# Zásada

Sborník, podzim 2024

Natália Bátorová
Káťa Danilina
Matěj Doležálek
Alica Dományová
Vojta Gaďurek
Matěj Gajdoš
Klárka Grinerová
Vít Hanika
Michal Pecho
Daniel Perout
Zdeněk Pezlar
Josef „José“ Soural
Jolča Štraitová
Adéla Karolína Žáčková

Autoři: Natália Bátorová, Káťa Danilina, Matěj Doležálek, Alica Dományová, Vojta Gaďurek, Matěj Gajdoš, Klárka Grinerová, Vít Hanika, Michal Pecho, Daniel Perout, Zdeněk Pezlar, Josef „José“ Soural, Jolča Štraitová, Adéla Karolína Žáčková
Editor: Káťa Danilina
vydání první, náklad 44 výtisků
září 2024
Díky za pomoc všem, kterým je za co děkovat.

Za podporu soustředění děkujeme:

ČESKÁ MATEMATICKÁ SPOLEČNOST

qminers

# Eulerova funkcia

Natália Bátorová

Abstrakt. V prednáške sa stretneme s pár aritmetickými funkciami, najmä Eulerovou. Ukážeme si, ako využiť multiplikativitu a zoznámime sa s Eulerovou vetou. Navyše spočítame kopec príkladov, kde si aritmetické funkcie precvičíme.

## Úvod do aritmetických funkcií

**Definícia.** *Aritmetická funkcia* je funkcia z prirodzených čísel do reálnych čísel.

Príklady aritmetických funkcií:

(1) $\pi(n)$ – počet prvočísel menších nanajvýš rovných $n$,
(2) Eulerova funkcia $\varphi(n)$ – počet prirodzených čísel nesúdeliteľných s $n$, ktoré sú menšie rovné $n$,
(3) $\tau(n)$ – počet všetkých kladných deliteľov $n$,
(4) $\sigma(n)$ – súčet všetkých kladných deliteľov $n$,
(5) Möbiova funkcia $\mu$

$$\mu(n) = \begin{cases} 1, & \text{ak } n = 1, \\ (-1)^r, & \text{ak } n = p_1 \cdot p_2 \dots p_r \text{ súčin } r \text{ rôznych prvočísel}, \\ 0, & \text{inak.} \end{cases}$$

**Úloha 1.** Ukážte, že platí $\tau(n) \leq 2\sqrt{n}$.

**Úloha 2.** Rozmyslite si, že $\sum_{d|n} \frac{1}{d} = \frac{\sigma(n)}{n}$.

**Úloha 3.** Je dané prirodzené číslo $k > 1$. Ukážte, že existuje nekonečne veľa čísel $n$ takých, že $\tau(n) = k$, ale len konečne veľa čísel $n$ takých, že $\sigma(n) = k$.

**Úloha 4.** Ukážte, že

$$\sum_{d|n} \mu(d) = \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1 & \text{ak } n = 1, \\ 0 & \text{inak.} \end{cases}$$

**Definícia.** Aritmetická funkcia je *multiplikatívna* ak $f(1) \neq 0$ a pre všetky nesúdelné čísla $m$, $n$ platí $f(mn) = f(m) \cdot f(n)$. Funkcia je *úplne multiplikatívna*, pokiaľ $f(mn) = f(m) \cdot f(n)$ platí pre všetky dvojice prirodzených čísel.

**Úloha 5.** Ukážte, že ak je $f$ multiplikatívna funkcia, tak nutne $f(1) = 1$.

**Úloha 6.** Ukážte, že ak je $f\colon \mathbb{N} \to \mathbb{N}$ rastúca multiplikatívna funkcia a $f(2) = 2$, tak už nutne $f(n) = n$ pre všetky prirodzené $n$.

**Úloha 7.** Ktoré z funkcií $\pi$, $\varphi$, $\tau$, $\sigma$, $\mu$ sú multiplikatívne?

### Eulerova funkcia

**Tvrdenie.** *Nech $n = p_1^{s_1} \cdots p_r^{s_r}$ je prvočíselný rozklad čísla $n > 1$, potom*

$$\varphi(n) = (p_1 - 1) \cdot p_1^{s_1 - 1} \cdots (p_r - 1) \cdot p_r^{s_r - 1}.$$

K dôkazu tohto tvrdenia sa nám môžu hodiť nasledovné vety.

**Veta.** (Čínska veta o zvyškoch) *Nech $m_1, \ldots, m_n$ sú po dvoch nesúdeliteľné prirodzené čísla. Označme $M = m_1 \cdot m_2 \cdots m_n$. Nech $a_1, \ldots, a_n$ sú ľubovoľné celé čísla. Potom existuje práve jedno $x \in \{0, \ldots, M-1\}$ spĺňajúce*

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

**Veta.** (Princíp inklúzie a exklúzie) *Nech $A_1, A_2, \ldots A_n$ sú konečné množiny. Potom*

$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{\substack{I \subset \{1,2,\ldots,n\} \\ I \neq \emptyset}} (-1)^{|I|+1} \left| \bigcap_{i \in I} A_i \right|.$$

**Cvičenie 8.** Dokážte tvrdenie pomocou čínskej vety o zvyškoch.

**Cvičenie 9.** Dokážte tvrdenie pomocou princípu inklúzie a exklúzie.

**Úloha 10.** Ukážte, že pre $n \geq 3$ je $\varphi(n)$ vždy párne.

**Úloha 11.** Dokážte, že ak $a \mid b$, tak potom $\varphi(a) \mid \varphi(b)$. Platí aj opačná implikácia?

**Úloha 12.** Nájdite všetky $n$ také, že $\varphi(n) \leq 2$.

**Úloha 13.** Dokážte, že ak $n = p \cdot q$ a poznáme hodnotu $n$ a $\varphi(n)$, tak vieme jednoznačne určiť prvočísla $p$, $q$.

**Úloha 14.** Ukážte, že

$$\sum_{\substack{1 \leq d \leq n \\ \gcd(d,n)=1}} d = \frac{n \cdot \varphi(n)}{2}.$$

**Úloha 15.** (ťažšia) Ukážte, že $n$ je prvočíslo práve vtedy, keď $n+1 \mid \sigma(n)$ a zároveň $\varphi(n) \mid n - 1$.

**Úloha 16.** Ukážte, že existuje nekonečne veľa čísel $n$ takých, že $n+\varphi(n)$ je piatou mocninou nejakého prirodzeného čísla.

**Úloha 17.** Sú dané čísla $n$, $k$ také, že $n$ je zložené číslo, ktoré má najviac sedem prvočíselných deliteľov a $n-1=k\varphi(n)$. Ukážte, že potom $k=2$.

**Úloha 18.** Ukážte, že

$$\sum_{d|n}(-1)^{\frac{n}{d}}\cdot\varphi(d)=\begin{cases}0, & \text{ak je } n \text{ párne},\\ -n, & \text{ak je } n \text{ nepárne}.\end{cases}$$

**Úloha 19.** Nájdite najmenšie párne $k$ také, že $\varphi(n)\neq k$ pre všetky $n\in\mathbb{N}$.

**Úloha 20.** (ťažšia) Nájdite všetky $n$ také, že $\varphi(n)+\sigma(n)=2n+8$.

**Cvičenie 21.** Dokážte, že platí

$$\varphi(n)=\sum_{d|n}\frac{n}{d}\cdot\mu(d).$$

**Veta.** (Eulerova) *Nech* $x,n\in\mathbb{N}$ a $\gcd(x,n)=1$, *potom* $x^{\varphi(n)}\equiv 1 \pmod{n}$.

**Cvičenie 22.** Dokážte Eulerovu vetu.

**Úloha 23.** Nájdite všetky $n$ spĺňajúce $\varphi(n)=2\cdot 3^{6k+1}$.

**Úloha 24.** Ukážte, že $n\mid\varphi(a^n-1)$.

**Úloha 25.** Ukážte, že $n\mid\varphi(a^n-b^n)$.

### Návody

**1.** Delitele $n$ sa dajú vhodne spárovať.

**2.** To zvládneš!

**3.** Využi, že prvočísel je nekonečne veľa (vieš tento fakt dokázať?). Odhadni $\sigma$ zospodu.

**4.** Použi binomickú vetu.

**5.** Opäť multiplikativita.

**6.** Ukáž, že $f(3)=3$ a rozdeľ si $n$ na štyri prípady mod 4. Použi indukciu.

**7.** Všetky okrem $\pi$. Nájdeš pre túto funkciu protipríklad?

**8.** Označ $m_i=p_i^{s_i}$. Rozmysli si, že každé $x$ nesúdeliteľné s $n$ dáva zvyšok $a_i \pmod{m}_i$ taký, že $p_i\nmid a_i$. Koľko je teda rôznych možností pre výber zvyšku $a_i$?

**9.** Spočítaj čísla súdeliteľné s $n$.

**10.** To zvládneš!

**11.** Aj toto zvládneš!

**12.** Čo keby $n$ bolo prvočíslo? Ako maximálne ho môžeme zväčšiť?

**13.** Urč ich ako korene nejakého polynómu.

**14.** Ako sa líšia $\gcd(d, n)$ a $\gcd(n - d, n)$?

**15.** $n$ je bezštvorcové. $n$ je nepárne alebo $n = 2$. $4 \nmid n+1$. Ak $n = p_1 \cdot p_2 \cdots p_r$, tak dokonca $2^{r-1} \cdot (n + 1) \mid \sigma(n)$.

**16.** Skús hľadať napríklad medzi $n$, ktoré majú najviac 2 prvočíselné delitele.

**17.** Ukáž, že $n$ je bezštvorcové a odhadni $k$ zvrchu. Môže byť $n$ párne?

**18.** Pokiaľ je $n$ párne číslo, kedy je $\frac{n}{d}$ párne a kedy nepárne? Rozmysli si, že

$$\sum_{d|n} \varphi(d) = \sum_{d|n} \varphi\left(\frac{n}{d}\right)$$

a $\varphi(\frac{n}{d})$ je počet čísel menších rovných $n$, ktorých najväčší spoločný deliteľ s $n$ je $d$.

**19.** To zvládneš!

**20.** Ukáž, že $n$ má najviac 2 prvočíselné delitele (využi napr. vzťah $\sum_{d|n} \varphi(n) = n$) a rozober možnosti.

**21.** Skús použiť princíp inklúzie a exklúzie.

**22.** Rozmysli si, že ak $\gcd(x, n) = 1$, tak pre množiny

$$M = \{m \bmod n \mid \gcd(x, n) = 1\},$$
$$xM = \{x \cdot m \bmod n \mid \gcd(x, n) = 1\}.$$

platí $M = aM$.

**23.** Koľko rôznych prvočíselných deliteľov má $n$? Pozri sa na $\varphi(n) \bmod 7$.

**24.** $a^n \equiv 1 \pmod{a^n - 1}$ rovnako tak $a^{\varphi(a^n-1)} \equiv 1 \pmod{a^n - 1}$. Čo teraz s tým?

**25.** Stačí uvažovať $\gcd(a, b) = 1$ (prečo to stačí?). Potom vieme nájsť $c$ také, že $ac \equiv b \pmod{a^n - b^n}$. Aký zvyšok mod $a^n - b^n$ dáva $c^n$? Aký zvyšok dáva $c^{\varphi(a^n-b^n)}$?

### Literatura a zdroje

[1] Pepa Svoboda: *Aritmetické funkce*, Hojsova Stráž, 2016.
[2] *Archív olympiád, https://artofproblemsolving.com/community*.

# Největší společný dělitel

Káťa Danilina

Abstrakt. Tento příspěvek čtenáře seznámí s vlastnostmi největšího společného dělitele a ukáže, že ve spojení s Eukleidovým algoritmem pomůže s řešením spousty příkladů.

**Úmluva.** Není-li řečeno jinak, číslem budeme myslet celé číslo.

**Definice.** Řekneme, že číslo $a \neq 0$ *dělí* číslo $b$ (píšeme $a \mid b$), pokud existuje číslo $c$ takové, že $ac = b$.

**Tvrzení.** *Pokud $a \mid b$ a zároveň $b \neq 0$, pak $|a| \leq |b|$. Pokud navíc $|a| \neq |b|$, tak $2 \cdot |a| \leq |b|$ atd.*

**Úloha 1.** Určete všechna celá kladná čísla $m$, $n$ taková, že $n$ dělí $2m-1$ a zároveň $m$ dělí $2n-1$. (MO 59–A–II–3)

**Definice.** Mějme čísla $a$, $b$. Pak jejich *největší společný dělitel* (NSD) je největší přirozené číslo $d$ takové, že $d \mid a, b$. Značíme ho $(a, b)$. Podobně *nejmenší společný násobek* (nsn) je nejmenší přirozené číslo $d$ takové, že $a \mid d$ a $b \mid d$, značíme jej $[a, b]$.

Na NSD se můžeme dívat jako na číslo, které je dělitelné všemi ostatními společnými děliteli. Podobně nsn dělí všechny společné násobky.

**Tvrzení.** *Platí:*

(i) $(a, a) = (a, 0) = (-a, 0) = [a, a] = [a, 1] = |a|$.
(ii) $(a, b) = (b, a) = (a - b, b) = (b - a, b) = (a - b, a) = (a + b, a)$.
(iii) $(a, b) = |a|$, *právě když* $a \mid b$, *a také právě když* $[a, b] = |b|$.
(iv) $(ab, ac) = a(b, c)$.
(v) $(a, b)[a, b] = ab$.
(vi) *Pokud* $d \mid a, d \mid b$, *tak i* $d \mid (a, b)$.
(vii) $(b, c) \mid (ab, c) \mid (a, c)(b, c) \mid a(b, c)$.

**Tvrzení.** (Eukleidův algoritmus) *Díky druhé vlastnosti můžeme spočítat $(a, b)$ tak, že odečteme menší číslo od většího, dostaneme novou dvojici čísel (se stejným* NSD*) a postup budeme opakovat, dokud nebude jedno z čísel nula.*

Dost často se vyplatí rovnou odečíst menší číslo tolikrát, kolikrát to jde, neboli jím dělit se zbytkem.

**Úloha 2.** Určete, kolik (uspořádaných) dvojic přirozených čísel $a$, $b$ splňuje rovnici $[a, 70] + [b, 70] = 210$.

**Tvrzení.** (Bézout) *Mějme čísla $a$ a $b$. Potom jsou čísla tvaru $ka + \ell b$ pro celá $k$ a $\ell$ vždy násobky $(a, b)$ a naopak každý násobek $(a, b)$ umíme vyjádřit ve tvaru $ka + \ell b$.*

**Definice.** O číslech $a$, $b$ řekneme, že jsou *nesoudělná*, pokud $(a, b) = 1$.

**Tvrzení.** *Platí:*

(i) *Pokud* $(b, c) = 1$, *pak* $(ab, c) = (a, c)$.
(ii) *Pokud* $(b, c) = 1$, *pak* $(a, bc) = (a, b)(a, c)$.

**Úloha 3.** Určete, pro která čísla $a$, $b$, $c$ platí $[a, c] + [b, c] = (a + b)c$.

**Úloha 4.** Určete možné hodnoty výrazů pro nesoudělná čísla $a$, $b$:

(i) $(a + b, ab)$,
(ii) $(a^2 + b^2, ab)$,
(iii) $(a + b, a - b)$,
(iv) $\left(a^3, (a + 1)^5\right)$.

**Úloha 5.** Ukažte, že zlomek

$$\frac{21n + 4}{14n + 3}$$

je v základním tvaru pro každé přirozené číslo $n$. (IMO 1959)

**Úloha 6.** Pro která celá čísla $n$ je výraz

$$\frac{n^3 - 3}{n - 3}$$

celočíselný? (Náboj 2007)

**Úloha 7.** S využitím vztahu $F_{n+m} = F_{m+1} \cdot F_n + F_m \cdot F_{n-1}$ ukažte, že pro Fibonacciho posloupnost platí $(F_m, F_n) = F_{(m,n)}$.

**Úloha 8.** Zjistěte, pro která přirozená čísla $a$, $b$ je hodnota podílu

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

rovna celému číslu. (MO 57–A–III–3)

**Úloha 9.** Dokažte, že pro všechna přirozená $m, n$ splňující $n \geq m \geq 1$ je výraz

$$\frac{(m, n)}{n} \binom{n}{m}$$

přirozené číslo.

### Rozklad na $du$, $dv$

Často se v úlohách vyplatí rozepsat čísla $a$, $b$ jako $a = du$, $b = dv$, kde $d = (a, b)$.

**Úloha 10.** Určete, pro která čísla $a$, $b$ platí $(a, b) + [a, b] = a + b$.

**Úloha 11.** Rozhodněte, zda součet některých dvou přirozených čísel je dělitelem jejich nejmenšího společného násobku.

**Úloha 12.** Najděte všechny dvojice přirozených čísel $x$, $y$ takové, že

$$\frac{xy^2}{x+y}$$

je prvočíslo. (MO 58–A–I–3)

**Úloha 13.** Nechť $n$, $k$ jsou přirozená čísla a $k$ je navíc bezčtvercové[1]. Předpokládejme, že

$$\frac{n^3 + 2n^2 + k}{n^2 + k}$$

je celé číslo. Dokažte, že pak už platí $n = k$. (MKS 33–9–1)

**Úloha 14.** Jsou dána přirozená čísla $a$, $b$, $c$, dokažte, že

$$[a, b] \neq [a + c, b + c].$$

(Japonsko 2017)

**Úloha 15.** Pro dané prvočíslo $p$ najděte všechny trojice přirozených čísel $(a, b, c)$ z množiny $\{1, 2, \ldots, 2p^2\}$ splňující

$$\frac{[a, c] + [b, c]}{a + b} = \frac{p^2 + 1}{p^2 + 2} \cdot c.$$

(MO 59–A–I–6)

### Řešení pro jedno prvočíslo

Nechť v prvočíselných rozkladech $a$ a $b$ je $p^\alpha$ a $p^\beta$, pak v prvočíselných rozkladech $(a, b)$ a $[a, b]$ bude $p^{\min(\alpha,\beta)}$ a $p^{\max(\alpha,\beta)}$.

**Úloha 16.** Ukažte, že pro všechna přirozená $a$, $b$, $c$ platí

$$[a, b][a, c][b, c] \geq [a, b, c]^2.$$

[1] Bezčtvercové číslo je takové, které pro $a > 1$ není dělitelné číslem $a^2$.

**Úloha 17.** Dokažte, že pro libovolná přirozená čísla $a$, $b$, $c$ platí

$$\frac{[a,b,c]^2}{[a,b]\cdot[b,c]\cdot[c,a]} = \frac{(a,b,c)^2}{(a,b)\cdot(b,c)\cdot(c,a)}.$$

(USAMO 1972)

**Úloha 18.** Ukažte, že pokud $[a,b,c](a,b,c) = abc$, pak $(a,b) = 1$, $(a,c) = 1$ a $(b,c) = 1$.

**Úloha 19.** Platí, že $(a,b,c) = 1$ a zároveň $c = \frac{ab}{a-b}$. Dokažte, že $(a-b)$ je čtverec.

**Úloha 20.** Nechť $a_1, \ldots, a_k, b_1, \ldots, b_k$ jsou přirozená čísla, která splňují $(a_i, b_i) = 1$ pro každé $i \in \{1, \ldots, k\}$. Dále buď $m = [b_1, \ldots, b_k]$. Ukažte, že platí

$$\left(\frac{a_1 m}{b_1}, \ldots, \frac{a_k m}{b_k}\right) = (a_1, \ldots, a_k).$$

(IMO shortlist 1974)

## Návody

**1.** Rozeber možnosti $n = 2m - 1$ (resp. $m = 2n - 1$) a pak využij první tvrzení.

**2.** Jedno z čísel musí být dělitel 70 a druhé násobek 4 a dělitel 140.

**3.** Platí, že $[a, c] \mid ac$.

**4.** V (i), (ii) použij $(a, bc) = (a, b)(a, c)$ pro nesoudělná $b, c$ a poté $(a, b) = (a-b, b)$. Pro (iii) opět $(a, b) = (a - b, b)$. Ve (iv) se zabývej společným prvočinitelem obou výrazů.

**5.** Eukleidův algoritmus.

**6.** Výraz je celočíselný, právě když $|n - 3| = (n^3 - 3, n - 3)$. Následně aplikuj Eukleidův algoritmus.

**7.** Nejprve dokaž, že po sobě jdoucí členy jsou nesoudělné, poté že pokud $i \mid j$, pak $F_i \mid F_j$. Poté použij Eukleidův algoritmus na indexy.

**8.** Jmenovatel musí dělit i součet čitatele se jmenovatelem. Tento součet rozlož na součin a ukaž, že jeden člen je se jmenovatelem nesoudělný.

**9.** Vyjádři si NSD pomocí Bézouta, pak upravuj.

**10.** Po substituci $a = du$, $b = dv$ a úpravě výrazu rozlož na součin.

**11.** Po substituci $a = du$, $b = dv$ a podělení obou stran dělitelnosti $d$ ukaž, že obě strany dělitelnosti jsou nyní nesoudělné.

**12.** Po substituci $x = du$, $y = dv$ ukaž, že $u+v \mid d^2$ a $uv^2$ dělí celý zlomek. Rozeber dva případy, $v = 1$ a $u > 1$ a rozlož $d^2 - 1$ na součin. V druhém případě jen dosaď za $u$ a $v$.

**13.** Po substituci $n = du$, $k = dv$ si uvědom, že $(d, v) = 1$ a zkus něco vytknout. Potom si všimni velikostí.

**14.** Označ si $(a, b) = d$ a $(a + c, b + c) = e$, pak $a = du$, $b = dv$ a $a + c = ex$, $b + c = ey$. Pak si pomocí nových proměnných vyjádři nsn a $a - b$.

**15.** Využij $[a, c] = \frac{ac}{(a,c)} = \frac{a}{(a,c)}c$. Poté odhaduj podle velikosti $(a, c)$ a $(b, c)$.

**16.** Označ si mocniny prvočísel v jednotlivých rozkladech.

**17.** Podívej se na největší mocniny prvočísla $p$ v jednotlivých výrazech.

**18.** Uvaž kolikrát je $p$ v jednotlivých číslech.

**19.** Uvaž prvočíslo, co dělí $(a, b)$. Pak si označ největší mocniny takové, že $p^\alpha \mid a$ a $p^\beta \mid b$, rozmysli si, co pro ně musí platit, aby byla splněná rovnost ze zadání.

**20.** Dokazuj pro jedno prvočíslo. Pokud $p \mid m$, vyber si takové $i$, že $b_i$ má největší mocninu $p$.

## Literatura a zdroje

Děkuji Fílovi Čermákovi, jehož příspěvek z Lipové-lázně roku 2022 jsem s malými úpravami převzala.

# Pellova rovnice a kvadratické řády

Matěj Doležálek

Abstrakt. Podíváme se na zub diofantické rovnici $x^2 - Dy^2 = 1$, zvané Pellova. Cesta do hlubin její duše nás zavede do zákoutí teorie čísel, kde se s odmocninami smí pracovat jako s celými čísly. Tento pohled odhalí bohatou strukturu „pod“ řešeními Pellovy rovnice a umožní nám ukázat, jak všechna řešení vyrobit z toho nejmenšího.

Jako „Pellova“ je známa diofantická rovnice

$$x^2 - Dy^2 = 1, \tag{♡}$$

kde $D$ smí být jakékoliv kladné celé číslo, které není čtvercem celého čísla, a řešení $(x, y)$ hledáme opět v celých číslech. Zajímavá je pro nás především tím, že v sobě skrývá poměrně hlubokou strukturu, a skýtá tak lehký úvod do algebraické teorie čísel.

Dvě řešení Pellovy rovnice jsou okamžitě zjevná: $(\pm 1, 0)$. Anžto nejsou moc zajímavá, budeme jim říkat *triviální řešení*. Postupně ukážeme, že Pellova rovnice má vždy netriviální řešení a že to „nejmenší“ z nich „generuje“ všechna ostatní – stačí jen vágním výrazům v uvozovkách dodat korektní význam.

**Úmluva.** Neřekneme-li jinak, bude $D$ vždy nějaké kladné celé nečtvercové číslo. Občas předpoklady o něco zesílíme a budeme požadovat, aby to bylo *bezčtvercové* kladné celé číslo, tedy aby jej žádné prvočíslo nedělilo v druhé mocnině.

**Úmluva.** „Úlohy“ jsou v tomto příspěvku příklady povětšinou takového stylu, že by se (teoreticky) daly potkat v nějaké olympiádě. „Zamyšlení“ jsou cvičeníčka, která pomohou utvořit si ucelenější představu nebo jsou zajímavé z více vysokoškolského hlediska, ale při řešení úloh nejspíš nepomohou. Naproti tomu „Cvičení“ jsou přístupné pravdy, které se hodí mít na paměti a při řešení úloh pomoci velice mohou.

### Přidáváme odmocninu

**Definice.** *(Reálným) kvadratickým tělesem* budeme rozumět množinu (reálných) čísel tvaru $\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\}$, tedy množinu všech $a + b\sqrt{D}$ pro všechna možná $a, b \in \mathbb{Q}$.

Obecně *tělesem* nazýváme množinu $K$, ve které umíme sčítat, odčítat, násobit a dělit (nenulovými prvky) za platnosti všech obvyklých pravidel (a výsledky těchto operací vždy opět leží v $K$). Že je $\mathbb{Q}(\sqrt{D})$ skutečně tělesem, budeme schopni ověřit po vybudování několika nástrojů.

**Zamyšlení 1.** Kdy platí $\mathbb{Q}(\sqrt{D_1}) = \mathbb{Q}(\sqrt{D_2})$?

**Cvičení 2.** Rozmyslete si, že pokud pro $a_1, b_1, a_2, b_2 \in \mathbb{Q}$ platí $a_1 + b_1\sqrt{D} = a_2 + b_2\sqrt{D}$, pak už nutně $a_1 = a_2$ a zároveň $b_1 = b_2$.

Poslední cvičení tedy ospravedlňuje, že „$a + b\sqrt{D}$ umí poznat svoje $a$ a $b$“. Může nás proto napadnout uvnitř $\mathbb{Q}(\sqrt{D})$ rozeznat význačnou množinu těch čísel, která mají $a$ i $b$ celočíselné, tedy $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}$. Ta tvoří *okruh*: množinu, kde umíme sčítat, odečítat a násobit podle obvyklých pravidel (a která je uzavřená na tyto operace). Budeme je používat jako obdobu celých čísel v $\mathbb{Q}(\sqrt{D})$.[1]

**Zamyšlení 3.** Nahlédněte, že $\mathbb{Z}[\sqrt{D}]$ skutečně je okruh.

**Zamyšlení 4.** Pro $D \equiv 1 \pmod 4$ je i $\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] = \left\{a + b\frac{1+\sqrt{D}}{2} \;\middle|\; a, b \in \mathbb{Z}\right\}$ okruh.

**Definice.** Pro každé $\alpha = a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$ definujeme jeho *sdružené číslo* jako $\overline{\alpha} = a - b\sqrt{D}$. Následně pak definujeme jeho *normu* $\mathrm{N}(\alpha) = \alpha\overline{\alpha} = a^2 - Db^2$ a jeho *stopu* $\mathrm{Tr}(\alpha) = \alpha + \overline{\alpha} = 2a$.

**Zamyšlení 5.** Rozmyslete si:

(i) Jediným $\alpha \in \mathbb{Q}(\sqrt{D})$ s $\mathrm{N}(\alpha) = 0$ je $\alpha = 0$.
(ii) Pro $0 \neq \alpha \in \mathbb{Q}(\sqrt{D})$ je $\frac{1}{\alpha} = \frac{\overline{\alpha}}{\mathrm{N}(\alpha)}$.
(iii) $\mathbb{Q}(\sqrt{D})$ je skutečně těleso.

**Cvičení 6.** ((i)racionální část) Pro $a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$ platí

$$a = \frac{\alpha + \overline{\alpha}}{2} \qquad \text{a} \qquad b = \frac{\alpha - \overline{\alpha}}{2\sqrt{D}}.$$

Na prvky kvadratických těles jsme se od začátku dívali jako $\alpha = a + b\sqrt{D}$, tedy jako na dvojici $(a, b)$. Tenhle pohled ale není vždy ten nejužitečnější, přinejmenším je trochu arbitrární a nepřirozený. Občas může být lepší se na $\alpha$ dívat jako na dvojici reálných čísel $(\alpha, \overline{\alpha})$, ačkoliv ne každá dvojice reálných čísel tímto způsobem odpovídá nějakému $\alpha \in \mathbb{Q}(\sqrt{D})$. Předchozí cvičení však ilustruje, že lze od $(\alpha, \overline{\alpha})$ snadno přejít k $(a, b)$.

**Cvičení 7.** (sdružení je homomorfismus) Rozmyslete si, že pro $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$ platí $\overline{(\alpha\beta)} = \overline{\alpha}\,\overline{\beta}$ a $\overline{(\alpha + \beta)} = \overline{\alpha} + \overline{\beta}$.

**Cvičení 8.** (norma je multiplikativní) $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\,\mathrm{N}(\beta)$.

**Zamyšlení 9.** (stopa je aditivní) $\mathrm{Tr}(\alpha + \beta) = \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta)$.

[1] Tahle věta morálně vzato trochu kecá, tak ji berte jen neformálně.

Označíme-li nyní $\omega = x + y\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$, pak lze Pellovu rovnici přeformulovat jako $\mathrm{N}(\omega) = 1$. Už víme, že $\omega$ jako reálné číslo zná svoje $x$ a svoje $y$, proto si dovolíme samotné $\omega$ nazývat *řešením Pellovy rovnice*. Triviálními řešeními jsou v tomto pohledu $\pm 1$.

Všimněme si, že toto už nám zadarmo dává možnost např. násobit řešení Pellovy rovnice mezi sebou navzájem, což při pohledu skrz $(x, y)$ nedávalo moc smysl. Multiplikativita normy ospravedlňuje, že součin dvou řešení je opět řešení, což už je předzvěstí struktury, již odhalíme v následující kapitole.

**Cvičení 10.** (dolní celé části) Pokud $\alpha \in \mathbb{Z}[\sqrt{D}]$ splňuje $\overline{\alpha} \in (0, 1)$, pak $\lfloor \alpha \rfloor = \mathrm{Tr}(\alpha) - 1$.

### Existence a struktura řešení Pellovy rovnice

Dokažme nyní, že Pellova rovnice má vždy netriviální řešení. Propracujeme se k tomu několika kroky.

**Věta.** (Dirichletova o diofantických aproximacích) *Budiž $\alpha$ reálné číslo a $N$ kladné celé číslo. Pak existují $q \in \{1, \dots, N\}$ a $p \in \mathbb{Z}$ takové, že $|q\alpha - p| < \frac{1}{N}$.*

**Lemma A.** *Pro iracionální $\alpha$ existuje nekonečně mnoho zlomků $\frac{p}{q}$ v základním tvaru splňujících $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$. Je-li $\alpha = \sqrt{D}$, pak navíc všechna tato $\frac{p}{q}$ splňují $\left|\mathrm{N}(p + q\sqrt{D})\right| < 2\sqrt{D} + 1$.*

**Lemma B.** *Pokud $\mathrm{N}(x + y\sqrt{D}) = \mathrm{N}(z + w\sqrt{D}) = n$ a zároveň $x \equiv z$ a $y \equiv w \pmod{n}$, pak už $\frac{x+y\sqrt{D}}{z+w\sqrt{D}} \in \mathbb{Z}[\sqrt{D}]$, a rovnou se jedná o řešení Pellovy rovnice.*

**Věta.** (existence) *Pro nečtvercové kladné celé $D$ má Pellova rovnice $x^2 - Dy^2 = 1$ netriviální řešení.*

*Důkaz.* (skeč) Lemmatem A nagenerujeme nekonečně mnoho prvků $\mathbb{Z}[\sqrt{D}]$, které mezi sebou mají jen konečně mnoho různých norem. Nějaká norma $n$ je pak zastoupena nekonečně mnoha prvky. Ty se rozdělí mezi $n^2$ dvojic zbytkových tříd racionální a iracionální části modulo $n$, nějaká tak bude mít nekonečně mnoho zástupců. Lemmatem B je podíl kterýchkoliv dvou z nich řešením Pellovy rovnice. □

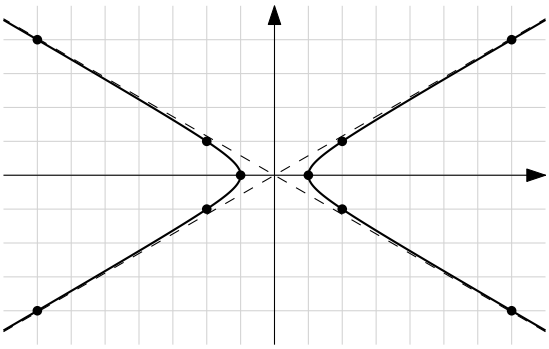
Celkem efektivně lze řešení hledat pomocí řetězových zlomků, ale tím se tu nebudeme zabývat (zvídavý čtenáři, viz kapitolu 2 v [2]).

