Mrtník

Sborník, jaro 2023

Natália Bátorová
φla Čermák
Matěj Doležálek
Klárka Grinerová
Petr Hladík
Verča Hladíková
Terka Kučerová
Lucka Kundratová
Anna Marie Minarovičová
Radek Olšák
Michal Pecho
Daniel Perout
Zdeněk Pezlar
Marian Poljak
Adéla Karolína Žáčková

Autoři: Natália Bátorová, φla Čermák, Matěj Doležálek, Klárka Grinerová, Petr Hladík, Verča Hladíková, Terka Kučerová, Lucka Kundratová, Anna Marie Minarovičová, Radek Olšák, Michal Pecho, Daniel Perout, Zdeněk Pezlar, Marian Poljak, Adéla Karolína Žáčková
Editoři: Matěj Doležálek, Michal Pecho
vydání první, náklad 44 výtisků
březen 2023
Díky za pomoc všem, kterým je za co děkovat.
Realizace projektu byla podpořena Ministerstvem školství, mládeže a tělovýchovy.

Kongruencie

Natália Bátorová

Abstrakt. Kongruencie sú jedným z nástrojov teórie čísel. Umožňujú nám získať jednoduchší náhľad na deliteľnosť. Dajú sa uplatniť v matematickej olympiáde či iných súťažiach. V tejto prednáške si ich definujeme a naučíme sa s nimi od základov pracovať.

Definícia. Nech a, b sú celé čísla a m prirodzené. Povieme, že a *je kongruentné s* b *modulo* m, pokiaľ $m \mid (a-b)$. Píšeme

$$a \equiv b \pmod{m}.$$

Ak a je kongruentné s b modulo m, tak čísla a, b dávajú rovnaký zvyšok po delení číslom m. Špeciálne $m \mid a$ môžeme zapísať ako $a \equiv 0 \pmod{m}$. Ukážeme si, že s kongruenciami je možné pracovať skoro ako s rovnicami.

Tvrdenie. (vlastnosti kongruencie) *Nech* $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$ a $n \in \mathbb{N}$. *Potom:*

(1) $a + c \equiv b + d \pmod{m}$,
(2) $a \cdot c \equiv b \cdot d \pmod{m}$,
(3) $a^n \equiv b^n \pmod{m}$,
(4) *ak* $d \mid m$, *tak* $a \equiv b \pmod{d}$.

Úloha 1. Spočítajte $83^{83} + 25^{25} \bmod 4$.

Úloha 2. Aký zvyšok dáva číslo 11^{13} po delení číslom 15?

Cvičenie. Ukážte, že vo všeobecnosti neplatí, že ak $a \cdot c \equiv b \cdot c \pmod{m}$, tak $a \equiv b \pmod{m}$.

Tvrdenie. *Nech* $a \cdot c \equiv b \cdot c \pmod{m}$, *potom* $a \equiv b \pmod{m/\operatorname{NSD}(m,c)}$.

Dôsledok. *Ak* $\operatorname{NSD}(m,c) = 1$ a $a \cdot c \equiv b \cdot c \pmod{m}$, *tak* $a \equiv b \pmod{m}$.

Úloha 3. Nájdite všetky $x \in \mathbb{N}$, aby platilo $12x + 27^2 \equiv 18 \pmod{30}$.

Úloha 4. Nájdite všetky $x \in \mathbb{Z}$ spĺňajúce $3x + 6 \equiv 8 \pmod{20}$ a všetky $y \in \mathbb{Z}$ spĺňajúce $3y + 6 \equiv 8 \pmod{4}$.

Veta. (Bézoutova) *Nech aspoň jedno z celých čísel* a, b *je nenulové. Potom existujú celé čísla* x, y *také, že* $\operatorname{NSD}(a,b) = ax + by$.[1]

Príklad. Rozmyslite si na základe predchádzajúcej vety, že ak $\operatorname{NSD}(a,b) = 1$, tak $ax \equiv 1 \pmod{b}$ má vždy riešenie. Budeme ho značiť a^{-1}, teda $a \cdot a^{-1} \equiv 1 \pmod{b}$. Platí to aj v prípade, že $\operatorname{NSD}(a,b) > 1$?

[1] Všimnite si, že dvojica koeficientov (x,y) nie je určená jednoznačne. Rovnosť tiež spĺňajú dvojice $(x+b, y-a)$, $(x-b, y+a)$, $(x+2b, y-2a)$, ...

Riešenie. Z Bézoutovej vety vieme, že existujú x, y zo $\mathbb{Z}$ také, že $1 = \mathrm{NSD}(a,b) = xa + yb$. Pozrieme sa na rovnicu mod b a dostaneme $xa \equiv 1 \pmod{b}$. Pre vyriešenie druhej časti označme $\mathrm{NSD}(a,b) = d > 1$, potom využitím vlastnosti kongruencie dostaneme $0 \equiv ax \equiv 1 \pmod{d}$, teda táto kongruencia nemá žiadne riešenie.

Ešte by sa nám hodilo vedieť spočítať Bézoutove koeficienty. Tu nám pomôže *Euklidov algoritmus*.

Definícia. (rozšírený Euklidov algoritmus) Nech $a, b \in \mathbb{N}$, $|a| > |b|$, potom môžeme $\mathrm{NSD}(a,b)$ a riešenie rovnice $ax + by = \mathrm{NSD}(a,b)$ nájsť nasledujúcim spôsobom:

(1) Pripravíme si tabuľku s tromi stĺpčekmi, do prvého riadku napíšeme postupne a, 1, 0 a do druhého b, 0, 1.
(2) Pokiaľ nemáme v prvom stĺpci 0, opakujeme nasledujúce kroky:
  (2.1) Označme k_1, k_2, k_3 a l_1, l_2, l_3 hodnoty v posledných dvoch vyplnených riadkoch tabuľky.
  (2.2) Spočítame delením so zvyškom $k_1 : l_1 = d$ (zv. z).
  (2.3) Do nového riadku napíšeme čísla z, $k_2 - l_2 \cdot d$ a $k_3 - l_3 \cdot d$.

Posledné dve hodnoty predposledného riadku potom dávajú hľadané x a y. Prvá hodnota predposledného riadku je $\mathrm{NSD}(a,b)$.

Úloha 5. Nájdite $\mathrm{NSD}(37, 10)$ a príslušné Bézoutove koeficienty.

Úloha 6. Nájdite $\mathrm{NSD}(89, 55)$ a príslušné Bézoutove koeficienty.

Úloha 7. Určte $25^{-1} \bmod 36$.

Úloha 8. Nájdite nejaké riešenie rovnice $185x + 40y = 5$, kde $x, y \in \mathbb{Z}$. Ako budú vyzerať všetky riešenia?

Úloha 9. Nájdite všetky riešenia rovnice $x^2 + 10x - 1 \equiv 0 \pmod{17}$.

Kongruencia a štvorce

Využitie kongruencie nájdeme aj pri riešení týchto príkladov. Stačí si uvedomiť, že ak je číslo štvorec, tak môže mať len niektoré zvyšky modulo vhodné číslo.

Úloha 10. Rozhodnite, ktoré z čísel $\{4, 44, 444, 4444, \dots\}$ sú štvorcom, teda možno ich zapísať ako n^2 pre $n \in \mathbb{N}$.

Úloha 11. Je možné v čísle 2468101214 preusporiadať cifry tak, aby to bol štvorec?

Úloha 12. Je možné v čísle 1234567891011121314 preusporiadať cifry tak, aby to bol štvorec?

Úloha 13. Nájdite všetky prirodzené n, pre ktoré $4^n + 6^n + 9^n$ je štvorcom.
(ELMO Shortlist 2012)

Na záver pár zložitejších úloh ...

Úloha 14. Nájdite všetky prvočísla, ktoré spĺňajú $3p^4 - 5q^4 - 4r^2 = 26$.
(Junior Balkan MO 2014)

Úloha 15. Nájdite všetky čísla n, pre ktoré je číslo $2^n + 12^n + 2011^n$ štvorcom.
(USA Junior MO 2011)

Úloha 16. Nájdite všetky prvočísla p, pre ktoré sú $p + 2$ aj $p^2 + 2p - 8$ prvočísla.
(Albanian National Math Olympiad 2012)

Úloha 17. Nájdite všetky prvočísla, pre ktoré $p+q+r = 2023$ a $pqr+1$ je štvorec.
(Olympiada Mátematica de Andalucía 2023)

Úloha 18. Nájdite všetky nezáporné riešenia $7^a = 4^b + 5^c + 6^d$.
(TST Kirgizsko)

Úloha 19. Nech p je prvočíslo a $2^p + 3^p = a^n$. Ukážte, že potom $n = 1$.

Návody

1. Využite vlastnosti kongruencie, navyše platí $3 \equiv -1 \pmod 4$.

2. Využite $11 \equiv -4 \pmod{15}$.

4. Využite vlastnosti kongruencie.

7. Spočítajte Euklidovým algoritmom.

8. Pozrite sa na NSD$(185, 40)$.

10. Vydeľte 4 a skúste mod 4.

11. Skúste mod 3.

12. Tentoraz mod 9.

13. Skúste mod 5 a mod 13.

14. Pozrite sa na rovnicu mod 3 a mod 5.

15. Pozrite sa na rovnicu mod 3 a potom mod 4.

16. Skúste mod 3.

17. Vyskúšajte mod 4.

18. Skúste postupne mod 3, 4, 5, 25.

19. Vyriešte pre $p = 2$ a potom sa pozrite na rovnicu mod 5 a mod 25. Využite binomickú vetu.

Literatura a zdroje

[1] Filip Bialas: *Kongruence*, Zásada, 2017.
[2] Tomáš Novotný: *Dělitelnost*, Paseky, 2018.

Algebraické triky neboli... φgle

φla Čermák

Abstrakt. Příspěvek obsahuje řadu algebraických triků, které se hodí při řešení příkladů nebo jejich částí. Velkým zdrojem triků, které člověk více či méně často použije, bývají nerovnosti a velkým zdrojem k řešení nerovností je zase seriál MKS od Michala Rolínka a Pavla Šaloma, který najdete na našich stránkách[2]. Ten tedy doporučuji přečíst každému, kdo má pocit, že se potřebuje v algebraických manipulacích zlepšit.

Úmluva. Úlohy jsou v tomto příspěvku označeny slovem **Příklad**, pokud patří mezi ty snazší, a slovem **Úloha**, pokud patří mezi ty náročnější.

Poznámka. (symetrie a cykličnost) Výraz v několika proměnných je symetrický, pokud se nezmění prohozením libovolných dvou z nich. Pak můžeme BÚNO předpokládat, že proměnné jsou v námi vybraném pořadí (např. od největší po nejmenší).

Výraz je cyklický, pokud se nezmění po cyklické záměně (např. x za y, y za z a zároveň z za x). Poté můžeme BÚNO předpokládat například to, že jedna z proměnných je největší. Tyto úvahy často zkrátí sepisování řešení alespoň na polovinu.

Dosazení

Máme-li soustavu rovnic, často stačí jednu proměnnou vyjádřit a dosadit.

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

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

Příklad 2. Pro nenulová reálná čísla a, b, c platí

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

Ukažte, že pak platí i $a^2-c^2=ab$.

Rozklady na součin

Mají-li se v úloze najít všechna prvočísla určitého tvaru, zpravidla se snažíme příslušný výraz rozložit na součin, protože pak je snadné říci, kdy půjde o prvočísla (jen jeden z činitelů je různý od ± 1). Ale umět rozkládat na součin se hodí i jindy.

Příklad 3. Najděte dvě čtyřmístná čísla, jejichž součinem je $4^8+6^8+9^8$.

Příklad 4. Najděte všechna celá čísla n, pro něž je n^4-3n^2+9 prvočíslo.

(MO 61-III-1)

[2] *http://mks.mff.cuni.cz/archive/29/9.pdf*

Úloha 5. Dokažte, že existuje nekonečně mnoho kladných celých čísel a takových, že pro žádné $n \in \mathbb{N}$ není $n^4 + a$ prvočíslo. (IMO 1969)

Úloha 6. Najděte nejmenší trojciferné číslo n, pro nějž má soustava

$$x^3 + y^3 + x^2y + xy^2 = n,$$
$$x^2 + y^2 + x + y = n + 1$$

pouze celočíselná řešení.

Substituce $xyz = 1$

Máme-li na proměnné podmínku $xyz = 1$, často pomůže substituce

$$x = \frac{a}{b}, \qquad y = \frac{b}{c}, \qquad z = \frac{c}{a}.$$

Cvičení. Rozmyslete si, že tuto substituci opravdu můžeme použít, tedy že pro každá x, y, z splňující tuto podmínku existují vhodná a, b, c.

Příklad 7. Opět vyřešte Příklad 1.

Příklad 8. Kladná čísla a, b, c splňují $abc = 1$. Dokažte

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

Úloha 9. Pro kladná a, b, c splňující $abc = 1$ dokažte

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

(MO 52-III-6)

Substituce $x' = x + c$

Ještě jednodušší substituce je pouhý posun všech proměnných o konstantu, často ale vyřeší celou úlohu.

Příklad 10. Najděte všechna reálná x splňující

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

V následujícím příkladu budeme využívat jedno zajímavé tvrzení o polynomech (jinak ale pro naši přednášku nedůležité).

Věta. (Eisensteinovo kritérium) *Budiž $P(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ polynom s celočíselnými koeficienty a p prvočíslo takové, že*

(i) $p \nmid a_n$,
(ii) $p \mid a_i, \quad \forall i \in \{0, \ldots, n-1\}$,
(iii) $p^2 \nmid a_0$.

Potom je polynom $P(x)$ ireducibilní nad $\mathbb{Q}$ (tedy neexistují nekonstantní polynomy s racionálními koeficienty, jejichž součin by byl rovný P).

Příklad 11. Nechť p je prvočíslo. S pomocí Eisensteinova kritéria dokažte, že polynom $P(x) = x^{p-1} + x^{p-2} + \cdots + 1$ je ireducibilní nad $\mathbb{Q}$.

Úloha 12. Jsou dána reálná čísla x, y, z, která splňují

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

Ukažte, že alespoň jedno z čísel x, y, z je nejvýše rovno třem a alespoň jedno je větší nebo rovno pěti. (MO 60-III-3)

Linearita proměnné

Máme-li výraz, který je v některé proměnné lineární, pak bude nabývat svých extrémů pro její krajní hodnoty. To úlohu mnohdy velmi zjednoduší nebo úplně vyřeší.

Příklad 13. Jsou dána čísla a, b, c z intervalu $\langle 0, 1\rangle$. Ukažte nerovnosti

$$6 \geq 3abc + 4(1-a)(1-b)(1-c) + a + b + c \geq 1.$$

(MKS 28-7-6)

Příklad 14. Nalezněte minimum a maximum výrazu

$$a(1-b) + b(1-c) + c(1-a),$$

v němž a, b, c jsou z intervalu $\langle 0, 1\rangle$.

Příklad 15. Pro $x, y \in \mathbb{R}$ a $z \in \langle -2, 2\rangle$ ukažte nerovnost

$$x^2 + y^2 \geq xyz.$$

Příklad 16. Nechť $n \geq 2$, $0 \leq x_i \leq 1$, $i = 1, 2, \ldots, n$. Dokažte nerovnost

$$\sum_{i=1}^{n} x_i - \sum_{i=1}^{n} x_i x_{i+1} \leq \left\lfloor \frac{n}{2} \right\rfloor,$$

kde $x_{n+1} = x_1$. (Výběrové soustředění 2016)

Homogenita

Definice. (homogenita) Výraz $V(a, b, c)$ nazveme homogenní stupně α, pokud existuje $\alpha \in \mathbb{R}$ takové, že pro každé $t > 0$ platí

$$V(ta, tb, tc) = t^\alpha V(a, b, c).$$

Máme-li homogenní nerovnost, můžeme si pomoci tím, že si přidáme nějakou podmínku (jejíž splnění můžeme zaručit právě pomocí t v předchozí definici).

Příklad 17. Pro $a, b \geq 0$ a $s \geq r$ dokažte

$$(a^r + b^r)^{\frac{1}{r}} \geq (a^s + b^s)^{\frac{1}{s}}.$$

Příklad 18. Pro $a, b > 0$ ukažte

$$a^4 + 2b^4 \geq a^2b^2 + 2ab^3.$$

Úloha 19. Dokažte Cauchy-Schwarzovu nerovnost: $n \in \mathbb{N}$, dále $u_1, u_2, \ldots, u_n \in \mathbb{R}$ a $v_1, v_2, \ldots, v_n \in \mathbb{R}$. Pak

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

(Ne)rovnost

Máme-li nějakou rovnici nebo soustavu rovnic, můžeme si někdy pomoci tím, že ukážeme, že jedna strana je větší než druhá, a využijeme, že víme, kdy v námi použité nerovnosti nastává rovnost.

Úloha 20. V oboru reálných čísel řešte soustavu rovnic

$$\begin{aligned} x^4 + y^2 + 4 &= 5yz, \\ y^4 + z^2 + 4 &= 5zx, \\ z^4 + x^2 + 4 &= 5xy. \end{aligned}$$

(MO 61-III-6)

Úloha 21. Určete všechny trojice (a, b, c) kladných reálných čísel, které jsou řešeními soustavy rovnic

$$\begin{aligned} a\sqrt{b} - c &= a, \\ b\sqrt{c} - a &= b, \\ c\sqrt{a} - b &= c. \end{aligned}$$

(ČPS 2010)

Polynomy

Příklad 22. Mějme reálná čísla x, y, z, pro která platí

$$\begin{aligned} x + y + z &= 0, \\ xy + yz + zx &= 0. \end{aligned}$$

Dokažte, že $x = y = z = 0$.

Příklad 23. Ukažte, že pokud pro nenulová reálná čísla a, b, c platí rovnost

$$\frac{a-b}{c}+\frac{b-c}{a}+\frac{c-a}{b}=0,$$

tak se dvě z těchto tří čísel rovnají.

Příklad 24. Jakých hodnot může nabývat výraz

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

pro všechny možné trojice po dvou různých reálných čísel a, b, c?

(Výběrové soustředění 2013)

Úloha 25. Nechť a, b, c, d, e, f jsou přirozená čísla. Označme $S = a+b+c+d+e+f$. Platí, že S dělí výrazy $abc + def$ a $ab + bc + ca - de - ef - fd$. Dokažte, že S je složené. (IMO shortlist 2005)

Algebra? Ne, geometrie!

Úloha 26. Dvojice nekonečných posloupností celých čísel $a_1, a_2, \ldots$ a $b_1, b_2, \ldots$ splňuje pro $n \geq 3$ vztah

$$(a_n - a_{n-1})(a_n - a_{n-2}) + (b_n - b_{n-1})(b_n - b_{n-2}) = 0.$$

Ukažte, že existuje přirozené k takové, že $a_k = a_{k+2016}$. (iKS 5. ročník, A5)

Úloha 27. Vyřešte úlohu 12, tentokrát geometricky.

Trikové úpravy

Úloha 28. Celá čísla x, y, z splňují vztah

$$(x-y)^2 + (y-z)^2 + (z-x)^2 = xyz.$$

Dokažte, že výraz $x^3 + y^3 + z^3$ je dělitelný $x + y + z + 6$.

Úloha 29. Nechť existuje $n > 0$ reálných čísel $x_1, x_2, \ldots, x_n$, která pro každé $i = 1, \ldots, n$ splňují

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

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

Úloha 30. Pro libovolná nezáporná reálná čísla a a b dokažte nerovnost

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

a zjistěte, kdy nastane rovnost. (MO 63-III-6)

Návody

1. Dosaďte $z = \frac{1}{xy}$ a zlomky zjednodušte a sečtěte.

2. Z první rovnice dosaďte za c do druhé a třetí. Nyní má z druhé rovnice plynout třetí. Všimněte si, že druhou rovnici lze vydělit a, a potom ji vytkněte ze třetí rovnice.

3. Přičtěte 6^8, abyste mohli využít vzorečku, a pak ho opět odečtěte a využijte jiného vzorečku. Ověřte čtyřmístnost obou čísel.

4. Přičtěte a odečtěte $9n^2$ a s pomocí dvou vzorečků rozložte na součin.

5. Zvolte $a = 4m^4$ pro $m > 1$ a rozložte na součin.

6. Označte $a = x^2 + y^2$, $b = x + y$, odvoďte $a = n$, $b = 1$. Vyřešte kvadratickou rovnici a odvoďte, v jakém tvaru musí být n. Výsledek by měl být 113.

7. Tady se fakt nedá nic nového radit :D. Udělejte substituci a upravte (sečtěte zlomky).

8. Udělejte substituci a použijte AG-nerovnost (jde to i rovnou bez substituce, ale po substituci je to lépe vidět).

9. Po substituci nerovnost vynásobte třemi a rozložte ji na součet tří cyklických AG-nerovností.

10. Rozložte kvadratické trojčleny na součin, zvolte $y = x-1$ a následně $z = y^2$. Vyřešte kubickou rovnici v z natipováním kořenů.

11. Polynom sečtěte na $P(x) = \frac{x^p-1}{x-1}$, uvažte polynom $Q(x) = P(x+1)$ a dokažte, že je ireducibilní. Uvědomte si, že P je pak také nutně ireducibilní.

12. Pro první část uvažme $x = a + 3$, $y = b + 3$, $z = c + 3$. Pro druhou $x = 5 - a$ atd. Potom už stačí říct, že je jedno z a, b, c nekladné.

13. Stačí rozebrat osm možností, kdy $a, b, c \in \{0, 1\}$. Díky symetrii výrazu můžete navíc předpokládat $a \geq b \geq c$ a rozebírat jen čtyři možnosti.

15. Díky linearitě v proměnné z stačí rozebrat případy $z = \pm 2$.

16. Využijte linearitu a představte si n kuliček na kružnici, kde některé jsou černé a některé bílé. Co počítá výraz na levé straně?

17. BÚNO předpokládejte $a^r + b^r = 1$. Pak $1 \geq a, b \geq 0$, a tedy $a^r \geq a^s$ a $b^r \geq b^s$.

18. BÚNO předpokládejte $b = 1$ a polynom rozložte na součin tipováním kořenů.

19. Nejprve z homogennosti v $u_1, \ldots, u_n$ BÚNO předpokládejte $u_1^2 + \cdots + u_n^2 = 1$, pak ještě stejnou úvahu zopakujte pro $v_1, \ldots, v_n$. Nakonec využijte odhady $\frac{1}{2}u_i^2 + \frac{1}{2}v_i^2 \geq u_i v_i \geq -\left(\frac{1}{2}u_i^2 + \frac{1}{2}v_i^2\right)$.

20. Využijte odhad $4x^2 \leq x^4 + 4$ a jeho cyklické záměny a získané nerovnosti sečtěte.

21. BÚNO předpokládejte, že a je největší a dokažte postupně $b \leq 4$, $c \geq 4$ a $c \leq b$.

22. Uvažte polynom třetího stupně s kořeny x, y, z a pomocí Viètových vztahů odvoďte, že je tvaru $t^3 + c = 0$.

23. Vynásobte abc a uvažujte jako polynom v a. Dokažte, že se rovná polynomu $(b-c)(a-b)(a-c)$.

24. Označte výraz ze zadání jako výraz $V(a)$ v neznámé a s parametry b, c. Uvažte polynom $P(a) = V(a)(a-b)(b-c)(c-a)$, ukažte, že je druhého stupně a b i c jsou jeho kořeny (pozor, to není jasné, protože $V(a)$ není polynom!). Stejně jako v předchozím příkladu rozložte polynom $P(a)$, když znáte jeho kořeny.

25. Uvažte polynom $P(x) = (x+a)(x+b)(x+c) - (x-d)(x-e)(x-f)$.

26. Uvažujte body v rovině $X_n = (a_n, b_n)$. Rozmyslete si, že trojúhelník X_n, X_{n-1}, X_{n-2} má pravý úhel u vrcholu X_n. Z Pythagorovy věty odvoďte, že vzdálenosti mezi po sobě jdoucími body se nezvětšují, a využijte celočíselnosti.

27. Uvědomte si, že soustava rovnic definuje kružnici v prostoru. Tu rozdělte na šest částí (vždy získáte dva body při průniku kružnice s rovinou danou dvěma osami) a pro každou část si rozmyslete, jakých hodnot v ní nabývají jednotlivé souřadnice.

28. Využijte vzoreček $a^3 + b^3 + c^3 - 3abc = (a + b + c)(a^2 + b^2 + c^2 - ab - bc - ca)$.

29. V součtu druhých mocnin nahraďte vždy jedno x_i pomocí vztahu v zadání.

30. Roznásobte, upravte, aby na obou stranách byl rozdíl odmocnin, a netradičním způsobem využijte vztah $x^2 - y^2 = (x - y)(x + y)$.

Literatura a zdroje

Obrovský dík patří *Štěpánu Šimsovi*, od něhož byl příspěvek (skoro beze změn) převzat.

[1] Štěpán Šimsa: *Algebrické triky*, Lipová-lázně, 2016.
[2] Michal „Kenny“ Rolínek: *Algebraické legrácky*, Blansko-Obůrka, 2011.
[3] Michal „Kenny“ Rolínek, Pavel Šalom: *Zdolávání nerovností*, *http://mks.mff.cuni.cz/archive/29/9.pdf*.
[4] Martina Vaváčková: *Rozklady na součin*, Hojsova Stráž, 2011.

Funkcionální rovnice

φla Čermák

Abstrakt. Na přednášce si představíme základní metody řešení funkcionálních rovnic. Následuje pak řada příkladů různé obtížnosti na procvičení.

Pár slov úvodem

Co jsou to vlastně ty funkcionální rovnice zač? Podrobně si to vysvětlíme na následujícím příkladu:

Úloha. Nalezněte všechny rostoucí funkce $f : \mathbb{R} \to \mathbb{R}$, které pro všechna $x, y \in \mathbb{R}$ splňují

$$f(x + y) = f(x) + f(y).$$

Úlohu si můžeme představovat jako řešení soustavy rovnic s nekonečně mnoha neznámými (které jsou označeny $f(x)$ pro $x \in \mathbb{R}$). Kvůli tomu, že je neznámých tolik, nemají klasické metody na řešení soustav moc velkou šanci fungovat. Například výše uvedená rovnice je „lineární“[1], takže kdyby se jednalo o konečnou soustavu, uměli bychom ji snadno vyřešit. Přítomností nekonečna však můžeme získat mnohem bohatší strukturu, například bez přidané podmínky „f je rostoucí“ by daná rovnice měla spoustu extrémně divných a divokých řešení. Potřebujeme tedy přijít s nějakými novými metodami, které budou fungovat i na nekonečné soustavy. Pojďme si některé z nich předvést a vysvětlit na příkladech!

Substituční metoda

Nejběžnější metodou řešení funkcionálních rovnic je tzv. substituční metoda. Za tímto slušivým názvem se však neskrývá nic jiného než „dosazujeme do rovnice konkrétní věci a doufáme, že z toho něco vypadne“. Pokud totiž rovnice platí pro libovolné hodnoty x, y, tak jistě platí například i pro konkrétní volbu $x = 6$, $y = 2$. V těch nejjednodušších případech můžeme přímo dostat tvar, ve kterém řešení musí být. Občas dostaneme nějaké informace o jejích hodnotách v konkrétních bodech. Nejčastěji však zbude nějaká jiná funkcionální rovnice, která je s trochou štěstí hezčí nebo jednodušší než ta původní.

V těžších úlohách se však typicky stává, že postupně dokazujeme různé vlastnosti hledané funkce, které jdou dále dobře využít. Následuje výčet užitečných vlastností funkcí, které je třeba mít na paměti:

[1] Ať už to znamená, co to znamená.

Definice. O funkci f (do $\mathbb{R}$) řekneme[2], že je:

(1) *sudá* pokud $f(x) = f(-x)$,
(2) *lichá*, pokud $f(x) = -f(-x)$,
(3) *prostá* (nebo že je f *injekce*), pokud $f(x) = f(y)$ vynucuje $x = y$,
(4) *na* (nebo *surjektivní*), pokud pro každé $y \in \mathbb{R}$ existuje x, pro něž $f(x) = y$,
(5) *bijekce*, pokud je *prostá* i *na*,
(6) *rostoucí*, pokud $f(x) < f(y)$ pro $x < y$,
(7) *klesající*, pokud $f(x) > f(y)$ pro $x < y$,
(8) *periodická s periodou p*, pokud je $x+p$ v definičním oboru a $f(x+p) = f(x)$,
(9) *omezená*, pokud existuje M takové, že $|f(x)| \leq M$.

Existuje několik typů dosazení, které se hodí obzvlášť často. Patří mezi ně například:

(1) $x = 0$ a/nebo $y = 0$, případně další konstanty, které situaci zjednoduší,
(2) prohodit x a y,
(3) $x = y$ a $x = -y$: zbaví nás jednoho stupně volnosti, například z toho vyplyne parita hledané funkce,
(4) něco, co vytvoří soustavu rovnic – občas se může stát, že správná dosazení poskytnou například soustavu lineárních rovnic v $f(A(x, y))$, $f(B(x, y))$, $f(C(x, y))$ pro nějaké výrazy A, B, C; pak ji (s)prostě vyřešte!
(5) Zkuste si tipnout jedno řešení $c(x)$. Pokud si myslíte, že je jediné, zkuste dosadit za $f(x) = c(x) + g(x)$, a dokázat že $g(x)$ je dost vychované.
(6) $y = f(x)$ a naopak. Nelze zapomínat, že $f(x)$ je reálné číslo jako každé jiné, takže ho můžeme do rovnice dosadit.
(7) Dosazení, kterým vyrovnáme dva argumenty: například jestliže na jedné straně rovnice máme $f(y \cdot f(x))$ a na druhé $f(x)$, tak se výrazy při volbě $y = \frac{x}{f(x)}$ vykrátí a rovnice značně zjednoduší.
(8) Krok v důkazu sporem: dokazujete-li například prostotu f, často se vyplatí zkoumat, co by se stalo po dosazení $a \neq b$ s $f(a) = f(b)$ za jednu z proměnných.
(9) Vytváření symetrie: například z $f(x + f(y)) = f(x) + y$ plyne po dosazení $x = f(t)$ symetrická rovnice $f(f(t) + f(y)) = f(f(t)) + y$, ze které okamžitě plyne $f(f(y)) + t = f(f(t)) + y$.

Úmluva. Dosazení hodnot $x = a$, $y = b$ do funkcionální rovnice se většinou pro stručnost a přehlednost značí $[a, b]$.

Úmluva. Není-li v úloze upřesněn definiční obor či obor hodnot, míní se jím $\mathbb{R}$.

Aplikaci těchto metod si ukážeme na následujících příkladech:

Úloha 1. $f : \mathbb{R}^+ \to \mathbb{R}^+$, $f(x^2) = x + f(y) - \frac{y}{f(y)}$.

Úloha 2. $f(xy + 1) + f(x + y) = (f(x) + 1)(y + 1)$.

[2]V těchto definicích chceme, aby vztah platil pro všechna x, resp. y z definičního oboru f.

Úloha 3. $f(f(x)+f(y))=f(x)+y$.

Úloha 4. (varovná) $f(x+f(y))=f(x)+f(y)^2+2xf(y)$.

Úloha 5. (též varovná) $f(x^2+y)+f(f(x)-y)=2f(f(x))+2y^2$.

Úloha 6. $f:\mathbb{R}\setminus\{0,1\}\to\mathbb{R}$, $f(x)+f(\frac{1}{1-x})=x$.

Úloha 7. $f:\mathbb{R}^+\to\mathbb{R}^+$, $(1+yf(x))(1-yf(x+y))=1$.

Úloha 8. $f(f(x))=x$, f je rostoucí.

Cauchyho rovnice a kamarádi

Jedná se nejspíše o nejznámější funkcionální rovnici. Vyplatí se znát ji (i se způsobem řešení). V řešení se totiž objevuje řada užitečných myšlenek: indukce, přechod z $\mathbb{Q}$ do $\mathbb{R}$, ...

Úloha. (Cauchyho rovnice nad $\mathbb{Q}$) $f:\mathbb{Q}\to\mathbb{Q}$, $f(x+y)=f(x)+f(y)$.

Může se zdát, že by nemělo být těžké přejít od řešení nad racionálními čísly k řešení nad reálnými, ale opak je bohužel pravdou. Existuje totiž spousta patologických řešení, jejichž pouhý popis je nad rámec přednášky. Můžeme ale přidat nějaké podmínky, které situaci zachrání:

Úloha. (Cauchyho rovnice nad $\mathbb{R}$) $f(x+y)=f(x)+f(y)$, přičemž známe jednu z následujících vlastností f:

(1) f je monotónní na nějakém intervalu,
(2) f zobrazuje $\mathbb{R}^+$ na $\mathbb{R}^+$,
(3) f je omezená na nějakém intervalu.

