# Mamutov

Sborník, podzim 2023

Natália Bátorová
Fíla Čermák
Káťa Danilina
Matěj Doležálek
Vojta Gaďurek
Klárka Grinerová
Vít Hanika
Lenka Kopfová
Magdaléna Mišinová
Vendula Onderková
Daniel Perout
Martin Raška
Matouš Šafránek
Adéla Karolína Žáčková

Autoři: Natália Bátorová, Fíla Čermák, Káťa Danilina, Matěj Doležálek, Vojta Gaďurek, Klárka Grinerová, Vít Hanika, Lenka Kopfová, Magdaléna Mišinová, Vendula Onderková, Daniel Perout, Martin Raška, Matouš Šafránek, Adéla Karolína Žáčková
Editoři: Káťa Danilina, Matěj Doležálek
vydání první, náklad 48 výtisků
listopad 2023
Díky za pomoc všem, kterým je za co děkovat.

Soustředění podpořily:

ČESKÁ MATEMATICKÁ SPOLEČNOST

qminers

# RSA

Natália Bátorová

Abstrakt. Pánové Diffie a Hellman popsali v roce 1976 asymetrické šifry, ve kterých se používají dva klíče. Jedním se zpráva šifruje a druhým dešifruje. Sami však neimplementovali konkrétní algoritmus, s tím přišli o rok později pánové Rivest, Shamir a Adleman, z jejichž jmen vznikl název RSA. Ještě v roce 1974 popsal ekvivalentní algoritmus britský matematik Cocks, který ale skončil ve složce přísně tajné a zůstal skryt až do roku 1997. Tehdy algoritmus již všichni znali pod názvem RSA. A že to je moc hezký algoritmus, používá se dodnes. Proto se na téhle přednášce podíváme na všechno od popisu RSA až po útoky. Doprovázet nás budou Eulerova a taky Čínská zbytková věta. Nechť nám tedy cestou tento příběh připomíná, že objevy se ne vždy jmenují po svých prvních objevitelích ...

**Definice.** Nechť $n \in \mathbb{N}$, označme

$$\Phi_n = \{d \mid 0 < d < n,\ \gcd(d, n) = 1\}.$$

Pak hodnotu *Eulerovy funkce* $\varphi(n)$ definujeme jako počet prvků množiny $\Phi_n$.

Eulerova funkce tedy vyjadřuje počet přirozených čísel menších nebo rovných $n$, která jsou nesoudělná s $n$. Pro malá čísla je jednoduché to spočíst i přímo z definice, ale pro větší čísla budeme využívat následující tvrzení.

**Tvrzení.** *Nechť $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$, je prvočíselný rozklad čísla $n > 1$, pak*

$$\varphi(n) = (p_1 - 1) \cdot p_1^{\alpha_1 - 1} \cdots (p_m - 1) \cdot p_m^{\alpha_m - 1}.$$

**Věta.** (Eulerova) *Nechť $x, n \in \mathbb{N}$ a $\gcd(x, n) = 1$, pak $x^{\varphi(n)} \equiv 1 \pmod{n}$.*

Připomeňme si ještě značení $x^{-1} \bmod n$, zkráceně (pokud nehrozí nedorozumění) jenom $x^{-1}$, definované jako takové přirozené číslo menší nebo rovno $n$, pro které $x \cdot x^{-1} \equiv 1 \pmod{n}$. Spočteme ho pomocí rozšířeného Euklidova algoritmu.

**Cvičení 1.** (těžší) Ukažte, že pro každé $n$ a $x \in \Phi_n$ je $x^{-1}$ definované jednoznačně (a taky leží v $\Phi_n$).

**Cvičení 2.** Rozmyslete si, že pro $x$ takové, že $\gcd(x, n) > 1$, není $x^{-1}$ definováno.

**Věta.** (Čínská věta o zbytcích) *Buďte $m_1, \ldots, m_n$ po dvou nesoudělná přirozená čísla. Označme $M = m_1 \cdot m_2 \cdots m_n$. Buďte $a_1, \ldots, a_n$ libovolná celá čísla. Pak existuje právě jedno $x \in \{0, \ldots, M-1\}$ splňující*

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

## RSA

Nejdřív si popíšeme generování klíče:

(1) Zvolíme si dvě velká prvočísla $p$ a $q$ a spočteme jejich součin $n = p \cdot q$.
(2) Spočteme hodnotu $\varphi(n) = (p-1)(q-1)$.
(3) Zvolíme $e \in \Phi_{\varphi(n)}$.
(4) Spočteme $d = e^{-1} \bmod \varphi(n)$, tedy $d \cdot e \equiv 1 \pmod{\varphi(n)}$.

Veřejným klíčem je dvojice $(e, n)$, soukromým dvojice $(d, n)$. A jak probíhá šifrování a dešifrování?

Alice (A) chce poslat zprávu Bobovi (B).

B: Vygeneruje si klíč a zveřejní $(e, n)$.
A: Napíše zprávu $x$ a pošle Bobovi $x^e \bmod n$.
B: Obdrží šifrovanou zprávu $y$ a spočte $y^d \bmod n$. Tím zprávu dešifruje.

**Cvičení 3.** Vygenerujte si klíč a pak si s nějakým kamarádem vyměň veřejný klíč a pošlete si šifrované zprávy. Tak co, uměli jste obdrženou zprávu dešifrovat?

Algoritmus lze zrychlit pomocí ČZV a to tak, že při generování klíče v kroku

(2) spočteme hodnotu $k = \operatorname{lcm}(p-1, q-1)$,
(3) zvolíme $e \in \Phi_k$,
(4) spočteme $d = e^{-1} \bmod k$, tedy $d \cdot e \equiv 1 \pmod{k}$.

Pak totiž $x^{d \cdot e} \equiv x \pmod{p}$, protože $d \cdot e \equiv 1 \pmod{p-1}$, a $x^{d \cdot e} \equiv x \pmod{q}$, protože $d \cdot e \equiv 1 \pmod{q-1}$. Vyřešením soustavy nám vyjde $x^{d \cdot e} \equiv x \pmod{n}$.

**Cvičení 4.** (těžší) Jak bychom mohli zrychlit dešifrování?

### Podpis založený na RSA

Už umíme zprávy šifrovat a dešifrovat, ale co kdyby útočník posílal zprávy pod naším jménem? Kde bude mít příjemce jistotu, že jsme zprávu poslali opravdu my? Řešením tohoto problému je digitální podpis. Odesílatel zprávu podepíše a příjemce ověří podpis.

**Cvičení 5.** Jak by mohlo fungovat podepisování zpráv s využitím RSA? A co když útočník zprávu odchytí a nějak ji pozmění?

V praxi není ve zvyku podepisovat celou zprávu, ale její otisk – hash. Hashovací funkce mají takovou vlastnost, že pro všechna $n$ je jednoduché spočíst $h(n)$, ale těžké najít inverz $h^{-1}(n)$. Proto se využívají pro zaručení integrity zpráv. Odesílatel pošle spolu se zprávou její hash, tedy dvojici $(h(x), c(x))$, kde $c(x)$ je zašifrovaná zpráva. Příjemce si pak dešifruje zprávu a spočte si k ní $h(x)$. Pokud se hodnota shoduje s tou, kterou obdržel od odesílatele, nedošlo v průběhu přenosu ke změně zprávy. Samotný hash ještě, ovšem, nepostačuje na autentizaci, toho se docílí až podepsáním hashe.

### Slepý podpis a RSA

Slepý podpis je moc důležitý a využíváme jej, když potřebujeme aby naši zprávu podepsala nějaká instituce, ale přitom neznala její obsah.

**Cvičení 6.** Napadne vás konkrétní příklad, kdy je slepý podpis potřebný?

Typickým příkladem jsou digitální platby. Potřebujeme, aby všechny digitální peníze byly podepsány bankou, ale zároveň nechceme, aby měla banka o plátci příliš mnoho informací. Pokud bychom banku jen požádali o podepsání peněz, které budeme chtít používat, mohla by si tyto konkrétní peníze zapamatovat. Potom by přesně věděla, kdy a kde (případně za co) je utrácíme. To z hlediska GDPR není vhodné, zejména když zvážíme nákupy jízdenek, léků, jídla, ... Třetí strana se tím dozví o našem životě hodně informací.

Proto požádáme banku o podepsaní peněz, ale předtím je zaslepíme. Banka vidí sumu a zná naši totožnost, na základě čehož peníze podepíše a pošle zpátky. Taky je odepíše z účtu. My pak odstraníme zaslepení, přičemž podpis na penězích zůstane, a koupíme si za ně děsně cool PraSečí disky. Prodejce si ověří podpis a odešle podepsané peníze do banky. Banka ověří podpis a jestli nedošlo k duplicitě platby a když je všechno v pořádku, můžeme si jít zahrát frisbee. Banka při platbě nezjistí naši totožnost, ale ví, že někomu tyhle peníze někdy podepsala, tedy nejsou falešné.

Další využití slepého podpisu najdeme při elektronických volbách. Všechny volební lístky musí být podepsány volebním komisařem (jinak jsou neplatné), ten však nesmí vědět, komu jsme hlas odevzdali.

A jak tedy funguje slepý podpis založený na RSA? Ať banka má veřejný klíč $(e, n)$, soukromý $(d, n)$.

| | |
|---|---|
| My: | Chceme podepsat $x$. Zvolíme zaslepující hodnotu $\alpha \in \Phi_n$, spočteme hodnotu $\alpha^{-1}$, kterou si zapamatujeme a odešleme na podpis $x \cdot \alpha^e \bmod n$. |
| Banka: | Obdrží zprávu $y$ a pošle nám zpátky $y^d \bmod n$. |
| My: | Obdržíme $z \equiv y^d \equiv x^d \cdot \alpha^{e \cdot d} \equiv x^d \cdot \alpha \pmod{n}$. Obchodníkovi zašleme $z \cdot \alpha^{-1} \equiv x^d \pmod{n}$. |

## Do útoku!

Při použití dostatečně velkého klíče (v dnešní době minimálně 2048 bitů) je algoritmus RSA považovaný za bezpečný, protože pro rozklad čísla na prvočinitele není známý žádný efektivní algoritmus (který by čísla uměl rozložit v polynomiálním čase). Zároveň ale není dokázáno, že takový algoritmus neexistuje. Útočník ale může využít některé slabiny generování klíče.

Úplně nejhorší je použít $p$ víckrát pro různá $q_i$. Součiny $n_{1,2} = p \cdot q_{1,2}$ jsou veřejné a kdokoli může spočíst $\gcd(n_1, n_2)$. Nebo když jsou zpráva a veřejný klíč příliš malé, při umocnění nedojde k přetečení a stačí tak zprávu klasicky odmocnit.

**Cvičení 7.** (těžší) Ukažte, že ze znalosti $n$ a $\varphi(n)$ lze určit prvočíselný rozklad $p$, $q$.

Použití stejného $n$ vícekrát je také špatné, protože ze znalosti $n$, $e$ a $d$ lze určit prvočíselný rozklad $n$. My si ukážeme jednodušší útok. Alice poslala Bobovi a Cyrilovi stejné zprávy $x$, přičemž Bob a Cyril sdílejí stejný modul $n$. Zpráva $x$ je malá, ale Alice spoléhá na to, že Bob a Cyril mají velké veřejné exponenty. My si odchytíme zašifrované zprávy $y_B \equiv x^{e_B} \pmod{n}$ a $y_C \equiv x^{e_C} \pmod{n}$. Spočteme si Bézoutovy koeficienty $\gcd(e_B, e_C) = a \cdot e_B + b \cdot e_C$. Platí $y_C^a \equiv x^{e_C \cdot a} \pmod{n}$, $y_C^b \equiv x^{e_C \cdot b} \pmod{n}$ a proto $y_B^a \cdot y_C^b \equiv x^{\gcd(e_B, e_C)} \pmod{n}$. Pokud je $\gcd(e_B, e_C)$ dostatečně malé a nedojde k přetečení při mocnění, odmocněním zjistíme zprávu $x$.