**Lemma.** *Uvažujme $x_1 + y_1\sqrt{D}, x_2 + y_2\sqrt{D} \in \mathbb{Q}(\sqrt{D})$, která mají obě normu 1 a navíc $x_1, x_2, y_1, y_2 \geq 0$. Potom*

$$x_1 \leq x_2 \quad \Longleftrightarrow \quad x_1 + y_1\sqrt{D} \leq x_2 + y_2\sqrt{D} \quad \Longleftrightarrow \quad y_1 \leq y_2.$$

Je tedy jedno, zda porovnáváme řešení Pellovy rovnice (aspoň ta s kladnými částmi) jako reálná čísla, nebo podle jejich $x$, nebo podle jejich $y$ – výsledek bude vždy stejný.

Podívejme se nyní na množinu řešení $\omega = x + y\sqrt{D}$ Pellovy rovnice. Už víme, že existují nějaká netriviální. Znaménko u $x$ i $y$ můžeme vždy obrátit, takže se BÚNO stačí dívat na řešení s kladnými částmi. Pak můžeme vybrat to s nejmenším $x$ a bude to totéž, jako vybrat to s nejmenším $y$ nebo prostě to nejmenší $\omega$. Tomuto nejmenšímu $\omega$ budeme říkat *fundamentální řešení Pellovy rovnice.*



**Věta.** (grupová struktura) *Ať je $\omega_0$ fundamentální řešení Pellovy rovnice. Potom jsou řešeními Pellovy rovnice právě všechna čísla tvaru $\pm\omega_0^n$ pro $n \in \mathbb{Z}$.*

**Cvičení 11.** (znaménka) Ať je $\omega_0$ fundamentální řešení Pellovy rovnice a $\omega_0^n = x + y\sqrt{D}$. Pak je $x$ vždy kladné, zatímco $y$ má stejné znaménko jako $n$.

Velikost fundamentálního řešení je velice těžko předvídatelná, proto může být jeho hledání hrubou silou zrádné. I pro některá vcelku malá $D$ může být veliké, např. pro $D = 61$ je $\omega_0 = 1766319049 + 226153980\sqrt{61}$.

**Cvičení 12.** Nahlédněte, že:

(i) Uvážíme-li rovnici $|\mathrm{N}(\omega)| = 1$ místo $\mathrm{N}(\omega) = 1$, stále existuje nějaké $\omega_0$ („fundamentální jednotka“) takové, že všechna řešení jsou $\omega = \pm\omega_0^n$ pro $n \in \mathbb{Z}$.

(ii) Pokud $D \equiv 1 \pmod 4$, pak i pro $\omega \in \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$ existuje „fundamentální řešení“ $\omega_0$ rovnice $\mathrm{N}(\omega) = 1$ splňující, že všechna řešení jsou $\omega = \pm\omega_0^n$ pro $n \in \mathbb{Z}$. Taktéž s $|\mathrm{N}(\omega)| = 1$ (potenciálně s jiným $\omega_0$).

**Cvičení 13.** Nalezněte explicitní předpis pro fundamentální řešení Pellovy rovnice v závislosti na kladném celočíselném parametru $a$, pokud

(i) $D = a^2 - 1$, (ii) $D = a^2 + 1$, (iii) $D = a^2 - 2$, (iv) $D = a^2 + 2$.

### Základní úlohy

**Úloha 14.** *Pythagorejským trojúhelníkem* rozumějme pravoúhlý trojúhelník s celočíselnými délkami stran. Rozhodněte, zda existuje nekonečně mnoho (navzájem neshodných) pythagorejských trojúhelníků, v nichž se délky odvěsen liší o 1.

**Úloha 15.** Najděte nějaké kladné celé $n \geq 1000$, pro než je $1+2+\cdots+n$ čtverec.

**Úloha 16.** Kladné celé číslo nazvěme *aspoňčtvercovým*, pokud jsou všechny exponenty v jeho prvočíselném rozkladu alespoň 2. Dokažte, že existuje nekonečně mnoho párů po sobě jdoucích aspoňčtvercových čísel.

**Úloha 17.** Uvažujme $n$ kladné celé. Dokažte, že pokud je $2+2\sqrt{28n^2+1}$ celé, pak už je rovnou čtverec.

**Cvičení 18.** Nahlédněte:

(i) Pokud má pro nějaké $c \in \mathbb{Z}$ rovnice $x^2 - Dy^2 = c$ celočíselné řešení, pak už jich má nekonečně mnoho.

(ii) Ať je $\omega_0$ fundamentální řešení Pellovy rovnice. *Orbitou* nazvěme množinu tvaru $\{\pm\omega_0^n\alpha \mid n \in \mathbb{Z}\}$ pro nějaké $\alpha \in \mathbb{Z}[\sqrt{D}]$. Dokažte, že množina prvků $\beta \in \mathbb{Z}[\sqrt{D}]$ normy $c$ je tvořena konečně mnoha (např. nanejvýš $c^2$) orbitami.

**Cvičení 19.** (těžší) Pro prvočíslo $p \equiv 1 \pmod 4$ má záporná Pellova rovnice $x^2 - py^2 = -1$ řešení.

**Úloha 20.** Dokažte, že existuje nekonečně mnoho kladných celých čísel $n$, pro něž $n^2+1 \mid n!$.

**Úloha 21.** Dokažte, že pokud $n^2$ je rozdílem třetích mocninc dvou po sobě jdoucích celých čísel, pak je $2n-1$ čtverec celého čísla.

**Úloha 22.** (polynomální Pell) Dokažte, že pro každé kladné celé $n$ existují polynomy $f$, $g$ s celočíselnými koeficienty takové, že $f$ má stupeň $n$ a zároveň $f^2 = (x^2-1)g^2+1$.

**Úloha 23.** Najděte nekonečně mnoho trojic kladných celých čísel $(a,b,c)$, které tvoří aritmetickou posloupnost a navíc splňují, že $ab+1$, $bc+1$ i $ca+1$ jsou čtverce.

**Cvičení 24.** (dvojky) Ať $\alpha \in \mathbb{Z}[\sqrt{D}]$ má normu 2 nebo $-2$. Potom $\alpha^2 = 2\omega$ pro nějaké $\omega \in \mathbb{Z}[\sqrt{D}]$ s normou 1.

### Vysokoškolštější pohled

Dosud jsme trochu chodili kolem horké kaše ohledně toho, že kromě $\mathbb{Z}[\sqrt{D}]$ se občas můžeme taky dívat na $\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$ pro $D \equiv 1 \pmod 4$. Taky jsem možná naznačil, že není úplně fér označit $\mathbb{Z}[\sqrt{D}]$ za „celá čísla v $\mathbb{Q}(\sqrt{D})$“. Nyní je čas postavit se těmto nuancím čelem. Začneme motivujícím cvičením:

**Cvičení 25.** Každé $\alpha \in \mathbb{Q}(\sqrt{D})$ splňuje $\alpha^2 = \mathrm{Tr}(\alpha)\alpha - \mathrm{N}(\alpha)$.

To naznačuje, že k tomu, aby $\{a+b\alpha \mid a,b \in \mathbb{Z}\}$ byl okruh, je klíčové $\mathrm{Tr}(\alpha)$, $\mathrm{N}(\alpha) \in \mathbb{Z}$. To motivuje:

**Definice.** Řekneme, že $\alpha \in \mathbb{Q}(\sqrt{D})$ je *celistvé*, pokud jsou $\mathrm{Tr}(\alpha)$ i $\mathrm{N}(\alpha)$ celá čísla. *Řádem v* $\mathbb{Q}(\sqrt{D})$ budeme rozumět množinu tvaru $\mathbb{Z}[\alpha] = \{a + b\alpha \mid a, b \in \mathbb{Z}\}$ pro nějaké celistvé[2] $\alpha \in \mathbb{Q}(\sqrt{D}) \setminus \mathbb{Q}$.

Takhle zformulovaná definice pořád trochu kecá – správnější by bylo říct, že řád je mřížka uzavřená na násobení obsahující jedničku. Ale to bychom museli zase říct, co je to mřížka, a na to tu není čas, proto se spokojíme s tímhle. Pozor na dvojici nástrah: Zaprvé, tato definice je specificky šitá na míru kvadratickým tělesům, pro práci v tělesech vyššího stupně by bylo potřeba pracovat ještě o úroveň obecněji (zvídavý čtenáři, viz [4]). Zadruhé, *řád* je v matematice bohužel dost nadužívané slovo, vyvarujte se proto záměně s dalšími jeho významy (multiplikativní řád zbytkové třídy modulo něco, řád grupy, řád čtvercové matice, řád ve smyslu uspořádání…).

Pointou zavedení řádů je hlavně uvědomění, že $\mathbb{Z}[\sqrt{D}]$ a $\mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$ se příliš zásadně neliší a můžeme v nich pracovat v podstatě stejně.

**Zamyšlení 26.** Nahlédněte, že každý řád v $\mathbb{Q}(\sqrt{D})$ je okruh a že všechny prvky libovolné řádu jsou celistvé.

**Zamyšlení 27.** Ať je $D$ bezčtvercové. Pak množina $\mathcal{O}_K$ celistvých prvků v $K = \mathbb{Q}(\sqrt{D})$ splňuje

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}], & D \equiv 2, 3 \pmod 4, \\ \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right], & D \equiv 1 \pmod 4, \end{cases}$$

takže se jedná o řád. Nazývá se *okruh celistvých prvků* $K$.

### Modulení

**Definice.** Ať je $\mathcal{O} \subset \mathbb{Q}(\sqrt{D})$ řád a $\alpha, \beta \in \mathcal{O}$. Řekneme, že $\alpha$ *dělí* $\beta$ (nebo že $\beta$ *je násobkem* $\alpha$) *v* $\mathcal{O}$, pokud existuje $\gamma \in \mathcal{O}$ takové, že $\beta = \alpha\gamma$. Značíme $\alpha \mid \beta$; pokud nebude $\mathcal{O}$ zjevné z kontextu, můžeme ho připsat do dolního indexu jako $\alpha \mid_{\mathcal{O}} \beta$.

Pozor: takto definovaná dělitelnost závisí na tom, v jakém řádu ji uvažujeme! Kupříkladu 2 dělí $1 + \sqrt{5}$ v $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$, ale nikoliv v $\mathbb{Z}[\sqrt{5}]$.

**Definice.** Buď $\mathcal{O} \subset \mathbb{Q}(\sqrt{D})$ řád a $\alpha, \beta, \gamma \in \mathcal{O}$. Řekneme, že $\alpha$ *je kongruentní* $\beta$ *modulo* $\gamma$ *(v* $\mathcal{O}$*)*, pokud $\gamma \mid \alpha - \beta$ v $\mathcal{O}$. Tuto skutečnost značme $\alpha \equiv \beta \pmod \gamma$, anebo, chceme-li zdůraznit, v kterém řádu pracujeme, $\alpha \equiv \beta \pmod{\gamma\mathcal{O}}$.

*Zbytkovou třídou modulo* $\gamma$ *(v* $\mathcal{O}$*)* rozumíme množinu všech prvků $\mathcal{O}$ kongruentní jednomu danému $\alpha$ modulo $\gamma$. Množinu všech zbytkových tříd modulo $\gamma$ značme $\mathcal{O}/\gamma\mathcal{O}$.

Zdůrazněme, že opět závisí na volbě řádu, ve kterém pracujeme: $\sqrt{5} \equiv 1 \pmod 2$ v $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$, ale nikoliv v $\mathbb{Z}[\sqrt{5}]$.

[2]Podmínka $\alpha \notin \mathbb{Q}$ je trochu technická, ale zjednodušeně řečeno nechceme povolit, aby $\mathbb{Z}$ byl řád v $\mathbb{Q}(\sqrt{D})$.

Zafixujme na okamžik $\gamma$ a $\mathcal{O}$ a značme $[\alpha] = \{\alpha' \in \mathcal{O} \mid \alpha' \equiv \alpha \pmod{\gamma\mathcal{O}}\}$ zbytkovou třídu $\alpha$. Potom můžeme zavést sčítání a násobení zbytkových tříd pomocí

$$[\alpha] + [\beta] = [\alpha + \beta] \qquad \text{a} \qquad [\alpha][\beta] = [\alpha\beta].$$

Z definic pak lze dokázat, že toto je dobře definované, tedy že nezáleží na tom, které konkrétní $\alpha$ si zvolíme jako reprezentanta zbytkové třídy $[\alpha]$ (a obdobně které $\beta$ pro $[\beta]$). Pokud jste někdy viděli odůvodnění, proč funguje počítání v $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ (celých číslech modulo $n$), pak vězte, že tady se děje naprosto totéž, jen trochu obecněji.

Takto zadefinované sčítání a násobení pořád funguje, jak má, čímž činí z $\mathcal{O}/\gamma\mathcal{O}$ okruh. Pozor, v těchto okruzích může součin dvou nenulových prvků být nulový.

**Tvrzení.** *Pro řád $\mathcal{O} \subset \mathbb{Q}(\sqrt{D})$ má okruh $\mathcal{O}/\gamma\mathcal{O}$ má přesně $|\mathrm{N}(\gamma)|$ prvků.*

*Důkaz.* Pro $\gamma \in \mathbb{Z}$ zřejmé. Obecnější důkaz naznačím na konzultacích. □

**Definice.** Ať je $R$ nějaký okruh. Řekneme, že $u \in R$ je *invertibilní (v $R$)*, pokud existuje nějaké $v \in R$ splňující $uv = 1$.

Neformálně řečeno, invertibilní prvky jsou ty, kterými dovedeme dělit.

**Zamyšlení 28.** V řádu $\mathcal{O} \subset \mathbb{Q}(\sqrt{D})$ je $\alpha$ invertibilní, právě když $\mathrm{N}(\alpha) = \pm 1$.

**Cvičení 29.** (v podstatě Eulerova věta) Ať v $\mathcal{O}/\gamma\mathcal{O}$ existuje přesně $m$ invertibilních zbytkových tříd a ať je $\alpha$ jednou z nich. Potom $\alpha^m \equiv 1 \pmod{\gamma\mathcal{O}}$.

**Úloha 30.** Rozhodněte, zda existuje nekonečně mnoho necelých reálných čísel $\alpha$ s následující vlastností: pro každé kladné celé $n$ je $\lfloor \alpha^n \rfloor - 1$ násobek 2024.

**Úloha 31.** Ať $p(n)$ značí množinu prvočíselných dělitelů celého čísla $n$. Dokažte, že existuje nekonečně mnoho dvojic kladných celých čísel $a$, $b$ takových, že $p(a^2 + 1) = p(b^2 + 1)$.

**Definice.** Množinu $S \subseteq \mathcal{O}/\gamma\mathcal{O}$ nazveme *multiplikativní*, pokud je neprázdná, obsahuje jen invertibilní prvky a je uzavřená na násobení.[3]

**Cvičení 32.** (modulární podmínka) Mějme multiplikativní množinu $S \subset \mathcal{O}/\gamma\mathcal{O}$ a invertibilní $\alpha \in \mathcal{O}/\gamma\mathcal{O}$. Potom existuje kladné celé číslo $k$ takové, že $\alpha^n \in S$, právě když $k \mid n$.

V úlohách tohoto příspěvku se nejčastěji potkáme se situací, kdy $\gamma \in \mathbb{Z}$. Jako $\alpha$ nejčastěji využijeme fundamentální řešení.

**Cvičení 33.** Mějme $a + b\sqrt{D} = (x + y\sqrt{D})^n$, kde $a, b, x, y \in \mathbb{Z}$. Potom:

(i) Vždy platí $y \mid b$.
(ii) Pro liché $n$ je též $x \mid a$.
(iii) Pro sudé $n$ je dokonce $2xy \mid b$.

**Úloha 34.** Pokud jsou $p$, $q$ prvočísla řešící $p^2 - Dq^2 = 1$, pak už je $p + q\sqrt{D}$ dokonce fundamentální řešení.

[3] Pro fajnšmekry je to prostě podgrupa $(\mathcal{O}/\gamma\mathcal{O})^\times$.

**Úloha 35.** Kladná celá čísla $a$, $x$, $y$ splňují $x^2-(a^2+1)y^2=1$. Dokažte, že $x\equiv 1 \pmod{a^2}$. (PraSe 40–2s–2)

**Úloha 36.** Nalezněte všechna $n$, pro něž je $2^n+1$ čtverec.

**Úloha 37.** (těžší) Nalezněte všechna $n$, pro něž je $5^n-4$ čtverec.

**Úloha 38.** (Lucasův-Lehmerův test prvočíselnosti) Ať je $p$ liché prvočíslo a $M_p = 2^p-1$ ať je $p$-té Mersenneovo číslo. Dále definujme posloupnost celých čísel $s_0, s_1, \ldots$ pomocí $s_0=4$ a rekurence $s_{i+1}=s_i^2-2$. Pokud $M_p \mid s_{p-2}$, pak je $M_p$ prvočíslo.

Poznamenejme, že platí i druhá implikace: pokud je $M_p$ prvočíslo, pak $M_p \mid s_{p-2}$. Nicméně ta není pro naše potřeby tolik zajímavá.

### Binomické a rekurenční triky neboli fígle

**Věta.** (rekurence v geometrické posloupnosti) *Uvažujme posloupnosti racionálních čísel $x_i$, $y_i$ definované pomocí $x_i+y_i\sqrt{D}=\alpha^i\beta$ pro nějaká $\alpha,\beta\in\mathbb{Q}(\sqrt{D})$. Potom platí $x_{i+2}=\mathrm{Tr}(\alpha)x_{i+1}-\mathrm{N}(\alpha)x_i$ a $y_{i+2}=\mathrm{Tr}(\alpha)y_{i+1}-\mathrm{N}(\alpha)y_i$.*

**Úloha 39.** Dokažte, že pro každé kladné celé $n$ existují celá $a,b>1$ taková, že $a^2+1=2b^2$ a zároveň $a\equiv b \pmod{n}$.

**Úloha 40.** Definujme posloupnost *Fibonacciho čísel* vztahy $F_0=0$, $F_1=1$ a $F_{n+2}=F_{n+1}+F_n$ pro $n\geq 0$. Dokažte, že pro $x\in\mathbb{N}$ je alespoň jedno z čísel $5x^2\pm 4$ čtverec, právě pokud je $x$ Fibonacciho číslo.

**Úloha 41.** Rozhodněte, zda je $(2^n-1)(3^n-1)$ čtverec pro nějaké kladné celé $n$.

**Věta.** (binomická) *Platí* $(x+y)^n=x^n+nx^{n-1}y+\cdots+\binom{n}{i}x^{n-i}y^i+\cdots+nxy^{n-1}+y^n$.

**Úloha 42.** Rozhodněte, zda existuje nekonečně mnoho trojic kladných celých čísel $(a,b,c)$ takových, že pro každé prvočíslo $p$ je $\lfloor(a+b\sqrt{2024})^p\rfloor - c$ je násobkem $p$. (CAPS 2024)

**Cvičení 43.** (odmocninové LTE) Buď $a+b\sqrt{D}=(x+y\sqrt{D})^n$ a uvažme prvočíslo $p$ takové, že $p\mid y$, ale $p\nmid x$. Potom[4] $v_p(b)=v_p(y)+v_p(n)$.

**Úloha 44.** (těžší) Nalezněte všechna $n$, pro něž je $3^n-2$ čtverec.

**Úloha 45.** (těžší) Nalezněte všechna $n$, pro něž je $7^n+2$ čtverec.

Závěrem si ukážeme aplikaci v důkazu Størmerovi věty – ta neformálně říká, že hezká čísla málokdy následují po sobě.

**Lemma.** *Ať má $\omega=x+y\sqrt{D}$ normu 1. Potom má pro každé $n>1$ iracionální část $\omega^n$ prvočíselného dělitele, který nedělí $y$.*

**Věta.** (Størmer) *Buď dána konečná množina prvočísel $P$. Kladné celé číslo nazvěme* hladkým, *pokud všichni jeho prvočíselní dělitelé leží v $P$. Pak existuje pouze konečně mnoho párů po sobě jdoucích hladkých čísel.*

[4] $v_p(n)$ neboli *$p$-valuace $n$* značí ten největší exponent $e$ splňující $p^e \mid n$.

*Důkaz.* (skeč) Jsou-li $n$, $n+1$ hladká, pak $n(n+1) = Dy^2$ pro $y$ hladké a $D$ bezčtvercové hladké – takových je jen konečně mnoho. Z toho $(2n+1)^2 - 4Dy^2 = 1$. Pro každou možnou sadu prvočíselných dělitelů $y$ (těch je konečně mnoho) jsou řešení, v nichž je $y$ násobkem těchto prvočinitelů, přesně mocniny nějakého konkrétního $\omega$ (cvičení o modulární podmínce). Pak ale $\omega^\ell$ pro $\ell > 1$ má v iracionální složce nějaký zakázaný prvočinitel. □

### Návody

**10.** $\alpha + \overline{\alpha} = \mathrm{Tr}(\alpha) \in \mathbb{Z}[\sqrt{D}]$.

**13.** Jsou to postupně $a + \sqrt{D}$, $2a^2 + 1 + 2a\sqrt{D}$, $a^2 - 1 + a\sqrt{D}$, $a^2 + 1 + a\sqrt{D}$.

**14.** Měl(a) bys narazit na $D = 2$.

**15.** Mělo by se objevit $x^2 - 8y^2 = 1$.

**16.** Řešení $x^2 - D^3y^2 = 1$ pro Tvoje oblíbené $D$.

**17.** Až nebudeš vědět, jak dál, podívej se v $\mathbb{Z}[\sqrt{7}]$ místo $\mathbb{Z}[\sqrt{28}]$ a najdi čtverec.

**18.** (i) Přenásobení řešením Pellovy rovnice zachová normu.
(ii) Lemma B.

**19.** Vezmi fundamentální řešení $x^2 - py^2 = 1$ a rozlož $(x-1)(x+1) = py^2$. Při výběru, do které závorky přijde extra $p$, pomůže minimalita.

**20.** Vezmi vhodnou zápornou Pellovu rovnici $x^2 + 1 = Dy^2$.

**21.** Až to bude vypadat, že výsledek není čtverec, rozšiř na $\frac{\omega^{\ell+1} - 2 + \omega^{-\ell}}{2\omega}$ a věz, že $2\omega$ je čtverec.

**22.** Kdyby se jednalo o celá čísla, ihned bys viděl(a) fundamentální řešení. Ignoruj, že se jedná o polynomy, a nageneruj další „$f + g\sqrt{x^2 - 1}$“, jako by se jednalo o celá čísla.

**23.** Vyrob na základě řešení $x^2 - 3y^2 = 1$.

**24.** Lemma B na $\alpha$ a $\overline{\alpha}$.

**28.** $\pm 1$ jsou jediné invertibilní prvky v $\mathbb{Z}$.

**29.** Jsou-li $\beta_1, \ldots, \beta_m$ všechny invertibilní zbytkové třídy, porovnej $\beta_1 \cdots \beta_m$ s $(\alpha\beta_1) \cdots (\alpha\beta_m)$.

**30.** Zvol $\alpha = x + y\sqrt{D}$, $x \equiv 1$, $y \equiv 0 \pmod{2024}$ tak, aby navíc $x - y\sqrt{D} \in (0, 1)$.

**31.** Zkus třeba řešení $a^2 + 1 = 5(b^2 + 1)$ v nichž $5 \mid b^2 + 1$. Jakmile najdeš jedno se správným $b \pmod 5$, násob řešeními Pellovy rovnice, která jsou $1 \pmod 5$. Mimochodem, všechna vhodná $b$ budou Fibonacciho čísla, to souvisí s úlohou 40.

**33.** Dívej se modulo $x$ či $y$.

**34.** V mocninách fundamentálního řešení vždycky bude jedna ze složek vždy násobkem něčeho menšího. Pozor, co když má fundamentální řešení iracionální složku 1?

**35.** Víš přesně, jak vypadá fundamentální řešení. Dívej se mod $a^2$, rozliš paritu exponentu. Alternativně můžeš rozepsat binomickou větou.

**36.** Dá se pohodlně vyřešit bez Pellovy rovnice, ale je poučné pro liché $n = 2m+1$ rozepsat $\mathrm{N}(x+2^m\sqrt{2}) = 1$ a všimnout si, kdy je iracionální část $(3+2\sqrt{2})^\ell$ násobek 4.

**37.** $n = 2m+1$, pak má $\frac{x+5^m\sqrt{5}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ normu $-1$, let's go.

**38.** (i) Ať $\omega = 2+\sqrt{3}$, potom $s_i = \omega^{2^i} + \omega^{-2^i}$.

(ii) $M_p \mid s_{p-2} \implies \omega^{2^{p-1}} \equiv -1 \pmod{M_p} \implies e = 2^p$ je ten nejmenší exponent splňující $\omega^e \equiv 1 \pmod{M_p}$.

(iii) Ať je $M_p$ složené a $q \mid M_p$ nejmenší prvočinitel. Pak vše v (ii) platí i mod $q$.

(iv) $M_p < 2^p = e < q^2$ (v podstatě Euler), spor.

**39.** Seřaď si řešení $a^2+1 = 2b^2$ do posloupnosti $a_n+b_n\sqrt{2}$ a dívej se na $c_n = a_n-b_n$. Ta začíná v 0, stačí proto vykoukat, že její rekurence se obrátit.

**40.** Podmínka $5x^2 \pm 4 = a^2$ odpovídá $\mathrm{N}\left(\frac{a+x\sqrt{5}}{2}\right) = \pm 1$. Pak si stačí všimnout, že $\alpha = \frac{1+\sqrt{5}}{2}$, $\beta = 1$ vyrobí v rekurenční větě přesně Fibonacciho posloupnost.

**41.** Odvoď $2 \mid n$. Potom má $2^{n/2}$ i $3^{n/2}$ být racionální částí nějakého řešení $x^2 - Dy^2 = 1$ pro to samé $D$. Rozeber, že fundamentální řešení má $6 \mid \mathrm{Tr}(\omega_0)$, takže racionální část jakéhokoliv řešení je sudá, právě když je násobkem tří.

**42.** Zvol $a$, $b$ tak, aby $a - b\sqrt{2024} \in (0,1)$, dolní celá část se pak zjednoduší. Binomický rozvoj bude modulo $p$ taky vypadat docela jednoduše.

**43.** BÚNO ber $n$ prvočíslo. Každý iracionální člen následující po $nx^{n-1}y$ bude mít ostře větší valuaci.

**44.** Využij cvičení o dvojkách, aby se objevila mocnina fundamentálního řešení. Dělitelnost iracionální části třemi dává modulární podmínku. Pak už budou valuace fungovat krásně.

**45.** Stejně jako předchozí úloha.

### Literatura a zdroje

Příspěvek je přepracovanou verzí toho, který jsem připravil na podzimní soustředění 2019 ve Skleném. Níže uvádím také další zdroje, které jsem při přípravě využil:


[1] Matěj Doležálek: *Pellova rovnice a kvadratické okruhy*, Sklené, 2019.

[2] Víťa Kala: *Teorie čísel*, skripta k přednášce na MFF UK, *https://www.karlin.mff.cuni.cz/~kala/files/TC23.pdf*.

[3] Fíla Čermák, Matěj Doležálek: *Teorie (nejen) čísel 2 – Jednotky*, PraSečí seriál, 40. ročník.

[4] Siu Hang Man: *Algebraic Number Theory*, lecture notes k přednášce na MFF UK, *https://sites.google.com/view/shman/algebraic-number-theory-summer-2223*.

[5] Evan Chen: *An Infinitely Large Napkin*, XIV: Algebraic NT I, *https://web.evanchen.cc/napkin.html*.

# Kombinatorické nepočítání

Alica Dományová

Abstrakt. Když chceme ukázat, že dvě množiny jsou stejně velké, je často zbytečně pracné počítat jim prvky. Přitom může stačit sestrojit bijekci či prostě jen „nahlédnout“, že je to v obou případech totéž.

**Definice.** *Kombinační číslo* $\binom{n}{k}$ udává počet možností, jak do $n$ přihrádek umístit $k$ nerozlišitelných kuliček, do každé nejvýše jednu.

### Rozcvička

**Úloha 1.** 🖼 Nahlédněte, že $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$.

**Úloha 2.** 🕮 Nahlédněte, že roznásobením $(a+b)^n$ dostaneme

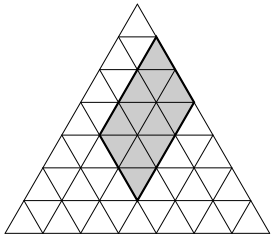
$$\binom{n}{0}a^0b^n + \binom{n}{1}a^1b^{n-1} + \cdots + \binom{n}{n}a^nb^0.$$

**Úloha 3.** 🖼 Nahlédněte

$$1^2 + 2^2 + \cdots + n^2 = 2\binom{n+1}{3} + \binom{n+1}{2}.$$

**Úloha 4.** 🕮 Nahlédněte, že počet možností, jak na šachovnici umístit blíže neurčený počet střelců tak, aby se vzájemně neohrožovali, je druhou mocninou přirozeného čísla.

**Úloha 5.** 🖼 Uvědomte si, že počet všech rovnoběžníků v rovnostranném trojúhelníku o straně délky $n$ s trojúhelníkovou mřížkou je $3\binom{n+2}{4}$.



### Všehochuť

**Úloha 6.** 🕮 Je dáno přirozené číslo $k$ a $n \geq k$. Uvažme náhodnou permutaci na $\{1, 2, \ldots, n\}$. Nahlédněte, že pravděpodobnost, že prvky $1, 2, \ldots, k$ leží v jednom cyklu, nezávisí na volbě $n$.

**Úloha 7.** 🕮 Označme $x_n$ počet slov délky $n$ z písmen $A$, $B$ neobsahujících podslovo $ABABA$ ani $BABAB$ a dále označme $y_n$ počet slov délky $n$ z písmen $A$, $B$ neobsahujících nikde pět stejných po sobě jdoucích písmen. Nahlédněte, že $x_n = y_n$.

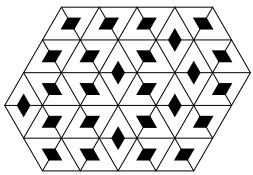
**Úloha 8.** 🖼 Alča si nakreslila čtvercovou mřížku $n \times n$ a do každého políčka napsala počet všech obdélníků (a čtverců) v mřížce, které obsahují dané políčko (na obrázku je situace pro $n = 3$). Uvědomte si, že součet čísel ve všech políčkách je roven $\binom{n+2}{3}^2$. (PraSe 29–3–7, Rakousko 2002)

| | | |
|---|---|---|
| 9 | 12 | 9 |
| 12 | 16 | 12 |
| 9 | 12 | 9 |

**Úloha 9.** 🖼 Letecká společnost provozuje (obousměrné) spoje mezi některými (neuspořádanými) dvojicemi z $n$ měst (povolené je i neprovozovat žádný spoj či všechny). Města přitom mají různé priority. Pokud navíc existuje spoj mezi městy $a$, $b$ a město $c$ má vyšší prioritu než $b$, existuje i spoj mezi $a$, $c$. Uvědomte si, že počet možností, jak spoje provozovat, je $2^{n-1}$.