Úloha 9. $f(x+y)=f(x)f(y)$, f je rostoucí.

Úloha 10. $f:\mathbb{R}^+\to\mathbb{R}$, $f(xy)=f(x)f(y)$ a $f(x)>1$ pro $x>1$.

Úloha 11. Dokažte, že identita je jediná reálná funkce, zachovávající sčítání i násobení.

Úloha 12. $f(x+y)+f(x)f(y)=f(xy)+f(x)+f(y)$. (Bulharská olympiáda)

Další tipy a triky

Dříve, než se vrhnete na řešení příkladů, tak následuje ještě pár užitečných tipů:

Tipujte řešení
Při hádání můžete postupovat buď intuitivně, nebo do rovnice dosazovat obecné předpisy (například) pro konstantní, lineární, kvadratickou nebo lineární lomenou funkci. Pokud už nějaká řešení znáte, tento přístup vám může výrazně napomoci: například pokud vyhovuje $f:\mathbb{R}\to\mathbb{R}$, $f(x)=x^2$, nemá cenu dokazovat, že f je prostá či monotónní. Někdy nám může řešení poradit dobrou substituci: je-li jediné řešení $f(x)=x+1$, pak substituce jako $g(x)=f(x)-1$ či $h(x)=f(x-1)$ můžou rovnici krásně zpřehlednit.

Dbejte definičního oboru
Pokud řešíte rovnici nad kladnými čísly, nezkoušejte dosazovat nulu (nebo třeba dvojici $(x, -x)$). Naopak definiční obor může někdy něco prozradit o řešení: například je-li to $\mathbb{R} \setminus \{1\}$, pak můžete očekávat jedničku někde ve jmenovateli.

Mějte přehled o tom, co už víte
Při řešení funkcionálek budete typicky dostávat spoustu všemožných vztahů, o kterých si nemůžete být předem jistí, jestli vůbec k něčemu budou. Proto si velmi zjednodušíte život, když budete postupovat co nejsystematičtěji (například zkoušet kombinovat nově získané rovnice s těmi předchozími) a přehledně zapisovat veškerý pokrok, kterého se vám zatím podařilo dosáhnout[3].

Postupujte odzadu
Velmi se hodí včas si uvědomit, že už například jenom stačí dokázat, že f je prostá. Ušetříte si tím spoustu času a pokud se vám náhodou během soutěže nepovede danou vlastnost dokázat, tak můžete rovnici dořešit s tím, že ji budete předpokládat. Pokud se této vlastnosti využívá i ve vzorovém řešení (nebo ji není těžké dokázat), tak i za to dostanete body :).

Dělejte zkoušku ...
... nebo alespoň napište, že jste ji udělali. I soutěžící na IMO kvůli tomu občas zbytečně ztrácí body. Kdybyste si měli z téhle přednášky odnést jednu jedinou věc, tak tohle je ta jediná pravá. Proč je zapotřebí? V průběhu řešení typicky odvozujeme řadu nutných podmínek, které musí funkce f splňovat. Na konci řešení však typicky nevíme nic o tom, jestli jsou tyto podmínky i postačující!

Konečně příklady!

Příklad 13. $f(y - xy) = f(x)y + (x-1)^2 f(y)$. (CKMO 2017–3)

Příklad 14. $f : \mathbb{R}^+ \to \mathbb{R}^+$, $f(x)f(y) = f(y)f(xf(y)) + \frac{1}{xy}$. (CKMO 2011–6)

Příklad 15. $f(x^2 + f(x)f(y)) = xf(x+y)$. (MEMO 2017–I1)

Příklad 16. $f : \mathbb{R} \setminus \{0\} \to \mathbb{R} \setminus \{0\}$, $f(x^2 y f(x)) + f(1) = x^2 f(x) + f(y)$. (MEMO 2015–T2)

Příklad 17. $f : \mathbb{R}^+ \to \mathbb{R}^+$, $f(x + f(y)) = yf(xy+1)$. (MEMO 2012–I1)

Příklad 18. $f : \mathbb{R}^+ \to \mathbb{R}^+$, $\frac{f^2(w)+f^2(x)}{f(y^2)+f(z^2)} = \frac{w^2+x^2}{y^2+z^2}$ pro čtveřice čísel splňující $xw = yz$. (IMO 2008–4)

Příklad 19. $f(\lfloor x \rfloor y) = f(x) \lfloor f(y) \rfloor$, kde $\lfloor t \rfloor$ je největší celé číslo, které je menší nebo rovno t. (IMO 2010–1)

Příklad 20. $f : \mathbb{Q}^+ \to \mathbb{Q}^+$, $f(x^2 f(y)^2) = f(x)^2 f(y)$. (IMO SL 2018–A1)

[3] Ne, že bych to sám dělal. Ale jo, fakt to pomůže.

Příklad 21. $(f(x)+f(y))(f(u)+f(v)) = f(xu-yv)+f(xv+yu)$. (IMO 2002–5)

Příklad 22. $f:\mathbb{Q}^+\to\mathbb{R}$, splňující:

(1) $f(x+y)\geq f(x)+f(y)$,
(2) $f(xy)\geq f(x)f(y)$,
(3) $f(a)=a$ pro nějaké $a>1$. (IMO 2013–5)

Příklad 23. $f(f(x)+x+y^2)=2x+f(y)^2$. (iKS 4–A6)

Příklad 24. $f:\mathbb{Q}\to\mathbb{Q}$, $f(x)+f(w)=f(y)+f(z)$ pro aritmetické posloupnosti $x<y<z<w$. (iKS 6–A1, USAJMO 2015–4)

Příklad 25. $f:\mathbb{R}^+\to\mathbb{R}^+$, $f(x+f(x)y)=f(x)f(y)$. (Golabova-Schinzelova rovnice)

Návody

13. $[x,1]$, $[1-x,y]$ a symetrie.

14. $[1,y]$, $[x,1]$ a pak zkuste vše vyjádřit s pomocí parametru $c=f(1)$.

15. f má kořen, tak ho dosaďte; pak dokažte prostotu (pro nekonstantní f).

16. Dosazováním jedniček ukažte $|f(1)|=1$, pak substituujte $g(x)=x^2f(x)$ a zkoumejte obor hodnot g.

17. Vyrovnejte argumenty a pak pro $y>1$ zvolte x, aby $y=xy+1$.

18. $f(x)^2=f(x^2)$, pak vhodné dosazení dá $f(x)=x$ nebo $f(x)=\frac{1}{x}$ pro každé x; pak třeba zkoušky.

19. Dosaďte nuly a rozeberte pár případů.

20. $f(x^2)=f(x)^2$ a pak dokažte, že $f(x)$ je 2^n-tá mocnina racionálního čísla pro každé $n\in\mathbb{N}$.

21. Různě tam dosazujte nuly, eliminujte konstantní řešení, pak vyjde $f(ab)=f(a)f(b)$, takže stačí monotonie f a lehce obměněný příklad 10.

22. Dokažte, že funkce nabývá jen nezáporných hodnot, z toho odvoďte, že je rostoucí a $f(x)\geq x$.

23. Dokažte $f(0)=0$, lichost a pak převeďte na Cauchyho rovnici.

24. Přidejte si pátý člen posloupnosti.

25. Vyrovnejte argumenty.

Literatura a zdroje

Tímto děkuji *Danilu Koževnikovi*, jehož přednášku jsem více(méně) převzal.

[1] Vít Musil: *Funkcionální rovnice*, Oldřichov, 2012.
[2] Franta Konopecký: *Funkcionální rovnice*, Rapotín, 2007.
[3] *Art of Problem Solving*, *https://artofproblemsolving.com/*.

Diskrétní spojitost

Matěj Doležálek

Abstrakt. Nepříliš vtipný vtip o statisticích praví: „Vydají se tři statistici na lov a narazí na PraSe. První statistik vystřelí, ale mine zleva. Druhý vystřelí, ale mine zprava. ‚Máme ho!', prohlásí nadšeně třetí." Tento vtip, vzdor profesi svých protagonistů, poměrně věrně popisuje kombinatorickou techniku zvanou *diskrétní spojitost*: když veličina dovede být velká i malá a neumí přeskakovat hodnoty uprostřed, pak je musí taky trefit.

Úloha 0. (motivační) Na rovinné louce se pase 2023 bodových prasátek. Pastevec Rado se doslechl, že se k louce blíží vlk, který chce prasátka sežrat. Samozřejmě chce prasátka zachránit, a proto by kolem nich rád postavil kruhovou ohradu (jiné tvary neuznává). Zároveň by si ovšem rád naklonil Štěstěnu na svoji stranu, proto by chtěl nechat právě 42 prasátek mimo ohrádku, a tím učinit krvavou oběť svému Pánu a Spasiteli Belzebubu. Ukažte, že takovou ohrádku skutečně umí postavit.

Řešení. Nejprve ukážeme, že existuje bod B, na kterém nestojí žádné prasátko a který zároveň nemá k žádným dvěma prasátkům stejnou vzdálenost. To plyne z toho, že pokud má bod ke dvěma prasátkům stejnou vzdálenost, potom leží na ose úsečky, která je spojuje. Tím máme ale zakázaný jen konečný počet (konkrétně $\binom{2023}{2}$) přímek a konečný počet bodů, což nám určitě nepokryje celou rovinu. Proto bod B s požadovanými vlastnostmi vskutku existuje.

Nyní, když jsme hotovi s technikáliemi, přejdeme na skutečné použití diskrétní spojitosti. Uvažujme kružnici k_1 se středem v B, která neobsahuje žádné prasátko (ta existuje – prostě zvolme poloměr menší, než je vzdálenost B k nejbližšímu prasátku). Postupně ji nafukujme, dokud všechna prasátka neleží uvnitř kružnice. Na začátku se mimo kružnici páslo $2023 > 42$ prasátek, na konci je to $0 < 42$. Protože při nafukování najednou přidáme vždy jen jedno prasátko (protože B nemá k žádným dvěma prasátkům stejnou vzdálenost), musí jednou určitě nastat taková situace, kdy se právě 42 prasátek nachází mimo ohrádku.

Základní úlohy

Úloha 1. Dánsko a Anglie spolu hrály fotbal. Dánský tým dal celkem osm gólů, kdežto anglický pět. Musel během utkání existovat okamžik, kdy se počet gólů, které již Anglie dala, rovnal počtu gólů, které Dánsko ještě dá? (PraSe 37–1j–1)

Úloha 2. E.T. k narozeninám dostal krásný kruhový dort a hned se rozhodl půlkruhovou část z něj věnovat nejlepšímu řešiteli PraSátka. Než ji ale stihl odkrojit, Pepa už dort nakrájel tradičním způsobem na právě $4k$ dílků tak, že $2k$ z nich bylo větších (navzájem stejných) a $2k$ menších (též navzájem stejných). Dokažte, že E.T. i tak našel několik sousedních dílků, které tvořily půlkruh. (PraSe 33–1j–5)

Úloha 3. V oboustranně nekonečné řadě stojí pionýři a žampióny. Je známo, že v libovolném úseku několika vedle sebe stojících organismů se počet pionýrů a žampiónů liší nanejvýš o 1000. Dokažte, že v nějakém úseku 2000 organismů stojí přesně 1000 pionýrů a 1000 žampiónů. (Itálie 2013)

Úloha 4. Nekonečná posloupnost $\{a_i\}_{i=1}^{\infty}$ splňuje, že $a_1 = 1$ a pro libovolné přirozené i je rozdíl $a_{i+1} - a_i$ roven 0 nebo 1. Víte-li, že pro jisté n platí $a_n = \frac{n}{1000}$, dokažte, že existuje m splňující $a_m = \frac{m}{500}$.

Úloha 5. Každá ze stěn osmi jednotkových krychliček je obarvena modře, nebo červeně, přičemž celkově je modrých stěn stejně jako červených. Dokažte, že krychličky lze složit do jedné krychle $2 \times 2 \times 2$, na jejímž povrchu bude modrá barva zabírat stejnou plochu jako červená.

Úloha 6. Ukažte, že existuje 1000 po sobě jdoucích přirozených čísel, mezi nimiž je právě 5 prvočísel. (PraSe 30–1p–4)

Úloha 7. Přirozené číslo n nazveme *budovatelské*, pokud se dá zapsat ve tvaru $n = a^b + b$ pro přirozená čísla $a, b > 1$. Dokažte, že existuje úsek 2014 po sobě jdoucích přirozených čísel s přesně x budovatelskými čísly

(i) pro $x = 2012$, (Srbsko 2014)
(ii) (těžší) pro libovolné $x \in \{0, 1, \ldots, 2014\}$.

Úloha 8. Je dána rostoucí posloupnost přirozených čísel $a_0, a_1, \ldots$ Dokažte, že existuje právě jedno přirozené $n \geq 1$ splňující

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

(IMO 2014)

Úloha 9. Jsou dána přirozená čísla p, q, n, kde $p + q < n$, a $(n+1)$-tice čísel $(x_0, x_1, \ldots, x_n)$, pro niž platí:

(i) $x_0 = x_n = 0$.
(ii) Pro každé $i \in \{1, \ldots, n\}$ je $x_i - x_{i-1}$ buďto p, nebo $-q$.

Dokažte, že existují indexy $i < j$ s $(i, j) \neq (0, n)$, pro něž platí $x_i = x_j$.

(IMO 1996)

Záludnější úlohy

Diskrétní spojitost není vždy tím jediným, nebo dokonce ani ne tím hlavním, co úloha potřebuje. Často ji potkáme jako jednu z mnoha ingrediencí, kterou je třeba šikovně kombinovat s něčím dalším – třeba indukcí nebo Dirichletovým principem. Tyto úlohy neřadím nutně podle obtížnosti, spíše podle společných témátek.

Úloha 10. V každém vrcholu pravidelného 2018úhelníku seděl ráno jeden termit. Tito termiti byli v nějakém pořadí označení čísly 1 až 2018 (každé číslo bylo použito). Jediné, co termiti umějí, je vyměnit si místo se svým sousedem. Večer se každý termit nacházel ve vrcholu naproti tomu, v němž začínal. Dokažte, že se někdy v průběhu dne prohodili dva termiti se součtem čísel 2019. (PraSe 38–1p–7)

Úloha 11. (těžší) Máme n červených a n modrých karet, na každé z nichž je nějaké číslo od 1 do n (čísla se mohou opakovat). Je vždy možné vybrat několik modrých a několik červených karet tak, aby měly modrá a červená skupinka stejný součet? (PraSe 40–4j–5b)

Následuje pár úložek s posloupnostmi:

Úloha 12. Uvažme posloupnost $\{a_n\}_{n=0}^{\infty}$ takovou, že $a_0 = 0$. Další členy definujme následovně. Pro přirozené číslo n označme ℓ_n největší liché číslo, které dělí n. Pak položme $a_n = a_{n-1} + 1$, pokud ℓ_n dává po dělení čtyřmi zbytek 1, a $a_n = a_{n-1} - 1$, pokud dává zbytek 3. Dokažte, že pro každé přirozené číslo m existuje nekonečně mnoho i takových, že $a_i = m$. (PraSe 39–1j–5)

Úloha 13. Nechť $p(n)$ pro přirozené číslo $n > 1$ značí největší prvočíslo, které dělí n. Nekonečná posloupnost $\{a_i\}_{i=1}^{\infty}$ splňuje $a_1 > 1$ a rekurenci $a_{i+1} = a_i + p(a_i)$. Dokažte, že v posloupnosti $\{a_i\}$ se vyskytuje čtverec. (Čína 2020)

Úloha 14. (těžší) Jsou dány dvě posloupnosti $\{a_n\}_{n=1}^{\infty}$ a $\{b_n\}_{n=1}^{\infty}$ přirozených čísel, přičemž pro všechna přirozená n je b_n rovno součinu všech různých prvočísel dělících a_n. Dále pro všechna $n \geq 2$ platí $a_n = a_{n-1} + b_{n-1}$. Dokažte, že existuje přirozené k splňující $\frac{a_k}{b_k} = 2019$. (PraSe 39–2p–7)

Úloha 15. (těžší) Jsou dána nesoudělná přirozená čísla p, q. Na číselné ose stojí klokan, a poněvadž jej baví skákat, skáče si po číselné ose, přičemž se může pohybovat doleva či doprava. Vždy, když skáče doprava, skáče o vzdálenost p, zatímco při poskakování doleva skáče vždy o q. Po jisté době doskáče zpátky tam, kde začal. Dokažte, že pro každé přirozené číslo $d < p + q$ existují dvě čísla, která klokan navštívil a která jsou od sebe vzdálena přesně d. (iKS–12–C6)

A na závěr něco málo z kombinatorické geometrie:

Úloha 16. V rovině je dáno n modrých a n červených bodů, přičemž žádné tři barevné body neleží na jedné přímce. Dokažte, že lze nakreslit n úseček spojujících modrý a červený bod tak, že žádné dvě nebudou mít společný bod (ani koncový).

Úloha 17. Nechť $n > 1$ je přirozené číslo. V rovině se pase n bodových kraviček a n bodových oveček. Žádná tři zvířátka neleží na jedné přímce. *Balanční přímkou* nazveme přímku procházející jednou ovečkou a jednou kravičkou tak, že na každé straně od přímky je stejně oveček jako kraviček. Ukažte, že existují alespoň dvě balanční přímky. (USAMO 2005)

Úloha 18. (těžší) Nechť S je množina alespoň dvou bodů v rovině, z nichž žádné tři neleží na jedné přímce. *Větrným mlýnem* rozumíme následující proces: Na počátku je vybrána nějaká přímka ℓ procházející právě jedním bodem $P \in S$. Tato přímka se začne otáčet ve směru hodinových ručiček se středem otáčení P, dokud „nenarazí“ na další bod množiny S, označme jej Q. Přímka se nadále otáčí ve směru hodinových ručiček, ovšem se středem otáčení Q, dokud nenarazí na další bod množiny S, a tak dále. Tento proces neustále pokračuje (nekonečně dlouho). Dokažte, že lze zvolit bod $P \in S$ a přímku ℓ procházející bodem P tak, že jimi začínající větrný mlýn bude mít každý bod z S za střed otáčení nekonečněkrát. (IMO 2011)

Návody

1. Dívej se na $A - D$ jako funkci času. A a D jsou to, co by tak člověk čekal.

2. Posouvej zvolenou $2k$-tici dílků a sleduj počet menších, které jsou zvolené.

3. Kdyby úloha neplatila, zkonstruuješ dlooouhatánský úsek s větší převahou jednoho organismu, než je povolena.

4. Může $\frac{n}{a_n}$ přeskočit celé číslo?

5. Zprvu slož krychličky libovolně, pak je otáčej, abys dosáhl(a) opačné (ne)rovnováhy modré a červené barvy na povrchu.

6. Na začátku číselné osy je prvočísel hodně. Zkonstruuj úsek, kde je jich fakt málo.

7. Úsek s mnoha budovatelskými čísly sestrojíš explicitně. Pro část (ii) odhadni, kolik budovatelských čísel menších než x může existovat.

8. Co lze říct o posloupnosti $d_n = a_0 + a_1 + \cdots + a_n - na_n$?

9. BÚNO ber $\mathrm{NSD}(p, q) = 1$ a sleduj počty skoků o p v úsecích délky $p + q$.

10. Neprohodivší se doplňkoví termiti museli mít stejnou cestu.

11. Nakresli si tabulku $(n + 1) \times (n + 1)$ a zanes do ní součty částečných součtů modrých a červených karet. Rozparcelováním tabulky na slupky tvaru L kolem jednoho rohu spolu s diskrétní spojitostí a Dirichletem najdi dvě políčka se stejným číslem.

12. Odvoď a_{2n} na základě a_n. Z toho pak nahlédni, že posloupnost neomezeně poroste a nekonečně častokrát se vrátí do 1.

13. Ukaž, že posloupnost $b_n = \frac{a_n}{p(a_n)}$ je neomezená. Pak si můžeš zvolit nějaké šikovné číslo, které by měla trefit.

14. Kdy posloupnost $c_n = \frac{a_n}{b_n}$ roste? Nahlédni její neomezenost – to pomůže také ukázat, že se vždy vrátí k 1.

15. Pomocí Bézoutových koeficientů urči vhodný počet skoků a kolik $+p$ skoků v něm chceš najít. Technické nesnáze odstraň periodickým nakopírováním skoků. Kdyby nešla aplikovat diskrétní spojitost, posloupnost by utíkala k $\pm\infty$.

16. Snaž se vyřešit jednu libovolnou dvojici bodů. Nejde-li to snadno, rozděl úlohu na dvě menší.

17. Když na konvexním obalu sousedí ovečka a kravička, je to snadné. V těžším případě toč přímkou skrz zvířátko na konvexním obalu.

18. Zvol P, aby byl uprostřed ve směru kolmém na ℓ. Uděl ℓ orientaci a sleduj, kolik bodů je během otáčení nalevo a napravo od ní.

Literatura a zdroje

[1] Rado van Švarc: *Dvě neobvyklé existenční techniky*, Hojsova Stráž, 2016.
[2] *https://artofproblemsolving.com/community*.

Iterace

Matěj Doležálek

Abstrakt. Jak zkrotit funkci aplikovanou mnohokrát za sebou? Nakreslíme si obrázek a vydáme se na cestu po šipkách. Možná půjdeme do nekonečna a ještě dál, anebo se možná dostaneme do bludného kruhu, ale s trochou štěstí nám obojí něco poví o zkoumané funkci.

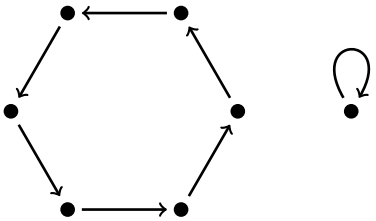
Úmluva. Nechť je f funkce. Pro přirozené n budeme značit

$$f^n(x) = (\underbrace{f \circ \cdots \circ f}_{n\text{-krát}})(x) = \underbrace{f(f(\cdots f(}_{n\text{-krát}} x)\cdots)),$$

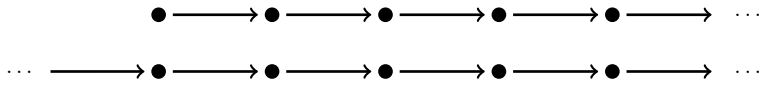
tedy f aplikováno n-krát na x, a pro $n = 0$ dodefinujeme $f^0(x) = x$. Kdybychom náhodou chtěli zapsat n-tou mocninu hodnoty $f(x)$, napíšeme $(f(x))^n$.

Úmluva. S funkcí $f\colon M \to M$ budeme zacházet jako s orientovaným grafem na množině vrcholů M. Šipka z a do b povede právě tehdy, když $f(a) = b$. Následně budeme pro takovou funkci používat grafově motivované termíny:

- *Cyklem* nazveme konečnou posloupnost vrcholů, mezi nimiž dokola vedou šipky. Cyklus délky 1 je *pevný bod*, tedy prvek, který se zobrazuje sám na sebe.



- *Řetězem* nazveme posloupnost navzájem různých vrcholů spojených postupně šipkami, která je ve směru šipek nekonečná. Pokud je řetěz nekonečný i proti směru šipek, nazveme jej *oboustranným řetězem*.



- *Cestou* z vrcholu bude rozumět posloupnost vrcholů, na něž se dostaneme, když prostě půjdeme po šipkách, což odpovídá opakovanému aplikování funkce na příslušný prvek. Cesta se může buď zacyklit, nebo může být řetězem.

Pozorování. *Funkcím $f\colon M \to M$ odpovídají právě ty grafy na množině vrcholů M, kde z každého vrcholu vychází právě jedna šipka.*

Pozorování. *Pro funkci na konečné množině se cesta z libovolného vrcholu zacyklí.*

Pozorování. *Nechť x leží v cyklu délky k na funkci f. Potom $f^n(x) = x$, právě když $k \mid n$.*

Pozorování. *Funkce uvažovaná jako graf je*

- *prostá, když do každého vrcholu vede nejvýše jedna šipka,*
- *na, když do každého vrcholu vede alespoň jedna šipka,*
- *bijektivní, když do každého vrcholu vede právě jedna šipka.*

Pozorování. *Nechť je M konečná množina. Potom je funkce $f\colon M \to M$ prostá, právě když je na.*

Pozorování. *Bijekce se sestává jen z navzájem disjunktních cyklů a oboustranných řetězů.*

Pozorování. *Prostá funkce se sestává jen z navzájem disjunktních cyklů, jednostranných řetězů a oboustranných řetězů. Počáteční vrcholy jednostranných řetězů jsou přitom přesně ty prvky, který chybí v oboru hodnot.*

Úlohy s iteracemi dovedou být dost různorodé a kromě výše uvedených pozorování nemáme moc silnější zbraně. Časté postupy a nástroje zahrnují:

- *prostost a bijektivita*: Pokud dokážeme, že je funkce prostá či bijektivní, značně to zjednoduší obrázek. Následně už lze zvlášť pracovat s cykly a řetězy.
- *extremální princip*: Na cyklech se může vyplatit podívat se na největší nebo nejmenší prvek. Stejně tak může někdy pomoci minimální prvek oboru hodnot. Obecněji má každá podmnožina $\mathbb{N}$ minimum.
- *pořadí a vzdálenost*: Hodí se uvažovat o pořadí a vzdálenostech prvků na řetězu. Někdy se taky hodí porovnat to s pozicemi na číselné ose.
- *indukce*: Iterace často potkáme nad přirozenými čísly. Indukovat potom můžeme obyčejně podle argumentu, anebo třeba podle pořadí v cyklu či na řetězu.
- *funkcionálkové triky*: Funkcionálka s iterací je pořád funkcionálka. Chytré dosazení, úprava nebo symetrie mohou úlohu zpřehlednit.

Rozcvička I – procházky

Úloha 1. David na svých cestách zabloudil do země, kde je konečně mnoho silnic, každá z nich začíná a končí křižovatkou a každá křižovatka je tvaru Y. (Silnice mohou být klikaté a mimoúrovňově se křížit.) Řekl si, že by si ji rád prohlédl, ale trochu se obával, aby se tam úplně neztratil. Naplánoval si to tak, že vyrazí z křižovatky u hospody Na mýtince a střídavě bude na křižovatkách odbočovat doleva a doprava. Může si být jistý tím, že se po nějakém čase ocitne opět u hospody Na mýtince?

(PraSe 35–4j–5)

Úloha 2. V každém patře nekonečně vysoké začarované věže se nachází magický portál, na kterém je napsáno přirozené číslo. Tato přirozená čísla tvoří nerostoucí posloupnost a zároveň každé číslo udává, do kolikátého patra příslušný portál vede. Mezi patry věže lze cestovat pouze pomocí portálů a každý portál je pouze jednosměrný. V jednom z pater si malá myška usmyslela, že se vydá na výzvědy, a začala putovat skrze portály. Ukažte, že za nějakou dobu zůstane uvězněná ve dvojici pater, případně dokonce jen v jediném. (PraSe 35–1p–4)

Úloha 3. Město má tvar obdélníka. Jeho hlavní ulice jsou úsečky rovnoběžné s některým jeho okrajem (stranou obdélníka) a rozdělují jej na obdélníkové čtvrti. *Centrem* nazveme takovou čtvrť, která nesousedí s okrajem. Podle vyhlášky žádná hlavní ulice nevede napříč celým městem. Dokažte, že město má centrum.
(PraSe 34–1j–6)

Úloha 4. Na tabuli jsou v nějakém pořadí napsána čísla 1 až 2023 v řadě. V jednom kroku se podíváme na první číslo, nechť je to k, a obrátíme pořadí prvních k čísel – tedy $a_1, a_2, \ldots, a_{k-1}, a_k$ přepíšeme na $a_k, a_{k-1}, \ldots, a_2, a_1$. Dokažte, že po konečném počtu kroků dostaneme na první pozici jedničku.

Rozcvička II – iterujeme jenom trochu

Úloha 5. Rozhodněte, zda existuje funkce $f\colon \mathbb{N} \to \mathbb{N}$ taková, že $f(f(n)) < f(n)$ pro každé $n \in \mathbb{N}$. (PraSe 36–4p–2)

Úloha 6. Je dána funkce $g\colon \mathbb{N} \to \mathbb{N}$. Zkonstruujte $f\colon \mathbb{Z} \to \mathbb{Z}$ takovou, že $f^n(x) = 0$ má přesně $g(n)$ řešení pro každé $n \in \mathbb{N}$. (zobecněné PraSe 37–4p–3)

Úloha 7. Najděte všechny funkce $f\colon \mathbb{N} \to \mathbb{N}$, které pro všechna $n \in \mathbb{N}$ splňují

$$f(n) + f(f(n)) + f(f(f(n))) = 3n.$$

Úloha 8. Rozhodněte, zda existuje funkce $f\colon \mathbb{Z} \to \mathbb{Z}$ splňující $f(f(n)) = 3n$ pro všechna $n \in \mathbb{Z}$. (USAYNO)

Cykly

Úloha 9. Je dána bijekce $f\colon \mathbb{R} \to \mathbb{R}$. Musí nutně existovat nekonečně mnoho funkcí $g\colon \mathbb{R} \to \mathbb{R}$ takových, že $f(g(x)) = g(f(x))$ pro každé $x \in \mathbb{R}$? (ELMO SL 2018)

Úloha 10. Najděte všechny bijekce $f\colon \mathbb{N} \to \mathbb{N}$, které splňují

$$f(f(n)) \leq \frac{n + f(n)}{2}$$

pro libovolné $n \in \mathbb{N}$. (Rumunsko 2004)

Úloha 11. Funkce $f\colon \mathbb{N} \to \mathbb{N}$ splňuje

$$f^{f(n)}(n) = \frac{n^2}{f(f(n))}$$

pro každé $n \in \mathbb{N}$. Určete všechny možné hodnoty $f(2020)$. (USAMO 2019)

Úloha 12. Nechť $S = \{1, 2, \ldots, n\}$. Funkce $f\colon S \to S$ je *krutopřísná*, pokud pro každé $k \in S$ platí $f^{f(k)}(k) = k$. Dokažte, že každá krutopřísná funkce má alespoň $P + 1$ pevných bodů, kde P je počet prvočísel v intervalu $(\sqrt{n}, n\rangle$.
(PraSe 36–4p–7)

Úloha 13. O reálném polynomu $f(x) = x^2 + ax - 1$ je známo, že rovnice $f^{47}(x) = x$ má alespoň 50 reálných řešení. Dokažte, že tato rovnice má alespoň 96 řešení.
(Russia TST 2020)

Úloha 14. Funkci $f\colon \mathbb{N} \to \mathbb{N}$ nazveme *žůžovou*, pokud

$$f^{f^{f(n)}(n)}(n) = n$$

pro každé $n \in \mathbb{N}$. Najděte všechna m taková, že každá žůžová funkce f splňuje $f^{2014}(m) = m$. (ELMO SL 2014)

Řetězy

Úloha 15. Jsou dána $a, k \in \mathbb{N}$. Dokažte, že funkce $f\colon \mathbb{N} \to \mathbb{N}$ splňující $f^k(n) = n + a$ pro každé $n \in \mathbb{N}$ existuje, právě když $k \mid a$. Bonus: kolik takových funkcí existuje?