**Cvičení 8.** Odchytili jste zašifrované zprávy $y_1 = 1$ s veřejným klíčem $(89, 517)$ a $y_2 = 509$ s veřejným klíčem $(141, 517)$. Zjistěte, jak zněla původní zpráva.

### Håstadův útok na malý veřejný exponent

Alice poslala stejnou zprávu $k$ různým lidem, kteří měli stejný veřejný exponent $e$, přičemž $k \geq e$, a různé moduly $n$, tedy jejich veřejný klíč byl $(e, n_i)$. My jsme cestou odchytili zašifrované zprávy $y_i$, máme tedy soustavu rovnic:

$$\begin{aligned} x^e &\equiv y_1 \pmod{n_1}, \\ &\vdots \\ x^e &\equiv y_k \pmod{n_k}. \end{aligned}$$

Můžeme předpokládat, že $n_i$ jsou po dvou nesoudělné. Pak z ČZV dostaneme řešení $x^e \equiv y \pmod{n_1 \cdots n_k}$. Označme $n_0 = \min\{n_i \mid i = 1, \ldots, k\}$. Jelikož $x < n_0$ a $k \geq e$, tak $x^e < n_0^e \leq n_0^k < n_1 \cdots n_k$. Takže nedošlo k přetečení a klasickým odmocněním zjistíme zprávu $x$.

**Cvičení 9.** Vyzkoušejte si Håstadův útok pro $e = 3$ a moduly $n_1 = 51$, $n_2 = 65$, $n_3 = 77$. Odchycené zprávy jsou postupně 2, 57 a 50.

## Návody

**1.** Pro důkaz existence použij Bézouta. Pokud neznáš Bézoutovu větu, můžeš zkusit dokázat (třeba rozšířeným Eukleidovým algoritmem), že pokud $\gcd(n, x) = 1$, tak existují koeficienty $k, l \in \mathbb{Z}$ takové, že $k \cdot n + l \cdot x = 1$. Co je tedy $x^{-1}$?

**2.** Pokud $d = \gcd(n, x) > 1$, tak $x \equiv 0 \pmod{d}$. Pokud $d \mid n$ a $x \equiv y \pmod{n}$, pak taky $x \equiv y \pmod{d}$.

**4.** Použij opět ČZV a dešifruj nejdřív mod $p$ a pak mod $q$.

**7.** Hledej je jako kořeny nějakého polynomu.

## Literatura a zdroje

[1] Andrew Kozlík: Přednášky z Úvodu do kryptografie, MFF UK, 2023.
[2] Michal Töpfer: *Asymetrické šifrování*, Branná, 2019.
[3] Jakub Klemsa: *Rozlouskneme RSA?*, Lysečiny, 2013.

# Ciferné součty

Fíla Čermák

Abstrakt. V tomto příspěvku se podíváme na různé typy úloh obsahující ciferné součty a ukážeme si techniky, které nám s jejich řešením pomůžou. Občas se podíváme i na ciferné součty v jiných soustavách.

Ciferné součty se v olympiádních úlohách neobjevují často, ale jednou za čas je v nějaké úloze najdete. Obecně není mnoho typů úloh, které lze na ciferné součty vymyslet, a tak tady (až na ty nejbrutálnější) projdeme téměř všechny.

Nejprve ale přiblížíme, co přesně znamená ciferný součet a jak ho v tomto příspěvku budeme značit.

**Definice.** Ciferným součtem čísla $n$ rozumíme číslo, které dostaneme sečtením všech cifer čísla $n$ v jeho desítkovém zápisu. Tedy, pokud desítkový zápis čísla $n$ je $\overline{a_n \dots a_0}$, tj. $n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0$, pak jeho ciferný součet je $S(n) = a_k + a_{k+1} + \cdots + a_0$.

Ciferný součet čísla $n$ budeme značit $S(n)$.

**Příklad 1.** Nechť $d$ je počet cifer v desítkovém zápise čísla $n$. Pokud označíme $n_k$ číslo, které vznikne smazáním posledních $k$ cifer z čísla $n$, dokažte vztah

$$n = S(n) + 9n_1 + 9n_2 + \cdots + 9n_{d-1}.$$

(APMO 2001)

### Písemné sčítání, přechod přes desítku

Většina technik, které budeme používat, je poměrně intuitivní a my začneme tou nejintuitivnější – co se stane při písemném sčítání s ciferným součtem v závislosti na přechodech přes desítku.

**Příklad 2.** Najděte číslo $n$, pro které jsou $S(n)$ i $S(n+1)$ dělitelná sedmi.
(PraSe 36–7–3)

**Příklad 3.** Mějme dáno přirozené číslo $n$, jehož cifry jsou ostře rostoucí zleva doprava. Určete ciferný součet čísla $9n$. (PraSe 23–6–2)

**Příklad 4.** Skripta MFF jsou číslována šesticifernými čísly, přičemž jsou povoleny nuly na začátku. *Šťastnými* nazveme ta z nich, která mají stejný ciferný součet prvních tří a posledních tří cifer. Dokažte, že součet označení všech šťastných skript je dělitelný sedmi. (PraSe 23–6–3)

**Příklad 5.** Dokažte, že mezi 39 po sobě jdoucími přirozenými čísly můžeme vždy najít nějaké, jehož ciferný součet je dělitelný 11. (Sovětská MO 1961)

**Příklad 6.** Najděte přirozená čísla $a$, $b$, $c$ taková, že

$$S(a+b)<5, \qquad S(b+c)<5, \qquad S(c+a)<5, \quad S(a+b+c)>50.$$

(PraSe 32–1–6)

**Příklad 7.** Nechť $m$, $n$ jsou přirozená čísla a navíc $m$ má $d$ cifer a $d<n$. Vypočítejte ciferný součet $(10^n-1)m$.

**Příklad 8.** Vypočítejte ciferný součet $9\cdot 99\cdot 9999\cdots(10^{2^n}-1)$ v závislosti na $n$.

**Příklad 9.** Ciferný součet čísla $N$ je 100, ciferný součet čísla $5N$ je 50. Dokažte, že $N$ je sudé.

### Nerovnosti

Můžeme nahlédnout následující rovnost, druhou nerovnost dokázat pomocí písemného sčítání a třetí nerovnost pak ukázat indukcí.

**Tvrzení 10.**

(1) $S(10a)=S(a)$,
(2) $S(a+b)\le S(a)+S(b)$,
(3) $S(ab)\le S(a)S(b)$.

**Příklad 11.** Dokažte, že pro každé přirozené číslo $n$ platí

$$S(2n)\le 2S(n)\le 10S(2n).$$

(PraSe 23–6–1)

**Příklad 12.** Najděte největší možnou hodnotu poměru $\frac{S(n)}{S(16n)}$. (PraSe 35–2–8)

### Kritéria dělitelnosti

Ciferné součty se dají občas použít jako jednoduchá kritéria dělitelnosti. Určitě všichni znáte například kritérium dělitelnosti devíti. Číslo $n$ je dělitelné devíti právě tehdy, když je dělitelné devíti číslo $S(n)$. Co už není tak známé, je, že toto kritérium můžeme jednoduše rozšířit na všechny zbytky:

**Tvrzení 13.** $S(n)\equiv n \pmod 9$.

Samozřejmě co platí pro devítku, platí taky pro všechny její dělitele, v tomto případě pro trojku, takže $S(n) \equiv n \pmod 3$.

Devítku jsme ale nevybrali jen tak náhodou. Tato kongruence platí právě proto, že základ naší soustavy (desítka) je kongruentní s 1 modulo 9. Takže pokud budeme pracovat s ciferný součty v jiné soustavě, například o základu $q$, pak naše kongruence bude platit pro $q-1$.

**Příklad 14.** Vezmeme přirozená čísla od jedné do bilionu a každé z nich postupně zredukujeme na jednociferné číslo tak, že jej opakovaně nahradíme jeho ciferným součtem. Dostaneme víc jedniček nebo dvojek? (Sovětská MO 1964)

**Příklad 15.** Existuje přirozené číslo $n$ takové, že $S(2^n) = S(2^{n+1})$?

**Příklad 16.** Je možné najít 19 různých přirozených čísel takových, že jejich součet je 1999 a všechna mají stejný ciferný součet? (Ruská MO 1999)

**Příklad 17.** Najděte všechny možné hodnoty ciferného součtu druhých mocnin přirozených čísel. (domácí kolo MO 1993)

**Příklad 18.** Najděte všechna přirozená čísla $d$ taková, že libovolné přirozené číslo dělitelné $d$ zapsané ve 2023-kové soustavě má ciferný součet dělitelný $d$. (PraSe 23–6–4)

### Maximální ciferný součet

Principem této techniky je poznatek, že ze všech $n$-ciferných čísel má největší ciferný součet číslo $99\ldots9$. Můžeme tedy jednoduše shora omezit ciferný součet velkých čísel číslem $9(\lfloor \log n \rfloor + 1)$.

**Příklad 19.** Na tabuli je napsané číslo $2018^{2018}$. Když jej 2018-krát nahradíme jeho ciferným součtem, jaké číslo nám na tabuli zbude?

**Příklad 20.** Určete hodnotu výrazu $S(S(S(4444^{4444})))$. (IMO 1975)

### Další všemožné úlohy

**Příklad 21.** Nalezněte číslo $n$, které je dělitelné $S(n) + 2017$. (PraSe 36–7–1)

**Příklad 22.** Mějme dáno přirozené číslo $n$ takové, že $S(n) = 100$ a $S(44n) = 800$. Najděte hodnotu $S(3n)$. (Ruská MO 1999)

**Příklad 23.** Dokažte, že existuje nekonečně mnoho čísel $n$ takových, že

$$S(n) > 2018 \cdot S(3n).$$

**Příklad 24.** Nechť $f_1(n) = [S(n)]^2$ a $f_{k+1}(n) = f_1(f_k(n))$. Určete hodnotu výrazu $f_{1991}(2^{1990})$. (IMO Shortlist 1990)

**Příklad 25.** Nechť $f(n) = S(n) + n$. Existuje číslo takové, že $f(n) = 1980$? Dokažte, že pro každé přirozené číslo $m$ můžeme najít číslo $n$ takové, že buď $f(n) = m$ nebo $f(n) = m + 1$. (Sovětská MO 1980)

**Příklad 26.** Je dán polynom $P(n)$ s celočíselnými koeficienty. Označíme $s_n$ ciferný součet čísla $P(n)$. Dokažte, že alespoň jedna hodnota se v posloupnosti $s_n$ vyskytuje nekonečně mnohokrát. (Polská MO 1987)

### Unique [Ja:'ni:k] Puzzliky

**Příklad 27.** Najdi tři cifry $a$, $b$, $c$ takové, že pro ně platí $28a + 30b + 31c = 365$.

**Příklad 28.** Číslo $2^{29}$ obsahuje všech 10 cifer kromě jedné. Jaká to je?

**Příklad 29.** Jsou právě tři 8 ciferná čísla pro něž platí, že součet 8. mocnin jejich cifer je roven tomuto číslu. Dvě z nich jsou 24678051 a 88593477. Urči to třetí.