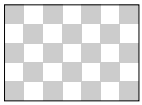
**Úloha 10.** 🖼 Jsou dána přirozená čísla $a$, $b$, $c$. Uvažujte všechny tabulky nezáporných celých čísel $a \times b$, v nichž všechny řádky a sloupce jsou nerostoucí a všechna čísla jsou rovna nejvýše $c$ (levý obrázek). Na druhé straně uvažujte šestiúhelník s vnitřními úhly 120° a stranami délek $a$, $b$, $c$, $a$, $b$, $c$ a sadu kosočtverečků slepených ze dvou jednotkových rovnostranných trojúhelníků (pravý obrázek). Nahlédněte, že počet tabulek je stejný jako počet možností, jak vyskládat šestiúhelník kosočtverečky.

| | | | |
|---|---|---|---|
| 2 | 2 | 1 | 1 |
| 2 | 2 | 0 | 0 |
| 1 | 1 | 0 | 0 |



**Úloha 11.** 🖼 Buďte $a$, $b$ nesoudělná lichá čísla. Na pravítku dlouhém $ab$ vyznačme nejprve každou $a$-tou rysku, pak každou $b$-tou rysku, a nakonec obtáhněme každý druhý úsek mezi vyznačenými ryskami (začneme obtáhnutím prvního). Uvědomte si, že celková délka obtaženého úseku je rovna počtu černých políček na šachovnici $a \times b$, jejíž rohová políčka jsou černá. (PraSe 31–8–6, ruský folklór)





**Úloha 12.** 🕮 Permutacím $\sigma$ na množině $\{1, 2, \ldots, 2n\}$, pro něž existuje $i < 2n$ takové, že $|\sigma(i) - \sigma(i+1)| = n$, říkejme *dobré*. Ostatní nazývejme *špatné*. Uvědomte si, že dobrých permutací je více než špatných. (IMO 1989–6)

**Úloha 13.** 🕮 Jsou dána čísla $n \geq k$ stejné parity. V řadě stojí $2k$ lamp očíslovaných $1, \ldots, 2k$. Na začátku jsou všechny zhasnuté. Jeden krok spočívá v rozsvícení zhasnuté lampy nebo zhasnutí rozsvícené. Označme $X$ počet $n$-prvkových posloupností kroků, po kterých budou svítit právě lampy $1, \ldots, k$, a dále označme $Y$ počet $n$-prvkových posloupností kroků, po kterých budou svítit právě lampy $1, \ldots, k$, přičemž byly přepínány pouze tyto lampy. Rozmyslete si, že

$$\frac{X}{Y} = \frac{2^n}{2^k}.$$

(IMO 2008–5)

**Úloha 14.** 🕮 Je dáno $n \geq 3$ bodů očíslovaných $1, 2, \ldots, n$. Z bodu s menším číslem vede vždy šipka do bodu s větším číslem. Obarvení šipek červenou a modrou nazveme *jednobarevné*, pokud pro libovolnou dvojici různých bodů $A$, $B$ neexistuje zároveň modrá a červená cesta z $A$ do $B$. Uvědomte si, že počet jednobarevných obarvení je $n!$. (ARO 2005)

**Úloha 15.** 🕮 Jako *plné $n$-tice* přirozených čísel budeme označovat ty, ve kterých pro každé $i \geq 2$, jež se v $n$-tici vyskytuje, platí, že se v $n$-tici vyskytuje i $i - 1$, přičemž první výskyt $i - 1$ je před posledním výskytem $i$. Rozmyslete si, že plných $n$-tic je $n!$. (IMO Shortlist 2002)

**Úloha 16.** 🖼 Označme $G(n)$ počet všech možných stromů (souvislých grafů bez kružnic) na daných $n$ vrcholech. Bijektivně ukažte

$$n^n = G(n) \cdot n^2.$$

### Cesty v mřížce

**Úloha 17.** 🕮 Nahlédněte, že počet cest délky $a+b$ z levého dolního rohu do pravého horního v mřížce $a \times b$ je $\binom{a+b}{a}$.

**Úloha 18.** 🖼 Nahlédněte, že

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}.$$

**Úloha 19.** 🖼 Nechť $a$, $b$ jsou přirozená čísla. Uvažme cesty podél mřížky z bodu $[0,0]$ do bodu $[a,b]$, které nikdy nejdou doleva, nachází se v nich právě jeden krok dolů a žádný vrchol není navštívený vícekrát. Uvědomte si, že jejich počet je roven $(a+1)\binom{a+b}{a-1}$. (variace na celostátní kolo MO 2015)

**Úloha 20.** 🖼 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. Uvědomte si, že výsledný součet je roven

$$(n+1)\binom{2n}{n}.$$

(MO 66–A–III–4)

**Úloha 21.** 🖼 Označme

$$f(n) = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n-k}{k} 2^k.$$

Rozmyslete si, že $f(n) + f(n-1) = 2^n$.

**Úloha 22.** 🖼 Bijektivně ukažte

$$\sum_{k=0}^{n} \binom{2k}{k} \binom{2(n-k)}{n-k} = 2^{2n}.$$

### Rozklady

**Definice.** *Rozkladem* čísla $n$ délky $k \geq 1$ rozumíme konečnou nerostoucí posloupnost přirozených čísel $a_1, \ldots, a_k$ splňující $a_1 + \cdots + a_k = n$.

**Úloha 23.** 🕮 Nahlédněte, že počet všech rozkladů čísla $n$ je roven počtu rozkladů čísla $2n$ délky $n$.

**Úloha 24.** 🖼 Nahlédněte, že počet rozkladů čísla $n$ délky $k$ je stejný jako počet všech rozkladů $n$, kde $a_1 = k$.

**Úloha 25.** 🖼 Rozklad nazveme *symetrickým*, pokud pro každé $i$ udává $a_i$ počet prvků rozkladu velkých alespoň $i$. Uvědomte si, že symetrických rozkladů čísla $n$ je stejně jako těch rozkladů čísla $n$, kde jsou jednotlivá $a_i$ různá a současně lichá.

**Úloha 26.** 🖼 Pro $m, n \in \mathbb{N}$ označme $f(m,n)$ počet $n$-tic $(x_1, x_2, \ldots, x_n)$ celých čísel splňujících $|x_1| + \cdots + |x_n| \leq m$. Rozmyslete si, že $f(m,n) = f(n,m)$.

**Úloha 27.** 🖼 Označme si jako $A(n)$ počet posloupností $a_1 \geq a_2 \geq \cdots \geq a_k$ přirozených čísel takových, že $a_1 + \cdots + a_k = n$ takových, že $a_i + 1$ je mocnina dvojky. Dále nechť $B(n)$ je počet posloupností $b_1 \geq b_2 \geq \cdots \geq b_m$ přirozených čísel takových, že $b_1 + \cdots + b_m = n$ a pro každé $j < m$ platí $b_j \geq 2b_{j+1}$. Bijektivně ukažte, že pro každé přirozené $n$ je $A(n) = B(n)$.

**Úloha 28.** 🕮 Bijektivně ukažte, že počet rozkladů čísla $n$, ve kterých jsou všechna $a_i$ různá, je stejný jako počet rozkladů čísla $n$, ve kterých jsou všechna $a_i$ lichá.

**Úloha 29.** 🕮 Bijektivně ukažte, že počet rozkladů čísla $n$, které neobsahují druhou mocninu přirozeného čísla, je stejný jako počet rozkladů čísla $n$, ve kterých se každé číslo $i$ vyskytuje nanejvýš $(i-1)$-krát.

### Fibonacciho čísla

**Definice.** Počet možností, jak vyskládat tabulku $(n-1) \times 1$ kostičkami $1 \times 1$ a $2 \times 1$, nazýváme *$n$-tým Fibonacciho číslem* a značíme $F_n$.

**Úloha 30.** 🕮 Nahlédněte, že počet možností, jak vyskládat tabulku $(n-1) \times 2$ dominovými kostičkami, je roven $F_n$.

**Úloha 31.** 🖼 Nahlédněte

$$F_{a+b+1} = F_{a+1}F_{b+1} + F_a F_b.$$

**Úloha 32.** 🖼 Nahlédněte, že pro každé $n \geq 4$ platí $F_n^2 = 2F_{n-1}^2 + 2F_{n-2}^2 - F_{n-3}^2$.

**Úloha 33.** 🖼 Uvědomte si, že počet možností, jak rozdělit tabulku $(n+1) \times 1$ na dílky větší než $1 \times 1$, je $F_n$.

**Úloha 34.** 🖼 Uvědomte si, že počet možností, jak vyskládat tabulku $n \times 1$ kostičkami s lichými rozměry, je $F_n$.

**Úloha 35.** 🖼 Uvědomte si, že $F_k \mid F_{nk}$.

**Úloha 36.** 🖼 (Cassiniho identita) Rozmyslete si, že $F_{n-1} \cdot F_{n+1} = F_n^2 + (-1)^n$.

## Návody

**2.** Sčítanec $a^i b^{n-i}$ dostaneme tolikrát, kolik je možností, jak v $i$ závorkách vybrat $a$ a ve zbylých $n-i$ vybrat $b$.

**4.** Počet možností, jak je umístit na bílá políčka, krát počet možností, jak je umístit na černá.

**6.** Při procházení cyklu začínajícího bodem 1 přeskakuj čísla vyšší než $k$.

**7.** Invertuj každou druhou pozici.

**12.** Ve špatné permutaci přesuň první prvek ke svému „kamarádovi“.

**13.** Vyjádři pomocí $X$, případně $Y$, počet $n$-prvkových posloupností kroků takových, že na konci bude pro každé $i \leq k$ svítit právě jedna z dvojice lamp $i$, $k+i$.

**14.** Obraťte červené šipky.

**15.** $2,1,2,1,2,1,3,3 \iff 6,3,5,2,4,1,8,7$.

**17.** Právě $a$ ze všech $a+b$ kroků povede vodorovně.

**23.** V rozkladu délky $n$ sniž každý sčítanec o 1.

**28.** $(1+1+1+1)+(1+1)+(1)+(3+3)+(3) = 4+2+1+6+3$.

**29.** Nahrazuj v prvním typu rozkladů vždy $k$ stejných čísel $k$ za číslo $k^2$.

**30.** Stačí první řádek.

## Literatura a zdroje

Děkuji Radečkovi za skvělou přednášku, ze které jsem čerpala. A samozřejmě taky všem autorům přednášek, ze kterých čerpal on :).

[1] Radek Olšák: *Kombinatorické nepočítání*, Meziměstí 2022
[2] Mirek Olšák: *Kombinatorické nepočítání*, sborník *i*KS, 2016.
[3] Mirek Olšák: *Pravděpodobnostní paradoxy*, Uhelná Příbram, 2014.
[4] Josef Minařík: *Nahlížíme identity*, online, 2020.
[5] Anna Mlezivová: *Fibonacciho čísla*, Lipová-Lázně, 2022.

# Švrčkův bod

Alica Dományová

Abstrakt. Přednáška uvádí do problematiky Švrčkova bodu, který je klíčový mimo jiné pro řešení olympiádních geometrických úloh, a ukazuje jeho užitečné vlastnosti. Nuže, pojďme se ponořit do hlubin krásné syntetické geometrie!

**Tvrzení.** (Švrčkův bod) *V trojúhelníku $ABC$ se osa vnitřního úhlu $BAC$, osa strany $BC$ a kružnice opsaná protínají v jednom bodě. Tento bod nazýváme Švrčkův bod příslušející vrcholu $A$ a značíme $\check{S}_A$.*

**Tvrzení.** *Střed kružnice vepsané trojúhelníku $ABC$, střed kružnice připsané straně $BC$, bod $B$ a bod $C$ leží na jedné kružnici se středem v $\check{S}_A$.*

**Tvrzení.** *Nechť se kružnice $k$, $\ell$ vnitřně dotýkají v bodě $T$, tětiva $AB$ kružnice $k$ se dotýká $\ell$ v bodě $U$. Pak $UT$ je osa úhlu $ATB$.*

**Tvrzení.** (Shooting lemma) *Nechť $M$ je střed oblouku $PQ$ na kružnici $\omega$ a přímka $p$ procházející bodem $M$ protíná přímku $PQ$ v $X$ a $\omega$ v $Y$. Pak platí:*

(1) $|MX| \cdot |MY| = |MP|^2$.
(2) *Nechť $I$ je vepsiště $\triangle PYQ$, pak $|MX| \cdot |MY| = |MI|^2$.*
(3) *Nechť $p'$ je další přímka procházející $M$, která protíná přímku $PQ$ v $X'$ a $\omega$ v $Y'$, pak $X$, $Y$, $X'$ a $Y'$ leží na jedné kružnici.*

**Úmluva.** V přednášce budeme používat následující značení (pokud nebude řečeno jinak): $I$ je střed kružnice vepsané (vepsiště), $O$ střed kružnice opsané (opsiště), $J_A$ střed kružnice připsané k $BC$ (připsiště) (obdobně $J_B$, $J_C$). Dále nechť $AD$ je osa úhlu $CAB$, kde $D$ leží na $BC$, obdobně $BE$ a $CF$.

### A jde se řešit

**Úloha 1.** Je dán trojúhelník $ABC$. Označme $O$ střed kružnice opsané trojúhelníku $BCI$. Dokažte, že $|\sphericalangle OKB| = |\sphericalangle OLC|$, kde $K$, $L$ jsou body dotyku kružnice vepsané $ABC$ po řadě se stranami $AB$, $AC$. (China girls 2012/5)

**Úloha 2.** Čtyřúhelník $ABCD$ je vepsán do kružnice $\omega$. Středy sousedních oblouků $AB$, $BC$, $CD$, $DA$ označme postupně $\check{S}_A$, $\check{S}_B$, $\check{S}_C$, $\check{S}_D$. Dokažte, že přímky $\check{S}_A\check{S}_C$ a $\check{S}_B\check{S}_D$ jsou na sebe kolmé.

**Úloha 3.** V trojúhelníku $ABC$ s běžným značením ukažte, že $I$ je ortocentrem trojúhelníka $\check{S}_A\check{S}_B\check{S}_C$.

**Úloha 4.** Dokažte, že body $J_B$, $J_C$, $B$, $C$ leží na jedné kružnici.

**Úloha 5.** Označme $\check{N}_A$ průsečík osy vnějšího úhlu u vrcholu $A$ a osy protější strany. Ukažte, že tento „antišvrk“

(i) leží na kružnici opsané trojúhelníku $ABC$,
(ii) leží ve středu $J_BJ_C$
(iii) a jeho vzdálenost od přímky $BC$ je $\frac{r_B+r_C}{2}$, kde $r_B$ a $r_C$ značí poloměry kružnic připsaných naproti vrcholům $B$ a $C$.

**Úloha 6.** Je dán trojúhelník $ABC$ se středem kružnice vepsané $I$ a vnitřním bodem $P$. Dále platí

$$|\sphericalangle PBA| + |\sphericalangle PCA| = |\sphericalangle PBC| + |\sphericalangle PCB|.$$

Ukažte, že $|AP| \geq |AI|$, přičemž rovnost nastává, právě když $P = I$. (IMO 2006)

**Úloha 7.** Nechť jsou $AL$ a $BK$ osy úhlů nerovnoramenného trojúhelníku $ABC$ ($L$ leží na straně $BC$, $K$ leží na straně $AC$). Osa úsečky $BK$ protne přímku $AL$ v bodě $M$. Bod $N$ leží na přímce $BK$ a platí, že $LN$ je rovnoběžná s $MK$. Dokažte, že $|LN| = |NA|$. (Junior Balkan 2010)

**Úloha 8.** Kružnice $\omega_1$ a $\omega_2$ mají vnější dotyk v bodě $T$ a obě se vnitřně dotýkají kružnice $\omega$ postupně v bodech $R$ a $S$. Buď $Q$ druhý průsečík $RT$ a $\omega$. Ukažte, že $|\sphericalangle QST| = 90°$. (KMS)

**Úloha 9.** Nechť $BC$ je průměr kružnice $k$ se středem $O$. Dále buď $A$ bod na $k$ takový, že $|\sphericalangle AOB| < 120°$, a $D$ buď střed toho oblouku $AB$, který neobsahuje $C$. Rovnoběžka s $DA$ vedená bodem $O$ protne $AC$ v bodě $I$. Osa úsečky $OA$ protne $k$ v bodech $E$ a $F$. Ukažte, že $I$ je středem kružnice vepsané trojúhelníku $CEF$. (IMO 2002)

**Úloha 10.** V konvexním čtyřúhelníku $ABCD$, kde označíme $M$ střed $AC$, platí $|\sphericalangle BMC| = |\sphericalangle CMD| = |\sphericalangle BAD|$. Dokažte, že $ABCD$ je tětivový.

**Úloha 11.** Nechť $ABC$ je ostroúhlý trojúhelník s $|AB| \neq |AC|$. Kružnice nad průměrem $BC$ protne strany $AB$ a $AC$ postupně v bodech $M$ a $N$. Označme $O$ střed strany $BC$ a $R$ průsečík os úhlů $BAC$ a $MON$. Dokažte, že kružnice opsané trojúhelníkům $BMR$ a $CNR$ se protínají na straně $BC$. (IMO 2004)

**Úloha 12.** Trojúhelník $ABC$ splňuje vztah $|AC|+|BC| = 3\cdot|AB|$. Kružnice jemu vepsaná se středem $I$ se dotýká stran $BC$ a $CA$ postupně v bodech $D$ a $E$. Nechť $K$, $L$ jsou obrazy bodů $D$, $E$ ve středové souměrnosti podle $I$. Ukažte, že body $A$, $B$, $K$ a $L$ leží na jedné kružnici. (IMO shortlist 2005)

**Úloha 13.** Je dán trojúhelník $ABC$ se středem $I$ kružnice vepsané a kružnicí opsanou $\Gamma$. Přímka $AI$ protne kružnici $\Gamma$ podruhé v bodě $D$. Buď $E$ bod na oblouku $BDC$ a $F$ bod na úsečce $BC$ takový, že $|\sphericalangle BAF| = |\sphericalangle CAE| < \frac{1}{2}|\sphericalangle BAC|$. Dále buď $G$ střed úsečky $IF$. Dokažte, že přímky $EI$ a $DG$ se protínají na kružnici $\Gamma$. (IMO 2010)

**Úloha 14.** Přímka $\ell$ protíná kružnici $\Gamma$ v bodech $A$, $B$. Kružnice $\Gamma_1$ a $\Gamma_2$ jsou vepsané do stejné úseče určené přímkou $\ell$ a mají vnější dotyk. Dokažte, že jejich vnitřní společná tečna prochází pevným bodem, pohybují-li se $\Gamma_1$, $\Gamma_2$ ve vymezené úseči. (Prasolov)

**Úloha 15.** Je dán rovnoramenný lichoběžník $ABCD$ s delší základnou $AB$. Nechť $I$ je střed kružnice vepsané trojúhelníku $ABC$ a $J$ střed kružnice připsané straně $AD$ trojúhelníku $ACD$. Dokažte, že přímky $IJ$ a $AB$ jsou rovnoběžné.

**Úloha 16.** V trojúhelníku $ABC$ platí $|AB| < |BC|$. Označme $M$ střed $AC$. Dokažte, že $|\sphericalangle IMA| = |\sphericalangle I\check{N}_B B|$.

**Úloha 17.** Kružnice $\omega_1$ a $\omega_2$ se obě zevnitř dotýkají kružnice $\omega$ postupně v bodech $A$ a $B$. Společná tečna $\omega_1$ a $\omega_2$ se jich dotýká postupně v bodech $C$ a $D$. Ukažte, že $ABDC$ je tětivový čtyřúhelník.

**Úloha 18.** Nechť kružnice $\Omega$ a $\omega$ mají vnitřní dotyk v bodě $P$, přičemž $\omega$ leží uvnitř $\Omega$. Buď $AB$ tětiva $\Omega$, která se dotýká $\omega$ v bodě $C$. Průsečík $PC$ s $\Omega$ různý od $P$ si označme $Q$. Nechť tečny z bodu $Q$ ke kružnici $\omega$ protínají kružnici $\Omega$ v bodech $R$ a $S$. Vepsiště trojúhelníků $APB$, $ARB$ a $ASB$ si postupně označíme jako $I$, $X$ a $Y$. Ukažte, že $|\sphericalangle PXI| + |\sphericalangle PYI| = 90°$. (Rumunsko TST 2013)

**Úloha 19.** Je dán trojúhelník $ABC$, jeho kružnice opsaná $\omega$ a bod $D$ na straně $BC$. Buď $\omega_1$ kružnice dotýkající se úsečky $AD$ v bodě $F$, strany $BC$ v bodě $E$ a kružnice $\omega$ v bodě $K$. Dokažte, že střed $I$ kružnice vepsané $\triangle ABC$ leží na přímce $EF$. (Sawayama–Thebault theorem, PraSe 29/myšmaš)

### Návody

**1.** Všimni si, že na poloze bodů $B$ a $C$ příliš nezáleží, úloha je symetrická podle osy úhlu.

**2.** Úhel mezi $\check{S}_A\check{S}_C$ a $\check{S}_B\check{S}_D$ je součet velikostí oblouků nad $\check{S}_A\check{S}_B$ a nad $\check{S}_C\check{S}_D$. Jakou část kružnice tyto oblouky dohromady zabírají?

**3.** Úhel mezi $\check{S}_B\check{S}_C$ a $A\check{S}_A$ je součet velikostí oblouků nad $A\check{S}_C$ a nad $\check{S}_A\check{S}_B$. Jakou část kružnice tyto oblouky dohromady zabírají?

**4.** Využij vlastnosti os vnitřního a vnějšího úhlu.

**5.**

(i) Předefinuj si $\check{N}_A$ na průsečík osy $BC$ a kružnice opsané $ABC$. Dokaž, že leží na ose vnějšího úhlu při vrcholu $A$.

(ii) Všimni si, že kružnice opsaná $\triangle ABC$ je kružnice devíti bodů $\triangle J_A J_B J_C$. Alternativně využij výsledek předchozího příkladu a dokaž, že $\check{N}_A$ je střed kružnice $J_B J_C BC$.
(iii) Stejnolehlost.

**6.** Dokaž, že $P$ leží na kružnici opsané trojúhelníku $BIC$, a využij trojúhelníkovou nerovnost.

**7.** Ukaž, že $M$ je Švrčkův bod nějakého trojúhelníku. A pak to ukaž i pro $N$.

**8.** Dokresli si společnou tečnu $\omega_1$ a $\omega_2$. Pak dokaž, že $Q$ je antišvrk.

**9.** Všimni si, že $A$ je švrk trojúhelníku $CEF$. Potom dokaž, že $I$ leží na kružnici se středem v $A$ a poloměrem $AE$.

**10.** Přidej si do náčrtku střed kružnice opsané trojúhelníku $ABD$.

**11.** Ukaž, že $R$ je Švrčkův bod trojúhelníku $AMN$.

**12.** Tipni si, kde leží střed kružnice, a převeď úlohu na počítání vzdáleností.

**13.** Dokresli $J_A$, aby ses zbavil bodu $G$.

**14.** Využij Shooting lemma a mocnost bodu ke kružnici.

**15.** Dokresli si vepsiště trojúhelníku ABC, přidej Švrčkův bod $\triangle ADC$ a doúhli.

**16.** Dokresli si $J_A$, $J_B$ a podívej se na podobnost trojúhelníků $AIC$ a $J_C I J_A$.

**17.** Využij tvrzení o dotýkajících se kružnicích a dokaž, že střed oblouku určeného společnou tečnou kružnic leží na $BD$ i $AC$. Shooting lemma.

**18.** Uvědom si, že $Q$ je švrk všech tří trojúhelníků, a dokaž, že $X$, $Y$ jsou body dotyku tečen z něj ke kružnici $\omega$. Doúhli.

**19.** Protni osu úhlu u vrcholu $A$ s $EF$ (dokresli i Švrčkův bod) a využij Shooting lemma.

### Literatura a zdroje

Děkuji Ádě a všem autorům před ní za skvělý materiál, ze kterého jsem mohla čerpat.

[1] Adéla Karolína Žáčková: *Švrčkův bod*, Lipová-Lázně, 2022.
[2] Verča Hladíková: *Švrčkův bod*, Branná, 2019.
[3] David Hruška, Radovan Švarc: *Geometrie trojúhelníka*, PraSečí seriál, 36. ročník.

# Výpočetní složitost

Vojta Gaďurek

Abstrakt. Co je to $P = NP$, proč je to zajimávé a co s tím mají do činění Turingovy Stroje.

Jeden z problémů milénia je rozhodnout zda $P = NP$. Zlí jazykové říkají, že je to nějtěžší způsob jak vydělat milion dolarů. Cílem této přednášky je udělat drobný úvod do problematiky. Začněme tím, že si trochu připravíme půdu. Měli bychom začít osvětlením toho, co vlastně to $P$ a $NP$ znamená. $P = NP$ ve zkratce říká, že deterministický turingův stroj je stejně silný, jako nedeterministický turingův stroj.

Ještě než se do toho vrhneme musíme si zavést nějakou terminologii. V textu budeme pracovat s řetězci.

**Definice 1.** *Abeceda* je konečná množina symbolů.

**Definice 2.** *Slovo* nad abecedou $A$ je konečný řetezec symbolů z $A$.

**Definice 3.** *Universum* nad abecedou $A$ je množina všech slov nad $A$.

**Definice 4.** *Jazyk* nad abecedou $A$ je nějaká podmnožina universa nad jazykem $A$.

Jedním z nejčastějších problémů, který budeme řešit je zda nějaké slovo $a$ patří do jazyka $A$. Například můžeme mít jazyk korektních rovnic $J$ nad abecedou $Q := \{=, +, 1, 2\}$, pak $1 + 1 = 2$ je v $J$, ale $1 + 1 + 1 = 2$ v daném jazyce není. Mohli bychom také mít jazyk všech prvočísel $U$, pak 4 není v $U$, ale 7 ano. Mohlo by nás třeba zajímat, zda 139823922993291 je také v $U$.

Nyní by nás mělo napadnout, zda jsme schopni o každém slovu $a$ pro každý jazyk $A$ rozhodnout, zda $a$ je v $A$?

Než se pustíme do odpovědi, podíváme se na to co je to Tůringův stroj.

Turingův stroj (TS) má dvě části hlavu a pásku. Pásku si můžeme představit jako oboustraně nekonečnou řadu políček a káždé políčko může obsahovat jeden symbol z abecedy $A$. Hlava začína na libovolném políčku, které mu určíme a má k dispozi následující možnosti. Přepsat symbol na políčku, ve kterém se nachází, posunout se do leva, posunout se doprava, změnit svůj stav. Hlava provádí vždy nějaku podmnožinu z těchto akcí. Hlava se rozhoduje dle přechodové funkce, která

má jako vstup stav hlavy a symbol na políčku a jako výstup nějakou podmnožinu akcí.

Každý Tůringův stroj má alespoň dva stavy a to přijící a zamitací, stavů je vždy konečně mnoho.

Výpočet probíhá následovně stroji předložíme nějaké slovo $a$ zapsané na pásce. Turingův stroj vyhodnocuje přechodovou funkci, dokud stav hlavy není bud' přímající nebo zamitající. Pokud je přijimající, pak řekeneme, že daný turingův stoj $a$ přijal, je-li zamítací pak jej zamítl.

Všimněte si, že mohou nastat tři možné případy. Tůringův stroj slovo přijme, Tůringův stroj slovo zamítne a Tůringův stroj se nezastaví.

**Definice 5.** *Jazyk přijímaný Turingovým strojem $T$* nad abecedou $A$ je jazyk jehož všechna slova jsou $T$ přijata a žadná jiná ne.

**Definice 6.** *Jazyk rozhodnutelný Turingovým strojem $T$* nad abecedou $A$ je jazyk jehož všechna slova jsou $T$ přijata a všechna ostatní jsou zamítnuta.

**Úloha 7.** Můžeme si, také všimnout, že každému turingovu stroji odpovidá nějaký jazyk, který je jím přijímaný. Exituje ke každému, jazyku nějaký turingův stroj, který ho přijmá?, rozhoduje?

**Úloha 8.** Navrhněte turingův stroj, pro nad abecedou $0, 1$, který přijme všechny slova, které ve dvojkové soustavě jsou dělitelná třemi, odmítne všechny se zbytkem jedna po dělení třemi a ostatní ani nepříjme ani neodmítne.

U výpočtu Turingova stroje nás zajímají dvě metriky. Spotřebovaný čas a spotřebovaný prostor. Čas měříme v počtu vyhodnocení přechodové funkce, prostor jako počet políček mezi nelevějším navštíveným políčkem a nejpravějším navštíveným políčkem. Je dobré si uvědomit, že velikost slova, které dostane TS k vyhodnocení může být neomezeně velká. Tedy obě složitosti určujeme v závislosti na počtu symbolů v daném slově.

**Definice 9.** *TIME(f(n))* je třída jazyků takových, že pro každý jazyk existuje nějaký o něm rozhodující TS a nějaké $c$, že pro libolnou délku $n$ slova je počet kroků TS nejvýšše $c \cdot f(n)$

**Definice 10.** *SPACE(f(n))* je třída všech jazyků takových, že pro každý jazyk existuje nějaký o něm rozhodující TS a nějaké $c$, že pro libolnou délku $n$ slova je délka navštívené pásky TS nejvýšše $c \cdot f(n)$

**Definice 11.** $P := \bigcup_{k=0}^{\infty} TIME(n^k)$

Nyní jsme popsali deterministický turingův stroj. Jeho jednou z velkých výhod je, že ve svém chování velmi podobný počítačům, které máme nyní k dispozici. Dokonce se dá dokázat, že libolný problém rozhodnutelný na počítači je převoditelný na turingův stroj a obráceně pouze s polynomiálním zpožděním. Tedy, že výsledný program poběží nejhůře polynomialně pomaleji nebo s polynomialně větší pamětí.

TS lze zesílit. Jedním z nejjedonuších způsobůa je povolit nedeterminismus. To znamená, že přechodová funkce nemusí odpovědět jednou množinou akcí, ale může odpovedet libovolným počtem těchto množin. Výpočet se pak rozdělí na tolikrát, kolikrát kolik odpovědí od přechdové funkce dostal. Všechny výpočty, pak běží nezávisle na sobě, příjme-li jeden, pak se počítá jako by slovo bylo přijato. Takový stroj pak nazývaváme nedeterministický tůringův stroj a používáváme zkratku NTS.

**Definice 12.** *NTIME(f(n))* je třída jazyků, rozhodnutelných NTS, takových, že pro každý jazyk existuje nějaký o něm rozhodující NTS a nějaké $c$, že pro libolnou délku $n$ slova je počet kroků NTS nejvýšše $c \cdot f(n)$

**Definice 13.** *NSPACE(f(n))* je třída jazyků, rozhodnutelných NTS, takových, že pro každý jazyk existuje nějaký o něm rozhodující NTS a nějaké $c$, že pro libolnou délku $n$ slova je počet kroků NTS nejvýšše $c \cdot f(n)$

**Definice 14.** $NP := \bigcup_{c=0}^{\infty} NTIME(n^c)$.

**Úloha 15.** Ukažte, že $P \subset NP$

**Úloha 16.** Vicepáskové Turingovy stroje mohou mít více pásek a více hlav? Zvýší to sílu výpočtu?

**Úloha 17.** Pokud zákážeme TS zapisovat do již použitého políčka, změní to sílu výpočtu?

**Úloha 18.** Můžeme libolný TS zrychlit o 20 kroků přechodové funkce? Můžeme zrychlit libovolný TS o libovolných $c$ kroků, kde $c$ je nějaká konstanta.

**Úloha 19.** Můžeme libolný TS zrychlit na dvojnásobek? Můžeme zrychlit libovolný TS konstantně krát?

**Úloha 20.** Pokud TS zakážeme se pohybovat do leva, ale umožníme mu reset (tedy speciální akci, kterou se vrátí na začátek), změní se síla výpočtu?

**Úloha 21.** Existuje TS, který o jiném TS a nějakém vstupu do něj rozhodne zda TS zastaví? Navrhněte vhodnou reprezentaci.

