Zdobnice

Sborník, jaro 2024

Natália Bátorová
Káťa Danilina
Matěj Doležálek
Klárka Grinerová
Vít Hanika
Petr Hladík
Václav Janáček
Lenka Kopfová
Terka Kučerová
Radek Olšák
Daniel Perout
Zdeněk Pezlar
Matouš Šafránek
Josef „José“ Soural
Adéla Karolína Žáčková

Autoři: Natália Bátorová, Káťa Danilina, Matěj Doležálek, Klárka Grinerová, Vít Hanika, Petr Hladík, Václav Janáček, Lenka Kopfová, Terka Kučerová, Radek Olšák, Daniel Perout, Zdeněk Pezlar, Matouš Šafránek, Josef „José“ Soural, Adéla Karolína Žáčková
Editoři: Káťa Danilina, Matěj Doležálek
vydání první, náklad 44 výtisků
březen 2024
Díky za pomoc všem, kterým je za co děkovat.

Eukleidovské obory

Natália Bátorová

Abstrakt. Na přednášce si ukážeme, že Eukleidův algoritmus funguje i v obecnějších, tzv. eukleidovských oborech. Z toho pak plynou jednoznačné rozklady na ireducibilní prvky, což na konci využijeme k počítání diofantických rovnic.

Definice. Obor integrity R nazveme *eukleidovským oborem*, pokud existuje funkce $d : R \to \mathbb{N}_0$ splňující pro všechna $a, b \in R$, $b \neq 0$, následující podmínky:

(1) Platí $d(a) = 0$, právě když $a = 0$.
(2) Platí $d(a) \leq d(ab)$.
(3) Existují $q, r \in R$ taková, že $a = bq + r$ a zároveň $d(r) < d(b)$.

Funkci d budeme říkat *eukleidovská funkce*.

Eukleidovská funkce nám tedy dává ohodnocení prvků oboru integrity, při kterém pouze nula dává nulu, násobky nejsou nikdy menší než dělitelé a umíme dělit se zbytkem tak, aby zbytek byl menší než dělitel.

Definice. Buď R komutativní okruh. Prvek $d \in R$ nazveme *společným dělitelem* prvků $a, b \in R$, pokud $d \mid a$ a zároveň $d \mid b$. Prvek $g \in R$ nazveme *největším společným dělitelem* a, b, pokud současně platí:

(1) Prvek g je společným dělitelem a, b.
(2) Libovolný společný dělitel d prvků a, b dělí také g.

Návrat Eukleidova algoritmu

A teď si ukážeme, jak se dá dělit se zbytkem a pomocí toho spočíst největšího společného dělitele. Buď R eukleidovský obor.

Algoritmus. (Eukleidův) Na vstupu jsou dána $a, b \in R, 0 \neq d(a) \geq d(b)$. Postupně budeme konstruovat posloupnosti $\{a_n\}$, $\{x_n\}$, $\{y_n\}$:

(1) Počáteční hodnoty nechť jsou

$$\begin{aligned} a_1 &= a, & x_1 &= 1, & y_1 &= 0, \\ a_2 &= b, & x_2 &= 0, & y_2 &= 1. \end{aligned}$$

(2) Dokud je $a_n \neq 0$, vezměme dělení se zbytkem $a_{n-1} = qa_n + r$, $d(r) < d(a_n)$ a následně

$$a_{n+1} = r = a_{n-1} - qa_n, \qquad x_{n+1} = x_{n-1} - qx_n, \qquad y_{n+1} = y_{n-1} - qy_n.$$

Jakmile poprvé pro nějaké N nastane $a_N = 0$, vrátíme $(a_{N-1}, x_{N-1}, y_{N-1})$.

Tvrzení. *Uvažujme Eukleidův algoritmus spuštěný na $a, b \in R, 0 \neq d(a) \geq d(b)$. Pak:*

(i) *Algoritmus skončí v konečném počtu kroků.*
(ii) *Pro každé n platí $a_n = x_n a + y_n b$.*
(iii) *a_{N-1} je největším společným dělitelem a a b.*

Důkaz. (náznak) (i) Posloupnost $d(a_n)$ klesá. (ii) Rovnost platí na prvních dvou řádcích algoritmu, poté se zachovává odečítáním q-násobku celého řádku. (iii) Indukcí dokážeme, že $D = a_{N-1}$ dělí všechna a_n: platí to na posledních dvou řádcích algoritmu, v indukčním kroku se vracíme o jeden řádek zpět nahoru. Číslo D tedy dělí všechna a_n, takže je D společný dělitel a, b. Abychom ukázali, že je největším společným dělitelem, mějme $d \mid a, b$. Z (ii) $d \mid x_{N-1}a + y_{N-1}b = D$, tedy D je největší společný dělitel. □

Vidíme tedy, že v eukleidovském oboru mají všechny dvojice prvků největší společné dělitele. Nyní se blíž podíváme, jak vlastně ty prvky vypadají.

Definice. Pokud $a \mid b$ a zároveň $b \mid a$, řekneme, že prvky a, b jsou *asociované*, značíme $a \parallel b$. Řekneme, že a je *jednotka*, pokud $a \parallel 1$. Řekneme, že a je *ireducibilní*, pokud a není jednotka a každý jeho dělitel je jednotka nebo asociovaný s a.

Cvičení. Které prvky jsou jednotkami a které jsou ireducibilní v $\mathbb{Z}$? Jak to vypadá v $\mathbb{Q}$?

Cvičení. Hodnota eukleidovské funkce je pro všechny jednotky stejná. Navíc, pokud $d(a) = d(1)$, tak je a jednotka.

Teď si ukážeme, že ireducibilní prvky a prvočinitelé jsou to samé. Pro jistotu připomeneme definici prvočinitelů:

Definice. Ať R je obor a $p, a, b \in R, p \nparallel 1$. Pak p je prvočinitel, pokud splňuje následující podmínku: pokud $p \mid ab$, pak $p \mid a$, nebo $p \mid b$.

Věta. *Ireducibilní prvky jsou prvočinitelé.*

Důkaz. Ať p je ireducibilní a $p \mid ab$. Pokud $p \mid b$, máme hotovo. Předpokládejme, že $p \nmid b$. Označme D největšího společného dělitele p, b. Pak z ireducibility plyne, $D \parallel 1$ a tedy $\exists x, y : x \cdot p + y \cdot b = 1$. Z toho plyne $x \cdot ap + y \cdot ab = a$ z čeho vidíme, že p dělí levou stranu a tedy musí dělit i pravou, tedy $p \mid a$. □

Jednoznačný rozklad na ireducibilní prvky

Lemma. *Pro nenulové a, b platí, že pokud $a \mid b$ a $a \nparallel b$, pak $d(a) < d(b)$.*

Důkaz. Platí, že $a = bq + r$, kde $d(b) > d(r)$. Protože $b \nmid a$, musí $r \neq 0$. Pak $r = a - bq$, a dělí pravou stranu a tedy $a \mid r$. Z toho máme $d(a) \leq d(r) < d(b)$. □

Věta. *V Eukleidovském oboru můžeme každý nenulový prvek zapsat jako součin jednotky a ireducibilních prvků.*

Důkaz. Budeme postupovat indukcí dle $d(x)$. Pro každé nenulové x platí, že $d(1) \leq d(1 \cdot x) = d(x)$. Pokud $d(x) = d(1)$, z cvičení víme, že x je jednotka a tvrzení platí. Tím máme dokázaný základní krok. Vezměme prvek x takový, že $d(x) = n$ a předpokládejme, že tvrzení platí pro všechna y splňující $d(y) < n$. Pokud je x ireducibilní, máme hotovo. Pokud není ireducibilní, pak $x = x_1 \cdot x_2$, přičemž $d(x_1) < n$ a $d(x_2) < n$, tedy x_1, x_2 lze zapsat jako součiny jednotky a ireducibilních prvků. Dohromady máme, že x lze zapsat jako součin jednotky a ireducibilních prvků. □

Věta. *Rozklad prvků na ireducibilní činitele je jednoznačný až na asociovanost.*

Důkaz. Ať pro prvek $x \nparallel 1$ máme rozklady: $vq_1 \cdots q_m = x = up_1 \cdots p_n$, kde $n \leq m$. Víme, že p_1 je prvočinitel, proto $\exists i : p_1 \mid q_i$. BÚNO $p_1 \mid q_1$, pokud ne, přeznačíme prvky. Protože q_1 je ireducibilní a p_1 není jednotka, nutně $p_1 \parallel q_1$, tedy $\exists v_1 : q_1 = v_1 p_1$. Pak můžeme vykrátit:

$$vv_1 p_1 q_2 \cdots q_m = up_1 \cdots p_n$$
$$(vv_1) q_2 \cdots q_m = up_2 \cdots p_n$$

Opakováním procesu po n krocích zjistíme, že $m = n$ a rozklady jsou asociované. □

Příklad. Obor $\mathbb{Z}[\sqrt{-2}]$ je eukleidovský.

Řešení. Jako eukleidovskou funkci zvolíme normu $N(\alpha) = \alpha \cdot \overline{\alpha}$. Pro ni platí $N(\alpha) = 0$ právě když $\alpha = 0$ a $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta) \geq N(\alpha)$. Zůstává tedy ověřit třetí podmínku.

Pro $x, y \in \mathbb{Z}$ vyjádříme normu jako $N(x + y\sqrt{-2}) = x^2 + 2y^2$, což je celé číslo. Ukažme tedy, jak budeme dělit se zbytkem. Mějme $a, b \in \mathbb{Z}[\sqrt{-2}]$, kde $b \neq 0$. Chceme zvolit $q \in \mathbb{Z}[\sqrt{-2}]$ tak, že

$$N(a - qb) = N(r) < N(b).$$

Vydělme $\frac{a}{b} = \frac{a \cdot \overline{b}}{N(b)} = x + y\sqrt{-2}$, kde $x, y \in \mathbb{Q}$, protože $\overline{b}$ je prvek $\mathbb{Z}[\sqrt{-2}]$, takže celý čitatel $a\overline{b}$ je prvek $\mathbb{Z}[\sqrt{-2}]$. Můžeme tedy využít multiplikativity normy a naši „cílovou“ nerovnost ekvivalentně upravit na

$$N\left(\frac{a}{b} - q\right) < 1.$$

Nyní stačí zvolit $q = x_0 + y_0\sqrt{-2}$ tak, že zaokrouhlíme x, y na nejbližší celé číslo (nižší či vyšší podle toho, které je blíž). Tím bude zaručeno $|x - x_0|, |y - y_0| \leq \frac{1}{2}$,

což nám dá

$$N\left(\frac{a}{b}-q\right)=(x-x_0)^2+2(y-y_0)^2\leq\left(\frac{1}{2}\right)^2+2\cdot\left(\frac{1}{2}\right)^2\leq\frac{3}{4}<1.$$

Tím už je dokázáno, že norma je eukleidovská funkce v oboru $\mathbb{Z}[\sqrt{-2}]$.

Cvičení. Ukažte, že $\mathbb{Z}[i]$ je taky eukleidovský.

Občas se nám bude hodit spíš geometrický náhled.

Příklad. Uvažme komplexní číslo $\alpha=\frac{1+i\sqrt{7}}{2}$, které splňuje $\alpha^2=\alpha-2$. Potom je obor $\mathbb{Z}[\alpha]=\{x+y\alpha : x,y\in\mathbb{Z}\}$ eukleidovský s normou jako eukleidovskou funkcí.

Řešení. Platí $\alpha+\overline{\alpha}=1$ a $\alpha\overline{\alpha}=\frac{1-(-7)}{4}=2$, takže pro $x,y\in\mathbb{Z}$ má prvek $x+y\alpha\in\mathbb{Z}[\alpha]$ normu

$$(x+y\alpha)(x+y\overline{\alpha})=x^2+xy\cdot(\alpha+\overline{\alpha})+y^2\cdot\alpha\overline{\alpha}=x^2+xy+2y^2,$$

což je celé číslo. Stejně jako v předchozím příkladu použijeme trik s dělením, takže budeme pro $\frac{a}{b}=x+y\alpha$, kde $x,y\in\mathbb{Q}$, hledat taková $x_0,y_0\in\mathbb{Z}$, že

$$N\Big((x-x_0)+(y-y_0)\alpha\Big)<1.$$

Na tento problém můžeme nahlížet geometricky. Nerovnice $x^2+xy+2y^2<1$ určuje v kartézské rovině vnitřek nějaké elipsy.[1] To, že odečítáme $x_0+y_0\alpha$, odpovídá tomu, že se souřadnice nějakého zadaného (x,y) snažíme posunout o celá čísla tak, aby výsledek spadl dovnitř této elipsy.

S tím už se lze vypořádat celkem jednoduše. Nejprve zaokrouhlíme y na nejbližší celé číslo y_0. Tím bude rozdíl $y-y_0$ ležet mezi $-\frac{1}{2}$ a $\frac{1}{2}$. Když elipsu protneme s přímkou $y=\frac{1}{2}$, budou x-ové souřadnice průsečíků řešeními rovnice $x^2+\frac{x}{2}-\frac{1}{2}=0$. Těmi jsou $x_{1,2}=\frac{-\frac{1}{2}\pm\sqrt{\frac{1}{4}+4\cdot\frac{1}{2}}}{2}$, takže tyto dva průsečíky jsou od sebe vzdáleny

$$\sqrt{\frac{1}{4}+4\cdot\frac{1}{2}}=\sqrt{\frac{9}{4}}=\frac{3}{2}>1.$$

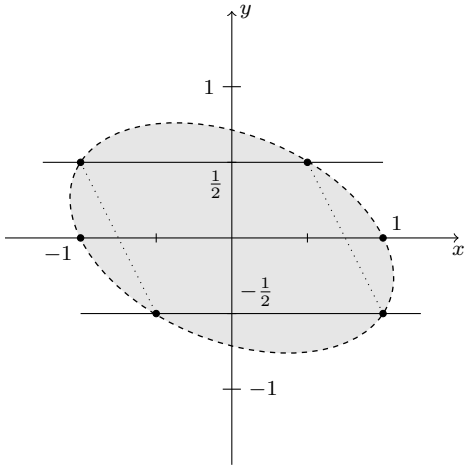
Důležité je, že vzdálenost je větší než 1. Na přímce $y=-\frac{1}{2}$ máme další dva průsečíky, středově souměrné podle počátku s prvními dvěma. Tyto čtyři průsečíky jsou vrcholy rovnoběžníku, který leží uvnitř této elipsy (vyjma vrcholů, ty leží na elipse), protože elipsa je konvexní útvar.[2] Tento rovnoběžník má výšku přesně 1 a šířku (délku příslušné strany) ostře větší než 1. Tyto vlastnosti už zaručují, že se do něj

[1] Že tato nerovnice skutečně určuje elipsu, zde nebudeme dokazovat. Pokud si tedy lámeš hlavou nad tím, proč by tomu tak mělo být, prosíme Tě, abys nám to prostě věřil(a) :-).

[2] Je to totiž jenom splácnutá kružnice.

dovedeme trefit vhodnou volbou x_0, y_0 – nejprve se výběrem y_0 trefíme mezi $-\frac{1}{2}$ a $\frac{1}{2}$ a následně budeme schopni vybrat x_0, protože se trefujeme do intervalu delšího než 1.

Pro formální správnost postupu jenom musíme rovnoběžník o velmi malý kousek zmenšit, aby ležel v elipse celý, včetně vrcholů. Vrcholy leží přímo na elipse, takže jakkoliv malé zmenšení nám postačí. Je tedy zřejmé, že tohle dovedeme provést tak, abychom zachovali šířku větší než 1.



Cvičení. Ukažte, že $\mathbb{Z}[\sqrt{-3}]$ není eukleidovský obor.

Úloha 1. V oboru $\mathbb{Z}[i]$ nalezněte největšího společného dělitele 2 a $3+5i$.

Úloha 2. Najděte všechna celočíselná řešení rovnice $x^2 = y^3 - 1$.

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

Úloha 4. Je $3+i$ ireducibilní v $\mathbb{Z}[i]$?

Úloha 5. Najděte všechna celočíselná řešení rovnice $3b^4 + 3b^2 + 1 = a^2$.

Úloha 6. Je obor $\mathbb{Z}[\sqrt{2}]$ eukleidovský?

Návody

2. Rozlož na ireducibilní prvky.

3. Rozlož na ireducibilní prvky.

4. Použij normu pro určení kandidátů pro dělitele.

5. Vynásob obě strany $9b^2$ a použij vhodnou substituci.

6. Zkus funkci $N(x + y\sqrt{2}) = |x^2 - 2y^2|$.

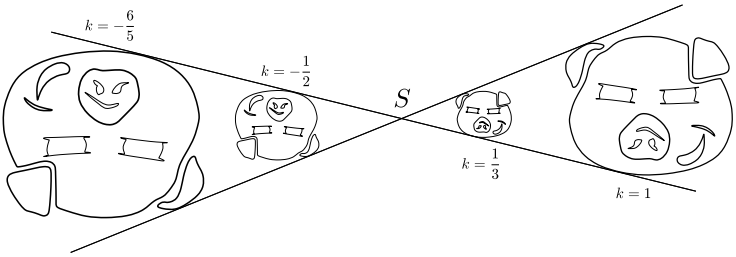
Literatura a zdroje

[1] Filip Čermák, Matěj Doležálek: *Teorie nejen čísel*, 2020.

Stejnolehlost

Káťa Danilina

Abstrakt. V příspěvku si představíme stejnolehlost, ukážeme si, jak ji hledat a že k tomu, abychom vyřešili celou úlohu, občas stačí najít vhodnou stejnolehlost.



Definice. *Stejnolehlost* $\mathrm{H}(S, k)$ je zobrazení určené bodem S (střed stejnolehlosti) a nenulovým reálným číslem k (koeficient stejnolehlosti), ve kterém se bod S zobrazí sám na sebe a každý bod $X \neq S$ na bod X' tak, že $|X'S| = |k| \cdot |XS|$.

(i) Pro $k > 0$ leží bod X' na polopřímce SX.
(ii) Pro $k < 0$ leží bod X' na polopřímce opačné k SX.

Tvrzení. (vybrané vlastnosti) *Stejnolehlost:*

(i) *Je podobné zobrazení.*
(ii) *Zobrazuje přímky na přímky s nimi rovnoběžné.*
(iii) *Pro dva podobné mnohoúhelníky s rovnoběžnými odpovídajícími si stranami existuje stejnolehlost (případně posunutí či identita), která zobrazuje jeden na druhý.*

Příklad. (Eulerova přímka) Je dán trojúhelník ABC. Body H, T a O jsou postupně ortocentrum, těžiště a opsiště. Dokažte, že tyto tři body leží na jedné přímce a zároveň platí $|TH| = 2 \cdot |TO|$.

Řešení. Označíme si K, L a M postupně středy úseček BC, AC a AB. Stejnolehlost se středem v T a koeficientem $-\frac{1}{2}$ zobrazí vrcholy A, B, C postupně na K, L, M. Zároveň, když se bod A zobrazí na K, výška z bodu A se zobrazí na rovnoběžku skrz K, což bude osa strany BC.

Po zobrazení všech vrcholů dostaneme, že se průsečík výšek zobrazí na průsečík os stran, tedy ortocentrum se zobrazí na střed kružnice opsané. Takže H, T a O budou ležet na přímce, zároveň bude platit, že $|TH| = 2 \cdot |TO|$, jelikož stejnolehlost zobrazí TH na opačnou polopřímku a zmenší její vzdálenost dvakrát.

Úlohy

Úloha 1. Nechť $ABCD$ je lichoběžník s rovnoběžnými stranami AB a CD, jeho průsečík úhlopříček označme E. Najdeme body F a G tak, aby trojúhelníky ABF a CDG byly rovnostranné a zároveň byly vně $ABCD$. Dokažte, že E, F a G leží na jedné přímce.

Úloha 2. Jsou dány dvě kružnice k_1 a k_2, které se zvenčí dotýkají v bodě T. Dokažte, že pro každé dva body A na k_1 a B na k_2 takové, že platí $|\sphericalangle ATB| = 90°$, prochází přímka AB pevným bodem.

Úloha 3. Kružnice k, ℓ mají vnitřní dotyk v bodě T (k leží uvnitř ℓ). Na ℓ zvolíme body A, B tak, že AB se dotýká k v bodě S. Dokažte, že TS je osou úhlu ATB.

Úloha 4. Je dán trojúhelník ABC. Body dotyků úsečky BC s kružnicí vepsanou a připsanou označme postupně D a E. Přímka AE protne kružnici vepsanou blíže bodu A v bodě F. Dokažte, že DF je kolmá na BC.

Úloha 5. Mějme přímku p a dvě kružnice k_1, k_2, které se dotýkají p ze stejné strany postupně v bodech T a U. Kružnice k neprotíná p a dotýká se zvnějšku k_1 a k_2 postupně v bodech K a L. Dokažte, že KT, LU a k mají společný bod.

Úloha 6. Kružnice k, ℓ mají vnější dotyk v bodě T. Navíc se obě vnitřně dotýkají kružnice m postupně v bodech R, S. Druhý průsečík přímky RT s kružnicí m označme Q. Dokažte, že $|\sphericalangle TSQ| = 90°$.

Úloha 7. Nechť ABC je trojúhelník a nechť D je průsečík tečny ke kružnici opsané trojúhelníku ABC v bodě A a přímky BC. Nechť E je průsečík kolmice na BC v B a osy strany BA. Analogicky nechť F je průsečík kolmice na BC v bodě C a osy strany CA. Dokažte, že D, E, F leží v přímce.

Úloha 8. V trojúhelníku ABC protínají osy vnitřních úhlů kružnici opsanou postupně v bodech S_A, S_B, S_C. Kružnice vepsaná se dotýká stran a, b, c postupně v bodech K, L, M. Dokažte, že přímky S_AK, S_BL, S_CM procházejí jedním bodem.

Úloha 9. V trojúhelníku ABC označme O střed kružnice vepsané, P střed kružnice připsané ke straně BC a D průsečík osy úhlu CAB se stranou BC. Dokažte, že platí

$$\frac{2}{|AD|} = \frac{1}{|AO|} + \frac{1}{|AP|}.$$

(MO 59–II–4)

Úloha 10. Označíme H, O a I postupně ortocentrum, střed opsané kružnice a střed vepsané kružnice v trojúhelníku ABC a buď K bod, kde se kružnice vepsaná dotkne BC. Dokažte, že pokud OI je rovnoběžná s BC, pak AO je rovnoběžná s HK.

Skládání stejnolehlostí

Silným a o něco obtížnějším nástrojem je skládání stejnolehlostí. Budeme používat následující velmi užitečné lemma.

Lemma 11. *Nechť* $\mathrm{H}_1(S_1, k_1)$ *a* $\mathrm{H}_2(S_2, k_2)$ *jsou stejnolehlosti takové, že* $S_1 \neq S_2$ *a* $k_1 \cdot k_2 \neq 1$. *Pak jejich složením je opět stejnolehlost, a to se středem na přímce* S_1S_2.

Úloha 12. (Mongeova věta) V rovině jsou dány tři kružnice. Pro každé dvě můžeme sestrojit průsečík jejich vnějších společných tečen. Dokažte, že pak tyto tři průsečíky leží na přímce.

Úloha 13. V trojúhelníku ABC označme k kružnici jemu opsanou. Najdeme kružnici k_a, která se dotýká přímek AB a AC a navíc se vnitřně dotýká k v bodě A'. Obdobně najdeme k_b, k_c a body B' a C'. Dokažte, že AA', BB' a CC' procházejí jedním bodem.

Úloha 14. V trojúhelníku jsou dány tři kružnice k_a, k_b, k_c tak, že každé dvě mají vnější dotyk, k_a se dotýká stran AB, AC, k_b stran BC, BA a k_c stran CA, CB. Bod dotyku k_b s k_c označíme A_1, bod dotyku k_c s k_a označíme B_1. Dokažte, že přímky AB_1, BA_1 a osa úhlu u vrcholu C procházejí jedním bodem.

Úloha 15. Jsou dány kružnice k_1, k_2 a k_3 takové, že žádná neleží uvnitř jiné. Kružnice ℓ s nimi má vnitřní dotyk postupně v bodech A_1, A_2 a A_3 a kružnice m s nimi má vnější dotyk postupně v bodech B_1, B_2 a B_3. Dokažte, že přímky A_1B_1, A_2B_2 a A_3B_3 procházejí jedním bodem.

Úloha 16. Do kružnice k je vepsán rovnoramenný trojúhelník ABC, kde $|AB| = |AC|$. Dále vepíšeme kružnice k_b a k_c do úsečí kružnice k, které jsou určené postupně tětivami AC a AB tak, aby kružnice ležely mimo ABC. Ty se dotknou kružnice k postupně v bodech B' a C'. Společná vnější tečna kružnic k_b a k_c protne AC v bodě P a AB v bodě Q. Dokažte, že se přímky $C'Q$ a $B'P$ protnou na ose úhlu BAC.

(Polsko 2012)

Těžké úlohy

Úloha 17. Jsou dány dvě kružnice, jejich středy jsou vzdálené 10 jednotek a mají poloměry 1 jednotku a 3 jednotky. Najděte množinu středů úseček XY, kde X leží na jedné kružnici a Y na druhé. (Putnam 1996)

Úloha 18. Kružnice k a ℓ mají vnější dotyk v bodě T. Navíc mají vnitřní dotyk s kružnicí m v bodech A a B. Společná tečna k a ℓ v bodě T protne m v bodě P. AP protne k podruhé v bodě X, BP protne ℓ podruhé v bodě Y. Dokažte, že XY je společná tečna kružnic k a ℓ.

Úloha 19. Buď $ABCD$ konvexní čtyřúhelník a P bod na straně AB takový, že kružnice vepsaná trojúhelníku CPD mající střed v I se dotýká kružnic vepsaných trojúhelníkům APD, PBC postupně v bodech K, L. Označme $E = AC \cap BD$ a $F = AK \cap BL$. Dokažte, že body E, I, F leží v přímce.

Úloha 20. V trojúhelníku ABC označíme M průsečík těžnice se stranou BC a N průsečík osy úhlu BAC se stranou BC. Kolmice na AN z bodu N protne MA a AB postupně v bodech Q a P. Kolmice v bodě P na AB protne osu úhlu BAC v bodě O. Dokažte, že QO je kolmá na BC (APMO 2000)

Úloha 21. V trojúhelníku ABC platí $|AC| + |BC| = 3 \cdot |AB|$. Kružnice vepsaná se středem I se dotkne stran BC, AC postupně v bodech D, E. Nechť body K a L jsou postupně obrazy bodů D a E ve středové symetrii se středem v I. Dokažte, že body A, B, K a L leží na jedné kružnici. (IMO 2005 shortlist)

Návody

1. Hledej stejnolehlost, jejíž střed bude E.

2. Dokaž, že body jsou na stejném místě v rámci své kružnice.

3. Rozmysli si, kam se zobrazí S po stejnolehlení k na ℓ z T a co bude platit o tečně v novém bodě.

4. Zobraz připsanou na vepsanou. Kam se zobrazí E?

5. Dokresli si bod X na k co nejdále od p a dokaž, že K, T, X a L, U, X leží na přímkách.

6. Označ P bod, kde ST protne m. Stačí dokázat, že PQ je průměr m.

7. Vedeme bodem B rovnoběžku s AC, ta protne tečnu v A v bodě G. Stačí dokázat, že E je střed kružnice opsané nově vzniklého trojúhelníku AGB.

8. Je to střed stejnolehlosti, v níž kružnice vepsaná přejde na kružnici opsanou.

9. Najdi středy obou stejnolehlostí mezi vepsanou a připsanou kružnicí, zapiš si poměry, které ti stejnolehlosti řeknou, a vyjádři pomocí délek AP, AD a AO.

10. Dokresli si bod L tak, aby KL byl průměr. Teď dokaž, že O leží na přímce AL.

12. Interpretuj dva průsečíky jako středy stejnolehlostí, tyto stejnolehlosti slož.

13. Dokresli si vepsanou kružnici a zkus ji zobrazit na opsanou.

14. Je to střed záporné stejnolehlosti zobrazující k_c na kružnici vepsanou.

15. Je to střed stejnolehlosti, kdy m přejde na ℓ.

16. Dokreslíme kružnici vepsanou trojúhelníku APQ.

17. Zafixuj Y a zobraz X ve stejnolehlosti se středem Y a $k = \frac{1}{2}$. Pak si rozmysli, jak se hýbe střed této kružnice, když se Y mění.

18. Mocnost z bodu X.

19. Dokaž, že $CDPA$ a $CDBP$ jsou tečnové, a dokresli si kružnici, která se dotýká DA, AB a BC.

20. Dokresli si Švrčkův bod a pak hledej, co můžeš stejnolehlit.

21. Platí, že $|AB| = |CD|$, dále si dokresli D' jako dotyk připsané kružnice. Dokazuj, že $ABKI$ je tětivový.

Literatura a zdroje

Příspěvek jsem s malými úpravami převzala od Davida Hrušky, který ho s malými úpravami převzal od Tomáše „Šavlíka“ Pavlíka, kterým tímto děkuji.

[1] David Hruška: *Stejnolehlost*, Staré město, 2015.

Chvála Eukleidova algoritmu

Matěj Doležálek

Abstrakt. Tento příspěvek má jediný cíl: přesvědčit čtenáře, že elementární teorie čísel vychází z jediného místa – Eukleidova algoritmu.

Úmluva. (tabula rasa) Na začátku tohoto příspěvku nemáme nic. Teorie čísel je pustá a prázdná. Vznáší se tu pouze množina celých čísel $\mathbb{Z}$, ve které umíme sčítat, odečítat, násobit a porovnávat. Důvěrně známé koncepty jako dělitelnost, prvočísla a jednoznačný rozklad na ně, to vše teprve budeme muset vybudovat.

Úmluva. Neřekne-li se jinak, všechna čísla jsou celá.

Základy

Definice. Říkáme, že a *dělí* b (nebo b *je násobkem* a, nebo a *je dělitelem* b), pokud existuje k splňující $b = k \cdot a$. Značíme $a \mid b$.

Tvrzení. (základní vlastnosti dělitelnosti) *Pro libovolná a, b, c, d platí:*

(i) $1 \mid a$,
(ii) $a \mid a$,
(iii) $a \mid 0$,
(iv) $a \mid b$ a zároveň $b \mid c \implies a \mid c$,
(v) $a \mid b$ a zároveň $a \mid c \implies a \mid b + c$,
(vi) $a \mid b$ a zároveň $c \mid d \implies ac \mid bd$,
(vii) $a \mid b$ a zároveň $b \neq 0 \implies |a| \leq |b|$.