### Návody

**1.** Použij definici ciferného součtu.

**2.** O kolik se $S(n + 1)$ sníží oproti $S(n) + 1$ s každou cifrou, která při přičtení jedničky přejde přes desítku?

**3.** Všimni si, že $9n = 10n - n$.

**4.** Jaký tvar mají šťastná čísla? Co nějaké párování?

**5.** Co můžeme říct o ciferném součtu čísel dělitelných 10?

**6.** Uvažovat $x = a + b$, $y = b + c$ a $z = a + c$ je možná jednodušší.

**7.** Prostě to spočítejte jako na základce.

**8.** Indukce.

**9.** $5N = \frac{10N}{2}$ a pak už zase dělení pod sebou.

**11.** Pro druhou nerovnost: co je $S(10n)$?

**12.** Co je $S(10000n)$?

**14.** Uvažuj mod 9.

**15.** Uvažuj mod 3.

**16.** Uvažuj mod 9 a pak zkus nejmenší varianty.

**17.** Uvažuj mod 9.

**18.** Hledáš čísla, která ve 2023-kové soustavě dávají kritérium dělitelnosti ciferného součtu.

**19.** Kolik maximálně cifer má $2018^{2018}$? Jakou nejvyšší hodnotu tak může mít $S(2018^{2018})$? Zkus mod 9.

**20.** Uvažuj horní odhad každého z ciferných součtů. Použij mod 9.

**21.** Nech $S(n) + 2017$ být mocninou desíti.

**22.** Uvažuj přechod přes desítku při násobení.

**23.** Najdi jedno a násob ho deseti. Abys ho našel, zkus vydělit velké číslo s malým ciferným součtem třemi.

**24.** Najdi $f_{1998}(11)$. (Což byla mimochodem úloha na AIME 1988.)

**25.** Při přechodu přes desítku se $f(n)$ zmenší, ale přesto se dostane libovolně vysoko.

**26.** Násob mocninami deseti.

**27.** Zkus $29a + 30b + 31c = 366$.

**28.** Zkus mod 9.

**29.** To určitě. :D

### Literatura a zdroje

Přednášku jsem založil na příspěvku Jáchyma Soleckého ze soustředění v Horních Lysečinách 2018. Do něj jsem přidal několik dalších úloh, které se v posledních letech na toto téma objevily. Jinak jsem čerpal ze stránek PraSátka a různých dalších matematických olympiád a soutěží.

# Lineární algebra v kombinatorice

Fíla Čermák

Abstrakt. Díky znalosti základů lineární algebry se objevuje, možná nečekaná, možnost je aplikovat při řešení rozličných úloh středoškolské matematiky, zejména kombinatoriky. Přednáška navazuje na přednášku o lineární algebře. Příspěvek je jen o aplikaci.

### Co je třeba znát

Přednáška navazuje na Úvod do lineární algebry. Předpokládá znalost a použití základních pojmů z lineární algebry, jako je lineární nezávislost vektorů, báze vektorového prostoru nebo hodnost matice. Také neuškodí vědět, co je to Gaussova eliminace, jelikož je to velmi užitečný nástroj pro náhled do světa lineární algebry.

Na ověření znalostí si připomeňte následující: x

**Příklad.**

(1) Definici lineární závislosti vektorů.
(2) Definici báze.
(3) Vektorový součin.
(4) Kolik vektorů potřebuji na vygenerování prostoru $\mathbb{Z}_2^5$?
(5) Mějme matici $A \in \mathbb{R}^{100\times 2}$. Je v pohodě udělat $A^TA$ i $AA^T$?
(6) Rozmyslete si, že hodnost té jedné správné možnosti z minulého bodu je menší rovna $r(A)$.
(7) Jaký je determinant matice, která má na diagonále 1 a jinde 2?

Také není na škodu tušit pár základů teorie grafů, jako co je to graf, cyklus nebo třeba stupeň vrcholu.

### Zvolme si správný prostor a najděme v něm závislost, nebo nagenerujme všechno

**Úloha 1.** V obdélníkovém sále s $r$ řadami po $s$ sedadlech ($r > s$) na některá místa usedli lidé. Dokažte, že můžeme vybrat $k \geq 1$ řad tak, aby v každém sloupci sedadel byl počet lidí sedících ve vybraných řadách sudý.

**Úloha 2.** V tabulce $5 \times 5$ jsou zapsána celá čísla. Je dovoleno vybrat libovolný čtverec $3\times 3$ nebo $2\times 2$ a zvětšit v něm všechna čísla o 1. Je vždy možné postupným

prováděním těchto operací získat tabulku, ve které jsou všechna čísla dělitelná 2011?

**Úloha 3.** Nechť $a_1, a_2, \ldots, a_5, b_1, b_2, \ldots, b_5$ jsou ne nutně různá čísla z množiny $\{1, 2, \ldots, 10\}$ taková, že $a_i \geq b_i$ pro $1 \leq i \leq 5$. Dokažte, že existují celá čísla $\alpha_1, \ldots, \alpha_5$, ne všechna nulová, taková, že

$$\binom{a_1}{b_1}^{\alpha_1} \binom{a_2}{b_2}^{\alpha_2} \binom{a_3}{b_3}^{\alpha_3} \binom{a_4}{b_4}^{\alpha_4} \binom{a_5}{b_5}^{\alpha_5} = 1.$$

**Úloha 4.** V řadě je $N$ žárovek očíslovaných postupně 1 až $N$. Krokem rozumíme přepnutí tří žárovek, jejichž čísla $a$, $b$, $c$ splňují $a + c = 2b$. Určete všechna $N$, pro která lze konečnou posloupností takových kroků všechny žárovky zhasnout nezávisle na jejich počátečním stavu. (C5, 1. ročník *i*KS)

**Úloha 5.** Nechť $A_1, A_2, \ldots, A_{n-1}$ jsou po dvou různé podmnožiny množiny $M = \{1, \ldots, n\}$. Dokažte, že pro nějaké $1 \leq k \leq n$ jsou množiny $A_i \setminus \{k\}$ také po dvou různé.

**Úloha 6.** Mějme přirozená čísla $k$, $n$ splňující $k < n$ a množinu $S = \{1, \ldots, n\}$. Nechť $A_1, \ldots, A_k$ jsou neprázdné podmnožiny $S$. Dokažte, že je možné obarvit některé prvky $S$ dvěma barvami – červenou a modrou – tak, aby byly splněny následující podmínky:

(1) každý prvek $S$ je buď neobarvený, nebo je červený, nebo je modrý,
(2) alespoň jeden prvek $S$ je obarven,
(3) každá z množin $A_i$ je buď celá neobarvená, nebo se v ní vyskytuje alespoň jeden prvek z každé ze dvou barev. (VJIMC 2009)

**Úloha 7.** (Lindströmova věta, „baby“ verze) Pokud jsou $A_1, \ldots, A_m$ podmnožiny množiny $\{1, \ldots, n\}$ a $m > n$, pak existují dvě disjunktní množiny $I_1, I_2 \subseteq \{1, \ldots, m\}$, z nichž je alespoň jedna neprázdná a pro které platí

$$\bigcup_{i \in I_1} A_i = \bigcup_{i \in I_2} A_i.$$

**Úloha 8.** (Lindströmova věta) Pokud navíc v předchozí úloze $m > n + 1$, pak můžeme požadovat, aby platilo

$$\bigcap_{i \in I_1} A_i = \bigcap_{i \in I_2} A_i.$$

**Úloha 9.** Sedm trpaslíků po 16 dní pracovalo následujícím způsobem:

(1) každý trpaslík celý den kutal stříbro nebo sbíral maliny,
(2) pro každé dva dny platí, že během nich alespoň tři trpaslíci dělali obojí,
(3) první den všichni kutali stříbro.

Dokažte, že některý den všichni trpaslíci sbírali maliny. (EGMO 2013/6)

**Úloha 10.** Na matematické konferenci se každá dvojice matematiků buď navzájem zná, nebo nezná. Každý matematik bude obědvat v jedné ze dvou velkých jídelen. Každý trvá na tom, aby jedl v jídelně, ve které má sudý počet známých. Dokažte, že počet způsobů, jak rozdělit matematiky do jídelen, je mocninou dvou (tedy tvaru $2^k$ pro nezáporné celé číslo $k$). (USAMO 2008)

**Úloha 11.** Máme množinu 13 závaží s racionálními hmotnostmi. Pokud odebereme kterékoli z nich, zbylých 12 závaží lze vždy rozdělit na dvě skupiny po 6 se stejnou celkovou váhou. Dokažte, že všechna závaží mají stejnou hmotnost.

### Úlohy s městy aneb násobení a skalární součiny

**Úloha 12.** V licho-sudém městě žije $n$ lidí a existuje $m$ klubů takových, že každý z nich má lichý počet členů a každé dva různé mají sudý počet společných členů. Dokažte, že $m \leq n$.

**Úloha 13.** Ve městě žije $n$ lidí, existuje $m$ filmových klubů $F_1, \ldots, F_m$ a $m$ divadelních klubů $D_1, \ldots, D_m$ takových, že $2 \mid |F_i \cap D_j| \Leftrightarrow i \neq j$. Dokažte, že $m \leq n$.

**Úloha 14.** Nechť $p$ je liché prvočíslo a $k$ přirozené číslo. Ve městě žije $n$ lidí a existuje $m$ klubů $K_1, \ldots, K_m$ takových, že $p^k \mid |K_i \cap K_j| \Leftrightarrow i \neq j$. Dokažte, že $m \leq n$.

**Úloha 15.** V sudo-lichém městě žije $n$ lidí a existuje $m$ klubů takových, že každý z nich má sudý počet členů a každé dva různé mají lichý počet společných členů. Dokažte postupně, že

(1) $m \leq n + 1$,
(2) $m \leq n$,
(3) pro sudá $n$ dokažte, že $m \leq n - 1$.

**Úloha 16.** Nechť $n \in \mathbb{N}$ je sudé a $A_1, \ldots, A_n \subseteq \{1, \ldots, n\}$ mají všechny sudý počet prvků. Dokažte, že existují dvě různá čísla $1 \leq i, j \leq n$ taková, že $A_i \cup A_j$ má také sudý počet prvků.

**Úloha 17.** (Fisherova nerovnost 1) V rybářské vesnici žije $n$ rybářů, kteří tvoří $m$ odborových sdružení. Každá dvě sdružení sdílejí přesně jednoho člena. Dokažte, že $m \leq n$.

**Úloha 18.** (Fisherova nerovnost 2) V rybářské vesnici žije $n$ rybářů, kteří tvoří $m$ odborových sdružení. Každá dvě sdružení sdílejí přesně $k$ členů. Dokažte, že $m \leq n$.

**Úloha 19.** (Mod-q města) Mějme číslo $q$. Ve městě žije $n$ lidí, kteří tvoří $m$ klubů $K_1, \ldots, K_m$, přičemž platí, že $q \mid |K_i \cap K_j| \Leftrightarrow i \neq j$. Dokažte, že $m \leq c(q)n$, kde $c(q)$ je funkce nezávislá na $n$.

(1) Nejprve, kde $q = p_1 p_2 \cdots p_r$ pro různá prvočísla,
(2) pak obecně, kde $q = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$.