**Úloha 22.** Rozmyslete si jaké inkluze, platí pro $NTIME(fn))$, $TIME(fn))$, $NSPACE(fn))$, $SPACE(fn))$ pro $f(n) \in \omega(log(n)$? Proč je v úloze $log(n)$ a ne jiná hodnota?

$f \in \omega(g)$ znamena, že funkce $f$ vzdy preroste $g$, tedy pro všechna $e > 0$, existuje nějaké $n_0$ takové, že pro všechna $n \geq n_0$ platí $f(n) > eg(n)$

**Úloha 23.** Existuje nějaké $f(n)$, takové, že $NTIME(f(n)) = TIME(f(n))$? Pokud existuje, zkuste najít nejrychleji rostoucí $f$.Říkáme, že $f$ roste rychleji než $l$ pokud $f \in \omega(l)$.

### Návody

**7.** Existuje TS takový, že umí simulovat libovolný jiný TS?
Kolik je TS a kolik je jazyků?

## Literatura a zdroje

[1] Barak *Complexity Theory, Modern Aproach*, Cambridge Press, 2014.

# Nelineární soustavy rovnic

Matěj Gajdoš

Abstrakt. V příspěvku se podíváme na několik běžnějších technik, které se dají s výhodou použít při řešení nelineárních soustav rovnic. Vysvětlíme si, co dělá takovou soustavu nelineární, jak se poznají soustavy cyklické a symetrické a jak lze soustavy řešit pomocí známých nerovností nebo substituce.

Soustavy rovnic můžeme poněkud hrubě rozdělit do dvou tříd. Tou první jsou soustavy lineární, které dobře známe ze základní a střední školy, jsou vcelku předvídatelné a vždy je lze efektivně algoritmicky řešit:

**Definice.** Buďte $m, n$ přirozená čísla a $\alpha_{11}, \alpha_{12}, \ldots, \alpha_{1n}, \alpha_{21}, \ldots, \alpha_{mn}, \beta_1, \ldots, \beta_m$ čísla reálná. Pak *lineární soustavou $m$ rovnic o $n$ neznámých* rozumíme sadu rovnic tvaru

$$\begin{aligned}
\alpha_{11}x_1 + \alpha_{12}x_2 + \cdots + \alpha_{1n}x_n &= \beta_1,\\
\alpha_{21}x_1 + \alpha_{22}x_2 + \cdots + \alpha_{2n}x_n &= \beta_2,\\
&\vdots\\
\alpha_{m1}x_1 + \alpha_{m2}x_2 + \cdots + \alpha_{mn}x_n &= \beta_m,
\end{aligned}$$

kde $x_1, \ldots, x_n$ jsou neznámé.

*Nelineární soustavy* jsou pak všechny reálné soustavy nevyhovující předchozí definici. Jedná se tedy o mnohem širší skupinu soustav, o které je mnohem náročnější něco obecného říct (například už jen počet řešení konkrétní nelineární soustavy, natož pak jejich výčet).

Řešení olympiádních soustav tak obvykle spočívá v tricích a chytrých manipulacích. Na některé běžnější metody se teď podíváme. V principu ale lze se soustavou dělat leccos, nejen ekvivalentní úpravy, na které se klade důraz u lineárních soustav. Stačí se držet legálních vod matematiky (tj. nedělit výrazem, který by mohl nabýt nuly, bez ošetření tohoto případu zvlášť, nelogaritmovat nekladná čísla etc.) a u všech nalezených kandidátů na řešení ověřit zkouškou, že po dosazení opravdu vyhovují původní soustavě.

### Na rovnosti nerovnostmi

Překvapivě silným nástrojem k řešení soustav rovnic je chytré použití nerovností. Obvykle se snažíme nějaký výraz odhadnout shora i zdola stejnou hodnotou, čímž ukážeme, že se již této hodnotě musí rovnat, případně zjistíme, že v některém odhadu musí nastat rovnost (a to nám dodá nějakou novou informaci, například že se všechny členy nějakého výrazu rovnají). Nevýhodou je, že se nám nemusí podařit najít ten správný těsný odhad. Na druhou stranu se ale s nerovnostmi dá flexibilněji pracovat a můžeme se opřít o paletu známých nerovností, které nám odhadovaný výraz s trochou štěstí zjednoduší. Za zmínku stojí například nerovnosti mezi průměry (obzvlášť AG), Cauchyho–Schwarzova nerovnost nebo nerovnost Jensenova. Mnohdy pomůže i jednoduchý fakt, že čtverec reálného čísla je vždy nezáporný.

**Věta.** (Nerovnost aritmetického a geometrického průměru) *Nechť $a_1, a_2, \ldots, a_n$ jsou nezáporná reálná čísla. Pak*

$$\sqrt[n]{a_1 a_2 \cdots a_n} \leq \frac{a_1 + a_2 + \cdots + a_n}{n},$$

*přičemž rovnost nastává právě tehdy, když $a_1 = a_2 = \cdots = a_n$.*

**Věta.** (Cauchyova–Schwarzova nerovnost) *Nechť $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n$ jsou reálná čísla. Pak*

$$(x_1 y_1 + x_2 y_2 + \cdots + x_n y_n)^2 \leq \left(x_1^2 + x_2^2 + \cdots + x_n^2\right)\left(y_1^2 + y_2^2 + \cdots + y_n^2\right),$$

*přičemž rovnost nastává právě tehdy, když existuje $\lambda \in \mathbb{R}$ taková, že $x_i = \lambda y_i$ pro všechna $i \in \{1, 2, \ldots, n\}$.*

**Příklad.** Řešte reálnou soustavu

$$\begin{aligned} x + 2y + 3z &= 28, \\ x^2 + y^2 + z^2 &= 56. \end{aligned}$$

*Řešení.* Podle Cauchyovy–Schwarzovy nerovnosti platí

$$14\left(x^2 + y^2 + z^2\right) = (1 + 4 + 9)\left(x^2 + y^2 + z^2\right) \geq (x + 2y + 3z)^2.$$

Přitom levá strana je $14 \cdot 56 = 784$ a pravá $28^2 = 784$, v aplikaci Cauchyovy–Schwarzovy nerovnosti tak musí nastat rovnost. Díky tomu (ze znalosti vlastností této nerovnosti) víme, že musí $x = \lambda$, $y = 2\lambda$ a $z = 3\lambda$ pro nějaké $\lambda \in \mathbb{R}$. Dosazením do první rovnice soustavy zjistíme, že $\lambda = 2$, čímž dostáváme jediného kandidáta na řešení $(2, 4, 6)$. Zkouškou snadno ověříme, že se opravdu jedná o řešení.

### Symetrie v neznámých

Často se setkáme s *cyklickými soustavami*. Ty poznáme tak, že při provedení cyklické záměny všech neznámých ve všech rovnicích je nová soustava totožná s tou starou. Například soustava

$$\begin{aligned} x^2 + \sin(x+2y) &= 2^z, \\ y^2 + \sin(y+2z) &= 2^x, \\ z^2 + \sin(z+2x) &= 2^y \end{aligned}$$

je cyklická, protože při záměně neznámých $x \to y \to z \to x$ vznikne až na pořadí stejná soustava – například nová první rovnice bude totožná se starou druhou rovnicí. Vlastně v případě cyklické soustavy jsme schopni vhodným „procyklením“ neznámých získat všechny rovnice soustavy jen z rovnice jedné. Proto se občas takové soustavy zadávají ve zkráceném tvaru a například předchozí soustava by se psala jako „cyklická soustava $x^2 + \sin(x+2y) = 2^z$ ve třech neznámých“.

Pro libovolné řešení cyklické soustavy $(x_1, \ldots, x_n)$ platí, že i libovolná cyklická záměna $(x_k, x_{k+1}, \ldots, x_n, x_1, x_2, \ldots, x_{k-1})$ soustavu řeší (kde $k \in \{1, 2, \ldots, n\}$). Můžeme se proto při řešení úlohy omezit jen na řešení s nějakou vlastností a po jejich nalezení nagenerovat zbytek cyklickou záměnou. Například můžeme v principu vždy bez újmy na obecnosti uvažovat, že $x_1$ je maximální/minimální/největší v absolutní hodnotě, což je zvlášť užitečné u soustav o dvou či třech neznámých (neboť je tím uspořádání neznámých už plně/skoro jednoznačné), ale i v případě více neznámých se může tento předpoklad ukázat výhodným, viz následující příklad:

**Příklad.** Řešte v kladných reálných číslech cyklickou soustavu $x_1 + \frac{1}{x_2} = 2$ v třinácti neznámých.

*Řešení.* Předpokládejme bez újmy na obecnosti, že je $x_1$ maximální, tj. $x_1 \geq x_i$ pro všechna $i \in \{1, \ldots, 13\}$. Z toho ihned dostáváme

$$2 = x_1 + \frac{1}{x_2} \geq x_2 + \frac{1}{x_2} \geq 2,$$

kde poslední odhad je vcelku známý a můžeme ho rychle nahlédnout například z AG nerovnosti nebo (ekvivalentně) drobnou úpravou nerovnosti $(x_2 - 1)^2 \geq 0$.

Výraz $x_2 + \frac{1}{x_2}$ je tak z obou stran odhadnut dvojkou, a tudíž již musí být dvojce roven, z čehož plyne $x_2 = 1$. Obdobným dosazováním nalezených neznámých do dalších rovnic nakonec zjistíme, že řešením je $(x_1, \ldots, x_{13}) = (1, \ldots, 1)$.

Kromě cyklických soustav lze narazit i na *symetrické soustavy*, které se vyznačují tím, že libovolné propermutování neznámých celkovou soustavu nezmění (zatímco u cyklických soustav se omezujeme jen na určitý typ permutací, tj. každá symetrická soustava je i cyklická). V takovou chvíli lze při řešení dokonce předpokládat celkové uspořádání neznámých, tj. například $x_1 \geq x_2 \geq \cdots \geq x_n$, zbylá řešení se z takto nalezených dovytvoří všemi možnými permutacemi.

### Substituce

Někdy může soustavu zpřehlednit vhodná substituce neznámých. Zvlášť při přechodu ke goniometrickým funkcím lze s výhodou využít velké množství známých vztahů, které splňují. Při substitucích si musíme dát pozor na to, abychom neztratili nějaká potenciální řešení. Například pokud o soustavě v $x, y$ dopředu víme akorát to, že jsou její neznámé reálné, není vhodné substituovat například $x = \sin\alpha$ a $y = \sin\beta$ pro $\alpha, \beta \in \mathbb{R}$, protože v takovémto tvaru se omezujeme pouze na $-1 \leq x, y \leq 1$. Vhodnější substituci si ukážeme v následujícím příkladu:

**Příklad.** Řešte v reálných číslech cyklickou soustavu $2x + x^2y = y$ ve třech neznámých.

*Řešení.* Vyjádříme neznámé ve tvaru $x = \operatorname{tg}\alpha$, $y = \operatorname{tg}\beta$ a $z = \operatorname{tg}\gamma$ pro nějaká $\alpha, \beta, \gamma \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ – na tomto intervalu nabývá tangens všech reálných hodnot, takže se nám touto substitucí nemůže žádné řešení ztratit. Zároveň na tomto intervalu neexistuje dvojice různých bodů, v nichž by tangens nabýval stejné hodnoty, takže nalezením různých trojic $(\alpha, \beta, \gamma)$ nemůžeme dostat duplicitní $(x, y, z)$.

Dosazením dostáváme cyklickou soustavu

$$2\operatorname{tg}\alpha + \operatorname{tg}^2\alpha \operatorname{tg}\beta = \operatorname{tg}\beta$$

a vynásobením obou stran výrazem $\cos^2\alpha\cos\beta$, který je nenulový díky omezení se na $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$, obdržíme

$$2\sin\alpha\cos\alpha\cos\beta + \sin^2\alpha\sin\beta = \cos^2\alpha\sin\beta,$$

což lze upravit na

$$(\cos\alpha\cos\beta + \sin\alpha\sin\beta)\sin\alpha = (\cos\alpha\sin\beta - \sin\alpha\cos\beta)\cos\alpha.$$

Závorky odpovídají součtovým vzorcům pro sinus a cosinus, konkrétně platí

$$\cos(\beta - \alpha)\sin\alpha = \sin(\beta - \alpha)\cos\alpha.$$

Po převedení na jednu stranu znovu aplikujeme součtový vzorec sinu a obdržíme

$$\sin(\alpha - (\beta - \alpha)) = 0.$$

To nastane právě tehdy, když $2\alpha - \beta = k\pi$, $2\beta - \gamma = l\pi$ a $2\gamma - \alpha = m\pi$ pro nějaká $k, l, m \in \mathbb{Z}$. Postupným vyjádřením $\beta = 2\alpha - k\pi$ a dosazením do druhé rovnosti obdržíme $\gamma = 4\alpha - (2k + l)\pi$, ze třetí rovnosti pak $7\alpha = (4k + 2l + m)\pi$. Výraz $4k + 2l + m$ se může rovnat libovolnému celému číslu, takže lze jednodušeji ekvivalentně psát $\alpha = \frac{1}{7}n\pi$ pro nějaké $n \in \mathbb{Z}$. Abychom dodrželi $\alpha \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$, musí $n \in \{-3, -2, \ldots, 2, 3\}$.

K danému $n$ již dopočteme kandidáty na řešení

$$(x, y, z) = \left(\operatorname{tg} \frac{n\pi}{7}, \operatorname{tg} \frac{2n\pi}{7}, \operatorname{tg} \frac{4n\pi}{7}\right)$$

pro $n \in \{-3, -2, \ldots, 2, 3\}$. O řešení se opravdu ve všech případech jedná. To se v tomto případě bude zkouškou ověřovat hůř, ale stačí si uvědomit, že všechny na soustavu použité úpravy byly ekvivalentní (ať už násobení nenulovým výrazem nebo přechod ke kořenům sinu).

### Úlohy

**Úloha 1.** Řešte cyklickou soustavu $x^2 = yz$ ve třech neznámých.

**Úloha 2.** Řešte cyklickou soustavu $a^5 = b + b^5$ v pěti nezáporných neznámých.

**Úloha 3.** Řešte cyklickou soustavu $x(x + 1) = y(z + 1)$ ve třech neznámých.

**Úloha 4.** Řešte v $\mathbb{R}$

$$\begin{aligned} x^2 + y^2 + z^2 &= 361, \\ \frac{1}{x} + \frac{1}{y} + \frac{1}{z} &= 0, \\ x - y + z &= 11. \end{aligned}$$

**Úloha 5.** Řešte v $\mathbb{R}$

$$\begin{aligned} 4x^2 - 3y + 3 &= z, \\ y^2 - 5z + 4 &= x, \\ 9z^2 - 3x - 1 &= y. \end{aligned}$$

**Úloha 6.** Řešte v $\mathbb{R}$

$$\begin{aligned} x^2 - yz &= |y - z| + 1, \\ y^2 - zx &= |z - x| + 1, \\ z^2 - xy &= |x - y| + 1. \end{aligned}$$

(MO 68–A–III–1)

**Úloha 7.** Řešte cyklickou soustavu $a_1^2 + a_1 - 1 = a_2$ v $n$ neznámých.

(PraSe 41–1j–7)

**Úloha 8.** Řešte cyklickou soustavu $a(b^2 + c) = c(c + ab)$ ve třech neznámých.

(MO 64–A–III–4)

**Úloha 9.** Řešte cyklickou soustavu $x^4 + y^2 + 4 = 5yz$ ve třech neznámých.

(MO 61–A–III–6)

**Úloha 10.** Řešte cyklickou soustavu $x_1 - \frac{1}{x_1} = 2x_2$ v pěti neznámých.

### Návody

**1.** Sčítej.

**2.** Zvol maximální neznámou.

**3.** Cauchy–Schwarz.

**4.** Urči $(x+y+z)^2$.

**5.** Čtvercuj.

**6.** Soustava je symetrická a absolutní hodnoty nemáme rádi.

**7.** Hledej průměry.

**8.** Přezávorkuj a rozeber případy.

**9.** Vhodně odhadni.

**10.** Substituuj.

### Literatura a zdroje

[1] Marian Poljak: *Soustavy rovnic*, Zásada, 2021.
[2] Tonda Češík: *Soustavy rovnic*, Horní Lysečiny, 2018.
[3] Vít Musil: *Cyklické soustavy rovnic*, Mentaurov, 2013.
[4] RNDr. Jaroslav Švrček, CSc.: *Metody řešení soustav algebraických rovnic*, *https://kag.upol.cz/ucitprir/texty/MetResSousAR_JS.pdf*.

# Indukce v kombinatorice

Klárka Grinerová

Abstrakt. V této přednášce si spolu ukážeme, jak správně lézt po žebříku a jak nám lezení příčku po příčce může pomoct k vyřešení různorodých úložek. Také si ukážeme, že když budeme opatrní, můžeme brát příčky i po dvou nebo po třech.

Matematická indukce je jedna ze základních důkazových metod, která se obvykle používá, chceme-li dokázat, že nějaké tvrzení či matematická věta platí pro všechny objekty, které jsou spjaté s přirozenými čísly – libovolně velké tabulky a mřížky, $n$-úhelníky, $n$-prvkové množiny či jen že tvrzení platí pro všechna přirozená čísla. Nejprve si uvedeme motivační příklad, který ilustruje princip matematické indukce.

**Příklad.** Naty by se chtěla naučit vylézt ze země po žebříku. Káťa se umí dostat ze země na žebřík, ale po žebříku lézt neumí. Jolča umí na žebříku udělat krok z jedné příčky na druhou. Dokažte, že společnými silami mohou Káťa a Jolča naučit Naty vylézt na žebřík nehledě na to, jak dlouhý žebřík bude.

*Řešení.* Káťa naučí Naty udělat první krok, tedy dostat se ze země na první příčku. Jolča pak naučí Naty udělat krok z příčky na příčku. Naty se pak umí dostat ze země na první příčku a jelikož umí udělat krok z příčky na příčku, umí se dostat z první příčky na druhou, z druhé příčky na třetí, ... , z $n$-té příčky na $(n+1)$-ní. Naty tak umí vylézt ze země po libovolně dlouhém žebříku.

Postup předchozího důkazu formálně shrnuje následující tvrzení

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

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

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

Řešení využívající matematickou indukci zpravidla sestává ze dvou kroků. Nejprve ověříme první podmínku, které se také říká základ nebo báze indukce, takové ověření obvykle snadno provedeme přímo dosazením. Nejčastěji dosazujeme nejmenší přirozené číslo, které má smysl uvažovat. V některých případech se nám může hodit základ indukce rozšířit, tedy ověřit základ pro více než jednu hodnotu, potom můžeme na žebříku brát příčky po dvou (může se například hodit pro práci se sudými

a lichými čísly zvlášť). Potom provedeme tzv. indukční krok, důkaz druhé podmínky. Ten obvykle vedeme tak, že předpokládáme platnost $V(k)$ a odvodíme $V(k+1)$, někdy se nám pro zjednodušení této části může hodit využít odvození $V(k)$ z platnosti $V(k-1)$.

**Příklad.** Ukaž, že pro všechna přirozená čísla $n$ platí

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

*Řešení.* Snadno vypočteme, že pro 1 rovnost platí. Předpokládejme, že rovnost platí pro nějaké přirozené číslo $k$. Tedy

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}.$$

Potom pro $k+1$ máme

$$1 + 2 + \cdots + k + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}.$$

Což je přesně daná rovnost pro $k+1$. Ukázali jsme, že pokud rovnost platí pro $k$, platí i pro $k+1$. Dohromady s ověřením, že vztah platí pro 1, dostáváme, že je platný i pro každé následující číslo, a tedy postupně pro všechna přirozená čísla.

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

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

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

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

*Řešení.* Důkaz provedeme principem silné indukce. Základní krok pro $n = 2$ je jednoduchý, $2 = 2^1$ je hledaný prvočíselný rozklad. Následuje indukční krok. Předpokládáme, že prvočíselný rozklad existuje pro všechna přirozená čísla $k$, pro která platí $2 \leq k < n+1$. Nastane jeden ze dvou případů:

(i) Číslo $n+1$ je prvočíslo $p$, potom $n+1 = p^1$ je hledaný prvočíselný rozklad.
(ii) Číslo $n+1$ je složené číslo. Pak existují dvě přirozená čísla $a$ a $b$ taková, že platí $n+1 = a \cdot b$ a $1 < a < n+1$ a $1 < b < n+1$. Podle indukčního předpokladu existuje prvočíselný rozklad $a$ a prvočíselný rozklad $b$. Poté stačí vynásobit tyto dva rozklady a získáme rozklad čísla $n+1 = a \cdot b$.

Tím jsme dokázali, že každé číslo má prvočíselný rozklad.

### Úlohy

**Úloha 1.** Ukaž, že pro každé $n \geq 1$ je stejná pravděpodobnost, že při současném hodu $n$ kostkami bude výsledný součet sudý, jako, že bude lichý.

**Úloha 2.** Matěj napsal na tabuli písmeno $M$ v každém kroku jedno písmeno $M$ smazal a nahradil jej sekvencí $(M + M)$. Dokaž, že počet písmen $M$ na tabuli byl po každém kroku větší nebo rovný čtvrtině celkového počtu znaků na tabuli. Pravá závorka, levá závorka a znaménko plus jsou znaky. (BRKOS XIX–4–1)

**Úloha 3.** Na šachovnici $2^n \times 2^n$ jedno náhodně vybrané políčko chybí. Ukaž, že zbylou plochu lze vydláždit dlaždicemi, která mají tvar „L“ a zabírají tři políčka.

**Úloha 4.** Petr do roviny nakreslil $n$ přímek, z nichž žádné dvě nejsou rovnoběžné a žádné tři se neprotínají v jednom bodě. Na kolik oblastí přímky dělí rovinu?

**Úloha 5.** Alicka nakreslila do roviny $n$ kružnic, které dělí rovinu na několik oblastí. Ukaž, že Alicka může každou z těchto oblastí vybarvit jednou ze dvou barev tak, že žádné dvě oblasti se stejnou barvou spolu nesousedí.

**Úloha 6.** Ukaž, že pro každé přirozené číslo $n$ platí $6 \mid 2n^3 + 3n^2 + n$.

**Úloha 7.** Mějme reálné číslo $x$ takové, že $x + \frac{1}{x}$ je celé číslo. Dokaž, že pak je i $x^n + \dfrac{1}{x^n}$ celé číslo pro libovolné $n \in \mathbb{N}$. (MKS 26–4–3)

**Úloha 8.** Ukaž, že pro každou neprázdnou konečnou množinu platí, že počet jejích podmnožin sudé velikosti (o sudém počtu prvků) je roven počtu jejích podmnožin liché velikosti.

**Úloha 9.** Urči počet úhlopříček v $n$-úhelníku.

**Úloha 10.** Ukaž, že je možné uspořádat čísla $1, 2, \ldots, n$ tak, aby pro žádná dvě z nich nebyl jejich aritmetický průměr roven některému z čísel, která jsou v uspořádání mezi nimi.

**Úloha 11.** Ukaž, že pro všechna přirozená čísla $n$ platí nerovnost

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

**Úloha 12.** Dokaž, že pro každé $n \in \mathbb{N}$ existuje $n$-ciferné přirozené číslo dělitelné číslem $2^n$, které má za cifry pouze jedničky a dvojky. (MKS 26–4–6)

**Úloha 13.** Je dáno $n \geq 4$ bodů v rovině takových, že každé čtyři z nich jsou vrcholy konvexního čtyřúhelníka. Dokažte, že jsou to vrcholy konvexního $n$-úhelníka.

**Úloha 14.** Dokažte, že pro každé přirozené číslo $n$ platí: Přičteme-li k číslu, jež má $4n - 3$ číslic, číslo, které z něho vznikne obrácením pořadí číslic, bude mít výsledný součet alespoň jednu číslici sudou.

**Úloha 15.** V PraSestánu jsou alespoň tři křižovatky. Pro libovolné tři různé křižovatky $A$, $B$, $C$ platí, že z $A$ do $B$ se lze dostat jinudy než přes $C$. Dokažte, že pro libovolné dvě různé křižovatky $X$, $Y$ platí, že z $X$ do $Y$ se lze dostat dvěma cestami, které nemají kromě $X$, $Y$ žádnou společnou křižovatku.

**Úloha 16.** Áďa si koupila novou knížku o matematice. Na knihy platila akce, Áďa mohla přilákat do obchodu dva nové zákazníky $B$ a $C$, kteří si tam ještě nic nekoupili. Pokud každý ze zákazníků $B$ a $C$ tímto způsobem přesvědčí (přímo či nepřímo) alespoň dalších $n$ nových zákazníků (pro nějaké dané přirozené $n$), dostane Áďa zdarma záložku. Ukažte, že pokud si $z$ zákazníků koupí knihu, nejvýše $\frac{z}{n+2}$ z nich může dostat záložku. (BRKOS XIX–4–4)

### Návody

**1.** Rozmysli si případ s jednou kostkou a podívej se, co se stane když k hodu $n$ kostkami přidáš další.

**2.** Zkoumej, jak se změní počet znaků na tabuli pokud udělá Matěj $(k+1)$-ní krok.

**3.** Rozděl šachovnici na čtvrtiny a umísti jedno L.

**4.** Rozmysli si, kolik oblastí vznikne přidáním jedné přímky.

**5.** Rozmysli si, co se stane po přidání jedné další kružnice do roviny, která už nějaké kružnice obsahuje a je korektně obarvena.

**6.** Uvaž výraz kde za $n$ dosadíš $k+1$ a upravuj.

**7.** $\left(x+\frac{1}{x}\right)\cdot\left(x^n+\frac{1}{x^n}\right)$

**8.** Odeber jeden prvek a rozděl množiny podle toho, zda daný prvek obsahovaly a nebo ne.

**9.** Uvědom si, kolik úhlopříček vede z jednoho vrcholu.

**10.** Rozděl na sudá a lichá čísla.

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

**12.** Jaký zbytek dává $10^{n-1}$ resp. $2\cdot 10^{n-1} \mod 2^n$?

**13.** Uvaž $k+1$ bodů a jeden bod označ, protáhni strany konvexního $k$-úhelníku tvořeného zbylými body.

**14.** Předpokládej spor pro $k+1$ a odvoď, že pak nemohlo tvrzení platit pro $k$.

**15.** Uvažuj dvojice křižovatek takové, že na cestě mezi nimi leží právě $k$ křižovatek pro rostoucí $k$.

**16.** Postupuj indukcí podle počtu záložek co zákazníci dostali.

### Literatura a zdroje

[1] Verča Hladíková: *Indukce*, Paseky, 2018.
[2] *Sbírka řešených úloh*, *http://matematika.reseneulohy.cz/*.
[3] Káťa Panešová: *Matematická indukce I – Padající domina*, PraSečí seriál, 41. ročník.

# Jensenova nerovnost

Vít Hanika

Abstrakt. Jensenova nerovnost je překvapivě silná a může pomoct, když klasické AG nerovnosti nebo CS nerovnosti selžou. Obecně si rozumí i se složitějšími funkcemi a díky tomu ji budete pravidelně potkávat i na vysoké škole.

### Konvexní kombinace

**Definice.** Nechť $x_1, \ldots, x_n \in \mathbb{R}$, $\lambda_1, \ldots, \lambda_n \in \langle 0, 1\rangle$ a $\lambda_1 + \lambda_2 + \cdots + \lambda_n = 1$. Pak číslo $\lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_n x_n$ nazveme *konvexní kombinací* bodů $x_1 \ldots x_n$ s koeficienty $\lambda_1 \ldots \lambda_n$.

Naprosto obdobně fungují i konvexní kombinace bodů ve vyšších dimenzích. Pro porozumění Jensenově nerovnosti se nám bude hodit umět vážit body v rovině.

**Definice.** Nechť $[x_1, y_1], \ldots, [x_n, y_n]$ jsou souřadnice $n$ bodů v rovině, $\lambda_1, \ldots, \lambda_n \in \langle 0, 1\rangle$ a $\lambda_1 + \cdots + \lambda_n = 1$. Pak bod o souřadnicích

$$[\lambda_1 x_1 + \cdots + \lambda_n x_n,\ \lambda_1 y_1 + \cdots + \lambda_n y_n]$$

nazýváme *konvexní kombinací* bodů $[x_1, y_1], \ldots, [x_n, y_n]$.

**Poznámka.** Když konvexně kombinujeme nějaké body, občas říkáme, že je *vážíme*, přičemž o $\lambda_1, \ldots, \lambda_n$ mluvíme jako o vahách, které daným bodům dáváme. Tato představa vede na následující cvičení:

**Cvičení.** Rozmysli si, že množina konvexních kombinací dvou bodů v rovině je úsečka mezi nimi. Jak vypadají množiny konvexních kombinací více bodů než dvou?

### Konvexní a konkávní funkce

**Definice.** Nechť $I \subseteq \mathbb{R}$ je interval a $f\colon I \to \mathbb{R}$ je funkce. Pokud pro každou dvojici $x, y \in I$ a každé $\lambda \in \langle 0, 1\rangle$ platí

$$f(\lambda x + (1-\lambda)y) \leq \lambda f(x) + (1-\lambda) f(y),$$

řekneme, že $f$ je *konvexní* na $I$.

Duálně (s opačnou nerovností) definujeme *konkávní* funkci. Pokud pro $\lambda \in (0,1)$ platí ostrá varianta uvedené nerovnosti, mluvíme o *ryze konvexní* (resp. *ryze konkávní*) funkci.

### Jensenova nerovnost

**Věta.** (Jensen) *Nechť $f$ je konvexní funkce na intervalu $I$. Potom pro libovolná $x_1, \dots, x_n \in I$ a $\lambda_1, \dots, \lambda_n \in \langle 0, 1\rangle$ taková, že $\lambda_1 + \cdots + \lambda_n = 1$, platí*

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

*Pro konkávní funkci platí obrácená nerovnost.*

Často nám bude stačit jednodušší tvar nerovnosti, kdy jsou všechna $\lambda_i = \frac{1}{n}$:

$$\frac{f(x_1) + \cdots + f(x_n)}{n} \geq f\left(\frac{x_1 + \cdots + x_n}{n}\right).$$

**Cvičení.** Interpretujte obě strany nerovnosti geometricky pomocí konvexních kombinací bodů a uvědomte si, že tvrzení se tím stává téměř triviálním.

**Cvičení.** Rozmyslete si, kdy v Jensenově nerovnosti nastává rovnost.

Nyní si můžeme blahopřát, neboť jsme téměř zadarmo získali velmi obecně vyhlížející nerovnost, která se ukáže být silnou zbraní. Ke správnému použití Jensenovy nerovnosti je třeba umět rozhodnout, zda je daná funkce konvexní (resp. konkávní). K tomu se v praxi používá následující lemma.

**Lemma.** *Má-li funkce $f$ na intervalu $I$ nezápornou (resp. nekladnou) druhou derivaci, je $f$ na $I$ konvexní (resp. konkávní).*

Pokud jste o derivaci (natož o druhé derivaci) neslyšeli, nezoufejte. U jednoduchých funkcí se dá konvexnost (resp. konkávnost) dobře odhadnout z grafu, případně lze použít vhodný matematický software. Přísně korektní zdůvodnění se v tomto případě nevyžaduje ani v MO, a o jednoduchých funkcích se považuje za známé, zda jsou konvexní či konkávní. Konvexní jsou například $\frac{1}{x}$, $\frac{1}{\sqrt{x}}$ na $\mathbb{R}^+$ nebo sudé mocniny $x$ na $\mathbb{R}$. Typické konkávní funkce jsou $\sqrt{x}$ nebo $\log(x)$ na $\mathbb{R}^+$.

### Logaritmus

Občas se při používání Jensenovy nerovnosti setkáme s logaritmem. Bude pro nás užitečný, protože svým způsobem převádí násobení na sčítání a mocnění na násobení. Přesněji o tom hovoří následující poznámka.

**Poznámka.** Nechť $a > 1$. Funkce $f(x) = \log_a(x)$ definovaná na $\mathbb{R}^+$ jako inverzní funkce ke $g(x) = a^x$ má následující vlastnosti:

(i) $f$ je rostoucí ryze konkávní funkce na $\mathbb{R}^+$,
(ii) $f(xy) = f(x) + f(y)$,
(iii) $f\left(\frac{1}{x}\right) = -f(x)$,
(iv) $f(x^y) = yf(x)$.