Definice. (školská) Kladné číslo p nazveme *prvočíslem*, pokud má právě dva kladné dělitele (1 a p).

Tahle definice ... ujde. Dá se s ní žít, ale později uvidíme lepší.

Úloha 1. Každé číslo $n > 1$ má prvočíselného dělitele.

Úloha 2. Existuje nekonečně mnoho prvočísel.

Největší společný dělitel a jak ho najít

Definice. Nejsou-li a, b obě nulová, označíme za jejich *největšího společného dělitele* (značíme $\mathrm{NSD}(a,b)$) to největší z čísel, které je obě dělí. Pokud $\mathrm{NSD}(a,b)=1$, řekneme, že jsou a, b *nesoudělná*.

Tautologické definice jsou tautologické. Větší síly nabude pojem NSD skrze důsledky toho, jak jej počítáme. K tomu nejprve pomocné tvrzení formalizující intuitivně jasnou věc:

Lemma. (dělení se zbytkem) *Mějme celá čísla a, b, přičemž $b \neq 0$. Pak lze zvolit celá q, r tak, že $a = qb + r$ a zároveň $0 \leq |r| < |b|$.*

Pozor, v této konvenci není zbytek určen zcela jednoznačně, mohou existovat dvě možnosti.

Algoritmus. (Eukleidův) Na vstupu jsou dána celá čísla a, b, ne obě nulová. Postupně budeme konstruovat posloupnosti $\{a_n\}$, $\{x_n\}$, $\{y_n\}$:

(1) Počáteční hodnoty nechť jsou

$$a_1 = a, \qquad x_1 = 1, \qquad y_1 = 0,$$
$$a_2 = b, \qquad x_2 = 0, \qquad y_2 = 1.$$

(2) Dokud je $a_n \neq 0$, vezměme dělení se zbytkem $a_{n-1} = qa_n + r$, $0 \leq |r| < |a_n|$ a následně

$$a_{n+1} = r = a_{n-1} - qa_n, \qquad x_{n+1} = x_{n-1} - qx_n, \qquad y_{n+1} = y_{n-1} - qy_n.$$

Jakmile poprvé pro nějaké N nastane $a_N = 0$, vrátíme $(a_{N-1}, x_{N-1}, y_{N-1})$.

Tvrzení. *Uvažujme Eukleidův algoritmus spuštěný na nějaká a, b. Pak:*

(i) *Algoritmus skončí v konečném počtu kroků.*
(ii) *Pro každé n platí $a_n = x_n a + y_n b$.*
(iii) $|a_{N-1}| = \mathrm{NSD}(a,b)$.

Důkaz. (náznak) (i) Posloupnost $|a_n|$ klesá. (ii) Rovnost platí na prvních dvou řádcích algoritmu, poté se zachovává odečítáním q-násobku celého řádku. (iii) Indukcí dokážeme, že $D = |a_{N-1}|$ dělí všechna a_n: platí to na posledních dvou řádcích algoritmu, v indukčním kroku se vracíme o jeden řádek zpět nahoru. Číslo D tedy dělí všechna a_n, takže je D společný dělitel a, b. Abychom ukázali, že je největší, mějme $d \mid a, b$. Z (ii) $d \mid x_{N-1}a + y_{N-1}b = \pm D$, takže $d \leq |d| \leq |D| = D$, tedy D je největší společný dělitel. □

Z důkazu tvrzení o Eukleidově algoritmu rovnou plyne:

Důsledek. (lepší definice NSD) *Pokud $d \mid a, b$, pak už i $d \mid \mathrm{NSD}(a,b)$.*

Důsledek. (Bézoutova rovnost) *Pro libovolná celá a, b (ne obě nulová) lze zvolit celá x, y tak, že $\mathrm{NSD}(a,b) = xa + yb$. Těmto x, y říkáme Bézoutovy koeficienty.*

Pozor, Bézoutovy koeficienty nejsou jednoznačně určeny, existuje spousta takových párů (x, y).

Úloha 3. Kdykoliv je (x, y) pár Bézoutových koeficientů k a, b, pak je jím taky $(x + kb, y - ka)$ pro každé k.

Úloha 4. Nahlédněte, že pro každé k platí $\mathrm{NSD}(a, b) = \mathrm{NSD}(b, a - kb)$.

Společenstvo důsledků a jednoznačný rozklad na prvočísla

Nyní už je čas vylepšit definici prvočísla. Při práci v teorii čísel málokdy používáme přímo školskou definici prvočísla, tedy že „prvočíslo moc nejde rozkládat na součin“. Mnohem častěji se o slovo hlásí vlastnost prvočísel při dělení součinů:

Definice. (morálně správná) Kladné číslo $p > 1$ nazveme *prvočíslem*, pokud pro libovolná a, b splňující $p \mid ab$ platí $p \mid a$ nebo $p \mid b$.

Proč tyto dvě definice rozlišovat? V obecnějším zasazení těchto pojmů (přijďte na přednášku o eukleidovských oborech!) se může stát, že tyto dvě vlastnosti „prvočísel“ nechodí spolu – je radostnou, nesamozřejmou událostí, že v celých číslech spolu jsou svázány.

Než dokážeme, že uvedené dvě definice prvočísla ve skutečnosti určují tu samou množinu čísel, budeme pro rozlišení prvočíslům podle školské definice říkat *ireducibilní prvky* a prvočíslům podle morálně správné definice *prvočinitelé*.

Úloha 5. Nahlédněte, že každý prvočinitel musí být ireducibilním prvkem.

Lemma. (Eukleidovo) *V celých číslech je každý ireducibilní prvek prvočinitelem.*

Důkaz. (stručně) Pro spor ať ireducibilní p má k sobě nějaká a, b, že $p \mid ab$, ale přitom $p \nmid a$, $p \nmid b$. Potom je $\mathrm{NSD}(p, a) = 1$, takže pro nějaké Bézoutovy koeficienty máme $x_1 p + y_1 a = 1$. Analogicky $x_2 p + y_2 b = 1$, ale znásobením je

$$1 = (x_1 p + y_1 a)(x_2 p + y_2 b) = x_1 x_2 p^2 + x_1 y_2 pa + x_2 y_1 pb + y_1 y_2 ab$$

násobek p, což je spor. □

Dohromady už máme, že ireducibilní prvky a prvočinitelé jsou v $\mathbb{Z}$ totéž, proto se můžeme bezpečně vrátit k označení *prvočísla*.

Věta. (základní aritmetiky) *Každé*[1] *kladné číslo n se rozkládá na součin konečně mnoha prvočísel $p_1 \cdots p_k$, a tento rozklad je jednoznačný až na změnu pořadí činitelů.*

V praxi se typicky více hodí seskupit kopie téhož prvočísla do jedné mocniny, tedy psát prvočíselný rozklad ve tvaru $n = p_1^{e_1} \cdots p_k^{e_k}$ a předpokládat, že $p_1, \ldots, p_k$ jsou navzájem různá.

Úloha 6. Rozmysli si poctivě, že známe-li rozklady $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$ (exponenty smí být nulové), pak platí $a \mid b$ právě tehdy, když $\alpha_i \leq \beta_i$ pro $i = 1, \ldots, k$.

[1] O 1 si představujeme, že se rozkládá na prázdný součin, tedy součin žádných prvočísel.

Jednoznačný rozklad na prvočísla je kanón. Následujících pár důsledků Bézoutovy rovnosti s mottem „V nesoudělnosti je síla“ lze ubít tímto kanónem, anebo je lze nahlédnout přímo a elegantněji opět z Bézoutovy rovnosti.

Úloha 7. Jsou-li a, b nesoudělná a platí $a \mid bc$, pak už $a \mid c$.

Úloha 8. Jsou-li a, b nesoudělná a platí $a \mid c$ i $b \mid c$, pak už $ab \mid c$.

Kongruence

Definice. Říkáme, že *a je kongruentní b modulo m* (značíme $a \equiv b \pmod{m}$), pokud $m \mid a - b$.

Tvrzení. (vlastnosti kongruencí) *Pro celá čísla a, b, c, d, m platí:*

(i) $a \equiv b \pmod{m}$ *a zároveň* $c \equiv d \pmod{m} \implies a + c \equiv b + d \pmod{m}$ *a také* $ac \equiv bd \pmod{m}$,
(ii) $ac \equiv bc \pmod{m}$ *a zároveň* $0 \neq c \mid m \implies a \equiv b \pmod{\frac{m}{c}}$,
(iii) $ac \equiv bc \pmod{m}$ *a zároveň jsou c, m nesoudělná* $\implies a \equiv b \pmod{m}$.

Množině všech b kongruentních danému a modulo m říkáme *zbytková třída*, konkrétně je to tedy $\{a + km \mid k \in \mathbb{Z}\}$. Bod (i) předešlého tvrzení ospravedlňuje, že pokud nás ve výsledku nějakého výpočtu (obnášejícího jen sčítání a násobení) zajímá pouze výsledek modulo m, taktéž vstupy nám stačí znát jen modulo m. Tedy můžeme $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ chápat jako množinu všech zbytkových tříd s operacemi definovanými libovolnou volbou reprezentantů.

Tvrzení. (multiplikativní inverz) *Uvažujme a a m. Nějaké b takové, že $ab \equiv \pmod{m}$, existuje právě tehdy, když* $\mathrm{NSD}(m, a) = 1$. *V takovém případě už je toto b jednoznačně určené modulo m a značíme jej jako a^{-1} či $\frac{1}{a} \pmod{m}$.*

Poznámka. (modulení s neznámými) Pokud modulíme jeden výraz s neznámou druhým, často bývá dobrým úhlem pohledu si říci, že modulo nám říká hodnotu neznámé. To nemusí být vždy možné, ale když to jde, typicky to zjednoduší a zrychlí úpravy:

Příklad. Najděte největší n takové, že $n + 10 \mid n^3 + 100$. (AIME 1986)

Řešení. Modulo $n + 10$ *doslova* platí $n \equiv -10$, takže $n^3 + 100 \equiv (-10)^3 + 100 \equiv -900$. Největším dělitelem -900 je 900, takže největším vyhovujícím n bude 890.

Úlohy!

Úloha 9. Ukažte, že pro každé kladné n je zlomek $\frac{21n+4}{14n+3}$ v základním tvaru. (IMO 1959)

Úloha 10. V závislosti na nezáporném n určete $\mathrm{NSD}(n! + 1, (n+1)! + 1)$.

Úloha 11. Nahlédněte, že známe-li faktorizace $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$, potom $\mathrm{NSD}(a, b) = p_1^{\gamma_1} \cdots p_k^{\gamma_k}$ pro $\gamma_i = \min\{\alpha_i, \beta_i\}$.

Úloha 12. Pokud víte, že $\mathrm{NSD}(a, b) = 1$, určete
(i) $\mathrm{NSD}(ab, a + b)$, (ii) $\mathrm{NSD}(a + b, a^2 + b^2)$.

Úloha 13. Pro libovolná nezáporná a, b platí $\mathrm{NSD}(2^a - 1, 2^b - 1) = 2^{\mathrm{NSD}(a,b)} - 1$.

Úloha 14. Najděte všechny funkce $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, jež pro každá $x, y \in \mathbb{N}$ splňují

$$f(x, x) = x, \qquad f(x, y) = f(y, x), \qquad (x + y)f(x, y) = yf(x, x + y).$$

(*i*KS–8–N4)

Návody

1. Indukce.

2. Jsou-li $p_1, \ldots, p_n$ všechna prvočísla, podívej se na $p_1 \cdots p_n + 1$.

3. Jakože … fakt to vyjde, nekecám.

4. Když vynecháme sloupce pro $\{x_n\}$, $\{y_n\}$, tohle je to, co se děje v Eukleidově algoritmu.

5. $p = ab$ speciálně znamená $p \mid ab$.

6. Dokud je prvočíslo v obou, lze ho zkrátit a jet dál, takže stačí ukázat, že prvočísla v rozkladu a nesmí chybět v b.

7. Vezmi Bézoutovu rovnost pro a, b a vynásob ji c.

8. Použij předchozí úlohu a definici dělitelnosti.

9. Pusť Eukleidův algoritmus na výrazy s neznámou n.

10. Použij úlohu 4.

11. Dělitele už umíš vůči faktorizaci charakterizovat z úlohy 6, poté už lze uvažovat zcela přímočaře.

12. Uvažuj, zda by prvočísla $p \mid ab$ mohla být společným dělitelem. V (ii) nejprve vhodně uprav argumenty.

13. Nahlédni, že pokud r je zbytek po $a : b$, pak i $2^r - 1$ je zbytek po $(2^a - 1) : (2^b - 1)$.

14. Označ $g(x, y) = \frac{xy}{f(x,y)}$, potom $g(x, x) = x$, $g(x, y) = g(y, x)$ a konečně $g(x, y) = g(x, x + y)$. Co to je za algoritmus?

Literatura a zdroje

Tuto přednášku jsem poskládal primárně podle *Proseminář z teorie čísel*, který v letním semestru 2024 cvičím. Sekundárně mi posloužily starší příspěvky a seriál, které níže uvádím.

[0] *Proseminář z teorie čísel*, cvičení na MFF UK, LS 2023/2024, *https://sites.google.com/view/proseminar*.
[1] Fíla Čermák, Matěj Doležálek: *Teorie (nejen) čísel*, PraSečí seriál, 40. ročník.
[2] Natália Bátorová: *Kongruencie*, Mrtník, 2023.
[3] Štěpán Šimsa: *Největší společný dělitel*, Staré Město, 2015.

Čínská zbytková věta

Matěj Doležálek

Abstrakt. Ukážeme si, jak se koukat na úlohy modulo více různých čísel naráz, jak tyto pohledy skládat dohromady, a hlavně k čemu je to všechno dobré. Dokážeme Čínskou zbytkovou větu a procvičíme dva hlavní způsoby jejího použití: vyrábění čísel s hromadou dobrých vlastností v konstrukčních úlohách a lámání problému na více menších kousků v důkazových úlohách.

Dvě modula

Kdykoliv počítáme modulo mn, pak každou zbytkovou třídu můžeme „hruběji“ zmodulit mod m a mod n. To může být výhodné v tom, že jednodušší prvočíselný rozklad modula zpravidla vede k příjemnějšímu počítání, např. pro prvočísla p, q bychom mohli přejít od počítání modulo složené pq k počítání modulo dvěma prvočísly zvlášť. Otázkou však je, zda tímto neztrácíme nějakou část informace, kterou jsme modulo mn měli. Ukážeme, že pro *nesoudělná* m, n tímto přechodem žádnou informaci neztratíme, takže počítat modulo mn je totéž jako „počítat modulo m a modulo n zároveň“.

Věta. (Čínská zbytková) *Uvažujme nesoudělná m, n. Potom pro libovolná a, b existuje x splňující $x \equiv a \pmod{m}$, $x \equiv b \pmod{n}$ a všechna taková x jsou si navzájem kongruentní modulo mn.*

Důkaz. (náznak) Chceme ukázat, že zobrazení

$$\psi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$$
$$x \bmod mn \mapsto (x \bmod m, x \bmod n)$$

je bijekce. Prostost plyne z nesoudělnosti implikací $m, n \mid x - x' \implies mn \mid x - x'$, zatímco díky Bézoutovy rovnosti bude ψ na: jestliže $ym + zn = 1$, pak

$$\psi(bym + azn) = (a, b). \qquad \square$$

Indukcí se pak věta snadno rozšíří pro libovolný počet kongruencí:

Věta. (obecněji) *Ať jsou dána po dvou nesoudělná $m_1, \ldots, m_k$. Potom pro libovolná $a_1, \ldots, a_k$ existuje x splňující všech k kongruencí $x \equiv a_i \pmod{m_i}$, a navíc jsou si všechna taková x navzájem kongruentní modulo $M = m_1 \cdots m_k$.*

Příklad. Král Vendelín si chtěl po velké bitvě, do které vyslal 1200 trpaslíků, rychle spočítat ztráty. Nechal si proto přeživší trpaslíky nastoupit postupně po třech, pěti, sedmi a jedenácti. Nejprve mu zbyli dva trpaslíci, poté dvakrát po třech trpaslících a nakonec jich zbylo deset. Kolik trpaslíků tedy přežilo?

Použití Čínské zbytkové věty jde rozlišit na dva hlavní přístupy. V jednom si pro nějaká čísla poručíme vlastnosti, které jsou v úloze užitečné, a zbytkovka zařídí jejich existenci. V druhém si vezmeme k srdci to, že (s jistými omezeními) kongruence platí modulo M, právě když platí modulo jednotlivá m_i. Formálně sice v obou případech děláme totéž, ale jedná o dvě různé strategie, kterými lze úlohy řešit.

Čínská zbytková věta umožňuje celočíselné proměnné poručit libovolné množství modulárních podmínek, dokud jsou příslušná modula vzájemně nesoudělná. Tu a tam se hodí umět tímto způsobem vyčarovat nejen tak ledajaké číslo, ale dokonce prvočíslo. K tomu lze užít následující kanón – poznamenejme, že jeho důkaz daleko přesahuje možnosti běžných olympiádních nástrojů.

Věta. (Dirichletova) *Nechť jsou a, n nesoudělná přirozená čísla. Potom existuje nekonečně mnoho prvočísel p splňujících $p \equiv a \pmod{n}$.*

Obecněji se Čínská zbytková věta často používá kombinováním s nějakým dalším modulárně zabarveným tvrzením. Hodit se proto může třeba následující:

Věta. (malá Fermatova) *Pro celé číslo a a prvočíslo $p \nmid a$ platí $a^{p-1} \equiv 1 \pmod{p}$.*

Konstrukce šikovných čísel

Úloha 1. Dokažte, že pro každé $n \in \mathbb{N}$ existuje n-tice po sobě jdoucích čísel, z nichž každé je dělitelné čtvercem nějakého přirozeného čísla většího než 1.

Úloha 2. Dokažte, že pro každé přirozené n existuje n po sobě jdoucích přirozených čísel, z nichž žádné není prvočíselná mocnina.

Úloha 3. Uvažujme v rovině mřížové body (a, b) s celočíselnými souřadnicemi. Bod (a, b) je *viditelný*, pokud jsou a, b nesoudělná celá čísla. Dokažte, že pro libovolné $n \in \mathbb{N}$ existuje čtverec $n \times n$ mřížových bodů, z nichž žádný není viditelný.

Úloha 4. Dokažte, že pro každé přirozené číslo k lze zvolit $2k$ navzájem různých přirozených čísel $a_1, \ldots, a_k, b_1, \ldots, b_k$ takových, že zlomky

$$\frac{a_1}{b_1}, \quad \frac{a_2}{b_2}, \quad \ldots, \quad \frac{a_k}{b_k}$$

jsou všechny v základním tvaru a tvoří aritmetickou posloupnost.

Úloha 5. Jsou dána celá čísla a, b taková, že pro všechna přirozená n platí

$$b^n + n \mid a^n + n.$$

Dokažte, že $a = b$. (ISL 2005 N6)

Úloha 6. Rozhodněte, zda lze přirozená čísla seřadit do posloupnosti $a_1, a_2, \ldots$ (přičemž každé přirozené číslo se vyskytne právě jednou) tak, aby pro každé přirozené n platilo $n \mid a_1 + \cdots + a_n$.

Úloha 7. Najděte všechny trojice přirozených čísel (a, b, c) takové, že pro každé přirozené číslo n, které nemá žádného prvočíselného dělitele menšího než 2014, platí $n + c \mid a^n + b^n + n$. (ELMO SL 2014)

Úloha 8. Budiž $f : \mathbb{N} \to \mathbb{N}$ funkce splňující pro každá $a, b \in \mathbb{N}$:

(i) $f(a)$, $f(b)$ jsou nesoudělná, právě když a, b jsou nesoudělná.
(ii) $a \leq f(a) \leq a + 2012$.

Dokažte, že když prvočíslo p dělí $f(n)$, pak už i $p \mid n$. (USA TSTST 2012)

Úloha 9. Tabulka 2018×2018 je vydlážděna dominy 2×1. Dokažte, že lze do políček vepsat přirozená čísla tak, že:

(i) Součet dvou čísel na každém dominu je vždy stejný.
(ii) Libovolná dvě čísla, jejichž políčka sousedí stranou, jsou nesoudělná, právě pokud leží na stejném dominu. (PraSe 37–4p–8)

Rozkládání a skládání modul

Úloha 10. Jsou dána prvočísla $p \neq q$. Dokažte, že $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

Úloha 11. Dokažte, že $4a^2 + 9b^2 \equiv 1 \pmod{n}$ má pro libovolné přirozené n řešení.

Úloha 12. Je dáno přirozené číslo n. Budiž A množina těch čísel $a \in \{1, 2, \ldots, n\}$, která splňují $a^2 \equiv a \pmod{n}$. Dokažte, že počet prvků A je mocnina dvojky. (PraSe 40–3s–1)

Úloha 13. Nechť $\varphi(n)$ značí počet čísel z množiny $\{1, \ldots, n\}$, která jsou nesoudělná s n. Vyjádřete $\varphi(n)$ pro n s prvočíselným rozkladem $p_1^{k_1} \cdots p_r^{k_r}$.

Úloha 14. Dokažte, že pro každé $n \in \mathbb{N}$ existuje n-tice po dvou nesoudělných čísel $k_1, \ldots, k_n > 1$ taková, že $k_1 \cdot k_2 \cdots k_n - 1$ je součin dvou po sobě jdoucích přirozených čísel. (USAMO 2008)

Úloha 15. Rozhodněte, zda existuje přirozené n takové, že pro libovolné celé číslo x nemá $x^2 + x + n$ žádného prvočíselného dělitele menšího než 2021.

Úloha 16. Jsou dána přirozená čísla $a > b > c \geq 3$ splňující

$$a \mid bc + b + c, \qquad b \mid ca + c + a, \qquad c \mid ab + a + b.$$

Dokažte, že alespoň jedno z a, b, c je složené číslo.

Úloha 17. Jsou dána přirozená čísla $n, k \geq 2$ a k-tice po dvou různých čísel $a_1, \ldots, a_k$ z množiny $\{1, 2, \ldots, n\}$ taková, že $n \mid a_i(a_{i+1} - 1)$ pro $i = 1, \ldots, k-1$. Dokažte, že $n \nmid a_k(a_1 - 1)$. (IMO 2009/1)

Úloha 18. Pro konečnou množinu X přirozených čísel nechť $S(X)$ značí součet jejích prvků a $P(X)$ jejich součin. Dále uvažujme dvě konečné množiny přirozených čísel A, B takové, že $|A| = |B|$, $P(A) = P(B)$, ale $S(A) \neq S(B)$. Pokud pro každé $n \in A \cup B$ a jeho prvočíselného dělitele p platí $p^{36} \mid n$, ale $p^{37} \nmid n$, dokažte, že $|S(A) - S(B)| > 10^6$. (NIMO 2013)

Návody

1. Předepiš každému číslu čtvercového dělitele.

2. Předepiš každému číslu dva prvočíselné dělitele.

3. Poruč si v každém bodě čtverce prvočíslo, kterým mají být souřadnice soudělné.

4. Vezmi zkrácenou posloupnost $\frac{x+1}{N}, \ldots, \frac{x+k}{N}$ pro vhodná x, N. Jednotlivá b_i odliš zkrácenými prvočísly, a_i pak už odlišíš snadno.

5. Vyrob pro $a-b$ hodně prvočíselných dělitelů. Modula p a $p-1$ jsou nesoudělná!

6. Přidávej členy po dvou – jeden zvol libovolně a jeden urči.

7. S pomocí kanónu ukaž, že $a+b-c$ má hodně prvočíselných dělitelů. Navol si zbytky v různých modulech dle libosti nejprve pro p, potom pro n.

8. Zkus nejdřív zapomenout na n, p a pomocí zbytkovky zkonstruovat takové x, že $f(x) = x$. Potom do výrobního procesu přidej $x \equiv 0 \pmod{p}$, $x \equiv 1 \pmod{n}$.

9. Vyplňuj na jednotlivá domina dvojice čísel $S \pm x_i$ podle šachovnicového obarvení. Kdekoliv má dvojice čísel být soudělná, zvol si na to zvláštní prvočíslo.

10. Podívej se zvlášť mod p a mod q.

11. Vyřeš modulo prvočíselné mocniny. Mocniny 2 a 3 jsou trochu výjimečné, ostatní jsou snadné.

12. Nejprve vyřeš prvočíselné mocniny.

13. Nejprve vyřeš prvočíselné mocniny.

14. Jen se chce, aby $x^2 + x + 1$ umělo mít hodně prvočíselných dělitelů. Pouprav důkaz existence nekonečně mnoha prvočísel.

15. Polynom $x^2 + x$ neumí modulo p nabývat všech možných hodnot – podle toho navol n mod p pro $p < 2021$.

16. Slož do modula abc.

17. Kdyby $n \mid a_k(a_1 - 1)$, pak buďto $a_i \equiv 0 \pmod{p^r}$ pro všechna i, nebo $\equiv 1$ pro všechna i.

18. Součin prvočísel p, pro něž $p - 1 \mid 36$. Když se místo malého Fermata použije Euler, lze odhad vylepšit až na asi $6 \cdot 10^7$.

Literatura a zdroje

Příspěvek je kopií stejnojmenného příspěvku, který jsem připravil na podzimní soustředění 2021 v Zásadě. Děkuji proto svému minulému já za to, že od té doby Čínskou zbytkovou větu nezapomnělo, a umožnilo mi tím tento příspěvek přednášet znovu.

[1] Matěj Doležálek: *Čínská zbytková věta*, Zásada, 2021.

Vytvořující funkce

Klárka Grinerová

Abstrakt. Účastníci, toto jsou vytvořující funkce, vytvořující funkce, toto jsou účastníci, seznamte se prosím. Pro bližší poznání si ukážeme, jak nám takové funkce pomůžou skákat z kombinatoriky do analýzy a zase zpátky, což nám umožní získat zajímavý náhled na některé kombinatorické problémy a úlohy.

Příklad. (motivační) Áďa namalovala vajíčka třemi barvami. Má 4 zelená, 7 modrých a 5 žlutých vajíček. Daník přišel na koledu, kolika různými způsoby si může vybrat 6 vajíček?

Řešení. Hledáme počet uspořádaných trojic nezáporných celých čísel (i, j, k) takových, že $i + j + k = 6$, kde $i \in \{0, 1, 2, 3, 4\}$ odpovídá počtu zelených, $j \in \{0, \dots, 7\}$ modrých a $k \in \{1, \dots, 5\}$ žlutých vajíček, která si Daník vezme. Počet takových trojic najdeme snadno jako koeficient u x^6 v součinu $(1+x+x^2+x^3+x^4)(1+\cdots+x^7)(1+\cdots+x^5)$. Daník má tak 24 možností, jak si vybrat 6 vajíček.

Kombinatorickou úlohu tak můžeme velmi jednoduše převést na hledání koeficientů u mocnin x v součinu několika polynomů. Než se pustíme do nějakých novot, připomeneme si pár vět, co už jistě znáte.

Věta. (geometrická řada) *Pro libovolné $x \in \mathbb{R}$ různé od 1, $n \in \mathbb{N}_0$ platí*

$$1 + x + x^2 + \cdots + x^n = \frac{x^{n+1} - 1}{x - 1}.$$

Věta. (binomická) *Pro libovolné $x \in \mathbb{R}$, $n \in \mathbb{N}$ platí*

$$\binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n = (x+1)^n.$$

V předchozích případech se jedná vždy o konečné součty. Jediný nekonečný součet, který budeme do začátku potřebovat znát, je součet nekonečné geometrické řady.

Věta. (nekonečná geometrická řada) *Pro všechna $x \in (-1, 1)$ platí*

$$\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n.$$

V případě $x = 0$ v předchozí větě používáme konvenci $0^0 = 1$. Když už jsme se dostali k nekonečným součtům, bylo by dobré vědět, co taková nekonečná řada $\sum_{n=0}^{\infty} a_n x^n$ vlastně je. Na takovou řadu se lze dívat dvěma způsoby. Jednak jako na *formální řadu*, tj. posloupnost jejích koeficientů $a_0, a_1, a_2, \dots$, za kterými jsou symboly x^n. Takovéto formální řady si můžeme sčítat i násobit, jako by to byly polynomy. To odpovídá kombinatorické straně naší teorie.

V druhém případě bychom mohli chtít za x dosazovat. Pokud by to šlo, odpovídala by řada $\sum_{n=0}^{\infty} a_n x^n$ nějaké funkci $f(x)$, která číslu x přiřadí onen nekonečný součet. O řadě bychom pak říkali, že *konverguje*. To ale bohužel nefunguje vždycky – pokud se koeficienty a_i chovají nepěkně, takový součet vůbec nemusí dávat smysl.

Tvrzení. *Pokud řada $a(x) = \sum_{n=0}^{\infty} a_n x^n$ konverguje pro všechna $x \in (-\varepsilon, \varepsilon)$ pro nějaké dostatečně malé $\varepsilon > 0$, pak jsou její koeficienty jednoznačně určeny hodnotami funkce $a(x)$.*

Funkce $a(x)$ má v bodě 0 derivace všech řádů a pro $n = 0, 1, 2, \dots$ tak platí $a_n = \frac{a^{(n)}(0)}{n!}$, kde $a^{(n)}(0)$ značí n-tou derivaci funkce $a(x)$ v bodě 0.

Jelikož nás zajímá spíš kombinatorická stránka problematiky, konvergencí a hlubším pochopením tohoto tvrzení se příliš nebudeme zabývat. K tomu, aby řada konvergovala na nějakém $(-\varepsilon, \varepsilon)$ například bohatě stačí, aby pro všechna $n \in \mathbb{N}$ platilo $a_n < K^n$ pro nějaké pevné číslo K. Jakmile tedy koeficienty a_n rostou dostatečně pomalu, jsou jednoznačně určeny funkcí $a(x)$, která ve svém zápisu neobsahuje žádný nekonečný součet, ale přitom je rovna našemu požadovanému součtu a navíc v sobě ukrývá informace o celé posloupnosti. Typicky a_n bude hledaný počet nějakých kombinatorických objektů o „velikosti“ n. Takovým objektům bude odpovídat funkce $a(x)$.