Úloha 16. Najděte všechna přirozená k, pro než existují funkce $f\colon \mathbb{N} \to \mathbb{N}$ a $g\colon \mathbb{N} \to \mathbb{N}$ takové, že g nabývá nekonečně mnoha hodnot a $f^{g(n)}(n) = f(n) + k$ pro každé $n \in \mathbb{N}$. (MEMO 2020 I1)

Úloha 17. Najděte všechny funkce $f\colon \mathbb{N} \to \mathbb{N}$ takové, že

$$f^{f^{f(x)}(y)}(z) = x + y + z + 1$$

pro libovolná $x, y, z \in \mathbb{N}$. (ELMO 2020)

Úloha 18. Najděte všechny funkce $f\colon \mathbb{N}_0 \to \mathbb{N}_0$, které splňují $f(f(f(n))) = f(n + 1) + 1$ pro každé $n \in \mathbb{N}_0$. (ISL 2013)

Trocha teorie čísel

Úloha 19. Pro dané celé číslo $a_0 > 1$ definujme posloupnost $a_0, a_1, a_2, \ldots$ pro každé $n \geq 0$ předpisem

$$a_{n+1} = \begin{cases} \sqrt{a_n}, & \text{pokud je } \sqrt{a_n} \text{ celé číslo,} \\ a_n + 3, & \text{jinak.} \end{cases}$$

Určete všechny hodnoty a_0, pro něž existuje číslo A takové, že $a_n = A$ platí pro nekonečně mnoho indexů n. (IMO 2017)

Úloha 20. Je dáno celé číslo a_1, z něhož je dále definována nekonečná posloupnost celých čísel předpisem $a_{n+1} = a_n^2 - a_n + 1$ pro každé přirozené n. Dokažte, že pro každé přirozené n je a_{n+1} nesoudělné s $2n + 1$. (*i*KS–11–N2)

Úloha 21. Definujme posloupnost přirozených čísel $a_1, a_2, a_3, \ldots$ takto: $a_1 = 1$ a pro každé přirozené k je $a_{k+1} = a_k^3 + 1$. Dokažte, že pro všechna prvočísla p tvaru $3\ell + 2$, kde ℓ je celé nezáporné, existuje přirozené n, že $p \mid a_n$. (MEMO 2018 T7)

Úloha 22. Určete největší přirozené $N < 2020$, pro něž existuje polynom P s celočíselnými koeficienty takový, že $2020 \mid P^k(0)$, právě když $N \mid k$. Bonus: jak se odpověď změní, když místo 2020 napíšeme 2021? (USA EGMO TST 2020)

Úloha 23. Je dán nekonstantní polynom P s celočíselnými koeficienty. Dokažte, že neexistuje funkce $f\colon \mathbb{Z} \to \mathbb{Z}$ taková, že pro každé $n \in \mathbb{N}$ je počet řešení $f^n(x) = x$ roven $P(n)$. (ISL 2009 N5)

Návody

1. Jako stavy Davidovy cesty ber třeba trojice (silnice, směr, parita).

2. Každá cesta se zacyklí – podívej se na cyklus.

3. Rozmysli si, že ve městě neexistují zatáčky, které zároveň nejsou křižovatky. Potom se zkus procházet uvnitř města.

4. Podívej se na cyklus a učiň extremální volbu.

5. Podívej se na cestu z libovolného n.

6. Prostě si nakresli stromeček.

7. Nahlédni prostost a poté indukuj.

8. Zkus si tipnout.

9. Rozděl komponenty souvislosti na oboustranné řetězy, pevné body a ostatní cykly.

10. Oboustranné řetězy vysporuj, v cyklech učiň extremální volbu.

11. Rozmysli si, že f musí být poskládána z dvojcyklů a pevných bodů.

12. Délky cyklů.

13. Kolik je cyklů délek 1 a 47?

14. Rozmysli si bijektivitu. Uvnitř cyklu indukuj proti směru šipek.

15. Kolik prvků se s každou aplikací f ztrácí z oboru hodnot?

16. Cesta z $f(n)$ navštíví skoro celou zbytkovou třídu $f(n) \bmod k$. Buď najdi spor s neomezeností g, anebo zkus vhodně poskládat graf.

17. Řetěz z 1 musí obsahovat vše. S pomocí úlohy 15 si rozmysli $1 \mapsto 2 \mapsto 3$ a je vyhráno.

18. Porovnej f^4 na argumentech n a $n-1$, vyjde to hezky. Následně porovnávej, kolik prvků chybí v oborech hodnot f a f^3. Pak už si stačí rozmyslet pořadí prvních čtyř prvků na řetězu – jsou dvě možnosti, které fungují.

19. Rozmysli si modulo 3. Potom se dívej na minimum cyklu.

20. Iteruj $f(x) = x^2 - x + 1$ modulo $p \mid a_{n+1}$. Do jednoho vrcholu nemůže přicházet příliš mnoho šipek – ukaž, že $p > 2n + 1$.

21. Trik: $0^3 + 1 \equiv 1 \pmod{p}$.

22. Rozlož úlohu do $\mathbb{Z}_4$, $\mathbb{Z}_5$ a $\mathbb{Z}_{101}$. Jak funguje délka cyklů při skládání zpět?

23. Pomocí délek cyklů něco řekni o $P(pq)$ pro prvočísla p, q.

Literatura a zdroje

Tento příspěvek je zkrácenou a mírně aktualizovanou druhou *iterací* přednášky, kterou jsem připravil na soustředění *i*KSka v roce 2021. Rád bych si zde proto poděkoval za to, jak skvěle jsem ji tehdy napsal a jak všeobecně úžasný a skromný jsem.

[1] Martin „Vodka“ Vodička: *Funkcionálky nad prirodzenými číslami*, sborník *i*KS, 2017.
[2] Vít „Vejtek“ Musil: *Funkcionální rovnice*, Oldřichov, 2012.
[3] Rado van Švarc: *Dvě neobvyklé existenční techniky*, Hojsova Stráž, 2016.

Catalanova čísla

Klárka Grinerová

Abstrakt. Catalanova čísla jsou vedle kombinačních čísel jednou z nejčastěji se vyskytujících posloupností čísel v kombinatorice. V tomto příspěvku si představíme, co to vlastně je, a podíváme se na překvapivé množství úloh, kde hrají roli.

V této přednášce se podíváme na Catalanova čísla. Jedná se o posloupnost přirozených čísel, u které na první pohled není vůbec zřejmé, proč by si měla vysloužit svůj vlastní název nebo nějaké větší množství pozornosti. Ve skutečnosti ale existuje mnoho kombinatoricky zajímavých struktur, jejichž počet Catalanova čísla popisují.

Definice. Symbolem C_n značíme n-té *Catalanovo číslo*.

$$C_n = \binom{2n}{n} - \binom{2n}{n+1} = \frac{1}{n+1}\binom{2n}{n}$$

Poznámka. Často se definuje i $C_0 = 1$. Prvních několik Catalanových čísel je postupně 1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796, 58786, ...

Definice. *Obdélníkem* $m \times n$ rozumíme obdélník ve čtvercové mřížce, který je m políček vysoký a n políček široký. *Cestou* v obdélníku pak nazýváme trasu z levého dolního do pravého horního rohu, která vede po hranách mřížky, a to pouze doprava a nahoru.

Cvičení. Dokažte, že v obdélníku $m \times n$ existuje $\binom{m+n}{n}$ různých cest.

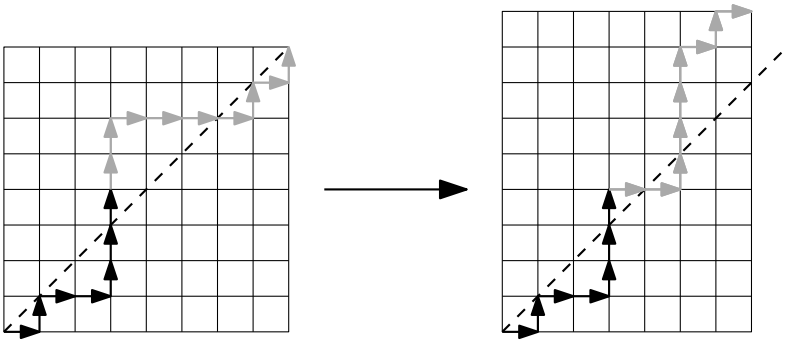
Definice. *Úhlopříčkou* ve čtverci $n \times n$ nazveme úsečku spojující levý dolní roh s pravým horním.

Definice. Cesta ve čtverci je *Dyckova*, pokud se žádná její část nenachází nad úhlopříčkou.

Věta. *Počet cest ve čtverci $n \times n$, které jsou celé pod úhlopříčkou, je C_n.*

Důkaz. Uvážíme všechny cesty ve čtverci $n \times n$. Každá cesta se skládá z $2n$ pohybů, a jelikož se cesty skládají pouze z pohybů doprava a nahoru, každou cestu lze jednoznačně určit výběrem n pohybů doprava z celkových $2n$ pohybů. Cest je tak celkem $\binom{2n}{n}$. Ne všechny cesty jsou ale Dyckovy.

Spočítáme tak počet nevyhovujících cest (tzn. cest, které překračují uhlopříčku), tento počet následně odečteme od celkového počtu. Uvažme libovolnou nevyhovující cestu c. Tato cesta v nějakou chvíli překročí úhlopříčku směrem nahoru. Nechť c' je taková cesta, která odpovídá původní cestě c až po krok, který překročí úhlopříčku. Zbytek cesty je převrácený, jak naznačuje obrázek (z cest nahoru se stanou cesty doprava a naopak).



Nově vzniklá cesta c' bude obsahovat $n+1$ kroků směrem nahoru a $n-1$ kroků směrem doprava, bude tedy cestou v obdélníku $(n+1)\times(n-1)$. Překlopením nazpátek ve stejném místě dostaneme jednoznačně určenou původní cestu, tedy toto zobrazení z c na c' je prosté.

Stejně tak můžeme z libovolné cesty v obdélníku $(n+1)\times(n-1)$ analogickým překlopením získat nevyhovující cestu v obdélníku $n\times n$ a toto zobrazení je rovněž prosté. Existuje tedy bijekce mezi cestami ve čtverci $n\times n$ překračujícími úhlopříčku a cestami v obdélníku $(n+1)\times(n-1)$, kterých je $\binom{2n}{n+1}$. Potom dostáváme počet Dyckových cest jako $\binom{2n}{n}-\binom{2n}{n+1}=\frac{1}{n+1}\binom{2n}{n}=C_n$ □

Příklad 1. Kolik existuje různých cest v obdélníku $m\times n$, které jsou celé pod úhlopříčkou levého čtverce $m\times m$?

Rekurentní vzorec

Tvrzení. *Mějme posloupnost $(a_n)_{n\geq 0}$ splňující vztahy*

$$a_0=1, \qquad a_{n+1}=\sum_{i=0}^{n} a_i a_{n-i}.$$

Pak $a_n=C_n$.

Příklad 2. Kolik existuje korektních uzávorkování n párů závorek?

Příklad 3. Kolik existuje různých triangulací konvexního n-úhelníka[1]?

Zobecnění Catalanových čísel

Definice. Definujeme rozšíření Catalanových čísel $C(n,k)$ pro $0\leq k\leq n$ jako

$$C(n,k)=\binom{n+k}{k}-\binom{n+k}{k-1}.$$

Věta. *Počet cest v obdélníku $k\times n$, které jsou celé pod úhlopříčkou, je $C(n,k)$.*

[1]Rozdělení na $n-2$ trojúhelníků, jejichž vrcholy jsou vrcholy původního n-úhelníka.

Náznak důkazu. Rozšíříme důkaz předešlé věty charakterizující Catalanova čísla, čímž dostaneme podobný vztah. Uvážíme všechny cesty, kterých je v takovém obdélníku $\binom{n+k}{k}$. Dále pak spočítáme všechny nevyhovující cesty, které někde překračují uhlopříčku, a najdeme bijekci mezi takovými cestami a cestami v obdélníku $(n+1) \times (k-1)$, kterých je $\binom{n+k}{k-1}$. Tyto cesty odečteme od celkového počtu a dostáváme tak vztah $C(n,k) = \binom{n+k}{k} - \binom{n+k}{k-1}$.

Přirozená struktura této konstrukce nám dovoluje vytvořit Catalanův trojúhelník, který je znázorněný na obrázku.

						132	$\cdots$
					42	132	$\cdots$
				14	42	90	$\cdots$
			5	14	28	48	$\cdots$
		2	5	9	14	20	$\cdots$
	1	2	3	4	5	6	$\cdots$
1	1	1	1	1	1	1	$\cdots$

Číslo $C(n,k)$ je v $(n+1)$-ním sloupci a $(k+1)$-ním řádku. Catalanova čísla jsou přesně na diagonále.

Při volbě $k = n$ dostáváme $C(n,n) = C_n$. Opět lze přejít k rekurentnímu vztahu $C(n,k) = C(n,k-1) + C(n-1,k)$ pro $0 \leq k \leq n$. Ten říká, že číslo v Catalanově trojúhelníku je součtem čísla pod ním a nalevo od něj. Tento trojúhelník má, stejně jako ten Pascalův, množství pěkných vlastností. Například si lze všimnout, že součet n-tého sloupce dává n-té Catalanovo číslo.

Úložky

Úloha 4. Radeček skáče po ose přirozených čísel. Začíná v bodě 1 a v každém z deseti kroků buď skočí o 1 číslo vpřed, o 1 číslo vzad (pokud již nestojí v bodě 1), nebo se mu nikam nechce a zůstane stát. Po 10 krocích byl Radeček v bodě 1. Kolika různými způsoby mohl Radeček v 10 krocích skákat a lenošit na ose, když se nikdy nemohl dostat pod číslo 1?

Úloha 5. Matěj nakreslil na papír N tramvajových zastávek (bodů) na centrální lince (přímce) s pravidelnými rozestupy 1. Následně do obrázku dokreslil několik tras tramvajových linek (úseček, bod není úsečka) tak, že každá začíná a končí v některých vyznačených bodech. Navíc pro každé dvě tramvajové trasy (úsečky) a, b platilo, že pokud je jejich průnik nějaká úsečka c, pak $a = c$ nebo $b = c$. Pro dané N Matěj nakreslil největší možný počet linek. Kolika způsoby mohl to mohl v závislosti na N udělat?

Příklad 6. Nechť n je přirozené číslo. Kolik existuje cest v kartézské soustavě souřadnic, které vedou z bodu $(0,0)$ do bodu $(2n,0)$, takových, že z libovolného bodu (x,y) cesta pokračuje buď do bodu $(x+1,y+1)$, nebo do bodu $(x+1,y-1)$? Kolik z těchto cest nikdy neklesne pod osu x?

Příklad 7. Kolik existuje posloupností přirozených čísel délky n splňujících $1 \leq a_1 \leq a_2 \leq \cdots \leq a_n$ a navíc $a_i \leq i$?

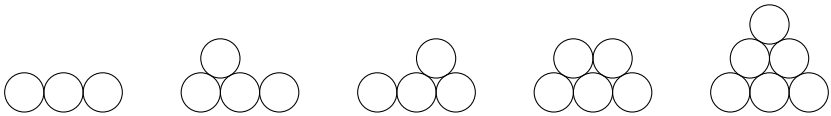
Příklad 8. Kolika způsoby si může $2n$ lidí podat ruce přes stůl tak, aby se žádné dva páry rukou nekřížily (každý člověk podává právě jednu ruku jinému člověku)?

Příklad 9. Kolik existuje úplných binárních stromů s $n+1$ listy? Rozlišujeme „pravé“ a „levé“ syny.

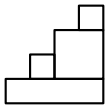
Příklad 10. Kolika způsoby lze vyplnit tabulku $2 \times n$ čísly 1 až $2n$ tak, aby čísla v obou řádcích i ve všech sloupcích byla rostoucí?

Příklad 11. Kolik existuje binárních stromů na n vrcholech? Rozlišujeme „pravé“ a „levé“ syny.

Příklad 12. Kolika způsoby je možné navršit mince na hromádku, je-li ve spodní řadě n mincí? Na obrázku jsou všechny možné hromádky pro $n = 3$.



Příklad 13. Kolika způsoby je možno postavit schodiště o n schodech pomocí n obdélníků? Na obrázku je schodiště o 4 schodech postavené ze 4 obdélníků.

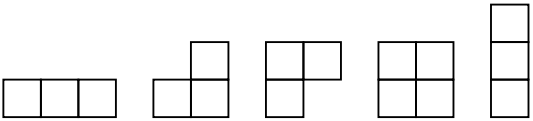


Příklad 14. Kolik je permutací množiny $\{1,\ldots,n\}$, které neobsahují klesající podposloupnost délky větší než 2?
(Označíme-li permutaci p, pak neexistují $i,j,k \in \{1,\ldots,n\}$ takové, že $i<j<k$ a zároveň $p(i)>p(j)>p(k)$.)

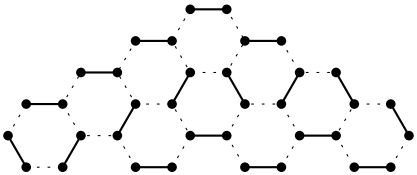
Příklad 15. Pro která n je C_n liché?

Příklad 16. Polyomino[2] nazveme *neklesající*, pokud je každý jeho sloupec souvislý (tj. není rozdělen na více částí oddělených prázdnými čtverečky), pozice horního čtverečku v každém sloupci se zleva doprava nesnižuje a obdobně se v každém sloupci nesnižuje pozice nejnižšího čtverečku zleva doprava. Kolik existuje *neklesajících* polyomin s obvodem délky $2n$? Obrázek zachycuje případ pro $n = 4$.

[2]Útvar vzniklý sloučením několika jednotkových čtverců dotýkajících se hranou.



Příklad 17. Kolik existuje úplných párování vrcholů na šestiúhelníkové pyramidě šířky n? Úplné párování na šestiúhelníkové pyramidě šířky 4 může vypadat například takto:



Návody

2. Převeď na počet cest pod diagonálou nebo rekurzi podle první korektní podposloupnosti.

4. Rozmysli si, že v každou chvíli měl Radeček za sebou alespoň tolik skoků vpřed, jako vzad.

5. Převeď centrální linku na n-úhelník.

6. Převeď na cesty pod diagonálou.

7. Převeď na hledání cest pod diagonálou - dívej se na vodorovné hrany.

8. Hledej triangulaci.

9. Převeď na uzávorkování.

10. Bijekce na cesty pod diagonálou. Pořadí pohybu danými směry.

11. Použij rekurzi a převeď na uzávorkování.

12. Rekurze, nejpravější mezera v druhé vrstvě odspodu.

13. Dvě různá políčka na úhlopříčce nemůžou být ve stejném obdélníku. Roh.

14. Zaznač si permutaci to tabulky $n \times n$ a najdi pomocí ní cestu nad/pod diagonálou.

15. Použij rekurentní vztah a indukci.

16. Koukni se na horní a dolní trasu z levého dolního do pravého horního rohu polyomina. Poskládej pomocí nich trasu pod diagonálou čtverce.

17. Otoč si obrázek o 150° po směru hodinových ručiček. V každé vrstvě svislých hran je na párování použita právě jedna hrana. Po otočení jde vidět přirozená bijekce mezi volbou těchto hran a hledání cest pod uhlopříčkou.

Literatura a zdroje

Velká část příspěvku je převzatá z přednášek *Martina Rašky*, a rekurzivně tak i z příspěvků *Martina Hory* a *Anči Chejnovské*, kterým děkuji.

[1] Martin Raška, *Catalanova čísla*, Branná, 2019.

[2] BRKOS team: *Pomocný text k 3. sérii – Catalanova čísla*, *https://brkos.math.muni.cz/files/povidani/povidani273.pdf*.

Obarvování a dláždění

Petr Hladík

Abstrakt. Seznámíme se s tím, jak řešit a dokazovat některé kombinatorické úlohy pomocí obarvování.

Obarvování je názorný a účinný způsob, jak vyřešit některé kombinatorické úlohy. V principu rozdělíme množinu (typicky čtvercovou síť) na konečný počet podmnožin a pro lepší představu pak jednotlivé části obarvíme různými barvami. V typických úlohách se často objevuje černobílá šachovnice, ale občas je potřeba využít barev více. Řešení problému obarvováním je v podstatě třífázové – nejdříve si musíme uvědomit, že úloha je obarvovací, dále vymyslet vhodné rozdělení na části a pak už zbývá jen okomentovat, proč něco je, nebo není možné.

Příklad. Dokažte, že šachovnici 8×8, které chybí dva protější rohy, nelze pokrýt dominy.

Řešení. Všimneme si, že každé domino pokryje právě jedno bílé a jedno černé políčko. Tedy, aby tabulka šla pokrýt dominy, musí mít stejný počet bílých a černých políček, což ale nemá. Tedy naše šachovnice nelze pokrýt dominy.

Úlohy

Úloha 1. Mějme pět tetromin různých druhů (tedy od každého jedno). Lze z nich vytvořit obdélník?

Úloha 2. Na každém poli šachovnice $n \times n$ sedí beruška. Po zaznění výstřelu se každá přesune na pole, které hranou sousedí s jejím původním místem. Pro která n mohou být znovu obsazená všechna políčka?

Úloha 3. Schodištěm velikosti n nazvěme část šachovnice $n \times n$, která obsahuje všechna políčka hlavní diagonály a všechna políčka, která jsou pod ní. Kolik nejméně cest je potřeba na pokrytí schodiště? Cesta je posloupnost políček, kde každá dvě po sobě jdoucí sdílí hranu.

Úloha 4. Je možné tabulku 2021×2021 vydláždit vodorovnými obdélníky 2×1 a svislými 1×3?

Úloha 5. Tabulka $m \times n$ je vyplněna dlaždicemi 2×2 a 1×4. Dokažte, že nemůžeme jednu dlaždici 2×2 nahradit dlaždicí 1×4, ani když ostatní dlaždice libovolně přeskládáme.

Úloha 6. Na nekonečnou tabulku položíme 2021 čtverců $n \times n$, mohou se překrývat. Dokažte, že počet políček zakrytých lichým počtem čtverců je aspoň n^2.

Úloha 7. Obdélník $a \times b$ lze pokrýt obdélníky $1 \times n$, právě když $n \mid a$ nebo $n \mid b$. Dokažte. Kdy jej lze pokrýt obdélníky $m \times n$?

Úloha 8. Mějme nekonečnou šachovnici a v ní nějaký útvar P skládající se z několika políček, který lze vydláždit S-tetrominy. Dokažte, že když P vydláždíme S a Z-tetrominy, musíme použít sudý počet Z-tetromin. (Shortlist 2014 C4)

Úloha 9. Je možno vyplnit krychli $10 \times 10 \times 10$ pomocí 250 cihel $1 \times 1 \times 4$?

Úloha 10. Na šachovnici 2020×2020 je umístěno 2020 šachových dam tak, že se žádné dvě navzájem neohrožují. Ukažte, že se v každém z rohových čtverců 1010×1010 nachází alespoň jedna dáma.

Úloha 11. Alice a Bob hrají hru na šachovnici $n \times n$, na začátku jsou všechna políčka bílá, jenom levé dolní je černé a stojí na něm věž. Alice a Bob v každém tahu pohnou věží na bílé políčko a obarví jej na černo. Kdo nemůže táhnout, prohrál. Kdo má vyhrávající strategii, jestliže začíná Alice?

Úloha 12. Dokaž, že tabulku $2^n \times 2^n$ s jedním chybějícím políčkem lze vydláždit L-triominy.

Úloha 13. Tabulka 6×6 je vydlážděna dominy. Dokažte, že je možné ji rozříznout svisle nebo vodorovně tak, aby nebylo porušeno žádné domino.

Úloha 14. Šachovnice 8×8 je vydlážděna dominy. Dokažte, že počet vodorovných domin, jejichž levé políčko je bílé, je stejný jako počet domin, jejichž pravé políčko je bílé.

Úloha 15. Tabulka 100×100 je obarvena černě a bíle. Všechna políčka na okraji jsou černá a navíc žádný čtverec 2×2 není jednobarevný. Dokažte, že existuje čtverec 2×2, který je obarvený šachovnicově. (Rusko 2017)

Úloha 16. V tabulce $n \times n$ je $n - 1$ nakažených políček. V každém kroku se nakazí všechna políčka, která sousedí s aspoň dvěma nakaženými. Dokažte, že aspoň jedno políčko zůstane zdravé.

Návody

1. Šachovnice.
2. Šachovnice.
3. Konstrukce na $\lceil \frac{n}{2} \rceil$ je triviální, optimalita plyne z šachovnicového obarvení.
4. Obarvi řádky třemi barvami.
5. Děravé šachovnicové obarvení.
6. Použij n^2 barev tak, aby každý čtverec obsahoval právě jedno políčko od každé barvy.
7. Obarvi diagonály.
8. Najdi vhodné diagonální a sloupcové obarvení.
9. Zkus obarvit 4 barvami.
10. Dámy musí být v protilehlých čtvercích, potom máme málo diagonál.
11. Záleží na paritě n, políčka popáruj.
12. Indukce.
13. Může nějaký řez protnout jenom jedno domino?
14. Stejná myšlenka jako v předchozí úloze, přidá se šachovnicové obarvení.
15. Spočítej hrany oddělující černé a bílé políčko.
16. Obvod.

Literatura a zdroje

[1] Matthew Brennan: *Grids and Related Problems*, Canadian IMO Training, 2018.
[2] Stan Wagon: *Fourteen Proofs of a Result About Tiling a Rectangle*, The American Mathematical Monthly, 1987.
[3] Josef Minařík: *Úlohy s tabulkami*, Lysečiny, 2021.

Mocnost bodu ke kružnici

Verča Hladíková

Abstrakt. Příspěvek seznamuje se základními vlastnostmi mocnosti bodu ke kružnici a ilustruje její použití v geometrických úlohách.

Trocha teorie na úvod

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

Poznámka. Pokud bod M leží vně kružnice k, je číslo $p(M,k)$ kladné. Pokud leží uvnitř k, pak je $p(M,k)$ záporné. Leží-li bod M na kružnici k, je $p(M,k) = 0$.

Poznámka. Nechť M a N jsou dva různé body. Pak $p(M,k) = p(N,k)$, právě když $|MO| = |NO|$.

Tvrzení. *Nechť přímka p vedená bodem M protne kružnici k v bodech A, B. Pak platí*

$$p(M,k) = \begin{cases} |MA| \cdot |MB|, & \text{leží-li } M \text{ vně } k, \\ -|MA| \cdot |MB|, & \text{leží-li } M \text{ uvnitř } k. \end{cases}$$

Jestliže speciálně M leží vně k a označíme T bod dotyku tečny ke kružnici k vedené bodem M, pak $p(M,k) = |MT|^2$.

Tvrzení. *Nechť $ABCD$ je čtyřúhelník a $M = AD \cap BC$. Pak $ABCD$ je tětivový, právě když $|MA| \cdot |MD| = |MB| \cdot |MC|$.*

Definice. Nechť k, l jsou kružnice. Množinu bodů X splňujících $p(X,k) = p(X,l)$ nazýváme *chordálou* kružnic k, l.

Tvrzení. *Chordála dvou nesoustředných kružnic je přímka kolmá na spojnici jejich středů.*

Tvrzení. *Uvažme tři kružnice k_1, k_2, k_3. Pak jejich vzájemné chordály procházejí jedním bodem (nebo jsou všechny rovnoběžné). Tomuto bodu se říká potenční střed kružnic k_1, k_2, k_3.*

Příklady

Příklad 1. Kružnice k, l se středy K, L se protínají v bodech A, B. Přímka AB protne společnou tečnu kružnic k, l, která se jich dotýká v bodech T, U, v bodě P. Pak $|PT| = |PU|$.

Příklad 2. Na prodloužení tětivy KL kružnice k se středem O leží bod A. Tečny z bodu A ke kružnici k se jí dotýkají v bodech T, U. Označme M střed úsečky TU. Ukažte, že čtyřúhelník $KLMO$ je tětivový.

Příklad 3. Kružnice vepsaná trojúhelníku ABC se dotýká jeho stran AB, BC, CA v bodech F, D, E. Označme písmeny Y_1, Y_2, Z_1, Z_2, M středy úseček FB, BD, DC, CE, BC. Konečně buď $X = Y_1Y_2 \cap Z_1Z_2$. Dokažte, že $XM \perp BC$.

Příklad 4. Mějme pravoúhlý trojúhelník ABC s přeponou AB. Na jeho odvěsně AC zvolme bod D. Nyní sestrojme kružnici k_1, která se dotýká AB v bodě A a prochází bodem D. Dále též kružnici k_2, která se dotýká AB v bodě B a též prochází bodem D. Označme E druhý průsečík kružnic k_1 a k_2. Dokažte, že úhly BAC a DEC jsou shodné. (Hradiště 2007)

Příklad 5. Tečny skrz A ke kružnici k se jí dotýkají v bodech T a U. Buď M střed AT. Úsečka MU protne k podruhé v bodě X. Dokažte, že $|XA| = 2 \cdot |MX|$.

Příklad 6. Na přímce p leží body A, B, C, D v tomto pořadí. Kružnice nad průměry AC, BD se protnou v X, Y. Na přímce XY zvolíme bod P ($P \notin BC$). Přímka CP protne kružnici nad AC podruhé v bodě M, přímka BP kružnici nad BD v bodě N. Ukažte, že přímky AM, DN, XY procházejí jedním bodem. (IMO 1995)

Příklad 7. V trojúhelníku ABC označme B_0, C_0 paty příslušných výšek. Zvolme bod P tak, aby přímka PB byla tečnou ke kružnici opsané $\triangle PAC_0$ a přímka PC tečnou ke kružnici opsané $\triangle PAB_0$. Dokažte, že AP je kolmá na BC. (MEMO 2011, MR&JT)

Příklad 8. Body P a Q leží na stranách CA a AB trojúhelníka ABC. Označme K, L a M postupně středy úseček BP, CQ a PQ. Dále předpokládejme, že přímka PQ je tečnou ke kružnici opsané trojúhelníku KLM. Ukažte, že body P a Q jsou stejně vzdálené od středu kružnice opsané $\triangle ABC$. (IMO 2009)

Příklad 9. Je dán ostroúhlý trojúhelník ABC s kolmištěm H. Kružnice se středem ve středu strany BC procházející bodem H protne BC v A_1, A_2. Body B_1, B_2, C_1, C_2 definujeme podobně. Dokažte, že těchto šest bodů leží na kružnici. (IMO 2008)

Příklad 10. Je dána kružnice k a přímka p. Bod P se nachází na p. Tečny z P ke k se jí dotýkají v T a U. Uvažme kružnici se středem P procházející body T, U. Dokažte, že všechny takové kružnice procházejí dvěma společnými body.

Příklad 11. Na straně BC trojúhelníka ABC s výškami BM, CN a kolmištěm H je dán bod W. Body X, Y jsou zvoleny tak, aby WX, WY byly průměry kružnic BWN, respektive CWM. Dokažte, že body X, Y, H leží na přímce. (IMO 2013)

Příklad 12. Nechť $ABCD$ je čtyřúhelník vepsaný do kružnice k takový, že přímky AD a BC se protínají v bodě Q. Označme M průsečík přímky BD a rovnoběžky s přímkou AC vedené bodem Q. Zvolme $T \in k$ tak, aby MT byla tečnou kružnice k. Dokažte, že $|MT| = |MQ|$. (MKS 2005)

Příklad 13. Je dán trojúhelník ABC s vepsištěm I a opsištěm O. Kolmice na AI skrz I protne BC v A'. Podobně definujme B' a C'. Dokažte, že body A', B', C' leží na přímce kolmé na OI.

Příklad 14. Úhlopříčky nerovnoramenného lichoběžníku $ABCD$ se protínají v bodě P. Nechť A_1 je druhý průsečík kružnice opsané $\triangle BCD$ s přímkou AP, body B_1, C_1, D_1 definujeme obdobně. Dokažte, že $A_1B_1C_1D_1$ je také lichoběžník.
(Turnaj měst 2008)

Příklad 15. Osy úhlů u vrcholů A, B protnou protější strany trojúhelníka ABC v bodech D, E a samy sebe v I. Přímka DE protne kružnici opsanou v M a N. Dokažte, že připsiště I_A a I_B leží na kružnici MIN. (ARO 2006)

Příklad 16. V pravoúhlém trojúhelníku ABC s přeponou AB označme G těžiště. Bod P na polopřímce AG splňuje $|\sphericalangle CPA| = |\sphericalangle CAB|$, bod Q na polopřímce BG splňuje $|\sphericalangle CQB| = |\sphericalangle ABC|$. Dokažte, že se kružnice AQG a BPG protínají na AB.
(Kanada 2013)

Návody

1. Uvažujte mocnost z bodu P.
2. Použijte pravoúhlé trojúhelníky.
3. Uvažujte B, C jako nulové kružnice.
4. Přímka DE prochází středem úsečky AB, použijte úsekové úhly.
5. Dokreslete kružnici opsanou AXU.
6. Hledaný průsečík bude potenčním středem.
7. Bod P je průsečík výšky z vrcholu A a Thaletovy kružnice nad BC.
8. Ukažte, že trojúhelníky MKL a AQP jsou si podobné.
9. Dokažte, že na kružnici leží vždy dvě dvojice bodů. Mohlo by se jednat o různé kružnice?
10. Přímka p je chordála k a nějakého bodu.
11. Protněte kružnice podruhé.
12. Dokažte, že MQ je tečnou ke kružnici opsané BDQ.
13. Uvažujte I jako kružnici s nulovým poloměrem.
14. Kombinujte čtyři rovnosti získané z mocností.
15. Dokažte, že DE je chordála dvou kružnic.
16. Úhlové podmínky převeďte na tečnosti a tipněte správný bod na AB.