### Motivační příklady

Konečně se dostáváme k úlohám. Začneme zlehka:

**Příklad.** Ukažte, že pro každé reálné $x > 1$ platí

$$\frac{1}{x-1} + \frac{1}{x} + \frac{1}{x+1} \geq \frac{3}{x}.$$

*Řešení.* Použijeme Jensenovu nerovnost pro funkci $f(x) = \frac{1}{x}$, která je konvexní na $\mathbb{R}^+$, a konvexní kombinaci kladných čísel $x-1$, $x$, $x+1$ s koeficienty

$$\lambda_1 = \lambda_2 = \lambda_3 = \frac{1}{3}.$$

Dostáváme

$$\frac{1}{3}\left(\frac{1}{x-1} + \frac{1}{x} + \frac{1}{x+1}\right) \geq \frac{1}{\frac{x-1}{3} + \frac{x}{3} + \frac{x+1}{3}} = \frac{1}{x} \implies \frac{1}{x-1} + \frac{1}{x} + \frac{1}{x+1} \geq \frac{3}{x}.$$

Jistě by vám nedělalo problém tuto nerovnost dokázat zcela přímočaře roznásobením. Zkusíme tedy něco těžšího – zástupce typické skupiny úloh řešitelných Jensenovou nerovností:

**Příklad.** Jsou-li $\alpha$, $\beta$, $\gamma$ velikosti úhlů v trojúhelníku, dokažte

$$\sin\alpha + \sin\beta + \sin\gamma \leq \frac{3\sqrt{3}}{2}.$$

*Řešení.* Jensenovu nerovnost aplikujeme na funkci $f(x) = \sin x$, která je konkávní na intervalu $(0, \pi)$. Platí $\alpha, \beta, \gamma \in (0, \pi)$, tedy

$$\frac{1}{3}\sin\alpha + \frac{1}{3}\sin\beta + \frac{1}{3}\sin\gamma \leq \sin\left(\frac{\alpha+\beta+\gamma}{3}\right) = \frac{\sqrt{3}}{2}.$$

U této nerovnosti bychom již přímočařejší přístup hledali těžko. Jensenova nerovnost je pro dokazování nerovností s úhly v trojúhelníku často užitečná, neboť známe jejich součet (což je jejich nejjednodušší lineární kombinace).

Pořád je tmoc snadné? Jensenova nerovnost jde použít i na dokazování nerovností mezi průměry:

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

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

**Tvrzení.** (AH nerovnost) *Pro nezáporná čísla $x_1, x_2, \ldots, x_n$ platí*

$$\frac{x_1 + \cdots + x_n}{n} \geq \frac{n}{\frac{1}{x_1} + \cdots + \frac{1}{x_n}}.$$

### Na rozjezd

**Úloha 1.** Ukažte, že pro libovolná reálná čísla $a, b \in \langle -1, 1\rangle$ platí

$$\sqrt{1-a^2} + \sqrt{1-b^2} \leq \sqrt{4-(a+b)^2}.$$

**Úloha 2.** Dokažte, že pro kladná reálná čísla $a$, $b$ splňující $a + b = 1$ platí

$$\left(a + \frac{1}{a}\right)^2 + \left(b + \frac{1}{b}\right)^2 \geq \frac{25}{2}.$$

**Úloha 3.** Dokažte, že pro všechna přípustná $x \in \mathbb{R}$ platí

$$\sqrt{x+1} + \sqrt{2x-3} + \sqrt{50-3x} \leq 12.$$

**Úloha 4.** Pro velikosti úhlů v trojúhelníků $\alpha$, $\beta$, $\gamma$ dokažte nerovnosti

(i) $\sin\frac{\alpha}{2} + \sin\frac{\beta}{2} + \sin\frac{\gamma}{2} \leq \frac{3}{2}$,

(ii) $\cos\frac{\alpha}{2} + \cos\frac{\beta}{2} + \cos\frac{\gamma}{2} \leq \frac{3\sqrt{3}}{2}$,

(iii) $\operatorname{tg}\frac{\alpha}{2} + \operatorname{tg}\frac{\beta}{2} + \operatorname{tg}\frac{\gamma}{2} \geq \sqrt{3}$,

(iv) $\sin\alpha \sin\beta \sin\gamma \leq \frac{3\sqrt{3}}{8}$.

**Úloha 5.** Pro kladná $a$, $b$, $c$ dokažte

$$\sqrt[4]{27\,(a^7 + b^7 + c^7)} \geq \sqrt[4]{a^7} + \sqrt[4]{b^7} + \sqrt[4]{c^7}.$$

**Úloha 6.** Kladná reálná čísla $x$, $y$ splňují $x + y = 1$. Dokažte, že platí

$$\frac{x}{1+y} + \frac{y}{1+x} \geq \frac{1}{1+2xy}.$$

**Úloha 7.** Dokažte, že pro kladná reálná $a$, $b$, $c$, $d$ splňující $a + b + c + d = 4$ platí

$$\sum_{\text{cyc}} \frac{a}{b(b+1)} \geq \frac{8}{(a+c)(b+d)}.$$

### Pořádné úlohy

**Úloha 8.** Ukažte, že pro kladná reálná $x$, $y$, $z$ splňující $x+y+z=xyz$ platí

$$\frac{1}{1+xy}+\frac{1}{1+yz}+\frac{1}{1+zx}\le\frac{3}{4}.$$

**Úloha 9.** Pro kladná $a$, $b$, $c$ dokažte

$$\frac{a}{(b+c)^2}+\frac{b}{(c+a)^2}+\frac{c}{(a+b)^2}\ge\frac{9}{4(a+b+c)}.$$

**Úloha 10.** Pro $a,b\ge 0$ dokažte

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

(MO 63–III–6)

**Úloha 11.** Pro kladná reálná $x$, $y$ dokažte

$$\frac{1}{(1+\sqrt{x})^2}+\frac{1}{(1+\sqrt{y})^2}\ge\frac{2}{x+y+2}.$$

(Indonésie 2008 P2)

**Úloha 12.** Pro kladná reálná $a$, $b$, $c$ dokažte, že $a^a b^b c^c\ge(abc)^{\frac{a+b+c}{3}}$.

**Úloha 13.** Pro reálná $x_1,\dots,x_n\ge 1$ dokažte

$$\frac{1}{x_1+1}+\cdots+\frac{1}{x_n+1}\ge\frac{n}{\sqrt[n]{x_1\cdots x_n}+1}.$$

(IMO Shortlist 1998)

**Úloha 14.** Dokažte, že platí

$$\frac{x\sqrt{x}}{y+z}+\frac{y\sqrt{y}}{z+x}+\frac{z\sqrt{z}}{x+y}\ge\frac{\sqrt{3}}{2}.$$

**Úloha 15.** Pro kladná $a$, $b$, $c$ dokažte

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

(IMO 2001)

### Karamatova nerovnost

Podobně jako můžeme vážit AG nerovnosti a když nás to přestane bavit, objevíme Muirheadovu nerovnost, tak i v případě Jensenovy nerovnosti existuje zobecnění, které se zbaví omezení, že na pravé straně odhadu je jen funkční hodnota váženého průměru čísel. Abychom tuto obecnou verzi nerovnosti mohli snadno popsat, zavedeme pojem majorizace.

**Definice.** Řekneme, že konečná posloupnost $a = (a_1, a_2, \ldots, a_n)$ *majorizuje* $b = (b_1, b_2, \ldots, b_n)$ (budeme značit $a \succ b$), když mají následující vlastnosti:

(1) $a_1 \geq a_2 \geq \cdots \geq a_n$, $b_1 \geq b_2 \geq \cdots \geq b_n$,
(2) $a_1 + a_2 + \cdots + a_i \geq b_1 + b_2 + \cdots + b_i$ pro všechna $1 \geq i \geq n$,
(3) $a_1 + a_2 + \cdots + a_n = b_1 + b_2 + \cdots + b_n$.

**Věta.** (Karamata) *Nechť $f$ je konvexní funkce na intervalu $I$. Potom pro libovolná $x_1, \ldots, x_n, y_1, \ldots, y_n \in I$ splňující $x \succ y$ platí*

$$f(x_1) + \cdots + f(x_n) \geq f(y_1) + \cdots + f(y_n).$$

*Pro konkávní funkci platí obrácená nerovnost.*

**Úloha 16.** Dokažte, že platí

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} \geq 2\left(\frac{1}{a+b} + \frac{1}{b+c} + \frac{1}{c+a}\right) \geq \frac{9}{a+b+c}.$$

**Úloha 17.** Pro strany trojúhelníku $a$, $b$, $c$ dokažte

$$\sqrt{a+b-c} + \sqrt{b+c-a} + \sqrt{c+a-b} \leq \sqrt{a} + \sqrt{b} + \sqrt{c}.$$

(APMO 1996)

**Úloha 18.** Nechť $a_1 \geq a_2 \geq \cdots \geq a_n$ a $b_1 \geq b_2 \geq \cdots \geq b_n$ jsou dvě posloupnosti kladných reálných čísel splňující podmínky

$$a_1 \geq b_1, \quad a_1a_2 \geq b_1b_2, \quad a_1a_2a_3 \geq b_1b_2b_3, \quad \ldots, \quad a_1a_2\cdots a_n \geq b_1b_2\cdots b_n.$$

Dokažte, že platí

$$a_1 + a_2 + \cdots + a_n \geq b_1 + b_2 + \cdots + b_n.$$

**Úloha 19.** Pokud $x_1, \ldots, x_n \in \left\langle -\frac{\pi}{6}, \frac{\pi}{6} \right\rangle$, dokažte

$$\cos(2x_1 - x_2) + \cos(2x_2 - x_3) + \cdots + \cos(2x_n - x_1) \leq \cos x_1 + \cdots + \cos x_n.$$

**Úloha 20.** Nechť jsou $a_1, \ldots, a_n$ kladná reálná čísla. Dokažte, že platí

$$(1 + a_1)(1 + a_2)\cdots(1 + a_n) \leq \left(1 + \frac{a_1^2}{a_2}\right) \cdot \left(1 + \frac{a_2^2}{a_3}\right) \cdots \left(1 + \frac{a_n^2}{a_1}\right).$$

### Návody

**1.** Funkce $f(x) = \sqrt{1-x^2}$ je konkávní.

**2.** Funkce $f(x) = (x + \frac{1}{x})^2$ je konvexní.

**3.** Odmocnina je konkávní funkce.

**4.** Sinus je konkávní, cosinus taky a tangens konvexní. Pozor na jakém intervalu funkci chceme, aby předchozí věta platila!

**5.** Funkce $f(x) = \sqrt[4]{x}$ je konkávní.

**6.** Funkce $f(x) = \frac{1}{1+x}$ je konvexní.

**7.** Funkce $f(x) = \frac{1}{x^2+x}$ je konvexní.

**8.** Rozšiř zlomek třetí proměnnou a uvědomte si, že funkce $f(x) = \frac{x}{x+S}$, kde $S = x + y + z$ je konkávní.

**9.** Zafixuj si $S = a + b + c$ a uvědom si, že $b + c = S - a$. Alternativně použij homogenitu.

**10.** Využij, že funkce $f(x) = \frac{1}{x}$ je konvexní.

**11.** Funkce $f(x) = \frac{1}{(1+\sqrt{x})^2}$ je konvexní.

**12.** Funkce $f(x) = x \log x$ je konvexní.

**13.** Zkus podobný trik jako při důkazu AG nerovnosti, tj. že platí $x = e^{\ln x}$.

**14.** Funkce $f(x) = \frac{x^{3/2}}{S-x}$ je na intervalu $(0, S)$ konvexní, kde $S = x + y + z$ .

**15.** Můžeš použít homogenizaci, případně celé podělit. Uvědom si, že $f(x) = \frac{1}{x}$ je konvexní, nebo že $f(x) = \frac{1}{\sqrt{1+8x}}$ je konvexní.

**16.** Funkce $f(x) = \frac{1}{x}$ je konvexní.

**17.** Správně si je seřaď a nahlédni, že jde o majorizaci.

**18.** Stejně jako logaritmus pomáhá měnit součet v součin, tak exponenciální funkce pomáhá měnit součin v součet.

**19.** Správně seřaď (opět).

**20.** Logaritmus se hodí pro převod na součet. Pokud si nechceš rozmýšlet chování $a$-ček, tak si řekni, že to jsou exponenciály.

### Poděkování a zdroje

Děkuji Martinu Töpferovi a Fílovi Čermákovi, jejichž příspěvky na stejné téma postupně z Hojsovy stráže (2016) a Zásady (2021) jsem s malými změnami převzal. Nové úlohy pocházejí z webu AoPS: *https://artofproblemsolving.com/community*.

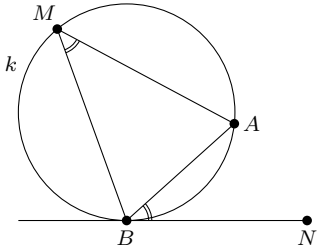
# Dotyčnice

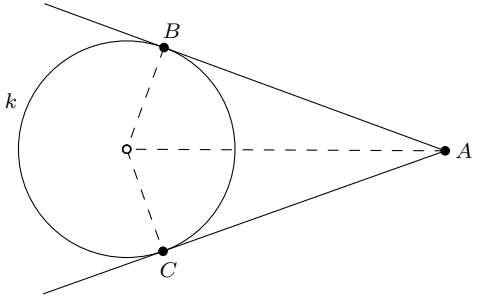
Michal Pecho

Abstrakt. S dotyčnicami sa stretávame napríklad v olympiádnej geometrii pomerne často. V prednáške sa pozrieme na niektoré ich základné vlastnosti a ukážeme si, ako sa vďaka nim naučiť riešiť aj zložitejšie príklady.

**Veta.** (O úsekovom uhle) *Majme na kružnici $k$ tetivu $AB$ a bod $M$ rôzny od $A$, $B$. Veďme priamku $t$, ktorá sa dotýka kružnice v bode $B$. Zvolíme bod $N$ ležiaci na $t$ tak, že body $M$ a $N$ ležia v rôznych polorovinách vzhľadom na $AB$. Uhol $ABN$ nazveme úsekovým uhlom k tetive $AB$. Úsekový uhol má rovnakú veľkosť ako obvodový uhol $AMB$.*

**Tvrdenie.** *Majme kružnicu $k$ a bod $A$ ležiaci mimo kružnice. Veďme bodom $A$ dotyčnice ku $k$, body dotyku s kružnicou označme $B$, $C$. Potom $|AB| = |AC|$.*




**Tvrdenie.** *Priamky $p$ a $q$ sú spoločnými vonkajšími dotyčnicami kružníc $k_1$ a $k_2$. Priamka $p$ sa kružnice $k_1$ dotýka v bode $A$ a kružnice $k_2$ v bode $B$, priamka $q$ sa kružníc dotýká v bodoch $C$ a $D$. Potom platí, že*

(i) $|AB| = |CD|$,
(ii) *ak sa kružnice nepretínajú a ich vnútorná dotyčnica $r$ pretína priamky $p$ a $q$ v bodoch $X$ a $Y$, potom $|AB| = |CD| = |XY|$.*

**Tvrdenie.** *Kružnica vpísaná trojuholníku $ABC$ sa dotýka strán $BC$, $CA$ a $AB$ po rade v bodoch $D$, $E$ a $F$. Potom $|AE| = |AF| = \frac{-a+b+c}{2}$.*

**Tvrdenie.** *V trojuholníku $ABC$ sa kružnica pripísaná strane $BC$ dotýka priamok $BC$, $CA$, $AB$ po rade v bodoch $D$, $E$, $F$. Potom platí, že*

(i) $|AE| = |AF| = \frac{a+b+c}{2}$,

(ii) $|BD| = |BF| = \frac{a+b-c}{2}$, $|CD| = |CE| = \frac{a-b+c}{2}$,

(iii) *body dotyku vpísanej a pripísanej kružnice so stranou $BC$ sú stredovo súmerné podľa stredu strany $|BC|$.*

### Úsekové uhly

**Úloha 1.** Nech $ABCD$ je lichobežník s $AB \parallel CD$. Kružnica opísaná trojuholníku $BCD$ pretne priamku $DA$ v bode $E$ rôznom od $D$. Ukážte, že $CB$ je dotyčnica ku kružnici opísanej trojuholníku $ABE$.

**Úloha 2.** Je daný trojuholník $ABC$, pre ktorý platí $|AC| > |AB|$. Dotyčnice ku kružnici jemu opísanej v bodoch $A$ a $B$ sa pretínajú v bode $T$. Os strany $BC$ pretína stranu $AC$ v bode $S$. Dokážte, že priamka $ST$ je rovnobežná s $BC$.

**Úloha 3.** Sú dané kružnice $k$, $l$, ktoré sa pretínajú v bodoch $A$, $B$. Označme $K$, $L$ po rade body dotyku ich spoločnej dotyčnice zvolenej tak, že bod $B$ je vnútorným bodom trojuholníka $AKL$. Na kružniciach $k$ a $l$ zvoľme po rade body $N$ a $M$ tak, aby bod $A$ bol vnútorným bodom úsečky $MN$. Dokážte, že štvoruholník $KLMN$ je tetivový práve vtedy, keď je priamka $MN$ dotyčnicou ku kružnici opísanej trojuholníku $AKL$.

**Úloha 4.** Na strane $AC$ trojuholníka $ABC$ leží bod $X$. Na stranách $AB$ a $BC$ nájdeme také body $P$ a $Q$, aby $PX$ bola dotyčnica ku kružnici opísanej $XBC$ a $QX$ bola dotyčnica ku kružnici opísanej $XBA$. Dokážte, že priamka $PQ$ je rovnobežná s $AC$.

**Úloha 5.** Nech $ABC$ je ostrouhlý trojuholník. Zvoľme kružnicu $\omega$ prechádzajúcu bodmi $B$ a $C$, ktorá pretne druhýkrát úsečky $AB$ a $AC$ postupne v bodoch $D \neq A$ a $E \neq A$. Nech $F$ je priesečník priamok $BE$ a $CD$. Nech $G$ je bod na kružnici opísanej trojuholníku $ABF$ taký, že $GB$ je dotyčnicou ku kružnici $\omega$. Podobne, nech $H$ je bod na kružnici opísanej trojuholníku $ACF$ taký, že $HC$ je dotyčnicou ku kružnici $\omega$. Dokážte, že existuje taký bod $T \neq A$, ktorý nezávisí na voľbe kružnice $\omega$, že kružnica opísaná trojuholníku $AGH$ prechádza bodom $T$. (MEMO 2024)

### Dotyčnice a ich dĺžky

**Úloha 6.** Dokážte, že v pravouhlom trojuholníku $ABC$ s pravým uhlom pri vrchole $A$ je polomer vpísanej kružnice rovný $s - |BC|$, kde $s$ je polovica obvodu trojuholníka $ABC$.

**Úloha 7.** Majme kružnicu $k$ so stredom $S$, polomerom 1 a bod $P$ taký, že $|PS| = 3$. Týmto bodom veďme dotyčnice ku kružnici $k$, ktoré sa jej dotknú v bodoch $A$, $B$. Ďalej si zvoľme ľubovoľný bod $T$ kratšieho oblúku $AB$ kružnice $k$ a ním veďme

dotyčnicu ku $k$. Táto dotyčnica pretne úsečky $AP$ a $BP$ v bodoch $X$ a $Y$. Určite obvod trojuholníka $PXY$. (Náboj 2008)

**Úloha 8.** Daný je trojuholník $ABC$ s kružnicou vpísanou $k$. Body $X$ a $Y$ ležia na stranách $AB$ a $AC$ tak, že $XY$ je dotyčnica ku kružnici $k$ a platí $|AB| = 6$, $|BC| = 7$, $|CA| = 8$. Určite obvod trojuholníka $AXY$.

**Úloha 9.** Majme trojuholník $ABC$. Nakreslíme tri dotyčnice k jeho vpísanej kružnici tak, že každá odreže iný z vrcholov trojuholníka. Obvody odrezaných trojuholníkov sú 1, 2 a 3. Dokážte, že pôvodný trojuholník bol pravouhlý. (MKS 32–6–3)

**Úloha 10.** Zostrojte trojuholník $ABC$, ak poznáte jeho obvod $o$, polomer $\rho$ kružnice pripísanej k strane $BC$ a veľkosť výšky $v$ na túto stranu. (MO 68–A–I–5)

**Úloha 11.** V danom trojuholníku $ABC$ označme $D$ bod dotyku kružnice vpísanej so stranou $BC$. Kružnica vpísaná trojuholníku $ABD$ sa dotýka strán $AB$ a $BD$ v bodoch $K$ a $L$. Kružnica vpísaná trojuholníku $ADC$ sa dotýka strán $DC$ a $AC$ v bodoch $M$ a $N$. Dokážte, že body $K$, $L$, $M$, $N$ ležia na jednej kružnici. (MO 64–A–I–5)

**Úloha 12.** Daný je rovnobežník $ABCD$, pričom $|AB| > |BC|$. Body $K$ a $M$ sú bodmi dotyku kružníc vpísaných trojuholníkom $ACD$ a $ABC$ s uhlopriečkou $AC$. Body $L$ a $N$ sú podobne bodmi dotyku kružníc vpísaných trojuholníkom $BCD$ a $ABD$ s $BD$. Dokážte, že $KLMN$ je obdĺžnik. (MO 54–A–I–2)

**Úloha 13.** Daný je ostrouhlý trojuholník $ABC$. Na polpriamke opačnej k polpriamke $BC$ leží bod $P$ taký, že $|AB| = |BP|$. Analogicky na polpriamke opačnej k polpriamke $CB$ leží bod $Q$ taký, že $|AC| = |CQ|$. Označme $J$ stred kružnice pripísanej strane $BC$ daného trojuholníka a $D$, $E$ postupne jej body dotyku s priamkami $AB$ a $AC$. Predpokladajme, že polpriamky opačné k polpriamkam $DP$ a $EQ$ sa pretínajú v bode $F$ rôznom od $J$. Dokážte, že $AF \perp FJ$. (MO 68–A–III–4)

### A ideme ďalej

**Tvrdenie.** (o dotyčnicovom štvoruholníku) *Daný je štvoruholník $ABCD$, ktorý má vpísanú kružnicu (dotýka sa všetkých štyroch strán). Potom platí, že $|AB| + |CD| = |BC| + |AD|$. Dokážte.*

**Úloha 14.** Daný je rovnobežník $ABCD$, pričom $|AB| = 2 \cdot |BC|$. Určte všetky priamky, ktoré delia daný rovnobežník na dva dotyčnicové štvoruholníky. (MO 64–A–S–2)

**Úloha 15.** Daný je štvoruholník $ABCD$ taký, že $|AB|+|CD| = |BC|+|AD|$. Dokážte, že kružnice vpísané trojuholníkom $ABC$ a $ADC$ sa uhlopriečky $AC$ dotýkajú v jednom bode.

**Úloha 16.** Daný je štvoruholník $ABCD$ taký, že $|AB| + |BC| = |CD| + |AD|$. Kružnice vpísané trojuholníkom $ABD$ a $CBD$ sa uhlopriečky $BD$ dotýkajú v bodoch $X$ a $Y$. Dokážte, že body $X$ a $Y$ sú rovnako vzdialené od stredu úsečky $BD$.

**Úloha 17.** Na priamke $a$, na ktorej leží strana $BC$ trojuholníka $ABC$, sú dané body dotyku všetkých troch jemu pripísaných kružníc (body $B$ a $C$ nie sú známe). Nájdite na tejto priamke bod dotyku kružnice vpísanej. (MO 63–B–I–3)

**Úloha 18.** Vo vnútri strán $BC$, $CA$, $AB$ daného trojuholníka $ABC$ zvolíme postupne body $D$, $E$, $F$ tak, aby sa úsečky $AD$, $BE$, $CF$ pretli v jednom bode, ktorý označíme $G$. Ak sa dajú štvoruholníkom $AFGE$, $BDGF$, $CEGD$ vpísať kružnice, z ktorých každé dve majú vonkajší dotyk, tak je trojuholník $ABC$ rovnostranný. Dokážte. (MO 52–A–III–2)

**Úloha 19.** Majme trojuholník $ABC$ s obvodom 4. Na polpriamkach $AB$ a $AC$ označme postupne body $X$, $Y$ tak, že $|AX| = |AY| = 1$ a úsečky $BC$ a $XY$ sa pretínajú v bode $M$. Dokážte, že aspoň jeden z trojuholníkov $ABM$, $ACM$ má obvod 2. (Rusko 2011)

## Návody

**1.** Využi vetu o úsekovom uhle.

**2.** Nájdi tetivový štvoruholník.

**3.** Využi viackrát úsekové uhly.

**4.** Nájdi 4 body ležiace na kružnici.

**5.** Nájdi kružnice s rovnakým polomerom. Využi symetriu podľa osi strany $BC$.

**6.** Čím je zaujímavý štvoruholník $AP_1IP_2$, kde $I$ je stredom kružnice vpísanej a $P_1$, $P_2$ sú jej body dotyku s odvesnami?

**7.** Čo vieme o úsečke $PB$?

**8.** Nech $P$ je bod dotyku kružnice $k$ a strany $AB$. Pomôže nám potom dĺžka úsečky $AP$?

**9.** Skús využiť poznatky z minulého príkladu.

**10.** Vieme z kružnice pripísanej získať bod $A$? Je potom $BC$ dotyčnica ešte k nejakej inej kružnici?

**11.** Skús dokázať, že sa osi úsečiek $KL$, $LM$ a $MN$ pretínajú v jednom bode, konkrétne v strede kružnice vpísanej trojuholníku $ABC$.

**12.** Dokáž pomocou preklápania dotyčníc, že v $KLMN$ sa uhlopriečky rozpoľujú a sú rovnako dlhé.

**13.** Dokáž, že $F$ leží na kružnici opísanej štvoruholníku $ADJE$, teda že $|\sphericalangle ADP| = |\sphericalangle AEF|$.

**14.** Dokáž, že ak $ABCD$ nie je obdĺžnik, potom také priamky existujú práve dve, obe prechádzajú priesečníkom uhlopriečok a na rovnobežníku vytínajú úsečky dĺžky $BC$. Ako je to pre obdĺžnik?

**15.** Vyjadri si vzdialenosti bodov dotyku jednotlivých kružníc s $AC$ a dokáž, že sa rovnajú.

**16.** Dokáž, že $|BX| = |DY|$, a zamysli sa, prečo vďaka tomu už máme vyhrané.

**17.** Dokáž, že $|BX| = |CZ|$ a zostroj stred úsečky $BC$.

**18.** Uvedom si, že kružnica vpísaná štvoruholníku $AFGE$ je zároveň kružnicou vpísanou trojuholníkom $ABE$ a $AFC$, a vyjadri veľkosť dotyčníc. Dokáž, že priamky $AD$, $BE$ a $CF$ sú osi vnútorných uhlov trojuholníka $ABC$ a využi ich vlastnosti.

**19.** Dokresli pripísanú kružnicu k $ABC$ a kružnicu so stredom v $A$ s nulovým polomerom.

## Literatúra a zdroje

[1] Adéla Karolína Žáčková: *Překlápění tečen*, Zásada, 2021.
[2] *Stránky matematické olympiády*, *http://www.matematickaolympiada.cz*.
[3] *Art of problem solving*, *https://artofproblemsolving.com*.

# Pascal

Michal Pecho

Abstrakt. Pascalová veta má obrovské množstvo podôb a môže často (väčšinou omylom) prekĺznuť do úloh v rôznych olympiádach. Riešenia potom môžu byť veľmi stručné, obsahujúce tak 6 alebo 12 písmeniek.

**Veta.** (Pascal) *Body $A$, $B$, $C$, $D$, $E$, $F$ ležia na jednej kužeľosečke práve vtedy, keď $AB \cap DE$, $BC \cap EF$ a $CD \cap FA$ ležia na priamke.*

**Veta.** (Pascal pre kružnice) *Uvažujme body $A$, $B$, $C$, $D$, $E$, $F$ ležiace na jednej kružnici. Potom $AB \cap DE$, $BC \cap EF$ a $CD \cap FA$ ležia na priamke.*

**Veta.** (Pappus) *Majme body $A$, $C$, $E$ ležiace na jednej priamke a body $B$, $D$, $F$ na tej druhej. Potom $AB \cap DE$, $BC \cap EF$, $CD \cap FA$ ležia na jednej priamke.*

**Úloha 1.** Daný je tetivový šesťuholník $ABCDEF$, pre ktorý platí $AB \parallel DE$ a $BC \parallel EF$. Dokážte, že platí $CD \parallel AF$.

**Úloha 2.** Dokáž, že sa výšky v trojuholníku pretnú v jednom bode.

**Úloha 3.** Označme $\omega$ kružnicu opísanú trojuholníku $ABC$, $E$ je stred oblúka $AC$ a $F$ je stred oblúka $AB$. Priamky $AF$ a $BE$ sa pretnú v $P$. Analogicky, $CF$ a $AE$ sa pretnú v $R$. Dotyčnica k $\omega$ v $A$ pretne $BC$ v $Q$. Dokážte, že $P$, $Q$, $R$ ležia na priamke.

**Úloha 4.** Buď $ABC$ ostrouhlý trojuholník a $k$ jeho kružnica opísaná. Označme postupne $t_A$, $t_B$, $t_C$ dotyčnice ku $k$ v $A$, $B$, $C$. Dokážte, že $AB \cap t_C$, $BC \cap t_A$ a $CA \cap t_B$ ležia na jednej priamke.

**Úloha 5.** Nech $ABCD$ je tetivový štvoruholník. Dotyčnice v $A$ a $C$ sa pretnú v $P$, dotyčnice v $B$ a $D$ sa pretnú v $Q$. Nech $R$ je priesečník $AB$ a $CD$, a $S$ nech je priesečník $AD$ a $BC$. Dokážte, že $P$, $Q$, $R$, $S$ ležia na priamke.

**Úloha 6.** Daný je rovnoramenný $\triangle ABC$ so základňou $AB$ a bod $P$ vnútri jeho výšky z vrcholu $C$. Priamka $AP$ pretína kružnicu opísanú $\triangle ABC$ v bode $Q$ rôznom od $A$. Rovnobežka so základňou $AB$ vedená bodom $P$ pretína rameno $BC$ v bode $R$. Dokážte, že polpriamka $QR$ je osou uhla $AQB$. (MO 71-A-II-3)

**Úloha 7.** Majme rovnobežník $ABCD$. Na priamke $AB$ je zvolený bod $X$ a na priamke $AD$ je zvolený bod $Y$. Označme $Z$ preklopené $A$ podľa stredu $XY$. Dokážte, že priamky $XD$, $BY$ a $CZ$ prechádzajú jedným bodom.

**Úloha 8.** Na kružnici $\omega$ ležia body $A$, $B$, $C$, $D$, $E$ v takomto poradí, pričom platí $|AB| = |AE|$. Označme $S$ priesečník $AC$ s $BD$ a $T$ priesečník $AD$ s $CE$. Priamka $ST$ pretne $\omega$ v bodoch $X$ a $Y$. Dokážte, že platí $|AX| = |AY|$.

**Úloha 9.** Štyri body $A$, $B$, $C$, $D$ ležia na kružnici so stredom v $O$. Body $X$ a $Y$ ležia postupne na $AB$ a $AD$ tak, že $CX \perp CD$ a $CY \perp BC$. Dokážte, že $O$, $X$, $Y$ ležia na jednej priamke.

**Úloha 10.** Na kružnici opísanej trojuholníku $ABC$ sú zvolené body $D$ a $E$. Priamky $AD$ a $AE$ pretnú $BC$ postupne v $X$ a $Y$. Označme $D'$ a $E'$ postupne preklopené $D$ a $E$ podľa osi strany $BC$. Dokážte, že $D'Y$ a $E'X$ sa pretínajú na kružnici opísanej.

