloupnost a_n taková, že $0 \leq x_n - a_n \leq k$. Pokud existuje prvek a_n, který nedělí žádný prvek x_n, můžeme z posloupnosti x_n vybrat $(k-1)$-skoro aritmetickou posloupnost.

Literatura a zdroje

Základním zdrojem pro mne byla přednáška Mirka Olšáka ze soustředění v Oldřichově, kterou jsem bezostyšně zkopíroval. Ta čerpala z následujících zdrojů:

[1] Gabriel Carroll: *Combinatorial Number Theory (Teacher's Edition)*
[2] Peter Vandendriessche, Hojoo Lee: *Problems in Elementary Number Theory*

The Big Picture

Rado van Švarc

Abstrakt. V příspěvku prozkoumáme konfiguraci určenou tětivovým čtyřúhelníkem zvanou The Big Picture.

Začneme několika základními definicemi, úmluvami a tvrzeními.

Úmluva. Kružnici opsanou trojúhelníku XYZ budeme značit jako (XYZ).

Věta. (Miquelova) *Pokud v trojúhelníku ABC zvolíme body X, Y, Z na přímkách BC, CA a AB, pak se kružnice (YAZ), (ZBX) a (XCY) protínají v jednom bodě.*

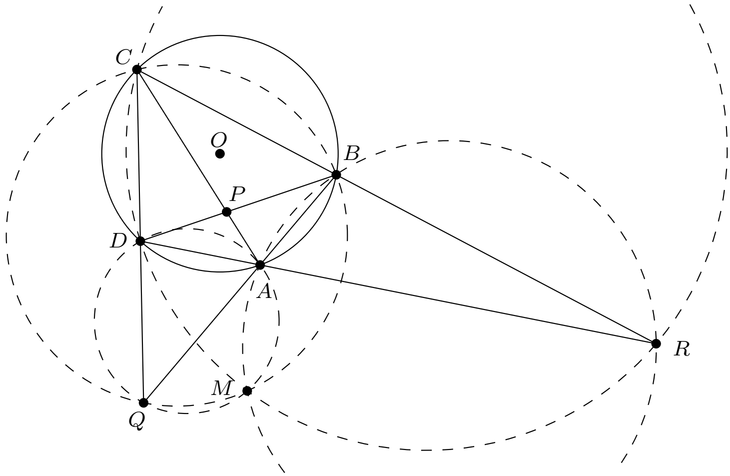
Tvrzení. *Nechť ℓ_1, ℓ_2, ℓ_3 a ℓ_4 jsou čtyři přímky, z nichž žádné dvě nejsou rovnoběžné. Nechť C_{ijk} je kružnice opsaná trojúhelníku určenému přímkami ℓ_i, ℓ_j a ℓ_k (říkáme jim Miquelovy kružnice). Pak se C_{123}, C_{234}, C_{341} a C_{412} protínají v jednom bodě (zvaném Miquelův).*

Tvrzení. *Nechť A, B, C a D jsou čtyři body v rovině, které neleží na jedné přímce. Přímky AB a CD se protínají v bodě Q a přímky DA a CB se protínají v bodě R. Pak Miquelův bod určený přímkami AB, BC, CD a DA leží na přímce QR právě tehdy, když A, B, C a D leží na jedné kružnici.*

Úmluva. Dále budeme *Vobrázkem* myslet následující konfiguraci:

Na kružnici se středem O leží čtyři různé body A, B, C a D. Přímky AC a BD se protínají v P, přímky AB a CD se protínají v Q a přímky AD a BC se protínají v R. Dále M je Miquelův bod určený přímkami AB, BC, CD a DA.

Vobrázku se též někdy říká *The Big Picture*. Pozor, neplést se stejnojmennou konfigurací pro trojúhelník propojující připsiště a Feuerbachovu kružnici. Až na sdílené jméno nemají pranic společného. Protože se ovšem pod tímto názvem obvykle myslí „ta druhá“, budeme v příspěvku i na přednášce používat termín Vobrázek.