Definice. Buď $(a_i)_{i=0}^{\infty} = (a_0, a_1, a_2, \dots)$ nekonečná posloupnost reálných čísel. Její *vytvořující* (generující) funkce je mocninná řada

$$a(x) = a_0 + a_1 x + a_2 x^2 + \cdots = \sum_{i=0}^{\infty} a_i x^i.$$

Pointa je následující. Máme-li nějakou posloupnost čísel, která nás zajímá, můžeme z ní vytvořit příslušnou vytvořující funkci. Tu ale s trochou štěstí dokážeme vyjádřit v uzavřeném tvaru. Kombinatorické či algebraické vlastnosti původní posloupnosti jsou pak uschovány ve velmi kompaktním tvaru, ve kterém s nimi umíme jednoduše manipulovat a pokud příslušné řady konvergují, umíme se kdykoli beztrestně vrátit zpět.

Zobecněná binomická věta

Definice. Pro libovolné $r \in \mathbb{R}$, $k \in \mathbb{N}$ definujeme kombinační číslo $\binom{r}{k}$ předpisem

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

Nazýváme jej *zobecněné kombinační číslo.*

Věta. (zobecněná binomická) *Pro $x \in (-1,1)$ platí*

$$(1+x)^r = \binom{r}{0} + \binom{r}{1}x + \binom{r}{2}x^2 + \cdots$$

Pro $r \in \mathbb{N}$ je tedy předchozí tvrzení běžná binomická věta. Pro $r \in \mathbb{Z}$ nebo obecněji $r \in \mathbb{Q}$ ale dostáváme nové rovnosti, ve kterých najednou napravo vystupují nekonečné řady. Kromě součtu nekonečné geometrické řady tedy známe další druh součtu, díky čemu se umíme mnohem lépe vypořádat s některými dalšími vytvořujícími funkcemi.

Jako důsledek zobecněné binomické věty platí pro každé $n \in \mathbb{N}$ a $x \in (-1,1)$

$$\frac{1}{(1-x)^n} = \sum_{i=0}^{\infty} (-1)^i \binom{n+i-1}{n-1} x^i.$$

Cvičení. Ukažte, že opravdu platí $\binom{-r}{i} = (-1)^i \binom{r+i-1}{r-1}$.

Operace s posloupnostmi a jejich vytvořujícími funkcemi

Budeme pracovat s posloupnostmi $(a_0, a_1, a_2, \dots)$, $(b_0, b_1, b_2, \dots)$, $(c_0, c_1, c_2, \dots)$, jejich vytvořujícími funkcemi $a(x)$, $b(x)$, $c(x)$ a reálným číslem α.

(1) Součtu $a(x) + b(x)$ odpovídá posloupnost $(a_i + b_i)_{i=0}^{\infty}$.
(2) Vynásobení reálným číslem $\alpha a(x)$ odpovídá $(\alpha a_i)_{i=0}^{\infty}$
(3) Vynásobení $x^n a(x)$ odpovídá posunutí vpravo $(\underbrace{0, \dots, 0}_{n}, a_0, a_1, \dots)$.
(4) Dělení $\frac{a(x) - (a_0 + a_1 x + a_2 x^2 + \cdots)}{x^n}$ odpovídá posunutí vlevo $(a_n, a_{n+1}, a_{n+2}, \dots)$.
(5) Dosazení αx místo x $a(\alpha x)$ odpovídá $(a_0, \alpha a_1, \alpha^2 a_2, \alpha^3 a_3, \dots)$.
(6) Dosazení x^n místo x $a(x^n)$ odpovídá $(a_0, \underbrace{0, \dots, 0}_{n-1}, a_1, \underbrace{0, \dots, 0}_{n-1}, a_2, \dots)$.
(7) Zderivováním $a(x)$ dostaneme $b(x) = a'(x)$ se členy $b_n = (n+1)a_{n+1}$, potom $a'(x)$ odpovídá $((n+1)a_{n+1})_{i=0}^{\infty}$.
(8) Integrování $\int_0^x a(t)\,\mathrm{d}t$ odpovídá $(0, a_0, \frac{1}{2}a_1, \frac{1}{3}a_2, \frac{1}{4}a_3, \dots)$.

Úlohy

Úloha 1. Matěj šel koupit barevné stužky na svou pomlázku. Má s sebou 8 jednokorun, 6 dvoukorun a 3 pětikoruny. Kolika způsoby může mincemi za stužky zaplatit 11 korun, aniž by mu pokladní musela vracet?

Úloha 2. Káťa se chystá péct beránky, mazance a jidáše. Ráda by připravila pro ostatní orgy košík sladkého pečiva, který bude obsahovat 7 kousků, nejvýše 3 beránky, sudý nenulový počet jidášů a alespoň 2 mazance. Kolika způsoby může napéct pečivo do košíku?

Úloha 3. Terka má 10 stejných kraslic, které chce rozdělit mezi své dva kamarády a dvě kamarádky. Kolika způsoby to může udělat, má-li každý kamarád dostat aspoň jednu kraslici a každá kamarádka nejméně dvě?

Úloha 4. Naty se chystá obarvit 25 vajíček, má 4 barvy, ale některé má raději než jiné. Chce mít maximálně jedno červené, nejvýše 10 modrých, alespoň 6 zelených a alespoň 8 žlutých. Kolika způsoby může všechna vajíčka nabarvit?

Úloha 5. Lenka se taky chystá barvit vajíčka 4 barvami. Má jich n a chtěla by, aby počet červených byl sudý, počet žlutých byl dělitelný pěti, nejvýše 4 byla oranžová a zelené bylo jedno nebo žádné vajíčko. Kolika způsoby se jí to může podřit?

Úloha 6. Najděte vytvořující funkce pro následující posloupnosti:

(1) $(1, -1, 1, -1, 1, -1, \dots)$,
(2) $(1, 0, 1, 0, 1, 0, \dots)$,
(3) $(1, 2, 3, 4, 5, 6, \dots)$,
(4) $(1, -1, 2, -2, 3, -3, 4, -4, \dots)$,
(5) $(2, 1, 4, 3, 6, 5, \dots)$,
(6) $(1, -3, 5, -7, 9, -11, \dots)$,
(7) $(1, 1, 2, 2, 4, 4, 8, 8, \dots)$,
(8) $(1^2, 2^2, 3^2, \dots)$.

Úloha 7. Petr a Radeček místo pletení pomlázek hrají kostky. Nejsou žádní troškaři a mají 12 hracích kostek. Jaká je pravděpodobnost, že při hodu všemi kostkami padne přesně 30?

Úloha 8. Najděte dvě nestandardní šestistěnné hrací kostky A a B, na jejichž stěnách jsou přirozená čísla, takové, že pro každé $n \in \mathbb{N}$ je pravděpodobnost, že na A a B padne dohromady přesně n, stejná jako pravděpodobnost, že n padne na dvou standardních šestistěnných hracích kostkách.

Úloha 9. Určete koeficient u příslušné mocniny x ve výrazech:

(1) u x^{15} v $(x^2 + x^3 + x^4 + \dots)^4$,
(2) u x^5 v $(1 - 2x)^{-2}$,
(3) u x^k v $\frac{1}{\sqrt{1-2x}}$ pro libovolné $k \geq 0$,
(4) u x^4 v $(x^2 - 5x + 6)^{-1}$.

Úloha 10. S pomocí vytvořujících funkcí sečtěte následující řady:

(1) $\sum_{k=0}^{n} \binom{n}{k}^2$,
(2) $\sum_{k=0}^{n} k\binom{n}{k}$,
(3) $\sum_{k=0}^{n} k^2\binom{n}{k}$.

Úloha 11. Posloupnost $a_0, a_1, a_2, \dots$ má generující funkci $g(x)$. Jakou generující funkci pak bude mít posloupnost částečných součtů $a_0, a_0 + a_1, a_0 + a_1 + a_2, \dots$?

Návody

1. Vyjádři hledaný počet jako koeficient u $x^1 1$ ve vhodném součinu mnohočlenů.

2. Vyjádři hledaný počet jako koeficient u x^7 ve vhodném součinu mnohočlenů.

3. Pro určení koeficientu u x^{10} použij zobecněnou binomickou větu.

4. $\frac{x^{14}(1+x)(1-x^{11})}{(1-x)^3} = (x^{14} + x^{15} - x^{25} - x^{26}) \sum_{i=0}^{\infty} \binom{i+2}{i} x^i$.

5. Najdi vytvořující funkci pro každou barvu.

6.

(1) Dosaď vhodné αx do vytvořujíc funkce pro posloupnost $(1, 1, 1 \dots)$.
(2) Dosaď vhodné x^n do vytvořujíc funkce pro posloupnost $(1, 1, 1 \dots)$.
(3) Derivace je kamarád.
(4) Rozlož na součet dvou posloupností, které umíš získat výše.
(5) Chytře rozlož na součet dvou posloupností.
(6) Zapomeň nejdřív na znaménka, najdi posloupnost všech sudých čísel.
(7) Rozlož na součet stejných posloupností, jedna je o pozici posunutá.
(8) Derivuj a derivuj ještě jednou.

7. Vytvořující funkce pro pravděpodobnosti součtů hozených ok je

$$P(x) = \frac{1}{6^{12}}(x + x^2 + \cdots + x^6)^{12}.$$

8. $(x + \cdots + x^6)^2 = x^2(x+1)(x^3+1)(x^2+x+1)(x^4+x^2+1)$.

9.

(1) Najdi nejprve kombinatorickou interpretaci, poté použijte úpravy vytvořujících funkcí a zobecněnou binomickou větu.
(2) Použij zobecněnou binomickou větu.
(3) Taky použij zobecněnou binomickou větu.
(4) Rozlož racionální lomenou funkci na parciální zlomky.

10.

(1) Použij konvoluci dvou posloupností.
(2) Vytkni n z kombinačního čísla.
(3) Vytknutím $n(n?1)$ z kombinačního čísla a použij předchozít variantu.

11. $\frac{1}{(1-x)} \cdot g(x)$.

Literatura a zdroje

Nemalá část přednášky je převzatá z příspěvku Generující funkce, jehož autorem je Kuba Löwit, kterému tímto děkuji.

[1] Jakub Löwit: *Generující funkce*, Branná, 2019.
[2] Filip Čermák: *Generující funkce*, sborník *i*KS, 2023.
[3] Eva Ondráčková: *Vytvořující funkce*, Prudká, 2002.

Dirichletův princip

Vít Hanika

Abstrakt. Podíváme se na jednoduché tvrzení zvané Dirichletův princip, které využijete při spoustě velmi různorodých úloh.

Věta. (Dirichletův princip) *Pokud umístíme $n+1$ předmětů do n přihrádek, budou alespoň v jedné přihrádce alespoň dva předměty.*

Jak tuto větu využít? Předpokládáme-li, že žádný člověk nemá na hlavě více než milión vlasů, a vzpomeneme-li si na hodiny zeměpisu, zjistíme, že v Praze nutně musí žít dva lidé s přesně stejným počtem vlasů. Podařilo se nám tedy bez práce dokázat, že existuje dvojice lidí s určitou vlastností. Ovšem Dirichletův princip nám nijak neporadí, jak tyto dva lidi najít. Ale tak už to v matematice chodí.

Položme si nyní otázku, kolik lidí se stejným počtem vlasů bychom určitě našli v celé České republice. Odpověď nám dá (opět při dostatečných znalostech reálií) následující zobecnění:

Věta. (Dirichletův princip, obecněji) *Pokud umístíme $kn+1$ předmětů do n přihrádek, bude alespoň v jedné přihrádce alespoň $k+1$ předmětů.*

Uveďme si ještě další možné zesílení našeho výchozího tvrzení. V úlohách ovšem většinou vystačíme s některou z předchozích verzí.

Věta. (Dirichletův princip, ještě obecněji) *Mějme přirozená čísla $n_1, n_2, \ldots, n_t$, množinu X s alespoň $1+\sum_{i=1}^{t}(n_i-1)$ prvky a její rozklad na množiny $X_1, X_2, \ldots, X_t$. Potom určitě existuje i takové, že X_i má alespoň n_i prvků.*

A ještě nekonečná verze:

Věta. (nekonečný Dirichletův princip) *Pokud umístíme nekonečně mnoho předmětů do konečně mnoha přihrádek, bude alespoň v jedné přihrádce nekonečně mnoho předmětů.*

Nyní už se vrhneme na úlohy, kde budeme toto tvrzení využívat. Vždy je klíčové rozmyslet si, co bude v úloze přestavovat „přihrádky“ a co rozmísťované předměty.

Úloha 1. V zásuvce je celkem 10 černých, 12 modrých a 8 šedých ponožek. Kolik jich musíme vytáhnout, abychom určitě měli alespoň jeden pár stejné barvy?

Úloha 2. Dokažte, že mezi 82 různými přirozenými čísly vždy najdu dvojici a, b tak, že $81 \mid (a-b)$.

Úloha 3. Ve čtverci 6 cm × 6 cm je náhodně rozmístěných 37 bodů. Dokažte, že vždy existuje čtverec 2 cm × 2 cm, ve kterém se nachází alespoň pět z nich.

(PraSe, 14. ročník)

Úloha 4. Mějme skupinu n lidí, z nichž některé dvojice se navzájem znají (známost je vzájemná). Ukažte, že existují dva lidé, kteří znají přesně stejný počet lidí.

Úloha 5. Dokažte, že pro libovolná celá čísla a, b, c, d je výraz

$$(a-b)(a-c)(a-d)(b-c)(b-d)(c-d)$$

dělitelný číslem 12.

Úloha 6. Na šachovnici 8×8 políček máme rozestavěných 33 věží. Najdeme mezi nimi pět takových, které se navzájem neohrožují? Dvě věže se navzájem ohrožují, pokud jsou ve stejném řádku nebo sloupci (i pokud je mezi nimi jiná věž).

(PraSe 20–3–1)

Úloha 7. Dokažte, že když vybereme 53 čísel z množiny $\{1, 2, \ldots, 100\}$, bude mezi nimi vždy dvojice čísel s rozdílem přesně 12.

Úloha 8. Vybereme-li v rovnostranném trojúhelníku o straně a libovolně 10 bodů, pak vzdálenost některých dvou vybraných bodů je nejvýše $\frac{a}{3}$. Dokažte.

Úloha 9. Ukažte, že z libovolné posloupnosti n přirozených čísel $a_1, \ldots, a_n$ dokážeme vybrat (neprázdnou) skupinu za sebou jdoucích prvků tak, aby jejich součet byl násobkem n.

Úloha 10. Hrací plán hry „Člověče, nezlob se“ obsahuje 36 políček uspořádaných do kruhu. Kolik nejméně figurek musí být ve hře, abychom vždy mohli některou z nich vyřadit pomocí jiné nezávisle na jejich rozložení a výsledku hodu kostkou?

(PraSe 20–3–2)

Úloha 11. Do políček tabulky 10×10 zapíšeme libovolná celá čísla tak, aby se žádná dvě čísla, která spolu sousedí ve stejném řádku nebo sloupci, nelišila o více než 5. Dokažte, že v tabulce se vždy najdou dvě stejná čísla.

Úloha 12. Dokažte, že z libovolné pětice vrcholů pravidelného devítiúhelníku umíme jeden odstranit tak, aby zbylé čtyři tvořily vrcholy lichoběžníku.

Úloha 13. Dokažte, že pro všechna nesoudělná čísla a a b je desetinný rozvoj $\frac{a}{b}$ buď konečný, nebo má periodu maximálně $b-1$.

Úloha 14. V rovině je rozmístěno $2n+1$ bodů tak, že žádné z nich netvoří trojúhelník se všemi stranami delšími než 1. Dokažte, že nalezneme $n+1$ bodů, které je možno uzavřít do kružnice s poloměrem 1.

Úloha 15. Po čtvercovém stole 1 m × 1 m leze 51 much. Ukažte, že s pomocí kruhového hrnce s poloměrem $\frac{1}{7}$ m můžeme chytit alespoň 3 mouchy jednou ranou.

Úloha 16. New York je kromě jiného známý i pravidelností svých ulic – má 151 severojižních a 151 východozápadních ulic, které se vždy po 100 metrech kříží. Ve městě je rozmístěno celkem 11401 telefonních automatů (ne nutně na křižovatkách). Dokážeme tam najít dva automaty, které jsou od sebe vzdálené maximálně 200 metrů chůze po chodníku? (PraSe 20–3–3)

Úloha 17. Dokažte, že mezi libovolnými osmi složenými přirozenými čísly menšími než 360 existují vždy dvě čísla, která mají společného dělitele.

(PraSe, 14. ročník)

Úloha 18. Dokažte, že z každé $(n+1)$-prvkové podmnožiny $\{1, 2, \ldots, 2n\}$ lze vybrat dvě různá čísla tak, že jedno dělí druhé. (PraSe 20–3–7)

Úloha 19. Najděte co nejdelší aritmetickou posloupnost s diferencí 60, jejíž všechny prvky jsou prvočísla. (PraSe 18–1–1)

Úloha 20. Dokažte, že pro libovolné přirozené číslo n existuje jeho přirozený násobek složený jen z cifer 0 a 1. Dokážete toto tvrzení nějak zesílit?

V následujících dvou úlohách se skrývají věty, v jejichž důkazech je klíčem Dirichletův princip:

Úloha 21. (Dirichletova věta o aproximaci) Pro každé reálné číslo a a kladné číslo n existují celá čísla p, q tak, že $1 \leq q \leq n$ a $|aq - p| \leq \frac{1}{1+n}$.

Úloha 22. (Erdősova–Szekeresova věta) Z každé posloupnosti n^2+1 různých čísel dokážeme vybrat rostoucí nebo klesající podposloupnost délky alespoň $n+1$.

Úloha 23. Během přednášky, na kterou přišlo právě 5 účastníků, každý právě dvakrát usnul. Zároveň pro každou dvojici účastníků existoval okamžik, kdy spali oba současně. Ukažte, že někdy spali tři účastníci najednou.

Úloha 24. Je dána nekonečná rostoucí posloupnost přirozených čísel taková, že $a_1 = 1$ a $a_{n+1} \leq 2n$ pro všechna $n > 1$. Dokažte, že pro každé přirozené m existují dva členy posloupnosti, jejichž rozdíl je m.

Úloha 25. Dokažte, že z libovolného šestnácticiferného čísla umíme vybrat neprázdnou skupinu za sebou jdoucích cifer, jejíž ciferný součin je druhou mocninou celého čísla. (PraSe 28–5–7)

Úloha 26. Na přímce p leží postupně 6 úseků $u_1, u_2, \ldots, u_6$ s délkami po řadě $d_1, d_2, \ldots, d_6$, které jsou po dvou disjunktní. V jedné polorovině určené přímkou p sestrojíme body $S_1, S_2, \ldots, S_6$ tak, že vrchol S_i tvoří spolu s úsečkou u_i rovnostranný trojúhelník $(i = 1, 2, \ldots, 6)$. Nakonec vytvoříme kruhy se středy v bodech $S_1, S_2, \ldots, S_6$ a poloměry $d_1, d_2, \ldots, d_6$. Dokažte, že neexistuje bod, který by ležel ve všech šesti kruzích. (PraSe 28–5–6)

Úloha 27. Mějme v rovině n bodů $x_1, \ldots, x_n$ v obecné poloze[1], přičemž některé z těchto bodů jsou spojené úsečkami. *Stupněm* bodu x_k budeme nazývat počet spojnic, které z něho vedou. Dokažte, že pokud žádné dva body stejného stupně nemají společného „souseda“ a navíc je alespoň jedna dvojice bodů spojená úsečkou, pak nutně existuje bod, jehož stupeň je 1. (PraSe, 14. ročník)

Úloha 28. Ukažte, že existuje přirozené číslo N tak, že každé přirozené číslo $a > N$ dokážeme „osekat“ z krajů na přirozený násobek čísla 2011.

(Kanadská MO 2011)

Úloha 29. Majda se snaží vyvolat TeMné VelePraSe podle příručky černé magie, kterou nalezla v knihovně. Už má na zemi nakreslenou kružnici, jejíž každý bod je obarven jednou z 2022 barev. Další krok obřadu vyžaduje, aby našla lichoběžník, jehož vrcholy leží na této kružnici a mají všechny stejnou barvu. Dokažte, že se jí to může vždy podařit bez ohledu na to, jak jsou body kružnice obarveny.

(PraSe 42-1-8)

Úloha 30. Ve skupině 90 dětí má každé aspoň 30 kamarádů (kamarádství je vzájemné). Dokažte, že je lze rozdělit do tří 30členných skupin tak, aby každé dítě mělo ve své skupince alespoň jednoho kamaráda. (Celostátní kolo MO 2011/2012)

Úloha 31. Ukažte, že je možné obarvit prvky množiny $\{1, 2, \ldots, 1987\}$ čtyřmi barvami tak, aby nešlo najít jednobarevnou desetiprvkovou aritmetickou posloupnost. (IMO Shortlist 1987)

Úloha 32. Pravidelnému 432-úhelníku bylo 108 vrcholů obarveno červeně, 108 zeleně, 108 modře a zbylých 108 žlutě. Dokažte, že je možné najít čtyři shodné trojúhelníky takové, že vrcholy jednoho jsou všechny červené, druhého žluté, třetího modré a čtvrtého zelené. (USAMO 2012)

Úloha 33. Mějme v prostoru n bodů ($n \geq 3$), přičemž jejich spojnice jsou různě dlouhé a r z těchto úseček je obarvených. Dokažte, že potom z těchto obarvených spojnic umíme vytvořit tah[2] z alespoň $\lceil \frac{2r}{n} \rceil$ úseček, ve kterém délka úseček narůstá.[3]

(PraSe 17–2–5)

Návody

1. Na počtu ponožek od jednotlivých barev nezáleží.

2. Podívej se na zbytky po dělení 81.

3. Rozděl čtverec na 9 menších.

4. Může někdo znát 0 a někdo jiný $n - 1$ lidí?

5. Vyřeš zvlášť dělitelnost 3 a 4.

6. Rozděl šachovnici na 8 částí.

---

[1] Množina bodů je v *obecné poloze*, pokud žádné tři z nich neleží na přímce.

[2] *Tah* je posloupnost na sebe navazujících hran, které se neopakují. Mohou se křížit.

[3] Symbol $\lceil x \rceil$ označuje *horní celou část* čísla x, tedy nejmenší celé číslo y, takové že $x \leq y$.

7. Kolik nejvýše čísel může dávat jaký zbytek?

8. Vhodně rozděl trojúhelník.

9. Podívej se na skupiny začínající prvním prvkem posloupnosti.

10. Kolik nejvýše figurek může ohrožovat jedno políčko?

11. O kolik se mohou nejvýše čísla lišit?

12. Tři dvojice vybraných vrcholů mají stejnou vzdálenost.

13. Kolik je možných zbytků po dělení b?

14. Najdi nejvzdálenější body. Ostatní rozděl do dvou skupin.

15. Chceme 25 přihrádek.

16. Ve městě je 22 801 křižovatek.

17. Každé z čísel má v rozkladu prvočíslo menší než 19.

18. Jedno z čísel je dokonce 2^k-násobek jiného.

19. Zkoumej modulo 7.

20. Stačí dokonce dvě cifry 1. Tedy, skoro vždy.

22. Jak dlouhá je nejdelší rostoucí posloupnost končící daným číslem? A klesající?

23. Máme 10 časových intervalů, kde spali právě dva, každý začíná usnutím účastníka.

24. Koukni se na prvních $m + 1$ členů.

25. Nula tam není. Máš 4 prvočísla, $2^4 = 16$.

26. $30 \cdot 6 = 180$.

27. Podívej se na bod s největším stupněm.

28. Stačí sekat z jedné strany.

29. Podívej se na pravidelný N-úhelník a rozmysli si, co to znamená, že body tvoří lichoběžník.

30. V kolika z možných rozdělení nemáš ve skupině žádného kamaráda?

31. Kolik je možných aritmetických posloupností?

32. Přihrádky jsou rotace.

33. Najdi $2r$ věcí a n přihrádek.

Literatura a zdroje

Příspěvek je téměř zcela převzat od *Vaška Janáčka* z roku 2021, který zase hojně využíval příspěvek *Kuby Krásenského* z roku 2013, oběma tímto děkuji.

Konečné automaty

Petr Hladík

Abstrakt. Jedním z hlavních objektů, které zkoumá teoretická informatika, jsou Turingovy stroje. Protože o Turingových strojích je ale za jednu přednášku obtížné dokázat cokoli zajímavého, podíváme se na jejich (o několik stupňů) slabší brášky – konečné automaty.

V teoretické informatice často řešíme, jak složité je pro různé množiny řetězců rozhodnout, který řetězec do nich patří a který ne. Abychom ale mohli mluvit o řetězcích, musíme nejprve nadefinovat terminologii.

Definice. Konečné množině znaků budeme říkat *abeceda* a budeme ji značit Σ. Abeceda může být například $\{a, b, c, \ldots, z\}$, ale taky třeba množina obsahující #, @, § a !. My však budeme nejčastěji používat binární abecedu $\{0, 1\}$, či dokonce unární abecedu obsahující pouze nulu nebo pouze jedničku. Prvkům abecedy budeme říkat *znaky abecedy*, nebo prostě *znaky*. *Řetězec* (nebo taky *slovo*) pak bude konečná (klidně prázdná) posloupnost znaků. *Délkou řetězce* w budeme rozumět počet jeho znaků a budeme ji značit $|w|$. Řetězec délky 0 (prázdné slovo) budeme značit ε. Máme-li řetězce u a v, budeme uv nebo $u \cdot v$ značit jejich zřetězení, tedy řetězec w takový, že $|w| = |u| + |v|$ a ve w jsou nejprve všechny znaky u v tom samém pořadí jako v u a potom obdobně všechny znaky v. Podobně budeme u^k pro $k \in \mathbb{N}_0$ značit řetězec u k-krát zřetězený sám za sebe (tedy například zápisem $1(10)^3$ budeme rozumět řetězec 1101010). Pro řetězec u budeme u^R značit ten samý řetězec pozpátku. Máme-li řetězec w, tak pro $k \in \mathbb{N}$, $k \leq |w|$ budeme $w[k]$ značit k-tý znak řetězce w.

Dále budeme potřebovat terminologii a značení mluvící o množinách řetězců. Dovolíme si jistou formální nepřesnost a budeme tam, kde to dává smysl, volně zaměňovat řetězec s jednoprvkovou množinou, která obsahuje právě tento řetězec.[1]

Dovolíme si podobně, jako zřetězujeme řetězce, zřetězovat i množiny. Tedy například $\{0, 1\} \cdot \{2, 3\} = \{02, 03, 12, 13\}$. Dále pokud M je množina řetězců, M^* budeme značit libovolný počet opakování něčeho z M, tedy $M^* = \{\varepsilon\} \cup M \cup M^2 \cup M^3 \cup \cdots$ Například Σ^* je tedy množina všech možných konečných řetězců nad abecedou Σ. $\{01, 02\}^*$ obsahuje například ε, 01, 01020102, ale ne 010.

[1] Také budeme zaměňovat znak a řetězec délky jedna obsahující právě tento znak.

Definice. *Jazykem* nad abecedou Σ budeme rozumět množinu $L \subseteq \Sigma^*$. Jejím prvkům budeme říkat *slova* jazyka L.

Příkladem jazyka nad abecedou $\{0, 1\}$ může být například množina všech řetězců reprezentujících prvočíslo, množina všech řetězců, které reprezentují ve dvojkové soustavě číslo menší než 42. Nebo množina všech řetězců, které začínají jedničkou.

Konečné automaty

Nyní již konečně máme vše, co potřebujeme, abychom nadefinovali konečný automat.

Definice. *Konečným automatem* nad abecedou Σ rozumíme konečnou množinu *stavů* Q společně s *přechodovu funkcí* $\delta : Q \times \Sigma \to Q$. Právě jeden ze stavů označíme jako počáteční a některé stavy označíme jako přijímající (jejich množinu značíme F).

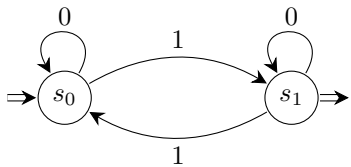
Výpočet konečného automatu nad řetězcem w probíhá následovně: Automat začne v počátečním stavu q_0. Poté přečte první znak řetězce $w[1]$ a přejde do stavu $q_1 = \delta(q_0, w[1])$ (ne nutně různého od q_0). Dále přečte znak $w[2]$ a přejde do stavu $q_2 = \delta(q_1, w[2])$. Tak pokračuje, dokud nepřečte poslední znak w a nepřejde do stavu $s_{|w|}$. Pak řekneme, že automat řetězec w přijal, právě když výpočet skončil v přijímajícím stavu, tedy pokud $s_{|w|} \in F$.

Definice. *Jazyk $L(A)$ přijímaný automatem A* je množina všech slov z Σ^*, které automat přijme.

Průběh výpočtu si tedy můžeme představit tak, že automat čte řetězec znak po znaku a do svého stavu si ukládá nějakou informaci o tom, co už přečetl. Ve většině případů si však například nemůže uložit celou část řetězce, kterou už přečetl, protože jeho stav může nabývat jen konečně mnoha různých hodnot, kdežto řetězce můžou být obecně libovolně dlouhé.

Pro přehlednost budeme typicky automat nezadávat přímo, ale orientovaným grafem, kde vrcholy odpovídají stavům automatu a orientované hrany označené znaky abecedy odpovídají přechodové funkci.

Úloha 1. Mějme například automat nad abecedou $\{0, 1\}$, který má množinu stavů $\{s_0, s_1\}$, kde s_0 je počáteční stav a s_1 jediný přijímající stav. Dále ať přechodová funkce říká, že při přečtení nuly zůstaneme v témže stavu a při přečtení jedničky přejde do druhého z možných stavů. Tento automat by též šel popsat následujícím obrázkem:



Jaký jazyk automat na obrázku vlastně přijímá?

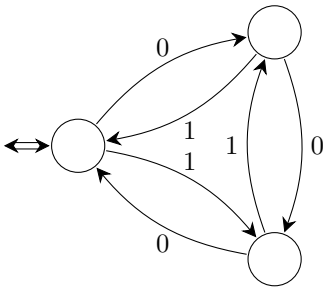
Úloha 2. Nakreslete konečný automat nad abecedou $\{0, 1\}$, který přijímá právě slova začínající 01. Co slova končící 01?