**Úloha 11.** Priamka $AB$ sa dotýka kružnice $\omega$ v bode $Y$, ktorý leží na úsečke $AB$. Na kružnici $\omega$ leží bod $X$ taký, že $XY$ je priemerom $\omega$. Priamky $XA$, $XB$ pretnú $\omega$ druhýkrát postupne v $C$, $D$ a $AD$ a $BC$ pretnú $\omega$ postupne v $E$, $F$. Dokážte, že platí $|XE| = |XF|$.

**Úloha 12.** Majme trojuholník $ABC$ s kružnicou opísanou $\omega$. Označme $\Omega$ kružnicu dotýkajúcu sa zvnútra $\omega$ a strán $AB$ a $AC$ postupne v bodoch $T$,$B_1$, $C_1$. Dokážte, že stred $B_1C_1$ je stredom kružnice vpísanej $ABC$.

**Úloha 13.** Majme konštrukciu z predošlej úlohy. Označme $M_A$ stred oblúku $BC$ neobsahujúceho $A$. Dokážte, že $BC$, $TM_A$ a $B_1C_1$ prechádzajú jedným bodom.

**Úloha 14.** Nech $ABC$ je ostrouhlý trojuholník. Zvoľme kružnicu $\omega$ prechádzajúcu bodmi $B$ a $C$, ktorá pretne druhýkrát úsečky $AB$ a $AC$ postupne v bodoch $D \neq A$ a $E \neq A$. Nech $F$ je priesečník priamok $BE$ a $CD$. Nech $G$ je bod na kružnici opísanej trojuholníku $ABF$ taký, že $GB$ je dotyčnicou ku kružnici $\omega$. Podobne, nech $H$ je bod na kružnici opísanej trojuholníku $ACF$ taký, že $HC$ je dotyčnicou ku kružnici $\omega$. Dokážte, že existuje taký bod $T \neq A$, ktorý nezávisí na voľbe kružnice $\omega$, že kružnica opísaná trojuholníku $AGH$ prechádza bodom $T$. (MEMO 2024)

**Úloha 15.** Majme tetivový konvexný šesťuholník $ABCDEF$. Označme $K$, $L$ postupne priesečníky $AB$ s $CD$ a $AF$ s $DE$. Ďalej nech je $P$ priesečník $BE$ s $CF$. Označme $O_1$, $O_2$ postupne stredy kružníc opísaných trojuholníkom $BCK$ a $EFL$. Dokážte, že body $O_1$, $P$ a $O_2$ ležia na priamke. ($i$KS)

**Úloha 16.** Nech $\omega$ je kružnica opísaná pravouhlému trojuholníku $ABC$ ($|\sphericalangle BAC| = 90°$). Dotyčnica k $\omega$ v $A$ pretne $BC$ v $P$. Označme $M$ stred oblúku $AB$ a druhý priesečník $PM$ a $\omega$ ako $Q$. Dotyčnica k $\omega$ v bode $Q$ pretne $AC$ v $K$. Dokážte, že $|\sphericalangle PKC| = 90°$. (IGO 2016 Medium 4)

**Úloha 17.** Daný je trojuholník $ABC$ s ortocentrom $H$. Nech $M$ je stred $BC$ a $D$, $E$ postupne päty výšok vedených z $C$, $B$. Nech $P$ je priesečník $AH$ a $DE$. Kolmica na $AH$ v $H$ pretne $DM$ v $Q$. Dokážte, že body $P$, $Q$, $B$ ležia na priamke.

**Úloha 18.** Majme kružnicu $\omega$ a priamku $d$ mimo ňu. Označme $AB$ priemer $\omega$ taký, že $AB \perp d$ ($B$ je bližšie k $d$). Na $\omega$ zvoľme bod $C$. Označme $D = AC \cap d$. Jedna z dotyčníc k $\omega$ z $D$ sa dotýka $\omega$ v $E$ ($E$ leží v rovnakej polrovine ako $B$ vzhľadom k $AC$). Označme $F = BE \cap d$. Priamka $AF$ pretne $\omega$ druhýkrát v $G$. Dokážte, že bod, ktorý dostaneme preklopením $G$ podľa $AB$, leží na $CF$. (ISL 2004)

**Úloha 19.** Daný je tetivový štvoruholník $ABCD$. Nech $E$ je priesečník $AC$, $BD$. Kružnica $ABE$ pretne $AD$, $BC$ druhýkrát postupne v $F$ a $G$. Priamky $AE$ a $FB$ sa pretnú v $P$ a priamky $EB$ a $AG$ sa pretnú v $Q$. Nech $X$, $Y$ sú body, ktoré dostaneme preklopením $F$ a $G$ cez priamky $AE$, $EB$. Nech $K$ je priesečník $BD$ a $XP$, a nech $L$ je priesečník $AC$ a $QY$. Dokážte, že $KL$ a $AB$ sú rovnobežné.

**Úloha 20.** Majme bod $P$ vo vnútri trojuholníka $ABC$. Rovnobežky so stranami trojuholníka cez $P$ pretnú strany trojuholníka v šiestich bodoch. Dokážte, že týchto šesť bodov leží na jednej kužeľosečke.

**Úloha 21.** Je daný ostrouhlý trojuholník $ABC$ s ortocentrom $H$ a so stredom kružnice opísanej $O$. Označme $O_A$, $O_B$ a $O_C$ body, ktoré dostaneme preklopením $O$ postupne podľa strán $BC$, $AC$ a $AB$. Označme $P$, $Q$, $R$ postupne priesečníky $HO_A \cap BC$, $HO_B \cap AC$ a $HO_C \cap AB$. Dokážte, že priesečníky $BC \cap RQ$, $AC \cap PR$ a $AB \cap PQ$ ležia na priamke.

**Úloha 22.** Daný je ostrouhlý trojuholník $ABC$ so stredom opísanej kružnice $O$. Bod $T$ je na výške na stranu $AB$ taký, že $|\sphericalangle TBA| = |\sphericalangle ACB|$. Priamka $CO$ pretína stranu $AB$ v bode $K$. Dokážte, že os strany $AB$, výška na $BC$ a priamka $KT$ sa pretínajú v jednom bode.

### Návody

**1.** Využi nevlastnú priamku.

**2.** Využi pravé uhly.

**3.** Čo ak v Pascalovi použijeme dva body, ktoré sú veľmi blízko pri sebe?

**4.** Použi to, čo v predošlej úlohe, ale viackrát. Sprav „Pascalov trojuholník“.

**5.** Použi Pascala dvakrát.

**6.** Skús využiť Švrčkov bod. Ako sa chová dotyčnica v ňom?

**7.** Tentokrát nepoužijeme Pascala. Využi nevlastné body.

**8.** Preveď úlohu na úlohu so Švrkmi.

**9.** Skús pridať na kružnicu dva body tak, aby si vedel(a) pracovať lepšie s $O$.

**10.** Skús si zadefinovať $T$ ako priesečník $D'Y$ a potom použi Pascala.

**11.** Využi nevlastný bod.

**12.** Rozmysli si, že priamky $TB_1$ a $TC_1$ prechádzajú Švrkmi.

**13.** Skús použiť predošlú úlohu.

**14.** Využi mocnosť bodu ku kružnici.

**15.** Skús dokázať $KO_1 \parallel LO_2$. Potom použijeme Pascala dvakrát.

**16.** Použi Pascala dvakrát. Preveď úlohu na dokazovanie rovnobežností.

**17.** Nájdi kružnicu tak, aby sa dala použiť dotyčnica v $D$.

**18.** Pretni $GE$ a $BC$.

**19.** Dokáž, že body $P$, $X$, $E$, $Q$, $Y$ ležia na kružnici.

**20.** Skús využiť opačnú implikáciu Pascala.

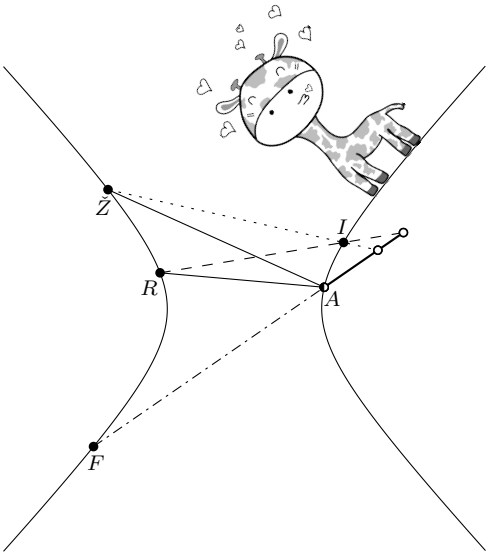
**21.** Nájdi elipsu.

**22.** Nájdi hyperbolu.

## Literatura a zdroje

[1] Radek Olšák: *Pascal Chasing*, Lysečiny, 2021.
[2] Carl Joshua Quines: *Pascal's theorem*, *https://cjquines.com/files/pascals.pdf*.
[3] *https://artofproblemsolving.com/*.

Ide žirafa po ľubovoľnej kužeľosečke a Pascal jej hovorí: „Priesečníky $\check{Z}I$ s $AF$, $IR$ s $FA$ a $\check{Z}A$ s $RA$ ležia na priamke.“ A žirafa na to: „Ja viem!“



# Diskrétní kalkulus

Daniel Perout

Abstrakt. V příspěvku je představena čistě početní metoda tzv. *diskrétního kalkulu*. Přívlastek *diskrétní* odkazuje k tomu, že předmětem zájmu budou posloupnosti namísto reálných funkcí, které zkoumá klasický kalkulus. Analogie některých metod z klasického kalkulu proto můžeme využít pro zkoumání posloupností a jejich součtů. Uplatnění tak lze najít i v kombinatorických úlohách.

**Příklad.** (Motivační) Sečtěte

$$\sum_{i=1}^{n} \frac{1}{i(i+1)}.$$

(folklor)

*Řešení.* Trikově upravme:

$$\sum_{i=1}^{n} \frac{1}{i(i+1)} = \sum_{i=1}^{n} \left( \frac{1}{i} - \frac{1}{i+1} \right) = 1 - \frac{1}{n+1}.$$

Vskutku, v prvním kroku jsme pouze upravili zlomek uvnitř sumy, v druhém kroku se požrala většina sousedních členů.

Přijít na takový trik napoprvé určitě není lehké. Ale když už o něm víme, nejde zobecnit i na další sumy? Pointa předchozího výpočtu přece spočívala pouze ve vyjádření členů sumy pomocí rozdílů následujících členů nějaké vhodné posloupnosti.

### Posloupnosti, jejich derivace a integrály

Naším základním objektem budou celočíselné posloupnosti – ty si budeme představovat jako funkce $f : \mathbb{N} \to \mathbb{Z}$ nebo trochu obecněji $f : \mathbb{Z} \to \mathbb{Z}$. V textu tak budeme slova posloupnost a funkce běžně zaměňovat.

Posloupnosti umíme sčítat i násobit po prvcích: Součtem posloupností $a$, $b$ myslíme posloupnost definovanou jako $(a + b)(x) = a(x) + b(x)$. Obdobně součinem posloupností $a$, $b$ rozumíme $(a \cdot b)(x) = a(x) \cdot b(x)$. Každé $c \in \mathbb{Z}$ navíc určuje konstantní posloupnost $f_c(x) = c$.

**Definice.** *Diskrétní derivací* funkce $f : \mathbb{Z} \to \mathbb{Z}$ myslíme funkci $\Delta f$ definovanou jako

$$\Delta f(x) = f(x+1) - f(x).$$

Pro $n \geq 0$ značíme symbolem $\Delta^n f$ opakované $n$-násobné použití diskrétní derivace na funkci $f$. Funkce $\Delta^n f$ se nazývá *$n$-tá diskrétní derivace* funkce $f$.

**Definice.** *Diskrétním integrálem* funkce $f : \mathbb{Z} \to \mathbb{Z}$ myslíme libovolnou funkci $g : \mathbb{Z} \to \mathbb{Z}$ splňující $\Delta g = f$. Značíme jej $\Sigma f$.

**Cvičení.** Diskrétní integrál funkce $f$ je jednoznačně určený až na přičtení celočíselné konstanty $c$.

**Poznámka.** (formální) Striktně vzato, symbol $\Sigma f$ označuje jednu konkrétní volbu diskrétního integrálu. Všechny ostatní pak můžeme získat přičítáním celočíselných konstant.

Ještě trochu formálněji, symbol $\Sigma f$ může označovat množinu všech diskrétních integrálů funkce $f$. Tím se lze zbavit vší nejednoznačnosti.

**Poznámka.** Definice diskrétní derivace $\Delta$ a diskrétního integrálu $\Sigma$ se nápadně podobají definicím derivace a integrálu reálných funkcí a v mnoha ohledech se proto chovají podobně.

Čistě z technických důvodů si ještě zavedeme značení pro posun indexů dané posloupnosti.

**Definice.** Pro posloupnost $f : \mathbb{Z} \to \mathbb{Z}$ definujeme její *posunutí* $Ef$ pomocí předpisu $Ef(a) = f(a+1)$. Obecněji, pro celé $n$ značíme $E^n f$ posloupnost definovanou jako $E^n f = f(a+n)$.

**Poznámka.** (formální) Symboly $\Delta$, $\Sigma$, $E$ vždy umíme napsat před nějakou posloupnost $f$, a tím získat novou posloupnost. S trochou představivosti je proto můžeme vnímat jako *operátory na množině všech posloupností*. Tento pohled trochu zjednodušuje značení: chceme-li třeba říct „při výpočtech nezáleží na vzájemném pořadí diskrétního derivování a posouvání“, stačí napsat $E\Delta = \Delta E$. Podobně je zřejmé, že operátor $\Delta^n$ je $n$-násobným složením operátoru $\Delta$.

Z našich definic je jasné, že operace $\Delta$ a $\Sigma$ jsou k sobě v podstatě inverzní – pro jakoukoli posloupnost $f$ platí $\Delta\Sigma f = f$, zatímco $\Sigma\Delta f = f$ platí až na přičtení konstanty.

Diskrétní integrál $\Sigma f$ má ale mnohem přímočařejší interpretaci: až na konstantu je dán prefixovými součty posloupnosti $f$.

**Cvičení.** (klíčové) Dokažte, že pro libovolná $a \leq b \in \mathbb{Z}$ platí[1]

$$(\Sigma f)(b+1) - (\Sigma f)(a) = f(a) + f(a+1) + \cdots + f(b).$$

[1]Pozor na indexy! Na levé straně opravdu vystupuje $b+1$, ale napravo sčítáme jenom k $b$.

**Definice.** Pro funkci $g : \mathbb{Z} \to \mathbb{Z}$ a hodnoty $a, b \in \mathbb{Z}$ označme

$$[g]_a^b = g(b) - g(a).$$

Předchozí vztah tak pomocí nové notace můžeme přepsat jako

$$[\Sigma f]_a^{b+1} = \sum_{i=a}^{b} f(i).$$

**Cvičení.** Spočtěte $\Delta f$ a $\Sigma f$ konstantní posloupnosti $f(x) = 1$. Co se bude dít pro jiné konstanty?

**Cvičení.** Spočtěte diskrétní derivaci a integrál Fibonacciho posloupnosti definované na nezáporných celých číslech, tedy posloupnosti definované jako

$$F(0) = 0, \qquad F(1) = 1, \qquad F(n+2) = F(n+1) + F(n).$$

**Cvičení.** Ukažte, že pro každou posloupnost $f$, která je nenulovým polynomem, platí $\deg \Delta f = \deg f - 1$.

**Cvičení.** Buď $c \in \mathbb{Z}$. Jaká je diskrétní derivace posloupnosti $f(x) = c^x$?

**Cvičení.** Buď $d \geq 0$. Jaká je diskrétní derivace posloupnosti $f(x) = \prod_{i=0}^{d-1}(x - i)$?

Předchozí cvičení ukazuje důležitý příklad posloupnosti s pěknou, a níže ukážeme že i významnou, diskrétní derivací. Pro budoucí využití zavedeme jednoduché značení.

**Definice.** Polynom $x^{\underline{d}} = \prod_{i=0}^{d-1}(x - i)$ nazveme *d-tou klesající mocninou.*

**Poznámka.** Klesající mocniny lze smysluplně definovat i pro záporná $d$ jako $x^{\underline{d}} = \prod_{i=1}^{-d} \frac{1}{x+i}$. Pro každé $d \neq 0$ pak platí

$$\Delta x^{\underline{d}} = d \cdot x^{\underline{d-1}}.$$

**Tvrzení.** (Aritmetika diskrétní derivace)

(i) *Buď $f : \mathbb{Z} \to \mathbb{Z}$ posloupnost a $c \in \mathbb{Z}$. Potom platí $\Delta(c \cdot f) = c \cdot \Delta f$.*
(ii) *Mějme dvě posloupnosti $f, g : \mathbb{Z} \to \mathbb{Z}$. Potom platí $\Delta(f + g) = \Delta f + \Delta g$.*
(iii) *Mějme dvě posloupnosti $f, g : \mathbb{Z} \to \mathbb{Z}$. Potom platí $\Delta(f \cdot g) = f \cdot \Delta g + \Delta f \cdot Eg$. Tato rovnost se někdy označuje jako Leibnizovo pravidlo.*
(iv) *$n$-tá diskrétní derivace posloupnosti $f$ je explicitně dána vztahem*

$$\Delta^n f(x) = \sum_{i=0}^{n} (-1)^{n-i} \cdot \binom{n}{i} \cdot f(x+i).$$

**Důsledek.** *Mějme dvě posloupnosti $f, g : \mathbb{Z} \to \mathbb{Z}$. Potom platí*

$$\Delta^n(f \cdot g) = \sum_{i=0}^{n} \binom{n}{i} \cdot \left(\Delta^i f\right) \cdot \left(\Delta^{n-i} E^i g\right).$$

Z předchozího tvrzení lze odvodit, že vztahy obdobné (i) a (ii) platí i pro diskrétní integrály.

Násobení uvnitř integrálu je ale o poznání složitější. Lze využít takzvanou *integraci per partes*, kterou dostáváme přepsáním Leibnizova pravidla.

**Tvrzení.** (integrace per partes)

$$\Sigma(f \cdot \Delta g) = f \cdot g - \Sigma(\Delta f \cdot Eg).$$

Využijeme ji v případě, kdy chceme určit diskrétní integrál součinu dvou funkcí $f$, $h$ a zároveň známe diskrétní integrál $g$ funkce $h$, v takovou chvíli postačí spočítat diskrétní integrál součinu $\Delta f \cdot Eg$.

### Kalkulujme ...

Pojďme si teď nabyté znalosti vyzkoušet na několika příkladech. Jak už jsme zmínili výše, nejpřímočařejším použitím diskrétního kalkulu je prosté sčítání sum. Myšlenka je přímočará. Sumační index si představíme jako proměnnou a posléze se pokusíme spočítat diskrétní integrál posloupnosti v sumě. Pokud se to povede, stačí správně dosadit krajní hodnoty.

**Úloha 1.** Pro $n \geq 0$ sečtěte

$$\sum_{i=0}^{n} i(i+1).$$

**Úloha 2.** Pro $n \geq 0$ sečtěte

$$\sum_{i=0}^{n} i^2.$$

Rozmyslete si, že podobně umíme postupovat i pro vyšší exponenty.

**Úloha 3.** Pro $n \geq 0$ sečtěte

$$\sum_{i=0}^{n} i \cdot 2^i.$$

### Přemýšlejme ...

Čas od času však člověk může narazit i na sofistikovanější úlohu, kterou výše předvedená teorie značně ulehčí.

Myšlenka diskrétního kalkulu se může hodit i ve více kombinatorických úlohách. Pokud se třeba snažíme vyjádřit nějakou kombinatoricky zadanou posloupnost algebraickým předpisem, stačí kombinatoricky určit její diferenci. I když člověk diskrétní kalkulus moc nezná, dívat se na diference se zkrátka vyplatí.

**Úloha 4.** Nalezněte všechny množiny kladných celých čísel $\{a_1, \ldots, a_n\}$, které pro každé kladné celé $x$ splňují $a_1 \cdots a_n \mid (x + a_1) \cdots (x + a_n)$. (ELMO SL 2018)

**Úloha 5.** Pro $m > n \geq 0$ sečtěte

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

**Úloha 6.** Pro $n \geq 0$ sečtěte

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

**Úloha 7.** Pro $n \geq 0$ sečtěte

$$\sum_{i=0}^{n} (-1)^i i^2.$$

**Úloha 8.** Sečtěte

$$\sum_{k=1}^{n} k \binom{n}{k}.$$

**Úloha 9.** Sečtěte

$$\sum_{k=1}^{n} k^2 \binom{n}{k}.$$

**Úloha 10.** Buď $p$ prvočíslo. Posloupnost celých čísel $(z_n)_{n=0}^{\infty}$ se nazývá *péčková*, jestliže pro každé přirozené číslo $e$ existuje takové $d \geq 0$, že pro všechna celá $m \geq d$ platí

$$p^e \,\Big|\, \sum_{i=0}^{m} (-1)^i \binom{m}{i} z_i.$$

Dokažte, že pokud jsou obě posloupnosti $(x_n)_{n=0}^{\infty}$ a $(y_n)_{n=0}^{\infty}$ péčkové, je péčková i posloupnost $(x_n y_n)_{n=0}^{\infty}$. (USA TST 2011)

**Úloha 11.** Pro $n > m \geq 0$ dokažte

$$\sum_{k=0}^{n} (-1)^k \cdot \binom{2n+1}{n-k} \cdot (2k+1)^{2m+1} = 0.$$

(Crux 2019)

**Úloha 12.** (Pólya) Polynom $f \in \mathbb{Q}[x]$ s racionálními koeficienty se nazývá *numerický*, jestliže se dá zapsat jako celočíselná lineární kombinace polynomů $\binom{x}{d}$ pro $d \in \mathbb{N}_0$. Dokažte, že polynom $f \in \mathbb{Q}[x]$ je numerický právě tehdy, když na celých číslech nabývá pouze celočíselných hodnot.[2]

### Návody

**1.** Diskrétní integrál funkce $x(x+1)$ už – až na posunutí – znáš. Výsledek bude $\frac{1}{3}(n+2)(n+1)n$.

**2.** Rozepiš polynom $x^2$ pomocí klesajících mocnin. Vyjde $\frac{(2n+1)(n+1)n}{6}$. Podobný postup funguje pro jakýkoli pevně zvolený exponent – pouze je třeba přecházet mezi běžným tvarem polynomu a jeho rozepsáním do klesajících mocnin.

**3.** Diskrétní integrál funkce $2^x$ je opět $2^x$, použij per partes. Pozor na posun indexu! Vyjde $2^{n+1}(n-1)+2$.

**4.** Diskrétní derivace polynomu $f(x) = (x+a_1)\cdots(x+a_n)$ je dělitelná $a_1 \cdots a_n$. Co jeho $n$-tá derivace? Vyjádři přesně $\Delta^n f(x)$.

**5.** Vezmi polynom $f(x) = (m-x)^n$, jak vypadá $\Delta^n f$? Vyjádři jeho hodnotu v 0 druhým způsobem.

**6.** Uvaž polynom $f(x) = x^n$ a zamysli se nad polynomem $\Delta^n f$ a jeho hodnotou v 0.

**7.** Per partes. A pak? Per partes. Pokud se nepřepočítáš, vyjde $\frac{(-1)^n n(n+1)}{2} = (-1)^n \binom{n+1}{2}$.

**8.** Vyjádři dvěma způsoby $n$-tou diskrétní derivaci funkce $f(x) = (-1)^x \cdot x$. Téměř všechny vyšší derivace funkce $g(x) = x$ jsou nulové.

**9.** Obdobný trik jako v předchozí úloze.

**10.** Posloupnost $f$ je péčková, právě když se $\Delta^m f(0)$ při zvětšování $m$ stává víc a víc dělitelné $p$. Použij Leibnizovo pravidlo. Co zbývá ukázat o výrazech $\Delta^m g(j)$ pro péčkovou posloupnost $g$ a čísla $j \geq 0$?

**11.** Tipni polynom $f(x) = (2n+1-2x)^{2m+1}$. Spočti $\Delta^{2n+1} f(0)$ jednoduše a složitě. Posléze formálně přepiš Leibnizovskou sumu jako dvojnásobek zadaného výrazu.

**12.** Použití operací $\Delta$ a $\Sigma$ zachovává numeričnost. Úlohu dokazuj indukcí podle stupně $f$.

### Literatura a zdroje

Příspěvek je převzán od Jakuba Löwita, který navazuje na příspěvek Michala Szabadose. Oběma zmíněným tímto děkuji.

[1] Jakub Löwit: *Kombinatorické identity*, sborník *i*KS, 2021.
[2] Michal Szabados: *Diskrétný kalkulus (alebo ako počítať sumy)*, Oldřichov, 2010.

[2] Toto tvrzení tedy v jistém smyslu vysvětluje, proč se kombinační čísla objevují tak často: kdykoli lze nějakou celočíselnou posloupnost definovat racionálním polynomem, už se dá zapsat jako jejich celočíselná kombinace.

# Eliptické křivky

Zdeněk Pezlar

Abstrakt. Co mají společného rozkládání čísel na prvočísla, Velká Fermatova věta a ovoce? Jak se ukáže, jeden z nejdůležitějších objektů v algebře a teorii čísel – Eliptické křivky. O nich si popovídáme, včetně nějakých nedávných pokroků.

*„It is possible to write endlessly on elliptic curves. This is not a threat.“*

– Serge Lang

Okolo roku 1637 se Pierre de Fermat zamyslel nad rovnicí

$$X^3 + Y^3 = Z^3,$$

přesněji jejími racionálními řešeními. Jeden způsob, jak si rovnici můžeme přiblížit, je substituce. Substituujme $X/Z = u + v$, $Y/Z = u - v$, čímž se zbavíme dvou kubických členů a získáme $2u^3 + 6uv^2 - 1 = 0$. Další substituce $x = -\frac{6}{u}$, $y = \frac{36u}{v}$ vede na jednodušší tvar $y^2 = x^3 - 432$. Získali jsme právě rovnici známou jako eliptickou křivku. Pojďme se jim podívat na zub.

**Úmluva.** Cvičení jsou úlohy pro čtenáře na procvičení materiálu. Úlohy pořešíme na přednášce a bez mašinérie ani moc řešitelné nejsou.

**Definice.** *Projektivní prostor* nad $\mathbb{Q}$ definujeme jako prostor trojic racionálních čísel (bodů) $(X : Y : Z) \neq (0 : 0 : 0)$, kde ztotožníme body $(X : Y : Z)$ a $(kX : kY : kZ)$. *Eliptickou křivku* definujeme jako množinu bodů splňujících

$$E : Y^2Z = X^3 + aXZ^2 + bZ^3$$

pro $4a^3 + 27b^2 \neq 0$. Křivce přísluší *afinní varianta*

$$y = x^3 + ax + b,$$

kde body $(x, y)$ přísluší bodům $(x : y : 1)$. Označme $O = (0 : 1 : 0)$ *bod v nekonečnu* křivky, který nemá afinní reprezentaci.

**Cvičení.** Nakresli křivky $y^2 = x^3 + x$, $y^2 = x^3 - x$ a $y^2 = x^3 + 10$.

**Cvičení.** Uvažme křivku $y^2 = x^3 - 7x^2 + 10x$ a dva její body $(2, 0)$ a $(8, 12)$. Přímka skrz tyto dva body protíná křivku ve třetím bodě. Urči jeho souřadnice.

**Cvičení.** Rozmysli si, že přímka skrz dva racionální body protíná křivku znovu v racionálním bodě.

**Definice.** Buď $P$ bod na eliptické křivce. Definujeme $-P$ jako bod s opačnou $y$-ovou souřadnicí než $P$. Dále pro libovolný $Q \neq \pm P$ definujeme součet bodů $P$, $Q$ následovně: označme $R$ třetí průsečík přímky skrz $P$ a $Q$ s křivkou. Jako součet $P+Q$ bereme bod $-R$.

Jako $P+P$ definujeme jako druhý průsečík tečny ke křivce procházející bodem $P$ s křivkou. Konečně, definujeme $P+(-P)=O$ a $P+O=P$.

Platí, že takto definované sčítání je asociativní[1], tedy body na eliptické křivce spolu s ním tvoří grupu.

**Věta.** *Sčítání je na eliptické křivce komutativní a asociativní.*

Věříme-li větě výše, poté můžeme pro $P \in E$ jednoznačně definovat bod

$$\underbrace{P+P+\cdots+P}_{n\text{-krát}},$$

říkejme mu *$n$-násobek bodu $P$* a značme jej $[n]P$.

**Příklad.** (Generování nových bodů) Uvažme křivku $E : y^2 = x^3 - 5x + 8$ a bod $P = (1,2) \in E$. Spočítáme $[2]P = P + P = \left(-\frac{7}{4}, -\frac{27}{8}\right)$. Dále

$$[3]P = P + [2]P = \left(\frac{553}{121}, -\frac{11950}{1331}\right),$$
$$[4]P = [2]([2]P) = [3]P + P = \left(\frac{45313}{11664}, \frac{8655103}{1259712}\right).$$

**Cvičení.** Vymysli efektivní algoritmus na získání $n$-násobku bodu.

O bodě řekneme, že leží v *$n$-torzi*, pokud jeho $n$-násobek je $O$. O bodě řekneme, že je *torzní*, pokud leží v nějaké $n$-torzi. Snadno si rozmyslíme, že množina torzních bodů je uzavřena na sčítání.

Velká část studia eliptických křivek se zaobírá jejich body nad racionálními čísly. Označme proto pro danou křivku $E(\mathbb{Q})$ množinu jejích bodů s racionálními souřadnicemi. Torzní body křivky $E(\mathbb{Q})$ lze hledat algoritmicky snadno, k tomu lze využít následující důležitou větu.

**Věta.** (Lutz–Nagell) *Buďte $a$, $b$ celá čísla, $E : y^2 = x^3 + ax + b$ eliptická křivka a $(x_1, y_1) \in E(\mathbb{Q})$ torzní bod. Pak buď $y = 0$ nebo $x_1, y_1 \in \mathbb{Z}$ a $y_1^2 \mid 4a^3 + 27b^2$.*

Tu si nedokážeme, možná si ukážeme trochu lehčí variantu.

**Věta.** (Lutz–Nagell bez steroidů) *Buďte $a$, $b$ celá čísla, $E : y^2 = x^3 + ax + b$ eliptická křivka a $P = (x_1, y_1) \in E(\mathbb{Q})$ je bod takový, že $P$ i $2P$ mají celočíselné souřadnice. Pak buď $y_1 = 0$ nebo $y^2 \mid 4a^3 + 27b^2$.*

**Cvičení.** Najdi všechny torzní body na křivce $y^2 = x^3 - px$, kde $p$ je prvočíslo.

[1] Ukázat tohle je těžké, případně si povíme na přednášce.

**Cvičení.** Najdi torzní a netorzní bod na křivce $E : y^2 = x^3 + 9$ nad racionálními čísly.

**Věta.** (Siegel) *Množina $E(\mathbb{Q})$ je konečně generovaná, tedy lze zvolit nějakých konečně mnoho bodů $P_1, \ldots, P_r$ tak, že*

$$E(\mathbb{Q}) = \{[a_1]P_1 + \cdots + [a_r]P_r \mid a_1, \ldots, a_r \in \mathbb{Z}\}.$$

### Úlohy

Následuje pár úloh, které možná překvapivě všechny souvisí s eliptickými křivkami. Na přednášce se na ně pořádně mrkneme. Pozor, odvážný řešiteli – některé z těchto příkladů doslova nejdou řešit bez pomoci počítače – jsou to úlohy 7, 8, 9 a 10.

**Úloha 1.** (Velký Fermat pro $n = 3$) Ukažte, že rovnice $X^3 + Y^3 = Z^3$ nemá netriviální racionální řešení.

*Řešení.* Došli jsme ke křivce $y^2 = x^3 - 432$, hledejme na ní racionální body. Torzní body spočítáme pomocí Lutz–Nagellovy věty a jsou pouze tři, $\{O, (12 : \pm 36 : 1)\}$. Tyto body dají pouze dvě řešení původní rovnice, $(t, 0, t)$ a $(0, t, t)$.

Zbývají nám tedy body netorzní. Lze poměrně těžko ukázat, že žádné nejsou, tudíž výše jsou všechna racionální řešení Fermatovy rovnice.