Poznámka. Ve Vobrázku platí, že M leží na QR.

Lemma. *Nechť W, X, Y a Z jsou čtyři body v rovině. Předpokládejme, že $W \neq X$ a $Y \neq Z$. Pak přímky WX a YZ jsou kolmé právě tehdy, když $|WY|^2 + |XZ|^2 = |WZ|^2 + |XY|^2$.*

Tvrzení. *Ve Vobrázku platí $OM \perp QR$.*

Tvrzení. *Ve Vobrázku prochází kružnice (AOC) a (BOC) bodem M.*

Důsledek. *Ve Vobrázku je přímka MO osou úhlů AMC a BMD.*

Tvrzení. *Ve Vobrázku leží body O, P a M na jedné přímce.*

Spiralizace

Na začátek tohoto oddílu si zopakujme pár základních tvrzení o spirální podobnosti.

Tvrzení. *Nechť W, X, Y a Z jsou čtyři body v rovině takové, že se WY a XZ protínají v bodě P. Buď Q průsečík kružnic (WXP) a (PYZ). Pak Q je střed spirální podobnosti přenášející W na Y a X na Z.*

Tvrzení. („Spirální podobnost chodí po dvou“) *Pokud Q je střed spirální podobnosti přenášející W na Y a X na Z, pak je to také střed spirální podobnosti přenášející W na X a Y na Z.*

Nyní získáváme zcela nový pohled na Vobrázek:

Poznámka. Ve Vobrázku je M střed spirální podobnosti přenášející A na B a D na C. Stejně tak se jedná o střed spirální podobnosti přenášející A na D a B na C.

S tímto pozorováním si novým způsobem ukážeme již dokázané tvrzení.

Tvrzení. *Ve Vobrázku platí $OM \perp QR$.*

Polarizace

V tuto chvíli si zavedeme několik základních pojmů vázajících se k polárám.

Definice. *Kruhová inverze* je geometrické zobrazení určené kružnicí k se středem O a poloměrem r, které bodu A různému od O přiřadí bod A' na polopřímce OA takový, že $|OA| \cdot |OA'| = r^2$.

Tvrzení. *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.*

Definice. Nechť k je kružnice se středem O. Pokud máme bod $P \neq O$ a přímku ℓ kolmou na OP a procházející inverzem k P vzhledem ke k, pak říkáme, že P je *pól* přímky ℓ a přímka ℓ je *polára* bodu P.

Tvrzení. *Pokud X je pól poláry ℓ_1 a Y je pól poláry ℓ_2, pak X leží na ℓ_2 právě tehdy, když Y leží na ℓ_1.*

Důsledek. *Tři póly leží na přímce právě tehdy, když jejich poláry prochází jedním bodem.*

Definice. Nechť k je kružnice a XYZ trojúhelník. Řekneme, že vzhledem ke k je XYZ *selfpolar* (někdy taktéž přezdívaný *tripolární*, ale to je méně zažitý název), pokud X je pól YZ, Y je pól ZX a Z je pól XY.

K čemu nám tyto definice a tvrzení jsou? Přinášejí totiž ještě jednu důležitou vlastnost Vobrázku.