Úloha 3. Nakreslete konečný automat nad abecedou $\{0, 1\}$, který přijímá právě ta slova, která reprezentují binární zápis sudého čísla. Co čísla dělitelná trojkou?

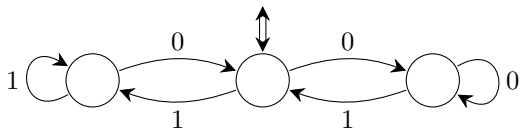
Úloha 4. Nakreslete konečný automat nad abecedou $\{0, 1\}$, který přijímá právě slova se sudým počtem nul. Pak nakreslete automat, který přijímá ta, v nichž je počet jedniček dělitelný třemi. Nakonec najděte automaty, které přijímají slova splňující alespoň jednu z těchto vlastností, respektive obě tyto vlastnosti.

Úloha 5. Rozhodněte, jaké jazyky přijímají následující automaty:

(a)



(b)



Nedeterminismus

Doteď jsme měli pouze konečné automaty, které vždy věděly, co mají dělat. Co kdybychom jim ale dali na výběr?

Definice. *Nedeterministickým konečným automatem* nad abecedou Σ rozumíme konečnou množinu *stavů* Q společně s *přechodovou funkcí* $\delta : Q \times (\Sigma \cup \{\lambda\}) \to \mathcal{P}(Q)$.

Některé stavy označíme jako *počáteční* a některé jako *přijímající*. Množinu všech počátečních značíme S a množinu všech přijímajících F.

Výpočet nedeterministického konečného automatu nad řetězcem w probíhá následovně: Automat začne v nějakém počátečním stavu $q_0 \in S$. Poté přečte první znak řetězce $w[1]$ a přejde do nějakého stavu $q_1 \in \delta(q_0, w[1])$ (ne nutně různého od q_0). Případně může také nečíst znak a přejít do nějakého stavu z množiny $\delta(q_0, \lambda)$ (a v příštím kroku pokračovat ve čtení tam, kde předtím skončil – tomu říkáme, že automat využil λ-přechod). Takto pokračuje ve výpočtu, dokud nepřečte poslední znak a případně ještě nevyužije nějaké λ přechody. Řekneme, že automat řetězec w *přijímá*, pokud existuje výběr počátečního stavu a stavů v průběhu výpočtu takový, že automat skončí v nějakém stavu z F.

Pokud během výpočtu nastane situace, že je automat ve stavu q, čte znak z a $\delta(q, z) = \emptyset$, výpočet se považuje za nepřijímající.

Zajímavé je, že přidání nedeterminismu nijak nezvyšuje sílu konečných automatů – pořád pomocí nich umíme přijímat jen ty samé jazyky jako s konečnými automaty.

Věta. *Pro každý nedeterministický konečný automat existuje deterministický konečný automat, který přijímá ten samý jazyk.*

Myšlenka důkazu. Nejprve si rozmyslíme, že λ přechody umíme odstranit poměrně jednoduše. Potom sestrojíme konečný automat, jehož stavy jsou všechny podmnožiny množiny stavů původního nedeterministického automatu. Rozmyslete si, jak nadefinovat přechodovou funkci. □

Úloha 6. Nakreslete nedeterministický konečný automat nad abecedou $\{0, 1\}$, který přijímá právě slova končící 01, a převeďte ho na deterministický.

Regulární jazyky a pumping lemma

Definice. O jazyku řekneme, že je *regulární*, pokud existuje konečný automat, který přijímá právě tento jazyk.

Úloha 7. Dokažte, že pro libovolné dva regulární jazyky L_1, L_2 nad abecedou Σ a jazyk L, který obsahuje všechna slova z abecedy Σ, jsou jazyky $L_1 \cup L_2$, $L_1 \cap L_2$, $L \setminus L_1$ také regulární.

Úloha 8. Rozmyslete si, že libovolný konečný jazyk je regulární.

Zatím jsme pouze konstruovali automaty, ale chyběly nám prostředky, jak dokázat, že nějaký jazyk regulární není. K tomu nám poslouží pumping lemma.

Věta. (pumping lemma) *Pro každý regulární jazyk L existují konstanty k a ℓ, takové, že pro každé slovo $u \in L$, kde $|u| \geq \ell$, existují řetězce w, x a y, takové, že:*

- $u = w \cdot x \cdot y$,
- $|w \cdot x| \leq k$,
- $|x| \geq 1$,
- *pro každé $n \in \mathbb{N}_0$ je slovo $w \cdot x^n \cdot y$ také v jazyce L.*

Myšlenka důkazu. Máme-li regulární jazyk, pak existuje konečný automat, který ho přijímá. Tento automat má $|Q|$ stavů a je nad $|\Sigma|$-prvkovou abecedou, takže pokud má slovo alespoň $|Q| \cdot |\Sigma| + 1$ znaků, musí se z Dirichletova principu nějaká kombinace čteného znaku a stavu stroje zopakovat (dokonce již mezi prvními $|Q| \cdot |\Sigma| + 1$ znaky). Část slova mezi těmito opakováními je ale možné vynechat či naopak libovolně mnohokrát zopakovat, protože pokud stroj čte týž znak a je v témže stavu, bude se vždy chovat stejně bez ohledu na to, co již přečetl. □

Příklad. Rozhodněte, zda jazyk $L = \{0^j \mid j \text{ je mocnina dvojky}\}$ je regulární.

Řešení. Jazyk regulární není. Pro spor připusťme, že by regulární byl. Pak existují k a ℓ s vlastnostmi ze znění pumping lemmatu. Najdeme n takové, že $2^{n-1} > \max(k, \ell)$. Pak slovo 0^{2^n} lze rozdělit na slova w, x a y podle pumping lemmatu. Protože ale $k < 2^{n-1}$, tak $1 \leq |x| < 2^{n-1}$, tedy $w \cdot y = w \cdot x^0 \cdot y$ je v L, ale současně $2^{n-1} < |w \cdot y| < 2^n$, což je ve sporu s definicí L. Jazyk L tedy není regulární.

Úloha 9. O následujících jazycích rozhodněte, zda jsou regulární: (Prostředky, které k tomu máte, jsou pumping lemma a uzavřenost regulárních jazyků na doplněk, průnik a sjednocení.)

(1) $L_1 = \{0^p \mid p \text{ je prvočíslo}\}$,
(2) $L_2 = \{0^n \cdot 1^m \mid n, m \in \mathbb{N}\}$,
(3) $L_3 = \{0^n \cdot 1^n \mid n \in \mathbb{N}\}$,
(4) $L_4 = \{0^n \cdot 1^m \mid n, m \in \mathbb{N}, n > m\}$,
(5) $L_5 = \{0^n \cdot 1^m \mid n, m \in \mathbb{N}, n \neq m\}$,
(6) $L_6 = \{w \cdot w^R \mid w \in \{0,1\}^*\}$.

Úloha 10. Nechť K_1 a K_2 jsou regulární jazyky. Pak rozhodněte, zda jsou následující jazyky regulární (pro každou volbu K_1 a K_2):

(1) $L_1 = \{w \mid w^r \in K_1\}$,
(2) $L_2 = \{w^* \mid w \in K_1\}$,
(3) $L_3 = K_1^*$ (tento příklad se od předchozího liší tím, že v předchozím případě se požaduje, aby w bylo pořád stejné, zde se za sebe můžou řetězit různá slova K_1),
(4) $L_4 = \{w \cdot v \mid w \in K_1, v \in K_2\}$,
(5) $L_5 = \{w \cdot v \mid v \cdot w \in K_1\}$.

Návody

5. (a) Podívej se, kolik jedniček a kolik nul mají přijímaná slova.
(b) Co se stane, když přijdou dva stejné znaky po sobě?

7. Jazyky L_1 a L_2 jsou regulární, tedy existuje konečné automaty, které je přijímají. Zkus z nich tedy vyrobit automat, který by přijímal jazyky $L_1 \cup L_2$ a $L_1 \cap L_2$. Bude se Ti hodit rozmyslet si, jak vypadá „kartézský součin“ dvou automatů.

9. Jazyk L_2 je jediný regulární. V části (5) si uvědom, že doplněk L_5 je jazyk všech řetězců, které vypadají jinak, než nějaké nuly a pak jiný počet jedniček. Kdyby ale L_5 byl regulární, je regulární i jeho doplněk a následně průnik jeho doplňku s L_2, což je přesně L_3. V části (6) si můžeme vzít například $w = 0^n \cdot 1$ pro nějaké dostatečně vysoké n.

10. Jazyk L_2 není regulární, myšlenka důkazu je podobná L_6 z Úlohy 8. Ostatní regulární jsou, popiš konstrukci nedeterministického automatu. L_5 zkus vyřešit nejdřív pro v a w pevné délky.

Literatura a zdroje

Příspěvek je upravenou verzí přednášky od *Michala Töpfera* z Lipové-lázně na jaře 2022, kterému tímto děkuji.

[1] Michal Töpfer, *Konečné automaty*, Lipová-lázně, 2022.

Fibonacciho čísla

Václav Janáček

Abstrakt. Příspěvek definuje Fibonacciho čísla a ukáže jejich základní vlastnosti. Obsahuje také množství úloh k procvičení.

Definice. *Fibonacciho čísla* jsou posloupnost celých čísel definovaná následující rekurencí:

$$\begin{aligned} F_0 &= 0, \\ F_1 &= 1, \\ F_{n+2} &= F_{n+1} + F_n. \end{aligned}$$

Několik prvních Fibonacciho čísel je: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ...

Příklad. (Fibonacciho králíci) V lednu si pořídíme jeden pár čerstvě narozených králíků. Víme, že králíci začnou plodit potomky dva měsíce po narození, porodí přitom další pár králíků každý měsíc. Kolik králíků budeme mít na konci roku? Kolik za dva roky?

Řešení. V únoru budeme mít stále jeden pár. V březnu se nám narodí 2 nový králíčci. V dubnu už budeme mít 3 páry. A co v květnu? Zůstanou nám všechny páry, které jsme měli v dubnu. Navíc páry, které jsme měli v březnu, porodí nové potomky. Budeme tedy mít tolik králíků, co v březnu a dubnu dohromady, tedy 5.

Všimněme si, že to přesně odpovídá definici Fibonacciho čísel. V lednu máme $F_1 = 1$ párů, v prosinci to bude $F_{12} = 144$ párů. Po dvou letech již budeme mít 92736 králíků.

Příklad. Kolika způsoby je možné vydláždit obdélník o rozměrech $1 \times (n-1)$ pomocí dlaždic 1×2 a 1×1?

Věta. (Binetova formule)

$$F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right] = \frac{\varphi^n - \psi^n}{\sqrt{5}}.$$

Důkaz. Pro důkaz stačí ověřit, že formule splňuje definici Fibonacciho čísel, tedy rekurzivní rovnost $F_{n+2} = F_{n+1} + F_n$ a platnost pro $n = 0$ a $n = 1$. Podrobné rozepsání si můžete vyzkoušet jako cvičení. □

Úlohy

Úloha 1. Kolika způsoby můžeme vyjít schodiště o n schodech, pokud lze každým krokem nejvýše jeden schod vynechat?

Úloha 2. Kolika způsoby je možné vydláždit obdélník o rozměrech $2 \times n$ pomocí dlaždic 1×2?

Úloha 3. Dokažte, že počet možností, jak vyskládat tabulku $(n+1) \times 1$ dílky většími než 1×1, je F_n.

Úloha 4. Dokažte, že počet posloupností nul a jedniček o délce n, které neobsahují dvě nuly vedle sebe, je roven F_{n+2}

Úloha 5. Dokažte, že $4n$-té Fibonacciho číslo je dělitelné třemi.

Úloha 6. Dokažte, že pro $n > 1$ platí $F_{n+5} > 10F_n$.

Úloha 7. Ukažte, že platí $F_1^2 + F_2^2 + F_3^2 + \cdots + F_n^2 = F_n \cdot F_{n+1}$.

Úloha 8. Dokažte $F_1 + F_3 + \cdots + F_{2n-1} = F_{2n}$.

Úloha 9. Ukažte, že platí $F_1 + F_2 + \cdots + F_n = F_{n+2} - 1$.

Úloha 10. Dokažte, že pro každé $n \geq 4$ platí $F_n^2 = 2F_{n-1}^2 + 2F_{n-2}^2 - F_{n-3}^2$.

Úloha 11. Ukažte, že $F_{n+m} = F_{n+1} \cdot F_m + F_n \cdot F_{m-1}$.

Úloha 12. Dokažte, že $F_k \mid F_{nk}$.

Úloha 13. (Cassiniho identita) Ukažte, že $F_{n-1} \cdot F_{n+1} = F_n^2 + (-1)^n$.

Úloha 14. Určete hodnotu $\displaystyle\sum_{n=2}^{\infty} \frac{F_n}{F_{n-1} \cdot F_{n+1}}$.

Úloha 15. Dokažte $F_{n+1} = \displaystyle\sum_{k=0}^{\lceil n/2 \rceil} \binom{n-k}{k}$.

Literatura a zdroje

Tento příspěvěk je z velké části převzatý z příspěvku Fibonacciho čísla od *Aničky Mlezivové*, které tímto děkuji.

[1] Calda Emil: *Sbírka řešených úloh*, Prometheus, 2006.

[2] Polster Burkard: *Q.E.D. Krása matematického důkazu*, Dokořán, 2014.

[3] Mirek Olšák: *Kombinatorické (Ne)počítání*, Hostětín, 2013.

[4] *Cut The Knot*, *http://www.cut-the-knot.org/arithmetic/combinatorics/FibonacciTilings.shtml*.

[5] *Wolfram Math World*, *http://mathworld.wolfram.com/FibonacciNumber.html*.

MO-P

Lenka Kopfová

Abstrakt. I když MO-P znamená Matematická olympiáda, kategorie programování, k jejímu (úspěšnému) řešení není třeba umět programovat. Každé kolo je alespoň z části teoretické, přičemž teoretické úlohy jsou rozhodně blíže úlohám z matematické olympiády než nějaké práci s počítačem. Na přednášce si ukážeme, jak se dostat do celostátka MO-P jen s minimem práce.

Úvod

MO-P nemá ani zdaleka tolik řešitelů jako například MO kategorie A, což také znamená, že je jednoduché dostat se z domácího kola do krajského a ne tak těžké se dostat z krajského do celostátního. V posledních letech stačilo na postup z domácího kola do krajského ne více než 10 bodů ze 40 a z krajského kola do celostátního ne více než 20 bodů ze 40. Nenaučíme se, jak MO-P vyhrát ani jak vyřešit úlohy optimálně. Naučíme se pouze, jak vyřešit úlohy nějak, což pro postup do celostátka často stačí. Také se podíváme na specifické úlohy, u kterých je potřeba opravdu umět „jen“ matiku. A vůbec, vždyť se přeci jedná o inforMatiku.

Úloha 1. Dostaneme číslo a několik operací s ním (např. $+2$, $\cdot 6$, -100, $!$, ^{4}, ...) a chceme najít takovou posloupnost těchto operací (operace se vyhodnocují postupně zleva doprava), aby byl výsledek co největší.

Úloha 2. Máme posloupnost celých čísel a chceme najít takovou souvislou podposloupnost, aby měla co největší součet.

Úloha 3. Chceme vykrást zlatnictví. Každý předmět ve zlatnictví má cenu a váhu. My uneseme jenom m a chceme si vzít takové předměty, abychom si odnesli co největší bohatství.

Úloha 4. Máme posloupnost čísel a chceme je seřadit od nejmenšího po největší.

Co to vlastně je programování? O čem úlohy jsou?

> **Citát.** Napsal jsem tam, že vyzkoušíme všechny možnosti ve faktoriálové složitosti, a dostal jsem se na celostátko.
>
> (Totožnost autora výroku je redakci známa.)

Definice 5. (vágní) *Algoritmus* je posloupnost kroků, kterým řešíme danou úlohu. Má vstup a výstup. Vstup je třeba číslo, několik čísel, nějaký text, graf atd. V algoritmu můžete používat proměnné, konstanty, základní aritmetické operace a přiřazování. Navíc můžete používat podmínky (pokud je tohle pravda, udělej a, jinak b) a cykly (dokud je tohle pravda, dělej a).

Algoritmus můžeme zapsat pomocí pseudokódu. Pseudokód není formální kód, ale spíše nějaký zjednodušený jazyk, který více přibližuje ideu, jak by se daný algoritmus dal dále předat počítači. U následujících příkladů si zkuste rozmyslet, jakou úlohu asi řeší daný algoritmus.

Příklad 6.

1. Načti čísla a, b.
2. Nastav $c := 0$.
3. Dokud $b > 0$:
4. Nastav $c := c + a$.
5. Sniž b o 1.
6. Vrať c.

Příklad 7.

1. Načti posloupnost čísel $a[i]$ dlouhou n.
2. Nastav $b := -\infty$.
3. Pro každé i od 1 do n:
4. Pokud $a[i] > b$:
5.   Nastav $b := a[i]$.
6. Vrať b.

Příklad 8.

1. Načti posloupnost čísel $a[i]$ dlouhou n.
2. Nastav proměnnou $setrideno := 0$.
3. Dokud $setrideno$ je 0:
4. Pro každé i od 1 do $n - 1$:
5.   Nastav $setrideno := 1$.
6.   Pokud $a[i] > a[i + 1]$:
7.   Prohoď prvky $a[i]$ a $a[i + 1]$.
8.   Nastav $setrideno := 0$.
9. Vrať posloupnost $a[i]$.

Složitost aneb škrtáme konstanty

U úloh je třeba určit časovou a paměťovou složitost. Časová složitost znamená, kolik řádově operací program provede v závislosti na velikosti vstupu. Paměťová složitost znamená, kolik řádově zabere paměti v závislosti na velikosti vstupu. Velikost vstupu je typicky třeba počet čísel nějaké posloupnosti či počet vrcholů a hran nějakého grafu.

Zajímá nás pouze, „jak rychle ta časová složitost roste“, tzn. provede-li program například $3n^2 - n + 6$ kroků, chceme jen, že to roste řádově jako n^2. Potom říkáme, že časová složitost programu je v $\mathcal{O}(n^2)$.

Klasickými příklady časové složitosti jsou například (seřazeny od nejrychlejší po nejpomalejší):

(i) $\mathcal{O}(1)$ – konstantní,
(ii) $\mathcal{O}(\log n)$ – logaritmická,
(iii) $\mathcal{O}(n)$ – lineární,
(iv) $\mathcal{O}(n \log n)$,
(v) $\mathcal{O}(n^2)$ – kvadratická,
(vi) $\mathcal{O}(n^3)$ – kubická,
(vii) $\mathcal{O}(2^n)$ – exponenciální,
(viii) $\mathcal{O}(n!)$ – faktoriálová.

Cvičení 9. Určete časovou a paměťovou složitost u předchozích příkladů.

Úlohy

Úloha 10. (policajti a zloděj) Mějme tabulku $r \times s$ takovou, že její řádky jsou očíslovány 1 až r a sloupce 1 až s. Na začátku se na dvou polích nacházejí policajti a na jednom jiném poli zloděj. Policajti a zloděj se střídají v tazích, začínají policajti. Když se hýbou policajti, tak si každý zvlášť vybere jedno stranou sousední políčko a na to se přesune. Obdobně, když se pohybuje zloděj, může buď zůstat na místě, nebo se přesunout na sousední políčko. Policajti zloděje chytí, když alespoň jeden z nich dojde na pole, na které právě stojí zloděj. Jak mají policajti postupovat a povede se jim zloděje vždy chytit? (MO-P 73-I-3)

Úloha 11. (Petra lyžuje) Petra brzy vystartuje do druhého kola slalomu. Na trati je n branek očíslovaných zhora dolů od 1 po n. Pro každou branku známe pravděpodobnost p_i, že ji Petra projede čistě. Jaká je pravděpodobnost, že projede všemi brankami čistě až na nanejvýš dvě branky? (Chtěli bychom lineární složitost.)

(varianta MO-P 73-II-1 za 5 bodů)

Úloha 12. (míchání karet) Máme balíček n karet, který obsahuje čtyři esa. Bombur umí balíček karet zamíchat pouze jedním daným způsobem, a to pomocí permutace čísel $a_1, \ldots, a_n$. To znamená, že karta, která před zamícháním byla i-tá shora, bude po zamíchání a_i-tá shora. Na vstupu dostaneme danou permutaci a původní pozici čtyř es v balíčku. Zjistěte, kolik nejvýše es může být po několika (možná i nula nebo jedna) mícháních mezi vrchními pěti kartami a po kolika mícháních bude mezi vrchními pěti kartami tento počet es poprvé. (MO-P 65-II-3)

Úloha 13. (trojnohý běh) Ve třídě je n chlapců a n dívek. O každém z nich víme, jakou má rychlost. Na závod v trojnohému běhu z nich chceme sestavit n dvojic. Rychlost dvojice je určena nižší z rychlostí obou dětí, které tuto dvojici tvoří.

Úkol A: Navrhněte co nejefektivnější algoritmus, který zjistí, jaký nejvyšší může být součet rychlostí všech sestavených dvojic.

Úkol B: Navrhněte co nejefektivnější algoritmus, který zjistí, jaký nejnižší může být součet rychlostí všech sestavených dvojic. (MO-P 65-III-1)

Úloha 14. (ďábel) V pekle žije N čertů očíslovaných od 1 do N. Chceme zjistit, zda je mezi nimi nějaký ďábel. Ďábel je čert s vlastností, že se jej všichni ostatní bojí a zároveň on se nebojí žádného jiného čerta. Není předem známo, který čert se kterého bojí. Abyste to zjistili, můžete se pro libovolné dva čerty s čísly a, b zeptat, zda se čert a bojí čerta b. Je ovšem možné, že dva různí čerti se ani jeden druhého nebojí, nebo naopak se bojí jeden druhého navzájem. Navrhněte postup, jak pokládat jednotlivé dotazy, aby bylo možné co nejdříve určit, zda se v pekle nachází vhodný kandidát na ďábla. Jako kvalitu vašeho řešení budeme hodnotit počet dotazů v nejhorším případě v závislosti na hodnotě N. Oproti běžným úlohám nás tentokrát bude zajímat přesný počet dotazů, nikoliv jen asymptotický odhad.

(MO-P 64-II-2)

Úloha 15. (červené jablíčko) Pepa má 1000 jablek a ví, že jedno z nich je červené a všechna ostatní jsou zelená. Jelikož je však od narození červeno-zeleně barvoslepý, všechna jablka pro něj vypadají stejně. Už od rána má chuť na červené jablko a naštěstí k němu právě na návštěvu dorazil Vašek, který červené jablko od zelených rozlišit umí. Vašek chce ale Pepu trochu potrápit, a tak se rozhodl, že mu neřekne přímo, které jablko je červené. Místo toho může Pepa ukázat na kteroukoliv množinu jablek a Vašek mu prozradí, zda mezi nimi je to červené. Aby to měl Pepa ještě těžší, Vašek mu řekl, že může v nejvýše jedné odpovědi lhát. Nechť x je počet otázek, které smí Pepa položit. Vyřešte úlohu pro a) libovolné x, b) pro $x \leq 21$, c) pro $x \leq 14$.

(MO-P 71-II-2)

Úloha 16. (převracení prefixů) Mějme pole $A[1..n]$, v němž je uložena nějaká permutace čísel od 1 do n. V jednom kroku můžeme provést operaci $flip(k)$, která převrátí pořadí prvních k prvků v poli A.

(1) Nalezněte algoritmus s polynomiální časovou složitostí, který libovolné vstupní pole A uspořádá pomocí operací $flip$.

(2) David se rozhodl, že bude stále opakovat operaci $flip(A[1])$. V každém kroku se tedy podívá na první prvek pole A a následně převrátí pořadí tolika prvků, jakou hodnotu měl první prvek pole. Je pravda, že se pro každou hodnotu n a pro každou permutaci čísel v poli A dostane časem na začátek pole A číslo 1?

(varianta MO-P 67-I-3)

Úloha 17. (reverze) Na polici je vyznačeno n pozic a na každé z nich leží jedno jablíčko. Pozice jsou očíslovány zleva doprava čísly od 0 do $n-1$. Jablíčko na pozici i má velikost a_i. Všechna jablíčka mají navzájem různé velikosti. Chceme všechna jablíčka uspořádat podle velikosti od nejmenšího po největší. V místnosti s jablíčky máme mechanické rameno. Pomocí něho můžeme sebrat jablíčka z libovolného souvislého úseku police a vrátit je zpátky na polici na jejich původní místa, ale v opačném pořadí. Tuto operaci nazveme *reverze*. Každá reverze trvá stejně dlouho bez ohledu na to, jak dlouhý úsek obracíme. Chceme použít lineárně mnoho reverzí, najděte řešení s kvadratickou a poté lineární časovou složitostí. (MO-P 69-II-1)

Úloha 18. (řazení kamenů) Na počítači budeme hrát jednoduchou logickou hru. Do kruhu je rozloženo n hracích kamenů označených čísly od 1 do n. Úkolem hráče je tyto kameny přerovnat tak, aby byly uspořádány podle svých čísel. To znamená, že když vyjdeme z hracího kamene číslo 1 a půjdeme ve směru pohybu hodinových ručiček, postupně navštívíme kameny s čísly $2, 3, \ldots, n$. Hráč může měnit pořadí kamenů jediným způsobem: Když na některý kámen klikne, tento kámen se přesune po obvodu kruhu o k pozic proti směru pohybu hodinových ručiček. Vzájemné pořadí ostatních kamenů se přitom nezmění. Na vstupu jsou zadána čísla n, k a seznam čísel všech hracích kamenů v tom pořadí, v jakém po sobě následují na obvodu kruhu při pohybu ve směru hodinových ručiček. Můžete předpokládat, že $n > k+1$. Navrhněte algoritmus, který zjistí, zda lze v zadané pozici hru vyhrát pro $k = 1$, $k = 3$ a $k = 2$.

(MO-P 65-I-3)

Literatura a zdroje

Přednáška byla inspirována přednáškou *Matěje Konečného* o MO-P z roku 2015, kterému tímto děkuji. Dalšími užitečnými zdroji, kde se dá dozvědět něco o MO-P nebo se něco obecně přiučit o soutěžním programování, jsou:

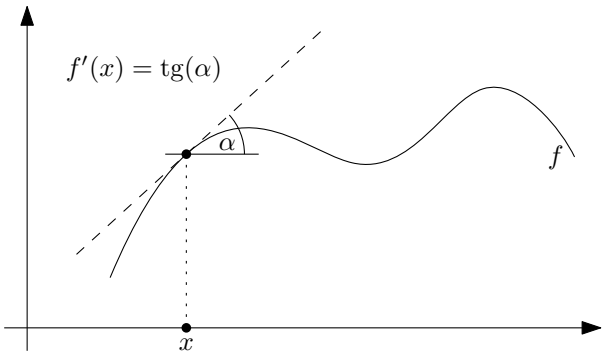
[0] Matěj Konečný: *MOP*, Sklené, 2015.
[1] KSP Kuchařky:
http://ksp.mff.cuni.cz/encyklopedie/kucharky/programatorske-kucharky.html.
[2] Stránky MO-P: *http://mo.mff.cuni.cz/p/*.
[3] Competitive Programmer's Handbook: *https://cses.fi/book/book.pdf*.
[4] Programátorská liaheň: *https://liahen.ksp.sk/*.
[5] CSES Problem Set, *https://cses.fi/problemset/*.
[6] Codeforces: *https://codeforces.com/*.

Derivace

Terka Kučerová

Abstrakt. Skamarádíme se s derivacemi, konkrétně s tím, jak je počítat. Do hluboké teorie nezabrousíme.

Budeme si povídat o derivacích, nebudeme si zavádět formální definici. Místo toho si derivaci pro nějakou funkci f představíme tak, že je to nějaká funkce f'. Tato funkce má super vlastnost, že v každém bodě x (kde je definovaná) nám určuje směrnici tečny na funkci f v bodě x.



Derivaci v bodě x funkce f můžeme značit různými způsoby, pro představu si uvedeme následující: $f'(x)$, $\frac{\mathrm{d}f}{\mathrm{d}x}(x)$.[1]

Derivace

Věta 1. (tabulka derivací) *Na celém definičním oboru příslušných funkcí platí tyto vztahy:*

(i) $(x^\alpha)' = \alpha x^{\alpha-1}$ *pro každé* $\alpha \in \mathbb{R}$,
(ii) $(e^x)' = e^x$,
(iii) $(\sin(x))' = \cos(x)$,
(iv) $(\cos(x))' = -\sin(x)$,
(v) $(\ln(x))' = \frac{1}{x}$.

[1] Co jsme si zde představili jsou tzv. první derivace, ovšem proces derivování můžeme opakovat. Druhou derivaci funkce f značíme f'' a dostaneme ji zderivováním funkce f'. Obdobně n-tou derivaci funkce f značíme f^n a spočítáme ji tak, že n-krát zderivujeme funkci f.

Věta 2. (aritmetika derivací) *Pro každou konstantu c a funkce f a g, pro něž výraz na pravé straně dává smysl, platí následující vztahy:*

(i) $(cf)'(x) = cf'(x)$,
(ii) $(f+g)'(x) = f'(x) + g'(x)$,
(iii) $(fg)'(x) = f'(x)g(x) + f(x)g'(x)$,
(iv) $(f \circ g)(x)' = f'(g(x))g'(x)$,
(v) $(f^{-1}(x))' = \frac{1}{f'(f^{-1}(x))}$.

Poznámka. (ke značení ve Větě 2)

(1) Symbolem $f \circ g$ myslíme složení funkcí f a g, tj. funkci definovanou vztahem $(f \circ g)(x) = f(g(x))$.
(2) Symbolem f^{-1} označujeme inverzní funkci k funkci f, pokud existuje.

Příklad. Zkusme pomocí předchozích vět spočítat derivaci funkce $2x^3$.

Řešení. K spočítání derivace funkce $f(x) = 2x^3$ nejprve použijeme bod (i) z Věty 2, čímž dostaneme, že platí $f'(x) = (2x^3)' = 2(x^3)'$. K spočítání derivace $(x^3)'$ použijeme bod (i) z Věty 1, dostaneme tak $(x^3)' = 3x^2$. Tudíž platí $f'(x) = (2x^3)' = 6x^2$.

Úloha 1. Radim a Petr by hrozně rádi spočítali derivace následujících funkcí, pomozte jim:

(a) $(1+x)^2$,
(b) $\sin(2x)$,
(c) $\sin^2(x) + \cos^2(x)$,
(d) $\mathrm{tg}(x)$,
(e) 2^x,
(f) $\arcsin x$,
(g) $\ln(\cos x)$.