**Úloha 20.** Dokažte, že pokud jsou všechny vzdálenosti mezi $m$ body v $\mathbb{R}^n$ stejné, platí $m \leq n+1$.

### Grafy a prostory cyklů

**Úloha 21.** Souvislý graf má 1000 vrcholů a 2022 hran. Kolika způsoby můžeme nějaké hrany vymazat tak, aby každý vrchol výsledného grafu měl sudý stupeň?

**Úloha 22.** Graf $G$ má 42 vrcholů (žádný izolovaný) a 60 hran. Radek má 21 kružnic (podgrafů $G$) a tvrdí, že z nich umí „slepit“ libovolný podgraf $G$, jehož vrcholy mají všechny stupně sudé. „Slepením“ dvou grafů vznikne graf, jehož množina hran je symetrickým rozdílem množin hran původních grafů. Dokažte, že $G$ má nejvýše tři komponenty.

**Úloha 23.** Je daný graf a v každém vrcholu rozsvícená žárovka. V jednom tahu můžeme vybrat jeden vrchol, přepnout žárovku v něm a ve všech vrcholech s ním spojených hranou. Dokažte, že můžeme konečným počtem tahů všechny žárovky zhasnout.

### Polynomy jsou taky jenom vektory

**Úloha 24.** Rozhodněte, zda existují reálné polynomy $a(x)$, $b(x)$, $c(y)$, $d(y)$ takové, že

$$1 + xy + x^2y^2 \equiv a(x)c(y) + b(x)d(y).$$

(Putnam 2003 B1)

**Úloha 25.** Nechť $P(x)$ je nenulový reálný polynom. Dokažte, že existuje nenulový polynom $Q(x)$ takový, že polynom $R(x) = P(x)Q(x)$ má nenulové koeficienty pouze u členů s prvočíselnými exponenty.

**Úloha 26.** Mějme $m$ bodů v prostoru $\mathbb{R}^n$, přičemž tyto body mají mezi sebou pouze dvě různé vzdálenosti. Dokažte, že

$$\binom{n+1}{2} \leq m \leq \frac{(n+1)(n+4)}{2}.$$

**Úloha 27.** Mějme $m$ bodů v prostoru $\mathbb{R}^n$, přičemž tyto body mají mezi sebou pouze $s$ různých vzdáleností. Dokažte že

$$\binom{n+1}{s} \leq m \leq \binom{n+1+s}{s}.$$

### Návody

**1.** Správně reprezentuj sál a využij nerovnost.

**2.** Kolik máme (vhodně zvolených) vektorů? Aha, takže to vyjde těsně…, nebo že by stačil najít závislý $4 \times 4$?

**3.** Kolik tak máme prvočísel do 10? A kolik že máme těch kombinačních čísel?

**4.** Pro kolik nejméně žárovek už nageneruješ všechno? Potom použij indukci.

**5.** Napiš si do tabulky charakteristické vektory. Není tam nějak mnoho sloupců? Vyjádři jeden pomocí ostatních a zahoď ho.

**6.** Udělej si tabulku charakteristických vektorů. V lineární kombinaci máš kladné a záporné koeficienty.

**7.** Závislost charakteristických vektorů jsi již jistě objevil(a), nyní už jen nějakou souvislost se sjednocením. Hlavně zvol správné těleso. Vzpomeň si na úlohu 6.

**8.** Převeď průniky na sjednocení a zopakuj postup z „baby“ verze. Pozor na prázdná sjednocení.

**9.** Každý den reprezentuj sedmisložkovým r(em nad $\mathbb{Z}_2$. Co říkají podmínky ze zadání? Že v souřadnicích r(ů je nějaký velký rozdíl. Ne všechny r(y ze $\mathbb{Z}_2$ mohou být dny kvůli druhé podmínce.

**10.** Najdi grafově alespoň jeden způsob rozdělení. Buď máme sudé stupně, nebo jeden lichý (pak sporuj minimálním takovým grafem). Dále si zkus pohrát s maticí sousednosti $A$, kde na úhlopříčce jsou stupně mod 2. Rozdělení by potom mohla být soustava rovnající se úhlopříčce.

**11.** Bez újmy na obecnosti můžeme předpokládat, že závaží mají celočíselné hmotnosti, dále i to, že jedno z nich má hmotnost 0 a že jedno z nich má lichou hmotnost. Rozeber případy podle počtu sudých a lichých vah, neboť víš, že součet každé 12-tice je sudý.

**12.** Dokaž (sporem), že charakteristické r(y jsou nezávislé. Za tímto účelem udělej skalární součin příslušné rovnosti s vhodným charakteristickým vektorem. Nebo si uvědom, co říká součin $A^T A$.

**13.** Analogie předchozího úkolu.

**14.** Zkus pracovat nad vhodnějším tělesem.

**15.** Pro bod jedna využij úlohu o licho-sudém městě. Pro zbytek koukni na hodnost matice $A$ a $A^T A$, třeba i podle parity.

**16.** Sporem. Mohou být charakteristické vektory nezávislé? Potom použij standardní trik se skalárním součinem a najdi nějaký pěkný spor.

**17.** Zamysli se nad tím, jak vypadá $A^T A$ a zkus spočítat determinant. Co kdyby nebyl nula?

**18.** To stejné jako minule.

**19.** Zkus najít důkaz pro $c(q) = r$. Když těch klubů vezmeš hodně, určitě tam najdeš nějaké, které budou spadat i do úlohy pro nějaké prvočíslo (Dirichlet). Pro 2) udělej to samé, ale můžeš využít úlohu 14.

**20.** Použij kosinovou větu a s využitím skalárního součinu dokaž, že vektory z jednoho bodu k ostatním jsou lineárně nezávislé.

**21.** Kružnice grafu spolu s jejich „xorováním“ generují vektorový prostor. Jaká je jeho dimenze a jaký je počet vektorů?

**22.** Radek musí mít alespoň tolik kružnic, jaká je dimenze příslušného prostoru kružnic.

**23.** Udělej si tabulku $n \times n$ (sloupce jsou vypínače, řádky žárovky) podle toho, co co přepíná. Chceš nakombinovat sloupce na samé jednotky. To vypadá jako nějaká soustava, ne? Co se nesmí stát, aby soustava měla řešení? Na zbytek použij vlastnosti tabulky, která je odvozena z grafu.

**24.** Ne, sporem. Vhodným vícenásobným dosazením za $y$ dostaň na levé straně lineárně nezávislé polynomy v $x$. Co na to pravá strana?

**25.** Představ si $P(x)$ a $R(x)$ jako vektory. Jak vypadají polynomy $x^k P(x)$ a jak je to s jejich (ne)závislostí? Zvětšuj $k$, dokud nebudeš mít více volných proměnných (neznámých, které se stanou koeficienty $R$) než podmínek (rovností, které musí platit, aby $P(x)Q(x)$ splňoval zadání).

**26.** Mějme body $A_1, \ldots, A_m$, vzdálenosti $a, b$ a uvažme funkci

$$F(X, Y) = (d^2(X, Y) - a^2)(d^2(X, Y) - b^2),$$

kde $d(X, Y)$ je euklidovská vzdálenost. Ukaž, že $F(X, A_i)$ jsou lineárně nezávislé a všechny spadají do dost malého prostoru polynomů v $n$ proměnných (souřadnicích bodu $X$).

**27.** Zobecni předchozí argument a pak to spočti.

### Literatura a zdroje

[1] Michal Staník: *Lineární algebra v kombinatorice*, sborník *i*KS, 2022.
[2] David Hruška: *Lineární algebra v kombinatorice*, sborník *i*KS, 2014.
[3] Jan Kratochvíl: *Aplikace lineární algebra v kombinatorice*, MFF UK, 2022.

# Simsonova přímka

Káťa Danilina

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

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

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

**Cvičení.** Simsonovou přímkou bodu naproti vrcholu na kružnici opsané je protější strana.

**Úmluva.** Zachováme značení z první věty a předpokládáme, že $P$ leží na kružnici.

**Tvrzení.** *Je-li $H$ ortocentrum, označíme průsečík přímky $HA$ se Simsonovou přímkou bodu bodu $P$ jako $Q$. Nyní platí, že $HQPP_a$ je rovnoběžník.*

**Důsledek.** *Simsonova přímka bodu $P$ půlí úsečku $PH$.*

**Věta.** (Steinerova přímka) *Označme $P'_a$, $P'_b$, $P'_c$ obrazy bodu $P$ podle stran trojúhelníka $BC$, $CA$, $AB$. Leží-li $P$ na kružnici opsané trojúhelníku $ABC$, pak body $P'_a$, $P'_b$, $P'_c$ leží na jedné přímce. Tato přímka navíc prochází ortocentrem.*

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

**Důsledek.** *Simsonovy přímky protějších bodů na kružnici jsou na sebe kolmé a protínají se na Feuerbachově kružnici.*[1]

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

[1] Více se o Feuerbachově kružnici můžete dozvědět v tomto příspěvku: *https://prase.cz/library/FeuerbachEulerHR/FeuerbachEulerHR.pdf*.

### Příklady

**Příklad 1.** Pro bod $P$ na kružnici opsané trojúhelníku $ABC$ platí, že obrazy přímek $PA$, $PB$, $PC$ v osových souměrnostech postupně podle os úhlů $BAC$, $CBA$, $ACB$ jsou rovnoběžné a navíc jsou kolmé na Simsonovu přímku bodu $P$.

**Příklad 2.** V trojúhelníku $ABC$ jsou $D, E, F$ postupně paty výšek na strany $BC$, $CA$, $AB$. Paty kolmic z bodu $D$ na přímky $AB$, $BE$, $CF$ a $AC$ označíme postupně $P$, $Q$, $R$ a $S$. Dokažte, že body $P$, $Q$, $R$ a $S$ leží na jedné přímce. (BMO1 2015, 5)

**Příklad 3.** Na kratším z oblouků $CD$ kružnice opsané pravoúhelníku $ABCD$ zvolme bod $P$. Paty kolmic z bodu $P$ na přímky $AB$, $AC$ a $BD$ označme postupně $K$, $L$ a $M$. Ukažte, že úhel $\sphericalangle LKM$ má velikost $45°$, právě když $ABCD$ je čtverec. (MO 58–III–2)

**Příklad 4.** (Miquelův bod) Mějme čtyři přímky v obecné poloze (žádné dvě nejsou rovnoběžné a žádné tři se neprotínají v jednom bodě). Každá trojice z nich definuje trojúhelník. Uvážíme-li kružnice opsané těmto čtyřem trojúhelníkům, protínají se v jednom bodě.

**Příklad 5.** Na přímce jsou dány body $A$, $B$, $C$ a mimo ni bod $P$. Dokažte, že bod $P$ leží na kružnici opsané trojúhelníku tvořenému středy kružnic opsaných trojúhelníkům $ABP$, $BCP$, $ACP$.

**Příklad 6.** V trojúhelníku $ABC$ protíná osa úhlu $BAC$ protější stranu v bodě $D$. Označme $P$, $Q$ paty kolmic z bodu $D$ na strany $AB$, $AC$. Kolmice na $BC$ z bodu $D$ protne $PQ$ v bodě $X$. Ukažte, že $X$ leží na těžnici z bodu $A$.

**Příklad 7.** V ostroúhlém trojúhelníku $ABC$ je bod $P$ pata výšky na stranu $AC$ z bodu $B$. Označíme si $D$, $E$ postupně středy stran $AB$, $AC$. Bod $Q$ je obraz bodu $P$ podle přímky $DE$. Dokažte, že $BQ$ prochází středem kružnice opsané trojúhelníku $ABC$.