Tvrzení. *Ve Vobrázku je trojúhelník PQR tripolární.*

Důsledek. *Ve Vobrázku je O kolmiště trojúhelníku PQR.*

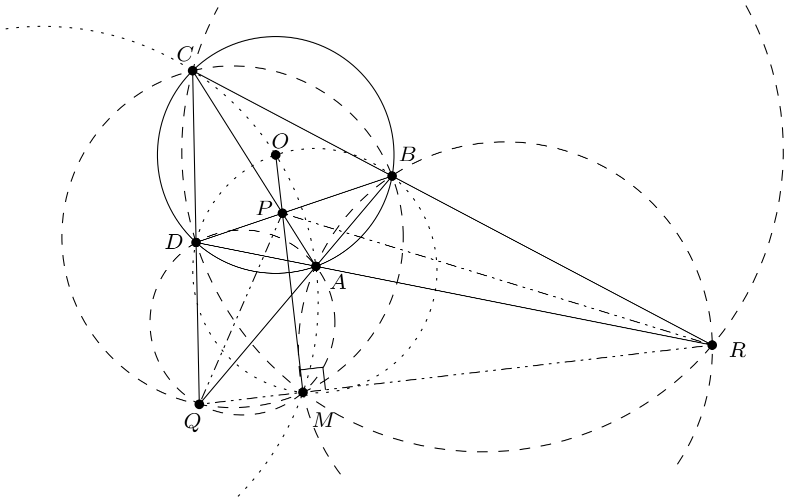
Shrnutí

Shrňme si vše důležité, co jsme zjistili, do jedné věty.

Věta. (Velká Věta Vo Vobrázku) *Nechť na kružnici se středem O leží čtyři různé body A, B, C a D. Přímky AC a BD se protínají v P, přímky AB a CD se protínají v Q a přímky AD a BC se protínají v R. Dále nechť přímka OP protíná přímku QR v bodě M. Potom platí:*

(1) *Kružnice (QAD), (QBC), (RAB), (RDC), (AOC) a (BOD) procházejí bodem M. Tedy M je Miquelovým bodem přímek AB, BC, CD a DA.*
(2) *Bod M je střed spirální podobnosti, která přenáší A na B a D na C. Zároveň se jedná o střed spirální podobnosti, která přenáší A na D a B na C.*
(3) *Platí $OM \perp QR$.*

(4) *Bod M je inverzem bodu P vzhledem ke kružnici $(ABCD)$.*
(5) *Trojúhelník PQR je tripolární vzhledem k této kružnici.*



Cvičení

Příklad 1. Kružnice se středem O prochází vrcholy A a C trojúhelníku ABC a protíná úsečky AB a BC znovu v bodech K a N. Kružnice (ABC) a (KBN) se protínají v bodech B a M. Dokažte, že $OM \perp MB$. (IMO 1985)

Příklad 2. Konvexní čtyřúhelník $ABCD$ je vepsán do kružnice ω se středem O. Jeho diagonály AC a BD se protínají v bodě P. Kružnice (APB) a (CPD) se protínají v bodech P a Q. Předpokládejme, že body O, P a Q jsou různé. Dokažte, že $OQ \perp QP$. (Čína 1992)

Příklad 3. Kružnice ω_1 a ω_2 se protínají v bodech O a M. Kružnice ω se středem v O protíná zbylé dvě kružnice ve čtyřech různých bodech A, B, C a D takových, že $ABCD$ je konvexní čtyřúhelník. Přímky AB a CD se protínají v bodě N_1 a přímky AD a BC v bodě N_2. Ukažte, že $OM \perp N_1N_2$.

Příklad 4. Uvažujme půlkružnici ω nad průměrem AB se středem O. Přímka ℓ protíná přímku AB v bodě M a půlkružnici ω v bodech C, D tak, že $|MA| > |MB|$ a $|MD| > |MC|$. Kružnice (AOD) a (BOC) se protínají v bodě K. Ukažte, že K leží na kružnici nad průměrem MO. (Rusko 1995, Rumunsko TST 1996, Írán 1997)

Příklad 5.

(1) Nechť A, B, C a D jsou čtyři body v rovině. Přímky AC a BD se protínají v P, přímky AB a CD v Q a přímky AD a BC v R. Přímka skrz P rov-

noběžná s QR protíná přímky AB a CD v bodech X a Y. Ukažte, že P je středem úsečky XY.

(2) (Butterfly Theorem) Buď ω kružnice s tětivou EF. Označme si střed EF jako P. Nechť skrz P prochází další dvě tětivy AC a BD. Nechť AB a CD protínají EF v bodech X a Y. Ukažte, že $|EX| = |YF|$.

Příklad 6. Nechť $ABCD$ je tětivový čtyřúhelník se středem O. Přímky AB a CD se protínají v bodě Q. Buď ℓ kolmice na OQ skrz Q. Přímky BD a AC protínají ℓ v bodech X a Y. Ukažte, že $|XQ| = |QY|$.