Úloha 2. Matěje by zajímalo, jak vypadá vzorec pro derivování podílu dvou funkcí. Odvoďte ho.

Úloha 3. Lucia chce vědět, jak vypadá rovnice tečny k funkci $\frac{1-x}{x^2-3}$ v bodě $x = -2$.

Úloha 4. Ondra se rozhodl spočítat derivace následujících funkcí na celém definičním oboru, pomůžete mu?

(a) $f(x) = x^x$,
(b) $f^{(n)}$ pro $f(x) = x^n$.

Úloha 5. Erik, Johana a Pavel našli staré zápočtové písemky z Matematické analýzy I. Nelenili a vrhli se na počítání, spočtěte s nimi derivace následujících funkcí ve všech bodech, kde existují:

(a) $f(x) = e^{2x\sin(x)}(\sqrt{x} - \ln(x))$,
(b) $f(x) = \arctan(x^5\cos(x))$,
(c) $f(x) = \frac{\mathrm{tg}(x) - \sin(x^6)}{e^x}$.

Derivace a extrémy funkcí

Proč se nám hodí umět derivaci počítat? Jedním z důvodů je, že derivace nám toho o funkci může spoustu říct. Může nám napovědět, kde je funkce rostoucí a kde klesající. Stejně tak nám poradí, kde může mít funkce lokální extrém (minimum nebo maximum).

Věta 3. *Jestliže má funkce f v bodě x kladnou derivaci, pak je na nějakém jeho okolí*[2] *ostře rostoucí. Pokud má derivaci zápornou, je naopak na nějakém okolí ostře klesající.*

Důsledek 4. *Jestliže má funkce f v bodě x lokální extrém*[3] *(minimum nebo maximum), pak derivace v tomto bodě buď neexistuje, nebo je nulová.*

Úloha 6. David, Matúš a Helča se nudí, a tak by je zajímalo, ve kterých bodech můžou mít následující funkce extrémy (maximum či minimum):

(a) 1,
(b) $x^3 + x^2 + 7x + 15$,
(c) $\sin$,
(d) $\cos$,
(e) 3^x,
(f) $xe^{-x^2/2}$.

Úloha 7. Verča našla lokální maximum funkce $\ln(2x) - x$, najdete ho taky?

Úloha 8. Pomožte Markétě a derivováním zjistěte, kde leží vrchol paraboly dané rovnicí $f(x) = ax^2 + bx + c$.

Derivace a slovní úlohy

Úloha 9. Tomáš si chce na břehu rovné řeky oplotit obdélníkovou zahradu tak, že na straně přilehlé k řece žádný plot nebude. Má k dispozici 800 m pletiva. Jakou největší plochu může mít jeho zahrada?

Úloha 10. Anna by si přála mít krabici ve tvaru kvádru o rozměrech a, b a c, kde c je výška krabice, a a b určují rozměry dna krabice. Poměr $a : b$ je roven Anninu oblíbenému kladnému α. Jak má dosáhnout co největšího objemu, pokud

(a) povrch nesmí překročit zadané S,
(b) součet rozměrů $a + b + c$ nesmí překročit zadané x?

Úloha 11. Z čtvercového papíru o straně 30 cm vystřihne Terka v rozích čtyři stejné čtverečky a zbytek přehne tak, aby vznikla otevřená krabice. Jak velké čtverečky má Terka odstřihnout, aby se do krabice vešlo, co nejvíce třpytek?

[2] Okolí bodu je interval, jehož je bod středem.
[3] Tím se myslí extrém na nějakém okolí.

Úloha 12. Marek si otevřel továrnu na čokoládu. Jednu tabulku čokolády prodává za 20 Kč, ale při objednávce nad 60 tabulek dává slevu na jednu tabulku ve výši 0,2 Kč, přičemž tato sleva se kumuluje. (Tedy 61. tabulka stojí 19,8 Kč, 62. tabulka už 19,6 Kč atd.) Doprava za jednu krabici Marka stojí paušálně 600 Kč a navíc ještě 3,2 Kč za každou přibalenou tabulku čokolády.

Richard od něj chce odkoupit krabici s objemem mezi 60 a 90 tabulkami čokolády. Poraďte Markovi, jak na Richardovi co nejvíce vydělat.

Úloha 13. Lucian se rozhodl, že vyrobí domeček pro mravence ve tvaru kvádru, domeček má objem 100 cm^3. Lucian by chtěl, aby jedna strana dna jeho domečku byla poloviční oproti druhé. Dno domečku je vyrobeno ze dřeva a stěny ze skla. Pomozte mu domeček vyrobit co nejlevněji, pokud víte, že centimetr čtvereční dřeva stojí 10 Kč a centimetr čtvereční skla stojí 6 Kč.

Derivace a funkce více proměnných

Pokud máme funkci více proměnných, pak se při derivování musíme rozhodnout, podle které z proměnných budeme tuto funkci derivovat.

Příklad. Spočítejte parciální derivace funkce $f(x, y) = x^2 + xy + y^3$.

Řešení. Když máme funkci $f(x, y) = x^2 + xy + y^3$, pak její derivaci podle proměnné x značíme $\frac{\partial f}{\partial x}$ a platí pro ni $\frac{\partial f}{\partial x} = 2x + y$. Všimněme si, že když derivujeme podle proměnné x, tak proměnou y považujeme za konstantu. Toto platí obecně u funkcí více proměnných: ty proměnné, podle kterých zrovna nederivujeme, jsou považovány za konstanty. Obdobně tedy pro derivaci podle y dostaneme $\frac{\partial f}{\partial y} = x + 3y^2$.

Úloha 14. Michal a Tomáš mají funkci $f(x, y) = x^2 + y^2$, pomozte jim spočítat, čemu se rovná derivace podle proměnné y v bodě $(1, 2)$.

Úloha 15. Kuba, Dominik a Jakub se rozhodli spočítat parciální derivace podle všech proměnných u následujících funkcí:

(a) $f(x, y) = \frac{\sin(y^2)}{x}$,
(b) $f(x, y, z) = \arcsin(\frac{y}{x}) + z^2$,
(c) $f(x, y) = (x + y)^y$.

Literatura a zdroje

Tento příspěvek se inspiroval následujícími starými přednáškami. Je rozšířený o některé úlohy a naopak mu byly ubrány zase nějaké jiné.

[1] Terka Kučerová, *Derivace*, Lipová-lázně, 2022.
[2] Kuba Krásenský, *Derivace (s trochou mýdla)*, Zásada, 2017.

Geometrie čtyřúhelníka

Radek Olšák

Abstrakt. Většinou se v geometrii zajímáme trojúhelníkem. Ukážeme si, že čtyřúhelník skrývá opravdu hodně tajuplných tvrzení, a dokonce, že nám pomůže i v těch trojúhelníkových úlohách.

Pokud neřekneme jinak, budeme používat následující značení. Máme čtyřúhelník $ABCD$. Dále $P = AB \cap CD$, $Q = AD \cap BC$ a $R = AC \cap BD$. Pokud je $ABCD$ tečnový, tak I značí jeho vepsiště, a pokud je tětivový, tak O je jeho opsiště.

Tvrzení 1. (Miquelův bod) *Kružnice*[1] (PAD), (QDC), (PBC), (QAB) *prochází jedním bodem, ten značíme* M. *Pokud je* $ABCD$ *tětivový, tak* M *leží na* PQ *a přímka* RO *je kolmá na* PQ.

Tvrzení 2. (o kamarádech) *Bod* X *v čtyřúhelníku má kamaráda právě tehdy, když* $|\sphericalangle AXB| + |\sphericalangle CXD| = 180°$.

Tvrzení 3. (Newtonova [Gaussova] přímka)

(1) *Středy úseček* AC, BD, PQ *na ní leží.*
(2) *Každý bod* X *na ní splňuje*[2] $[XAB] + [XCD] - [XAD] - [XCB] = 0$.
(3) *Uvažme všechny dvojice kamarádů* (K, L). *Pak Newtonova přímka je množina všech středů* KL.
(4) *Je množina středů všech vepsaných kuželoseček* $ABCD$.
(5) *Pokud je* $ABCD$ *tečnový,* I *na ní leží.*
(6) *Pokud je* $ABCD$ *tětivový, tak průsečík os* $\sphericalangle AQB$ *a* $\sphericalangle BPC$ *na ní leží.*

Tvrzení 4. (Aubertova [Steinerova] přímka)

(1) *Ortocentra trojúhelníků* PAD, PBC, QAB, QDC *na ní leží.*
(2) *Je kolmá na Newtonovu přímku.*
(3) *Kružnice nad průměry* AC, BD, PQ *prochází dvěma pevnými body* P_{l1} *a* P_{l2} *nazývanými Plückerovy body. Tyto body leží na Aubertově přímce.*
(4) *Pokud je* $ABCD$ *tětivový,* R *na ní leží.*
(5) *Překlopíme* M *podle přímek* AB, BC, CD, AD. *Tím dostaneme další čtyři body na Aubertově přímce.*

[1] (XYZ) značí kružnici opsanou trojúhelníku XYZ.
[2] $[XYZ]$ značí orientovaný obsah trojúhelníka XYZ.

Tvrzení 5. (konstrukce dvojstředových čtyřúhelníků) *Tečnový čtyřúhelník s body dotyku K, L, M, N je tětivový právě tehdy, když $KM \perp LN$.*

Tvrzení 6. (Clawson-Schmidt) *Uvážme $\sqrt{ac}$-inverzi v trojúhelníku MAC a označme ji φ. Pak pokud bod K má v $ABCD$ kamaráda L, platí $\varphi(K) = L$.*

Tvrzení 7. (konstrukce Clawson-Schmidt) *Mějme bod K. Označme K' druhý průsečík kružnic (ABK) a (CDK). Označme L druhý průsečík kružnic (BCK') a (ADK'). Pak $\varphi(K) = L$.*

Tvrzení 8. (kamarádské čtyřúhelníky) *Mějme (K, L), (G, H) dvojice kamarádů. Pak čtyřúhelník $KGLH$ sdílí s $ABCD$ Miquelův bod, Clawson-Schmidta a Newtonovu přímku.*

Tvrzení 9. *Uvažme množinu dvoustředých čtyřúhelníků $ABCD$ sdílejících kružnici vepsanou i opsanou. Pak sdílí i průsečík úhlopříček.*[3] *A platí, že průsečík úhlopříček leží na OI.*

Úloha 10. (lemma o kinklajícím úhlu) Mějme bod A a skrz něj přímky p_1, p_2. Mimo ně leží bod B. Skrz B se točí přímky q_1, q_2 tak, že úhel $|\sphericalangle q_1 q_2|$ je pevný. Označme $X = q_1 \cap p_1$ a $Y = q_2 \cap p_2$. Pak z definice body A a B vidí dvojici X, Y pod pevným úhlem. Dokažte, že existuje třetí bod s touto vlastností. (iKS–4–G6)

Úloha 11. Mějme trojúhelník ABC. Bod P je takový, že PB a PC jsou tečny k (ABC). Na AB a AC leží X, Y tak, že $|\sphericalangle XPY| = 2|\sphericalangle BAC|$ a P leží uvnitř AXY. Překlopíme A podle XY na Z. Dokažte, že (XYZ) prochází pevným bodem nezávisle na X, Y. (CPS 2020)

Úloha 12. Mějme trojúhelník ABC. Přímka p protne jeho strany BC, AC, AB postupně v X, Y, Z. Dokažte, že středy AX, BY, CZ leží na přímce.

Úloha 13. Mějme trojúhelník ABC. Označme D, E, F paty výšek postupně z vrcholů A, B, C. Uvnitř trojúhelníka leží bod P. Kružnice (ADP) protne BC podruhé v K, (BEP) protne AC podruhé v L, (CFP) protne AB podruhé v M. Dokažte, že K, L, M leží na přímce.

Úloha 14. Mějme čtyřúhelník $ABCD$. Označme O průsečík úhlopříček a P průsečík AB a CD. Mějme rovnoběžníky $AODE$ a $BOCF$. Dokažte, že E, F, P leží na přímce.

Úloha 15. Mějme trojúhelník ABC a přímku p. Ta protne BC, CA, AB v X, Y, Z. Překlop X, Y, Z podle středů stran ABC, na kterých leží na X', Y', Z'. Dokažte, že přímka $X'Y'Z'$ je rovnoběžná s Newtonovou přímkou $ABCp$.

Literatura a zdroje

[1] EQF: *https://chrisvantienhoven.nl/mathematics/encyclopedia.*

[3] Aneb důkaz Ponceletova porismatu pro $n = 4$.

Hrátky s nekonečnem

Radek Olšák

Abstrakt. Nekonečno je krásný matematický objekt, který často není intuitivní. Ukážeme si jak nad nekonečny uvažovat a jak pomocí nich PraSátka uhodnou náhodná reálná čísla o kterých nic neví, nebo jak pomocí nich dokázat konečná tvrzení.

Úvod

Příklad. (existence nejmenších/největších prvků) Kdykoli si vezmeme konečnou množinu reálných čísel, najdeme v ní největší i nejmenší prvek. U nekonečné množiny se to stát může, ale nemusí. Například uzavřený interval $\langle 0, 1\rangle$ má nejmenší prvek 0 a největší prvek 1, zatímco otevřený interval $(0, 1)$ nemá ani nejmenší, ani největší prvek.

Příklad. (libovolně velké není nutně nekonečné) Existuje libovolně dlouhá klesající posloupnost přirozených čísel. Pokud si usmyslíme, že chceme posloupnost délky n, sestrojíme ji coby $n, (n-1), \ldots, 2, 1$. Naopak nekonečná klesající posloupnost $a_0, a_1, a_2, \ldots$ přirozených čísel existovat nemůže.

Příklad. (Hilbertův Hotel)[1]

(1) Nekonečno +1 je stále nekonečno.
(2) Nekonečno +100 je stále nekonečno.
(3) Nekonečno + nekonečno je stále nekonečno.
(4) Nekonečno krát nekonečno je stále nekonečno.

Příklad 1. Lze nekonečnou čtverečkovou síť celou obarvit dvěma barvami, šedou a bílou, tak, aby každý řádek obsahoval jen konečně mnoho šedých políček a každý sloupec jen konečně bílých políček?

Definice. (dobře uspořádaná množina) Množina je dobře uspořádaná, pokud je lineárně uspořádaná a neexistuje v ní nekonečná klesající posloupnost.

Tvrzení. *Každá množina jde dobře uspořádat.*

[1] Pod nekonečnem zde si představ nějakou hodnotu počtu, která je větší než všechny konečné.

Axiom výběru, aneb tvůrce nemožných strategií.

Úloha 2. Zlý vlk chytil nekonečno PraSátek a postavil každé z nich na jedno přirozené číslo tak, že každé vidí všechna PraSátka na vyšších číslech. Každému pak dal na hlavu klobouk s nějakým reálným číslem. Každé PraSátko pak pošeptalo vlkovi reálné číslo. PraSátka vyhrají pokud všechna, až na konečně mnoho, pošeptají vlkovi číslo co mají na hlavě. Můžou si domluvit strategii aby dokázali vždy vyhrát?

Úloha 3. Stejná úloha jako předchozí, jen Vlk PraSátka nepostavil na přirozená čísla, ale na libovolnou dobře uspořádanou množinu.

Úloha 4. V řadě stojí 100 PraSátek a na hlavách mají klobouky 5 různých barev. Vidí všechny PraSátka před sebou a od zadu říkají nahlas tipy na barvu svého klobouku. Jakou si mají domluvit strategii, aby se nejvýše jedno z nich spletlo?

Úloha 5. Stejná úloha jako předchozí, ale PraSátek je nekonečno a stojí v řadě očíslované přirozenými čísly. Každé vidí všechna vyšší. Znovu najděte strategii takovou, aby se nejvýše jedno z nich spletlo.

Úloha 6. TeMnokněžník má v paláci tajemnou komnatu s nekonečno truhlami očíslovanými přirozenými čísly a v každé z nich je nějaké reálné číslo. Ve svém vězení vězní 100 PraSátek a rozhodl se, že jim dá možnost dostat se na svobodu. Každé PraSátko nezávisle na ostatních vejde do tajemné komnaty, tam si může libovolně otevřít nějaké truhly, klidně i nekonečně mnoho, a podívat se dovnitř. Následně musí ukázat na truhlu, kterou neotevřelo a tipnout si jaké je v ní reálné číslo. Pokud se trefí, je propuštěno na svobodu. Před vstupem dalšího PraSátka TeMnokněžník vrátí komnatu do původního stavu a tedy si PraSátka nemohou předávat žádnou informaci. Dokáží si PraSátka domluvit strategii aby se nejvýše jedno z nich spletlo?

Úloha 7. Stejná úloha jako předchozí, ale PraSátek je také nekonečno (očíslované přirozenými čísly). Dokáží si domluvit strategii aby

(1) Všechna až na konečně mnoho z nich se strefilo?
(2) Všechna až na jedno se strefí?

Úloha 8. Máme n PraSátek a každé dostane na hlavu klobouk jedné z mnoha barev. Všechny vidí barvy všech ostatních. Následně si každé z nich napíše na lísteček konečný seznam tipů jakou barvu klobouku má na sobě. Vyhrají pokud se alespoň jedno z nich trefí. Ukažte, že pro ně existuje výherní strategie pokud barev je $(n-1)$-tá nejmenší nekonečná množina. Počet přirozených čísel je 1. nejmenší nekonečná množina.

Poznámka: Použijte, že k-tou nejmenší nekonečnou množinu M můžeme mít dobře uspořádanou tak, že pro každý její prvek c je množina všech prvků $S = \{x : x \leq c\}$ ostře menší než M, tedy neexistuje bijekce mezi S a M.

Úloha 9. Existuje hra pro dva hráče, kde oba mají úplnou informaci, hra není náhodná a při tom ani jeden z nich nemá neprohrávající strategii?

Axiom výběru a dobré uspořádání, aneb nemožná konstrukce se prostě nějak udělá.

Následující úlohy jsou nad rámec jedné přednášky, ale přesto je zajímavé se podívat jaké styly věcí TeMno umí. Pokud vás o nich zajímá více, doporučuji se podívat na videoseriál Mirka Olšáka odkázaný v literatuře.

Úloha 10. Existuje množina bodů v rovině, taková, že na každé přímce leží právě dva?

Úloha 11. Existuje množina bodů v rovině, kterou každá kružnice protne právě ve třech bodech?

Úloha 12. Existuje množina kružnic v rovině taková, že každá přímka se dotýká právě dvou?

Úloha 13. Jde prostor $\mathbb{R}^3$ vyplnit pomocí disjunktních kružnic?

Kompaktnost, aneb libovolné je totéž co nekonečné.

Úloha 14. Máme množinu polyomin. Víme o nich, že jdou vyskládat do roviny tak, že zakryjí libovolně velký čtverec (můžou přečuhovat ven). Dokažte, že už pak pomocí nich lze vyskládat celá rovina.

Úloha 15. Mějme graf na vrcholech očíslovaných přirozenými čísly takový, že každý jeho konečný podgraf je obarvitelný čtyřmi barvami, pak celý graf jde obarvit pomocí čtyř barev.

Věta. (nekonečná Ramseyova) *Mějme graf na vrcholech očíslovaných přirozenými čísly. Jeho hrany jsou obarveny dvěma barvami. Pak existuje nekonečná podmnožina vrcholů taková, že všechny hrany mezi nimi jsou jednobarevné.*

Věta. (konečná Ramseyova) *Pro každé k (velikost jednobarevné množiny kterou chceme najít) existuje n (počet vrcholů) takové, že ať jsou hrany grafu na n vrcholech obarveny libovolně dvěma barvami, existuje množina k vrcholů taková, že všechny hrany mezi nimi jsou jednobarevné.*

Úloha 16. (nekonečný Ramsey implikuje konečného) Dokažte, že pokud platí nekonečná Ramseyova věta, tak platí konečná. A jako bonus si tu nekonečnou dokažte :-).

Úloha 17. (nekonečný Hall) Mějme bipartitní graf, kde obě partity A, B mají vrcholy očíslovány přirozenými čísly a každý vrchol má konečný stupeň. Ukažte, že pokud pro každou konečnou podmnožinu $A' \subseteq A$ platí, že má alespoň $|A'|$ sousedů v B, tak už existuje perfektní párování A a B.

Poznámka: Použijte, že pokud A a B jsou konečné a $|A| \geq |B|$, tak úloha platí z Hallovy věty.

Návody

1. Rozděl diagonálami na čtyři části.

2. Rozděl všechny posloupnosti reálných čísel do přihrádek tak, že v přihrádce se každé dvě posloupnosti liší jen na konečně mnoha pozicích (shodují se v nekonečném konci). Z každé takové přihrádky vyber jednu posloupnost jako reprezentanta a toho si PraSátka budou tipovat.

3. Vezmi množinu všech posloupností reálných čísel (odpovídající přiřazeným kloboukům) a dobře ji uspořádej. Každé PraSátko si pak vždy tipne nejmenší možnou posloupnost podle toho co vidí. Ukaž, že kdyby se jich spletlo nekonečno, tvořili by nekonečnou klesající posloupnost.

4. První řekne součet ostatních modulo 5.

5. Pomocí úlohy 1 se strefí všechny až na konečně mnoho, první řekne nápovědu pro těch konečně mnoho co by se jinak spletlo o kolik se spletou.

6. Každé PraSátko bude mít vlastní posloupnost krabic. Podívá se na nekonečný konec své posloupnosti a pak si tipne podle reprezentanta nějaký dřívější člen. Nejdříve si ale prohlédne posloupnosti ostatních PraSátek a podívá se jak daleko se jejich posloupnosti liší od reprezentanta.

7. (1) PraSátko se podívá na posloupnosti všech ostatních PraSátek a na nejmenší index od které se už vždy shodují s reprezentantem. Na těhle indexech budou hrát hru jako v úloze 1.
(2) Zkombinuj se strategií z předchozí úlohy pro těch konečně co se splete.

8. Umíš to pro $n = 2$? Umíš vyšší n převést na nižší? Předpokládej, že jedno z PraSátek co vidíš má nejvyšší barvu.

9. Přečti si PraSečí seriál :-).

14. Postupně vybírej větší a větší pokrytí, která rozšiřují ty předchozí. Dej si pozor aby ti nedošly.

15. Postupně vybírej větší a větší obarvení, která rozšiřují ty předchozí. Dej si pozor aby ti nedošly.

16. Předpokládej, že konečná Ramseyovka neplatí, tedy že pro nějaké k platí, že pro libovolný počet vrcholů existuje obarvení bez k-jednobarevné množiny. Zkonstruuj tak spor s nekonečnou Ramseyovkou. Pro důkaz nekonečné postupně zkonstruuj nekonečnou uspořádanou množinu vrcholů takovou, že z nich do vyšších vedou jen jednobarevné hrany.

Literatura a zdroje

[1] Mirek Olšák: *Do nekonečna a ještě dál.*
[2] Jakub Löwit: *Vězni, domorodci a kouzelníci*, Horní Lysečiny, jaro 2018.
[3] Mirek Olšák: *Esence teorie množin*, *www.youtube.com/@procdalsinazev*.

Diofantické rovnice

Daniel Perout

Abstrakt. Příspěvek seznamuje se základními technikami na řešení diofantických rovnic: zejména počítání s kongruencemi, rozkládáním, úpravou na čtverec a technikou nekonečného sestupu. Staví přitom na elementárních konceptech z teorie čísel jako jsou dělitelnost, zbytkové třídy a prvočísla.

Motivace

Co si představit pod slovním spojením diofantická rovnice? Jedná se o obyčejnou rovnici, hledáme však všechna její řešení v přirozených či celých číslech. Většina uvažovaných rovnic bude mít jen několik řešení (nebo žádná), proto se naučíme metody, kterými lze výrazně omezit počet kandidátů na řešení.

Úmluva. Ve všech příkladech budeme hledat všechna řešení dané rovnice a budeme uvažovat, že $a, b, c, d \in \mathbb{N}$, p, q jsou prvočísla a $x, y, z \in \mathbb{Z}$.

Kongruence

Pod tímto děsivým názvem se skrývá velice mocný nástroj. Se zbytkovými třídami po dělení určitým (kladným celým) číslem lze totiž provádět podobnou aritmetiku jako s normálními čísly – ale s tím rozdílem, že zbytkových tříd máme jen konečně mnoho. Pokud se totiž má v nějaké rovnosti levá strana rovnat pravé, musí se rovnat i zbytky obou stran po dělení libovolným číslem. Nalezením vhodného čísla tak často můžeme řešení velice zjednodušit nebo o rovnici dokonce říci, že řešení nemá.

Příklad. $3x^2 + 6x + 2 = 391$. (Pikomat 2018)

Řešení. Rovnici si upravíme na $3x^2 + 6x = 389$ a vidíme, že její levá strana je zřejmě dělitelná třemi, zatímco číslo 389 není.

Úloha 1. $x^2 + x = 2y + 1$.

Úloha 2. $7x^2 + 5y + 14 = 0$.

Úloha 3. $2^x = 11 + 7y$.

Úloha 4. $p^2 = 2q^2 + 1$. (PraSe 26–2–2)

Úloha 5. $2^p + p^2 = q$. (PraSe 35–2j–2)

Úloha 6. $a^6 + b^4 + c^2 = 1234567.$ (PraSe 7–3–3)

Rozlož to!

Zadaná rovnice se dá mnohdy pěkně upravit na součin. Pokud je navíc na jedné straně prvočíslo nebo nějaké konkrétní číslo, pak rovnou známe všechny jeho rozklady. Nejprve si to ukážeme na příkladě.

Příklad. $p + 400 = a^2$ pro p prvočíslo. (PraSe 2012)

Řešení. Rovnici upravíme do tvaru $p = (a - 20)(a + 20)$. Protože p je prvočíslo, musí nutně platit $a - 20 = 1$ a také $a + 20 = p$. Z toho plyne $a = 21$ a $p = 41$, což je skutečně jediným řešením této rovnice.

Úloha 7. $x^2 = 4y^2 + 13.$

Úloha 8. $xy + yz + zx = xyz + x + y + z.$

Úloha 9. $a^2b + ab^2 = 2(a^3 + b^3).$ (PraSe 22–1–2)

Úloha 10. $a^2 = 9^b + 7.$

Úloha 11. $x^4 - 3x^2 + 9 = p.$ (MO 61–III–1)

Úprava na čtverec

Další užitečnou metodou je upravit jednu stranu rovnice na součet čtverců (druhých mocnin nějakých výrazů). Snažíme se mít na druhé straně nějaké konkrétní číslo – nejlépe záporné (rovnice pak nemá řešení), nebo malé přirozené (zbývá jen několik kandidátů na řešení rovnice).

Příklad. $x^2 + 2x + y^2 = 1.$

Řešení. Nejprve k oběma stranám rovnice přičteme jedničku – dostaneme $x^2 + 2x + 1 + y^2 = 2$. Dále si všimneme, že výraz na levé straně lze snadno upravit na čtverec: $(x + 1)^2 + y^2 = 2$. Jedinou možností, jak rozložit číslo 2 na součet dvou čtverců, je 1 a 1, tedy $(x + 1)^2 = 1$ a $y^2 = 1$, z čehož máme čtyři celočíselná řešení: $x \in \{-2, 0\}, y \in \{-1, 1\}$.

Úloha 12. $x^2 + 2xy + 2y^2 + 6y = 1.$

Úloha 13. $5x^2 + 4xy + 2y^2 - 2x + 4y = -5.$

Úloha 14. $x^2 + xy + y^2 = x^2y^2.$

Po sobě jdoucí mocniny

Tvrzení. *Neexistují x, y, a taková, že $x^a < y^a < (x + 1)^a$.*

Toto zdánlivě jednoduché tvrzení má překvapivě mnoho uplatnění. Pokud má být například nějaký výraz roven nějaké mocnině (a zdá se nám, že tomu tak není),

pokusíme se najít dvě po sobě jdoucí mocniny, které ho semknou ostře mezi sebe, a to nám zaručí neexistenci řešení.

Příklad. $a^2 = b^2 + b$.

Řešení. Pro každé přirozené číslo b platí: $b^2 < b^2 + b < b^2 + 2b + 1 = (b+1)^2$, tedy výraz $b^2 + b$ nemůže být čtvercem.

Úloha 15. $a^2 = 4b^2 + 3b + 2$.

Úloha 16. $a^2 = 4^b + 4b^2 + 4$. (MO 59–A–III–1)

Úloha 17. $a^2 + b^2 + c^2 + 2ab + 2a(c-1) + 2b(c+1) = d^2$.

Úloha 18. $3a + b + 1 = (a + b + c)(c - a - b)$. (Rumunsko)

Úloha 19. $(x+1)^4 = (x-1)^4 + y^3$. (Austrálie)

Nekonečný sestup[1]

Poslední metoda se opírá o poměrně jednoduché tvrzení:

Tvrzení. *Neexistuje nekonečná klesající posloupnost přirozených čísel.*

Když chceme ukázat, že daná rovnice nemá netriviální řešení, uvažujeme nějaké řešení a dokážeme (obvykle pomocí některé z předešlých technik), že pak umíme najít řešení, které je v nějakém smyslu „menší“. Obecně přiřadíme n-tici čísel přirozené číslo určující její velikost (například součet čísel v n-tici) a dokážeme, že umíme najít řešení s ostře menší velikostí. Takto nagenerujeme nekonečnou posloupnost řešení s klesajícími velikostmi, což dle předešlého nelze, tudíž žádné řešení neexistuje. Abychom tuto metodu pochopili, opět si ji ilustrujeme na příkladě.

Příklad. $a^3 + 2b^3 + 4c^3 = 2abc$.

Řešení. Předpokládejme, že (a, b, c) je řešením dané rovnice v přirozených číslech. Kdyby a bylo liché, tak bychom měli na levé straně liché číslo, ale na pravé straně je číslo sudé. Proto $a = 2d$, rovnici můžeme po dosazení upravit do tvaru $b^3 + 2c^3 + 4d^2 = 2bcd$. Našli jsme tedy řešení (b, c, d), ale jeho součet je ostře menší než součet v řešení (a, b, c). Jinými slovy: pokud máme nějaké řešení v přirozených číslech, umíme vyrobit řešení s menším a menším součtem. Z těchto součtů tak dostáváme nekonečnou klesající posloupnost přirozených čísel, což je ale ve sporu s předchozím tvrzením. Proto rovnice nemá v přirozených číslech řešení.