Literatura a zdroje

Přednáška je převzata od *Hedviky Ranošové*, která čerpala z příspěvku *Tondy Le* a mého příspěvku a které tímto velice děkuji.

[1] Hedvika Ranošová : *Mocnost bodu ke kružnici*, Sklené, 2019.

Integrály

Terka Kučerová

Abstrakt. Pomocí derivací si zadefinujeme primitivní funkci a naučíme se jak spočítat některé neurčité integrály.

Úmluva. Není-li řečeno jinak, reálný interval (a, b) uvažujeme vždy neprázdný.

Co je neurčitý integrál?

Definice. Nechť jsou f, F funkce definované na reálném intervalu (a, b). Poté F nazveme *primitivní funkcí* k f na (a, b), jestliže pro každé x z intervalu (a, b) má F' v bodě x derivaci a platí $F'(x) = f(x)$.

Proces, při kterém k dané funkci f na vhodném intervalu (a, b) hledáme její primitivní funkci, nazýváme *integrací*. Primitivní funkce se někdy označuje jako *neurčitý integrál*, popřípadě *antiderivace*.

Fakt.

(1) Ne ke každé funkci existuje primitivní funkce. Např. funkce signum nemá primitivní funkci na $\mathbb{R}$.
(2) Ke každé spojité funkci f na intervalu (a, b) lze nalézt primitivní funkci.
(3) Pokud je F primitivní funkce k funkci f na intervalu (a, b), pak je F na tomto intervalu spojitá.
(4) Primitivní funkce je až na konstantu určena jednoznačně. Tedy pokud máme funkci f a k ní příslušné primitivní funkce F a G na intervalu (a, b), pak existuje $c \in \mathbb{R}$ takové, že pro každé x z (a, b) platí $F(x) = G(x) + c$. V tomto případě říkáme, že funkce F a G se *rovnají až na konstantu*, což značíme $F \overset{c}{=} G$.

Na základě výše uvedených faktů můžeme skutečnost, že F je primitivní funkce k f na (a, b), značit symbolicky jako

$$\int f(x)\,\mathrm{d}x \overset{c}{=} F(x) \text{ pro } x \in (a, b),$$

kde

(1) $\overset{c}{=}$ označuje rovnost až na konstantu,
(2) $\int$ je znak integrálu,
(3) $f(x)$ nazýváme *integrand*, tj. funkce, kterou integrujeme,
(4) $\mathrm{d}x$ je *diferenciál*, který jednak označuje konec integrálu a jednak proměnnou, podle níž se integruje.

Příklad. Spočítejte primitivní funkce k funkcím:

(1) x^α, (2) $\sin(x)$, (3) $\cos(x)$, (4) e^x,
(5) $\frac{1}{\cos^2(x)}$, (6) $\frac{1}{\sin^2(x)}$, (7) $\frac{1}{\sqrt{1-x^2}}$, (8) $\frac{1}{1+x^2}$.

Řešení.

(1) Ze vztahu $(x^\alpha)' = \alpha x^{\alpha-1}$ odvodíme $\int x^\alpha \,\mathrm{d}x \stackrel{c}{=} \frac{x^{\alpha+1}}{\alpha+1}$, kde $\alpha \neq -1$ a $x \in (0,\infty)$.
Ze vztahu $(\log(x))' = \frac{1}{x}$ odvodíme $\int x^{-1} \,\mathrm{d}x \stackrel{c}{=} \log(x)$, kde $x \in (0,\infty)$.

(2) Ze vztahu $(\cos(x))' = -\sin(x)$ odvodíme $\int \sin(x) \,\mathrm{d}x \stackrel{c}{=} -\cos(x)$ pro $x \in \mathbb{R}$.

(3) Ze vztahu $(\sin(x))' = \cos(x)$ odvodíme $\int \cos(x) \,\mathrm{d}x \stackrel{c}{=} \sin(x)$ pro $x \in \mathbb{R}$.

(4) Ze vztahu $(e^x)' = e^x$ odvodíme $\int e^x \,\mathrm{d}x \stackrel{c}{=} e^x$ pro $x \in \mathbb{R}$.

(5) Zderivujme

$$(\mathrm{tg}(x))' = \left(\frac{\sin(x)}{\cos(x)}\right)' = \frac{\sin'(x)\cos(x) - \cos'(x)\sin(x)}{\cos^2(x)} = \\ = \frac{\cos^2(x) + \sin^2(x)}{\cos^2(x)} = \frac{1}{\cos^2(x)}.$$

Je tedy vidět, že $\int \frac{1}{\cos^2(x)} \,\mathrm{d}x \stackrel{c}{=} \mathrm{tg}(x)$, kde $x \in (-\frac{\pi}{2}, \frac{\pi}{2})$.

(6) Zderivujme:

$$(\mathrm{cotg}(x))' = (\mathrm{tg}^{-1}(x))' = -\frac{1}{\mathrm{tg}^2(x)} \cdot \mathrm{tg}'(x) = -\frac{\cos^2(x)}{\sin^2(x)} \cdot \frac{1}{\cos^2(x)} = -\frac{1}{\sin^2(x)}.$$

A tedy $\int \frac{1}{\sin^2(x)} \,\mathrm{d}x \stackrel{c}{=} -\mathrm{cotg}(x)$, kde $x \in (0,\pi)$.

(7) Zderivujme:

$$(\arcsin(x))' = \frac{1}{\sin'(\arcsin(x))} = \frac{1}{\cos(\arcsin(x)} = \frac{1}{\sqrt{1-\sin^2(\arcsin(x)}} = \frac{1}{\sqrt{1-x^2}}.$$

Platí proto $\int \frac{1}{\sqrt{1-x^2}} \,\mathrm{d}x \stackrel{c}{=} \arcsin(x)$, kde $x \in (-1,1)$.

(8) Zderivujme:

$$(\mathrm{arctg}(x))' = \frac{1}{\mathrm{tg}'(\mathrm{arctg}(x)} = \frac{1}{\frac{1}{\cos^2(\mathrm{arctg}(x)}} = \cos^2(\mathrm{arctg}(x)) = \\ = \frac{\cos^2(\mathrm{arctg}(x))}{\sin^2(\mathrm{arctg}(x)) + \cos^2(\mathrm{arctg}(x))} = \frac{1}{\frac{\sin^2(\mathrm{arctg}(x)) + \cos^2(\mathrm{arctg}(x))}{\cos^2(\mathrm{arctg}(x))}} = \\ = \frac{1}{1 + \mathrm{tg}^2(\mathrm{arctg}(x))} = \frac{1}{1+x^2}.$$

Z toho odvodíme, že $\int \frac{1}{1+x^2} \,\mathrm{d}x \stackrel{c}{=} \mathrm{arctg}(x)$, kde $x \in \mathbb{R}$.

Jak integrovat?

Věta. (linearita primitivní funkce) *Nechť je (a,b) interval, F primitivní funkce k f na (a,b), G primitivní funkce ke g na (a,b) a α, β reálná čísla. Potom $\alpha F + \beta G$ je primitivní funkce k $\alpha f + \beta g$ na (a,b).*

Věta. (první věta o substituci) *Nechť jsou (a,b), (α,β) intervaly. Dále nechť F je primitivní funkce k funkci f na (a,b) a $\varphi\colon(\alpha,\beta)\to(a,b)$ je funkce, která má vlastní derivaci na celém intervalu (α,β). Potom*

$$\int f(\varphi(t))\varphi'(t)\,\mathrm{d}t \overset{c}{=} F(\varphi(t)) \quad \text{pro } t\in(\alpha,\beta).$$

Příklad. Spočtěte $\int \sin^5(t)\cos(t)\,\mathrm{d}t$, kde $t\in\mathbb{R}$.

Řešení. Abychom mohli použít první větu o substituci, musíme najít funkce f, φ, které budou splňovat $\sin^5(t)\cos(t) = f(\varphi(t))\varphi'(t)$. Klíčové je uvědomit si, že $(\sin(t))' = \cos(t)$, což motivuje zavést $\varphi = \sin$.

Najít funkci f, která splňuje $f(\sin(t)) = \sin^5(t)$, už je jednoduché: $f(x) = x^5$. K té nalezneme na $\mathbb{R}$ primitivní funkci $\int x^5\,\mathrm{d}x \overset{c}{=} \frac{x^6}{6}$.

Pokud položíme $(a,b) = (\alpha,\beta) = \mathbb{R}$, naplnili jsme podmínky věty, a tedy dostáváme závěr $\int f(\varphi(t))\varphi'(t)\,\mathrm{d}t \overset{c}{=} F(\varphi(t))$, po dosazení $\int \sin^5(t)\cos(t)\,\mathrm{d}t \overset{c}{=} \frac{1}{6}\sin^6(t)$.

Poznámka. Běžně si vystačíme se zkráceným zápisem, který obecně vypadá následovně:

$$\int f(\varphi(t))\varphi'(t)\,\mathrm{d}t = \left|\begin{array}{l} x=\varphi(t)\\ \mathrm{d}x=\varphi'(t)\,\mathrm{d}t\\ x\in(\alpha,\beta),\ t\in(a,b)\end{array}\right| = \int f(x)\,\mathrm{d}x.$$

Konkrétně v našem příkladu vypadá takto:

$$\int \sin^5(t)\cos(t)\,\mathrm{d}t = \left|\begin{array}{l} x=\sin(t)\\ \mathrm{d}x=\cos(t)\,\mathrm{d}t\\ x\in\mathbb{R},\ t\in\mathbb{R}\end{array}\right| = \int x^5\,\mathrm{d}x \overset{c}{=} \frac{x^6}{6} = \frac{1}{6}\sin^6(t).$$

Věta. (druhá věta o substituci) *Mějme intervaly (a,b), (α,β). Uvažujme funkci $\varphi\colon(\alpha,\beta)\to(a,b)$, která splňuje $\varphi[(\alpha,\beta)] = (a,b)$ a která má na celém (α,β) vlastní nenulovou derivaci. Dále nechť jsou $f\colon(a,b)\to\mathbb{R}$ a $G\colon(\alpha,\beta)\to\mathbb{R}$ funkce, pro které platí*

$$\int f(\varphi(t))\varphi'(t)\,\mathrm{d}t \overset{c}{=} G(t), \quad \text{kde } t\in(\alpha,\beta).$$

Potom $\int f(x)\,\mathrm{d}x \overset{c}{=} G(\varphi^{-1}(x))$ pro $x\in(a,b)$.

Příklad. Spočtěte $\int \sqrt{1-x^2}\,\mathrm{d}x$, kde $x \in (-1,1)$.

Řešení. Položme $(a,b) = (-1,1)$, $\varphi(t) = \sin(t)$, $(\alpha,\beta) = (-\frac{\pi}{2},\frac{\pi}{2})$, pak existuje vlastní nenulová derivace funkce φ na intervalu $(-\frac{\pi}{2},\frac{\pi}{2})$ a $\varphi[(-\frac{\pi}{2},\frac{\pi}{2})] = (-1,1)$. Dále $\varphi^{-1}(x) = a\arcsin(x)$, kde $x \in (a,b)$, a označme $f(x) = \sqrt{1-x^2}$ pro $x \in (-1,1)$. Platí rovnosti

$$\begin{aligned}\int f(\varphi(t))\varphi'(t)\,\mathrm{d}t &= \int \sqrt{1-\sin^2(t)}\cos(t)\,\mathrm{d}t = \int \cos^2(t)\,\mathrm{d}t = \\ &= \int \frac{1+\cos(2t)}{2}\,\mathrm{d}t \overset{c}{=} \frac{t}{2} + \frac{\sin(2t)}{4}, \quad \text{kde } t \in (\alpha,\beta).\end{aligned}$$

Proto dle druhé věty o substituci platí

$$\int \sqrt{1-x^2}\,\mathrm{d}x \overset{c}{=} \frac{\arcsin(x)}{2} + \frac{\sin(2\arcsin(x))}{4}, \quad \text{kde } x \in (-1,1).$$

Věta. (integrace per partes) *Nechť (a,b) je interval a f je spojitá funkce na (a,b). Dále nechť F je primitivní funkce k funkci f na (a,b) a G je primitivní funkce k funkci g na (a,b). Potom*

$$\int g(x)F(x)\,\mathrm{d}x = G(x)F(x) - \int G(x)f(x)\,\mathrm{d}x, \quad \textit{kde } x \in (a,b).$$

Příklad. Spočtěte $\int \operatorname{arctg}(x)\,\mathrm{d}x$ na $\mathbb{R}$.

Řešení. Z úpravy $\int \operatorname{arctg}(x)\,\mathrm{d}x = \int 1\cdot\operatorname{arctg}(x)\,\mathrm{d}x$ nahlédneme, že budeme chtít použít per partes pro funkce $F(x) = \operatorname{arctg}(x)$, $f(x) = \frac{1}{1+x^2}$, $g(x) = 1$, $G(x) = x$. Protože je f spojitá na $\mathbb{R}$, můžeme integraci provést, čímž po úpravě dostaneme

$$\begin{aligned}\int \operatorname{arctg}(x)\,\mathrm{d}x &= \int 1\cdot\operatorname{arctg}(x)\,\mathrm{d}x = x\operatorname{arctg}(x) - \int \frac{x}{1+x^2}\,\mathrm{d}x = \\ &= x\operatorname{arctg}(x) - \frac{1}{2}\int \frac{2x}{1+x^2}\,\mathrm{d}x.\end{aligned}$$

Nyní se nabízí použít první větu o substituci:

$$\int \frac{2x}{1+x^2}\,\mathrm{d}x = \left|\begin{array}{l} t = 1+x^2 \\ \mathrm{d}t = 2x\,\mathrm{d}x \\ t \in (0,\infty),\ x \in \mathbb{R}\end{array}\right| = \int \frac{1}{t}\,\mathrm{d}t \overset{c}{=} \log(t) = \log(1+x^2).$$

Celkově tedy máme

$$\int \operatorname{arctg}(x)\,\mathrm{d}x = x\operatorname{arctg}(x) - \frac{1}{2}\int \frac{2x}{1+x^2}\,\mathrm{d}x \overset{c}{=} x\operatorname{arctg}(x) - \frac{1}{2}\log(1+x^2), \quad \text{kde } x \in \mathbb{R}.$$

Úlohy k procvičení

Úloha 1. Dokažte, že funkce $F(x) = \frac{1}{2}x - \frac{1}{4}\sin(2x)$ je primitivní funkce k funkci $f(x) = \sin^2(x)$, kde $x \in \mathbb{R}$.

Úloha 2. Dokažte, že funkce $F_1(x)$ a $F_2(x)$ jsou primitivní funkce k téže funkci; určete, k jaké funkci jsou primitivní a o jakou konstantu se liší:

(1) $F_1(x) = -\frac{\cos(2x)}{2}$, $\quad F_2(x) = 3 - \cos^2(x)$,
(2) $F_1(x) = \cos(2x)$, $\quad F_2(x) = 6\cos^2(x) + 4\sin^2(x)$,
(3) $F_1(x) = \log\sqrt{x-2} + 3$, $\quad F_2(x) = \log\sqrt{2x-4}$.

Úloha 3. Spočtěte integrály a nalezněte intervaly:

(1) $\int (x^3 + x^2 - 2x)\,\mathrm{d}x$,
(2) $\int (2x^{-3} - x^{-1})\,\mathrm{d}x$,
(3) $\int (1 + 2x)^3\,\mathrm{d}x$,
(4) $\int 5x^2\sqrt{x}\,\mathrm{d}x$,
(5) $\int (\sin(x) - 2\cos(x))\,\mathrm{d}x$.

Úloha 4. Spočtěte integrály a nalezněte intervaly:

(1) $\int \sin(x)\cos(x)\,\mathrm{d}x$,
(2) $\int \cos^3(x)\sin(x)\,\mathrm{d}x$,
(3) $\int -2xe^{-x^2}\,\mathrm{d}x$,
(4) $\int \cos^3(x)\,\mathrm{d}x$.

Úloha 5. Spočtěte integrály:

(1) $\int e^x \sin(x)\,\mathrm{d}x$, kde $x \in \mathbb{R}$,
(2) $\int e^{-x}x\,\mathrm{d}x$, kde $x \in \mathbb{R}$,
(3) $\int x\cos(x)\,\mathrm{d}x$, kde $x \in \mathbb{R}$.

Úloha 6. Vypočtěte $\int \cos(\sqrt{x})\,\mathrm{d}x$.

Návody

1. Ověř z definice primitivní funkce.
2. Derivuj!
3. Použij linearitu primitivní funkce.
4. Použij první větu o substituci.
5. Použij integraci per partes.
6. Per partes a následně druhý věta o substituci.

Literatura a zdroje

[1] L. Pick, S. Hencl, J. Spurný, M. Zelený: *Skripta z Matematické analýzy https://www2.karlin.mff.cuni.cz/~pick/analyza-pro-studenty.pdf.*

Fermiho problémy

Lucka Kundratová

Abstrakt. Enrico Fermi byl jedním z nejvýznamnějších fyziků a matematiků minulého století. Mimo jiné proslul též rychlým řešením problémů velmi náročných na představu, jako například jak velkou plochu bychom pokryli krabicemi od pizzy, kterou zkonzumují Američané za rok, jaká je hmotnost všech proteinů v buňce či kolik ladičů pián je v Chicagu. Podobné otázky jsou oblíbené v přijímacích testech společností, jako například Google. V přednášce si ukážeme, jak k těmto problémům přistupovat, jak odhadovat, a to nejen výsledek, ale i chybu.

Enrico Fermi mimo jiné pracoval na vývoji atomového reaktoru a atomové bomby za druhé světové války. Legenda praví, že z pouhého hození papírové kuličky na stůl dokázal předpovědět sílu výbuchu atomové bomby. Jeho předpověď 10 kt TNT je v porovnání se skutečnou silou 20 kt TNT vskutku impozantní. Podobné odhady se dají využít všude, kam se jen podíváme, a mnohdy nám ušetří mnoho času s rozhodováním či například s výběrem vhodné metody pro provedení experimentu a měření (třeba na měření délky dálnice si nevezmeme milimetrové pravítko). Jak se dá k takovému odhadu dospět? Nejprve se uveďme na pár bodů, které nám k tomu pomohou.

(1) **Napiš řešení** – tedy, zamysli se nad rozumně blízkým řešením. Stačí, když odhadneš řešení s chybou jednoho řádu. Uveďme si příklad.

    Úloha. Jdeš nakupovat a máš dvousetkorunu, kterou jsi ochoten utratit za dobrý oběd. Když uvidíš (dobrý) oběd za 100, okamžitě ho koupíš. Když za 1000, určitě si ho nekoupíš. Pouze tehdy, když bude cena někde okolo té, kterou jsi ochoten zaplatit, budeš váhat. Obvykle nám tedy stačí odhadnout řešení řádově.

(2) **Rozděl a panuj!** Úlohu si rozděl na více částí, každou odhadni zvlášť s chybou do jednoho řádu a poté jednotlivé části spoj.
(3) Urči **horní a dolní hranice.**
(4) A následně je využij k dobrému odhadu pomocí **geometrického průměru**.
(5) **Porovnej svůj výsledek.** Často je možné najít nějakou podobnou úlohu, popřípadě vždy se dá vrátit zpět a podívat se – je můj výsledek příliš malý? Příliš velký? Akorát?
(6) Nebo ho odhadni jinak. **Vždy je více cest.**
(7) **Odhadni chybu.** Vždy chceme vědět, jak moc se můžeme mýlit.

Ale ještě než si uvedené body více rozebereme, uveďme si pár pomůcek, abychom se v tom dobře orientovali.

Zápis čísel pomocí mocnin

Budeme pracovat s velmi velkými a velmi malými čísly. Proto je výhodné přepsat vše ve formě násobku čísla a mocniny 10. Při jejich násobení (dělení) pak jen sečteme (odečteme) mocniny desítky a vynásobíme (vydělíme) číslo (koeficient). Pár příkladů takto zapsaných čísel, jež se nám budou hodit:

(1) Avogadrovo číslo (udává počet částic v jednom molu látky) – $N_A = 6 \cdot 10^{23}$.
(2) Počet obyvatel USA – $3 \cdot 10^8$.
(3) Počet obyvatel ČR – 10^7.
(4) Vzdálenost Země od Slunce v metrech – $1,5 \cdot 10^{11}$.

Počítání geometrického průměru

Definice. *Geometrický průměr* a dvou čísel b a c je definován jako $a = \sqrt{b \cdot c}$.

Při odhadech budeme často používat geometrický průměr, který nám pomůže i s vyjádřením chyby. Jeho počítání si rozdělíme na dva případy:

(1) Pokud po vynásobení je mocnina u desítky sudá, pak jen zprůměrujeme pomocí aritmetického průměru koeficienty a mocniny.

    Úloha. Geometrický průměr $2 \cdot 10^2$ a $3 \cdot 10^4$ je přibližně $\frac{2+3}{2} \cdot 10^{\frac{2+4}{2}} = 2,5 \cdot 10^3$. Přesná hodnota je 2449, tedy odhad je to velmi dobrý.

(2) Pokud po vynásobení je mocnina u desítky lichá, odečteme od mocnin jedničku, koeficienty vynásobíme třemi a pak postupujeme stejně jako v (1).

    Úloha. Geometrický průměr $2 \cdot 10^3$ a $3 \cdot 10^4$ je přibližně $\frac{2+3}{2} \cdot 3 \cdot 10^{\frac{3+4-1}{2}} = 7,5 \cdot 10^3$. Přesná hodnota je 7746.

A nyní hurá na řešení problémů!

Příklad. (rozehřívací) Šance, že vyhrajete loterii, je jednu ku sto milionům. Jak vysoký by byl štos, kdybyste losy pokrývající všechny možnosti poskládali na sebe?

Malá anketa na procvičení představivosti:

(1) Jako Sněžka (1600 m).
(2) Jako Mount Everest (10000 m).
(3) Poloměr Země (10^7 m).
(4) Vzdálenost na Měsíc (10^8 m).

Řešení. K vyřešení úlohy potřebujeme znát dvě informace, a to kolik je losů a jak je jeden los tlustý. Za předpokladu, že vyhrává jen jeden los, máme 10^8 možností, tedy losů.

Jak tlustý je jeden los? Pojďme to odhadnout. Balík papíru (500 ks) má šířku asi 5 cm. Losy však bývají o něco tlustší. Zkusme karty. Balíček 32 karet má šířku asi 1 cm. Tedy:

$$t = \frac{1\,\mathrm{cm}}{32\,\mathrm{losů}} = 0,03\frac{\mathrm{cm}}{\mathrm{los}} = 3 \cdot 10^{-4}\,\frac{\mathrm{m}}{\mathrm{los}}$$
$$\text{výška} = 3 \cdot 10^{-4}\,\frac{\mathrm{m}}{\mathrm{los}} \cdot 10^8\,\mathrm{losů}$$
$$\text{výška} = 3 \cdot 10^4\,\mathrm{m}$$

To je asi 30 km. Třikrát výše, než normálně létají dopravní letadla!

Úloha 1. (klasika) Kolik ladičů pián je v Praze (nebo v Londýně nebo ve Tvém městě)?

Úloha 2. Kdyby se vyroloval veškerý toaletní papír použitý za rok v ČR, jak dlouhou čáru by vytvořil?

Úloha 3. Kolik plechovek džusu potřebuješ vypít, abys měl energii nutnou na výstup „průměrné hory“?

Úloha 4. Kolik váží trilion Kč? Vyjádři, když je to trilion v bankovkách, mincích, zlatě, hodinách otrocké práce ...

Na následujícím příkladu si procvičíme, jak se dívat na problém z různých stran.

Příklad. Jakou plochu bychom pokryli se všemi krabicemi od pizzy, které Američané sní za rok?

Rozděl a panuj (a odhadni chybu)

Vyřešme následující problém a pak se vraťme zpět a odhadněme chybu.

Příklad. Kolik proteinů je v bakteriální buňce (E. Coli)?

Řešení. Předtím, než začneme řešit, si pojďme tipnout.

Řešení si opět rozdělme na menší kroky a u každého se pokusíme o odhad chyby. Rozdělení je následující:

(1) Velikost buňky – jak velká je buňka?
(2) Hmotnost buňky – jaká je hustota buňky (pozor na jednotky)? Pro lehčí výpočet přejděme nyní na jiné, užitečnější jednotky. Na Daltony (Da). A udělejme první aproximaci, $N_A \doteq 10^{24}$.

Definice. (Dalton) Jeden *Dalton* odpovídá hmotnosti vodíkového atomu. Dále platí, že 1 g je roven součinu Avogadrova čísla a hmotnosti 1 Da.

(3) Hmotnost proteinů – jakou chybu děláme? Jakou hmotnost zabírají proteiny? Co tvoří největší část, nejvíce hmotnosti?
(4) Počet proteinů – kolik váží jeden protein? Je složen z aminokyselin (AK), kolik AK má asi jeden protein a kolik váží jedna AK? Nyní už stačí jen vydělit hmotnost všech proteinů hmotností jednoho.

Vraťme se nyní zpět a podívejme se na chyby. První je velikost, dále počet AK, zastoupení proteinů v sušině, ... Vezměme to odzadu. Jak moc přispívají proteiny do hmotnosti? Zde jsou reálné hodnoty mezi $0,1$ až $0,2$. Počet AK je další velkou nepřesností, ale pohybujeme se v oblasti dvojnásobku, tedy reálně mezi 100 až 500, což je obojí docela malá chyba. Co objem? To může být problém, neboť se spoléháme na rozměr a objem roste s jeho třetí mocninou. Přesněji tedy můžeme rozdělit námi získanou informaci a vztáhnout ji pouze na objem jednoho mikrometru krychlového.

Úloha 5. (rozšíření předchozí) Kolik molekul mRNA je v této buňce?

Úlohy

Úloha 6. Kolik lidí právě teď telefonuje nebo píše zprávu na svém mobilu?

Úloha 7. Kolik je na Zemi stromů?

Úloha 8. Kolik buněk je v lidském těle? A co v těle obecného organismu?

Úloha 9. Vraťme se na chvilku k předchozí úloze. Při odběru krve Ti řekli, že počet červených krvinek ve Tvém vzorku je 4–6 milionů na mikrolitr krve. Porovnej jen odhad červených krvinek s výsledkem předchozí úlohy. Kde je problém?

Úloha 10. Kolik židlí se za rok prodá v ČR?

Úloha 11. Jak dlouho stráví voda v atmosféře než opět spadne na zem?

Trošku těžší

Úloha 12. Jaký je průměrný počet nohou zvířat? Za zvířata považuj obratlovce i bezobratlé.

Úloha 13. Jaká je orbitální rychlost Země kolem Slunce? A její kinetická energie?

Úloha 14. Jaký je objem všech na Zemi člověkem postavených struktur (budov, domů, aut, ...)?

Návody

1. Kolik je obyvatel ve městě? Kolik pián připadá na obyvatele? Kolikrát za rok je piáno laděno? Kolik času zabere naladění piána? Kolik hodin pracuje ladič za rok?

2. Kolik toaletního papíru denně/rolí za měsíc vypotřebuješ? Kolik žije lidí v ČR?

3. „Průměrná hora“ je vyšší než budova a nižší než Mt. Everest. Změna potenciální energie je dána vzorcem $E = mgh$, kde m je hmotnost tělesa, $g \doteq 10\ \mathrm{m}\,/\,\mathrm{s}^2$ gravitační zrychlení a h výška/vzdálenost, o kterou se v potenciálním poli posouváme. Jakou energetickou hodnotu má taková 330 ml plechovka?

4. Kolik je to bankovek/mincí a kolik váží jedna? Jakou hodnotu má zlato? Hustota zlata je 20 $\mathrm{t}\,/\,\mathrm{m}^3$.

5. Z počtu proteinů využij produkční rychlost proteinů (délka jednoho buněčného cyklu je v rozmezí 30 min a 1 h, použij 3000 s, a rychlost je počet za čas) a následně rychlost produkce protein/mRNA (rychlost je 0,1-1 prot/mRNA/s).

6. Kolik lidí je na světě? Kolik času/jakou frakci tráví lidé denně psaním či voláním?

7. Jak velkou plochu zabírá souš? Kolik je asi stromů na 1 km^2?

8. Jak velké je lidské tělo a jak velká je eukaryotická buňka?

9. V žilách nám obvykle koluje kolem 5 l krve.

10. Kolik židlí „vlastníš“ – na kolika sedíš? Jak často svou židli/své židle měníš?

11. Jaký je odpar vody na Zemi za rok? Kolik vody je v atmosféře? Ustálený stav říká, že je stejný přísun vody do atmosféry jako z atmosféry. Jak často tedy prší?

12. Jaký je průměrný počet nohou obratlovců? A co bezobratlých?

Bezobratlí – hmyzu je opravdu hodně, asi 10^{18}, ovšem červíků je ještě více. Členovců kolem 10^{18}, planktonu 10^{19-20}, hlístů, háďátek a tak podobně asi 10^{20}.

13. Jaká je doba oběhu a jaká je délka? Jaká je hmotnost Země? Poloměr je asi 6000 km, hustota je větší než vody ($1000\ \mathrm{kg}\,/\,\mathrm{m}^3$) a menší než železa ($8000\ \mathrm{kg}\,/\,\mathrm{m}^3$). Jeden rok má $\pi \cdot 10^7$ s.

14. Budovy dominují. Jak velká jsou místa, kde lidé žijí, a jak velká ta, kde pracují?

Literatura a zdroje

Chtěla bych poděkovat *Janu Kadlecovi*, jehož příspěvek jsem převzala.

[1] Lawrence Weinstein, John A. Adam: *Guesstimation: Solving the World's Problems on the Back of a Cocktail Napkin*, Princeton University Press, 2009.

[2] Lawrence Weinstein: *Guesstimation 2.0: Solving Today's Problems on the Back of a Napkin*, Princeton University Press, 2012.

[3] John Harte: *Consider A Spherical Cow: A Course in Environmental Problem Solving*, University Science books, 1988.

[4] Ron Milo, Rob Phillips: *Cell biology by the numbers*, Garland Science, 2015.

[5] Yinon M. Bar-On, Rob Phillips, Ron Milo: *The Biomass Distribution on Earth*, PNAS, 2018.

[6] Luis Villazon: *What is the average number of legs for an animal?*, *http://www.sciencefocus.com/qa/what-average-number-legs-animal*.

Úvod do lineární algebry

Anna Marie Minarovičová

Abstrakt. Cílem příspěvku je seznámit čtenáře se základními pojmy a koncepty týkajícími se lineární algebry a jejího použití.

V tomto příspěvku se budeme věnovati lineární algebře. Než se ale pustíme do definic a tvrzení, pojďme si uvést pár příkladů, k čemu nám může být lineární algebra užitečná.

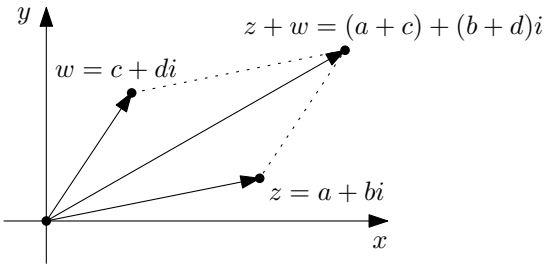
Příklad. Soustavu lineárních rovnic

$$\begin{aligned} x + 2y + 3z &= 4, \\ 2x + y &= -1, \\ -x + 2z &= 0 \end{aligned}$$

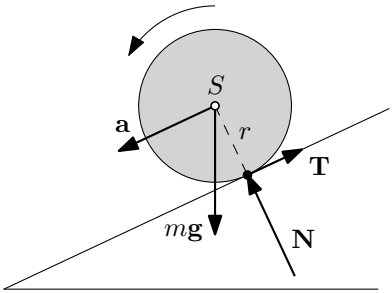
lze reprezentovat maticí

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 4 \\ 2 & 1 & 0 & -1 \\ -1 & 0 & 2 & 0 \end{array}\right).$$

Příklad. Komplexní čísla můžeme vyjadřovat pomocí vektorů v komplexní rovině. Operace s komplexními čísly pak mají přirozenou reprezentaci pomocí vektorových operací.



Příklad. Pokud chceme v klasické mechanice vyšetřovat pohyb tělesa, pomůžeme si 3-dimenzionálními vektory, jež u daného tělesa reprezentují polohu, rychlost, zrychlení (tyto veličiny jsou svázány derivacemi) a síly na dané těleso působící. Například si představme kutálející se balónek po nakloněné rovině.