Příklad 7. Buď ABC trojúhelník s kružnicí opsanou ω. Tečny k ω v bodech B a C se protínají s bodě T. Nechť S je bod na polopřímce BC takový, že $AS \perp AT$. Body B_1 a C_1 leží na polopřímce ST tak, že $|B_1T| = |BT| = |C_1T|$ tak, že C_1 leží na úsečce B_1S. Dokažte, že trojúhelníky ABC a AB_1C_1 si jsou podobné.

(USA TST 2007)

Příklad 8. Nechť ABC je trojúhelník s vepsištěm I. Označme si středy stran AB a AC jako M a N. Body D a E leží na stranách AB a AC tak, že $|DB| = |BC| = |CE|$. Přímka ℓ_1, resp. ℓ_2, je kolmice spuštěná z bodu D, resp. E, na přímku IM, resp. IN. Průsečík ℓ_1 a ℓ_2 označme jako P. Ukažte, že platí $AP \perp BC$.

Příklad 9. Buď $ABCD$ konvexní čtyřúhelník, jehož strany BC a AD jsou různoběžné a stejně dlouhé. Body E a F leží na stranách BC a AD tak, že $|BE| = |DF|$. Přímky AC a BD se protínají v bodě P, přímky BD a EF se protínají v bodě Q a přímky EF a AC se protínají v bodě R. Uvažujme všechny kružnice (PQR), když se body E a F hýbou po příslušných stranách. Ukažte, že všechny tyto kružnice mají společný bod různý od P. (IMO 2005)

Příklad 10. Nechť $ABCD$ je tečnový čtyřúhelník, jehož kružnice vepsaná se dotýká stran AB, BC, CD a DA v bodech E, F, G a H.

(1) Ukažte, že přímky AC, EF a GH procházejí jedním bodem.
(2) Ukažte, že přímky AC, BD, EG a FH procházejí jedním bodem.

Příklad 11. Nechť $ABCD$ je tětivový čtyřúhelník. Přímky AB a DC se protínají v bodě Q a přímky AD a BC v bodě R. Tečny z bodu R se dotýkají dané kružnice v bodech X a Y. Ukažte, že Q, X a Y leží na jedné přímce. (Čína 1997)

Příklad 12. Nechť $ABCD$ je tětivový čtyřúhelník se středem O. Přímky AB a CD se protínají v bodě E, přímky AD a BC v bodě F a přímky AC a BD v bodě P. Dále se přímky EP a AD protínají v K. Buď M kolmá projekce bodu O na AD. Dokažte, že $BCMK$ je tětivový čtyřúhelník.

Příklad 13. Body A_1, B_1 a C_1 leží na stranách BC, CA a AB trojúhelníka ABC. Kružnice (B_1AC_1), (C_1BA_1), (A_1CB_1) protínají (ABC) podruhé v bodech A_2, B_2 a C_2. Obrazy bodů A_1, B_1 a C_1 podle středů stran BC, CA a AB označme jako A_3, B_3 a C_3. Ukažte, že trojúhelníky $A_2B_2C_2$ a $A_3B_3C_3$ jsou si podobné.

(IMO SL 2006)

Příklad 14. Eulerův bod tětivového čtyřúhelníku

(1) Buď $ABCD$ tětivový čtyřúhelník. Nechť H_A, H_B, H_C a H_D jsou kolmiště trojúhelníků BCD, CDA, DAB a ABC. Ukažte, že $H_AH_BH_CH_D$ je jen obrazem $ABCD$ podle nějakého bodu E (tento bod nazýváme *Eulerův bod* čtyřúhelníku $ABCD$).
(2) Ukažte, že E leží na Feuerbachově kružnici trojúhelníku ABC.
(3) Ukažte, že E leží na Simsonově přímce trojúhelníku ABC a bodu D.
(4) Ukažte, že E je Eulerův bod čtyřúhelníku $H_AH_BH_CH_D$.
(5) Ukažte, že E leží na kolmici ze středu AB na přímku CD.