Úloha 20. $a^2 + b^2 = 7c^2$.

Úloha 21. Je $\sqrt{2}$ racionální?

Úloha 22. $x^4 + 4y^4 = 2(z^4 + 4w^4)$. (PraSe 12–2–2)

Úloha 23. $a^3 + 3b^3 + 9c^3 = 3abc$. (Kürschák)

[1] Též se označuje jako *Fermatova metoda* nekonečného sestupu.

Úloha 24. $x^2 + y^2 + z^2 = 2xyz.$ (Korea)

Návody

1. Modulo 2.

2. Modulo 5.

3. Modulo 7.

4. Modulo 3.

5. Modulo 3.

6. Modulo 8.

7. Uprav na $(x - 2y)(x + 2y) = 13$.

8. $(x - 1)(y - 1)(z - 1)$.

9. Převeď na jednu stranu a vytkni výraz $(a + b)$.

10. $a^2 - (3^b)^2$ je rozdíl čtverců.

11. Polynom na levé straně nemá reálné kořeny, zkus jej rozložit na dva kvadratické.

12. Doplň na čtverce: $(x + y)^2$ a $(y + 3)^2$.

13. Doplň na čtverce: $(2x + y)^2$, $(x - 1)^2$ a $(y + 2)^2$.

14. Přičti k oběma stranám xy a rozlož na součin.

15. Sevři mezi $(2b)^2$ a $(2b + 1)^2$.

16. Sevři mezi $(2^b)^2$ a $(2^b + 1)^2$.

17. Sevři mezi $(a + b + (c - 1))^2$ a $(a + b + (c + 1))^2$.

18. Uprav na $(a + b + 1)^2 = c^2 - a + b$. Sevři mezi $(a + b)^2$ a $(a + b + 2)^2$.

19. Sevři mezi x^3 a $(x + 1)^3$.

20. Dokaž, že pokud je (a, b, c) řešením, pak jsou a, b, c dělitelná sedmi a $(\frac{a}{7}, \frac{b}{7}, \frac{c}{7})$ je též řešením.

21. V podstatě řešíme diofantickou rovnici $\frac{a}{b} = \sqrt{2}$, neboli $a^2 = 2b^2$.

22. $2 \mid x, y, z, w$.

23. $3 \mid a, b, c$.

24. Jeden ze sčítanců vlevo musí být sudý. Ukaž, že sudí musí být všichni.

Literatura a zdroje

Tento příspěvek je sloučením příspěvků Luciena Šímy a Radovana Švarce, jejichž příspěvky jsou z velké části převzaty z přednášky Filipa Hláska. Všem zmíněným bych tímto chtěl poděkovat.

[1] Lucien Šíma: *Diofantické rovnice*, Horní Lysečiny, 2018.
[2] Rado van Švarc: *Úvod do diofantických rovnic*, Lipová-lázně, 2016.

Gaussovy a Jacobiho sumy

Zdeněk Pezlar

Abstrakt. Která čísla jsou čtverci modulo prvočíslo? A která čísla jsou modulo toto prvočíslo součtem čtverců? A kolik takových vyjádření existuje? Tyto přirozené otázky nás zavezou na výlet za velkou kopou krásné teorie, držte si klobouky!

Rozhodnout, zda kongruence $x^2 \equiv a \pmod{p}$ má řešení, je lehký počin pomocí teorie kvadratických zbytků. Co ale například kongruence $x^2 + y^3 \equiv a \pmod{p}$? Kolik vyhovujících dvojic bude existovat?

Nášup teorie na začátek

Definice. Pro p prvočíslo definujeme $\mathbb{Z}_p^*$ množinu všech nenulových zbytků po dělení p s operacemi násobení a sčítání.

Každý prvek je v této množině invertibilní, tedy $\mathbb{Z}_p^*$ je těleso. Následující fakt je o trochu méně jasný.

Věta. *V $\mathbb{Z}_p^*$ existuje primitivní prvek g, tj. takové g, že pro libovolné $a \in \mathbb{Z}_p^*$ existuje přirozené n takové, že $g^n \equiv a \pmod{p}$.*

Definice. Definujme $N(x^m = a)$ jako počet řešení rovnice $x^m = a$ v $\mathbb{Z}_p$.

Přirozená otázka je, kolik řešení má taková rovnice. Existence primitivního prvku nám zaručí, že tento problém můžeme velmi silně konkretizovat na dělitele $p-1$.

Tvrzení. *Pro $d = (m, p-1)$ platí $N(x^m = a) = N(x^d = a)$.*

Speciálně pro m nesoudělné s $p-1$ má daná rovnice vždy právě jedno řešení, tedy funkce příslušící mocnině $f(x) = x^m$ je na $\mathbb{Z}_p^*$ bijekce. To, asi uznáš, není zas tak zajímavé. Dále se proto podíváme na ty problémové mocniny.

Úloha 1. Dokažte, že pokud $p \equiv -1 \pmod{4}$, tak $p \mid x^2+y^2$ znamená $p \mid x$ a $p \mid y$.

Úloha 2. Dokažte, že pokud $p \equiv -1 \pmod{3}$, tak $p \mid x^2 + xy + y^2$ znamená $p \mid x$ a $p \mid y$.

Charaktery

Nyní budeme studovat mocniny, jejichž exponent dělí $p-1$. Než se do toho pustíme, definujme si tzv. charaktery, přirozená zobecnění například Legendreova symbolu.

Definice. O zobrazení $\chi : \mathbb{Z}_p^* \to \mathbb{C}^*$ řekneme, že je *charakter na* $\mathbb{Z}_p$, je-li splněno

$$\chi(a)\chi(b) = \chi(ab)$$

pro všechna $a, b \in \mathbb{Z}_p^*$, tedy χ zachovává operace násobení na $\mathbb{Z}_p^*$. Víc fancy řečeno, χ je homomorfismus mezi grupami $\mathbb{Z}_p^*$ a $\mathbb{C}^*$.

Příklad. Význačné charaktery jsou $\varepsilon(a) = 1$ pro každé $a \in \mathbb{Z}_p^*$ a Legendreův symbol definovaný následovně:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{pokud } p \mid a, \\ 1, & \text{pokud } a \not\equiv 0 \text{ a existuje } x \text{ takové, že } x^2 \equiv a \pmod{p}, \\ -1, & \text{jinak.} \end{cases}$$

Legendreův symbol lze spočítat jako $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Jeden malý podvod, co si povolíme, je definovat $\chi(0) = 0$, pokud $\chi \neq \varepsilon$ a $\varepsilon(0) = 1$. Můžeme pak uvažovat, že charaktery jsou definované na celém $\mathbb{Z}_p$.

Cvičení. Rozmysli si, že Legendreův symbol je charakter.

Pojďme si s charaktery nejprve trochu zacvičit. Jelikož charaktery jsou multiplikativní, platí pro libovolné $a \in \mathbb{Z}_p^*$ a primitivní prvek g takový, že $g^n \equiv a \pmod{p}$:

$$\chi(a) = \chi(g^n) = \chi(g)^n,$$

tedy χ je jednoznačně určené svou hodnotou v g. Charakterů tedy existuje právě $p-1$.

Tvrzení. *Pro charakter χ a $a \in \mathbb{Z}_p^*$ platí:*

(1) $\chi(1) = 1$,
(2) $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$,
(3) $\chi(a)^{p-1} = 1$.

Zbývá pár dalších definic a už se vrhneme na nějaká tvrzení.

Definice. Definujme *součin* charakterů χ a λ jako charakter $\chi\lambda$ splňující $\chi\lambda(a) = \chi(a) \cdot \lambda(a)$. *Řád* charakteru definujeme jako nejmenší n takové, že $\chi^n = \varepsilon$. Inverzní charakter χ^{-1} definujeme jako $\chi^{-1}(a) = \chi(a)^{-1} = \chi^{n-1}(a)$ pro každé $a \in \mathbb{Z}_p^*$.

Definice. Pro daný charakter χ definujeme jeho *sdružený charakter* $\overline{\chi}$ jako zobrazení splňující $\overline{\chi}(a) = \overline{\chi(a)}$ pro každé a.

Lemma. *Pro libovolné $a \in \mathbb{Z}_p^*$ existuje charakter λ na $\mathbb{Z}_p$ takový, že $\lambda(a) \neq 1$.*

Cvičení 3. Buď χ charakter na $\mathbb{Z}_p$. Pak $\sum_{t \in \mathbb{Z}_p} \chi(t) = p$, je-li $\chi = \varepsilon$, a 0 jinak.

Konečně, přichází věta, na kterou určitě čekáš. Vzorec na přesný počet odmocnin z daného čísla.

Lemma. *Buď $a \in \mathbb{Z}_p^*$ a $n \mid p-1$. Pokud $x^n \equiv a$ není řešitelné, potom existuje charakter χ takový, že $\chi^n = \varepsilon$ a $\chi(a) \neq 1$.*

Věta. *Buď $a \in \mathbb{Z}_p^*$ a $n \mid p-1$. Potom počet $x \in \mathbb{Z}_p^*$ takových, že $x^n = a$ je roven $\sum \chi(a)$, kde sčítáme přes všechny charaktery takové, že $\chi^n = \varepsilon$.*

Cvičení. Ověř si platnost předchozí věty na Legendreově symbolu.

Dobrý, co? Tím získáváme uspokojující odpověď na otázku, kolik řešení má kongruence $x^n \equiv a$. Co nám charaktery řeknou o komplikovanějších rovnicích, ku příkladu $y^2 = x^3 + b$?

Gaussovy sumy

V dobách dávno minulých se titáni jako Carl Gauss potýkali s otázkou, kdy je dané číslo kvadratickým zbytkem modulo p. Tato otázka má přirozené propojení s odmocninami z jedné, totiž pro $\omega = e^{\frac{2\pi}{3}}$, třetí odmocninu z jedné, platí

$$(\omega - \omega^2)^2 = -3,$$

tedy $\left(\frac{-3}{p}\right) = 1$ právě tehdy, když $\omega - \omega^2$ leží v $\mathbb{Z}_p$. Gauss nalezl analogický vztah pro pátou odmocninu z jedné ζ:

$$(\zeta - \zeta^2 - \zeta^3 + \zeta^4)^2 = 5,$$

kde ± 1 u sčítanců odpovídají tomu, zda daný exponent je kvadratickým zbytkem modulo 5, tedy koeficienty jsou Legendreovy symboly exponentů. Zobecněme tyto dva vztahy pro libovolný charakter.

Definice. Buď χ charakter na $\mathbb{Z}_p$ a $a \in \mathbb{Z}_p$. Definujme *Gaussovu sumu* $g_a(\chi) = \sum_{t \in \mathbb{Z}_p} \chi(t)\zeta^{at}$, kde ζ je primitivní p-tá odmocnina z jedné a $g(\chi) = g_1(\chi)$.

Úloha 4. Najděte podobný vztah pro dvojku. Jaké odmocniny použijete?

Úloha 5. Dokažte, že pro libovolný charakter platí $g_a(\overline{\chi}) = \overline{g_{-a}(\chi)}$.

Úloha 6. Dokažte, že pro $\chi \neq \varepsilon$ a $a \neq 0$ platí $g_a(\chi) = g(\chi)\overline{\chi}(a)$. Jak to vypadá, když $\chi = \varepsilon$ nebo $a = 0$?

Úloha 7. (těžší) Buď $\chi \neq \varepsilon$ charakter. Dokažte, že platí $|g(\chi)| = \sqrt{p}$.

Úloha 8. Buď χ Legendreův symbol. Dokažte, že platí $g(\chi)^2 = \left(\frac{-1}{p}\right)p$.

Jacobiho sumy

Příklad. Pojďme přitvrdit. Počítejme počet řešení rovnice $x^2 + y^2 \equiv 1 \pmod{p}$. To je rovno

$$\sum_{a+b=1} N(x^2 = a)N(x^2 = b) = \sum_{a+b=1} \left(1 + \left(\frac{a}{p}\right)\right)\left(1 + \left(\frac{b}{p}\right)\right),$$

což se pomocí cvičení 3 snadno upraví na

$$p + \sum_{a+b=1} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

V příkladu nám zbývá spočítat jednu jedinou sumu, pojďme se jí mrknout na zub.

Definice. Buďte χ a λ charaktery na $\mathbb{Z}_p$. Pak definujeme příslušnou *Jacobiho sumu*

$$J(\chi, \lambda) = \sum_{a+b=1} \chi(a)\lambda(b).$$

Jacobiho sumy jsou integrální při počítání počtů řešení různých rovnic. Ve zbytku přednášky si s nimi budeme hrát. Tak si pojďme hrát!

Úloha 9. Najděte počet řešení $x^3 + y^4 \equiv 1 \pmod{7}$.

Úloha 10. Spočítejte

(1) $J(\varepsilon, \varepsilon)$,
(2) $J(\varepsilon, \chi)$, kde $\chi \neq \varepsilon$,
(3) $J(\chi, \chi^{-1})$.

Úloha 11. Dokažte, že rovnice $x^2 + y^2 = 1$ modulo p má právě $p - (-1)^{\frac{p-1}{2}}$ řešení. Jakou Jacobiho sumu z předchozí úlohy využijete?

Úloha 12. Spočítejte počet řešení $x^2 + y^2 \equiv a \pmod{p}$ pro dané a.

Úloha 13. Najděte počet řešení rovnice $x^n + y^m \equiv 1 \pmod{p}$ v řeči Jacobiho sum.

Věta. (propojení Gaussových a Jacobiho sum) *Buďte χ a λ netriviální charaktery na $\mathbb{Z}_p$ takové, že $\chi\lambda \neq \varepsilon$. Pak*

$$J(\chi, \lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}.$$

Úloha 14. Buďte χ, λ netriviální charaktery na $\mathbb{Z}_p$ takové, že $\chi\lambda \neq \varepsilon$. Dokažte, že $|J(\chi, \lambda)| = \sqrt{p}$.

Úloha 15. Najděte počet řešení rovnice $y^2 \equiv x^3 + 1 \pmod{p}$ pomocí Jacobiho sumy.

Úloha 16. Pomocí vhodných Jacobiho sum dokažte, že pro $p \equiv 1 \pmod{4}$ existují celá a, b taková, že $p = a^2 + b^2$, a pro $p \equiv 1 \pmod{3}$ dokažte, že existují celá a, b taková, že $p = a^2 + ab + b^2$.

Úloha 17. Buď N počet řešení kongruence $x^3 + y^3 \equiv 1 \pmod{p}$. Dokažte, že platí $|N - p + 2| \leq 2\sqrt{p}$.

Úloha 18. Najděte podobný odhad jako v úloze výše pro rovnici $x^n + y^n \equiv 1 \pmod{p}$, kde $n \mid p - 1$.

Návody

1. $x^2 + y^2 = \frac{x^4 - y^4}{x^2 - y^2}$.

2. $x^2 + xy + y^2 = \frac{x^3 - y^3}{x - y}$.

3. Přenásob součet prvkem s $\chi(a) \neq 1$.

4. Vezmi součet dvou členů a vol tolikátou odmocninu, aby to vyšlo.

5. Jak se sdružují odmocniny z jedné?

7. Spočítej $\sum_a g_a(\chi)\overline{g_a(\chi)}$ dvěma způsoby.

8. Jaký je vztah mezi $\overline{g(\chi)}$ a $g(\overline{\chi})$? Využij předchozí úlohu.

9. Kterých hodnot nabývá x^3?

10. Jakých hodnot nabývá zlomek $\frac{a}{1-a}$ v $\mathbb{Z}_p$?

11. Legendreův symbol je svým vlastním inverzem.

12. Bacha na nulu!

13. Bude to součet $\sum_{i=1}^{n} \sum_{j=1}^{m} J(\chi^i, \lambda^j)$, kde χ, λ mají řády po řadě n a m.

15. Pro $p \equiv -1 \pmod{3}$ je to zjevné, pro $p \equiv 1 \pmod{3}$ počítej Jacobiho sumy.

16. Najdi charaktery takové, že příslušné Jacobiho sumy leží v $\mathbb{Z}[i]$ nebo $\mathbb{Z}[\omega]$.

17. Využij fakt, že Jacobiho suma má absolutní hodnotu $\sqrt{p}$ a odhaduj jednotlivé Jacobiho sumy.

Literatura a zdroje

[1] Ireland, Kenneth a Michael Rosen: *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics, Springer Verlag, 1990.

Kruhová inverze

Zdeněk Pezlar

Abstrakt. Velmi neambiciózně povězeno: tato přednáška Ti obrátí svět naruby. Hlavně teda kružnice.

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

Definice. Uvažme kružnici ω se středem O a poloměrem r. Pak *kruhovou inverzi* podle kružnice ω definujeme jako zobrazení, které

(i) Prohazuje body O a ∞,
(ii) Každý jiný bod roviny P zobrazí na bod P' ležící na polopřímce OP takový, že $|OP| \cdot |OP'| = r^2$.

Pokud neřekneme jinak, P' je obraz v inverzi podle kružnice ω se středem O a poloměrem r.

Cvičení. Rozmyslete si následující pozorování o kruhové inverzi podle kružnice ω:

(i) Body na kružnici ω se zobrazí samy na sebe.
(ii) Dvojí použití inverze je identita.
(iii) Vnitřek a vnějšek kružnice se zobrazí navzájem na sebe.

Nebudeme-li specifikovat poloměr kružnice a bude nás zajímat pouze střed inverze, řekneme, že invertujeme podle tohoto bodu.

Cvičení. Buďte A, $B \notin \{O, \infty\}$ dva body v rovině neležící na jedné přímce s O a A' a B' jejich obrazy. Pak A, B, A' a B' leží na kružnici.

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

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

(i) $|\sphericalangle OX'Y'| = |\sphericalangle XYO|$,
(ii) $|X'Y'| = |XY| \cdot \dfrac{r^2}{|OX| \cdot |OY|}$.

Tvrzení. (stěžejní) *Uvažme kruhovou inverzi určenou kružnicí k se středem O. Pak*

(i) *obrazem přímky procházející bodem O je ona sama,*

(ii) *obrazem přímky* **ne***procházející bodem O je kružnice procházející bodem O,*

(iii) *obrazem kružnice procházející bodem O je přímka* **ne***procházející bodem O,*

(iv) *obrazem kružnice* **ne***procházející bodem O je kružnice* **ne***procházející bodem O.*

Středy zobrazovaných kružnic se nezachovají!

Cvičení. Jak vypadají kružnice, které kruhová inverze zobrazí na sebe samotné?

Nyní už jen dodejme pár dobře míněných rad a už mezi Tebou a úlohami nestojí zhola nic.

(1) V celé řadě úloh nezávisí na poloměru kružnice, dle které se provádí inverze. Důležitý bývá hlavně její střed.

(2) Jako střed bývá zpravidla vhodné volit bod, jímž prochází podezřele velké množství kružnic.

(3) Často se vyplatí hledat inverzi, která převádí nějaký objekt ze zadání na jiný.

Úlohy na rozjezd

Úloha 1. Nechť ABC je pravoúhlý trojúhelník s pravým úhlem při C. Na odvěsnách AB, AC leží body X a Y. Kružnice se středy A, B, X, Y procházející bodem C se dohromady protínají ve čtyřech bodech. Dokažte, že tyto body leží na kružnici.

Úloha 2. Je dán pravoúhlý trojúhelník ABC s pravým úhlem u vrcholu C. Nechť D a E jsou body na úsečkách AC a BC. Dokažte, že paty kolmic vedené z bodu C na přímky AB, AE, BD a DE leží na jedné kružnici.

Úloha 3. (shooting lemma) Body A, B leží na kružnici k a S je střed nějakého oblouku AB. Dvě přímky procházející bodem S protnou k v bodech C a D a přímku AB v bodech E a F. Dokažte, že body C, D, E a F leží na kružnici.

Úloha 4. Jsou dány dvě pevné kružnice k a l, které se protínají v bodech A a B. Nechť m a n jsou kružnice, které mají s k vnější dotyk, s l mají vnitřní dotyk, navíc se samy dotýkají v bodě X. Ukažte, že bod X leží na kružnici nezávislé na volbě m a n.

Úloha 5. Jsou dány tři body A, B, C ležící na přímce a bod P mimo ní. Dokažte, že středy kružnic opsaných trojúhelníkům PBC, PAC a PBC leží na jedné kružnici s P.

Úloha 6. Kružnice vepsaná trojúhelníku ABC se dotýká jeho stran BC, CA a AB po řadě v bodech D, E a F. Nechť X je bod uvnitř trojúhelníka ABC takový, že kružnice vepsaná trojúhelníku ABX se dotýká jeho stran v bodech D, G a H. Dokažte, že body E, F, G, H leží na kružnici. (IMO shortlist 1995)

Úloha 7. Nechť k_1, k_2, k_3 a k_4 jsou kružnice takové, že k_1 a k_3 mají vnější dotyk v P a k_2 a k_4 mají rovněž vnější dotyk v P. Označme A, B, C, D druhé průsečíky k_1 s k_2, k_2 s k_3, k_3 s k_4 a k_4 s k_1. Dokažte, že platí

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

(IMO shortlist 2003)

Úloha 8. Nechť k a l jsou dvě kružnice protínající se v bodech A a B. Tečna ke k vedená bodem A protne l podruhé v bodě C. Tečna k l vedená bodem A protne k podruhé v bodě D. Nechť E je bod na polopřímce AB takový, že $|AE| = 2|AB|$. Dokažte, že body A, C, E a D leží na kružnici.

Úloha 9. Uvažme půlkružnici se středem O, průměrem AB a body C, D na ní tak, že přímka CD protíná přímku AB v bodě M tak, že $|MC| < |MD|$ a $|MB| < |MA|$. Dejme tomu, že se kružnice opsané trojúhelníkům AOC a BOD protínají znovu v bodě K. Dokažte, že $MK \perp KO$. (Iran 1996)

Úloha 10. Kružnice k_1, k_2 a k_3 mají po dvou vnější dotyk. Navíc se všechny tři dotýkají přímky l. Kružnice k o poloměru jedna má vnější dotyk s k_1, s k_2 i s k_3, ale nemá žádný společný bod s přímkou l. Jaká je vzdálenost středu kružnice k od přímky l?

$\sqrt{bc}$–inverze

Takový honosný název nese zobrazení, které je složením inverze v bodě A s poloměrem $\sqrt{bc}$ a poté překlopením podle osy úhlu. Toto zobrazení má mnoho výborných vlastností, zkus si pomocí něj vyřešit pár následujících úloh.

Tvrzení. *$\sqrt{bc}$-inverze*

(1) *prohazuje body B a C,*
(2) *prohazuje kružnici (ABC) a přímku BC,*
(3) *prohazuje vepsiště a připsiště.*

Cvičení. Kam se zobrazí kružnice s průměrem AB?

Úloha 11. Nechť ω je kružnice opsaná trojúhelníku ABC. Uvažme kružnici l, která se dotýká stran AB, AC a navíc kružnice ω v bodě T. Dále mějme kružnici připsanou trojúhelníku ABC proti vrcholu A, která se dotýká strany BC v bodě V. Dokažte, že $|\sphericalangle BAT| = |\sphericalangle CAV|$.

Úloha 12. V trojúhelníku ABC označme M střed strany BC a K průsečík tečen ke kružnici opsané v bodech B a C. Dokažte, že přímky AM a AK jsou sdružené podle osy úhlu $\sphericalangle BAC$. Přímku AK nazveme *symediánou.*

Úloha 13. V trojúhelníku ABC protne osa úhlu $\sphericalangle BAC$ stranu BC v bodě D a kružnici opsanou podruhé v bodě E. Kružnice ω s průměrem DE protíná podruhé kružnici (ABC) v bodě F. Ukažte, že F leží na symediáně v ABC. (Rusko 2009)

Úloha 14. Nechť Ω je kružnice opsaná trojúhelníku ABC. Uvažme kružnici ω, která se dotýká stran AC, BC a navíc má vnitřní dotyk s Ω v bodě P. Přímka rovnoběžná s AB se dotýká ω uvnitř trojúhelníku ABC v bodě Q. Dokažte, že $|\sphericalangle ACP| = |\sphericalangle QCB|$. (EGMO 2013)

Úloha 15. V trojúhelníku ABC kolmice ke straně AB v bodě B protne přímku AC v bodě K a podobně kolmice ke straně AC protne přímku AB v bodě L. Tyto dvě kolmice se protnou v bodě M (na kružnici opsané). Konečně, kružnice (KLM) protne kružnici (ABC) podruhé v bodě S. Dokažte, že přímka AS prochází průsečíkem tečen v bodech B a C ke kružnici opsané.

Úloha 16. V ostroúhlém trojúhelníku ABC je D pata osy úhly z A. Osa úsečky AD protíná kružnice nad průměry po řadě AB a AC vně trojúhelníka ABC v bodech E a F. Přímky DE a AC se protnou v bodě K a přímky DF a AB se protnou v bodě L. Dokažte, že body A, E, F, K a L leží na kružnici.

Návody

1. Invertuj podle C. Co se stane s kružnicemi?

2. Pravé úhly jsou výborné. Úžasné. Skvostné. Skvělé. Mocné. Krásné. Ok, už přestanu.

3. Prohoď k a AB.

4. Invertuj podle A, získáš dvě přímky.

5. Vhodně uchop středy kružnic. Připomíná ti ta přímka něco?

6. Inverzí vytvoříš dvě rovnoběžné přímky a spoustu kružnic, neboli rovnoramenné lichoběžníky.

7. Použij přepočítávací lemma.

8. Kam se zobrazí bod E?

9. Po inverzi získáš kružnici s nějakými patami a středem. Co je to za kružnici?

11. Kružnice se na sebe po inverzi zobrazí. Překvápko!

12. Kam se zobrazí tečny? Využij mocnost.

13. ω zůstane fixní.

14. Kam $\sqrt{bc}$-inverze zobrazí P? Ukaž, že body C, P^* a Q leží na přímce.

15. Kam se průsečík tečen zobrazí po BC inverzi?

16. Dokaž, že kružnice (EFD) prochází patou výšky z A. Pak už se vyuhlí.

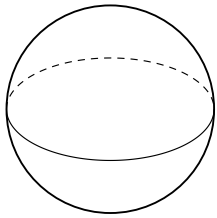
Literatura a zdroje:

Příspěvek byl adaptován a upraven od Filipa Bialase z jarního soustředění 2019, jenž příspěvek neotřele zkopíroval od Martina Hory z jarního soustředění 2016. Všem tímto z celého srdce děkuji.

Sférická geometrie

Matouš Šafránek

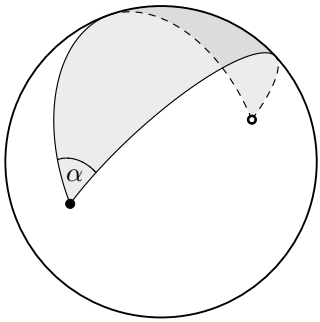
Abstrakt. Podíváme se, jak by to vypadalo, kdybychom nežili na nekonečné rovině, ale na kouli. Taky si zkusíme pracovat s úhly v prostoru a spočítat, jak chodí slunce.



Kdybychom šli po kouli pořád rovně, šli bychom po sférické analogii přímky, po takzvané *hlavní kružnici*. Často ji budeme nazývat prostě přímkou. Hlavní kružnice má střed ve středu koule a dělí ji na dvě polokoule. Příkladem na zemi jsou poledníky a rovník. Ostatní rovnoběžky jsou kružnice, ale ne hlavní kružnice.

Hlavní kružnice vede dokola – když prochází nějakým bodem, prochází i protipólem. Každými dvěma body se dá vést právě jedna přímka, pokud to ovšem nejsou protipóly. Každé dvě přímky se protínají ve dvou protipólech.

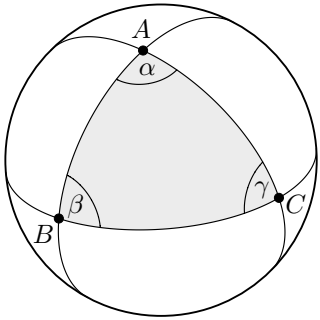
Pozorování. *Na sféře existuje dvojúhelník. Jeho vrcholy jsou protipóly.*



Úmluva. Předpokládáme, že má sféra poloměr 1, tedy obvod 2π a povrch (obsah) 4π.

Cvičení 1. Určete obsah dvojúhelníka v závislosti na jeho vnitřním úhlu.

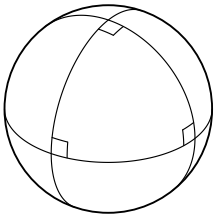
Sférický trojúhelník



Věta. *Sférický trojúhelník s vnitřními úhly α, β a γ má obsah $\alpha + \beta + \gamma - \pi$.*

Důkaz. Na druhé straně sféry vytnou strany shodný trojúhelník. Sečteme obsahy šesti dvojúhelníků vyťatých stranami, které obsahují jeden z nich. Ty pokryjí celou kouli a ještě dvakrát oba trojúhelníky. □

Důsledek. *Sférický trojúhelník má součet vnitřních úhlů větší než* $180°$.



Cvičení 2. Představte si rozdělení sféry třemi kolmými přímkami na osminy. Ověřte, že mají vyťaté trojúhelníky správný obsah.

Cvičení 3. Určete obsah sférického n-úhelníka.

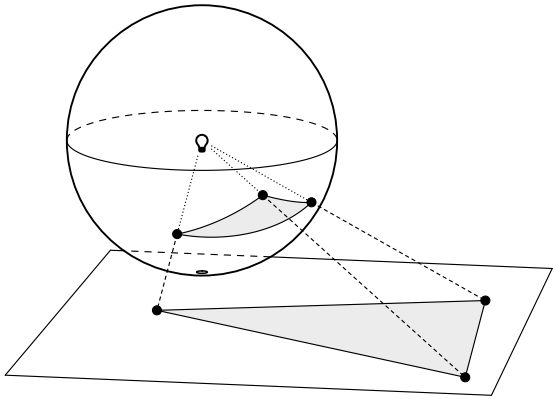
Cvičení 4. Dokažte, že se osy stran, respektive osy úhlů ve sférickém trojúhelníku protínají v jednom bodě.

Úloha 5. Jak poznáme podle vnitřních úhlů tětivový čtyřúhelník?