**Příklad 8.** Nechť $ABC$ je ostroúhlý trojúhelník a na kratším oblouku $BC$ jeho kružnice opsané si zvolíme bod $X$. Body $P$ a $Q$ budou paty z $X$ postupně na přímky $CA$ a $CB$. Bod $R$ je průsečík přímky $PQ$ a výšky na stranu $AC$ z bodu $B$. Přímka $\ell$ prochází bodem $P$ a je rovnoběžná s $XR$. Dokažte, že $\ell$ prochází pevným bodem nezávislým na poloze $X$. (USA TST 2014, 1)

**Příklad 9.** Na kružnici opsané trojúhelníku $ABC$ leží body $P$, $Q$ tak, aby $PQ \parallel BC$. Paty kolmic z bodů $P$ a $Q$ na $AB$, respektive $AC$ označme postupně $P_1$, $Q_1$, respektive $P_2$, $Q_2$. Dokažte, že přímky $P_1P_2$ a $Q_1Q_2$ se protínají na výšce na stranu $BC$.

**Příklad 10.** Konvexní pětiúhelník $AXYZB$ je vepsán do půlkružnice se středem $O$ a průměrem $AB$. Označme $P$, $Q$, $R$, $S$ postupně paty kolmic z bodu $Y$ na přímky $AX$, $BX$, $AZ$, $BZ$. Dokažte, že velikost ostrého úhlu, který svírají přímky $PQ$ a $RS$, je rovna $\frac{1}{2}|\sphericalangle XOZ|$. (USAMO 2010, 1)

**Příklad 11.** V ostroúhlém trojúhelníku $ABC$ je $H$ pata výšky z $A$. Na kružnici opsané $ABC$ jsou body $P, Q$ tak, že $|AP| = |PH|$ a $|AQ| = |QH|$. Průsečíky tečen ke kružnici opsané v $P$ a $Q$ se stranou $AB$, respektive $AC$ označíme $E_1$, $E_2$, respektive $F_1$, $F_2$. Dokažte, že poloměry kružnic opsaných trojúhelníkům $AE_1F_1$ a $AE_2F_2$ jsou stejné a že přímka procházející jejich středy je rovnoběžná s tečnou ke kružnici opsané $ABC$ v bodě $A$. (USA TSTST 2018, 5)

**Příklad 12.** Uvažujme pět bodů $A$, $B$, $C$, $D$, $E$ takových, že $ABCD$ je rovnoběžník a $BCED$ je tětivový čtyřúhelník. Přímka $\ell$, která prochází bodem $A$, protíná úsečku $DC$ v jejím vnitřním bodě $F$ a přímku $BC$ v bodě $G$. Platí-li $|EF| = |EG| = |EC|$, ukažte, že $\ell$ je osou úhlu $DAB$. (IMO 2007, 2)

**Příklad 13.** Nechť je $ABC$ trojúhelník s ortocentrem $H$. Na jeho kružnici opsané si zvolíme body $X, Y, Z$ . Definujeme $\ell_X$ jako přímku, která prochází patami kolmic z bodu $X$ na $AB$ a $AC$. Přímky $\ell_Y$ a $\ell_Z$ definujeme obdobně. Označíme $O$ střed kružnice opsané trojúhelníku, který vytýkají přímky $\ell_X, \ell_Y, \ell_Z$. Ortocentrum trojúhelníku $XYZ$ označíme $H'$. Dokažte, že $O$ je střed $HH'$.

(Brazil IberoAmerican TST 2022, 2)

**Příklad 14.** Označme $H$ ortocentrum ostroúhlého trojúhelníka $ABC$ a $\Omega$ jeho kružnici opsanou. Přímka procházející bodem $H$ protne kratší oblouky $AC$, $BC$ kružnice $\Omega$ postupně v bodech $M$, $P$. Rovnoběžka se Simsonovou přímkou bodu $P$ vzhledem k trojúhelníku $ABC$ vedená bodem $M$ protne $\Omega$ v bodě $K$. Rovnoběžka s $BC$ vedená bodem $P$ protne $\Omega$ podruhé v bodě $Q$. Označme $J$ průsečík $BC$ a $KQ$. Dokažte, že trojúhelník $KJM$ je rovnoramenný. (China TST 2011)

### Návody

**1.** Pro kolmost obrazu přímky $PA$ uvaž tětivový čtyřúhelník $PP_bAP_c$.

**2.** Hledej tětivové čtyřúhelníky.

**3.** Dokresli paty kolmic z $P$ na $AD$ a $BC$. Najdi Simsonovy přímky a uvědom si, že $|\sphericalangle LKM| = |\sphericalangle APB|$.

**4.** Protni dvě z kružnic v bodě $P$ a uvědom si, že paty kolmic v jednotlivých trojúhelnících definují stejné přímky.

**5.** Použij Simsonovu přímku bodu $P$ vůči trojúhelníku ze středů.

**6.** Dokresli trojúhelník tak, aby Simsonova přímka bodu $D$ vůči němu byla $PQ$.

**7.** Využij Steinerovu přímku vůči trojúhelníku ze středních příček.

**8.** Hledaným bodem je ortocentrum. Najdi rovnoběžník.

**9.** Dokresli paty kolmic z $P$, $Q$ na $BC$ a najdi rovnoběžníky.

**10.** Všimni si, že $PQ$ a $RS$ se protínají na $AB$.

**11.** Dokaž, že střed kružnice opsané $ABC$ leží na obou kružnicích.

**12.** Uvaž Simsonovu přímku bodu $E$ vzhledem k trojúhelníku $BCD$. Pomocí stejnolehlosti si rozmysli, že pata z $E$ je středem $BD$.

**13.** Stejnolehli trojúhelník $XYZ$ na polovinu z $H$. Nyní stačí dokázat, že $O$ je jeho ortocentrum. Pomocí tvrzení o úhlech mezi Simsonovými přímkami najdi tětivové čtyřúhelníky.

**14.** Označ $S = MP \cap BC$ a dokaž, že $KSJM$ je tětivový. Dokaž, že $MP$ je Steinerova přímka bodu $K$.

### Literatura a zdroje

Chtěla bych poděkovat *Martinu Raškovi*, od něhož jsem převzala většinu příspěvku a který již poděkoval *Štěpánu Šimsovi*, jehož příspěvek převzal.

[1] Martin Raška: *Simsonova přímka*, Sklené, 2019.
[2] *www.artofproblemsolving.com*.

# Interpolace

Matěj Doležálek

Abstrakt. Dozvíme-li se několik bodů, jimiž prochází graf neznámého polynomu, co z toho o něm můžeme vyvodit? Ukážeme si, že celkem dost.

**Věta.** (Lagrangeova interpolace) *Mějme navzájem různá $x_0, x_1, \ldots, x_n \in \mathbb{R}$ a libovolná $y_0, y_1, \ldots, y_n \in \mathbb{R}$. Pak mezi polynomy s koeficienty z $\mathbb{R}$ stupně nanejvýš $n$ existuje právě jeden, který splňuje $f(x_i) = y_i$ pro $i \in \{0, 1, \ldots, n\}$, a je to konkrétně*

$$f(x) = \sum_{i=0}^{n} y_i \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}. \qquad (\heartsuit)$$

**Úmluva.** Polynom na pravé straně v (♡) budeme nazývat *(Lagrangeovým) interpolačním polynomem* (skrz body $(x_0, y_0), (x_1, x_2), \ldots, (x_n, y_n)$).

**Cvičení.** Na reálných číslech není nic speciálního – rozmyslete si, že interpolace funguje i nad $\mathbb{Q}$, nad $\mathbb{C}$ nebo nad konečnými tělesy $\mathbb{Z}_p$ pro prvočísla $p$. (Obecně bychom ji tedy mohli zformulovat nad obecným *tělesem*.)

### Hodnoty v bodech

**Cvičení.** Všimněte si, že $\prod_{j \in \{0,1,\ldots,n\} \setminus \{k\}} \frac{n+1-j}{k-j} = (-1)^{n-k} \binom{n+1}{k}$.

**Věta.** (Binomická) *Pro nezáporné celé číslo $n$ platí $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$.*

**Úloha 1.** Reálný polynom $f$ stupně nanejvýš $n$ splňuje $f(k) = 2^k$ pro všechna $k = 0, 1, \ldots, n$. Spočtěte $f(n+1)$.

**Úloha 2.** Reálný polynom $f$ stupně nanejvýš $n$ splňuje $f(k) = \frac{1}{\binom{n+1}{k}}$ pro všechna $k = 0, 1, \ldots, n$. Určete $f(n+1)$.

**Úloha 3.** (těžká) Ať $F_i$ značí $i$-té Fibonacciho číslo, tedy $F_0 = 0$, $F_1 = 1$ a dále $F_{n+1} = F_n + F_{n-1}$. Pokud polynom $f$ stupně 990 splňuje $f(k) = F_k$ pro $k \in \{992, \ldots, 1982\}$, dokažte, že $f(1983) = F_{1983} - 1$. (IMO SL 1983)

### Koncepčnější pohled, aneb modulení polynomů

Pokusme se okopírovat principy modulární aritmetiky na počítání s polynomy. Pro jednoduchost uvažujme jako modulo nějaký monický lineární polynom $x - a$ a pracujme nad $\mathbb{R}$. Je-li dán reálný polynom $f$, co se s ním stane modulo $x - a$? Inu, ta nejprvotnější kongruence, co by modulo $x - a$ měla platit, je $x - a \equiv 0$, neboli $x \equiv a$. Jelikož polynom je jen výraz poskládaný ze sčítání a násobení, kterážto operace by modulární aritmetika měla respektovat, dostaneme $f = f(x) \equiv f(a)$. Jinými slovy, modulo $x - a$ je polynom $f$ kongruentní své hodnotě $f(a)$, takže v Lagrangeově interpolaci můžeme každou podmínku $f(x_i) = y_i$ přeložit jako $f \equiv y_i \pmod{x - x_i}$.

Máme tedy neznámou $f$, o které máme jen nějaké informace v několika různých modulech – bystří mohou větřit Čínskou zbytkovou větu. V okruhu $\mathbb{R}[x]$ polynomů nad $\mathbb{R}$ jsou naštěstí polynomy $x - a$, $x - a'$ pro $a \neq a'$ nesoudělné, takže v duchu Čínské zbytkové věty se sada podmínek v nesoudělných modulech $x - x_i$ má přeložit do jedné podmínky modulo $(x - x_0) \cdots (x - x_n)$. Už zbývá jen zpozorovat, že v každé takové zbytkové třídě je právě jeden polynom stupně nanejvýš $n$. Základní forma Lagrangeovy interpolace pak jen říká, že když má polynom splňující tyto podmínky navíc ještě malý stupeň, musí se jednat o tohoto unikátního reprezentanta. Nic nám však nebrání si ponechat volnější výsledek i pro $f$ libovolného stupně:

**Věta.** (Lagrangeova interpolace trochu obecněji) *Jsou-li $x_0, x_1, \ldots, x_n \in \mathbb{R}$ navzájem různá a $y_0, y_1, \ldots, y_n \in \mathbb{R}$ libovolná a $g$ je Lagrangeův interpolační polynom skrz body $(x_0, y_0), (x_1, x_2), \ldots, (x_n, y_n)$, pak libovolný reálný polynom $f$ (bez omezení stupně) splňuje $f(x_i) = y_i$ pro všechna $i \in \{0, 1, \ldots, n\}$, právě když*

$$f = g + q \cdot \prod_{i=0}^{n} (x - x_i)$$

*pro nějaký reálný polynom $q$.*

### Koeficienty

**Tvrzení.** *Je-li $f$ polynom stupně nanejvýš $n$ a $x_0, x_1, \ldots, x_n \in \mathbb{R}$ navzájem různá, pak je*

$$\sum_{i=0}^{n} \frac{f(x_i)}{\prod_{j \neq i} (x_i - x_j)}$$

*rovno koeficientu u $x^n$ v $f$.*

**Úloha 4.** Buď $a_n$ koeficient u $x^n$ v reálném polynomu $f$ stupně nanejvýš $n$. Dokažte, že potom platí

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

**Úloha 5.** Buď $f$ polynom s celočíselnými koeficienty stupně $d$ a buď $p$ prvočíslo. Dokažte, že pokud $f(0) = 0$, $f(1) = 1$ a pro každé $n \in \mathbb{N}$ dává $f(n)$ po dělení $p$ zbytek 0 nebo 1, potom $d \geq p - 1$. (IMO SL 1997)

### Nerovnosti

**Idea.** Vezmeme libovolný „Lagrangeovský výraz“, který se dosud objevil v příspěvku, a plácneme na něj absolutní hodnoty a trojúhelníkovou nerovnost.