Literatura a zdroje

[1] Yufei Zhao: *Cyclic Quadrilaterals - The Big Picture*, *http:/yufeizhao.com/olympiad/cyclic_quad.pdf*

Sinová věta

Martin Töpfer

Abstrakt. Sinová věta je jedno ze základních geometrických tvrzení, které se obzvláště hodí, když se v zadání vyskytují poměry (nebo rovnost) vzdáleností. Dobře si také poradí s kombinací vzdáleností a úhlů.

Věta. (Sinová věta) *Pro každý trojúhelník ABC s vnitřními úhly α, β, γ, stranami a, b, c a poloměrem kružnice opsané R platí*

$$\frac{a}{\sin\alpha} = \frac{b}{\sin\beta} = \frac{c}{\sin\gamma} = 2R.$$

Při používání sinové věty se velmi často hodí, že $\sin\alpha = \sin(180^\circ - \alpha)$. Také je dobré si zapamatovat hodnoty sinu pro úhly 30°, 45° a 60°, protože na soutěžích se předpokládá jejich znalost.

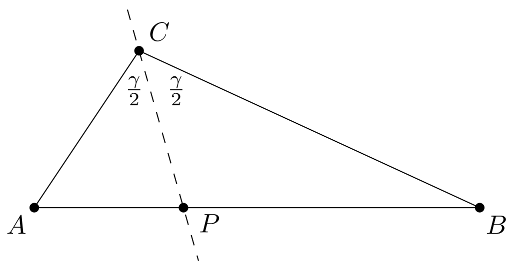
Úlohy na zahřátí

Příklad 1. (Angle bisector theorem) Mějme trojúhelník ABC, průsečík osy úhlu ACB se stranou AB označme P. Dokaž, že $\frac{|AP|}{|BP|} = \frac{|AC|}{|BC|}$.

Řešení. Použijeme sinovou větu na „sousední" trojúhelníky APC a CBP:

$$\frac{|AP|}{\sin\frac{\gamma}{2}} = \frac{|AC|}{\sin|\sphericalangle APC|} \qquad \text{a} \qquad \frac{|BP|}{\sin\frac{\gamma}{2}} = \frac{|BC|}{\sin|\sphericalangle CPB|}.$$

Jelikož ovšem $|\sphericalangle APC| = 180^\circ - |\sphericalangle CPB|$, je $\sin|\sphericalangle APC| = \sin|\sphericalangle CPB|$ a dokončení úlohy je již pouze otázkou vyjádření z předchozích rovnic.



Příklad 2. Body D a E dělí základnu rovnoramenného trojúhelníku ABC na tři stejně dlouhé části. Ukaž, že $|\sphericalangle BAD| < |\sphericalangle DAE|$.

Příklad 3. Je dán trojúhelník ABC, střed strany BC označme M. Nechť na straně AB leží bod P. Označme Q průsečík AM a PC. Dokaž, že $|CQ| = |AB|$ právě tehdy, když $|AP| = |PQ|$.

Příklad 4. Mějme rovnostranný trojúhelník ABC, jeho střed označme S. Na straně AB leží bod D takový, že $|AS| = |AD|$. Postupně označme E a F průsečíky přímky DS s AC a BC. Dokaž, že $|DE| = |EF|$.

Úlohy střední až těžké

Příklad 5. V rovnoběžníku $TUVW$ jsou na stranách TU a UV po řadě body X, Y tak, že $|TX| = |VY| > 0$. Přímky TY a VX se protínají v bodě P. Dokaž, že P leží na ose úhlu VWT.

Příklad 6. Mějme tětivový čtyřúhelník $ABCD$ s průsečíkem úhlopříček P. Dokaž, že platí

$$|AP| \cdot \sin\alpha + |CP| \cdot \sin\gamma = |BP| \cdot \sin\beta + |DP| \cdot \sin\delta.$$

Příklad 7. V trojúhelníku ABC označme M střed strany BC a T průsečík tečen v bodech B a C ke kružnici opsané trojúhelníku ABC. Dokaž, že potom $|\sphericalangle BAT| = |\sphericalangle MAC|$. Přímka AT je takzvaná *symediána*.