Věta. (Lexellova) *Jsou dány body A, B. Hýbeme-li bodem C po jedné kružnici procházející protipóly bodů A, B, je obsah trojúhelníka ABC konstantní.*

Něco funguje na sféře stejně jako v rovině, ale důkaz stejně provést nejde. Proto se bude hodit mít zobrazení mezi sférou a rovinou, které zachová aspoň některé vlastnosti.

Gnómonická projekce



Mějme v prostoru sféru a rovinu.[1] Gnómonická projekce je promítání, které bod na sféře zobrazí po přímce skrz střed sféry na rovinu. Zpětné zobrazení na sféru není jednoznačné – přímka skrz střed sféry protne sféru ve dvou protipólech. Ale viděli jsme, že protipóly jsou v mnohém ekvivalentní (třeba přímka projde oběma), takže nás to často nemusí trápit.

Pozorování. *Gnómonická projekce zobrazuje sférické přímky (tj. hlavní kružnice) na rovinné přímky.*

Důkaz. Uvažme v prostoru všechny přímky, po kterých se promítají body na hlavní kružnici. Ty tvoří rovinu a průsečík roviny s rovinou je přímka.

Z obecné gnómonické projekce tak vidíme, že na sféře platí všechny projektivní věty. Můžeme ale promítat na speciální rovinu, která se dotýká koule v daném bodě. Pak sférické kružnice, které mají v tom bodě střed, zůstanou kružnicemi a zachovají se úhly z toho bodu. Stejně jako v rovině tedy platí i projektivní věty s jednou kružnicí nebo úhly z jednoho bodu, například fungují póly a poláry.

Jinými speciálními polohami dokážeme i další tvrzení.

Úloha 6. Dokažte, že se těžnice sférického trojúhelníka protínají v jednom bodě.

Úloha 7. Dokažte, že se výšky sférického trojúhelníka protínají v jednom bodě.

Gnómonickou projekci můžeme zobecnit. Místo abychom zobrazovali jen z roviny, můžeme na sféru promítnout body v prostoru. Bod na sféře pak značí směr v prostoru, ve kterém se původní bod nachází. Přímky v prostoru se pořád zobrazují na hlavní kružnice.

[1] V libovolné poloze, jen nesmí rovina procházet středem sféry.

Úloha 8. (potenční střed) Jsou dány tři sférické kružnice. Každé dvě se protínají ve dvou bodech a těmi body vedeme přímku. Dokažte, že se všechny tři přímky protnou v jednom bodě.

Úloha 9. (Steinerova věta) Z každého vrcholu sférického trojúhelníka vedeme úsečku, která rozdělí obsah trojúhelníka napůl. Dokažte, že se tyto úsečky protnou v jednom bodě.

Úloha 10. Sestrojte úsečky z předchozí úlohy.

Úloha 11. (sférická Mongeova věta) Jsou dány tři sférické kružnice. Předpokládejme, že mají každé dvě z nich vnější společné tečny, a vyznačme jejich průsečíky. Dokažte, že leží všechny tyto průsečíky na jedné přímce.

Poznámka. Existuje ještě jedno dobré zobrazení mezi sférou a rovinou, *stereografická projekce*. Je to vlastně kulová inverze sféry se středem na té sféře. Z vlastností inverze plyne, že zachovává kružímky[2] a úhly mezi křivkami.

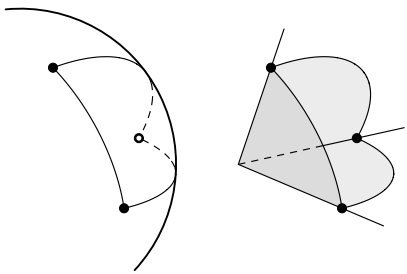
Poznámka. (rovinná limita) Když budeme na sféře kreslit obrázky velmi malé, neprojeví se křivost povrchu a bude v podstatě fungovat rovinná geometrie. Proto má každé sférické tvrzení přesnou rovinnou analogii. Jen u výpočtů je potíž, že se všechny délky musí považovat za prakticky nulové.

Úloha 12. Dokažte Eulerův vzorec pomocí rozdělení sféry na mnohoúhelníky.

Úhly v prostoru

Délky na sféře měříme po obloucích, takže jsou to vlastně zase úhly. Pokud počítáme s poloměrem 1, je délka sférické úsečky AB rovna úhlu $|\sphericalangle AOB|$, kde O je střed koule.

To nám umožňuje reprezentovat směry a úhly v prostoru. Uvažme množinu bodů, které se promítnou do jednoho bodu na sféře. To jsou všechny body v jednom směru, čili (polo)přímka ze středu sféry procházející daným bodem. Množina bodů, které se promítnou na jednu hlavní kružnici, je rovina procházející středem sféry, ve které ta kružnice leží. Díky tomu můžeme konfiguraci bodů a přímek na sféře převést na konfiguraci přímek a rovin v prostoru, které všechny prochází jedním bodem.



[2]Kružnice a přímky zobrazuje na kružnice nebo přímky.

Pozorování. *Dva body na sféře jsou od sebe tak daleko, jaký svírají úhel příslušné polopřímky. Dvě hlavní kružnice svírají stejný úhel jako příslušné roviny.*

Úloha 13. Zdeněk se nastěhoval do rohového podkrovního bytu. Má tam dvě stěny, které jsou (půdorysně) kolmé a obě jsou skloněné pod úhlem 45° do místnosti. Jaký svírají úhel mezi sebou?

Dualita

Sféra nám poskytuje dualitu, která je chytřejší než ta v rovině, protože dovede měnit vzdálenosti za úhly.

Pozorování. *Mějme úsečku délky* $\mathbf{a}$. *Kolmice na ní vztyčené v krajních bodech se protnou pod úhlem* $\mathbf{a}$.

Pozorování. *Všechny kolmice k jedné přímce se protnou v jednom bodě. Naopak všechny přímky z jednoho bodu mají společnou kolmici.*

Definice. *Dualita* na sféře je zobrazení, které přímkám přiřazuje body a naopak tak jako v předchozím cvičení.[3]

Cvičení 14. Značme dualitu čárkou. Pokud bod A leží na přímce a, leží bod a' na přímce A'.

Cvičení 15. Jak vypadá dualita v prostorovém náhledu, kde bereme body jako přímky a hlavní kružnice jako roviny?

Úloha 16. Sférickému trojúhelníku ABC sestrojíme takzvaný *polární trojúhelník* $A'B'C'$. Bod A' je ten duální bod k přímce BC, který leží od přímky BC na stejné polokouli jako A. Analogicky B', C'. Ukažte, že

$$\alpha' = \pi - \mathbf{a}, \qquad \mathbf{a}' = \pi - \alpha$$

a podobně.

Úloha 17. Dokažte, že sférický trojúhelník a jeho polární trojúhelník sdílí výšky.

Úloha 18. Sestrojte sférický trojúhelník, máte-li zadané velikosti vnitřních úhlů.

Trigonometrie

V devatenáctém století bylo, jak se zdá, nejvyšším cílem matematiky, aby byl pro každé možné zadání někde uveden vzorec, jak v trojúhelníku dopočítat všechny délky a úhly. Tady budeme střídmější.

Úmluva. Ve sférickém trojúhelníku ABC značme standardně vnitřní úhly α, β, γ a délky stran $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$. Střed sféry v prostoru značme O.

[3] V případě přiřazení bodu přímce je třeba upřesnit, který ze dvou protipólů bereme. Funguje to dělat podle orientace přímky.

Věta. (sférická sinová) *Platí*

$$\frac{\mathbf{sin}(\mathbf{a})}{\sin(\alpha)} = \frac{\mathbf{sin}(\mathbf{b})}{\sin(\beta)} = \frac{\mathbf{sin}(\mathbf{c})}{\sin(\gamma)}.$$

Důkaz. Uvažme v prostoru výšku z A na rovinu OBC. Spočítáme její délku dvěma způsoby. Přes délku výšky z A na OB vyjde $\mathbf{sin}(\mathbf{b})\sin(\gamma)$ a symetricky vyjde $\mathbf{sin}(\mathbf{c})\sin(\beta)$.

Cvičení 19. V rovině se sinus definuje vztahem $\sin(\text{úhel}) = \frac{\text{protilehlá}}{\text{přepona}}$. Najděte analogii tohoto vztahu ve sférickém trojúhelníku.

Cvičení 20. (návodné) Jaký úhel svírají stěny pravidelného čtyřstěnu?

Věta. (sférická kosinová pro strany) *Platí*

$$\mathbf{cos}(\mathbf{a}) = \mathbf{cos}(\mathbf{b})\,\mathbf{cos}(\mathbf{c}) + \mathbf{sin}(\mathbf{b})\,\mathbf{sin}(\mathbf{c})\cos(\alpha).$$

Důkaz. Promítneme trojúhelník gnómonicky na rovinu, která se koule dotýká v bodě A. Body B, C se zobrazí na B', C'. Zkombinujeme kosinové věty v trojúhelnících $AB'C'$ a $OB'C'$.[4]

Cvičení 21. Interpretujte kosinovou větu pro $\alpha = 0$ a $\alpha = 180°$.

Cvičení 22. Napište sférickou Pythagarovou větu. Jak to, že nejde při $\mathbf{b} = 90°$ určit $\mathbf{c}$?

Využití sférické trigonometrie je nasnadě – žijeme na zeměkouli. Počítejme s tím, že je Země skutečně koule a má poloměr 6371 km. Zdobnice má zeměpisné souřadnice 50,2° s. š, 16,4° v. d. New York má souřadnice 40,7° s. š, 74,0° z. d.

Úloha 23. Určete vzdálenost Zdobnice a New Yorku.

Úloha 24. Kdybychom ve Zdobnici udělali rozcestník na New York a na severní pól, jaký úhel by svíraly směrovky?

Úloha 25. Do jaké nejvyšší severní šířky se člověk dostane na přímé cestě ze Zdobnice do New Yorku?

Úloha 26. Určete obsah trojúhelníka vymezeného Zdobnicí, New Yorkem a severním pólem.

Úloha 27. Najít analogii definičního vztahu pro sinus bylo snadné. Jak je to s kosinem?

Úloha 28. (sférická kosinová věta pro úhly) Dokažte

$$\cos(\alpha) = -\cos(\beta)\cos(\gamma) + \sin(\beta)\sin(\gamma)\,\mathbf{cos}(\mathbf{a}).$$

[4] Pokud je $\mathbf{b}$ nebo $\mathbf{c}$ rovno 90°, promítne se C nebo B do nekonečna a důkaz nefunguje; pak je to potřeba dokázat jinak.

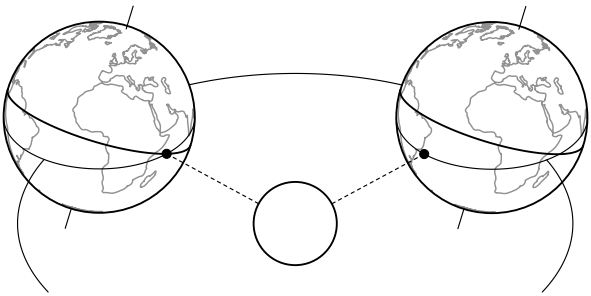
Úloha 29. Paní Mráčková si chce na střechu domu nainstalovat solární panely. Střecha však nemíří na jih, ale o 30° stranou. Paní Mráčková tedy zvažuje, že by panely naklopila, tedy pootočila okolo spádového směru střechy, aby mířily na jih. Má-li střecha spád 45°, o kolik je musí otočit?

Úloha 30. Zkoumejme, kolik pravidelných čtyřstěnů je možno umístit do prostoru tak, aby měly všechny vrchol v jednom bodě a neprotínaly se. Ukažte, že je to alespoň 20 a ne více než 22.

Slunce

Úmluva. Země obíhá Slunce po kružnici. Slunce je na obloze bod, je prakticky nekonečně daleko a zanedbáváme světelné jevy, takže svítí všem na Zemi ze stejného směru. Počítáme v pravém slunečním čase.

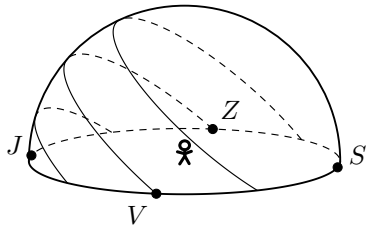
Slunce budeme standardně promítat do bodu na Zemi, tedy do bodu, který určuje, ve kterém směru se nachází. V tom bodě svítí přímo ze shora. Kdyby se Země netočila, pohybovalo by se Slunce po hlavní kružnici odchýlené od zemského rovníku o (přibližně) 23,5°. Oběhlo by ji za rok.



Země se ale navíc otáčí, a to mnohem rychleji, než obíhá Slunce (ve frekvenci). Proto Slunce každý den oběhne celou rovnoběžku, na které zrovna je. Jeho zeměpisná šířka se během dne změní, ale nepatrně.

Tato zeměpisná šířka se nazývá *deklinace*. Nejvyšší deklinace je tedy 23,5°.

Když Slunce pozorujeme, určujeme jeho polohu na nebeské sféře, velké imaginární kouli kolem nás, po které jakoby běhají nebeská tělesa. Opět je to jen reprezentace směru v prostoru, takže je dráha Slunce na nebeské sféře stejná jako v průmětu na Zemi, jen otočená podle zeměpisné šířky – podle toho, jak jsme vůči Zemi otočení my. O rovnodennosti jde Slunce po nebeském rovníku, o slunovratech po nebeských obratnících.



Příklad 31. Určete závislost sluneční deklinace na roční době.

Řešení. Vraťme se k variantě bez otáčení Země. O rovnodennosti je Slunce na rovníku a obíhá rovnoměrně, takže v čase T od rovnodennosti je od toho bodu ve vzdálenosti $d = T \cdot \frac{2\pi}{\text{rok}}$. Deklinace je vzdálenost Slunce od rovníku, změříme ji tedy po úsečce kolmé na rovník, kterou můžeme spočítat pomocí pravoúhlého trojúhelníku. Víme totiž, že dráha Slunce a rovník svírají úhel 23,5°. Vychází

$$\delta = \arcsin(\sin(d) \cdot \sin(23{,}5^\circ)).$$

V následujících úlohách předpokládejme, že máme danou zeměpisnou šířku φ a známe deklinaci Slunce δ.

Cvičení 32. Určete výšku slunce v poledne.

Úloha 33. Určete délku dne (od východu do západu slunce).

Úloha 34. Určete azimut východu slunce. Pro polární kruh určete, jak závisí na roční době.

Úloha 35. Určete čas podle výšky slunce.

Další úlohy

Úloha 36. Určete zeměpisné šířky míst A, B z následujících údajů: Když je Slunce na obratníku Raka, vychází v A o hodinu dřív než v B; když je na obratníku Kozoroha, vychází v B o hodinu dřív než v A.

Úloha 37. Pokud je na dané zeměpisné šířce Slunce na východě dvě hodiny po jeho východu, zjistěte deklinaci.

Úloha 38. Určete zeměpisnou šířku podle Slunce, bez dalších znalostí.

Návody

1. Jakou část povrchu celé koule zabírá?

3. Rozděl na trojúhelníky.

4. Stejně jako v rovině.

5. Dokresli spojnice s opsištěm.

6. Projekce na rovinu procházející vrcholy zachová středy stran.

7. Projekce na rovinu tečnou ke kouli v jednom vrcholu zachová všechny tři kolmosti.

8. Sférická kružnice je průnik sféry s rovinou.

9. Lexellova věta.

10. Lexellova věta.

11. Kružnice jsou průměty koulí v prostoru.

12. Sečti obsahy.

13. Překresli si to na sférický trojúhelník a dokresli trojúhelník se třemi pravými úhly.

15. Duální k rovině je kolmá přímka a naopak.

16. Je jen třeba si rozmyslet, jestli $\mathbf{a}$ nebo $\pi - \mathbf{a}$, což je podle toho, které duální body bereme.

17. Ukaž, že výška původního trojúhelníka prochází vrcholem polárního trojúhelníka a je kolmá na jeho stranu.

18. S délkami stran je to snadné.

19. Zjednoduš sinovou větu v pravoúhlém trojúhelníku.

21. Součtové vzorce.

23. Trojúhelník Zdobnice – New York – severní pól.

25. Výška trojúhelníku z vrcholu na severním pólu.

28. Polární trojúhelník.

29. Máš pravoúhlý trojúhelník nadhlavník – směr, kterým míří nenaklopené panely – směr, kterým míří naklopené.

30. Prostorová představa: čtyřstěn s vrcholem ve středu sféry znamená trojúhelník.

35. Nejdřív výšku v závislosti na čase. Může pomoct počítat trojúhelník pól – nadhlavník – Slunce.

Literatura a zdroje

[1] John Casey: *A treatise on spherical trigonometry, and its application to geodesy and astronomy, with numerous examples*, Hodges, Figgis, & co, 1889.

Viètovy vztahy

Josef „José“ Soural

Abstrakt. Viètovy vztahy (též Viètovy vzorce) jsou docela silný nástroj na úlohy o polynomech a o jejich kořenech. Na přednášce si ukážeme, jak Viètovy vztahy vypadají a jak je použít při řešení úloh.

Úmluva. Pokud není řečeno jinak, koeficienty všech polynomů jsou reálné.

Začneme s jednoduchým tvrzením pro kvadratickou rovnici.

Tvrzení. *Mějme kvadratickou rovnici*

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

Pro její kořeny $x_1, x_2 \in \mathbb{C}$ *platí* $x_1 + x_2 = -\frac{b}{a}$ a $x_1 \cdot x_2 = \frac{c}{a}$.

Poznámka. Pro $a = 1$ dostaneme $x_1 + x_2 = -b$ a $x_1 \cdot x_2 = c$.

Tohle tvrzení můžeme hezky zobecnit i pro rovnice vyššího stupně. Nejdřív si ale definujme, co je to polynom.

Definice. Buď n přirozené číslo nebo nula. *Polynomem stupně* n rozumíme výraz tvaru

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

kde $a_n \neq 0$. Reálná čísla a_i se nazývají *koeficienty* a x *proměnná*.

Definice. Číslo $r \in \mathbb{C}$ nazveme *kořenem* polynomu P, jestliže $P(r) = 0$.

Tvrzení. (důsledek základní věty algebry) *Polynom stupně* n *má právě* n *komplexních kořenů (každý kořen počítáme tolikrát, jaká je jeho násobnost).*

Teď už si konečně můžeme ukázat znění hlavní věty této přednášky.

Věta. (Viètovy vztahy) *Mějme polynom* $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, *který je stupně* n *a má kořeny* $r_1, r_2, \ldots, r_n$. *Pak pro každé* $k \in \{1, 2, \ldots, n\}$ *platí*

$$\sum_{1 \leq i_1 < \cdots < i_k \leq n} r_{i_1} \cdot r_{i_2} \cdots r_{i_k} = (-1)^k \cdot \frac{a_{n-k}}{a_n}.$$

Výraz na levé straně může vypadat děsivě, ale je to jenom symetrický polynom stupně k. To znamená, že vezmeme všechny součiny obsahující právě k různých kořenů a sečteme je. Zejména pro $k = 1$, resp. $k = n$ se jedná o součet, resp. součin všech kořenů. Všimněme si, že pro $a_n = 1$ jsou Viètovy vztahy o trochu přívětivější.

A nyní hurá na slíbené úložky!

Kvadratické rovnice

Úloha 1. Najděte kvadratickou rovnici s takovými kořeny, že jejich součet je 7 a jejich součin je 13.

Úloha 2. Označme α a β kořeny rovnice $2x^2 - 4x + 9 = 0$. Určete $\alpha^2 + \beta^2$, aniž byste tyto kořeny počítal.

Úloha 3. Určete všechny čtveřice reálných čísel a, b, c, d, pro které platí následující dvě podmínky: rovnice $x^2 + ax + b$ má kořeny c, d a rovnice $x^2 + cx + d$ má kořeny a, b.

Úloha 4. Nechť a a b jsou různá reálná čísla splňující $a^2 + 3a = b^2 + 3b = -1$. Najděte hodnotu výrazu $\frac{a}{b} + \frac{b}{a}$.

Úloha 5. Nechť jsou α a β kořeny rovnice $x^2 + 2x + 3$. Jak vypadá kvadratická rovnice, jejíž kořeny jsou $\left(\alpha - \frac{1}{\alpha}\right)^2$ a $\left(\beta - \frac{1}{\beta}\right)^2$?

Úloha 6. Najděte všechny uspořádané trojice reálných čísel, které tvoří aritmetickou i geometrickou posloupnost.

Polynomy vyššího stupně

Úloha 7. Polynom $x^3 - 3x^2 + 1$ má kořeny α, β a γ. Najděte polynom třetího stupně s kořeny α^2, β^2 a γ^2.

Úloha 8. V komplexních číslech vyřešte soustavu

$$\begin{aligned} a + b + c &= -3, \\ ab + bc + ac &= 3, \\ abc &= -1. \end{aligned}$$

Úloha 9. Polynom $x^3 - ax^2 + bx - 2010$ má tři přirozené kořeny. Jaká je nejmenší možná hodnota a? (AMC 2010)

Úloha 10. Nechť α, β a γ jsou kořeny polynomu $5x^3 - 11x^2 + 7x + 3$. Najděte hodnotu výrazu $\alpha^3 + \beta^3 + \gamma^3$.

Úloha 11. Nechť má polynom $x^3 + 3x^2 + 4x - 11$ kořeny α, β a γ a nechť má $x^3 + rx^2 + sx + t$ kořeny $\alpha + \beta$, $\beta + \gamma$ a $\alpha + \gamma$. Určete t.

Úloha 12. Určete součet všech kořenů polynomu $x^{2021} + \left(\frac{1}{2} - x\right)^{2021}$.
(AIME 2001)

Úloha 13. Mějme polynom $x^4 - 18x^3 + kx^2 + 200x - 1984$, pro který platí, že součin dvou jeho kořenů je -32. Najděte hodnotu parametru k. (USAMO 1984)

Úloha 14. Polynom $P(x) = x^3 + ax^2 + x + 10$ má tři různé reálné kořeny. Každý kořen $P(x)$ je také kořenem polynomu $Q(x) = x^4 + x^3 + bx^2 + 100x + c$. Určete hodnotu $Q(1)$. (AMC 2017)

Úloha 15. Nechť α a β jsou dva z kořenů polynomu $x^4 + x^3 - 1$. Dokažte, že součin $\alpha \cdot \beta$ je kořen polynomu $x^6 + x^4 + x^3 - x^2 - 1$. (USAMO 1997)

Obtížnější úlohy

Ačkoli jsou Viètovy vztahy mocná pomůcka na mnohé olympiádní problémy, je někdy třeba spolu s nimi použít i jiné nástroje. To si lze procvičit na následujících úlohách.

Úloha 16. Nechť p, q jsou nezáporná celá čísla. Dokažte, že pokud jsou všechny kořeny polynomu $x^n - px^{n-1} + qx^{n-2} + a_{n-3}x^{n-3} + \cdots + a_1x + a_0$ přirozené, potom lze do roviny nakreslit p přímek protínajících se v právě q různých bodech.
(Turnaj Měst 2020)

Úloha 17. Najděte všechny polynomy, jejichž všechny kořeny jsou reálné a jejichž koeficienty nabývají pouze hodnot ± 1. (Putnam 1968)

Úloha 18. Určete všechna reálná a, pro která má polynom

$$16x^4 - ax^3 + (2a + 17)x^2 - ax + 16$$

čtyři různé reálné kořeny tvořící geometrickou posloupnost. (Shortlist)

Návody

1. $x^2 - 7x + 13$.

2. $\alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta$. (Nelekni se výsledku, kořeny nemusí být reálné.)

3. Napiš si Viètovy vztahy a vyřeš soustavu.

4. $\frac{a}{b} + \frac{b}{a} = \frac{a^2+b^2}{ab}$.

5. Vyjádři součet a součin pomocí $\alpha + \beta$ a $\alpha\beta$.

6. Platí $a + c = 2b$ a zároveň $ac = b^2$.

7. $\alpha^2\beta^2 + \beta^2\gamma^2 + \alpha^2\gamma^2 = (\alpha\beta + \beta\gamma + \alpha\gamma)^2 - 2\alpha\beta\gamma(\alpha + \beta + \gamma)$.

8. Najdi polynom, jehož kořeny jsou a, b, c.

9. $2010 = 2 \cdot 3 \cdot 5 \cdot 67$.

10. $\alpha^3 + \beta^3 + \gamma^3 = (\alpha + \beta + \gamma)(\alpha^2 + \beta^2 + \gamma^2 - \alpha\beta - \beta\gamma - \alpha\gamma) + 3\alpha\beta\gamma$.

11. $(\alpha + \beta)(\beta + \gamma)(\alpha + \gamma) = (\alpha + \beta + \gamma)(\alpha\beta + \beta\gamma + \alpha\gamma) - \alpha\beta\gamma$.

12. Z binomické věty spočítej koeficienty u dvou nejvyšších mocnin.

13. Napiš si soustavu danou Viètovými vztahy a počítej ...

14. Urči kořen, který má $Q(x)$ navíc, označme jej r. Potom $Q(1) = (1 - r)P(1)$.

15. Substituuj za $\alpha + \beta$, $\alpha\beta$, $\gamma + \delta$ a $\gamma\delta$, pak to bude hezčí a jednodušší.

16. Rozděl přímky do několika rovnoběžných skupinek.

17. Využij toho, že aritmetický průměr čtverců kořenů musí být aspoň tak velký, jako je velký jejich geometrický průměr.

18. Hint první: Všimni si, že je zadaná rovnice reciproká, takže je-li α kořenem, bude jím i $\frac{1}{\alpha}$.

Hint druhý: $t^3 + \frac{1}{t^3} = \left(t + \frac{1}{t}\right)^3 - 3 \cdot \left(t + \frac{1}{t}\right)$.

Literatura a zdroje

Tento příspěvek je pouze s drobnými úpravami převzat od *Josefa Minaříka* z roku 2021, kterému tímto děkuji.

[1] Josef Minařík: *Viètovy vztahy*, Zásada, 2021.

Permutační nerovnost

Adéla Karolína Žáčková

Abstrakt. Permutační nerovnost, ačkoliv poměrně přímá, je ve skutečnosti docela silný nástroj na řešení mnohých příkladů. Na přednášce se v ní naučíme orientovat a vyřešíme spoustu příkladů.

Permutace? Co to je?

Než se vůbec ponoříme do toho, co je permutační nerovnost, bylo by hezké mít jasno v tom, co to vůbec je taková permutace.

Definice. *Permutace* σ množiny $\{1, 2, \ldots, n\}$ je nějaké její přeuspořádání.

Tak, teď máme úplně krásnou definici, ale my ji v přednášce vlastně vůbec nebudeme používat (snad kromě jejího značení). Cool, co? :D Já si taky myslím. A teď už k hlavní nerovnosti celé přednášky.

Věta. (permutační nerovnost) *Mějme posloupnosti reálných čísel*

$$x_1 \geq x_2 \geq \cdots \geq x_n \qquad \text{a} \qquad y_1 \geq y_2 \geq \cdots \geq y_n.$$

Dále ať σ *je libovolná permutace množiny* $\{1, 2, \ldots, n\}$, *která přeuspořádává* $(y_1, y_2, \ldots, y_n)$ *na* $(y'_1, y'_2, \ldots, y'_n)$. *Pak*

$$x_1y_1 + x_2y_2 + \cdots + x_ny_n \geq x_1y'_1 + x_2y'_2 + \cdots + x_ny'_n \geq x_1y_n + x_2y_{n-2} + \cdots + x_ny_1.$$

Poznámka. Nerovnost platí pro libovolné dvě n-tice reálných čísel.

Říkáte si, pfff, nějaké takové nerovnosti. Kdy já to vůbec použiji? Tak si představte následující situaci: Na stole leží n hromádek bankovek (v každé hromádce jsou bankovky jedné hodnoty). Každý z n dní přijdete ke stolu a můžete si vybrat hromádku, ze které jste ještě nic nebrali, a z ní si vzít daný počet bankovek. Předem máte pro každý den dáno, kolik bankovek (nehledě na hodnotu) si smíte vzít. Ano. Také se mi tato situace stává každý druhý den. A permutační nerovnost nám teď dává jasnou strategii, jak si můžeme vydělat co nejvíce (případně, co nejméně).

Cvičení. Kdy v permutační nerovnosti nastává rovnost?

Definice. Dvě posloupnosti $x_1, x_2, \ldots, x_n$ a $y_1, y_2, \ldots, y_n$ jsou *souhlasně uspořádané*, pokud $x_i \geq x_j$ právě tehdy, když $y_i \geq y_j$.

Obdobně, posloupnosti jsou *opačně uspořádané*, pokud $x_i \geq x_j$ právě tehdy, když $y_i \leq y_j$.

Permutační nerovnost nám tedy říká, že největší výraz získáme ze dvou souhlasně uspořádaných permutací, kdežto nejmenší ze dvou opačně uspořádaných.

Permutační nerovnost přitom typicky *homogenní* výrazy odhaduje opět homogenními výrazy stejného stupně. Často nám umožní velmi jednoduše odhadovat *cyklické* výrazy pomocí jiných cyklických výrazů.[1]

Je to zřejmé ...

Úloha 1. Pro reálná a, b, c dokažte $a^2 + b^2 + c^2 \geq ab + bc + ca$.

Úloha 2. Pro reálná $x, y, z \geq 0$ ukažte $x^3y + y^3z + z^3x \geq x^2yz + y^2zx + z^2xy$.

Úloha 3. Pro reálná x, y, z ukažte $x^4y^2 + y^4z^2 + z^4x^2 \geq x^3yz^2 + y^3zx^2 + z^3xy^2$.

Úloha 4. Pro reálná $a, b, c > 0$ dokažte $\frac{a^2}{b^2} + \frac{b^2}{c^2} + \frac{c^2}{a^2} \geq \frac{b}{a} + \frac{c}{b} + \frac{a}{c}$.

Úloha 5. Ať $x_1 \geq x_2 \geq \cdots \geq x_n$, $y_1 \geq y_2 \geq \cdots \geq y_n$ jsou reálná čísla a $(y'_1, y'_2, \ldots, y'_n)$ je permutace $(y_1, y_2, \ldots, y_n)$. Potom

$$(x_1 - y_1)^2 + (x_2 - y_2)^2 + \cdots + (x_n - y_n)^2 \leq (x_1 - y'_1)^2 + (x_2 - y'_2)^2 + \cdots + (x_n - y'_n)^2.$$

(IMO 1975)

Úloha 6. Pro kladná reálná čísla $(x_1, x_2, \ldots, x_n)$ a jejich libovolnou permutaci $(x'_1, x'_2, \ldots, x'_n)$ nahlédněte $\frac{x_1}{x'_1} + \frac{x_2}{x'_2} + \cdots + \frac{x_n}{x'_n} \geq n$.