Abychom se mohli zabývat lineární algebrou, pojďme si zadefinovat základní objekty, se kterými budeme dále pracovat.

Definice. Veličinu, jež je určená pouze svou velikostí, nazýváme *skalárem*. V matematice takto označujeme zpravidla jediné reálné či komplexní číslo.

Definice. *Aritmetickým vektorem* nad $\mathbb{R}$ s n složkami rozumíme uspořádanou n-tici reálných čísel. Vektory často reprezentujeme veličiny, jež mají velikost a směr.

Definice. *Reálnou maticí A typu $n \times m$* rozumíme obdélníkové schéma o m sloupcích a n řádcích, jejíž políčka obsahují reálná čísla. Těmto políčkům říkáme *prvky* matice A a prvek v i-tém řádku a j-tém sloupci značíme a_{ij}.

Maticové operace a speciální matice

Nyní se podívejme na základní operace, které používáme při práci s maticemi a vektory, jež jsou v podstatě speciální matice typu $n \times 1$.

Definice. *Jednotkovou maticí* typu $n \times n$ rozumíme čtvercovou matici, jež má na diagonále 1 a mimo diagonálu 0 (diagonálou myslíme hlavní diagonálu z levého horního rohu). Takovou matici značíme I_n.

Definice. (násobení skalárem) Pro matici $A = (a_{ij})$ typu $n \times m$ a skalár t definujeme t-násobek matice A jako matici $t \cdot A = tA = (ta_{ij})_{n \times m}$.

Definice. (sčítání matic) Mějme matice A a B typu $n \times m$. Pak jejich *součtem* je matice C typu $n \times m$, pro kterou platí $c_{ij} = a_{ij} + b_{ij}$.

Tvrzení. (asociativita a komutativita sčítání matic) *Máme-li matice A, B a C typu $n \times m$, potom platí*

(1) $A + B = B + A$,
(2) $(A + B) + C = A + (B + C)$.

Úloha. Jsou dány následující matice A, B a C:

$$A = \begin{pmatrix} 12 & 45 & 3 \\ 31 & 23 & 7 \\ 52 & 64 & 4 \end{pmatrix}, \qquad B = \begin{pmatrix} 115 & 153 & 9 \\ 54 & 104 & 72 \\ 435 & 345 & 35 \end{pmatrix}, \qquad C = I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Spočtěte $A + B$, $B - A$, $A - C$, $(A - C) + B$.

Definice. (násobení matic) Mějme matici A typu $m \times n$ a matici B typu $n \times p$. Pak *součinem* matic $A \cdot B$ rozumíme matici C typu $m \times p$, kde $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$.

Tvrzení. (asociativita násobení matic) *Máme-li matice A typu $m \times n$, B typu $n \times p$ a C typu $p \times q$, potom platí $(A \cdot B) \cdot C = A \cdot (B \cdot C)$.*

Úloha. Na následujících zadáních si procvičte násobení skalárem a násobení matic:

(a) $7 \cdot \begin{pmatrix} 6 & -4 \\ -3 & 8 \end{pmatrix}$, (b) $3 \cdot \begin{pmatrix} -6 & -7 \\ 1 & 3 \\ 0 & 4 \end{pmatrix}$, (c) $\begin{pmatrix} 5 & -4 & 3 \\ -2 & 7 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 8 \\ -5 \end{pmatrix}$,

(d) $\begin{pmatrix} 12 \\ 8 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 2 & -3 \end{pmatrix}$, (e) $\begin{pmatrix} -1 & 2 & -3 \end{pmatrix} \cdot \begin{pmatrix} 12 \\ 8 \\ 1 \end{pmatrix}$,

(f) $\begin{pmatrix} 4 & 2 & 3 \\ 1 & 3 & 2 \\ 5 & 8 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 15 & 9 \\ 5 & 10 & 2 \\ 4 & 3 & 5 \end{pmatrix}$, (g) $\begin{pmatrix} 4 & 2 & 3 \\ 1 & 3 & 2 \\ 5 & 8 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 15 & 9 \\ 5 & 10 & 2 \\ 4 & 3 & 5 \end{pmatrix} \cdot \begin{pmatrix} -2 \\ 0 \\ 1 \end{pmatrix}$.

Liší se výsledek úlohy (d) a (e)? Pokud ano, jak? Je násobení matic komutativní (násobení dvou matic je komutativní, pokud platí $A \cdot B = B \cdot A$)?

Cvičení. Co musejí splňovat matice A a B, aby byly definovány oba součiny $A \cdot B$ i $B \cdot A$? Najděte několik různých dvojic matic A a B, aby navíc platila rovnost $A \cdot B = B \cdot A$.

Definice. *Transponovaná matice* k matici A typu $n \times m$ je čtvercová matice A^T typu $m \times n$, pro jejíž jednotlivé prvky platí $a_{ij}^T = a_{ji}$.

Soustavy lineárních rovnic

Nyní se vrátíme k motivačnímu příkladu ze začátku

$$\begin{aligned} x + 2y + 3z &= 4, \\ 2x + y &= -1, \\ -x + 2z &= 0. \end{aligned}$$

Levou stranu, tedy koeficienty před neznámými, můžeme reprezentovat maticí A (každý sloupec matice A je svázán s jednou neznámou) a pravou stranu vektorem b. Dohromady celou soustavu reprezentujeme *rozšířenou maticí soustavy* $(A \mid b)$[1]:

$$(A \mid b) = \left(\begin{array}{ccc|c} 1 & 2 & 3 & 4 \\ 2 & 1 & 0 & -1 \\ -1 & 0 & 2 & 0 \end{array}\right).$$

[1] Touto maticí rozumíme matici A, kterou vpravo rozšíříme sloupcem tvořeným vektorem b.

Vyřešit soustavu lineárních rovnic (SLR) je potom ekvivalentní s nalezením všech vektorů u, které splňují rovnost $A \cdot u = b$, kde $u = (x\ y\ z)^T$. V maticovém zápisu má tedy naše SLR tvar

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 0 \\ -1 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 4 \\ -1 \\ 0 \end{pmatrix}.$$

Uveďme si nějaké základní pojmy, které nás dovedou až k samotnému algoritmu na řešení SLR, ke Gaussově eliminaci. Pro zjednodušení se zabývejme pouze případem, kdy má soustava pouze jedno jednoznačně určené řešení.

Definice. *Ekvivalentní úpravou* soustavy lineárních rovnic rozumíme úpravu, která nemění množinu všech řešení.

Definice. *Elementární úpravy* soustavy lineárních rovnic jsou

(1) prohození dvou rovnic,
(2) vynásobení nějaké rovnice nenulovým číslem t,
(3) přičtení t-násobku jedné rovnice k jiné rovnici.

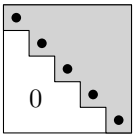
Tvrzení. *Elementární úpravy jsou ekvivalentní.*

Pokud soustavu reprezentujeme pomocí rozšířené matice soustavy $(A \mid b)$, dostáváme z elementárních úprav elementární řádkové úpravy.

Definice. *Elementární řádkové úpravy* rozšířené matice soustavy jsou

(1) prohození dvou řádků matice,
(2) vynásobení jednoho z řádků matice nenulovým číslem t,
(3) přičtení t-násobku násobku jednoho řádku k řádku jinému.

Gaussovou eliminací převádíme matici A posloupností elementárních řádkových úprav do *řádkově odstupňovaného tvaru* (tj. matici, ve které je každý následující řádek kratší než ten předcházející).



Eliminace jednoho sloupce (jedné proměnné) pro matici $A = (a_{ij})_{n\times m}$ probíhá následovně:

(1) najdeme první nenulový sloupec, ať to je k-tý sloupec,
(2) pokud $a_{1k} = 0$, prohodíme první řádek s libovolným řádkem i, ve kterém je $a_{ik} \neq 0$,
(3) není-li a_{1k} nulové, pak pro každé $i = 2, 3, \ldots, n$ přičteme $(-a_{ik}/a_{1k})$-násobek prvního řádku k i-tému řádku (ke každému řádku kromě prvního přičteme násobek prvního řádku, čímž vynulujeme prvky v daném sloupci ve všech řádcích kromě prvního).

Tento postup opakujeme pro všechny sloupce. Jakmile máme matici v řádkově odstupňovaném tvaru, uděláme zpětnou substituci, kdy jednotlivým proměnným připisujeme takové hodnoty, aby seděly ke sloupci pravých stran.

Ukažme si Gaussovu eliminaci a zpětnou substituci na našem příkladě:

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 4 \\ 2 & 1 & 0 & -1 \\ -1 & 0 & 2 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 2 & 3 & 4 \\ 0 & -3 & -6 & -9 \\ 0 & 2 & 5 & 4 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 2 & 3 & 4 \\ 0 & -3 & -6 & -9 \\ 0 & 0 & 3 & -6 \end{array}\right),$$

$$\begin{aligned} 3z = -6 \quad &\Longrightarrow \quad z = -2, \\ -3y - 6z = -3y + 12 = -9 \quad &\Longrightarrow \quad y = 7, \\ x + 2y + 3z = x + 14 - 6 = 4 \quad &\Longrightarrow \quad x = -4. \end{aligned}$$

Úloha. Najděte všechny vektory u splňující rovnice

$$\begin{pmatrix} 1 & 2 & 2 \\ 2 & 0 & 1 \\ 1 & 1 & 2 \end{pmatrix} \cdot u = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \qquad \begin{pmatrix} 3 & 2 & -1 \\ 2 & -2 & 4 \\ -1 & \frac{1}{2} & -1 \end{pmatrix} \cdot u = \begin{pmatrix} 1 \\ -2 \\ 0 \end{pmatrix}.$$

Definice. *Elementární matice* je matice, která vznikne z jednotkové matice jednou elementární řádkovou úpravou.

Úloha. Zkuste najít elementární matice E_1, E_2, E_3 typu 3×3 takové, že pokud jimi vynásobíme matici A zleva, tak docílíme:

(1) prohození prvního a druhého řádku,
(2) vynásobení druhého řádku číslem 5,
(3) přičtení trojnásobku druhého řádku k třetímu řádku,

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 0 \\ -1 & 0 & 2 \end{pmatrix},$$

$$E_1 \cdot A = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & 3 \\ -1 & 0 & 2 \end{pmatrix}, \qquad E_2 \cdot A = \begin{pmatrix} 1 & 2 & 3 \\ 10 & 5 & 0 \\ -1 & 0 & 2 \end{pmatrix}, \qquad E_3 \cdot A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 0 \\ 5 & 3 & 2 \end{pmatrix}.$$

Inverzní matice

Definice. Je-li A matice typu $n \times m$, X matice typu $m \times n$, pak X nazýváme *inverzní maticí zprava* k matici A, pokud platí $A \cdot X = I_n$, matice A se v tom případě nazývá *invertovatelná zprava*.

Definice. Je-li A matice typu $n \times m$, X matice typu $m \times n$, pak X nazýváme *inverzní maticí zleva* k matici A, pokud platí $X \cdot A = I_m$, matice A se v tom případě nazývá *invertovatelná zleva*.

Definice. Jsou-li A a X čtvercové matice typu $n \times n$, pak X nazýváme *inverzní maticí* k matici A (značíme ji X^{-1}), pokud platí $X \cdot A = A \cdot X = I_n$, matice A se v tom případě nazývá *invertovatelná matice*.

Cvičení. Musí inverzní matice existovat ke každé matici A? Je A^{-1} (pokud existuje) určena jednoznačně?

Úloha. Najděte matice inverzní zprava k maticím

$$\begin{pmatrix} -1 & 2 & 3 \\ 4 & -9 & 8 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 2 & -4 \\ 2 & 1 & -4 \end{pmatrix}.$$

Úloha. Najděte matice inverzní zleva k maticím

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}, \qquad \begin{pmatrix} 1 & -1 \\ 1 & 1 \\ 2 & 3 \end{pmatrix}.$$

Úloha. Najděte inverzní matice k maticím

$$\begin{pmatrix} 1 & 3 \\ -2 & 9 \end{pmatrix}, \qquad \begin{pmatrix} 4 & 3 \\ 3 & 2 \end{pmatrix}.$$

V předchozí části jsme si ukázali, že soustavu lineárních rovnic můžeme vyjádřit maticově jako $Au = b$. Všimněme si, že pokud je matice A invertovatelná, je možné vektor řešení vyjádřit jako $u = A^{-1}Au = A^{-1}b$.

Cvičení. Zamyslete se, proč řešení soustav, které nejsou reprezentované invertovatelnou maticí, nelze takto elegantně vyjádřit. Co to pro soustavu znamená?

Lineární zobrazení

Definice. *Lineární zobrazení* je takové zobrazení $f : \mathbb{R}^m \to \mathbb{R}^n$, pro které platí $f(u + v) = f(u) + f(v)$ a $f(tu) = tf(u)$ pro reálné číslo t a vektory u a v.

Tvrzení. *Ke každému lineárnímu zobrazení $f : \mathbb{R}^m \to \mathbb{R}^n$ existuje jednoznačně určená matice A typu $n \times m$ taková, že pro všechny $v \in \mathbb{R}^m$ platí $f(v) = Av$.*

Cvičení. Nalezněte matice typu 2×2 těchto lineárních zobrazení: identické zobrazení, osová souměrnost, středová souměrnost, stejnolehlost. Na jaký útvar se při nich zobrazí čtverec s vrcholy $(0, 0), (0, 1), (1, 1), (1, 0)$?

Cvičení. Nalezněte geometrický význam lineárního zobrazení určeného maticí

$$\begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix}.$$

Literatura a zdroje

[1] Libor Barto, Jiří Tůma: *Lineární algebra.*
[2] Terka Kučerová: *Lineární algebra*, Sklené, 2019.
[3] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, MIT Press, 2016.

Vězni, domorodci a kouzelníci

Radek Olšák

Abstrakt. Příspěvek sestává z hromady pěkných a často i notně trikových úloh na pomezí logiky a kombinatoriky, jejichž sjednocující myšlenkou je „kdo může co vědět“.

Budeme z různých úhlů zkoumat, co znamená „něco vědět“. Přesněji, bude nás zajímat, v čem všem může být skrytá šikovná informace – a to buď sama od sebe, nebo díky vychytralé domluvě.

Rozhovory

Začneme několika logickými úlohami, které jsou velmi dynamické. Rozmyslet si, co kdo ve kterou chvíli může vědět, totiž vůbec nemusí být triviální. Motto:

Tři logici přijdou do hospody.

„Dáte si všichni tři pivo?“

„Nevím . . . “

„Nevím . . . “

„Ano.“

Příklad 1. Albert a Bernard se snaží zjistit, kdy má Cheryl narozeniny. Už vědí, že je to některý z následujících deseti dnů: 15. květen, 16. květen, 19. květen, 17. červen, 18. červen, 14. červenec, 16. červenec, 14. srpen, 15. srpen, 17. srpen.

Když se všichni sešli, Cheryl pošeptala Albertovi, který měsíc je ten správný. Potom pošeptala Bernardovi správný den.

Cheryl: *„Už víte?“*

Albert: *„Ne, neví to ani jeden z nás!“*

Bernard: *„Teď už to ale vím!“*

Albert: *„Tak já teda taky.“*

Kdy má Cheryl narozeniny?

Příklad 2. V kruhu sedělo dvanáct bystrých mužů a každému z nich byla náhodně rozdána jedna z dvanácti karet – devíti prázdných a tří význačných označených jako J, Q a K. Každý z mužů se podíval na svou kartu a poté ji poslal sousedovi po pravé ruce. Takto se pokračovalo dále, přičemž po každém zhlédnutí karty byli všichni v jeden okamžik vyzváni, aby se přihlásili, pokud vědí, kdo právě drží kterou význačnou kartu. V prvních čtyřech kolech se nepřihlásil nikdo a po spatření páté karty zvedl ruku jeden člověk. Kolik lidí se přihlásilo po spatření šesté karty? A kolik po spatření sedmé? (Náboj)

Příklad 3. Mirek pověděl oběma, Kennymu a Pavlovi, jedno přirozené číslo. Dále jim sdělil, že jejich čísla jsou různá a jejich součtem je dvojciferné číslo. Pak se mezi Kennym a Pavlem odehrála následující konverzace:

Kenny: *„Nedovedu určit, kdo z nás má větší číslo.“*

Pavel: *„Ani já to nedovedu určit, ale prozradím, že moje číslo je dělitelné* 17*.“*

Kenny: *„Aha, tak teď už umím jednoznačně určit, jaký je součet našich čísel.“*

Určete součet jejich čísel. (Náboj)

Příklad 4. Anna má číslo a, Bill má číslo b, přičemž a, b jsou přirozená čísla lišící se o 1.

Anna: *„Neznám tvé číslo.“*

Bill: *„Já taky ne.“*

Anna: *„Já už ano.“*

Bill: *„Já také.“*

Najděte číslo, které některý z nich měl.

Příklad 5. Anna, Bill a Cath mají na čelech přilepené karty s přirozenými čísly. Přitom vědí, že součet dvou z těchto čísel dává číslo třetí.

Anna: *„Neznám své číslo.“*

Bill: *„Já taky ne.“*

Cath: *„Já taky ne.“*

Anna: *„Ha, moje číslo je* 50*.“*

Jaká jsou ta zbylá dvě?

Příklad 6. Je známo, že a, b jsou přirozená čísla splňující $1 < a < b$, navíc $a + b \leq 100$. Pavel zná součin ab a Sára součet $a + b$.

Pavel: *„Neznám ta původní čísla.“*

Sára: *„Věděla jsem, že je neznáš.“*

Pavel: *„Už je znám.“*

Sára: *„Já už taky.“*

Příklad 7. Dostali jste se do finále televizní soutěže. Před sebou vidíte troje zavřené dveře. Za jedněmi je nové auto, za zbylými dvěma koza. Můžete ukázat na jedny dveře. Pak moderátor otevře jiné, za nimiž bude koza, a dá vám možnost vaši dřívější volbu dveří změnit. Vyplatí se to?[1] (Monty Hall)

[1] Auto je lepší než koza.

Příklad 8. V jihoafrickém kmenu Bongo-bongo má každý domorodec na čele modrou nebo červenou tečku. Tisíciletá tradice praví, že kdykoli někdo zjistí barvu své tečky, musí si následující den vzít život. Jednou přijde do vesnice cizinec a na veřejném shromáždění sdělí všem svůj objev: „Někdo má na čele modrou tečku.“ Ukažte, že tím odstartuje vlnu sebevražd, která skončí smrtí úplně všech domorodců.
(folklor)

Vězni

Vězňům vždy zadáme na první pohled skoro nemožný úkol. Oproti předchozím úlohám je tu ale jeden velký rozdíl: vychytralí vězni si předem mohou domluvit strategii. Mají šanci?

Příklad 9. Sto vězňů stojí v řadě. Každý má na hlavě černý nebo bílý klobouk a vidí všechny před sebou. Kat jde postupně odzadu a ptá se na barvu klobouku. Když řekne vězeň svou, přežije, jinak je popraven. Všichni slyší odpovědi všech ostatních i jejich osudy. Navrhněte taktiku, při které co nejpravděpodobněji přežije co nejvíce vězňů, pokud se na ní mohou domluvit předem. (folklor)

Příklad 10. Řešte předchozí příklad pro klobouky, které mají n barev.

Příklad 11. Deset vězňů sedí v kruhu, každý má na čele napsané číslo od 1 do 10 (ne nutně každý jiné). Každý vidí čísla všech ostatních. Na povel všichni současně vykřiknou číslo. Pokud někdo vykřikne to své, jsou všichni osvobozeni. Navrhněte taktiku, při které budou vězni jistě osvobozeni, pokud se mohou domluvit předem.
(folklor)

Příklad 12. Ve vězení sedí 100 vězňů. Ředitel věznice se rozhodl, že jim dá šanci na svobodu. Do 100 očíslovaných šuplíků ve své obrovské 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 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 $1-\left(\frac{1}{51}+\frac{1}{52}+\cdots+\frac{1}{100}\right)>\frac{3}{10}$.
(folklor)

Příklad 13. V kruhu sedí n vězňů. Kouzelník si u každého hodí spravedlivou mincí a podle toho mu dá červený, nebo modrý klobouk. Každý vězeň vidí klobouky ostatních, ale ne ten svůj. Poté všichni najednou řeknou nějaká reálná čísla. Vyhrají právě tehdy, když bude součet jejich čísel kladný a červených klobouků bude sudý počet, nebo pokud bude součet jejich čísel záporný a červených klobouků bude lichý počet. Mohou si ovšem předem domluvit strategii. V závislosti na n nalezněte největší možné p, pro které existuje strategie taková, že vězni vyhrají s pravděpodobností p.
(iKS–5–C7)

Příklad 14. V kruhu sedí $n \geq 3$ vězňů. Soudce si u každého vězně hodí spravedlivou mincí a podle toho mu dá buď modrý, nebo červený klobouk. Každý z vězňů pak soudci buď pošeptá „červený“, „modrý“, nebo „nevím“. Aby nebyli odsouzeni, musí se alespoň jeden vězeň trefit a žádný se nesmí splést. Navrhněte strategii, při které uspějí s maximální pravděpodobností.

Kouzelníci

Nyní se dostáváme k úlohám, ve kterých vystupují různí kouzelníci se svými promyšlenými triky.

Příklad 15. Kouzelník Arutyun a jeho asistent Amayak předvedou následující supertrik. V místnosti je ruleta. Diváci na ní vyznačí 2007 bodů a Amayak jeden z nich smaže. Potom se Arutyun vrátí do místnosti a uhodne půlkružnici, na které smazaný bod ležel. Jak mohou tento trik provést? (ARO 2007)

Příklad 16. Dva kouzelníci Adam a Bonifác byli uvězněni a žalářník Emil s nimi chce hrát ďábelskou hru. Na stole v cele je pevně postavena šachovnice $n \times n$. Emil odvede Bonifáce pryč a po svém návratu na každé políčko šachovnice položí minci, na jejíž vrchní straně je buď panna, nebo orel. Následně ukáže Adamovi své nejoblíbenější políčko a Adam pak musí otočit právě jednu minci. Poté je Bonifác přiveden zpět. Uhodne-li Bonifác Emilovo oblíbené políčko, budou oba kouzelníci propuštěni. Pro která n lze Emila přelstít? (ITAMO 2013)

Příklad 17. Arutyun a Amayak ukazují další zázračný trik. Diváci napíší na tabuli posloupnost n cifer $0, 1, \ldots, 9$ a Amayak dvě sousední zakryje černým diskem. Posléze Arutyun přijde a dvě zakryté číslice bezchybně uhodne včetně jejich pořadí. Pro které nejmenší n takový trik mohou předvádět? (ARO 2007)

Příklad 18. Jsou dána přirozená n a k splňující $n \geq k \geq 2$. Hrajeme hru proti zlému čaroději. Ten má $2n$ pexesových karet, tj. balíček obsahuje n dvojic stejných karet. Tyto karty čaroděj umístí do řady, čímž hra začíná. V každém tahu můžeme otočit k karet. Pokud mezi nimi jsou dvě stejné, okamžitě vyhráváme. V opačném případě je čaroděj podle své nálady nějak zamíchá a umístí zpět do řady. Pro které hodnoty k umíme určitě v konečném počtu tahů vyhrát? (USAMO 2016)

Příklad 19. Kenny s Pepou se domluvili, že večer při ohni předvedou trik. Pepa nechal Olina vybrat pět písní ze zpěvníku se 124 písněmi. Sám pak z těchto pěti písní vybral čtyři a určil, v jakém pořadí se budou hrát. Na to zavolali Kennyho a ony čtyři písně mu v daném pořadí zazpívali. Jakmile dozpívali, Kenny ihned začal zpívat zbývající pátou. Jak to Pepa s Kennym mohli udělat? (PraSe-30-1-8)

Kódy

Plynule pokračujme v řešení dalších problémů, ve kterých je také potřeba najít nějaké chytré kódování.

Příklad 20. Na obvodu rulety jsou na n pozicích napsané cifry 0 a 1. Většina kola je však skrytá, vidět je jen k následujících pozic. Cifry jsou ale na kole napsané tak chytře, že z těchto k cifer vždy umíme poznat, jak je ruleta natočená. V závislosti na k nalezněte maximální n, pro které je to možné.

Příklad 21. Dva dobří přátelé si píší zprávy sestávající vždy přesně z k písmen n-písmenné abecedy. Aby se nemohlo dojít k nedorozumění, musí se každá dvě používaná slova lišit alespoň na dvou pozicích. Ukažte, že mohou používat k^{n-1} různých slov. (KMS 05/06 Z3 12)

Příklad 22. Medvěd měl sen o polynomu p s nezápornými celými koeficienty. Kdykoli Liška řekne číslo z, Medvěd jí prozradí hodnotu $p(z)$. Kolik nejméně otázek Liška potřebuje k tomu, aby určila Medvědův polynom? (PraSe-36-4-6)

Příklad 23. Dva ruští a jeden americký špion se potkali v Moskvě u partičky karet. Mají sedm různých karet. Oba Rusové si líznou tři a na Američana zbude jen jedna. Rusové by rádi ještě před začátkem partie zjistili, kdo drží které karty. To chtějí provést tak, aby si Američan stále nebyl jistý vlastníkem žádné další karty. Může mít ruská rozvědka takový protokol, který jim to umožní bez ohledu na to, zda jej Američan zná? (Moskva 2000)

Nekonečná jízda

Zkusme nakonec řešit další hádanky s vězni, ve kterých však bude vystupovat nějaké to nekonečno[2].

Příklad 24. Ve vězení sedí 100 vězňů. Čas od času vezme bachař některého z nich na výslech. Ve výslechové místnosti je jen jedna žárovka s vypínačem, který vězni mohou přepínat. Kterýkoli vězeň může při výslechu prohlásit: „Už jsme byli všichni vyslechnuti, takže nás nemáte důvod dál zadržovat!“ Je-li to pravda, budou všichni propuštěni, v opačném případě ihned popraveni. Bachař si přitom musí výslechy předem naplánovat tak, aby každého vězně potenciálně vyslýchal nekonečněkrát. Mohou se vězni bezpečně dostat na svobodu?

Příklad 25. Řešte předchozí úlohu s následující obtíží: Předem je dáno přirozené k a bachař smí až k-krát změnit stav žárovky.

Předchozí příklad má velmi zajímavá zobecnění, která vězňům umožňují skoro libovolnou komunikaci. My se však raději pustíme do dalších příkladů jiného rázu.

Příklad 26. Za sebou sedí prasátka postupně očíslovaná přirozenými čísly, přičemž každé vidí všechny před sebou. Každé má na hlavě klobouk v nějakém odstínu šedé[3]. Naráz všechna musí vykřiknout barvu svého klobouku. Existuje taková strategie, aby se spletlo pouze konečně mnoho z nich? (folklor)

[2]Kdykoli to hraje roli, věříme v *axiom výběru*.

[3]Každý takový odstín odpovídá nějakému reálnému číslu z intervalu od 0 do 1.

Příklad 27. Král má ve sklepení svého hradu za každé přirozené číslo právě jednu truhlu s hromadou zlata nějaké reálné hmotnosti. Jednoho dne zadal svým 100 komorníkům nelehký úkol. Komorníci budou po jednom chodit do sklepa. Každý komorník se pak může podívat do libovolně mnoha truhlic, ale ne do všech. Při výstupu ze sklepa pak musí oznámit číslo nějaké truhly, kterou neotevřel, a váhu zlata v ní. Pokud se splete nejvýše jeden komorník, budou všichni bohatě odměněni. Můžou se komorníci předem domluvit tak, aby to zvládli?

Příklad 28. V řadě stojí vězni, kteří jsou postupně označeni přirozenými čísly, přičemž každý vidí právě vězně s vyššími čísly. Každý vězeň má na zádech svého oblečení $k = 0, 1, \ldots, n$ černých proužků. Dozorce postupně prochází kolem a ptá se vězňů na počet jejich proužků. Každý z vězňů přitom slyší odpovědi svých předchůdců. Kdo odpoví správně, je propuštěn. Zachraňte jich co nejvíc!

Příklad 29. Štěpán poslal Filipovi a Radovi dva provázky spolu s informací, jak jsou dlouhé. Poté se odehrála následující mailová konverzace:

Štěpán: *„Poslal jsem vám dva různě dlouhé provázky, jejichž délka v centimetrech je*

$$a - \frac{1}{3^b} - \frac{1}{3^{b+c+1}},$$

kde a, b, c jsou přirozená čísla.“

Filip: *„To je zajímavé. Ale neumím říct, který z nich je delší.“*

Rado: *„Já taky ne.“*

Filip: *„Já taky ne.“*

Rado: *„Já taky ne.“*

Štěpán: *„Je jedno, kolikrát si tohle řeknete, stejně nebudete vědět, čí je delší.“*

Filip: *„To je fakt zajímavá informace. Ale pořád nevím, kdo má větší délku.“*

Rado: *„Já taky ne.“*

Filip: *„Já taky ne.“*

Štěpán: *„Opět, je jedno, kolikrát si tohle řeknete, stejně nebudete vědět, který z provázků je delší.“*

Filip: *„Ha. No, furt nevím, kdo má ten delší.“*

Rado: *„Já taky ne.“*

Filip: *„Já taky ne.“*

Rado: *„Já taky ne.“*

Štěpán: *„Ve skutečnosti, je jedno, kolikrát uděláme tento malý rozhovůrek, kde budete cik-cak tvrdit, že nevíte, kdo má delší provázek, a já vám řeknu, že je jedno, kolikrát si to řeknete a že to stejně nezjistíte, protože to ani z tohoto prohlášení nezjistíte. Navíc, pokud bych zopakoval předchozí větu ještě jednou, byla by stále pravdivá. A to dokonce i kdybych ji zopakoval ne jednou, ale i dvakrát, třikrát, ba i tisíckrát.“*

Filip: *„To je fakt super informace. Ale pořád neumím říct, který z nich je delší.“*

Rado: *„Já taky ne.“*

Filip: *„Já taky ne.“*

Štěpán: *„Jo, pořád je jedno, kolikrát si teď navzájem řeknete, že to furt nevíte, pořád to nebudete vědět. A i když vám teď tuhle větu řeknu dvatisícesedmnáctkrát, pořád to vědět nebudete.“*

Filip: *„Zajímavé. Ale pořád nevím, kdo má větší kus.“*

Rado: *„Já taky ne.“*

Filip: *„Já taky ne.“*

Rado: *„Já taky ne.“*

Filip: *„Ahá! Tak už vím, čí provázek je delší!“*

Jak dlouhý byl Filipův provázek? (*i*KS-7-C5)

Návody

1. Rozebírejte.

2. Po prvním zvednutí ruky ostatní okamžitě vědí, že tento člověk držel jako první a jako pátou význačné karty.

3. První dvě věty jim dávají pouze čísla 17 a 34. Protože Kenny ví jaké z nich Pavel má, musí mít sám to druhé.

4. První otázka zakazuje 1 pro Annu, druhá $1, 2$ pro Billa. Potom ale musel mít jeden z nich 3.

5. Řešení je $(a, b, c) = (50, 20, 30)$.

6. Vyjde 4 a 13, ale dá to hodně rozebírací práce.

7. Představ si, že by dveří bylo 100 a za 99 z nich byla koza. Moderátor by otevřel 98 z nevybraných a vyvedl kozy.

8. Indukce dle počtu modrých teček.

9. Parita, splést se může jen první.

10. Počítání modulo n, splést se může jen první.

11. Každý si zabere jeden součet modulo 10.

12. Vězni si mohou označit šuplíky svými jmény a podle nich je procházet.

13. Nalezněte strategii, která se rozbije pouze tehdy, když jsou všechny klobouky červené.

14. Představte si n-dimenzionální krychli. Vymyslete strategii, která buď funguje, nebo se spletou všichni.

15. Orientujte si kružnici a soustřeďte se na nejdelší oblouk.

16. Jde to pouze pro $n = 2^k$. Adam a Bonifác si čtverečky označí čísly ve dvojkové soustavě a chytře využijí jejich XOR. Pro jiná n kódování nevyjde kvůli dělitelnosti.

17. Díky nutnosti jednoznačného kódování odhadněte $n \geq 101$. Pro 101 si hrajte se součtem sudých a součtem lichých pozic modulo 10.