Příklad 8. Uvažujme konvexní čtyřúhelník $ABCD$, jehož strany AB, BC a CD jsou stejně dlouhé a který není lichoběžník.[1] Označme S průsečík jeho úhlopříček. Dokaž, že $|AS| = |SD|$, právě když $|\sphericalangle BAD| + |\sphericalangle ADC| = 120°$.

(MKS, ročník 28)

Příklad 9. V libovolném trojúhelníku ABC, ve kterém těžnice z C není kolmá na AC ani na BC, označme X a Y průsečíky osy této těžnice s přímkami AC a BC. Najdi všechny trojúhelníky ABC takové, že A, B, X a Y leží na jedné kružnici.

(MO-64-A-III-3)

Věta 10. (Cevova věta) *V trojúhelníku ABC mějme body $X \in BC$, $Y \in AC$, $Z \in AB$ na stranách trojúhelníku. Pak AX, BY a CZ se protínají v jednom bodě, právě když platí*

$$\frac{|BX|}{|CX|}\frac{|CY|}{|AY|}\frac{|AZ|}{|BZ|} = 1.$$

Příklad 11. Mějme trojúhelník ABC. Na výšce AX zvolme bod P. Dále $K = BP \cap AC$ a $L = CP \cap AB$. Dokažte, že $|\sphericalangle AXK| = |\sphericalangle AXL|$.

Příklad 12. Mějme konvexní pětiúhelník $ABCDE$ se všemi stranami shodné délky a. Průsečík úhlopříček AD a EC označme S. Víme, že $|\sphericalangle ASE| = 60°$. Dokaž, že dvě strany $ABCDE$ jsou rovnoběžné. (MEMO 2011, Mišo Szabados)

[1] Neboli žádné dvě jeho strany nejsou rovnoběžné.

Příklad 13. Je dán tětivový čtyřúhelník $ABCD$. Označme P, Q, R paty kolmic z bodu D postupně na BC, CA, AB. Dokaž, že $|PQ| = |QR|$ právě tehdy, když se osy úhlů $\sphericalangle ABC$ a $\sphericalangle ADC$ protnou na AC. (IMO 2003)

Věta 14. (Meneláova věta) *V trojúhelníku ABC mějme body $F \in BC$, $G \in AC$, $H \in AB$ tak, že právě jeden z nich neleží na příslušné straně. Pak F, G a H jsou v jedné přímce, právě když platí*

$$\frac{|AH|}{|HB|}\frac{|BF|}{|FC|}\frac{|CG|}{|GA|} = 1.$$

Literatura a zdroje

[1] Alča Skálová: *Sinová věta*, Oldřichov, 2012.
[2] Titu Andreescu, Zuming Feng: *103 Trigonometry Problems*, Birkhäuser, 2005.

Obsah

Nekonečně malá čísla (Tonda Češík) 3
Přehýbání (Tonda Češík) 8
Velké prostory (Anička Doležalová) 11
IMO 1 (mod 3) (David Hruška) 16
Řády a mocniny (David Hruška) 20
Úvod do kombinatoriky (Bára Kociánová) 26
Komplexní čísla (Honza Krejčí) 33
Permutace (Jakub Löwit) 38
Burnsideovo lemma (Viki Němeček) 49
AG nerovnost (Marian Poljak) 53
Extremální princip (Martin Sýkora) 59
Goniometrické substituce (Martin Sýkora) 61
Čínská zbytková věta (Lucien Šíma) 65
Minimální kostry (Štěpán Šimsa) 68
Simsonova přímka (Štěpán Šimsa) 74
Kombinatorická teorie čísel (Rado van Švarc) 77
The Big Picture (Rado van Švarc) 81
Sinová věta (Martin Töpfer) 87