**Úloha 2.** Z několika tenisáků postavíme pyramidu s čtvercovou základnou. Pokud tuto pyramidu rozpustíme, můžeme tenisáky uspořádat do čtverce. Kolik míčku jsme mohli mít? Najdi alespoň dvě celočíselná řešení.

*Řešení.* Pokud má pyramida výšku $x$, tak počet tenisáků je $1^2 + 2^2 + \cdots + x^2 = \frac{x(x+1)(2x+1)}{6}$. Hledáme tedy řešení rovnice $y^2 = \frac{x(x+1)(2x+1)}{6}$, což definuje (nad $\mathbb{R}$) eliptickou křivku. Dva zřejmé body jsou $(0, 0)$ a $(1, 1)$.

Spočítáme $(0, 0) + (1, 1) = \left(\frac{1}{2}, -\frac{1}{2}\right)$. Podobně $(1, 1) + \left(\frac{1}{2}, -\frac{1}{2}\right) = (24, -70)$, čímž získáme druhé řešení. Jsou ještě nějaká další? To tak lehko nezjistíme.

**Úloha 3.** Ukaž, že pokud rovnice $x^3 + y^3 = N$ má racionální řešení, pak jich má nekonečně mnoho.

**Úloha 4.** Ověř, že 6 není součtem dvou celých třetích mocnin, ale platí $6 = (17/21)^3 + (37/21)^3$. Převeď křivku $x^3 + y^3 = 6$ na eliptickou podobně jako u prvního příkladu.

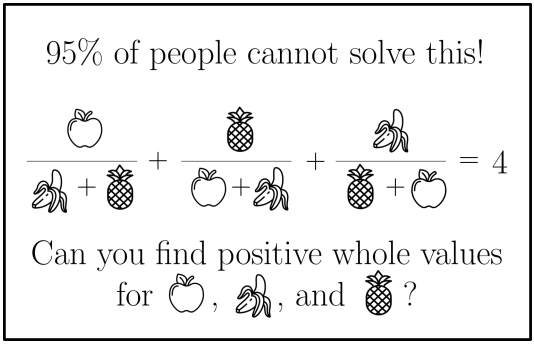
**Úloha 5.** Ukaž, že existuje posloupnost bodů

$$\ldots, \quad P_{-3}, \quad P_{-2}, \quad P_{-1}, \quad P_0, \quad P_1, \quad P_2, \quad P_3, \quad \ldots$$

v rovině taková, že platí: pro libovolnou trojici celých čísel $a, b$, a $c$, leží body $P_a$, $P_b$, a $P_c$ na jedné přímce právě tehdy, když $a + b + c = 2024$. (USAMO 2014)

**Úloha 6.** Zvolme celá čísla $b$, $c$, $d$ a polynom $P(x) = x^3 + bx^2 + cx + d$. Dejme tomu, že existují právě dvě celá čísla $x$ taková, že hodnota $P(x)$ je čtvercem, čísla 2024 a 2025. Ukaž, že jeden z těch čtverců je nula. (RMM 2016)

**Úloha 7.** (Úloha z facebooku) Vyřeš následující rovnici:




**Úloha 8.** Určete všechny trojúhelníky, jejichž jedna výška, jedna těžnice a jedna osa úhlu prochází jedním bodem.

**Úloha 9.** (Problém kongruentního čísla) Najděte pravoúhlý trojúhelník s racionálními stranami a obsahem 5.

**Úloha 10.** Najděte všechna přirozená $N$, pro která existují racionální $x$, $y$ a $z$ splňující

$$x + y + z = N = xyz.$$

Nakonec ještě poznamenejme, že eliptické křivky hrály důležitou roli v důkaze Velké Fermatovy věty i pro vyšší exponenty. Toto propojení je ale mnohem, mnohem složitější, než co stihneme na přednášce.

### Návody

**3.** Sčítání bodů.

**5.** Vezmi bod neležící v torzi nějaké křivky a jeho vhodné násobky.

**6.** Podívej se na součet těch dvou bodů.

**8.** Cevova věta, věta o ose úhlu, sinovka a kosinovka. Zamíchej dohromady, okořeň a získáš rovnici eliptické křivky svazující délky stran.

**9.** Pythagorova věta dává tři racionální čtverce, vynásob je.

### Literatura a zdroje

[1] Allan J. MacLeod: *Elliptic Curves in Recreational Number Theory*, *https://arxiv.org/pdf/1610.03430*.

[2] Lawrence C. Washington: *Elliptic curves: Number theory and cryptography*, 2008.

[3] Joseph H. Silverman: *An Introduction to the Theory of Elliptic Curves*, Summer School on Computational Number Theory and Applications to Cryptography, 2006.

[4] Geir Ellingsrud: *The Lutz–Nagell theorem and torsion points*.

# Velká čísla

Zdeněk Pezlar

Abstrakt. Asi ve čtvrté třídě jsme se ve třídě matematiky odpoutali od konkrétních čísel a to je celkem škoda. Tak si to na této přednášce vynahradíme. Pořádně.

V této přednášce si ukážeme, jak si poradit s *fakt velkýma* číslama. V obecnosti neexistuje jeden recept na všechno, bohužel budeme muset pořád přemýšlet, co s tímhle a nebo s tamtím číslem. Nejprve si hodíme nášup užitečných větiček.

**Definice.** Pro reálné číslo $x$ značíme jeho dolní celou část $\lfloor x \rfloor$ jako celé číslo splňující $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$. Necelou část $\{x\}$ čísla $x$ definujeme jako $\{x\} = x - \lfloor x \rfloor$.

### Velká fakta

**Věta.** (Wilsonova věta) *Pro libovolné prvočíslo $p$ platí $p \mid (p-1)! + 1$.*

**Definice.** Definujeme Eulerovu funkci $\varphi(n)$ jako počet čísel nepřevyšujících $n$, která jsou s $n$ nesoudělná.

**Tvrzení.** (Fakta o Eulerově funkci) *Pro $a$ a $n$ nesoudělná platí $a^{\varphi(n)} \equiv 1 \pmod{n}$. Pro $n = p_1^{a_1} \cdots p_k^{a_k}$ platí $\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$.*

**Tvrzení.** *Pro iracionální $\alpha$ je posloupnost $(\{k\alpha\})_{k=1}^{\infty}$ hustá v $[0,1)$ – tj. v libovolném netriviálním podintervalu $[0,1)$ existuje prvek posloupnosti.*

**Tvrzení.** *První cifra čísla $n$ je $\lfloor 10^{\{\log_{10} n\}} \rfloor$.*

Pár tipů před začátkem:

(1) Nelekni se velkých čísel,
(2) Na většinu následujících úloh stačí jen dávka kuráže, na některé vlastnosti řádů,
(3) Používej slabé odhady, v případě potřeby zesiluj.

### Velké cifry

**Úloha 1.** Určete první a poslední číslici a počet číslic čísla $7^{10000}$. Prozradím, že $\log_{10} 7 \approx 0.8450980\ldots$

**Úloha 2.** Ukažte, že čísla $0{,}12624120720\ldots$ a $0{,}248163264\ldots$, kde za desetinnou čárkou píšeme faktoriály, resp. mocniny dvojky, nejsou racionální.

**Úloha 3.** Určete poslední trojčíslí čísla $11^{11^{11}}$.

**Úloha 4.** Uvažme posloupnost $(a_n)_{n=1}^{\infty}$ se členy 2, $2^2$, $2^{2^2}$, $2^{2^{2^2}}$, ... Dokažte, že pro libovolné $m$ existuje $n$ takové, že pro každé $k \geq n$ platí $m \mid a_k - a_n$.

**Úloha 5.** Číslo $9^{4000}$ má 3817 cifer a začíná devítkou. Kolik čísel $9^k$ pro $k \in \{1, 2, \ldots, 3999\}$ začíná devítkou? (Prase 1992)

**Úloha 6.** Jaký je ciferný součet čísla $\underbrace{9999\ldots999}_{1000} \cdot 123456789$?

**Úloha 7.** Ukažte, že existuje mocnina 7, jejíž první tři cifry jsou 420.

**Úloha 8.** Ukažte, že každý prvočíselný dělitel čísla $10^{10^{10^{10}}} + 1$ má alespoň bilion cifer.

**Úloha 9.** Ukažte, že existuje nekonečně mnoho přirozených čísel $n$ takových, že číslo $\lfloor 2^n\sqrt{2} \rfloor + \lfloor 2^n\sqrt{3} \rfloor$ je sudé.

**Úloha 10.** (hnus) Ukažte, že existuje faktoriál, jehož první tři cifry jsou 420.

### Prostě jen velký čísla

**Úloha 11.** Které z čísel $\varphi\left(10^{10^{10^{10}}}\right)$ a $\varphi\left(10^{10^{10^{10}}} + 1\right)$ je větší?

**Úloha 12.** Najděte cifry $a$, $b$ a $c$ tak, že

$$34! = 29523279903960a14084761860964 35bc000000.$$

(Ázerbájdžán 2017)

**Úloha 13.** Ukažte, že $\left(10^{1800}\right)! > ((6!)!)! > \left(10^{1500}\right)!$.

**Úloha 14.** Ukažte, že rovnice $11^{10^{10}}x^2 + 10^{10^{10}}x + 9^{10^{10}} = 0$ má dva iracionální reálné kořeny.

**Úloha 15.** Tvoří kořeny polynomu $x^3 + 3^{2^{1002}+1}x^2 + 3^{2^{1001}+1}x + 3^{2^{1000}+1}$ v komplexní rovině rovnostranný trojúhelník?

**Úloha 16.** Určete paritu čísla $\left\lfloor \frac{2026!}{2027 \cdot 2028} \right\rfloor$. Prozradím, že 2027 je prvočíslo.

### Velké odmocniny

**Úloha 17.** Dokažte, že prvních 2024 cifer za desetinnou čárkou čísla $\left(5 + \sqrt{26}\right)^{2024}$ je stejných. (Brkos 2007)

**Úloha 18.** Určete první dvě číslice před a za desetinnou čárkou čísla $\sqrt{5^{362} + 5^{263}}$.

**Úloha 19.** Ukažte, že číslo $\sqrt{1000^2+1}+\sqrt{1001^2+1}+\cdots+\sqrt{2000^2+1}$ není celé. Jako (těžší) bonus ukažte, že už potom číslo není ani racionální. (Čína)

**Úloha 20.** Najděte dolní celou část čísla $\frac{1}{\sqrt{1}}+\frac{1}{\sqrt{2}}+\cdots+\frac{1}{\sqrt{20000}}$. (Brkos 2009)

### (Velké) mňamky na konec

**Definice.** Definujeme Ackermannovu funkci následovně

$$A(m,n)=\begin{cases} n+1, & \text{pro } m=0,\\ A(m-1,1), & \text{pro } m>0 \text{ a } n=0,\\ A(m-1,A(m,n-1)), & \text{jinak.}\end{cases}$$

Tato funkce roste velmi rychle, viz následující úloha.

**Úloha 21.** Ukažte, že

(1) $A(1,n)=n+2$,
(2) $A(2,n)=2n+3$,
(3) $A(3,n)=2^{n+3}-3$,
(4) $A(4,n)=\underbrace{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}}_{n+3}-3$.

**Úloha 22.** V každé ze šesti schránek $B_1$, $B_2$, $B_3$, $B_4$, $B_5$ a $B_6$ je na počátku jedna mince. Se schránkami můžeme provádět následující dvě operace:

(1) Vybrat neprázdnou schránku $B_j$ , kde $1\le j\le 5$, odebrat z ní jednu minci a přidat dvě mince do schránky $B_{j+1}$.
(2) Vybrat neprázdnou schránku $B_k$, kde $1\le k\le 4$, odebrat z ní jednu minci a navzájem vyměnit obsahy (případně prázdných) schránek $B_{k+1}$ a $B_{k+2}$.

Je možné mít v nějaký moment v jedné krabičce $2024^{2024^{2024}}$ mincí? (IMO 2010)

## Návody

**1.** Rozmysli, jak z logaritmu získat počet číslic.

**2.** Ukaž ne-periodicitu v nějaké soustavě, jak?

**3.** Binomická věta.

**4.** Indukuj na $\varphi(m)$.

**5.** Postupně mocni $9^k$. Kdy se přehoupne počet cifer?

**6.** Zapiš jako odečítání pod sebou.

**7.** Převeď na nerovnici v řeči logaritmů.

**8.** Odhadni řád 10 modulo $p$.

**9.** Řeš tu samou úlohu s $\lfloor 10^n\sqrt{2}\rfloor + \lfloor 10^n\sqrt{3}\rfloor$.

**10.** Z hustoty najdi $N$, že $\{\log_{10} N\}$ je malé. Pak se dívej na $(N+k)!$ pro malá $k$.

**11.** Jaká jsou čísla soudělná s $10^{10^{10^{10}}}$?

**12.** Na kolik nul končí tenhle faktoriál? Použij kritéria pro dělitelnosti založené na cifrách.

**13.** Platí $\left(\frac{n}{3}\right)^n < n! < \left(\frac{n+1}{2}\right)^n$.

**14.** Na diskriminant se bude hodit např. binomická věta. Pro iracionalitu vhodně zmodul.

**15.** Pokud by tvořily, posuň jeho střed do počátku. Jak by pak musel polynom vypadat?

**16.** Použij Wilsona a oddělej celou část.

**17.** $\left(5+\sqrt{26}\right)^{2024} + \left(\sqrt{26}-5\right)^{2024}$ je celé číslo.

**18.** Natvrdo urči celou část toho čísla. Číslice za desetinnou čárkou vem jak poslední cifry stonásobku.

**19.** Odhadni necelou část každé odmocniny.

**20.** Teleskopuj odhady $2\left(\sqrt{k}-\sqrt{k-1}\right) \geq \frac{1}{\sqrt{k}} \geq 2\left(\sqrt{k+1}-\sqrt{k}\right)$. Trochu to zjemni, aby to vyšlo.

**21.** Indukuj.

**22.** Ukaž, že maximální počet mincí vzhledem k počtu krabiček roste stejně rychle jako $A(n,n)$.

## Literatura a zdroje

[1] Radek Erban: *Velká čísla*, Matematický klub, 2000.

# Hledání extrémů, aneb „Nej-“ případy

Josef „José“ Soural

Abstrakt. Mnoho úloh nám dává za úkol najít „nejmenší/největší možný počet, hodnotu výrazu, délku úsečky, ...“, prostě najít minimum nebo maximum daného problému. Bohužel je právě tento úkol zdrojem jedné z vůbec nejčastějších úvahových chyb v důkazech, která nás pak může stát hodně bodíků (nejen) v soutěžích, jako je MO. V této přednášce si proto ukážeme a procvičíme, jak úlohy na nalezení extrému řešit správně.

**Příklad.** (Motivační)[1] Kolik nejvíce koňů je možné naskládat na klasickou šachovnici $8 \times 8$, aby se vzájemně neohrožovaly?

*Řešení.* (Špatné) Vezmeme osm koňů a dáme je do prvního řádku šachovnice. Pak vyškrtáme políčka, která musí zůstat prázdná, a zjistíme, že jsou to následující dva řádky. Do čtvrtého umístíme dalších osm koňů a zopakujeme postup. Vyjde nám, že na šachovnici můžeme koně umístit do tří celých řádků, a dohromady tedy můžeme umístit dvacet čtyři koňů. Jelikož jsme postupovali nejlepším možným způsobem, abychom na šachovnici dostali co nejvíce koňů, je 24 koňů maximum.

Proč je řešení špatně? Jak uvidíme, dává nesprávnou odpověď. Důležitější ale je, že tvrdí, že nějaký řešitelem vybraný způsob umisťování figurek je „nejlepší možný“. Není to pravda, a i kdyby náhodou byla, musel by to řešitel dokázat, a to pořádně.

*Řešení.* (Stále špatné) Umístíme 8 koňů na jednu z hlavních diagonál. Vyškrtáme políčka, která nějaký kůň ohrožuje. Všimneme si, že diagonály „ob jedna vedle“ zůstaly volné, tak na ně umístíme další koně. Podobným postupem dokážeme umístit koně na všechna políčka každé druhé diagonály, kterých je dohromady 32. To je tedy určitě maximum.

Toto řešení sice (náhodou) našlo správný výsledek, podobně jako předchozí ale jen tak tvrdí, že zrovna uvedený postup je nejlepší taktika na umisťování koňů. Vůbec ale neříká, proč by to měla být pravda. Co kdybychom začali na vedlejší diagonále, nepostavili bychom tam těch koňů náhodou víc? Nebo co kdybychom místo po diagonálách začali umisťovat koně nějak jinak? Zkrátka: postupů na umisťování koňů je nepřeberné množství. Jak tedy můžeme vědět, že neexistuje žádný lepší?

[1] Převzat z povídání k páté sérii sedmadvacátého ročníku. Doporučuji, je to poučné čtení.

### Jak to tedy dělat správně?

*Řešení.* (Správné!) Postavíme jednoho koně na šachovnici. Všimneme si, že ohrožuje jen ta políčka, která mají opačnou barvu než to, na němž stojí. Zamyslíme se nad tím a uvědomíme si, že to neplatí jen pro tohoto koně, ale zcela obecně. Tedy určitě umíme na šachovnici umístit alespoň 32 koňů, protože tolik je polí jedné barvy.

Je 32 ale opravdu maximum? Rozdělme si šachovnici na osm obdélníků $2 \times 4$. Kdyby na šachovnici mohlo být koňů víc, muselo by podle Dirichletova principu v některém z nich být aspoň pět koňů. Jenže každý z koňů v tomto obdélníku na jednom poli stojí a jedno ohrožuje, pět koňů (a tím spíš ne více) se tam tedy nevejde.

Tím jsme dokázali, že víc než 32 koňů na šachovnici být nemůže a že 32 jich tam umíme postavit, je to tedy skutečně maximum.

Výše uvedená špatná řešení jsou možná trochu přehnaná, ale je to opravdu častá úvahová chyba, byť ne vždy takto jasně viditelná.

Obecně se tedy důkaz, že je něco maximum (minimum) skládá ze dvou částí:

(1) Nalezneme nějakého kandidáta na extrém (resp. nějaký příklad, kdy dané hodnoty skutečně dosáhneme) a ukážeme, že splňuje podmínky ze zadání (je to validní řešení).
(2) Dokážeme, že nic většího (menšího) dané podmínky nesplňuje. Někdy to lze jedním argumentem jako výše, někdy musíme jednotlivě rozebrat a vyvrátit více možností.

A nebo klidně totéž v opačném pořadí. Kamenem úrazu je pak právě bod (2), na který se častokrát buď zcela zapomene, nebo se neprovede dostatečně důsledně. Ale nyní už hurá na příklady!

### Něco poučného na začátek

**Úloha 1.** Hokejového turnaje se zúčastnila čtyři družstva, každé hrálo s každým jiným právě jeden zápas. V každém zápase padl (nenulový) počet branek, který dělí celkový počet gólů v turnaji. Kolik nejméně mohlo celkem v turnaji padnout branek, jestliže v žádných dvou zápasech nepadl stejný počet branek? (MO 55–C–I–1)

Zde je dobré si rozmyslet, co se v předchozím příkladě stalo. Typicky mají úlohy na hledání extrému příliš mnoho řešení na to, abychom mezi nimi extrém našli prostým postupných zkoušením jednotlivých možností. V motivačním příkladě na začátku jsme po nalezení kandidáta na extrém (32 koňů) nalezli chytrý náhled na problém, jakousi „omezující podmínku“, která nám tohoto kandidáta bez další práce potvrdila.

V tomto příkladě jsme ovšem viděli, že někdy nám omezující podmínka nevydá extrém rovnou, ale jen omezí množství „přípustných kandidátů“ na počet, ze kterého již extrém dokážeme najít postupným vyzkoušením, rozebráním a eliminováním

jednotlivých možností. V krajních případech (když je již zpočátku možností malý počet) se dokonce může stát, že žádnou omezující podmínku ani nenajdeme a extrém musíme hledat takto „natvrdo“ a jednotlivé kandidáty vyřadit každého zvlášť.

**Úloha 2.** Nalezněte kladná reálná čísla $a$, $b$, $c$ taková, aby jejich součet byl 100 a jejich součin byl co největší. (PraSe 7–5–1)

**Úloha 3.** Nalezněte *přirozená* $a$, $b$, $c$ taková, aby jejich součet byl 100 a jejich součin byl co největší. (PraSe 7–5–1)

Menší spoiler k právě uvedeným úlohám: důkaz extrému sporem nebo využitím nějaké nerovnosti (se znalostí kdy nastává rovnost), je dosti častý. Ale dost bylo keců, teď už jsme připraveni nějaké ty úložky pokořit!

### Na zahřátí

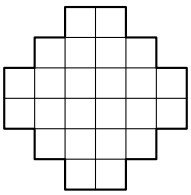
**Úloha 4.** Máme trojúhelník s čísly od jedné do šesti (každé právě jednou) napsanými u jeho vrcholů a středů stran. Když pro každou stranu sečteme tři čísla na ní napsaná, největší součet vyjde patnáct. Když po dvou sečteme čísla napsaná uprostřed stran, nejmenší součet bude čtyři. Jaký nejvyšší může být součet čísel napsaných u vrcholů? (PraSe 33–4p–1)

**Úloha 5.** Kolik nejvíce čísel můžeme vybrat z množiny $\{1, 2, \ldots, 99\}$ tak, aby součet žádných dvou z nich nebyl dělitelný jedenácti? (MO 58–C–I–5)

**Úloha 6.** Mějme šachovnici $2n \times 2n$, které někdo vylomil dvě protilehlá rohová políčka. Kolik nejvíce dominových kostek $1 \times 2$ na ni můžeme naskládat?

**Úloha 7.** Máme čísla od 1 do 2024 a chceme je uspořádat na kružnici tak, aby součet všech absolutních hodnot rozdílů sousedních čísel byl co nejmenší. Jak to máme udělat a jaké bude toto minimum? (PraSe 33–4p–2, upraveno)

**Úloha 8.** Mějme útvar složený z šesti řad čtverečků pod sebou o počtech dva, čtyři, šest, šest, čtyři a dva čtverečky, který je navíc osově souměrný podle svislé i vodorovné osy (viz obrázek). Kolik nejvíce čtverečků můžeme obarvit, aby v žádné šikmé řadě nebyly tři obarvené čtverečky vedle sebe? (MO 49–C–II–3, upraveno)



**Úloha 9.** Jaký nejvyšší počet podmnožin množiny $\{1, 2, \ldots, n\}$ můžeme vybrat, aby žádné dvě z nich neměly společné více než dva prvky?

### Zajímavější úložky

**Úloha 10.** Určete, jaký nejvyšší může být součet reálných čísel $x$, $y$, pro která platí $x^2 + 2xy + 4y^2 = 1$. (PraSe 21–1–2)

**Úloha 11.** Na čtverečkovaném papíře $5 \times 5$ hrajeme lodě, přičemž náš soupeř má právě jednu loď. Ta je tvaru tetromina $L$, tedy řady tří čtverečků, která má na některém konci nalepený jeden čtvereček do boku. Kolik nejméně polí musíme střelit, abychom měli jistotu, že loď zasáhneme (nehledě na její umístění, resp. otočení a překlopení)? (MO 58–B–II–2)

**Úloha 12.** Mějme pravoúhlý trojúhelník $ABC$ s pravým úhlem u vrcholu $C$. Pro jakou polohu bodu $P$ umístěného na jeho obvodu bude součet $|PA| + |PB| + |PC|$ nejmenší? (PraSe 27–5–3)

**Úloha 13.** Nalezněte reálná čísla $p$, $q$ tak, aby rovnice $x^2 + px + q + 1 = 0$ měla reálné řešení a součet $p^2 + q^2$ byl nejmenší možný. (PraSe 21–1–4)

### Něco těžšího na závěr

**Úloha 14.** Nalezněte nejmenší přirozené číslo $k$ takové, že každá $k$-prvková množina trojciferných po dvou nesoudělných čísel obsahuje alespoň jedno prvočíslo. (MO 56–B–I–3)

**Úloha 15.** Nalezněte reálné číslo $p$ takové, aby rovnice $x^2+4px+5p^2+6p-16 = 0$ měla dva různé reálné kořeny $x_1$, $x_2$ a aby součet $x_1^2 + x_2^2$ byl co nejmenší. (MO 51–B–I–1)

**Úloha 16.** Mějme ostroúhlý trojúhelník $ABC$. Pro libovolný bod $L$ jeho strany $AB$ označme $K$, $M$ paty kolmic z bodu $L$ na strany $AC$, $BC$. Pro kterou polohu bodu $L$ je úsečka $KM$ nejkratší? (MO 56–B–II–4)

**Úloha 17.** Pro $V(a,b,c) = a+b+c+4(1-a)(1-b)(1-c)+3abc$ a $a$, $b$, $c \in \langle 0,1\rangle$ dokažte nerovnost

$$1 \le V(a,b,c) \le 6.$$

(PraSe, seriál k 29. ročníku)

### Návody

**1.** Rozmysli si teoreticky nejmenší možný počet branek a pak vzestupně eliminuj ty počty, které nesplňují zbylé podmínky zadání.

**2.** Použij AG nerovnost.

**3.** Postupuj sporem.

**4.** Jakými způsoby lze rozložit na součet čísla 4 a 15?

**5.** Které zbytkové třídy $\pmod{11}$ se ti nesmí potkat?

**6.** Obě vylomená políčka mají stejnou barvu.

**7.** Použij jedno znění trojúhelníkové nerovnosti, konkrétně že pro všechna $a$, $b$, $c$ reálná platí $|a-b| \leq |a-c| + |c-b|$.

**8.** Všimni si, že útvar lze rozdělit na několik *disjunktních* šikmých řádků délky 3.

**9.** Sporem dokaž, že „nejvýhodnější“ je zahrnout všechny podmnožiny o třech a méně prvcích.

**10.** Přepiš do tvaru $(x+y)^2 = 1 - 3y^2$.

**11.** Herní pole si rozděl na čtyři obdélníky $2 \times 3$ (resp. $3 \times 2$) a jedno políčko uprostřed. Kolik políček musíš nejméně střelit v každém z těchto obdélníků?

**12.** Dva ze sčítanců se vždy sečtou na délku jedné ze stran, třetí je minimální, když $P$ je pata výšky. Kterou patu hledáme dokaž sporem.

**13.** Z diskriminantu dostaneme $p^2 \geq 4q + 4$. Pozor, že musíme zvlášť rozebrat případy, kdy (v závislosti na $q$) může a nemůže nastat rovnost.

**14.** Využij toho, že mocniny dvou různých prvočísel jsou nesoudělné.

**15.** Použij Viètovy vztahy.

**16.** Thaletova kružnice nad $CL$ a věta o obvodovém a středovém úhlu tě dovedou ke $|KM| = |CL| \cdot \sin\gamma$.

**17.** Všimni si, že výraz je lineární v každé proměnné. Kvůli tomu může svých extrémů nabývat jenom pro krajní hodnoty všech proměnných.

### Literatura a zdroje

Tento příspěvek je založen na příspěvku od *Báry Kociánové* z roku 2017, který jsem pouze trochu doplnil a zmodernizoval. Za jeho předlohu tímto Báře děkuji.

[1] Bára Kociánová: *Hledání extrémů*, Zásada, 2017.
[2] Úlohy pocházejí z uvedených ročníků matematické olympiády a MKS.

# Antirovnoběžnost a izogonály

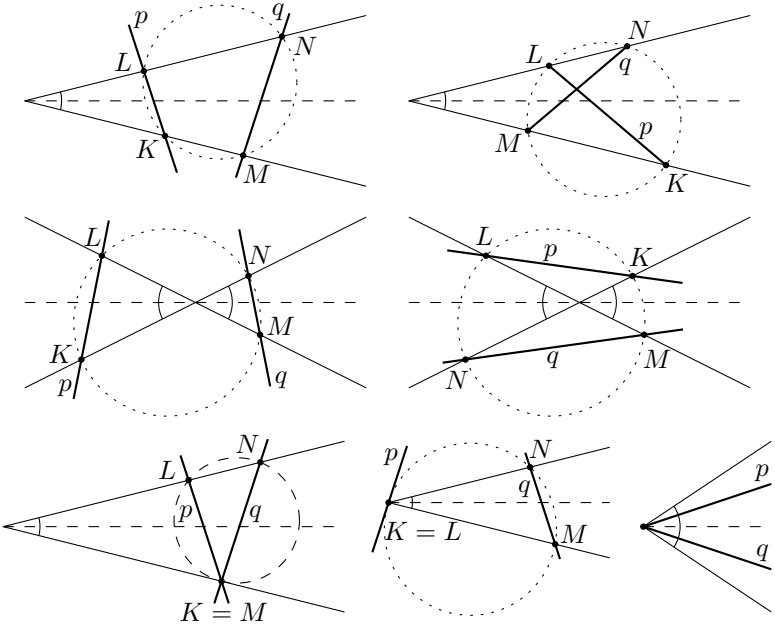
Jolča Štraitová

Abstrakt. Příspěvek se zabývá geometrickým principem antirovnoběžnosti a s ním souvisejících pojmů jako izogonály, isogonal conjugates (*kamarádi*) a symediány a především jejich využitím při řešení úloh. Znalost těchto pojmů a vztahů mezi nimi často nabízí možnost alternativního řešení úloh řešitelných i se základními znalostmi o úhlech.

## Antirovnoběžnost

**Definice.** Je dán úhel $XVY$ a jeho osa $o$. Přímky $p$ a $q$ nazveme *antirovnoběžné* v úhlu XVY, pokud pro osový obraz $p'$ přímky $p$ podle $o$ platí $p' \parallel q$.

**Tvrzení.** *Přímky $p$ a $q$ jsou antirovnoběžné v daném úhlu, právě když nastane jedna ze situací zachycených na následujících obrázcích.*



**Tvrzení.** (Antirovnoběžkové lemma) *Nechť je dán trojúhelník $ABC$ s kružnicí opsanou $\omega$. Dále předpokládejme, že přímka $p$ protne $\omega$ v bodech $P$ a $Q$. Potom jsou přímky $BC$ a $p$ antirovnoběžné v úhlu $BAC$ právě tehdy, když platí $|AP| = |AQ|$.*

**Úloha 1.** Na kružnici $k$ je dána tětiva $AB$. Označme $S$ střed kratšího oblouku $AB$. Bodem $S$ vedeme dvě různé přímky, které protnou $AB$ a $k$ ve čtyřech dalších bodech. Ukažte, že tyto čtyři body leží na kružnici.

**Úloha 2.** Nechť $ABCD$ je lichoběžník s $AB \parallel CD$. Kružnice opsaná trojúhelníku $BCD$ protne přímku $DA$ v bodě $E$ různém od $D$. Ukažte, že $CB$ je tečna ke kružnici opsané trojúhelníku $ABE$.

**Úloha 3.** Jsou dány kružnice $k$, $l$, které se protínají v bodech $A$, $B$. Označme $K$, $L$ po řadě body dotyku jejich společné tečny zvolené tak, že bod $B$ je vnitřním bodem trojúhelníku $AKL$. Na kružnicích $k$ a $l$ zvolme po řadě body $N$ a $M$ tak, aby bod $A$ byl vnitřním bodem úsečky $MN$. Dokažte, že čtyřúhelník $KLMN$ je tětivový právě tehdy, když přímka $MN$ je tečnou kružnice opsané trojúhelníku $AKL$.

**Úloha 4.** Nechť je $ABCD$ lichoběžník se základnami $AD$ a $BC$. Označme $O$ průsečík jeho úhlopříček a $o$ osu $\sphericalangle BOC$. Dále označme $B_1, C_1$ obrazy bodů $B$, $C$ v osové souměrnosti podle $o$. Dokažte, že úhly $BDB_1$ a $CAC_1$ jsou stejně velké.

### Izogonály a kamarádi

**Definice.** Je dán úhel $XVY$ a jeho osa $o$. Pak pokud jsou přímky $p$ a $q$ antirovnoběžné v úhlu $XVY$ a zároveň $V \in p$ a $V \in q$, potom tyto přímky nazýváme *izogonály* (jsou *izogonální* v úhlu $XVY$).