18. V jednom případě si vyrobte karty, které znáte. V druhém případě to zvolte tak, aby to nevyšlo.

19. Je třeba z každé pětice písní odebrat jednu tak, abychom každou čtveřici dostali 24krát. Z každé pětice seřazených písní odeberte tolikátou, jaký dává jejich součet zbytek modulo 5.

20. Uvažte orientovaný graf, jehož vrcholy jsou $(k-1)$-tice nul a jedniček a hrany odpovídají jejich překrývání na $(k-2)$ následujících pozicích. Všimněte si, že vyrobený graf je eulerovský.

21. Vyberte ta slova, jejichž součet písmen je stejný modulo k.

22. Dvě otázky stačí – nejdřív se zeptáme na $p(1)$ a posléze na hodnotu v tak obrovském čísle k, abychom měli k dispozici jednoznačný zápis v soustavě o základu k.

23. Vyzradí součet své ruky modulo 7, což stále neurčuje pozici žádné z karet.

24. Vězni si mezi sebou zvolí počtáře, kterému předají zprávu o svém výslechu rozsvícením zhasnuté žárovky.

25. Každý vězeň pošle $2k+1$ rozsvícení počtáři, který nahlásí úspěch po $100(2k+1)-k$ spočtených žárovkách.

26. Z každé skupinky posloupností, které se od nějakého indexu shodují, se prasátka (vybavená axiomem výběru) domluví na jednom reprezentantovi.

27. Vyřešte si to nejdřív pro dva.

28. Každé posloupnosti přiřaďte nějaký zbytek modulo $n+1$ tak, aby se posloupnosti s konečným počtem rozdílů lišily právě o součet těchto rozdílů.

29. Délka provázků odpovídá lexikografickému uspořádání čísel a, b, c. Choďte ve třírozměrné krychličkové mřížce se souřadnicemi odpovídajícím (a, b, c).

Literatura a zdroje

Tento příspěvek je kopií příspěvku *Kuby Löwita*, kterému bych tímto rád poděkoval za nalezení spousty pěkných úloh a za pomoc při jejich řešení.

[1] Jakub Löwit: *Vězni, domorodci a kouzelníci*, Horní Lysečiny, 2018.

Dokreslovanie

Michal Pecho

Abstrakt. Příspěvek obsahuje přes třicet geometrických úloh, v jejichž řešení se dokreslují body nebo přímky, které v zadání původně nebyly. Úlohy jsou seskupeny podle myšlenek, které dotyčná dokreslení motivují. Na konci příspěvku jsou k úlohám uvedeny návody.

Při řešení geometrických úloh se zpravidla snažíme obrázek zjednodušovat, jak jen je to možné (typicky tím, že úlohu přeformulujeme na ekvivalentní úlohu na méně bodech). Občas ale stojí za to naopak nějaké body nebo přímky dokreslit. Poznat, kdy je k tomu vhodná příležitost, vyžaduje notnou dávku intuice. Ta se ale dá získat :).

Protahujeme čáry

Přímka je přirozenějším geometrickým objektem než úsečka či polopřímka. Pokud tedy narazíme na jednu z posledních dvou jmenovaných, její protažení stojí za zvážení. Obzvláště tehdy, získáme-li tím druhý průsečík s kružnicí. Jindy protahujeme čáry proto, abychom na ně mohli nanést úsečky a tím „narovnat“ lomenou čáru.

Úloha 1. Pětiúhelník $ABCDE$ má všechny vnitřní úhly stejné velikosti. Dokažte, že osa strany AB, osa strany CD a osa úhlu DEA procházejí jedním bodem. (Polsko 2010)

Úloha 2. Ve čtyřúhelníku $ABCD$ platí $|AB| = 2$, $|BC| = \sqrt{2}$, $|CD| = 3$ a $|\sphericalangle ABC| = |\sphericalangle BCD| = 135°$. Určete $|AD|$. (PraSe 31–2j–3)

Úloha 3. Na průměru AB půlkružnice τ jsou dány body X, Y tak, že $|AX| = |BY|$. Rovnoběžné paprsky vedoucí z X a Y zasáhnou τ v P a Q. Dokažte, že hodnota součinu $|XP| \cdot |YQ|$ nezávisí na volbě směru paprsků.

Úloha 4. Je dán pravoúhlý trojúhelník ABC s pravým úhlem u vrcholu C. Označme D patu výšky z bodu C. Nechť X je bod uvnitř úsečky CD. Označme K ten bod na úsečce AX, pro který $|BK| = |BC|$. Podobně označme L ten bod na úsečce BX, pro který $|AL| = |AC|$. Dále nechť M je průsečík úseček AL a BK. Ukažte, že $|MK| = |ML|$. (IMO 2012, 5)

Úloha 5. Je dán trojúhelník ABC. Osy vnitřních úhlů u vrcholů A, B protnou protější strany v bodech P, Q. Platí-li $|\sphericalangle BAC| = 60°$ a $|AB| + |BP| = |AQ| + |QB|$, určete velikosti zbylých vnitřních úhlů v $\triangle ABC$. (IMO 2001, 5)

Poznáváme známou konfiguraci

Často dokreslujeme body tak, aby vznikla známá konfigurace – například trojúhelník s kolmištěm a kružnicí devíti bodů nebo třeba trojúhelník se Švrčkovými body[1] či připisišti. Nezřídka se totiž úloha jen snaží maskovat známé tvrzení ze známého obrázku.

Úloha 6. Uvnitř trojúhelníka ABC je dán bod P tak, že platí $|\sphericalangle ABP| = 30°$, $|\sphericalangle PBC| = 40°$, $|\sphericalangle BCP| = 20°$ a $|\sphericalangle PCA| = 30°$. Ukažte, že $AP \perp BC$.
(PraSe 32–4j–4a)

Úloha 7. V rovině jsou dány body A, B, C, D tak, že platí $|\sphericalangle ACB| = 20°$, $|\sphericalangle ADB| = |\sphericalangle ABC| = 40°$ a $|\sphericalangle ADC| = 80°$. Určete $|\sphericalangle ABD|$. (KMS 2008)

Úloha 8. Čtyřúhelník $ABCD$ je vepsán do půlkružnice s průměrem AB. Tečny k půlkružnici vedené body C, D se protnou v E a úhlopříčky AC, BD v bodě F. Označme M průsečík EF a AB. Dokažte, že body E, C, M, D leží na jedné kružnici.
(China West 2010)

Úloha 9. V tětivovém čtyřúhelníku $ABCD$ označme I, J postupně vepsiště trojúhelníků ABD, ABC. Dále označme K průsečík kolmic vedených z bodů I, J po řadě na přímky BD, AC. Dokažte, že trojúhelník IJK je rovnoramenný.
(MO 56–A–III–2)

Úloha 10. V ostroúhlém různostranném trojúhelníku ABC označme P patu A-výšky, H kolmiště, O opsiště, D průsečík AO a BC a konečně M střed úsečky AD. Dokažte, že přímka PM prochází středem úsečky OH. (MO 60–A–III–5)

Úloha 11. V trojúhelníku ABC označme M střed strany BC, I vepsiště a N střed toho oblouku BC kružnice opsané, který obsahuje bod A. Dokažte, že $|\sphericalangle INA| = |\sphericalangle IMB|$. (ARO 2005)

Středy a body v poměru

Samostatnou přednášku by zasloužilo zacházení se středy úseček. Obecně lze říci, že máme-li v obrázku středy alespoň dva, snažíme se dokreslit další, abychom využili vlastností středních příček. Je-li přítomen střed jeden, můžeme s výhodou použít středovou souměrnost (dokreslit rovnoběžník). Na závěr ještě zmiňme, že ačkoliv středy obecně nemají dobré úhlové vlastnosti, středy přepon pravoúhlých trojúhelníků jsou (jakožto středy opsaných kružnic) „úhlově“ příjemné.

Úloha 12. Ve čtyřúhelníku $ABCD$ svírá spojnice středů stran BC a AD stejné úhly s oběma úhlopříčkami. Dokažte, že tyto úhlopříčky jsou stejně dlouhé.
(ARO 1990)

[1] Je-li ABC trojúhelník, pak *Švrčkovým bodem* vzhledem k vrcholu A myslíme střed oblouku BC, na kterém neleží A.

Úloha 13. Mějme trojúhelník ABC, na jeho těžnici AM je dán bod K tak, že $|CK| = |AB|$. Označme L průsečík přímek CK a AB. Dokažte, že trojúhelník AKL je rovnoramenný.

Úloha 14. Je dán trojúhelník ABC vepsaný do kružnice k. Tečna k vedená bodem A protne přímku BC v bodě P. Označme M střed AP a Q druhý průsečík MB a k. Ukažte, že $|\sphericalangle PQA| = |\sphericalangle AQC|$. (Alex Zhai)

Úloha 15. Na straně BC ostroúhlého trojúhelníka ABC s kolmištěm H je dán bod D. Kolmice na DH vedená bodem H protne strany AB, AC v bodech F, E. Dokažte, že $\frac{|BD|}{|DC|} = \frac{|FH|}{|HE|}$. (Polsko)

Úloha 16. Na stranách BC, CA, AB trojúhelníka ABC jsou dány body P, Q, R tak, že $\frac{|BP|}{|PC|} = \frac{|CQ|}{|QA|} = \frac{|AR|}{|RB|}$. Navíc platí $|\sphericalangle ABC| = |\sphericalangle PRQ|$. Dokažte, že trojúhelníky ABC a PRQ jsou podobné. (ARO 1989)

Úloha 17. Úhlopříčky tětivového čtyřúhelníka $ABCD$ se protínají v bodě P. Označme K, L paty kolmic z P na AB, CD a dále buď M střed strany AD. Dokažte, že $|MK| = |ML|$. (USA TST 2000)

Stříhání a přelepování

Dokreslování hojně využíváme tehdy, je-li obrázek svázaný nezvyklými podmínkami. V takovém případě se ho snažíme přeorganizovat tak, aby podmínky začaly dávat lepší geometrický smysl.

Úloha 18. V konvexním čtyřúhelníku $ABCD$ platí $|\sphericalangle ADB| + |\sphericalangle ACB| = 90°$ a $|\sphericalangle DBC| + 2 \cdot |\sphericalangle DBA| = 180°$. Navíc $|AD| = 6$ a $|DB| + |BC| = 10$. Určete $|AC|$. (PraSe 26–6–7)

Úloha 19. V obdélníku $ABCD$ jsou dány body E, F tak, že $EF \parallel AB$, $AE \parallel FC$ a AE protíná stranu CD. Navíc $|AB| = 9$, $|BC| = 8$, $|AE| = 4$ a $|FC| = 6$. Určete $|EF|$. (AIME 2011)

Úloha 20. Uvnitř úhlu BAC je dán bod P. Na ramenech AB, AC najdeme body X, Y tak, aby $|AX| = |AY|$ a délka lomené čáry XPY byla nejkratší možná. Dokažte, že $|\sphericalangle APX| = |\sphericalangle APY|$. (Polsko 2008)

Úloha 21. V rovnoběžníku $ABCD$ je dán bod P tak, že $|\sphericalangle APB| + |\sphericalangle CPD| = 180°$. Dokažte, že $|\sphericalangle ABP| = |\sphericalangle ADP|$. (ruský folklór)

Úloha 22. Na stranách AB, AC trojúhelníka ABC s opsištěm O jsou dány body M, N tak, že $|\sphericalangle MON| = \alpha$. Dokažte, že obvod trojúhelníka MAN není menší než $|BC|$. (ARO 2002)

Úloha 23. Bod M uvnitř konvexního čtyřúhelníka $ABCD$ splňuje $|MA| = |MC|$, $|\sphericalangle AMB| = |\sphericalangle MAD| + |\sphericalangle MCD|$ a $|\sphericalangle CMD| = |\sphericalangle MCB| + |\sphericalangle MAB|$. Dokažte, že $|AB| \cdot |CM| = |BC| \cdot |MD|$ a $|BM| \cdot |AD| = |MA| \cdot |CD|$.

(IMO shortlist 1999, G7)

Magie

Ať se nám to líbí, či ne, je potřeba se smířit s tím, že stále budou existovat úlohy, které tak úplně nespadají do žádné z výše uvedených kategorií. Pak je potřeba vhodné dokreslení prostě vymyslet :). Nebojte se experimentovat!

Úloha 24. Je dán konvexní šestiúhelník $ABCDEF$ splňující $|AB| = |BC|$, $|CD| = |DE|$ a $|EF| = |FA|$. Dokažte, že osy úhlů ABC, CDE a EFA procházejí jedním bodem.

Úloha 25. V rovnoramenném trojúhelníku ABC se základnou BC označme M střed těžnice AD a P patu kolmice z D na BM. Dokažte, že $|\sphericalangle APC| = 90°$.
(Rumunsko 2006)

Úloha 26. Body X, Y, Z jsou dány na výškách AD, BE, CF trojúhelníka ABC tak, že $[ABZ] + [BCX] + [CAY] = [ABC]$ (kde symbolem $[PQR]$ značíme obsah trojúhelníka PQR). Označme H kolmiště trojúhelníka ABC. Dokažte, že body X, Y, Z, H leží na jedné kružnici.

Úloha 27. Je dán ostroúhlý trojúhelník ABC vepsaný do kružnice k se středem O. Ať AA' je její průměr. Tečna ke k vedená bodem A' protne přímku BC v bodě P. Přímka PO vytne na trojúhelníku ABC úsečku. Dokažte, že O je jejím středem.
(Výběrko 2007)

Úloha 28. Je dán čtyřúhelník $ABCD$ splňující $a + c = b + d$. Nad všemi jeho stranami jako nad průměry jsou sestrojeny kružnice. Dokažte, že existuje kružnice, která se jich všech dotýká. (Polsko 2013)

Úloha 29. Je dán konvexní čtyřúhelník $PIVO$. Osy stran PI a VO se protínají v bodě Y. Bod X uvnitř $PIVO$ splňuje

$$|\sphericalangle XVI| = |\sphericalangle XOP| < 90° \qquad \text{a} \qquad |\sphericalangle XIV| = |\sphericalangle XPO| < 90°.$$

Ukažte, že $|\sphericalangle VYO| = 2 \cdot |\sphericalangle XIV|$. (IMO shortlist 2000, G6)

Úloha 30. Kružnice vepsaná trojúhelníku ABC se dotýká jeho stran AB, AC v bodech Z, Y. Zkonstruujme body R, S tak, aby $BCYR$ a $BCSZ$ byly rovnoběžníky, a označme G průsečík přímek BY a CZ. Dokažte $|GR| = |GS|$.
(IMO shortlist 2009, G3)

Úloha 31. (Brianchonova věta) Lze-li šestiúhelníku $ABCDEF$ vepsat kružnici, pak úhlopříčky AD, BE, CF procházejí jedním bodem.

Návody

1. V rovnoramenném trojúhelníku splývá osa strany s osou úhlu.
2. Je to pravoúhlý trojúhelník s ustřiženým rohem.
3. Dokresli druhou polovinu obrázku a využij středové souměrnosti.

4. Nakresli vhodné kružnice se středy A, B, protni je podruhé, protáhni úsečky a najdi tětivový čtyřúhelník.

5. „Narovnej“ lomené čáry na přímky AB, AC. Poúhli a dokaž, že jelikož P není A-připisiště v $\triangle ABQ$, musí být $|QB| = |QT|$.

6. Poznej kolmiště.

7. Dokaž, že bod D je opsiště $\triangle ABC$.

8. Protáhni ramena a poznej obrázek s kolmištěm a kružnicí devíti bodů.

9. Dokresli Švrčkův bod (střed oblouku AB kružnice opsané čtyřúhelníku $ABCD$).

10. Obraz H podle strany BC padne na kružnici opsanou.

11. Dokresli B- a C-připisiště a uvědom si, že N je jejich středem.

12. Dokresli střed AB.

13. „Navaž“ na sebe shodné úsečky dokreslením rovnoběžníka $BKCX$.

14. Dokresli současně rovnoběžník $PBAX$ a tětivový čtyřúhelník $PQAX$.

15. Na polopřímku BH nanes X, aby $\frac{|BH|}{|HX|} = \frac{|BD|}{|DC|}$, a odhal kolmiště.

16. Dokresli průsečík BC a rovnoběžky s AB procházející bodem Q.

17. Středy PA a PD, jakožto středy přepon pravoúhlých trojúhelníků, vůbec nejsou špatné body.

18. Obrázek vznikl přehnutím podle AB (proto v něm není CD). Narovnej ho.

19. Vystřihni pásek skrz E a F.

20. Rozstřihni $AXPY$ podle AP a přelep.

21. Přelep $\triangle ABP$ na $\triangle DCX$, aby vznikl tětivový čtyřúhelník.

22. Využij toho, že $|OA| = |OB| = |OC|$, a přerovnej obvod $\triangle MAN$ do lomené čáry s konci B a C.

23. Rozstříhej $ABCD$ podle M na 4 trojúhelníky a přeskládej je (po případném nafukování) na rovnoběžník.

24. Dokresli trojúhelník ACE.

25. Dokresli obdélník $ADMX$.

26. Veď body X, Y, Z rovnoběžky s příslušnými stranami.

27. Ať M je střed BC.

28. Střed úhlopříčky!

29. Na osu strany VO dokresli body K, L tak, aby $\triangle VKL \sim \triangle VXI$ a $\triangle OKL \sim \triangle OXP$. Vyjde $|LP| = |LI|$.

30. Dokaž, že B a Y leží na chordále R a A-připsané.

31. Dokresli tři kružnice tak, aby úhlopříčky AD, BE, CF byly jejich chordálami.

Literatura

Tento příspěvek je téměř kopií stejnojmenného příspěvku od *Josefa Tkadlece*, jemuž tímto děkuji.

[1] Josef Tkadlec: *Dokreslování*, Horní Lysečiny, 2013.
[2] T. Andreescu, M. Rolínek, J. Tkadlec: *107 Geometry Problems*, XYZ Press, 2013.
[3] Archivy olympiád na *https://artofproblemsolving.com/community*.

Kolineácia

Michal Pecho

Abstrakt. Ukážeme si, ako mať na geometriu ten pravý uhol pohľadu. Budeme môcť BUNV predpokladať napríklad, že sú nejaké priamky rovnobežné, alebo že všeobecná tetiva je priemerom kružnice. A hlavne si ukážeme, ako spraviť z koňa žirafu.

Afinné zobrazenia

Afinné zobrazenia pre nás budú všetky zobrazenia spĺňajúce:

(i) Každá priamka sa zobrazí na priamku.
(ii) Na každej priamke sa zachová pomer vzdialeností. Takže kedykoľvek A, B, C ležia na priamke, tak $\frac{|AB|}{|AC|} = \frac{|A'B'|}{|A'C'|}$.
(iii) Rovnobežné priamky zobrazí na rovnobežné priamky.

Cvičenie.

(i) Rozmysli si, že zloženie dvoch afinných zobrazení je zobrazením afinným.
(ii) Rozmysli si, že inverzné zobrazenie k afinnému zobrazeniu je afinné.

Niektoré afinné zobrazenia už určite poznáte, pretože všetky zhodné zobrazenia sú afinné. My si však predvedieme i dve afinné zobrazenia, ktoré zhodné nie sú.

Zmačknutie: Vyberme si bod X mimo priamky p. Na kolmici na p prechádzajúcej bodom X zvolíme obraz X' taký, že neleží na p. Pomocou vlastností, ktoré sa musia zachovať, skonštruujeme obrazy všetkých bodov v rovine.

Skosenie: Vyberme si bod X mimo priamku p. Na rovnobežke s p prechádzajúcej bodom X zvolíme X'. Opäť sa pokúsime skonštruovať obrazy všetkých ostatných bodov roviny.

Všeobecné afinné zobrazenie zachováva:

(i) priamky,
(ii) rovnobežnosť,
(iii) pomery na priamkach,
(iv) pomery obsahov,
(v) elipsy. Dokonca existuje pre každú elipsu afinné zobrazenie, ktoré ju zobrazí na kružnicu.

A nezachováva:

(i) kružnice,
(ii) vzdialenosti,
(iii) uhly.

Príklad. (Blanchet[1]) V trojuholníku ABC označme D pätu výšky z vrcholu A. Na stranách AC a AB sú postupne body E, F také, že priamky BE a CF sa pretínajú na AD. Dokáž, že $|\sphericalangle EDA| = |\sphericalangle FDA|$.

Perspektíva a kolineácia

Definícia. Majme klasickú rovinu. Pre každý smer priamky pridáme bod v nekonečne. Rovinu rozšírenú o tieto body nazývame *projektívna rovina*.

Projektívna rovina bude pre nás zaujímavá, pretože všetkým rovnobežkám budeme vedieť určiť bod v „nekonečne“, v ktorom sa tieto rovnobežky pretnú.

Definícia. Majme priestor s počiatkom P, v ktorom sú umiestnené dve projektívne roviny ρ_1, ρ_2 neprechádzajúce počiatkom P. Nech X je ľubovoľný bod roviny ρ_1, potom *premietaním* z roviny ρ_1 na rovinu ρ_2 rozumieme zobrazenie, ktoré zobrazí bod X na taký bod X' roviny ρ_2, že body P, X, X' ležia na priamke.

Definícia. Majme priestor s počiatkom P v ktorom je umiestnená projektívna rovina ρ neprechádzajúca počiatkom P. Potom *perspektívou* rozumieme zloženie otočenia roviny ρ a následným premietnutím tejto otočenej roviny na pôvodnú rovinu.

Často sa hodí afinné zobrazenia a perspektívu medzi sebou rôzne skladať. Aby sme nemuseli vždy písať, aké všetky zobrazenia skladáme, bude pre nás *kolineácia* univerzálnym zobrazením, do ktorého spadajú všetky zloženia afinných a perspektívnych zobrazení.

Príklad. (Desargues) Majme v rovine dva trojuholníky ABC a $A'B'C'$. Označme priesečníky $X = BC \cap B'C'$, $Y = CA \cap C'A'$ a $Z = AB \cap A'B'$. Potom ak X, Y, Z ležia na jednej priamke, tak priamky AA', BB', CC' prechádzajú jedným bodom.

Majme kružnicu ω a priamku p mimo ňu.

(i) Označme q kolmicu na p prechádzajúcu stredom ω. Potom táto konfigurácia je podľa q symetrická. Pokiaľ zobrazíme p do nekonečna a ω zachovávame, výsledok bude podľa q' tiež symetrický. Pre dôkaz si rozlož perspektívu na otočenie v priestore a projekciu, a uvedom si, že symetria podľa q je zachovaná.

(ii) Na všeobecnej rovnobežke s p rôznej od p majme dané body A, B, C. Potom perspektíva, ktorá zobrazí p do nekonečna, zachová pomer $\frac{|AB|}{|BC|}$. Pre dôkaz znovu rozlož na otočenie v priestore a projekciu, a uvedom si, že na rovnobežkách s p sa projekcia chová ako rovnoľahlosť, a teda zachováva pomery.

Príklad. (butterfly) Majme kružnicu ω a na nej tetivu AB so stredom M. Na ω zvoľme body K_1, L_1. Označme K_2 priesečník K_1M s ω rôzny od K_1. Obdobne definujeme bod L_2. Nech $X = K_1L_1 \cap AB$ a $Y = K_2L_2 \cap AB$. Potom $|XM| = |YM|$.

[1] Čítaj [Blančet].

Cvičenie. Rozmyslite si, že pre body A, B, C, D vo všeobecnej polohe a body A', B', C', D' vo všeobecnej polohe existuje kolineácia, ktorá zobrazuje $A \to A'$, $B \to B'$, $C \to C'$, $D \to D'$.

Cvičenie. Majme trojuholník ABC s kružnicou vpísanou ω a trojuholník $A'B'C'$ s kružnicou vpísanou ω'. Pak existuje kolineácia, ktorá zobrazuje $A \to A'$, $B \to B'$, $C \to C'$ a $\omega \to \omega'$.

Úlohy

Úloha 1. Majme body P, A, B na priamke v tomto poradí. Označme p kolmicu na túto priamku vedenú bodom A. Ďalej majme dotyčnicu PX ku kružnici nad priemerom AB, kde X je bod dotyku (dotyčnice sú dve, uvažujme ľubovoľnú z nich). Označme Y ako priesečník BX a p. Dokáž, že PX rozpoľuje AY.

Úloha 2. Majme rovnoramenný trojuholník ABC ($|AB| = |AC|$). Na jeho ramene AB zvolíme bod X. Rovnobežka s BC vedená bodom X pretne AC v Y. Označme S stred XY a M stred BC. Nech P je priesečník MX a CS. Dokáž, že trojuholník PMC má polovičný obsah v porovnaní s ABC.

Úloha 3. Majme trojuholník ABC. Označme M stred strany BC. Priesečník dotyčníc ku kružnici opísanej trojuholníku ABC vedených bodmi B a C označme P. Dokážte, že platí $|\sphericalangle BAP| = |\sphericalangle CAM|$.

Úloha 4. Majme dotyčnicový štvoruholník $ABCD$. Označme body dotyku kružnice vpísanej ku stranám AB, BC, CD, DA postupne W, X, Y, Z. Dokáž, že priamky AC, WX, YZ prechádzajú jedným bodom.

Úloha 5. (těžší) Majme trojuholník ABC s kružnicou vpísanou ω. Označme D bod dotyku kružnice pripísanej k strane BC. Na priamke AD zvoľme bod X tak, aby úsečka XD neobsahovala žiadny bod ω. Dotyčnice z X k ω pretnú stranu BC v bodoch K, L. Dokáž, že $|BK| = |CL|$. (*i*KSko 2018/19)

Úloha 6. Majme danú polkružnicu nad priemerom UV. Na tejto polkružnici zvolíme body P, Q. Priesečník dotyčníc z P a Q označme R. Priesečník UP a VQ označíme S. Dokáž, že $SR \perp UV$.

Úloha 7. V trojuholníku ABC označme body dotyku kružnice vpísanej so stranami BC, CA, AB postupne D, E, F. Na úsečke AD vo vnútri kružnici vpísanej zvoľme bod L. Úsečky BL a CL pretnú kružnicu vpísanú postupne v bodoch X, Y. Dokáž, že priamky EF, BC, XY prechádzajú jedným bodom.

Úloha 8. Bod M je stredom strany AB trojuholníka ABC. Na polpriamke opačnej k MC zvoľme bod N a vo vnútri úsečky AM zvoľme bod P. Označíme Q priesečník priamok AC a NP, ďalej R priesečník QM a NB, a nakoniec S priesečník AB a RC. Dokáž $|PM| = |SM|$.

Úloha 9. Majme trojuholník ABC. Označme A' bod dotyku kružnice vpísanej so stranou BC. Druhý priesečník priamky AA' s kružnicou vpísanou označme P. Priesečníky BP a CP s kružnicou vpísanou označme postupne M, N. Dokáž, že BN, MC, AA' prechádzajú jedným bodom.

Úloha 10. V trojuholníku ABC označme M stred BC. Priamka AM pretína kružnicu vpísanú v bodoch P, Q. Rovnobežky s BC prechádzajúce bodmi P, resp. Q pretínajú kružnicu vpísanu znova v X, resp. Y. Priamky AX, AY pretínajú BC v K, L. Dokáž, že $|BK| = |CL|$.

Úloha 11. Majme pevnú úsečku AC a na nej bod B. Cez body A, C veďme kružnicu ω. Dotyčnice k ω v bodoch A a C sa pretínajú v P. Úsečka PB pretne kružnicu druhýkrát v Q (B leží na úsečke PQ), os uhlu AQC pretne AC v R. Dokáž, že pomer $\frac{|AR|}{|RC|}$ nezávisí na voľbe kružnice ω. (IMO Shortlist 2003/G2)

Úloha 12. Majme štvoruholník $ABCD$ taký, že $|\sphericalangle ABD| = |\sphericalangle ACD| = 90°$. Bod P leží na BD tak, že $|\sphericalangle PAD| = 90°$ a podobne Q leží na AC tak, že $|\sphericalangle QDA| = 90°$. AC a BD sa pretínajú v bode X a PC a BQ sa pretínajú v Y. Ukáž, že XY je kolmá na AD.

Návody

1. Zobraz P na nevlastný tak, aby sa zachoval pomer na priamke AY a kružnica.

2. Dokáž, že $PA \parallel BC$. Zobraz rovnobežku s BC prechádzajúcu bodom A na nevlastnú a ukáž, že potom je P tiež nevlastný.

3. Premietnutím na kružnicu preveď tvrdenie na rovnobežnosť.

4. Zobraz tak, aby sa zachovala kružnica a získal si z $ABCD$ kosoštvorec.

5. Nech I je stredom ω a E bod dotyku ω so stranou BC. Zobraz EI a KL na rovnobežky a zachovaj pomery a kružnicu.

6. Zobraz PQ a UV na rovnobežky a zachovaj kružnicu. Rozmysli si, že pravý uhol medzi RS a UV sa zachová, pretože se zachováva symetria podľa UV.

7. Označ K priesečník $CB \cap EF$. Zobraz priamku AK na nevlastnú.

8. Zobraz C na nevlastný a zachovaj pomery. Následne zrovnaj afinným zobrazením.

9. Pošli A na nevlastný.

10. Zachovaj kružnicu a zobraz A na nevlastný.

11. Ukáž, že vieš všetky povolené konštrukcie na seba previesť nejakou kolineáciou.

12. Dokresli Tálesovu kružnicu nad AD. Zobraz BC a AD na rovnobežky a zachovaj túto kružnicu.

Literatura a zdroje

[1] Radek Olšák, Lenka Kopfová: *Projektivní geometrie*, PraSečí seriál, 39. ročník, *https://prase.cz/archive/39/serial.pdf*.

Axiomatická geometrie

Daniel Perout

Abstrakt. Přednáška se věnuje axiomatizaci eukleidovské geometrie, což je součást syntetické planimetrie. V běžné školské matematice se začne od několika základních postulátů, která se zdají intuitivní, a na nich se synteticky buduje geometrie. Moderní matematika však pracuje s axiomy, což jsou jednoduchá (ne nutně intuitivní) tvrzení, na něž klademe určité nároky, jež považujeme za platné a na nichž budujeme konzistentní systémy. Příspěvek představuje Tarského axiomy rovinné eukleidovské geometerie a buduje některá základní tvrzení planimetrie. Věty jsou zamýšlené jako úlohy, čtenáři je doporučeno si věty dokázat s pomocí návodů na konci příspěvku.

„Výlučnou náplní čisté matematiky jsou tvrzení v tom smyslu, že pokud platí jistý výrok týkající se jakéhokoli objektu, potom o tomto objektu platí i nějaký jiný výrok. Je důležité neptat se, zda první výrok opravdu platí, a nezmiňovat se, co je oním objektem, o kterém příslušné výroky vypovídají. (...) Matematiku bychom vlastně mohli definovat jako nauku, v níž nikdy nevíme, o čem mluvíme, ani zda to, co říkáme, je pravda.“ – Bertrand Russell

„Nevím, jak mám s vašimi definicemi zodpovědět otázku, zda jsou moje kapesní hodinky bodem.“ – Gottlob Frege v reakci na axiomatizaci geometrie od Davida Hilberta

O Tarského axiomatizaci

Budeme pracovat v prvořádové logice[1] v jazyce $\{\simeq, \overline{\cdot}:\overline{\cdot}\}$, kde $\simeq$ je kvaternární relace *ekvidistance* (popř. *shodnosti*) a $\overline{\cdot}:\overline{\cdot}$ je ternární relace *mezitosti*. Ekvidistanci intuitivně chápeme jako tvrzení, že dva body na levé straně jsou od sebe stejně daleko jako dva body na druhé straně relace. Mezitost jako tvrzení, že prostřední bod leží na přímce mezi ostatními, přitom připouštíme, aby body splývaly.

V tomto systému budeme postupně postulovat axiomy, z nichž budeme odvozovat základní geometrická tvrzení.

Od ekvidistance k délkám úseček

Podívejme se na první čtyři axiomy, které postulují základní vlastnosti relace $\simeq$:

($\mathcal{G}1$) $\forall a, b\ (ab \simeq ba)$,
($\mathcal{G}2$) $\forall a, b, p, q, r, s\ (ab \simeq pq \wedge ab \simeq rs \to pq \simeq rs)$,
($\mathcal{G}3$) $\forall a, b, c\ (ab \simeq cc \to a = b)$,
($\mathcal{G}4$) $\forall a, b, c, q\ \exists x\ (\overline{q}\dot{a}\overline{x} \wedge ax \simeq bc)$.

Pracovat s ekvidistancí jako s kvaternární relací bodů může být nešikovné, daleko vhodnější je ji vnímat jako binární relaci mezi (neuspořádanými) dvojicemi bodů = úsečkami.