**Úloha 6.** Reálný polynom $f$ stupně nanejvýš $n$ splňuje na intervalu $\langle 0, 1\rangle$ nerovnost $|f(x)| \leq 1$. Dokažte, že $|f(-1/n)| \leq 2^{n+1} - 1$.

**Úloha 7.** Je dán monický reálný polynom $f$ a celá čísla $x_0 < x_1 < \cdots < x_n$. Dokažte, že pro nějaké $0 \leq i \leq n$ nastane $|f(x_i)| \geq \frac{n!}{2^n}$. (Crux Mathematicorum)

### Úlohy na procvičení

**Úloha 8.** Buď $F : \mathbb{Z}_p \to \mathbb{Z}_p$ zcela libovolná funkce. Nahlédněte, že ji lze zapsat polynomem s koeficienty ze $\mathbb{Z}_p$.

**Úloha 9.** (sdílení tajemství) Voldemutovým nejstřeženějším tajemstvím je reálné číslo $r$. Chtěl by navrhnout systém, ve kterém každému ze svých $n$ smrtijedomutů sdělí nějakou informaci tak, aby

(i) dovedlo libovolných 7 smrtijedomutů spojit své informace a zjistit z nich $r$,
(ii) ale libovolných 6 nebo méně smrtijedomutů nedovedlo ze svých informací zjistit o $r$ vůbec nic (např. ani žádný omezený interval, v němž musí $r$ ležet).

Poraďte Voldemutovi, jak toho docílit. Dovede ve vašem systému Voldemut přidávat nové smrtijedomuty, aniž by cokoliv nového říkal starším smrtijedomutům?

**Úloha 10.** Reálný polynom $f$ stupně nanejvýš $n$ nabývá celočíselných hodnot v bodech $0, 1, \ldots, n$. Nahlédněte, že potom už musí nabývat celočíselných hodnot na celém $\mathbb{Z}$.

**Úloha 11.** Dokažte, že pro navzájem různá $x_0, x_1, \ldots, x_n \in \mathbb{R}$ platí

$$\sum_{i=0}^{n} \frac{x_i^{n+1}}{\prod_{j\neq i}(x_i - x_j)} = \sum_{i=0}^{n} x_i.$$

**Úloha 12.** Dokažte, že každý monický reálný polynom stupně $n$ lze zapsat jako aritmetický průměr dvou reálných polynomů stupně $n$, z nichž každý má $n$ různých reálných kořenů. (USAMO 2002)

**Úloha 13.** Mějme celé číslo $n \geq 3$ a reálné polynomy $f$, $g$ takové, že body $(f(i), g(i))$ pro $i = 1, \ldots, n$ jsou vrcholy pravidelného $n$-úhelníku v rovině (čtené v kladném směru). Dokažte, že alespoň jeden z $f$, $g$ má stupeň alespoň $n - 1$. (Putnam 2008)

**Úloha 14.** Dokažte, že platí $\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}k^{n+1} = \frac{(n+1)!n}{2}$.

**Úloha 15.** (těžká) Dokažte, že pro každý monický polynom $f$ s komplexními koeficienty existuje komplexní číslo $z$ splňující $|z| = 1$ a zároveň $|f(z)| \geq 1$.

**Úloha 16.** (těžká) Reálný polynom $f$ stupně nanejvýš 2020 splňuje $f(k^2) = k$ pro $k = 0, 1, \ldots, 2020$. Určete $f(2021^2)$. (HMMT 2020)

### Návody

**1.** Dosaď do interpolačního polynomu a uprav směrem k binomické větě.

**2.** V interpolačním polynomu zmizí kombinační čísla.

**3.** Využij, že $F_n = \frac{1}{\sqrt{5}}\big(\varphi^n - (\overline{\varphi})^n\big)$, kde $\varphi = \frac{1+\sqrt{5}}{2}$, $\overline{\varphi} = \frac{1-\sqrt{5}}{2}$. Rozděl sumu, ke které se prointerpoluješ, na část s $\varphi$ a $\overline{\varphi}$.

**4.** Hodnoty $f$ v kterých bodech se tu objevují? Takže skrz co asi chceš interpolovat?

**5.** Interpoluj nad $\mathbb{Z}_p$ a vyjádři koeficient u $x^{p-1}$.

**6.** Interpoluj skrz $x_i = \frac{i}{n}$.

**7.** Využij celočíselnost k odhadu $\prod_{i\neq j}|x_i - x_j|$.

**8.** Interpoluj skrz všechny body.

**9.** Sděl smrtijedomutům hodnoty polynomu v bodech.

**10.** Interpretuj každý člen v interpolačním polynomu pomocí kombinačních čísel.

**11.** Čteš koeficient, ale stupeň je moc velký – zmodul.

**12.** Jeden polynom zinterpoluj tak, aby byl hooodně rozkmitaný, druhý dopočítej tak, aby vyšel průměr.

**13.** Interpoluj jeden komplexní polynom. Vhodné BÚNO situaci zjednoduší.

**14.** Interpoluj $f(x) = x^n$, ale dívej se na koeficient u $x^{n-1}$.

**15.** Použij kořeny $x^{n+1} - 1$. Výraz $\prod_{i\neq j}(x_i - x_j)$ je hodnota derivace v kořenu!

**16.** Interpolace dá děsivou sumu, ale jde to ubít. $\sum_{k=0}^{m}(-1)^k\binom{n}{k}$ jde spočítat!

### Literatura a zdroje

Tento příspěvek je z většiny založen na *i*KSkové přednášce Kuy Löwita, kterému tímto děkuji. Dále jsem některé úlohy přezval z obecnějších příspěvků o polynomech.


[1] Jakub Löwit: *Lagrangeova interpolace*, sborník *i*KS, 2018.

[2] Titu Andreescu, Gabriel Dospinescu: *Problems from the Book*, XYZ Press, 2008.

[3] Filip Sládek: *Aritmetické vlastnosti polynómov*, sborník *i*KS, 2013.

[4] Martin „E.T.“ Sýkora: *Polynomy bez Viètových vztahů*, Hojsova Stráž, 2016.

# Konečná tělesa a kde je najít

Matěj Doležálek

Abstrakt. Počítat modulo prvočíslo je fajn: skoro všechno má multiplikativní inverz a platí zde spousta užitečných větiček. V tomto příspěvku tyto poznatky zobecníme do pojmu *konečného tělesa* a ukážeme, že ač musíme některé exempláře hledat v exotických místech, stojí to za to. Standardní vysokoškolskou teorii odložíme na závěr, namísto toho se budeme co nejvíce věnovat olympiádním aplikacím.

**Definice.** *Těleso* je struktura, ve které máme význačné prvky 0, 1 (navzájem různé) a umíme sčítat, odečítat, násobit a nenulovými prvky také dělit za platnosti všech obvyklých pravidel. *Konečné těleso* je těleso, které má jen konečné mnoho prvků.

**Úmluva.** Je-li $F$ (konečné) těleso, nechť $F^\times$ značí množinu jeho nenulových prvků.

### Příklady a základní vlastnosti

**Příklad.** Pro prvočíslo $p$ tvoří celá čísla modulo $p$ konečné těleso $\mathbb{Z}_p$ s $p$ prvky. Abychom zdůraznili, že se jedná o tělesa, budeme je v tomto příspěvku značit $\mathbb{F}_p$.

**Příklad.** Je-li $n = ab$ složené číslo, kde $a, b > 1$, pak $\mathbb{Z}_n$ není těleso, např. protože (nenulovými) prvky $a$, $b$ nelze dělit.

**Příklad.** Položme $F = \{0, 1, \alpha, \beta\}$ a předepišme na této množině sčítání a násobení následovně:

| $+$ | $0$ | $1$ | $\alpha$ | $\beta$ |
|---|---|---|---|---|
| $0$ | $0$ | $1$ | $\alpha$ | $\beta$ |
| $1$ | $1$ | $0$ | $\beta$ | $\alpha$ |
| $\alpha$ | $\alpha$ | $\beta$ | $0$ | $1$ |
| $\beta$ | $\beta$ | $\alpha$ | $1$ | $0$ |

| $\cdot$ | $0$ | $1$ | $\alpha$ | $\beta$ |
|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $\alpha$ | $\beta$ |
| $\alpha$ | $0$ | $\alpha$ | $\beta$ | $1$ |
| $\beta$ | $0$ | $\beta$ | $1$ | $\alpha$ |

Všimněte si, že $F$ je čtyřprvkové těleso. Zdůrazněme, že je zcela odlišné od $\mathbb{Z}_4$, což koneckonců ani není těleso.

**Pozorování.** *Pro každé $a \in F^\times$ je zobrazení $b \mapsto ab$ bijekcí $F^\times \to F^\times$.*

**Věta.** (malý Fermat) *V konečném tělese o $n$ prvcích splňuje libovolné $a \in F^\times$ rovnost $a^{n-1} = 1$.*

**Důsledek.** *Nad konečným tělesem $F$ o $n$ prvcích platí rovnost polynomů*

$$x^n - x = \prod_{a \in F} (x - a).$$

**Cvičení.** (Wilsonova věta) Součin všech prvků konečného tělesa je roven $-1$.

**Úloha 1.** Najděte všechna přirozená čísla nesoudělná se všemi členy posloupnosti zadané předpisem $a_n = 2^n + 3^n + 6^n - 1$.

**Definice.** *Charakteristikou* konečného tělesa $F$ míníme nejmenší přirozené číslo $c$, pro něž je v $F$ součet $c$ jedniček roven nule.

**Cvičení.** Charakteristika konečného tělesa musí být prvočíslo.

**Tvrzení.** *Konečné těleso $F$ charakteristiky $p$ musí mít přesně $p^k$ prvků pro nějaké přirozené $k$.*

*Důkaz.* $F$ je vektorový prostor nad $\mathbb{Z}_p$ a musí mít konečnou dimenzi. □

**Cvičení.** (Frobeniův automorfismus) Buď $F$ konečné těleso charakteristiky $p$. Potom je zobrazení $\varphi : F \to F$ definované předpisem $\varphi(x) = x^p$ bijekce, která zachovává sčítání i násobení, tj. $\varphi(xy) = \varphi(x)\varphi(y)$ a $\varphi(x + y) = \varphi(x) + \varphi(y)$.