**Definice.** Nechť bod $P$ leží v rovině trojúhelníku $ABC$. Přímky $AP$, $BP$ a $CP$ zobrazíme podle os úhlů $CAB$, $ABC$ a $BCA$. Pokud se tyto tři přímky protínají v jednom bodě $Q$, pak tento bod nazveme *isogonal conjugate* bodu $P$ vzhledem k trojúhelníku $ABC$; neformálně mu budeme říkat *kamarád* bodu $P$ vzhledem k trojúhelníku $ABC$.

**Poznámka.** Co se kamarádů týče, nebudeme se zde věnovat bodům ležícím na kružnici opsané trojúhelníku a bodům ležících na přímkách, na kterých leží strany trojúhelníku.

**Tvrzení.** (Alternativní definice kamaráda) *Kamarád bodu $P$ je středem kružnice opsané trojúhelníku s vrcholy v osových obrazech $P$ podle stran trojúhelníku $ABC$.*

**Tvrzení.** *Každý bod má vzhledem k trojúhelníku $ABC$ kamaráda.*

**Tvrzení.** (Six feet theorem) *Nechť $P$ a $Q$ jsou kamarádi vzhledem k $\triangle ABC$. Nechť $P_a$ je projekce bodu $P$ na $BC$. Analogicky definujme $P_b$, $P_c$, $Q_a$, $Q_b$ a $Q_c$. Pak $P_a$, $P_b$, $P_c$, $Q_a$, $Q_b$ a $Q_c$ leží na jedné kružnici, jejíž střed splývá se středem $PQ$.*

**Úloha 5.** Najděte všechny body, které jsou svými vlastními kamarády.

**Úloha 6.** Ukažte, že kamarád kamaráda je původní bod.

### Kamarádi $H$ a $O$

**Tvrzení.** *V trojúhelníku $ABC$ jsou $H$ a $O$ postupně ortocentrum a střed kružnice opsané trojúhelníku $ABC$. Potom $AO$ a $AH$ jsou izogonální v úhlu $BAC$, neboli $O$ a $H$ jsou kamarádi vzhledem k trojúhelníku $ABC$.*

**Úloha 7.** V trojúhelníku $ABC$ platí, že výška a těžnice z vrcholu $A$ rozdělí úhel $BAC$ na třetiny. Určete vnitřní úhly v trojúhelníku $ABC$.

**Úloha 8.** V $\triangle ABC$ s ortocentrem $H$ osa úsečky $BH$ protíná strany $AB$ a $BC$ v bodech $D$ a $E$. Ukažte, že $|\sphericalangle BOD| = |\sphericalangle BOE|$.

### Symediány

**Definice.** Je dán trojúhelník $ABC$. Přímku, která je izogonální s těžnicí z vrcholu $A$ v úhlu $BAC$, nazveme *$A$-symediánou* trojúhelníku $ABC$.

**Tvrzení.** *Ke kružnici opsané trojúhelníku $ABC$ sestrojíme tečny v bodech $B$ a $C$ a jejich průsečík označíme $M$. Pak $AM$ je $A$-symediána v trojúhelníku $ABC$.*

**Tvrzení.** *Symediány se protínají v jednom bodě.*

**Úloha 9.** V konvexním čtyřúhelníku $ABCD$, kde označíme $M$ střed $AC$, platí $|\sphericalangle BMC| = |\sphericalangle CMD| = |\sphericalangle BAD|$. Dokažte, že $ABCD$ je tětivový.

**Úloha 10.** Je dán trojúhelník $ABC$ s kružnicí opsanou $\omega$, ve kterém platí $|AC| = 2 \cdot |AB|$. Tečny k $\omega$ v bodech $A$ a $C$ se protínají v bodě $P$. Dokažte, že průsečík přímky $BP$ a osy strany $BC$ leží na $\omega$.

**Úloha 11.** Nechť je $ABC$ rovnoramenný trojúhelník se základnou $BC$. Bod $P$ leží uvnitř trojúhelníka $ABC$ tak, že $|\sphericalangle CBP| = |\sphericalangle ACP|$. Nechť $M$ je střed $BC$. Dokažte, že $|\sphericalangle BPM| + |\sphericalangle CPA| = 180°$.

### Další úlohy

**Úloha 12.** Elipsa s ohnisky $P$ a $Q$ se dotýká stran $\triangle ABC$. Ukažte, že $P$ a $Q$ jsou kamarádi.

**Úloha 13.** Je dán úhel o velikosti $\alpha$ s hlavním vrcholem $A$ sevřený mezi polopřímkami $u_1$ a $u_2$ vycházejícími z $A$. Uvnitř úhlu $u_1u_2$ je dán bod $B$ neležící na jeho ose a je dána velikost úhlu $\beta$, kde $\alpha < \beta < 180°$. Uvažme všechny možné dvojice bodů $X$, $Y$ takové, že $X \in u_1$, $Y \in u_2$, $A$ leží mimo úhel $XBY$ a $\sphericalangle XBY = \beta$. Pak každý z bodů $A$, $B$ má tu vlastnost, že vidí úsečku $XY$ stále pod stejným úhlem. Ukažte, že existuje třetí bod s touto vlastností.

**Úloha 14.** V konvexním čtyřúhelníku $ABCD$ platí, že přímka $BD$ nepůlí ani úhel $\sphericalangle ABC$, ani $\sphericalangle CDA$. Bod $P$ ležící uvnitř $ABCD$ splňuje $|\sphericalangle PBC| = |\sphericalangle DBA|$ a $|\sphericalangle PDC| = |\sphericalangle BDA|$. Ukažte, že $ABCD$ je tětivový právě tehdy, když $|AP| = |CP|$.

### Návody

**1.** Použij Antirovnoběžkové lemma.

**2.** Rozmysli si pomocí Tvrzení 2, jak využít antirovnoběžky k důkazu toho, že je přímka tečnou.

**3.** Přímky antirovnoběžné ke stejné přímce v tomtéž úhlu jsou rovnoběžné.

**4.** Použij definici antirovnoběžnosti.

**5.** Jsou čtyři.

**6.** Použij originální definici kamaráda.

**7.** Střed kružnice opsané leží na těžnici.

**8.** Překlop $O$ a $H$ podle stran trojúhelníku.

**9.** Přidej si do náčrtku střed kružnice opsané trojúhelníku $ABD$.

**10.** Úhel, který svírá těžnice z bodu $B$ se stranou $BC$, je z izogonality stejný jako úhel, který svírá $B$-symediána se stranou $AB$.

**11.** Označme průnik přímky $AP$ se stranou $BC$ jako $X$. Pak chceš ukázat, že $|\sphericalangle BPM| = |\sphericalangle XPC|$. Úsečka $PM$ je těžnicí trojúhelníku $BPC$.

**12.** Elipsa je množina bodů s nějakou vlastností. Jakou?

**13.** Ten bod je kamarád k $B$ vzhledem k (libovolnému) trojúhelníku $XAY$. Pro důkaz toho, že je to pro všechny ten samý bod, použij definici kamaráda jako střed kružnice opsané obrazům přes strany.

**14.** Body $A$ a $C$ jsou kamarádi vzhledem k $\triangle BPD$.

### Literatura a zdroje


[1] Martin Raška: *Izogonály a kamarádi*, Lipová-lázně, 2022.
[2] Michal "Kenny" Rolínek: *Antirovnoběžnost*, Oldřichov, 2012.
[3] Michal Pecho: *Antirovnobežnosť a izogonály.*
[4] Radoslaw Zak: *Isogonal conjugate and a few properties of the point* $X_{25}$.
[5] Tran Quang Hung, Pham Huy Hoang: *Generalization of a Problem with Isogonal Conjugate Points.*

# Konvexní kombinatorická geometrie

Adéla Karolína Žáčková

Abstrakt. Pracovat s rovinou je strašná nuda. Jakože děsná nuda. V přednášce se podíváme na zoubek úlohám i ve vyšších dimenzích a zjistíme, že i když si je vysloveně neumíme představit, pracovat s nimi není tak obtížné. Zaměříme se na konvexní kombinatorickou geometrii, která se mnohdy vyskytuje v olympiádách. Bude to krásné a bude toho dost!

Kombinatorická geometrie je velice rozsáhlé odvětví, u kterého tak trochu platí, že každý příklad potřebuje svůj vlastní nápad. Proto se také mnohdy vyskytuje v olympiádách. Lze na ni využívat spoustu různých přístupů – spojitost, extremální princip, triangulaci, invarianty atd. atp. Hodně užitečnou bývá typicky téměř ve všech kombinatorických úlohách i indukce.

My se ale podíváme na jiné, trošku vysokoškolské odvětví, budeme si hrát hlavně s množinami bodů a podíváme se, co všechno v sobě mohou skrývat za taje.

Vzhůru do bitvy!

### Na rozehřátí

**Úloha 1.** Dokažte, že každý mnohoúhelník obsahuje alespoň jednu svoji diagonálu.

**Úloha 2.** Hokejista se připravuje na novou sezónu. Má tři puky a pokaždé jeden z nich odpálí tak, že proletí mezi zbylými dvěma. Může hokejista 2025. odpalem vrátit puky do původní pozice?

**Úloha 3.** Uvnitř $2n$-úhelníku se nachází Křivej Jack. Ze všech vrcholů najednou po něm vystřelíme. Žádná střela nezasáhla vrchol. Dokažte, že některá strana musela být zasažena dvakrát.

**Úloha 4.** Mějme konvexní $n$-úhelník ($n > 3$) a pro bod uvnitř něho uvažme jeho kolmé projekce na strany mnohoúhelníku (jakožto přímky). Dokažte, že alespoň jedna z projekcí leží uvnitř příslušné strany (jakožto úsečky).

### Ohmatejme si pojmy

**Definice.** (Obecná poloha) O množině bodů říkáme, že je v *obecné poloze*, pakliže žádné tři její body neleží v přímce.

V přednášce často budeme používat termín uzavřený poloprostor. V $\mathbb{R}^1$ tím myslíme polopřímku včetně hraničního bodu, v $\mathbb{R}^2$ je uzavřený poloprostor polorovina včetně hraniční přímky, v $\mathbb{R}^3$ je to rovina a všechno v jednom směru od ní atd. Pořádná definice je následující:

**Definice.** (Uzavřený poloprostor) Mějme nenulový vektor $a = (a_1, a_2, \ldots, a_d) \in \mathbb{R}^d$ a reálné číslo $b$. Pak množina bodů $x = (x_1, x_2, \ldots, x_d)$ splňujících $\sum_{i=1}^{d} a_i x_i \geq b$ je *uzavřený poloprostor*.

Pojďme si nejprve nějak intuitivně říct, co je to konvexita, než se ponoříme do té pořádné, formální definice. Všichni asi víte, že množina je konvexní právě tehdy, když vezmeme-li dva její body a úsečku mezi nimi, tak všechny body na takové úsečce stále leží v dané množině.

**Definice.** (Konvexní množina) Množina bodů $\mathcal{C} \subseteq \mathbb{R}^d$ je *konvexní*, pokud pro každé dva body $x, y \in \mathcal{C}$ a každé $t \in \langle 0, 1 \rangle$ leží $tx + (1-t)y$ v $\mathcal{C}$.

**Úloha 5.** Najděte příklad množiny $M \subseteq \mathbb{R}^2$, která je sjednocením dvou konvexních množin a jejíž doplněk se skládá z 5 navzájem oddělených oblastí (komponent souvislosti).

**Cvičení 6.** Zkuste si rozmyslet, že formální definice opravdu říká totéž.

Co by potom byl konvexní obal nějaké množiny? Intuitivně nějaká taková množina, která tu naši bude těsně obalovat (tedy bude nejmenší obsahující naše body) a zároveň bude konvexní. Můžeme si to představit tak, že okolo naší množiny umístíme gumičku a necháme ji se smrsknout. Gumička nám určitě zajistí, že to, co obklíčí, bude konvexní, zároveň, kdyby mohla být menší, tak by se gumička smrskla více. Jak si ale pořádně formalizovat toto obalování gumičky?

**Definice.** *Konvexní obal* množiny $C \subseteq \mathbb{R}^d$ ($\mathrm{conv}(C)$) je průnik všech konvexních nadmnožin $\mathcal{C}$.

**Definice.** *Konvexní kombinace* bodů $x_1, x_2, \ldots, x_n$ z množiny $C \subseteq \mathbb{R}^d$ je bod (vektor) tvaru $\sum \alpha_i x_i$, kde $\alpha_i \geq 0$ a $\sum \alpha_i = 1$.

**Cvičení 7.** Rozmyslete si, co vlastně konvexní kombinace znamená.

**Tvrzení.** *Konvexní obal množiny $C \subseteq \mathbb{R}^d$ tvoří všechny konvexní kombinace bodů z $C$.*

**Cvičení 8.** Existuje konvexní množina bodů taková, že když z ní odebereme libovolný bod, přestane být konvexní?

**Cvičení 9.** Dokaž, že průnik libovolného počtu konvexních množin je konvexní.

**Věta.** (Carathéodory) *Mějme množinu $X \subseteq \mathbb{R}^d$. Pak každý bod z $\mathrm{conv}(X)$ se dá vyjádřit jako konvexní kombinace maximálně $d+1$ bodů z $X$.*

**Věta.** (O oddělování) *Mějme konvexní neprázdné množiny $C, D \subseteq \mathbb{R}^d$, kde $C \cap D = \emptyset$. Pak je lze (neostře) oddělit nadrovinou.*

**Cvičení 10.** Rozmyslete si, jak musí množiny vypadat, aby šly oddělit ostře.

**Lemma.** (Radon) *Mějme množinu $A$ $d+2$ bodů v $\mathbb{R}^d$. Pak existují dvě disjunktní podmnožiny $A_1, A_2 \subset A$ takové, že $\mathrm{conv}(A_1) \cap \mathrm{conv}(A_2) \neq \emptyset$.*

**Poznámka.** Bodu v průniku těchto dvou podmnožin se říká *Radonův bod*.

**Cvičení 11.** V prostoru leží alespoň pět bodů. Dokažte, že je lze obarvit dvěma barvami tak, aby žádná rovina neoddělila ostře jednu barvu od druhé.

**Věta.** (Helly) *Mějme konvexní množiny $C_1, C_2, \ldots, C_n \subseteq \mathbb{R}^d$, $n \geq d+1$. Nechť je průnik každé $d+1$-tice těchto množin neprázdný. Pak je průnik všech $n$ množin neprázdný.*

**Cvičení 12.** Rozmyslete si, že $d$-tice nestačí.

**Cvičení 13.** Najděte nekonvexní množiny, pro které věta neplatí.

**Věta.** (Nekonečný Helly) *Pokud se každých $d+1$ z libovolně mnoha konvexních uzavřených a omezených podmnožin $\mathbb{R}^d$ protíná, protínají se všechny.*

### Začínáme

**Úloha 14.** Řekneme, že konečná množina bodů v rovině je *pospolitá*, pokud pro každé tři její body existuje jednotkový kruh, který tyto body obsahuje. Dokaž, že každou pospolitou množinu lze pokrýt jednotkovým kruhem. (PraSe 40–4j–4b)

**Úloha 15.** Čtvercový dort o rozměrech $6 \times 6$ chceme shora pokrýt kousky čokolády $2 \times 1$. Ukažte, že ať plochu vyplníme jakkoli, vždy můžeme dort rozkrojit, aniž bychom krájeli dvojdílek čokolády.

**Úloha 16.** Jane nakreslila na papír křivku a všimla si, že vzdálenost libovolných dvou jejích bodů je nejvýše 1. Dokaž, že Jane může namalovat čtverec o straně 1, který zakryje celou křivku.

**Úloha 17.** Lze prostor obarvit pěti barvami (každá musí být použita) tak, aby každá rovina byla nejvýše trojbarevná?

**Úloha 18.** Nechť $M$ je konečná množina alespoň čtyř bodů v rovině, z nichž některé jsou červené a zbylé modré. Navíc platí, že pro libovolnou čtveřici $V$ bodů z $M$ existuje přímka, která ostře odděluje červené body z $V$ od modrých bodů z $V$. Dokažte, že pak existuje přímka ostře oddělující všechny červené body z $M$ od všech modrých bodů z $M$.

**Úloha 19.** V rovině leží několik mnohoúhelníků, z nichž každé dva se protínají. Dokažte, že existuje přímka, která je všechny protíná.

**Úloha 20.** Je dán bod $A$ a několik mnohoúhelníků v rovině takových, že každé dva mají neprázdný průnik. Dokažte, že existuje kružnice se středem v $A$, která protíná všechny tyto mnohoúhelníky nebo se jich alespoň dotýká.

**Úloha 21.** Nechť A je množina bodů v rovině taková, že každé dva body mají vzdálenost nejvýše 1. Dokažte, že pak existuje kruh o poloměru $\frac{\sqrt{3}}{3}$ takový, že $A$ leží v tomto kruhu.

**Úloha 22.** Řekneme, že soubor $C = \{C_1, \ldots, C_n\}$ konvexních množin v rovině má $(p, q)$-*vlastnost*, pokud $n \geq p$ a z každé $p$-tice z $C$ lze vybrat $q$ množin s neprázdným průnikem. Nazvěme *špendlíkovostí* $s(C)$ souboru množin $C$ velikost nejmenší množiny bodů $X \subset \mathbb{R}^2$ takové, že každé $C_i \in C$ obsahuje alespoň jeden bod z $X$.

Dokažte, že je-li $C$ konečný soubor osových obdélníků (tj. uzavřených obdélníků s hranami rovnoběžnými s osami) s $(2, 2)$-vlastností, pak $s(C) = 1$.

**Úloha 23.** Dokažte, že pokud je $C$ konečný soubor osových obdélníků se $(4, 3)$-vlastností, pak $s(C) \leq 2$.

**Úloha 24.** Mějme $n$ bodů v rovině, $n \geq 3$, přičemž žádné tři z nich neleží v přímce. Uvažujme vnitřní úhly všech trojúhelníků s vrcholy v daných bodech a velikost nejmenšího takového úhlu označme $\varphi$. Pro dané $n$ najděte největší možné $\varphi$.

(MO A–64–II–4)

### Přitahuje

**Úloha 25.** Buď $I$ konečná množina rovnoběžných úseček v rovině. Nechť ke každý třem úsečkám z $I$ existuje přímka protínající všechny tři. Ukažte, že existuje přímka protínající všechny úsečky z $I$.

**Úloha 26.** V rovině je dáno $n \geq 3$ bodů. Zabodněte do roviny $2n - 5$ špendlíků tak, aby propíchly vnitřek každého trojúhelníku s vrcholy v daných bodech.

**Úloha 27.** Každé tři body z konečné podmnožiny roviny jdou pokrýt páskem šířky 1. Dokažte, že lze pokrýt celou množinu páskem šířky 2.

**Úloha 28.** Nechť $C_1, C_2, \ldots, C_n$, $n \geq 3$, je soubor konvexních množin v rovině a $K$ je úsečka $\langle 0, 1\rangle \times \{0\}$. Ukažte, že pokud průnik každé trojice množin obsahuje posunutou kopii $K$, pak průnik všech obsahuje také posunutou kopii $K$.

**Úloha 29.** Na vesmírné ploše se pase konečně mnoho krav, každá kráva je buď černá, nebo bílá. Krávy se nehýbou. Nechť v každé skupině čtyř krav lze rovným plotem oddělit černé od bílých. Ukažte, že v celém stádu lze rovným plotem oddělit černé od bílých.

**Úloha 30.** V lese nejtemnějším z nejtemnějších rostou tenké stromy, z nichž každý je nižší než 1012 metrů. Žádné dva stromy od sebe nejsou dál, než kolik činí rozdíl jejich výšek. Dokažte, že celý temný les bude příští rok možné obehnat zdí dlouhou 2025 metrů. (upravené MKS 26–1–7)

**Úloha 31.** Je dán mnohoúhelník o obsahu $n$. Dokažte, že je možné jej vložit do roviny tak, aby pokrýval (hranice se počítá) alespoň $n + 1$ mřížových bodů.

**Úloha 32.** V rovině jsou dány body $P, A_1, A_2, \ldots, A_{2024}$ v obecné poloze. Dokažte, že počet všech trojúhelníků $A_iA_jA_k$, uvnitř kterých leží bod $P$, je sudý.

**Úloha 33.** Máme dvě kružnice s obvodem 1000. Na jedné z nich je vyznačeno 1000 bodů a na druhé několik oblouků o celkovém součtu nejvýše 1. Dokažte, že na sebe můžeme obě kružnice položit tak, aby všechny vyznačené body ležely mimo vnitřky vyznačených oblouků.

**Úloha 34.** Máme v rovině 100 bodů v obecné poloze. Dokažte, že mezi všemi trojúhelníky tvořenými těmito body není více než 70 % ostroúhlých.

(IMO 1970)

**Úloha 35.** Nakreslíme do roviny trojúhelník $RGB$. Rozdělíme jej na několik menších trojúhelníčků tak, aby žádný trojúhelníček neměl vrchol uvnitř strany jiného trojúhelníčku. Nyní obarvíme vrcholy trojúhelníčků červeně, zeleně a modře tak, aby vrcholy velkého trojúhelníku dostaly příslušné barvy. Dále vrcholy na stranách musí dostat barvu jednoho z přilehlých vrcholů velkého trojúhelníka. Dokažte, že má pak jeden z malých trojúhelníčků všechny vrcholy různě barevné.

(Sylvester problem)

**Úloha 36.** Půdorys galerie má tvar $n$-úhelníku. Kolik strážníků (v závislosti na $n$) potřebujeme, abychom je mohli rozestavit tak, že dohromady uvidí na celou galerii? Strážník vidí všemi směry.

## Z IMO

**Úloha 37.** Rozmístění 4027 bodů v rovině nazveme kolumbijským, jestliže je z nich 2013 červených, 2014 modrých a žádné tři neleží v přímce. O skupině přímek v rovině řekneme, že je dobrá pro dané rozmístění, jestliže:

(1) žádná z přímek neprochází žádným bodem rozmístění,
(2) žádná z částí, na které je rovina přímkami rozdělena, neobsahuje body různých barev.

Najděte nejmenší $k$ takové, že pro libovolné kolumbijské rozmístění 4027 bodů v rovině v ní existuje skupina $k$ dobrých přímek. (IMO 2013-2)

**Úloha 38.** Každé straně $b$ konvexního mnohoúhelníku $P$ přiřadíme maximální obsah trojúhelníku, který celý leží v $P$ a jehož jedna strana je $b$. Dokažte, že součet obsahů přiřazených všem stranám mnohoúhelníku $P$ je větší nebo roven dvojnásobku obsahu mnohoúhelníku $P$. (IMO 2006-6)

**Úloha 39.** Nechť $S$ je čtverec se stranami délky 100 a $L$ je lomená čára uvnitř $S$, která se neprotíná (ani nedotýká). Předpokládejme, že pro každý bod $P$ na hranici $S$ je možné nalézt bod na $L$, který není od $P$ dál než $\frac{1}{2}$. Dokažte, že je možné na $L$ najít dva body $X, Y$ takové, že $|XY| \leq 1$, ale délka $L$ mezi $X$ a $Y$ je alespoň 198. (IMO 1982-6)

**Úloha 40.** Na nekonečné tabuli leží list papíru (vypadá jako tento ...). Mechanička Cassie si tajně zvolí konvexní 2024-úhelník $P$, který celý leží na listu papíru. Kapitán Callahan chce najít všechny vrcholy $P$. Callahan může v jednom kroku nakreslit na tabuli přímku $g$, která neprochází listem papíru. Poté mu Cassie vrátí přímku $h$ rovnoběžnou s $g$ takovou, která je ze všech rovnoběžných přímek procházejících alespoň jedním vrcholem $P$ nejblíže ke $g$. Dokažte, že existuje kladné celé číslo $n$ takové, že Callahan umí vždy určit všechny vrcholy $P$ v nanejvýš $n$ krocích.
(MEMO 2024–I2)

### Máte hlad? Dáme si sendvič!

**Definice.** Mějme $n$-bodovou množinu $X \subseteq \mathbb{R}^d$. Pak bod $x \in \mathbb{R}^d$ se nazývá *středobod*[1] množiny $X$, pokud každý uzavřený poloprostor obsahující $x$ obsahuje alespoň $\frac{n}{d+1}$ bodů z $X$.

**Definice.** Pokud v definici výše nahradíme koeficient $\frac{1}{d+1}$ obecnou $\alpha$, říká se bodu *$\alpha$-středobod*.

**Cvičení 41.** Jak vypadají množiny bodů, pro které existuje 1-středobod?

**Cvičení 42.** Nechť $X$ je konečná neprázdná množina bodů v rovině. Jak vypadá množina jejích $\frac{1}{|X|}$-středobodů?

**Věta.** (O středobodu (Centerpoint theorem)) *Každá konečná množina bodů v $\mathbb{R}^d$ má alespoň jeden středobod.*

**Věta.** (O sendviči) *Řekněme, že nadrovina $h$ půlí konečnou množinu $A$, pokud každý z otevřených poloprostorů definovaných $h$ obsahuje nanejvýš $\left\lfloor \frac{|A|}{2} \right\rfloor$ bodů z $A$. Tvrdíme, že každých $d$ konečných množin v $\mathbb{R}^d$ lze rozpůlit zároveň jednou nadrovinou.*

**Úloha 43.** Nechť $A_1, A_2, \ldots, A_d$ jsou disjunktní množiny v $\mathbb{R}^d$ takové, že každá $A_i$ obsahuje $n$ bodů a body z $\bigcup_{i=1}^{d} A_i$ jsou v obecné poloze (tedy žádná nadrovina neobsahuje víc než $d$ bodů z tohoto sjednocení). Ukažte, že potom lze body z $\bigcup_{i=1}^{d} A_i$ rozdělit do $n$ duhových $d$-tic (množin $\{x_1, x_2, \ldots, x_d\}$, kde $x_i \in A_i$), jejichž konvexní obaly jsou disjunktní.

Snad pro Tebe byla dvojpřednáška dost vyčerpávající :). Pokud by Tě zajímalo víc, určitě se podívej do skript k předmětu Základy kombinatorické a výpočetní geometrie, ze kterých jsem poměrně dost čerpala (a také získala nadšení pro toto téma).

[1] V angličtině centerpoint.

### Návody

**1.** Triangulace.

**2.** Jak se změní pořadí puků coby vrcholů trojúhelníku v kladném směru po jednom odpalu? Může zůstat po lichém počtu stejné?

**3.** Spoj si body ležící proti sobě. Podívej se, v jakých polorovinách Jack stojí.

**4.** Spoj bod uvnitř s vrcholy mnohoúhelníku. Můžou mít všechny vzniklé trojúhelníky pouze jeden ostrý úhel u stran mnohoúhelníku?

**14.** Uvaž jednotkové kružnice se středy v bodech množiny. Hmmm. Nejsou to náhodou konvexní útvary? Hmmm a neprotínají se náhodou?

**15.** Dokaž, že pokud na potenciální čáře řezu leží dílek, pak tam leží ještě aspoň jeden.

**16.** Pro tři čtverce s rovnoběžnými stranami platí, že když se každé dva z nich protínají, protínají se i všechny tři.

**17.** Ne. Vezmi čtyři různě barevné body a rozliš dva případy podle toho, zda leží v rovině, nebo ne.

**18.** Nechť $B$ je množina všech modrých bodů a $C$ množina všech červených. Uvaž jejich konvexní obaly a dokaž, že na ně jde použít Oddělovací větu.

**19.** Promítni mnohoúhelníky na přímku.

**20.** Pro každý z mnohoúhelníků uvaž ty hodnoty poloměru, pro které příslušná kružnice mnohoúhelník protíná. Co pro tato rozmezí platí?

**21.** Hellyho věta.

**22.** Vezmi si libovolnou trojici obdélníků a dokaž, že mají neprázdný průnik. Využij toho, že to jsou obdélníky.

**23.** Zafixuj si obdélník, který se neprotíná s co nejvíce obdélníky a rozděl na případy (je-li to žádný, jeden nebo dva a více).

**24.** Vezmi bod na konvexním obalu, kterému přísluší úhel alespoň $\frac{n-2}{n}180°$.

**25.** Vyjádři fikaně přímku jako bod v rovině a naroubuj na úlohu Hellyho větu.

**26.** Dvakrát vhodně posuň původní body a nakonec ještě něco ušetři.

**27.** Uvaž nejvzdálenější dvojici bodů.

**28.** Hellyho věta.

**29.** Uvaž konvexní obaly černých a bílých krav, použij Oddělovací a Caratheodoryho větu.

**30.** Projeď stromy od nejmenšího k největšímu a uzavři cestu.

**31.** Nakrájej mnohoúhelník mřížkou a vzniklé dílky naskládej na sebe.

**32.** Dokaž, že se parita zkoumaného počtu nezmění, když bod $P$ přeleze úsečku.

**33.** Na první kružnici připevni kreslicí bod a otáčej jím po druhé. Kreslicí bod nechť kreslí právě tehdy, když je aspoň nějaký bod na zakázaném území.

**34.** Dokaž tvrzení nejdřív pro 75 %, za tímto účelem uvaž čtveřice bodů. Pak vylepši odhad.

**35.** Uvaž graf, jehož vrcholy jsou malé trojúhelníčky a poslední vrchol je zbytek roviny. Dva vrcholy jsou spojeny hranou právě tehdy, když příslušné oblasti sdílí úsečku s červeným a zeleným krajním bodem. Zamysli se nad paritou stupňů vrcholů.

**36.** Rozděl $n$-úhelník na trojúhelníky a obarvi každý vrchol jednou ze tří barev tak, aby každý z trojúhelníků byl tříbarevný.

**37.** Dva body jdou oddělit od ostatních dvěma přímkami. Uvaž konvexní obal a odděluj tu lepší barvu. Pro odhad všechny body nasyp na pravidelný 2027-úhelník.

**39.** Představ si postupné kreslení této čáry. Po dokončení (uspokojení všech bodů) jedné strany čtverce budou dvě protější strany načaté, ale nedokončené. Z toho musí existovat cesta k jedné straně a zpátky, která bude dlouhá 198.

**43.** Indukcí, zkus dokázat $n \to 2n$ a $n \to 2n + 1$.

### Literatura a zdroje

Chtěla bych poděkovat především Davidu Hruškovi, z jehož *i*KSkové přednášky jsem převzala většinu příkladů. Děkuji také Majdě a Pepovi, kteří napsali super seriál!

[1] Jiří Matoušek: *Introduction to Discrete Geometry*, skripta KAM MFF UK, 2003.
[2] David Hruška: *Kombinatorická geometrie a konvexita* , sborník *i*KS, 2015.
[3] Pepa Minařík, Majda Mišinová: *Kombinatorická geometrie*, PraSečí seriál, 42. ročník.

# Obsah

**Eulerova funkcia** (Natália Bátorová) . . . . . 3
**Největší společný dělitel** (Káťa Danilina) . . . . . 7
**Pellova rovnice a kvadratické řády** (Matěj Doležálek) . . . . . 12
**Kombinatorické nepočítání** (Alica Dományová) . . . . . 22
**Švrčkův bod** (Alica Dományová) . . . . . 28
**Výpočetní složitost** (Vojta Gaďurek) . . . . . 32
**Nelineární soustavy rovnic** (Matěj Gajdoš) . . . . . 36
**Indukce v kombinatorice** (Klárka Grinerová) . . . . . 42
**Jensenova nerovnost** (Vít Hanika) . . . . . 46
**Dotyčnice** (Michal Pecho) . . . . . 53
**Pascal** (Michal Pecho) . . . . . 58
**Diskrétní kalkulus** (Daniel Perout) . . . . . 62
**Eliptické křivky** (Zdeněk Pezlar) . . . . . 68
**Velká čísla** (Zdeněk Pezlar) . . . . . 72
**Hledání extrémů, aneb „Nej-“ případy** (Josef „José“ Soural) . . . . . 76
**Antirovnoběžnost a izogonály** (Jolča Štraitová) . . . . . 81
**Konvexní kombinatorická geometrie** (Adéla Karolína Žáčková) . . . . . 85