[1] Tj. můžeme používat pouze logické spojky ($\neg$, $\wedge$, $\vee$, $\to$, $\leftrightarrow$), proměnné, přes které můžeme kvantifikovat jen *provšechnítkem* $\forall$ a *existítkem* $\exists$, a mimologické symboly daného jazyka.

Definice. (úsečka) Pro body a, b definujeme *úsečku* ab jako neuspořádanou dvojici $\{a, b\}$. Úsečku aa nazýváme *nulovou úsečkou*, pokud $a \neq b$, pak ab nazveme *vlastní úsečkou*.

Definice. (ekvivalence) Je-li relace E na množině A

- reflexivní, • symetrická, • tranzitivní,

pak ji nazveme *ekvivalencí*.

Definice. (rozklad) Pokud $A \subseteq \mathcal{P}(X)$ je systém podmnožin množiny X, který splňuje

- $\emptyset \notin A$, • $\forall x \in X\ \exists a \in A\ x \in a$, • $\forall a, b \in A\ (a \cap b \neq \emptyset \to a = b)$,

pak A nazveme *rozkladem* množiny X a každé $a \in A$ *třídami rozkladu* X.

Tvrzení 1. *Každá ekvivalence je ztotožnitelná s nějakým rozkladem a každý rozklad je ztotožnitelný s nějakou ekvivalencí, tj. mezi ekvivelancemi a rozklady na nějaké množině je vzájemně jednoznačná korespondence.*

Věta 2. (ekvidistance je ekvivalence nad úsečkami) *Ať a, b, c, d, e, f jsou body, pak platí*

(i) $ab \simeq ab$,
(ii) $ab \simeq cd \to cd \simeq ab$,
(iii) $ab \simeq cd \wedge cd \simeq ef \to ab \simeq ef$,
(iv) $ab \simeq cd \leftrightarrow ba \simeq cd$.

Věta 3. (nulové úsečky jsou ekvidistantní) *Ať jsou a, b body, pak $aa \simeq bb$.*

Ekvidistanci můžeme použít k definování shodnosti obrazců, které jsou tvořené konečně mnoha body, a to tak, že odpovídající si dvojice bodů mají stejnou vzdálenost.

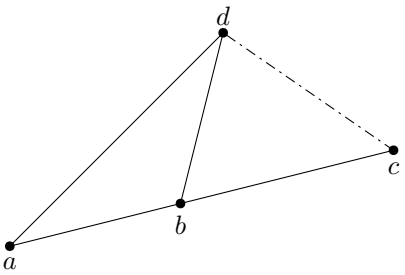
Definice. $(a_1 a_2 \dots a_n) \simeq (b_1 b_2 \dots b_n) \ :\leftrightarrow \bigwedge_{1 \leq i < j \leq n} a_i a_j \simeq b_i b_j$.

Z dokázaných vlastností ekvidistance uvedené vztahy postačují, abychom mohli odvodit i zbylé ekvidistance. Všimněme si, že pokud provedeme stejnou permutaci na obou n-ticích bodů, nezmění to platnost shodnosti.

Konfigurace pěti úseček a její využití

V této sekci se budeme zabývat pátým axiomem $\mathcal{G}5$, také zvaným *axiom pěti úseček*.

($\mathcal{G}5$) $\forall a, b, c, d, a', b', c', d'$
$(a \neq b \wedge \overline{abc} \wedge \overline{a'b'c'} \wedge ab \simeq a'b' \wedge bc \simeq b'c' \wedge ad \simeq a'd' \wedge bd \simeq b'd' \to cd \simeq c'd')$.



Abychom mohli používat axiom $\mathcal{G}5$ efektivněji, zavedeme následující značení.

Definice. (vnější konfigurace pěti úseček) Ať a, b, c, d, a', b', c', d' jsou body. Pak definujeme

$$\lambda \begin{pmatrix} a & b & c & d \\ a' & b' & c' & d' \end{pmatrix} :\leftrightarrow \quad \overline{a}\dot{b}\overline{c} \wedge \overline{a'}\dot{b'}\overline{c'} \wedge ab \simeq a'b' \wedge bc \simeq b'c' \wedge ad \simeq a'd' \wedge bd \simeq b'd'.$$

Zřejmě potom z axiomu $\mathcal{G}5$ platí, že $a \neq b \wedge \lambda \begin{pmatrix} a & b & c & d \\ a' & b' & c' & d' \end{pmatrix} \to cd \simeq c'd'$.

Věta 4. (o skládání úseček) *Ať a, b, c, a', b', c' jsou body a platí $\overline{a}\dot{b}\overline{c}$, $\overline{a'}\dot{b'}\overline{c'}$, $ab \simeq a'b'$ a $bc \simeq b'c'$. Pak platí $ac \simeq a'c'$.*

S pomocí axiomu $\mathcal{G}5$ můžeme vylepšit konstrukční axiom $\mathcal{G}4$ tak, že na dané polopřímce q, a je takový bod právě jeden.

Věta 5. (o jednoznačnosti přenášení vzdáleností) *Ať a, q jsou různé body a b, c jsou body. Pak existuje právě jeden bod x, tž. $\overline{q}\dot{a}\overline{x}$ a $ax \simeq bc$.*

Mezitost

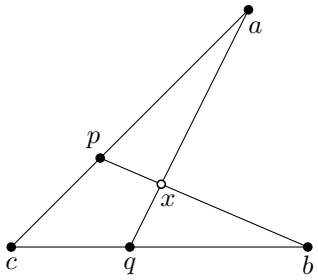
O vlastnostech mezitosti nám vypovídají další dva axiomy:

($\mathcal{G}6$) $\forall a, b\ (\overline{a}\dot{b}\overline{a} \to a = b)$,

($\mathcal{G}7$) $\forall a, b, c, p, q\ (\overline{a}\dot{p}\overline{c} \wedge \overline{b}\dot{q}\overline{c} \to \exists x\ (\overline{p}\dot{x}\overline{b} \wedge \overline{q}\dot{x}\overline{a}))$. (*Paschův axiom*[2])

Mezitost bychom chtěli interpretovat jako relaci úsečky a bodu, kde tento bod leží mezi krajními body oné úsečky, takže pro danou úsečku by všechny body ležící mezi jejími krajními body měly být jejími vnitřními body. Axiom $\mathcal{G}6$ nám říká, že speciálně pro nulovou úsečku jsou všechny její vnitřní body shodné s krajním bodem.

[2]Obeznámený čtenář si všimne, že toto není původní (tzv. *vnitřní*) formulace Paschova axiomu (tj. že přímka procházející stranou trojúhelníka mimo jeho vrchol musí tento trojúhelník protnout i v jedné z jeho dalších stran). Jde o tzv. *vnější formu*, z níž se dá za pomocí ostatních axiomů odvodit i vnitřní formu.



Axiom $\mathcal{G}7$, také zvaný *Paschův axiom* (resp. jde o jeho vnější formu), nám za jistých podmínek dovoluje konstruovat průsečíky úseček. Bod c můžeme tady chápat jako svědka, že přímky ap a bq nám vytyčují rovinu[3].

Věta 6. *Ať a, b, c jsou body, pak platí*

(i) $\overline{a}\dot{c}\overline{c}$ *(krajní bod úsečky je jejím vnitřním bodem),*
(ii) $\overline{a}\dot{b}\overline{c} \to \overline{c}\dot{b}\overline{a}$ *(symetrie krajních bodů úsečky),*
(iii) $\overline{a}\dot{b}\overline{c} \wedge \overline{b}\dot{a}\overline{c} \to a = b$.

Zaveďme nyní axiom o dimenzi:

($\mathcal{G}8$) $\exists a\, \exists b\, \exists c\, (\neg\, \overline{a}\dot{b}\overline{c} \wedge \neg\, \overline{b}\dot{c}\overline{a} \wedge \neg\, \overline{c}\dot{a}\overline{b})$.

Ve skutečnosti ale tento axiom nepotřebujeme v jeho plné síle, stačí nám následující důsledek.

Důsledek 7. *Existují alespoň dva různé body.*[4]

Díky tomuto důsledku můžeme velice jednoduše dokázat prodlužování přímky (jeden z Eukleidových postulátů).

Věta 8. *Ať a, b jsou body, pak existuje c různé od b splňující $\overline{a}\dot{b}\overline{c}$.*

Uspořádání na přímce

Jak definovat přímku pomocí mezitosti? Pokud máme tři body na přímce, měla by nastat alespoň jedna ze situací $\overline{a}\dot{b}\overline{c}$, $\overline{b}\dot{c}\overline{a}$, $\overline{c}\dot{a}\overline{b}$ (zbylé případy jsou pokryté ze symetrie krajních bodů úsečky). Kolinearitu tak můžeme definovat následovně.

Definice. O bodech a, b, c řekneme, že jsou *kolineární* (neboli *leží na jedné přímce*) pomocí vztahu

$$\mathrm{Col}\, abc \;:\leftrightarrow\; \overline{a}\dot{b}\overline{c} \vee \overline{b}\dot{c}\overline{a} \vee \overline{c}\dot{a}\overline{b}.$$

Cvičení 9. Rozmyslete si, kdy mohou nastat dvě z těchto mezitostí zároveň.

[3]Pamatujme, že zatím formulujeme tvrzení platná nezávisle na dimenzi prostoru.

[4]Všimněme si, že z dosavadních axiomů toto tvrzení nevyplývá – všechny axiomy $\mathcal{G}1$ až $\mathcal{G}7$ by platily, i kdybychom vystavěli geometrii pouze o jednom bodě.

Přímku určenou dvěma body je potom možné definovat jako množinu všech bodů, které jsou s danými dvěma body kolineární. Konkrétní vlastnosti přímek jako kolmosti nebo rovnoběžnosti jsou ale nad rámec této přednášky. Vystačíme si proto s pojmem kolinearity.

Kolinearita nám umožňuje stručněji formulovat některá tvrzení o bodech na jedné přímce. Zatím toho ale o pořadí bodů moc říct neumíme. K tomu nám poslouží následující věty.

Věta 10.

(i) $\overline{a}\dot{b}\overline{d} \wedge \overline{b}\dot{c}\overline{d} \to \overline{a}\dot{b}\overline{c} \wedge \overline{a}\dot{c}\overline{d}$,

(ii) $a \neq b \wedge \overline{a}\dot{b}\overline{c} \wedge \overline{b}\dot{c}\overline{d} \to \overline{a}\dot{c}\overline{d} \wedge \overline{a}\dot{b}\overline{d}$.

Tvrzení 11.

(i) $a \neq b \wedge \overline{a}\dot{b}\overline{c} \wedge \overline{a}\dot{b}\overline{d} \to \overline{a}\dot{c}\overline{d} \vee \overline{a}\dot{d}\overline{c}$,

(ii) $a \neq b \wedge \overline{a}\dot{b}\overline{c} \wedge \overline{a}\dot{b}\overline{d} \to \overline{b}\dot{c}\overline{d} \vee \overline{b}\dot{d}\overline{c}$,

(iii) $\overline{a}\dot{b}\overline{d} \wedge \overline{a}\dot{c}\overline{d} \to \overline{a}\dot{b}\overline{c} \vee \overline{a}\dot{c}\overline{b}$.

Věta 12. *Je-li úsečka ac rozdělena bodem b a jiná úsečka pr má stejnou délku jako ac, pak umíme pr rozdělit bodem q ve stejném poměru jako b dělí ac. Jinými slovy*

$$\overline{a}\dot{b}\overline{c} \wedge ac \simeq pr \to \exists q\ (\overline{p}\dot{q}\overline{r} \wedge (abc) \simeq (pqr)).$$

Věta 13. *Shodnost zachovává mezitost, jinými slovy*

$$\overline{a}\dot{b}\overline{c} \wedge (abc) \simeq (pqr) \to \overline{p}\dot{q}\overline{r}.$$

Předcházející dvě věty nyní zobecníme pro kolinearitu. V druhém případě je odvození triviální (kolinearita vyplývá z mezitosti), v prvním je třeba rozlišit dva případy mezitosti (tj. zda b leží uvnitř nebo vně úsečky ac).

Věta 14. *Ať a, b, c, p, r jsou body.*

(i) *Je-li* $\mathrm{Col}\, abc \wedge ac \simeq pr$, *pak existuje* q, *že* $(\mathrm{Col}\, pqr \wedge (abc) \simeq (pqr))$.

(ii) *Pokud je q bod splňující* $\mathrm{Col}\, abc \wedge (abc) \simeq (pqr)$, *pak* $\mathrm{Col}\, pqr$.

Porovnávání úseček

Definice. Ať ab, cd jsou úsečky, pak *ab je kratší než cd* (zapisujeme $ab \leq cd$), pokud existuje y splňující $\overline{c}\dot{y}\overline{d}$ a $ab \simeq cy$.

Věta 15. (charakterizace kratší úsečky) *Ať ab, cd jsou úsečky, pak platí*

$$ab \leq cd \ \leftrightarrow\ \exists x\ (\overline{a}\dot{b}\overline{x} \wedge ax \simeq cd).$$

Nyní jsme již plně vybavení k důkazu finální věty

Věta 16. *Ať a, b, c, d, a', b', c', d' jsou body. Pak platí*

(i) $ab \leq cd \wedge ab \simeq a'b' \wedge cd \simeq c'd' \to a'b' \leq c'd'$ *(invariance vůči ekvidistanci),*
(ii) $ab \leq ab$ *(reflexivita),*
(iii) $ab \leq cd \wedge cd \leq ef \to ab \leq ef$ *(tranzitivita),*
(iv) $ab \leq cd \wedge cd \leq ab \to ab \simeq cd$,
(v) $ab \leq cd \vee cd \leq ab$ *(každé dvě úsečky jsou porovnatelné),*
(vi) $aa \leq cd$ *(nulová úsečka je minimální),*
(vii) $\operatorname{Col} abc \to (\overline{a}\dot{\overline{bc}} \leftrightarrow ab \leq ac \wedge bc \leq ac)$ *(porovnání jednoznačně určuje pořadí na přímce).*

Návody

2. Klíčové je použít $\mathcal{G}2$; v každém z podtvrzení využij předchozí dokázané podtvrzení (v prvním zkus nějaký axiom).

3. Použij $\mathcal{G}4$ a $\mathcal{G}3$.

4. $\lambda\left(\begin{smallmatrix} a & b & c & a \\ a' & b' & c' & a' \end{smallmatrix}\right)$.

5. $\lambda\left(\begin{smallmatrix} q & a & x & x \\ q & a & x & x' \end{smallmatrix}\right)$.

6. (i) Využij $\mathcal{G}4$ a $\mathcal{G}3$. (ii) Použij $\mathcal{G}7$ na $\overline{a}\dot{\overline{bc}}$ a $\overline{b}\dot{\overline{cc}}$. (iii) Sestroj x, pro které ukážeš $a = x$ i $b = x$.

8. Použij zmíněný důsledek a axiom $\mathcal{G}4$.

10. Dokazuj nejprve levé konjunkty všech implikací a poté pravé konjunkty. Na první konjunkt první implikace použij $\mathcal{G}7$.

12. Dokresli si bod s splňující $\overline{s}\dot{p}\overline{r}$. Přenes vzdálenosti ab a ac od p, druhá vzdálenost by měla splynout s r.

13. Přenes bod b z úsečky ac na pr, dokaž, že tento nový bod a q splývají. Pomož si bodem ležícím mimo pr a dvakrát použij konfiguraci pěti úseček.

15. Máš-li x, resp. y, splňující $\overline{a}\dot{b}\overline{x}$, resp. $\overline{c}\dot{y}\overline{d}$, sestroj y, resp. x, pomocí přenášení vzdáleností.

16. (i) Využij větu o dělení v daném poměru. (ii) Platí $\overline{a}\dot{\overline{bb}}$. (iii) Využij větu o dělení v daném poměru. (iv) Použij chytře definici a charakterizaci kratší vzdálenosti; potom využij jednoznačné přenášení vzdáleností. (v) Vyplývá z Tvrzení 11. (vi) Platí $\overline{a}\dot{a}\overline{x}$. (vii) Uvaž, co by se stalo, kdyby $\overline{a}\dot{\overline{cb}}$.

Literatura a zdroje

[1] Wikipedia [en]: *Tarski's axioms*, *https://en.wikipedia.org/w/index.php?title=Tarski%27s_axioms&oldid=1144443705*.
[2] Wolfram Schwabhäuser, Wanda Szmielew, Alfred Tarski: *Metamathematische Methoden in der Geometrie*, Springer-Verlag, 1983.
[3] Alfred Tarski, Steven Givant: *Tarski's system of geometry*, The Bulletin of Symbolic Logic, 5 (2): s. 175–214.
[4] Zdeněk Halas: *Poznámky k axiomatizaci geometrie*, Pokroky matematiky, fyziky a astronomie, Vol. 63 (2018), No. 1, 51–67, *http://dml.cz/dmlcz/147209*.

Množiny bodů dané vlastnosti

Daniel Perout

Abstrakt. Příspěvek shrnuje základní geometrické množiny bodů a obsahuje řadu převážně snadných úloh, k nimž jsou na konci uvedeny stručné postupy a výsledky.

Věta. *Množina bodů, které mají:*

(i) *danou vzdálenost r od daného bodu S, je kružnice $k(S, r)$.*
(ii) *danou vzdálenost od dané přímky p, je dvojice přímek rovnoběžných s p.*
(iii) *stejnou vzdálenost od dvou daných bodů A, B, je osa úsečky AB.*
(iv) *stejnou vzdálenost od dvou daných přímek p, q, je dvojice přímek, které jsou osami úhlů vytvořenými přímkami p, q.*

Věta. (o obvodovém úhlu) *Množina bodů, z nichž je daná úsečka AB vidět pod daným úhlem φ, je sjednocení dvojice kružnicových oblouků s krajními body A, B, které jsou symetrické podle přímky AB, přičemž toto sjednocení uvažujeme bez krajních bodů A, B. Speciálně pro $\varphi = 90^\circ$ je hledanou množinou kružnice nad průměrem AB bez bodů A, B.*

Lehounké úložky

Úloha 1. Jsou dány rovnoběžné přímky p, q. Najděte množinu středů úseček AB takových, že bod A leží na p a bod B na q.

Úloha 2. Je dána kružnice k a bod O. Určete množinu středů všech úseček OP, kde P probíhá kružnici k.

Úloha 3. Jsou dány body A, B. Najděte všechny přímky p, jejichž vzdálenost od A je stejná jako od B.

Úloha 4. Je dána úsečka AB. Určete množinu obrazů A' bodu A v osové souměrnosti podle libovolné přímky procházející bodem B.

Úloha 5. Uvnitř kružnice k se středem O je dán bod P. Určete množinu středů všech tětiv AB kružnice k, které procházejí bodem P. Co kdyby bod P ležel vně kružnice k?

Úloha 6. Polem vede rovná cesta, po které se rozjel autobus.

(i) Kde musí člověk stát, aby autobus dostihnul, pokud běží stejnou rychlostí, jakou autobus jede?
(ii) Co kdyby člověk vyrážel o minutu dřív?
(iii) Co kdyby byl člověk dvakrát pomalejší?

Úloha 7. Po ramenech VX, VY pravého úhlu XVY se pohybují body A, B tak, že úsečka AB má konstantní délku d. Určete množinu středů M úseček AB.

Úloha 8. Je dána úsečka AB. Uvažme všechny dvojice kružnic k, l, které se dotýkají úsečky AB postupně v bodech A, B a navíc mají samy vnější dotyk v T. Určete množinu bodů T.

Běžné příklady

Úloha 9. Jsou dány kružnice k a l, které se protínají v bodech A a B. Na kružnici k zvolíme bod C a označíme D druhý průsečík přímky BC s l. Určete množinu vepsišť trojúhelníku ACD.

Úloha 10. Na úsečce AC je dán bod B. Určete množinu druhých průsečíků X shodných kružnic, z nichž jedna prochází body A, B a druhá body B, C.

Úloha 11. Osa úhlu ABC protne stranu AC trojúhelníku ABC v bodě D. Najdeme bod E v polorovině určené přímkou BC ve které neleží bod A, tak, aby $|\sphericalangle BCE| = |\sphericalangle BAC|$ a $|CE| = |AD|$. Dokažte, že střed úsečky DE leží na BC.

Úloha 12. Určete množinu středů všech úseček AB, jejichž krajní body leží na dané půlkružnici t.

Úloha 13. Bod C probíhá pevný kružnicový oblouk nad tětivou AB. Určete množinu opsišť, těžišť, ortocenter a vepsišť všech takových trojúhelníků ABC.

Úloha 14. V rovině je dána kružnice k se středem S a bod $A \neq S$. Určete množinu opsišť trojúhelníků ABC, jejichž strana BC je průměrem kružnice k.

(MO 56–A–I–5)

Úloha 15. Je dána kružnice k s tětivou AC, jež není průměrem. Na její tečně vedené bodem A zvolíme bod $X \neq A$ a označíme D průsečík kružnice k s vnitřkem úsečky XC (pokud existuje). Trojúhelník ACD doplníme na lichoběžník $ABCD$ vepsaný kružnici k. Určete množinu průsečíků přímek BC a AD odpovídajících všem takovým lichoběžníkům. (MO 59–A–III–4)

Úloha 16. Je dána kružnice k a na ní tětiva AB, ať C je bod probíhající kružnici k. Označme P patu kolmice vedené středem M strany BC na přímku AC. Určete množinu bodů P.

Úloha 17. Uvnitř trojúhelníka ABC je dán bod O tak, že $|\sphericalangle OBA| = |\sphericalangle OAC|$, $|\sphericalangle BAO| = |\sphericalangle OCB|$ a $|\sphericalangle BOC| = 90°$. Určete poměr $|AC| : |OC|$.

(Moskva 2011)

Úloha 18. V trojúhelníku ABC platí $|\sphericalangle ABC| = 120°$. Označme D, E, F průsečíky os vnitřních úhlů u vrcholů A, B, C s protějšími stranami. Ukažte, že platí $|\sphericalangle DEF| = 90°$.

Návody

1. Nakresli přímky vodorovně. Jak vysoko leží střed? (Vyjde osa pásu určeného přímkami p, q.)

2. Stejnolehlost. (Vyjde „poloviční“ kružnice vzhledem k bodu O.)

3. Konstruuj tečny ke stejně velkým kružnicím se středy v A a B. (Vyjdou rovnoběžky s AB a přímky skrz střed AB.)

4. Ukaž, že $\triangle ABA'$ je rovnoramenný. (Vyjde kružnice o středu B a poloměru $|BA|$.)

5. Tětiva je kolmá na spojnici svého středu se středem kružnice. (Vyjde Thaletova kružnice nad OP, případně její oblouk.)

6. Množina bodů, ze kterých je člověk schopen autobus dostihnout v jistém pevném bodě X, je kruh. Sjednoť tyto kruhy přes všechny přípustné body X. (Vyjde postupně polorovina, posunutá polorovina, úhel o velikosti $60°$.)

7. Vzdálenost středu přepony od vrcholu s pravým úhlem je rovna polovině délky přepony. (Vyjde čtvrtkružnice se středem V a poloměrem $\frac{1}{2}d$.)

8. Ať vnitřní společná tečna v T protne AB v M. Pak $|MA| = |MT| = |MB|$ (stejně dlouhé tečny). (Vyjde kružnice nad průměrem AB bez bodů A, B.)

9. Dokresli švrky M a N trojúhelníků ACB a ADB. (Vyjde kružnice opsaná trojúhelníku MNB.)

10. Úhly $\sphericalangle XAB$ a $\sphericalangle BCX$ jsou obvodové k téže tětivě ze stejně velkých kružnic, takže mají stejnou velikost. (Vyjde osa úsečky AC.)

11. Označme A' obraz A podle osy $\sphericalangle ABC$. Pak jsou $A'D$ a CE stejně dlouhé a svírají týž úhel s BC, tedy D je „nad“ BC přesně o tolik, o kolik je E „pod“.

12. Vyjde vnitřek půlkruhu bez půlkruhů nad průměry určenými koncovými body t a jejím středem.

13. Vyjde po řadě bod, „přitřetěný“ oblouk C ke středu strany AB, oblouk nad AB odpovídající úhlu $180° - \gamma$, oblouk odpovídající úhlu $90° + \frac{\gamma}{2}$ (resp. oblouk posunutý tak, aby procházel A a B).

14. Mocnost S ke všem takovým kružnicím je stejná ($|SB| \cdot |SC|$), takže druhý průsečík kružnice opsané trojúhelníku ABC a AS je pevný. (Vyjde osa úsečky spojující A s tímto pevným bodem.)

15. Dokresli si bod E, průsečík tečen ke k z bodů A, C. Hledanou množinou je sjednocení vnitřků kratších oblouků CE a AE kružnice opsané trojúhelníku EAC.

16. Ukaž, že všechny takové kolmice procházejí středem X tětivy kolmé na AB skrz B. (Vyjde Thaletova kružnice nad AX.)

17. Začni od $\triangle BOC$, nakresli obraz C' bodu C přes OB a ukaž, že A je bod dotyku tečny z C ke kružnici opsané $\triangle BOC'$. Z mocnosti vyjádři hodnotu poměru $\sqrt{2}$.

18. Ukaž, že D a F jsou připsiště trojúhelníků AEB a ECB.

Literatura a zdroje

Chtěl bych poděkovat *Lence Kopfové*, jejíž příspěvek jsem téměř beze změn převzal a jež poděkovala *Štěpánu Šimsovi*, jehož příspěvek téměř beze změn převzala a jenž poděkoval *Pepovi Tkadlecovi*, jehož příspěvek téměř beze změn převzal.

[1] Nathan Altschiller-Court: *An Introduction to the Modern Geometry of the Triangle and the Circle*, Dover Publications, New York, 2007.

[2] V. V. Prasolov: *Zadachi po planimetrii*, MCCME, Moskva, 2006.

[3] *http://www.problems.ru*.

N

Zdeněk Pezlar

Abstrakt. V teorii čísel se často zabýváme zbytky po dělení, hlavně když mocníme. V tomto příspěvku se vydáme na pouť těmito koncepty a uvidíme, jak daleko nás základní fakta dostanou.

Úmluva. Není-li řečeno jinak, pracujme s celými čísly. Pod p rozumíme prvočíslo.

Skutečnost, že $a = bk$, tedy a je násobek b, zapisujeme $b \mid a$ a říkáme „*b dělí a*“. Skutečnost, že $n \mid a - b$, značíme $a \equiv b \pmod{n}$ a říkáme „*a* je *kongruentní s b modulo n*“. Dále toto značení bereme za samozřejmé.

Tvrzení. *Mějme a nesoudělné s n, dále mějme čísla b a c, pak $ab \equiv ac \pmod{n}$ je ekvivalentní $b \equiv c \pmod{n}$.*

Definice. Množinu čísel nazýváme *úplnou sadou zbytků modulo n*, pokud každý zbytek modulo n je kongruentní s alespoň jedním prvkem z dané množiny.

Zase ta prvočísla ...

Tušíme, že bude na prvočísla jako vždy upřena speciální pozornost. Každé číslo, které není prvočíslem p dělitelné, je s p nesoudělné. Už samotný tento fakt má zajímavé důsledky.

Tvrzení. *Platí rovnost množin $\{0, 1, \ldots, p-1\} = \{a \cdot 0, a \cdot 1, \ldots, a \cdot (p-1)\}$ modulo p pro $p \nmid a$.*

Důsledek. (Malá Fermatova věta) *Buď p prvočíslo a a číslo s ním nesoudělné, potom*

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

Důkaz. Z předchozího tvrzení jsou množiny $\{1, \ldots, p-1\} = \{a \cdot 1, \ldots, a \cdot (p-1)\}$ stejné modulo p. Součin prvků obou množin musí být proto stejný modulo p:

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

Jelikož $(p-1)!$ je nesoudělné s p, tak jsme hotovi. □

Jiný důkaz lze vést kombinatoricky pomocí náhrdelníků. Bude-li zájem, ukážeme si na konzultacích.

Věta. (Wilsonova) *Přirozené číslo p je prvočíslo právě tehdy, když*

$$(p-1)! \equiv -1 \pmod{p}.$$

Eulerova věta a řády

Vzdalme se teď od prvočísel. Důkaz Malé Fermatovy věty totiž můžeme zobecnit na všechna přirozená čísla, získáme tak Eulerovu větu.

Cvičení. (Eulerova věta) Buď a nesoudělné s n a $\varphi(n)$ počet čísel menších než n nesoudělných s n. Potom

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

Tvrzení. *Eulerovu funkci $\varphi(n)$ lze spočítat následovně: pokud $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, pak $\varphi(n) = (p_1 - 1)p_1^{\alpha_1 - 1} \cdots (p_k - 1)p_k^{\alpha_k - 1}$.*

Všimněme si, že toto tvrzení říká, že Eulerova funkce je multiplikativní, tj. pro a, b nesoudělná platí $\varphi(ab) = \varphi(a) \cdot \varphi(b)$.

Cvičení. Spočítejte zbytek, který dává 5^{30} po dělení 62.

Definice. *Řád čísla a modulo n* nazveme nejmenší kladné celé číslo r takové, že $a^r \equiv 1 \pmod{n}$.

Cvičení. Jaké jsou řády čísel 1, 3, 5, 7 modulo 8?

Tvrzení. *Ať a, d jsou čísla taková, že $a^d \equiv 1 \pmod{n}$. Potom řád a modulo n dělí d.*

Důsledek. *Z Eulerovy věty plyne, že řád čísla dělí $\varphi(n)$.*

Definice. Zaveďme množinu $\mathbb{Z}_n^*$ obsahující všechny zbytky modulo n nesoudělné s n. Její velikost je tedy rovna $\varphi(n)$.

Poznámka. (pro frajery) Množina $\mathbb{Z}_n^*$ nám dělí celá čísla do zbytkových tříd. Na těchto třídách můžeme definovat násobení tak, že součin dvou tříd $[a]$, $[b]$ spadne do třídy $[ab]$. S takovým násobením $\mathbb{Z}_n^*$ tvoří grupu, jejíž řád je $\varphi(n)$. Z toho už přímo plyne Eulerova věta.

Multiplikativní inverze

Tvrzení. (existence inverzí) *Pro každé a nesoudělné s n existuje inverzní prvek x, tedy z definice číslo splňující $ax \equiv 1 \pmod{n}$. To plyne mimo jiné z důkazu Eulerovy věty. Rozmyslete si další důkaz pomocí Bezoutova lemmatu.*

Poznámka. Inverzní prvek k a v $\mathbb{Z}_n^*$ budeme značit $\frac{1}{a}$.

Cvičení. Jaké jsou inverze čísel 1, 3, 5, 7 modulo 8? Všimnete si obecného pravidla?

Cvičení. Jak plyne existence $\frac{1}{a}$ z Eulerovy věty? Jak lze inverzní prvek explicitně napsat vzhledem k a a n?

Cvičení. Dokažte pomocí multiplikativních inverzí Wilsonovu větu.

Cvičení. Ověřte si, že s takovými „zlomky“ můžeme pracovat obdobně jako s normálními racionálními čísly: jsou-li b a d nesoudělná s n, pak v $\mathbb{Z}_n^*$ platí

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}=(ad+bc)\frac{1}{bd}.$$

Pozor! Mějme pořád na paměti, že tyto „zlomky“ jsou pouze formální výrazy $\frac{a}{b}=a\frac{1}{b}$.

Úlohy

Úloha 1. Nechť $P(x)=5x^{13}+13x^5+9ax$. Najděte nejmenší a takové, že $P(x)$ je dělitelné 65 pro každé x. (Irsko 2000)

Úloha 2. Jaké zbytky dává číslo $(n-1)!$ modulo n větší než 1?

Úloha 3. Dokažte, že platí $\binom{p-1}{a}\equiv(-1)^a \pmod p$.

Úloha 4. Najděte všechna kladná n, pro která je $n!+5$ čtverec.

Úloha 5. Nechť $p>5$ je prvočíslo a číslo a je tvořeno $p-1$ jedničkami v soustavě o základu $p+6$. Dokažte, že $p\mid a$.

Úloha 6. Najděte všechna prvočísla p a q taková, že $p+q=(p-q)^3$. (Rusko 2001)

Úloha 7. Dokažte, že existují právě tři nejvýše n-ciferná přirozená čísla a taková, že $a^2\equiv a \pmod{10^n}$. (MKS–24–5–5)

Úloha 8. Ukažte, že pro různá prvočísla p a q platí

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

Úloha 9. Nechť p a q jsou prvočísla. Dokažte, že $p^{p(q-1)}-1$ není dělitelné číslem $(p^{q-1}-1)q$.