Úloha 7. Pro reálná $a, b, c > 0$ dokažte $\frac{1}{a^2} + \frac{1}{b^2} + \frac{1}{c^2} \geq \frac{a+b+c}{abc}$.

Rozpalme mozkové závity

Doteď permutační nerovnost řešila úložky za nás. Pojďme teď trošku namáhat své mozkové závity a vrhněme se na úložky, které už nebudou tak moc zadarmo, ale budeme s nimi muset vymyslet nějaký trošku tríček.

Úloha 8. Pro $0 < x < \frac{\pi}{2}$ najděte minimum výrazu $\frac{\sin^3 x}{\cos x} + \frac{\cos^3 x}{\sin x}$.

Úloha 9. Na stole leží n po dvou různých přirozených čísel $a_1, a_2, \ldots, a_n$. Dokažte $\frac{a_1}{1^2} + \frac{a_2}{2^2} + \cdots + \frac{a_n}{n^2} \geq 1 + \frac{1}{2} + \cdots + \frac{1}{n}$.

Úloha 10. Pro reálná $a, b, c > 0$ dokažte $\frac{a+1}{b\sqrt{b}} + \frac{b+1}{c\sqrt{c}} + \frac{c+1}{a\sqrt{a}} \geq 2\left(\frac{1}{a} + \frac{1}{b} + \frac{1}{c}\right)$.

[1] Výraz $V(a, b, c)$ je *cyklický*, pokud platí $V(a, b, c) = V(b, c, a) = V(c, a, b)$. Výraz $V(a, b, c)$ je *homogenní stupně* α, pokud toto reálné α splňuje, že pro každé $t > 0$ platí $V(ta, tb, tc) = t^\alpha V(a, b, c)$.

Úloha 11. Pro reálná $a, b, c > 0$ dokažte $\frac{a^2+b^2}{c} + \frac{b^2+c^2}{a} + \frac{c^2+a^2}{b} \geq 2(a+b+c)$.

Úloha 12. Pro reálná $x, y, z > 0$ dokažte $\frac{x^2-z^2}{y+z} + \frac{y^2-x^2}{z+x} + \frac{z^2-y^2}{x+y} \geq 0$.

Úloha 13. Jsou dána reálná $x, y, z > 0$. Ukažte odhad $\frac{x^3}{yz} + \frac{y^3}{zx} + \frac{z^3}{xy} \geq x + y + z$.

Úloha 14. Pro reálná $a, b, c > 0$ dokažte *Nesbittovu* nerovnost:

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

Úloha 15. Pro reálná $a, b, c > 0$ splňující $abc = 1$ dokažte

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

Úloha 16. Pro reálná $a, b, c > 0$ a přirozené n ukažte

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

Úloha 17. Jsou dána reálná $a_1, a_2 \ldots, a_n > 0$, pro přehlednost označme s jejich součet. Potom $\frac{a_1}{s-a_1} + \frac{a_2}{s-a_2} + \cdots + \frac{a_n}{s-a_n} \geq \frac{n}{n-1}$.

Úloha 18. Dána jsou reálná $a, b, c > 0$. Dokažte $a^a b^b c^c \geq \sqrt[3]{(abc)^{a+b+c}}$.

K čemu jsou mi ostatní nerovnosti, když mám tu permutační!

Už jsme viděli, že permutační nerovnost umí vyřešit velkou spoustu příkladů, víme, že nám zachovává homogenitu i cykličnost výrazů. K čemu je ale ještě dobrá? Ukážeme si, že z ní plynou nerovnosti, které určitě všichni dobře znáte, a nejen to!

Úloha 19. Pro reálná $x_1, x_2, \ldots, x_n \geq 0$ dokažte AG nerovnost:

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

Úloha 20. Pro reálná $x_1, x_2, \ldots, x_n \geq 0$, $n \geq m \in \mathbb{R}$ dokažte *nerovnost mezi průměry*:

$$K = \sqrt{\frac{x_1^2 + x_2^2 + \cdots + x_n^2}{n}} \geq A \geq G \geq H = \frac{1}{\frac{1}{x_1} + \frac{1}{x_2} + \cdots + \frac{1}{x_n}}.$$

Úloha 21. Pro reálná $a_1, a_2, \ldots, a_n$, $b_1, b_2, \ldots, b_n$ dokažte *Cauchy-Schwarzovu* nerovnost: $(a_1^2 + a_2^2 + \cdots + a_n^2)(b_1^2 + b_2^2 + \cdots + b_n^2) \geq (a_1 b_1 + a_2 b_2 + \cdots + a_n b_n)^2$.

Z permutační nerovnosti se také dá odvodit další dost šikovná nerovnost, jak záhy uvidíme.

Čebyšev

Věta. (Čebyševova nerovnost) *Ať $a_1 \geq a_2 \geq \cdots \geq a_n$, $b_1 \geq b_2 \geq \cdots \geq b_n$ jsou n-tice reálných čísel. Potom*

$$n\sum_{i=1}^{n} a_i b_i \geq \left(\sum_{i=1}^{n} a_i\right)\left(\sum_{i=1}^{n} b_i\right) \geq n\sum_{i=1}^{n} a_i b_{n+1-i}.$$

Důkaz. Pro první nerovnost dokola sečteme všech n permutačních nerovností tvaru $\sum a_i b_i \geq \sum a_i b_{i+k}$. Druhá nerovnost se dokáže analogicky. □

Tvrzení. *V Čebyševově nerovnosti nastává rovnost právě tehdy, když*

$$x_1 = x_2 = \cdots = x_n \qquad \textit{nebo} \qquad y_1 = y_2 = \cdots = y_n.$$

Na první pohled se zdá, že Čebyševova nerovnost musí být opravdu hloupá, neboť jsme ji získali nasčítáním hromady slabých permutačních nerovností. Překvapivě je ale poměrně silná a užitečná, a to právě kvůli tomu, že se na čísla dívá „z větší výšky“. Nyní si v praxi vyzkoušíme, co tato nerovnost umí.

Úloha 22. Pro reálná a, b, c ukažte $3(a^8 + b^8 + c^8) \geq (a^5 + b^5 + c^5)(a^3 + b^3 + c^3)$.

Úloha 23. Jsou dána reálná $a_1, a_2, \ldots, a_2 > 0$, která splňují $a_1 + a_2 + \cdots + a_n = 1$. Dokažte, že potom $\frac{a_1}{2-a_1} + \frac{a_2}{2-a_2} + \cdots + \frac{a_n}{2-a_n} \geq \frac{n}{2n-1}$.

Úloha 24. Pro reálná $a, b, c, d > 0$ dokažte nerovnost

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

Úloha 25. Pro reálná $a, b, c > 0$ ukažte nerovnost $\frac{ab}{a+b} + \frac{bc}{b+c} + \frac{ca}{c+a} \leq \frac{3(ab+bc+ca)}{2(a+b+c)}$.

Úloha 26. Mějme čísla $a_1, a_2, \ldots, a_n \in \left\langle 0, \frac{\pi}{2} \right\rangle$. Dokažte nerovnost

$$\left(\sum_{i=1}^{n} \sin a_i\right) \cdot \left(\sum_{i=1}^{n} \cos a_i\right) \leq \frac{n^2}{2}.$$

Úloha 27. Ať reálná $a, b, c, d > 0$ splňují $a + b + c + d = 4$. Potom ukažte

$$\frac{1}{11+a^2} + \frac{1}{11+b^2} + \frac{1}{11+c^2} + \frac{1}{11+d^2} \leq \frac{1}{3}.$$

Úloha 28. Ať $0 < x_1 \leq x_2 \leq \cdots \leq x_n$ je n-tice reálných čísel, která splňují $\frac{1}{1+x_1} + \frac{1}{1+x_2} + \cdots + \frac{1}{1+x_n} = 1$. Dokažte, že

$$\sqrt{x_1} + \sqrt{x_2} + \cdots + \sqrt{x_n} \geq (n-1) \cdot \left(\frac{1}{\sqrt{x_1}} + \frac{1}{\sqrt{x_2}} + \cdots + \frac{1}{\sqrt{x_n}}\right).$$

Úloha 29. Pro reálná $a, b, c, d \geq 0$ splňující $ab + bc + cd + da = 1$ ukažte

$$\frac{a^3}{b+c+d} + \frac{b^3}{a+c+d} + \frac{c^3}{a+b+d} + \frac{d^3}{a+b+c} \geq \frac{1}{3}.$$

(IMO Shortlist 1990)

Úloha 30. Reálná čísla $x, y, z \geq 0$ splňují $xyz = 1$. Dokažte nerovnost

$$\frac{x^3}{(1+y)(1+z)} + \frac{y^3}{(1+z)(1+x)} + \frac{z^3}{(1+x)(1+y)} \geq \frac{3}{4}.$$

(IMO Shortlist 1998)

Postřeh na závěr

Jsme matematici, proto nás zajímají co nejobecnější tvrzení. Pojďme si tedy zkusit permutační nerovnost zobecnit.

Úloha 31. Ať jsou $x_1 \geq x_2 \geq \cdots \geq x_n \geq 0$, $y_1 \geq y_2 \geq \cdots \geq y_n \geq 0$, $z_1 \geq z_2 \geq \cdots \geq z_n \geq 0$ posloupnosti reálných čísel a $(y'_1, y'_2, \ldots, y'_n)$, $(z'_1, z'_2, \ldots, z'_n)$ jsou permutace posloupností $(y_1, y_2, \ldots, y_n)$, $(z_1, z_2, \ldots, z_n)$. Potom platí

$$\sum_{i=1}^{n} x_i y_i z_i \geq \sum_{i=1}^{n} x_i y'_i z'_i.$$

Podobně můžeme permutační nerovnost zobecnit pro větší počet posloupností. Přitom je ale opravdu potřeba předpokládat nezápornost čísel. Předveďme si ještě duální verzi permutační nerovnosti, kde „zaměníme“ násobení se sčítáním.

Úloha 32. Jsou dána reálná čísla $x_1 \geq x_2 \geq \cdots \geq x_n \geq 0$, $y_1 \geq y_2 \geq \cdots \geq y_n \geq 0$, dále $(y'_1, y'_2, \ldots, y'_n)$ je permutace $(y_1, y_2, \ldots, y_n)$. Potom

$$\prod_{i=1}^{n}(x_i + y_i) \leq \prod_{i=1}^{n}(x_i + y'_i) \leq \prod_{i=1}^{n}(x_i + y_{n+1-i}).$$

Stejně jako minule, i tuto nerovnost lze zobecnit pro nezáporná čísla pro libovolný počet posloupností.

Návody

1. Vezmi dvakrát stejnou trojici (a, b, c).

2. Opačně uspořádané trojice (x^2, y^2, z^2) a (yz, zx, xy).

3. Dvě stejné (souhlasně uspořádané) trojice (x^2y, y^2z, z^2x).

4. Vezmi dvakrát trojici $\frac{a}{b}, \frac{b}{c}, \frac{c}{a}$.

5. Se zatnutými zuby roznásob závorky, zbav se druhých mocnin a vynásob (-1).

6. Uvědom si, že posloupnosti x_i a $\frac{1}{x_i}$ jsou opačně uspořádané.

7. Stačí vzít dvě stejné trojice $(\frac{1}{a}, \frac{1}{b}, \frac{1}{c})$ a upravit pravou stranu. Nebo můžeš nerovnost vynásobit abc a uvážit předešlou trojici společně s trojicí bc, ca, ab.

8. Uvaž kladné posloupnosti $\sin^3 x$, $\cos^3 x$ a $\cos^{-1} x, \sin^{-1} x$. Vyjde tedy $\sin^2 x + \cos^2 x = 1$.

9. Nejprve „setřepej“ čísla a_i dolů na čísla $1, 2, \ldots, n$ a poté očividným způsobem použij permutační nerovnost.

10. Odhadni čitatele jako dvojnásobky odmocnin a pak uvaž trojice $(\sqrt{a}, \sqrt{b}, \sqrt{c})$, $\left(\frac{1}{a\sqrt{a}}, \frac{1}{b\sqrt{b}}, \frac{1}{c\sqrt{c}}\right)$.

11. Zlomky si rozděl, následně použij na dvě trojice zlomků permutační nerovnost, která je odhadne jako $a + b + c$.

12. Záporné věci dej doprava. Posloupnosti (x^2, y^2, z^2) a $(\frac{1}{y+z}, \frac{1}{z+x}, \frac{1}{y+z})$ jsou souhlasně uspořádané.

13. Najednou to jde špatně. Zkus ale použít permutační nerovnost dvakrát za sebou, vždy tím nejjednodušším možným způsobem.

14. Vynásob nerovnost dvěma. Pokud BÚNO $a \geq b \geq c$, potom také platí

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

Posléze sečti dvě permutační nerovnosti tak, aby se jmenovatelé pokrátili.

15. Substituce $x = \frac{1}{a}$, $y = \frac{1}{b}$, $z = \frac{1}{c}$ situaci vyjasní, přitom stále $xyz = 1$. Vynásobení dvěma a použití dvou permutačních nerovností nám dá dolní odhad $x + y + z$, který je zřejmě větší roven třem díky podmínce.

16. Vynásob dvěma, pak dvakrát použij trojice (a, b, c) a $\left(\frac{a^{n-1}}{b+c}, \frac{b^{n-1}}{c+a}, \frac{c^{n-1}}{a+b}\right)$.

17. Vynásob $n - 1$, vezmi posloupnosti $(a_1, a_2, \ldots, a_n)$, $\left(\frac{1}{s-a_1}, \frac{1}{s-a_2}, \ldots, \frac{1}{s-a_n}\right)$ a sečti $n - 1$ cyklicky posunutých permutačních nerovností.

18. Nerovnost zlogaritmuj, vynásob třemi a následně vezmi trojice a, b, c a $\log a$, $\log b$, $\log c$.

22. Čebyšev dvou tříprvkových souhlasně uspořádaných posloupností.

23. Vynásob jmenovatelem pravé strany, které interpretuj jako součet všech jmenovatelů nalevo, pak přichází na řadu Čebyšev pro opačně uspořádané posloupnosti.

24. Pomocí Čebyševovy nerovnosti odhadni každý zlomek zvlášť jako $\frac{a^2+b^2+c^2}{3}$.

25. Vynásob jmenovatelem pravé strany. Pak jsou posloupnosti $\left(\frac{ab}{a+b}, \frac{ac}{a+c}, \frac{bc}{b+c}\right)$ a $(a + b, a + c, b + c)$ souhlasně uspořádané – BÚNO vol $a \geq b \geq c$, což jednoznačně určuje nerovnosti v obou trojicích. Dokazovaná nerovnost je pak odpovídající Čebyšev.

26. Siny a kosiny jsou opačně uspořádané, po zřejmém použití Čebyševovy nerovnosti je potřeba vynásobit vzniklou sumu dvěma a vhodné dvojice členů spojit pomocí součtových vzorců pro sinus.

27. Všechno převeď nalevo, tedy od každého zlomku odečti $\frac{1}{12}$. Využij faktu, že posloupnosti $(a-1, b-1, c-1, d-1)$, $\left(\frac{a+1}{11+a^2}, \frac{b+1}{11+b^2}, \frac{c+1}{11+c^2}, \frac{d+1}{11+d^2}\right)$ jsou souhlasně uspořádané, po provedení Čebyševa využij podmínku.

28. Přičti k nerovnosti ještě jednu závorku z pravé strany, na levé straně popáruj členy se stejnými neznámými a uprav. Levou stranu pak ještě jen tak pro radost vynásob podivnou jedničkou ze zadání. Ověř, že můžeš použít Čebyševa tak, jak bys chtěl(a) (pozor, dá to trochu práci).

29. Díky podmínce je nutně $a^2+b^2+c^2+d^2 \geq 1$. Jmenovatele označme A, B, C, D. Dvakrát za sebou Čebyševuj – poprvé logickým způsobem na zlomky, podruhé pro rozbití sumy třetích mocnin na součin sum prvních a druhých. Druhé mocniny zmizí, dále $3(a+b+c+d) = A+B+C+D$, což jde dokončit snadnou permutační nerovností.

30. Z podmínky si pouze odneseme $x+y+z \geq 3$. Nejdřív použij jasného Čebyševa (jednu posloupnost tvoří čitatele). Označ $x+y+z = 3a$, jmenovatele celého vzniklého výrazu odhadni shora jako $(1+a)^3$. Zbývá se vypořádat s odhadem součtu třetích mocnin pomocí a. Až budeš mít nějakou racionální funkci v a, použij $a \geq 1$.

31. Je potřeba jít trochu do hloubky, předpoklad na nezápornost opravdu musíš využít.

32. Postav se k důkazu stejně, jako k důkazu běžné permutační nerovnosti. Jedním prohozením si nepohoršíme, třeba díky AG.

Literatura a zdroje

Přednáška byla z velké míry inspirovaná přednáškou Fíly Čermáka ze soustředění v Horních Lysečinách (2021). Jeho příspěvek byl úplně megakrásně připravený, tímto jej chci ocenit a velice mu poděkovat.

[1] Filip Čermák: *Permutační nerovnost*, Horní Lysečiny, 2021.
[2] Zdravko Cvetkovski: *Inequalities: Theorems, Techniques and Selected Problems*, Springer-Verlag, 2012.
[3] Michal Rolínek, Pavel Šalom: *Zdolávání nerovností*, Univerzita J. E. Purkyně, 2012.
[4] Gabriel Dospinescu, Titu Andreescu: *Problems from the Book*, XYZ Press, 2008.

Pravděpodobnostní metoda

Adéla Karolína Žáčková

Abstrakt. Pravděpodobnostní metoda je elegantní způsob, jak řešit mnohé (zejména kombinatorické) úložky. V přednášce si ukážeme, že tuto poměrně jednoduchou metodu lze snadno využít na řešení mnohých IMO šestek a jiných jinak náročných příkladů.

Pravděpodobnost nás obklopuje každý den. My si ukážeme, že se dá využít i na jiné věci, než na odhadování, jak moc je pravděpodobné, že dostanu pětku z písemky z dějepisu, když jsem se na ni vůbec neučila. Nejdříve si ale pojďme zopakovat nějaké základy a definice.

Definice. *Elementárním jevem* nazýváme kompletní situaci, která nastala po náhodném procesu, tedy například: „Na první kostce padla trojka, na druhé dvojka a na třetí trojka.“

Definice. *Jevem* pak nazýváme nějakou vlastnost takové situace, například: „Na první kostce padlo sudé číslo.“

Symbolem $A \cap B$ značíme, že nastal jev A a současně nastal jev B, a $A \cup B$ značí, že nastal jev A nebo nastal jev B.

Definice. *Pravděpodobnost*, že jev A nastal, značíme $P(A)$.

Definice. *Nezávislé jevy* jsou takové, pro které platí $P(A \cap B) = P(A) \cdot P(B)$.

Definice. *Pravděpodobnostní prostor* je trojice $(\Omega, \mathcal{F}, P)$, kde Ω je množina elementárních jevů, $\mathcal{F} \subset \Omega$ je množina jevů a $P : \mathcal{F} \to [0, 1]$ pravděpodobnostní funkce, která splňuje následující:

(1) $P(\emptyset) = 0$,
(2) $P(\Omega) = 1$,
(3) pro po dvou disjunktní množiny $A_1, A_2, \ldots$ z $\mathcal{F}$ platí:

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

Příklad. Jako pravděpodobnostní prostor si tedy můžeme například představit házení dvěma kostkami. Naše Ω pak bude množina všech možných situací, které nám mohou nastat, $\mathcal{F}$ může být například množina různých součtů hodnot na obou kostkách.

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

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

Poznámka. Klíčová myšlenka pravděpodobnostní metody

Pokud má jev nenulovou pravděpodobnost, může někdy nastat. To se nám bude hodit v řešení příkladů (viz níže), kdy budeme chtít dokázat, že je něco možné. Mnohdy si tedy vytvoříme náhodnou situaci a u ní dokážeme, že pravděpodobnost chtěného jevu je nenulová.

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

Řešení. Zvolme si náhodnou 14-tici jazyků (uspořádanou, přičemž jazyky se můžou opakovat) a pevného učitele. Pravděpodobnost, že tento učitel nezná první jazyk, je nejvýše $\frac{1}{2}$, stejně tak u druhého jazyku atd. Celkem je tedy pravděpodobnost, že tento učitel nezná ani jeden ze 14 jazyků, rovna 2^{-14}. Za pomoci tvrzení výše získáváme, že pravděpodobnost, že alespoň jeden učitel nezná ani jeden z těchto 14 jazyků, je nejvýše $500 \cdot 2^{-14}$. Tedy pravděpodobnost, že všichni učitelé znají alespoň jeden z těchto 14 jazyků, je $1 - (500 \cdot 2^{-14}) > 0$. Jak jsme již zmínili, má-li jev nenulovou pravděpodobnost, může nastat. Tedy opravdu existuje 14-tice jazyků taková, že každý učitel mluví alespoň jedním z nich.

Úloha 2. Na společenském večeru je n účastníků a n účastnic. Víme, že existuje alespoň $n^2 - n + 1$ různých párů účastník–účastnice, které jsou ochotné spolu tancovat. Dokažte, že všech $2n$ účastníků umíme napárovat tak, aby byli ochotni tancovat v párech, ve kterých skončí.

Úloha 3. Jsou dána nesoudělná přirozená čísla m, n. Jaký je počet cest po mřížce v obdélníku $m \times n$ z levého dolního rohu do pravého horního, které vedou jen doprava a nahoru a jsou celé pod úhlopříčkou? (MKS 26–5)

Úloha 4. Ve skupině 90 dětí má každé alespoň 30 kamarádů (kamarádství je vzájemné). Dokažte, že lze děti rozdělit do tří 30členných skupin tak, aby každé dítě mělo ve své skupince alespoň jednoho kamaráda. (MO 61–III)

Úloha 5. Matematické soutěže se účastnilo 200 studentů, každý z nich řešil šest úloh. Je známo, že každou úlohu správně vyřešilo alespoň 120 studentů. Dokažte, že můžeme najít dva studenty, kteří dohromady vyřešili všechny úlohy. (IMC 2002)

Úloha 6. Ukažte, že je možné obarvit prvky množiny $\{1, 2, \ldots, 1987\}$ čtyřmi barvami tak, aby neexistovala jednobarevná desetiprvková aritmetická posloupnost. (IMO Shortlist 1987)

Úloha 7. V rovině je dáno 100 bodů v obecné poloze. Dokažte, že počet ostroúhlých trojúhelníků nepřekračuje 70 % počtu všech trojúhelníků. (IMO 1970)

Úloha 8. (Dolní odhad na Ramseyova čísla) Dokažte, že hrany úplného grafu na $2^{k/2}$ vrcholech je možné obarvit dvěma barvami tak, aby v nich nebyl žádný úplný jednobarevný podgraf na k vrcholech.

Úloha 9. V tabulce 100×100 jsou napsaná čísla $1, 2, \ldots, 5000$, každé právě dvakrát. Dokažte, že je možné vybrat 100 čísel tak, že z každého sloupce a z každého řádku vybereme právě jedno číslo, a navíc budou tato čísla různá.

Střední hodnota

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

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

$$E[X] = \sum_{\Omega} P(\omega) \cdot X(\omega).$$

Tvrzení. (Počítání střední hodnoty)

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

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

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

Poslední dvě vlastnosti souhrnně nazýváme jako linearitu střední hodnoty.

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

Tvrzení. *Buď X náhodná veličina. Pak existuje elementární jev, pro který platí $X \leq E[X]$, a také jiný elementární jev, pro který platí $X \geq E[X]$.*

Poznámka. Právě poslední zmíněné tvrzení bude pro nás klíčové. Díky němu pak můžeme dokázat existenci "nějaké vhodné konfigurace", která dosáhne alespoň (či nanejvýš) nějaké hodnoty (té střední).

Úloha 10. Skupinka n účastníků si náhodně propermutovala svoje (samozřejmě podepsané) hrníčky. Jaký je očekávaný počet lidí, kteří se mohou napít ze svého vlastního hrníčku?

Úloha 11. Botanický klasifikátor rozeznává 100 atributů rostlin – daná rostlina každý atribut buď má nebo nemá. Klasifikátor je dobrý, pokud každé dvě rostliny mají nanejvýš polovinu svých atributů společných. Dokažte, že dobrý klasifikátor umí popsat nanejvýš 50 rostlin.

Úloha 12. Každé posloupnosti složené z n nul a n jedniček přiřadíme číslo, které je počtem maximálních úseků stejných číslic v ní. (Například posloupnost 00111001 má 4 takové úseky 00, 111, 00, 1.) Pro dané n sečteme všechna čísla přiřazená jednotlivým takovým posloupnostem. Dokažte, že pak výsledný součet je roven $(n+1)\cdot\binom{2n}{n}$. (MO 66–III)

Úloha 13. Nechť F je množina všech n-tic $(A_1, A_2, \ldots, A_n)$, kde každé A_i je podmnožinou $\{1, 2, \ldots, 1998\}$. Označme $|A|$ počet prvků množiny A. Najděte hodnotu

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

(APMO 1998)

Úloha 14. V šachovém turnaji, kterého se zúčastnilo 40 hráčů, se odehrálo celkem 80 partií, přičemž žádná dvojice spolu nehrála víckrát. Ukažte pro co největší n, že existuje n hráčů, kteří mezi sebou nesehráli žádnou partii.

Úloha 15. Mějme n reálných čísel se součtem 0, přičemž alespoň jedno z nich je nenulové. Dokažte, že je umíme pojmenovat $a_1, a_2, \ldots a_n$ tak, že platí nerovnost $a_1a_2 + a_2a_3 + \cdots + a_na_1 < 0$.

Úloha 16. V soutěži je a soutěžících a b porotců, kde $b \geq 3$ je liché číslo. Každý porotce hodnotí každého soutěžícího buď jako „dobrý“, nebo jako „špatný“. Předpokládejme, že k je takové číslo, že pro libovolnou dvojici porotců se jejich hlasy shodovaly u nejvýše k soutěžících. Dokažte nerovnost $\frac{k}{a} \geq \frac{b-1}{2b}$. (IMO 1998)

Úloha 17. V turnaji n hráčů hrál každý s každým právě jednou. *Hamiltonovská cesta* je takové uspořádání n hráčů, že první porazil druhého, druhý třetího atd. Dokažte, že turnaj mohl dopadnout tak, že existovalo alespoň $\frac{n!}{2^{n-1}}$ hamiltonovských cest.

Úloha 18. Na večírku je $n \geq 2$ lidí, někteří se znají (vztah znát se je vzájemný). Dokažte, že existují dva lidé A, B takoví, že mezi zbylými $n-2$ najdeme $\left\lfloor \frac{n}{2} \right\rfloor - 1$ lidí, z nichž každý buď zná A i B, nebo oba nezná.

Úloha 19. Mějme graf G s n vrcholy a $m \geq 4n$ hranami. Dokažte, že kdykoli takový graf nakreslíme do roviny, bude obsahovat alespoň $\frac{m^3}{64n^2}$ průsečíků.

Návody

2. Zvol si náhodné párování. Jaká je pravděpodobnost, že spolu nějaký pár nebude chtít tancovat?

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

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

6. Zvol náhodně obarvení. S jakou pravděpodobností bude jedna vybraná aritmetická posloupnost jednobarevná?

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

8. Vyber náhodný graf. Jaká je pravděpodobnost, že na daných k vrcholech je jednobarevný podgraf?

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

10. Využij indikátorovou veličinu udávající, zda konkrétní účastník má vlastní hrníček.

11. Spočítej střední hodnotu počtu společných atributů pro náhodnou dvojici z r rostlin (bude to nějaký vzoreček v závislosti na r). Dokaž, že pro r bude tato hodnota ostře větší než $\frac{1}{2}$, tudíž bude jistě existovat nějaká dvojice rostlin s více než polovinou společných atributů.

12. Dokaž, že $(n+1)$ je průměrné číslo přiřazené jednotlivým posloupnostem.

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

14. Jaký je průměrný počet odehraných zápasů pro jednotlivé dvojice? Kolik dvojic maximálně tedy mohlo zápas neodehrát?

15. Náhodně popáruj jednotlivá čísla. Může se stát, že jsou všechny součty nulové?

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

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

18. Řeš podobně jako příklad 16.

19. Použij Eulerův vzorec, vyber libovolné nakreslení a následně s pevně zvolenou pravděpodobností smaž každý z vrcholů.

Literatura a zdroje

Tento příspěvek je s pár změnami, přidanými příklady a inspirací přednáškou Mariana Poljaka z MBLka (2020), převzat od Martina Rašky ze soustředění v Zásadě (2021), který jej beze změn převzal od Filipa Bialase ze soustředění v Pasekách (2018), který jej beze změny převzal od Martina Töpfera, který jej vytvořil na soustředění ve Skleném (2015). Všem zmíněným tímto děkuji.

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

Obsah

Eukleidovské obory (Natália Bátorová) . . . 3
Stejnolehlost (Káťa Danilina) . . . 8
Chvála Eukleidova algoritmu (Matěj Doležálek) . . . 13
Čínská zbytková věta (Matěj Doležálek) . . . 18
Vytvořující funkce (Klárka Grinerová) . . . 22
Dirichletův princip (Vít Hanika) . . . 27
Konečné automaty (Petr Hladík) . . . 32
Fibonacciho čísla (Václav Janáček) . . . 37
MO-P (Lenka Kopfová) . . . 39
Derivace (Terka Kučerová) . . . 44
Geometrie čtyřúhelníka (Radek Olšák) . . . 48
Hrátky s nekonečnem (Radek Olšák) . . . 50
Diofantické rovnice (Daniel Perout) . . . 54
Gaussovy a Jacobiho sumy (Zdeněk Pezlar) . . . 58
Kruhová inverze (Zdeněk Pezlar) . . . 63
Sférická geometrie (Matouš Šafránek) . . . 67
Viètovy vztahy (Josef „José“ Soural) . . . 76
Permutační nerovnost (Adéla Karolína Žáčková) . . . 80
Pravděpodobnostní metoda (Adéla Karolína Žáčková) . . . 87