### Řády a primitivní prvek

**Definice.** Buď $F$ konečné těleso. *Řádem* prvku $a \in F^\times$ rozumíme nejmenší přirozené $r$ takové, že $a^r = 1$. Značíme $r = \mathrm{ord}_F(a)$.

Pokud je z kontextu zřejmé, v jakém konečném tělese pracujeme, dovolíme si index $F$ vypustit.

**Tvrzení.** *Pro $a \in F^\times$ platí $a^e = 1$, právě když* $\mathrm{ord}(a) \mid e$.

**Důsledek.** *Je-li $F$ těleso s $n$ prvky, pak pro každé $a \in F^\times$ platí* $\mathrm{ord}(a) \mid n - 1$.

**Úloha 2.** V $n$-prvkovém tělese nenulová $a$, $b$ splňují $a^{2^s} + b^{2^s} = 0$. Dokažte, že $n \equiv 1 \pmod{2^{s+1}}$.

**Úloha 3.** Je dáno prvočíslo $p$. Dokažte, že existuje nekonečně mnoho prvočísel $q \equiv 1 \pmod{p}$.

Častým začátečnickým omylem kolem malé Fermatovy věty je předpokládat, že $a^e = 1$, právě když $n - 1 \mid e$ (co to říká o řádu $a$?). To obecně neplatí, triviálním protipříkladem je třeba $a = 1$. Nicméně ta $a$, která tuto vlastnost mají, jsou význačná a umíme o nich něco říct.

**Definice.** *Primitivním prvkem* v $n$-prvkovém tělese $F$ rozumíme takové $g \in F^\times$, že $\mathrm{ord}_F(g) = n - 1$

Jinými slovy: primitivní prvek je takové $g$, že $F^\times = \{g, g^2, \dots, g^{n-1}\}$. Primitivní prvek není ani zdaleka určen jednoznačně – např. když je primitivním prvkem $g$, musí jím být také $\frac{1}{g}$.

**Věta.** *V každém konečném tělese existuje primitivní prvek.*

Důkaz uvaříme z trojice lemmat. Ve všech nechť je $F$ konečné těleso s $n$ prvky.

**Lemma A.** *Pokud* $\ell \mid \operatorname{ord}(a)$, *pak* $\operatorname{ord}(a^\ell) = \frac{1}{\ell}\operatorname{ord}(a)$.

**Lemma B.** *Pokud* $r = \operatorname{ord}(a)$, $s = \operatorname{ord}(b)$ *a zároveň jsou* $r$, $s$ *nesoudělná, pak* $\operatorname{ord}(ab) = rs$.

**Lemma C.** *V tělese má nenulový polynom stupně* $d$ *nanejvýš* $d$ *různých kořenů.*

#### Využití primitivního prvku

**Cvičení.** Nahlédni, že zobrazení $a \mapsto a^m$ je v $n$-prvkovém tělese bijektivní, právě když je $m$ nesoudělné s $n-1$.

**Úloha 4.** Buď $F$ těleso s $p^k$ prvky. V závislosti na přirozeném čísle $e$ určete

$$\sum_{a \in F} a^e.$$

**Úloha 5.** Rozhodni, zda lze tabulku $10 \times 10$ vyplnit čísly $1, 2, \dots, 100$ a zvolit $A, B \in \mathbb{Z}_{101}$ tak, aby současně platilo:

(i) Součin prvků libovolného řádku dává po dělení 101 zbytek $A$.
(ii) Součet prvků libovolného sloupce dává po dělení 101 zbytek $B$.

**Definice.** *Multiplikativní množinou*[1] v konečném tělese $F$ budeme rozumět neprázdnou podmnožinu $M \subseteq F^\times$, která je uzavřená na násobení, tedy splňuje $ab \in M$ pro libovolná $a, b \in M$.

**Příklad.** Mějme $n$-prvkové těleso $F$ a uvažujme jisté $e \mid n-1$. Potom je

$$M_e = \{a^e \mid a \in F^\times\}$$

multiplikativní množina v $F$ s $\frac{n-1}{e}$ prvky. Navíc platí $b \in M_e \iff b^{\frac{n-1}{e}} = 1$.

**Tvrzení.** *Každá multiplikativní množina v konečném tělese* $F$ *je tvaru* $M_e$ *pro nějaké* $e \mid n-1$. *Z toho speciálně plyne, že multiplikativní množina je jednoznačně určena svou velikostí.*

**Cvičení.** (kvadratické zbytky) Buď $F$ konečné těleso liché charakteristiky s $n$ prvky. Kolik prvků $F^\times$ má v $F$ druhou odmocninu? Jak se tyto prvky poznají?

[1] Fajnšmekři mohou multiplikativním množinám říkat *podgrupy* (multiplikativní) *grupy* $F^\times$. My tu však do grup zabíhat nechceme, proto se tomuto – možná správnějšímu – označení vyhneme.

### Konečná tělesa ve volné přírodě

Doposud by si z tohoto příspěvku mohl vážený čtenář odnést dojem, že konečná tělesa jsou vlastně jen $\mathbb{Z}_p$ a možná tu a tam nějaký náhodný exemplář jako čtyřprvkové těleso a že pro potřeby olympiádního uplatnění jsou konečná tělesa jen kosmetickou omáčkou k obyčejné modulární aritmetice celých čísel. Zde si dovolíme drahého čtenáře vyvést z těchto hypotetických omylů. Na přednášce bohužel není prostor vše, co zde řekneme, podložit důkazy – laskavý čtenář je snažně žádán, aby to autorovi odpustil.

**Úmluva.** Když k něčemu připíšeme „$[\alpha]$“, znamená to „přidej $\alpha$ a uzavři na sčítání a násobení“. Připíšeme-li „$/(m)$“, znamená to „dívej se modulo $m$“. V tomto značení tedy např. $\mathbb{C} = \mathbb{R}[i]$, $\mathbb{F}_p = \mathbb{Z}/(p)$.

**Příklad.** (Gaussovská čísla) $\mathbb{Z}[i]$ je obor tvořený těmi komplexními čísly $a + bi$, kde $a, b \in \mathbb{Z}$. S využitím imaginární jednotky lze na součin rozložit i některá čísla, u kterých to v $\mathbb{Z}$ nešlo, např. $5 = (2+i)(2-i)$. Modulením zjistíme, že můžeme potkat staré známé v novém hávu, např. $\mathbb{Z}[i]/(2-i)$ je pětiprvkové těleso, které se nijak podstatně neliší od standardního $\mathbb{Z}/(5)$. Podobně se na součin dvou „Gaussovských prvočísel“ rozkládají všechna prvočísla $p \equiv 1 \pmod 4$ (důkaz je netriviální).

Naproti tomu prvočísla $p \equiv 3 \pmod 4$ zůstávají prvočiniteli i v $\mathbb{Z}[i]$, takže při modulení nimi dostaneme tělesa s $p^2$ prvky. Jelikož $\mathbb{Z}$ bydlí uvnitř $\mathbb{Z}[i]$, i po zmodulení budeme mít přirozeně vnořenou kopii $\mathbb{F}_p = \mathbb{Z}/(p)$ uvnitř $\mathbb{Z}[i]/(p)$. Alternativně se na věc taky můžeme dívat tak, že polynom $x^2 + 1$ neměl v $\mathbb{F}_p$ kořen, tak jsme mu ho přidali pod jménem $i$ a získali tak $\mathbb{F}_p[i]$.

Poznamejme též, že v $\mathbb{Z}[i]$ shodou šťastných okolností funguje jednoznačný rozklad na (Gaussovské) prvočinitele, podobně jako v $\mathbb{Z}$.

**Cvičení.** Najděte nějaký primitivní prvek v $\mathbb{Z}[i]/(3)$.

**Příklad.** (zlatý řez a Fibonacciho čísla) Označme jako $\varphi = \frac{1+\sqrt{5}}{2}$ jeden z kořenů polynomu $x^2 - x - 1$, tzv. *zlatý řez*. Druhým kořenem je $1 - \varphi$. Oba kořeny se hodí k explicitnímu vyjádření Fibonacciho čísel (definovaných pomocí $F_0 = 0$, $F_1 = 1$, $F_{n+1} = F_n + F_{n-1}$), jelikož $F_n = \frac{1}{\sqrt{5}}(\varphi^n - (1-\varphi)^n)$. Aritmetické vlastnosti Fibonacciho čísel proto může pomoci osvětlit pohled v $\mathbb{Z}[\varphi]$. Opět platí, že některá prvočísla se najednou dají rozložit, zatímco jiná nikoliv – ta potom modulením dávají $p^2$-prvková tělesa.

Dokonce platí, že prvočíslo $p$ zůstává prvočinitelem i v $\mathbb{Z}[\varphi]$ právě tehdy, když polynom $x^2 - x - 1$ nelze nad $\mathbb{F}_p$ rozložit na součin dvou lineárních polynomů. Proto např. $\mathbb{Z}[\varphi]/(2) = \mathbb{F}_2[\varphi]$ je čtyřprvkové těleso. Když pojmenujeme třeba $\alpha = \varphi$, $\beta = \varphi + 1$, zjistíme, že se jedná přesně o čtyřprvkové těleso z příkladu na začátku přednášky. Náhodička, hm?

**Příklad.** (obecněji) Kdykoliv si vezmeme kořen $\alpha$ ireducibilního monického polynomu $f(x)$ s celočíselnými koeficienty, můžeme se dívat na obor $\mathbb{Z}[\alpha]$. Ten se může chovat v mnoha ohledech zrádně, např. v něm často nebude fungovat jednoznačný rozklad na prvočinitele, ale kdykoliv si vezmeme prvočíslo $p$ takové, že $f(x)$ zůstává ireducibilním i nad $\mathbb{F}_p$, pak bude $\mathbb{Z}[\alpha]/(p) = \mathbb{F}_p[\alpha]$ těleso s $p^{\deg f}$ prvky.

**Úloha 6.** Nahlédněte, že pro prvočíslo $p \equiv 3 \pmod 4$ se Frobeniův automorfismus v konečném tělese $\mathbb{Z}[i]/(p) = \mathbb{F}_p[i]$ shoduje s komplexním sdružením.

**Úloha 7.** Buď $p \neq 5$ prvočíslo. Dokažte, že potom $p$-té Fibonacciho číslo dává po dělení $p$ zbytek $\pm 1$. Od čeho se znaménko odvíjí?

**Úloha 8.** Buď $p \equiv 3 \pmod 4$ prvočíslo a nechť celá čísla $a$, $b$ splňují $a^2 + b^2 \equiv 1 \pmod p$. Nahlédněte, že potom lze $a + bi$ modulo $p$ vyjádřit ve tvaru $(c + di)^{p-1}$ pro jistá $c, d \in \mathbb{F}_p$.

**Úloha 9.** Najděte periodu posloupnosti zbytků Fibonacciho čísel modulo 127.
(HMMT 2017)

**Úloha 10.** (těžká) Buď posloupnost nezáporných celých čísel zadána pomocí $a_0 = 2$ a $a_{k+1} = 2a_k^2 - 1$. Dokažte, že když liché prvočíslo $p$ dělí nějaké $a_n$, pak $p \equiv \pm 1 \pmod{2^{n+2}}$. Bonus: na čem závisí znaménko?