Úloha 10. Najděte všechna prvočísla p, pro která je výraz

$$\binom{p}{1}^2+\binom{p}{2}^2+\cdots+\binom{p}{p-1}^2$$

dělitelný p^3. (CPS 2008–3)

Úloha 11. Dokažte, že pro každé přirozené n platí $2022\mid n^{n^{n^{n^n}}}-n^{n^{n^n}}$.

Úloha 12. Dokažte, že pro každé liché n platí $n\mid 2^{n!}-1$ a pro každé sudé n platí, že n^2-1 dělí $2^{n!}-1$.

Úloha 13. Zjistěte, pro která přirozená n platí, že $n\mid 3^{n!}-2^{n!}$. (MKS 17–7–4)

Úloha 14. Určete hodnotu výrazu $\frac{1}{2} + \frac{2}{3} + \cdots + \frac{p-2}{p-1} \pmod p$ pro libovolné p.
(MKS 24–5–7)

Úloha 15. (Wolstenholmova věta) Ať $p > 3$ je liché prvočíslo. Dokažte, že čitatel zlomku

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

v základním tvaru je dělitelný p^2.

Úloha 16. Uvažujme posloupnost $a_1, a_2, \ldots$, definovanou vztahem $a_n = 6^n + 3^n + +2^n - 1$. Určete všechna přirozená čísla, která jsou nesoudělná s každým členem této posloupnosti. (IMO 2005)

Úloha 17. Pro liché prvočíslo p dokažte

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

(*i*KS 2012/N3)

Úloha 18. Ať $a_1, a_2, \ldots, a_p$ tvoří úplnou sadu zbytků modulo p. Dokažte, že $1 + x^1 + x^2 + \cdots + x^{p-1} \mid x^{a_1} + x^{a_2} + \cdots + x^{a_p}$.

Úloha 19. Definujme posloupnost následovně $a_1 = 2$, $a_n = 2^{a_{n-1}}$. Dokažte, že pro každé $n > 1$ existuje k takové, že všechny členy posloupnosti a_i splňující $i > k$ mají stejný zbytek po dělení n. (USAMO 1991/3)

Úloha 20. V úloze výše dokažte, že pro všechna $n > 1$ platí $n \mid a_n - a_{n-1}$.
(iKS 2012/N5)

Úloha 21. Ukažte, že pro p prvočíslo je každý prvočíselný dělitel čísla $2^p - 1$ větší než p.

Úloha 22. Dokažte, že pro každé $a > 1$ a n přirozené platí $n \mid \varphi(a^n - 1)$.

Úloha 23. Nechť je a liché přirozené číslo. Dokažte, že jsou $a^{2^n} + 2^{2^n}$ a $a^{2^m} + 2^{2^m}$ pro všechna přirozená $n \neq m$ nesoudělná.

Návody

3. Rozepiš pomocí faktoriálů a upravuj.

7. Pro $n = 1$ máme 1, 5, 6. První krok máme, co takhle pokračovat indukcí?

9. Zkus ten levý výraz rozložit.

10. Důležité je, že všechny členy jsou dělitelné p^2, pak už stačí dokázat jen dělitelnost p, navíc $(p-k)! \equiv (-1)^{p-k}k(k+1)\cdots p$.

12. Zase ta Eulerova funkce.

13. Použij Eulerovu funkci a předchozí příklad. Rozděl podle největšího společného dělitele n a 6.

14. Můžou být nějaké dva členy toho součtu stejné modulo p?

15. Popáruj členy a zbav se jednoho p. Mohou být inverze dvou různých nenulových zbytků stejné?

16. Můžeme nějak jednoduše zařídit, aby pro dané prvočíslo bylo některé a_n dělitelné p? Co zapojit inverze?

17. Kde jen už jsme to a^{p-2} viděli? Taky je docela fajn umět sčítat $1+1=2$, pak se to dá hezky rozložit binomickou větou.

18. Rozšiř obě strany dělitelnosti číslem $x-1$. Potom můžeš redukovat z Malé Fermatovy věty exponenty na pravé straně.

21. Uvaž nějaký prvočíselný dělitel q. Jak může vypadat řád 2 modulo q?

22. Najdi číslo, které má řád n modulo $a^n - 1$.

23. Pro spor jsou soudělná a jejich společný dělitel obsahuje prvočíslo p. Potom tedy chceš zkoumat řád $\frac{a}{2} \pmod p$.

Literatura a zdroje

Děkuji *φlovi Čermákovi*, jehož přednášku jsem ukradl a založil na ní tu svoji.

[1] Fíla Čermák: *Zbytky a mocnění*, Sklené, 2019.
[2] Radan Kučera: Přednášky z Algebry I, MUNI.
[3] Justin Stevens: *Olympiad Number Theory Through Challenging Problems*, 2016.
[4] *AoPS*, *http:/artofproblemsolving.com/community*.
[5] Staré ročníky *i*KS, *http:/iksko.org/problems.php*.

Šifrovací protokol RSA

Zdeněk Pezlar

Abstrakt. Život na internetu je závislý na soukromí – hesla k účtům od sociálních sítí, bankovní detaily nebo zprávy. Očekáváme, že tyto citlivé informace jsou nějakým způsobem chráněné. Jak ale?

Představme si následující situaci: Alfréd chce poslat Blaženě tajnou zprávu skrz tzv. *nezabezpečený kanál*. To znamená, že ještě před tím, než zpráva dojde k Blaženě, Eva si zprávu taky může přečíst. Jak zaručíme, aby Eva zůstala na holičkách, ale Blažena si zprávu přečetla?

(A)symetrické šifrování

Symetrická šifra je šifra, kde se pro zašifrování i rozšifrování používá ten samý klíč. Na rozšifrování tedy stačí znát tento klíč a vyhráli jsme. Klasický příklad je Caesarova šifra, kde každé písmeno posuneme o fixní číslo. Z textu „HESLO“ můžeme vytvořit GDRKN a nebo JGUNQ.

Příklad. Zpráva „IJOXNIJXJY“ je zašifrovaná pomocí Caesarovy šifry. Jak zní originál?

Od dob Julia Caesara až po šifrování pomocí stroje Enigma v období druhé světové války se po většinu lidské historie užívaly systémy založené na domluvě komunikujících stran, tedy na společném *klíči*, který pro zbytek světa zůstává ukrytý.

Cvičení. Alfréd a Blažena jsou ubytováni ve stejném hotelu v oddělených místnostech, které nemohou opustit. Jediná možnost, jak si mohou něco předat, je pomocí poslíčka Evy. Alfréd chce poslat Blaženě prstýnek, ale bojí se, že by ho Eva mohla ukrást. Oba milenci mají na svých pokojích několik trezorů, visacích zámků a odpovídajících klíčů. Zamčené trezory můžeme považovat za nedobytné a navíc víme, že Eva celé trezory nekrade. Jak to mají udělat, aby se prstýnek bezpečně dostal k Blaženě?

Kvůli rizikům symetrické kryptografie přišli Whitfield Diffie a Martin Hellman s revolučním nápadem, *asymetrickou kryptografií*. V takovém systému má každá strana dva klíče – *veřejný*, který je užíván pro zašifrování a je sdílený volně s širým světem, a druhý *soukromý*, kterým naopak zprávy dešifruje a nechá si jej pro sebe.

Cílem zašifrování je najít tzv. *jednostrannou funkci*, tedy funkci, u které snadno spočítáme obraz každého čísla. Požadujeme ale, aby ze znalosti $f(k)$ bylo číslo k těžko spočitatelné. Příkladem prominentní jednostranné funkce je zdánlivý rozdíl obtížnosti v násobení čísel a rozkladu čísla na prvočísla.

Rychlokurz teorie čísel

Často se v teorii čísel bavíme o dělitelnosti, resp. o modulární aritmetice – jaké zbytky dávají čísla po dělení jinými.

Cvičení. Jak souvisí Caesarova šifra s modulární aritmetikou?

Věta. (Eulerova věta) *Buď a nesoudělné s n a $\varphi(n)$ počet čísel menších než n nesoudělných s n. Potom*

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

Na znalosti zbytku $a^e \pmod{n}$ nám stačí spočítat $a^{e \pmod{\varphi(n)}} \pmod{n}$. Otázka inverzní operace, tedy ze znalosti zbytku získat exponent, nese honosný název „problém diskrétního logaritmu“. V tomto problému známe zbytek z a základ a a snažíme se dopočítat exponent e takový, že $a^e \equiv z \pmod{n}$. Tento problém může sloužit jako hledaná jednostranná funkce, alespoň když neznáme prvočíselný rozklad n.

Cvičení. Rozmyslete si, jak získat zbytek $a^e \pmod{n}$ pomocí méně než $\log_2(e)$ operací násobení.

Cvičení. Víme, že všechny prvočinitelé čísla n jsou menší než 1000. Vymyslete algoritmus na rozklad takového čísla na prvočinitele.

Cvičení. Dejme tomu, že známe prvočíselný rozklad čísla n. Popřemýšlejte nad algoritmem, který by našel řešení problému diskrétního logaritmu. Návod: Začněte s prvočísly a poté rozšiřte pomocí Čínské zbytkové věty.

Protokol RSA

Název protokolu vychází ze jmen autorů (Rivest, Shamir, Adleman).

Funkčnost systému je založena na pozorování, že je snadné vygenerovat dvě velká prvočísla p, q a vynásobit je $n = pq$. Jak jsme ale diskutovali, rozložit n zpátky na prvočísla je už podstatně těžší.

Situace je následující. Blažena (příjemce zprávy) si vygeneruje svůj soukromý klíč, který bude k, nejmenší společný násobek $\varphi(p) = p - 1$ a $\varphi(q) = q - 1$. Poté si zvolí číslo e z množiny $\mathbb{Z}_k^\times$, toto číslo má v $\mathbb{Z}_k^\times$ inverzi.

Právě na tento inverzní prvek k e se bude mocnit. Jak ho Blažena spočítá? Pomocí Eukleidova algoritmu spočítá Bézoutovy koeficienty $xe + yk = 1$, tedy $x \equiv \frac{1}{e} \pmod{k}$. Blaženin veřejný klíč je dvojice (n, e) a její tajný soukromý klíč je ona inverze, $x \equiv \frac{1}{e} \pmod{k}$.

Příklad. Jeden příklad za všechno. Blažena si vybere prvočísla $p = 17$ a $q = 11$. Poté $n = pq = 187$ a k je největší společný násobek $\varphi(p) = 16$ a $\varphi(q) = 10$, tj. $k = 80$. Vybere si číslo $e = 3$ nesoudělné s k. Ověřte si, že inverzí čísla e bude 27. Blaženin veřejný klíč tedy bude dvojice $(n, e) = (187, 3)$ a soukromý klíč $\left(n, \frac{1}{e}\right) = (187, 27)$.

Blažena má tedy svůj veřejný klíč. Jak je na tom nyní Alfréd? Alfréd zprávu z dešifruje snadno. Ten zná soukromý klíč $\left(n, \frac{1}{e}\right)$, jednoduše pak umocní

$$z^{\frac{1}{e} \pmod k} \equiv (m^e)^{\frac{1}{e}} \equiv m \pmod n.$$

Příklad. (pokračování) Blažena chce zašifrovat číslo $m = 15$. Šifrovaná zpráva bude pak číslo

$$z \equiv m^e \equiv 15^3 \equiv 9 \pmod{187}.$$

Nyní přichází čas pro Alfréda. Ten zná soukromý klíč $(187, 27)$ a zprávu z. Alfréd jednoduše umocní a získá hledanou tajnou zprávu $9^{27} \equiv 15 \pmod{187}$.

V následujícím předpokládejte, že můj veřejný klíč je $(629, 17)$ a že pro kódování zpráv používám ASCII (tedy například písmena A až Z se kódují postupně na čísla 65 až 90 a mezera se kóduje na 32).

Cvičení. Zašifrujte zprávu „MKS“ po písmenech.

Cvičení. Zachytili jste zašifrovanou zprávu

$$247, \quad 337, \quad 322, \quad 463, \quad 15, \quad 73, \quad 440, \quad 15, \quad 342, \quad 323, \quad 435.$$

Rozluštěte ji.

Bezpečnost RSA

Obecně je algoritmus RSA při použití dostatečně velkého klíče považován za bezpečný. V dnešní době je vhodné používat minimálně 2048-bitové klíče. Bezpečnost algoritmu je založena na tom, že pro rozklad čísel na prvočinitele není známý žádný efektivní algoritmus – alespoň na klasickém počítači ...

Literatura a zdroje

Děkuji *Michalu Töpferovi*, na jehož příspěvku jsem zakládal a některé části dočista ukradl.

[1] Michal Töpfer: *Asymetrické šifrování*, Branná, 2019.
[2] Radan Kučera: Přednášky z Algebry I. MUNI.
[3] Ronald L. Rivest, Adi Shamir a Leonard M. Adleman: *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. 1977.

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 přednášce se s ní seznámíme a ukážeme si všechny možné nekalé triky, které s ní můžeme provádět.

Věta. (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. Rovnost nastává právě tehdy, když $x_1 = x_2 = \cdots = x_n$.

Příklad.

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

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

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

Příklad. 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 mnoho, zatímco na druhé straně byl 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. Dokažte, že pro kladná reálná x, y, z platí

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

Cvičení. (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 nám ukázala, že rozložení nepříjemné nerovnosti 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. Dokažte, že pro kladná reálná a, b, c platí

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

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

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

Příklad. 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. Pomaličku začíná přituhovat a budeme bojovat se složitějšími výrazy. Abychom se v úpravách neztratili, vyzbrojíme se znakem tzv. *cyklické sumy*. Funguje to nějak takto: $\sum_{\text{cyc}} a = a + b + c$, $\sum_{\text{cyc}} xy^2 = xy^2 + yz^2 + zx^2$.

Lehké odhady na těžké nerovnosti

Asi největší využití AG nerovnosti spočívá ve 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 (a jejich používání vyžaduje notnou dávku praxe). Obojí si ukážeme.

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

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

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

Příklad. 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 Cauchy–Schwarzova nerovnost (ta druhá stěžejní nerovnost). 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. Pro $a, b, c > 0$ dokažte nerovnost

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

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

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

Příklad. Pro a, b, c kladná dokažte

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

Vážená verze AG nerovnosti

K jejímu důkazu je třeba vyššího matematického aparátu. Ale může se hodit.

Věta. (vážená AG nerovnost) *Pro libovolná reálná nezáporná čísla $x_1, x_2, \ldots, x_n$ a reálná nezáporná $w_1, w_2, \ldots, w_n$ s kladným součtem w. Pak platí*

$$\frac{w_1x_1 + w_2x_2 + \cdots + w_nx_n}{w} \geq \sqrt[w]{x_1^{w_1}x_2^{w_2}\cdots x_n^{w_n}}.$$

Poznámka. Rovnost nastává právě tehdy, když všechny x_i, pro která je $w_i > 0$, mají stejnou hodnotu. Pro $w_1 = w_2 = \cdots = w_n = \frac{1}{n}$ dostáváme klasickou AG nerovnost.

Příklad. Dokažte, že pro kladná reálná a, b, c splňující $a+b+c = 3$ platí $a^b b^c c^a \leq 1$.

Úlohy na procvičení (triviální až středně obtížné)

Úloha 1. Anička našla 4 kladná reálná čísla – součet dvou z nich je 42 a součet druhých dvou je 4. Jaký nejvyšší může být součin všech těchto čtyř čísel?

Úloha 2. Určete všechna kladná reálná x, y, z splňující $x + y + z = 6$ a $xyz = 8$.

Úloha 3. 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 4. Najděte minimum výrazu $\frac{9x^2 \sin x^2 + 4}{x \sin x}$ pro $0 < x < \pi$.

Úloha 5. 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 6. Nechť $xyz = 32$, kde x, y, z jsou kladná reálná. Najděte minimum výrazu

$$x^2 + 4xy + 4y^2 + 2z^2.$$

Úloha 7. Dokažte, že pro $0 \leq a \leq b \leq c$ platí $(a + 3b)(b + 4c)(c + 2a) \geq 60abc$.

Úloha 8. 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 9. Dokažte, že pro kladná a, b, c platí

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

Úloha 10. Dokaž, že pro kladná $a_1, a_2, \ldots, a_n$, jejichž součin je 1, platí

$$\frac{a_1}{1+a_1} + \frac{a_2}{(1+a_1)(1+a_2)} + \cdots + \frac{a_n}{(1+a_1)(1+a_2)\cdots(1+a_n)} \geq 1 - \frac{1}{2^n}.$$

Úloha 11. Dokažte, že pro $a, b, c > 0$ splňující $abc = 1$ platí

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

Úloha 12. 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 13. 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 14. Ukažte, že pro každou trojici kladných čísel a, b, c splňující $abc = 1$ platí

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

(IMO shortlist, 1996)

Úloha 15. 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 16. Nechť $n > 2$ je přirozené číslo a $x_1, x_2, \ldots, x_n$ jsou kladná reálná čísla. Ukažte, že

$$\sum_{\text{cyc}} \frac{1}{x_i^3 + x_{i-1}x_ix_{i+1}} \leq \sum_{\text{cyc}} \frac{1}{x_ix_{i+1}(x_i + x_{i+1})}.$$

(6. série A3, 6. ročník *i*KS)

Úloha 17. Nechť $n > 2$ a $a_2, a_3, \ldots, a_n$ jsou kladná reálná čísla splňující podmínku $a_2a_3\cdots a_n = 1$. Dokažte, že platí

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

(IMO 2, 2012)

Úloha 18. Nechť $a, b, c > 0$ a $a + b + c = 1$. Dokažte, že platí

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

Úloha 19. Ukažte, že pro každé přirozené n a každou n-tici kladných reálných čísel $x_1, x_2, \ldots, x_n$ platí

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

(35. ročník MKS, finální myšmaš)

Úloha 20. 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 21. 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 22. 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 23. Nechť $a, b, c > 0$ a $a + b + c = 1$. Dokažte, že platí

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

Návody

1. Dvě lehká AGčka, vyjde $\frac{441}{4}$.

2. Kdy nastává při AG nerovnosti rovnost? :)

3. Je to vlastně AG nerovnost.

4. Substituce $a = x \sin x$ pomůže, výsledek je 12.

5. $x^2 + (y^2 + z^2) \geq \cdots$

6. $(x + 2y)^2 \geq 8xy$, mělo by vyjít 96.

7. Podmínky je třeba využít – zkus po roznásobení zmenšit levou stranu tak, aby byl příklad ekvivalentní jediné AG nerovnosti.

8. Může se hodit $2(a^2 + b^2) \geq (a + b)^2$.

9. Roznásobit a dvě AGčka.

10. Dokaž indukcí, že levá strana je $\frac{(1+a_1)(1+a_2)\cdots(1+a_n)-1}{(1+a_1)(1+a_2)\cdots(1+a_n)}$.

11. Zkus v AGčku vyrušit jmenovatele – pozor, aby nastávala rovnost!

12. Po roznásobení se může hodit substituce $x = \frac{a}{b}$.

13. $\frac{2a}{b^2+c^2} + \frac{b^2+c^2}{2} + a^2 \geq \cdots$ je dobrý začátek. :)

14. Použij odhad $a^5 + b^5 \geq a^3b^2 + a^2b^3$.

15. Je třeba použít váženou AG nerovnost.

16. Použij úlohu 9 na odhad členů levé strany a upravuj.

17. Známá substituce umí odstranit podmínku. Potom např. $(x_2 + x_3)^3 = (\frac{x_2}{2} + \frac{x_2}{2} + x_3)^3 \geq \cdots$

18. Po úpravě do tvaru $\sum_{\text{cyc}} \frac{bc(1-a)}{a^2+bc} \geq 1$ jde roznásobit.

19. $(1 + x_1 + \cdots + x_i)^{n-i+2} \geq \frac{(n-i+2)^{n-i+2}}{(n-i+1)^{n-i+1}}(1 + x_1 + \cdots + x_{i-1})^{n-i+1}x_i$.

20. Dokaž $\frac{|OD|}{\sin|\sphericalangle OBD|} = \frac{|BC|}{\sin|\sphericalangle BOC|}$, použij vzorec $\frac{|BC|}{2\sin\alpha} = R$ a trochu goniometrie. AGčko je až poslední krok.

21. Odhadnout jmenovatele, zatnout zuby a nebát se homogenizovat pro $a = x^9$.

22. $a + a + \frac{7b+\frac{1}{a^2}}{8} \geq \cdots$ Alternativně lze řešit pomocí tzv. *Hölderovy nerovnosti*.

23. Je ekvivalentní

$$\sum_{\text{cyc}} a(a+b)\sqrt{bc(a+c)(a+b)} \leq \frac{1}{2}(a+b+c)(a+b)(b+c)(c+a).$$

Odhadni odmocninu hezkým AGčkem, zatni zuby a pokračuj.

Literatura a zdroje

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

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

p-valuace

Adéla Karolína Žáčková

Abstrakt. V mnohých příkladech z teorie čísel se řeší dělitelnost. Často nám ale nestačí jenom vědět, jestli dané prvočíslo dělí nějaké číslo, ale také jak moc ho dělí. To je podstata p-valuací. Na přednášce se naučíme pracovat s jejich základními vlastnostmi, které pak použijeme na nějaké záludnější příklady.

Definice. Pro celá čísla a, b říkáme, že a *dělí* b (značíme $a \mid b$), pokud existuje celé číslo c splňující $b = ac$.

Definice. Pro prvočíslo p definujeme p-valuaci celého čísla $a \neq 0$ jako největší nezáporné celé k takové, že $p^k \mid a$. Značíme $v_p(a) = k$. Pro $a = 0$ budeme brát $v_p(a) = \infty$ pro každé p.

To je spousta matematických symbolů. Co to ale znamená lidsky? p-valuací čísla a vyjadřujeme mocninu prvočísla vyskytujícího se v jeho rozkladu. To nám umožňuje se dívat na číslo z pohledu prvočísel, která je dělí, což, jak dále uvidíme, se nám mnohdy bude hodit. Získáváme tak totiž o něco více informací než pomocí pouhého modula.

Jak se p-valuace chovají?

Tvrzení. *$a \mid b$ právě tehdy, když $v_p(a) \leq v_p(b)$ pro každé prvočíslo p.*

Tvrzení. *Pro $a, b > 0$ platí $a = b$, právě když $v_p(a) = v_p(b)$ pro každé prvočíslo p.*

Tvrzení. *Platí $v_p(ab) = v_p(a) + v_p(b)$.*

Tvrzení. *Platí $v_p(a + b) \geq \min\{v_p(a), v_p(b)\}$. Pokud navíc $v_p(a) \neq v_p(b)$, potom v předchozí nerovnosti nutně nastane rovnost. Obdobně platí totéž pro rozdíl $a - b$.*

Cvičení 1. Spočítejte následující hodnoty:

(1) $v_2(2^n + 4)$,
(2) $v_3(v_3(18^{18}))$,
(3) $v_p((3p^3 + p^2)(p^3 + 2p^2 + 5p))$.

Cvičení 2. Máme tři čísla, z nichž žádné není dělitelné 8 ani 125. Kolika nejvíce nulami může končit jejich součin?

Cvičení 3. Rozmyslete si, že p-valuace se dají rozumně dodefinovat i pro racionální čísla a že i po tomto rozšíření většina z předchozího stále platí.

Cvičení 4. Nahlédněte, že pro přirozené n je $v_p(n) \leq \log_p n \leq n - 1$.

Tvrzení. *Přirozené číslo a je k-tou mocninou přirozeného čísla právě tehdy, když $k \mid v_p(a)$ pro každé prvočíslo p.*

Tvrzení. *Nechť* gcd *značí největšího společného dělitele a* lcm *nejmenší společný násobek. Potom platí*

$$v_p(\gcd(a,b)) = \min\{v_p(a), v_p(b)\}, \qquad v_p(\operatorname{lcm}(a,b)) = \max\{v_p(a), v_p(b)\}.$$

První krůčky

Úloha 5. Dokažte, že pro libovolná přirozená čísla a, b, c platí

$$\frac{(\gcd(a,b,c))^2}{\gcd(a,b)\cdot\gcd(b,c)\cdot\gcd(c,a)} = \frac{(\operatorname{lcm}(a,b,c))^2}{\operatorname{lcm}(a,b)\cdot\operatorname{lcm}(b,c)\cdot\operatorname{lcm}(c,a)}.$$

Úloha 6. Jsou dána přirozená čísla a, b taková, že

$$a \mid b^2, \quad b^2 \mid a^3, \quad a^3 \mid b^4, \quad b^4 \mid a^5, \quad a^5 \mid b^6, \quad \ldots$$

Dokažte, že $a = b$.

Úloha 7. Dokažte, že pro přirozená a, b, c, d splňující $ab = cd$ platí

$$\gcd(a,c)\cdot\gcd(a,d) = a\cdot\gcd(a,b,c,d).$$

Úloha 8. Jsou dána přirozená a, b, c splňující $a^b \mid b^c$, $a^c \mid c^b$. Dokažte, že $a^2 \mid bc$.

Úloha 9. Řekneme, že kladné reálné číslo je *copaté*, pokud není celé a v jeho desetinném zápisu následuje za desetinnou čárkou jen konečně mnoho nenulových číslic. Rozhodněte, zda existují copatá čísla a, b, c taková, že všechna tři čísla ab, bc i ca jsou celá. (MO 64–C–II–4)

Faktoriály a kombinační čísla

Jakmile se člověk setká v příkladu s faktoriálem, má asi tendenci začít trochu fňukat. Přece jenom, pro velká čísla nám vznikají pěkné obludnosti. Hodí se ho tedy nějak pěkně odhadnout. My to umíme pomocí tzv. *Legendreovy formule*, která sice až zas tak pěkně nevypadá (suma spousty dolních částí, fuj ble), ale dá se s ní dobře pracovat, alespoň co se dělitelnosti týče.

Tvrzení. (Legendreova formule) *Pro každé přirozené číslo n platí*

$$v_p(n!) = \sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor.$$

Poznámka. Součet ve vzorci je sice formálně nekonečný, pro libovolné p však od dostatečně velkého j bude p^j větší než n a pak budeme přičítat pouze nuly.

Věta. *Nechť $s_p(n)$ značí ciferný součet přirozeného čísla n v soustavě o základu p. Potom platí $v_p(n!) = \frac{n-s_p(n)}{p-1}$.*

Věta. (Kummer) *Kombinační číslo $\binom{n}{k}$ má p-valuaci rovnou počtu „přenosů jedničky do vyššího řádu“ při sčítání k a $n-k$ pod sebou v soustavě o základu p.*

Úloha 10. Pro prvočíslo p platí $p^n \nmid ((p-1)n)!$.

Úloha 11. Platí $v_p(n!) \leq \left\lfloor \frac{n-1}{p-1} \right\rfloor$.

Úloha 12. Najděte všechna přirozená n, pro něž $v_2(n!) = n-1$.

Úloha 13. Pro libovolná celá nezáporná m, n je

$$\frac{(2m)!(2n)!}{m!n!(n+m)!}$$

celé číslo.

Úloha 14. Dokažte, že pro přirozená n platí

$$(n+1) \cdot \operatorname{lcm}\left(\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}\right) = \operatorname{lcm}(1, 2, \ldots, n+1).$$

Úloha 15. Dokažte, že existuje konstanta c taková, že pro libovolná přirozená a, b, n splňující $a! \cdot b! \mid n!$ nutně platí $a + b < n + c \log n$. (Erdős)

Úloha 16. Pro přirozené $n \geq 3$ definujme posloupnost přirozených čísel $\alpha_1, \ldots, \alpha_k$ pomocí rozkladu

$$n! = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

kde $p_1 < p_2 < \cdots < p_k$ jsou prvočísla. Najděte všechna n, pro něž je posloupnost $\alpha_1, \ldots, \alpha_k$ geometrická. (MEMO 2017 T8)

IMO úlohy

Úloha 17. Najděte všechny dvojice přirozených čísel (n, k), které splňují

$$(2^k - 1)(2^k - 2)(2^k - 4) \cdots (2^k - 2^{k-1}) = n!.$$

(IMO 2019)

Úloha 18. Je dána nekonečná posloupnost $a_1, a_2, a_3, \ldots$ přirozených čísel taková, že

$$\frac{a_1}{a_2} + \frac{a_2}{a_3} + \cdots + \frac{a_{n-1}}{a_n} + \frac{a_n}{a_1}$$

je přirozené číslo pro všechna $n \geq k$, kde k je nějaké pevné přirozené číslo. Dokažte, že $a_n = a_{n+1}$ pro všechna $n \geq m$, kde m je nějaké pevné přirozené číslo.

(IMO 2018)

Úloha 19. Najděte všechny trojice (p, x, y), kde p je prvočíslo a x, y jsou přirozená čísla taková, že $x^{p-1} + y$ i $x + y^{p-1}$ jsou mocniny p. (ISL 2014)

Návody

5. BÚNO si seřaď valuace, potom přímočaře počítej.

6. $a^n \mid b^{n+1}$ znamená $\frac{v_p(a)}{v_p(b)} \leq \frac{n+1}{n}$. V podstatě totéž jde říct s logaritmem místo valuací.

7. Označ si p-valuace jednotlivých proměnných a rozebírej jejich možné pořadí.

8. AG nerovnost.

9. Chceš nezáporné 2-valuace a 5-valuace. Dirichlet pomůže.

10. V Legendreově formuli zahoď celé části.

11. Ukonči součet u indexu $j = k$ takového, že $1 \leq \frac{n}{p^k} < p$ a využij $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor$.

12. V nerovnostech z důkazu předchozí úlohy musela všude nastat rovnost.

13. Odhadni zvlášť každý člen

$$\left\lfloor \frac{2m}{p^j} \right\rfloor + \left\lfloor \frac{2n}{p^j} \right\rfloor - \left\lfloor \frac{m}{p^j} \right\rfloor - \left\lfloor \frac{n}{p^j} \right\rfloor - \left\lfloor \frac{n+m}{p^j} \right\rfloor$$

z Legendreovy formule.

14. Využij Kummerovu větu. Pokud $\alpha = v_p(n+1)$, pak $n+1$ zapsané v soustavě o základu p končí α nulami.

15. Dělitelnost dává nerovnost (třeba) 2-valuací. Vhodně odhadni celé části v nenulových členech, těch je asymptoticky $\log n$.

16. Hodí se Bertrandův postulát: pro každé přirozené číslo $n \geq 2$ existuje prvočíslo p splňující $n < p < 2n$.

17. Pomocí 2-valuace a 3-valuace omez k, zbytek dorozeber.

18. Stačí ukázat, že nepřibývají nová prvočísla a všechny p-valuace jsou od nějaké chvíle nerostoucí. Rozliš případy podle toho, zda někdy (za indexem k) nastane $v_p(a_n) \geq v_p(a_1)$.

19. Připrav se na spoustu rozebírání rozbitých případů. Hlavní myšlenka je hledat velké valuace p v rozdílech $y - x$ potažmo $y^p - x^p$.

Literatura a zdroje

Tímto bych chtěla poděkovat *Matěji Doležálkovi*, jehož přednášku jsem z velké části bezostyšně vykradla.

[1] Matěj Doležálek *p-valuace*, Lysečiny, 2021.
[2] Seriál Teorie čísel *33. ročník PraSe*, *https://prase.cz/archive/33/serial.pdf*.

Obsah

Kongruencie (Natália Bátorová) 3
Algebraické triky neboli... φgle (φla Čermák) 6
Funkcionální rovnice (φla Čermák) 13
Diskrétní spojitost (Matěj Doležálek) 18
Iterace (Matěj Doležálek) 22
Catalanova čísla (Klárka Grinerová) 28
Obarvování a dláždění (Petr Hladík) 33
Mocnost bodu ke kružnici (Verča Hladíková) 36
Integrály (Terka Kučerová) 39
Fermiho problémy (Lucka Kundratová) 44
Úvod do lineární algebry (Anna Marie Minarovičová) 49
Vězni, domorodci a kouzelníci (Radek Olšák) 55
Dokreslovanie (Michal Pecho) 63
Kolineácia (Michal Pecho) 68
Axiomatická geometrie (Daniel Perout) 72
Množiny bodů dané vlastnosti (Daniel Perout) 78
N (Zdeněk Pezlar) 81
Šifrovací protokol RSA (Zdeněk Pezlar) 86
AG nerovnost (Marian Poljak) 89
p-valuace (Adéla Karolína Žáčková) 96