**Úloha 11.** (těžká) Je dáno přirozené číslo $k$ takové, že $p = 4k-1$ je prvočíslo. Dále jsou dána po dvou nesoudělná $x$, $y$, $z$ tak, že $x^2+y^2 = z^k$. Dokažte, že $p \mid xy(x^2-y^2)$.
(PraSe 40–2s–3)

#### Standardní konstrukce a klasifikace konečných těles

Závěrem se sluší trochu poodkrýt vysokoškolskou oponu a říci, co se tu „děje doopravdy“.

**Cvičení.** Dejme tomu, že jsme v tělese charakteristiky $p$ a podíváme se na množinu $S$ všech kořenů polynomu $x^{p^k} - x$. Nahlédněte, že $S$ tvoří podtěleso (obsahuje 0, 1, je uzavřená na základní operace a dá se v ní dělit).

**Definice.** Buď $K$ těleso a $f$ nekonstantní polynom s koeficienty z $K$. Těleso $L \supset K$ nazveme *rozkladovým nadtělesem $f$ nad $K$*, pokud lze $f$ nad $L$ rozložit na součin lineárních polynomů a zároveň pro kořeny $\alpha_1, \ldots, \alpha_n \in L$ polynomu $f$ platí $L = K[\alpha_1, \ldots, \alpha_n]$.

**Tvrzení.** *Ke každému nekonstantnímu polynomu nad tělesem existuje rozkladové nadtěleso a všechna taková rozkladová nadtělesa jsou si navzájem izomorfní – liší se jen tím, že jim někdo přejmenoval prvky, ale jejich „skutečná“ struktura je stejná.*

**Věta.** (velká) *Pro každé prvočíslo $p$ a přirozené $k$ existuje až na izomorfismus právě jedno $p^k$-prvkové těleso: je to rozkladové nadtěleso polynomu $x^{p^k} - x$ nad $\mathbb{F}_p$ a značíme ho $\mathbb{F}_{p^k}$. Jiná konečná tělesa neexistují a platí $\mathbb{F}_{p^\ell} \subseteq \mathbb{F}_{p^k}$, právě když $\ell \mid k$.*

**Úloha 12.** Určete, kolik prvků $\alpha$ tělesa $\mathbb{F}_{2^{10}}$ splňuje $\mathbb{F}_{2^{10}} = \mathbb{F}_2[\alpha]$.

## Návody

**1.** $\frac{1}{2}+\frac{1}{3}+\frac{1}{6}=1$.

**2.** Podmínka ekvivalentně říká, že $-1$ je $2^s$-tá mocnina. Co pak může být řád základu této mocniny?

**3.** $\frac{p^p-1}{p-1}$.

**4.** Primitivní prvek dá geometrickou řadu. Alternativně se i bez primitivního prvku dá postupovat přímo z důsledku malého Fermata – je to mnohem techničtější, ale taky poučné.

**5.** Jak že se tahle kapitolka jmenuje?

**6.** Nezapomeň, že Frobenius funguje dobře i se sčítáním.

**7.** Pracuj v $\mathbb{F}_p$ anebo $\mathbb{F}_p[\varphi]$, kde $\varphi$ je zlatý řez. Frobenius pomůže.

**8.** Podmínka $a^2+b^2\equiv 1$ určuje multiplikativní množinu v $\mathbb{F}_p[i]$.

**9.** Ekvivalentně chceš najít řád $\varphi$ v konečném tělese $\mathbb{Z}[\varphi]/(127)$ (ověř si, že $x^2-x-1$ skutečně nemá kořen v $\mathbb{F}_{127}$). Frobenius je tvůj kamarád.

**10.** $a_k=\frac{1}{2}\left(\omega^{2^k}+\omega^{-2^k}\right)$, kde $\omega=2+\sqrt{3}$. Rozliš případy podle toho, zda $\sqrt{3}$ existuje v $\mathbb{F}_p$. Až ti někde bude chybět jedna dvojka, uvědom si, že $\omega$ je v příslušném konečném tělese čtverec.

**11.** S pomocí jednoznačného prvočíselného rozkladu v $\mathbb{Z}[i]$ zjisti, že $x+yi$ je $k$-tá mocnina. Potom využij toho, že i podmínka $p\mid xy(x^2-y^2)$ určuje v $\mathbb{F}_p[i]$ multiplikativní množinu.

**12.** Spočítej, kolik prvků $\mathbb{F}_{2^{10}}$ neleží v žádném menším konečném tělese.

## Literatura a zdroje


[1] Fíla Čermák a Matěj Doležálek: *Teorie nejen čísel*, seriál MKS, 40. ročník.
[2] Pavel Turek: *Konečná tělesa*, Lysečiny, 2021.
[3] Alexander „Olin“ Slávik: *Konečná tělesa*, Uhelná Příbram, 2014.

# Prolog

Vojta Gaďurek

Abstrakt. Prolog patří do rodiny logických programovacích jazyků, ve kterých se programuje trochu jinak než v jazycích imperativních. Ukážeme si jak Prolog funguje, k čemu se hodí a k čemu se absolutně nehodí.

Prolog je logický programovací jazyk, který vznikl na začátku sedmdesátých let minulého století. Dnes je tedy už poněkud zastaralý a nového softwaru v něm již moc nevzniká. Neobsahuje tak třeba typy a podobné vymoženosti, na které jsme z dobrých jazyků zvyklí. Pokud by vás Prolog zaujal, dá se najít i jeho novější varianta v podobě jazyka *Mercury*.

Než se ale vrhneme do samotného jazyka, je důležité si vybudovat nějaké ty teoretické základy.

## Relace

Relace jsou základem logického programování. Co to ale taková relace je? Jak si je můžeme představit?

**Příklad.** (Ilustrační) V příspěvku se nejednou setkáme s prasátky Šunkou, Krkovičkou, Guláškem a Kotletkou. Jednotlivá prasátka do sebe mohou být zamilována, jak je ale všeobecně známo, láska nemusí být vzájemná. Tedy pokud Šunka je zamilována do Krkovičky, nemusí být Krkovička zamilována do Šunky.

Relaci si pak můžeme představit jako seznam, kde jsou napsány všechny tyto vztahy. Vypadá třeba následovně:

- Krkovička je zamilována do Šunky
- Gulášek je zamilován do Šunky
- Šunka je zamilovaná do Krkovičky
- Šunka je zamilovaná do Kotletky

Všimněme si, že věty v daném seznamu jsou zbytečně dlouhé a jediné, na čem záleží, je pořadí jmen. Seznam tak můžeme nahradit zápisem

$$\{(\text{Krkovička}, \text{Šunka}), (\text{Gulášek}, \text{Šunka}), (\text{Šunka}, \text{Krkovička}), (\text{Šunka}, \text{Kotletka})\}.$$

Nyní nadešel čas na formální definici:

**Definice.** (Kartézský součin) *Kartézským součinem množin* $A_1, A_2, \ldots, A_n$ rozumíme množinu všech $n$-tic $(a_1, \ldots, a_n)$, že $a_1 \in A_1, \ldots, a_n \in A_n$.

**Definice.** *Relací* rozumíme (libovolnou) podmnožinu kartézského součinu dvou nebo více množin. Pokud je $n$-tice $(a_1, a_2, \ldots, a_n)$ prvkem dané relace $R$, píšeme $R(a_1, a_2, \ldots, a_n)$ a čteme „$(a_1, a_2, \ldots, a_n)$ je v relaci $R$“.

**Příklad.** Nalezněte nejmenší množiny $A$ a $B$ takové, aby

$$R := \{(\text{Krkovička}, \text{Šunka}), (\text{Gulášek}, \text{Šunka}), (\text{Šunka}, \text{Krkovička}), (\text{Šunka}, \text{Kotletka})\}$$

byla relace nad $A \times B$.

*Řešení.* Všimneme si, že množina $A$ odpovídá prasátkům, která jsou do někoho zamilována, tedy prasátkům Krkovička, Gulášek a Šunka. Množina $B$ zase odpovídá prasátkům, která někdo miluje, tedy prasátkům Šunka, Krkovička a Kotletka.

### Indukce, rekurze, rekurzivní definování relace

Indukce[1] je velmi používaným nástrojem užívaným pro konstrukci matematických důkazů. Rekurze se indukci velice podobá – stejně jako ona má základní případ, ve kterém umíme problém snadno vyřešit, a pak má rekurzivní krok, který spočívá v rozdělování problémů do řešení menších případů.

**Příklad.** (Fibonacciho posloupnost) Zadefinujme si následující posloupnost:

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

Můžeme si všimnout, že posloupnost má dva základní případy. Kdybychom měli jenom jeden, třeba $F(1) = 1$, nebyla by hodnota $F(2)$ zřejmá, protože neznáme hodnotu $F(0)$; náš rekurzivní krok by se nikdy nezastavil.

Můžeme si také všimnout, že $F(x)$ je definovaná pouze pro přirozená $x$.

**Definice.** (Pipe) Nechť $A$ je množina a $n$ je přirozené číslo. Mějme $n$-tici funkcí $F = (f_1, f_2, \ldots, f_n)$, kde $f_i$ je funkce z množiny $A$ do $A$. Potom definujeme

$$\text{Pipe}(F, n) := f_1 \circ f_2 \circ \cdots \circ f_n.$$

Pokud je $n$-tice $F$ tvořena jen a pouze danou funkcí $f : A \to A$, můžeme zápis zkrátit na $\text{Pipe}(f, n)$.

Pomocí rekurze si umíme zavést i „přirozená čísla“ (označme je $\mathcal{N}$): budeme je reprezentovat pomocí funkce $\text{N} : \mathcal{N} \to \mathcal{N}$, která pro normální přirozené číslo $n$ vrátí $n$-té „přirozené číslo“.

Nejprve definujeme $\text{N}(0) = 0$. Zbylá čísla definujeme rekurzivně pomocí funkce $\text{Succ} : \mathcal{N} \to \mathcal{N}$, kde $\text{Succ} : \text{N}(n) \mapsto \text{N}(n+1)$.

**Příklad.** Čemu se rovná $\text{N}(4)$?

[1] Matematické indukci se věnoval např. seriál 41. ročníku PraSátka: *https://prase.cz/archive/41/serial.pdf*.

*Řešení.* $N(4) = \text{Succ}(\text{Succ}(\text{Succ}(\text{Succ}(0))))$.

Nyní bychom mohli chtít na těchto přirozených číslech definovat sčítání. Stejně jako umíme rekurzivně definovat posloupnosti nebo funkce, umíme tak definovat i relace. Sčítání si můžeme představit jako relaci tří čísel, která říká: „součtem prvních dvou čísel je třetí číslo“.

Chceme tedy definovat relační symbol $\text{plus}(a, b, c)$ na přirozených číslech, který je v relaci právě tehdy, pokud $a + b = c$.

Začněme jednoduchým případem, kde požadujeme, aby pokud $a + 0 = c$, pak $a = c$, můžeme tedy definovat $\text{plus}(a, 0, a)$.

Dále v rekurzivním kroku definujme, že $\text{plus}(a, b, c)$ jsou v relaci, právě když $a = \text{Succ}(d)$ a zároveň $\text{plus}(\text{Succ}(a), d, c)$.

**Příklad.** Ověřte, že takto definovaná relace plus se chová přesně tak, jak bychom od sčítání očekávali.

**Příklad.** Zkuste definovat relační symboly $\text{minus}(a, b, c)$ (platící pro $a - b = c$), $\text{krat}(a, b, c)$ (platící pro $a \cdot b = c$) a $\text{delitelne}(a, b)$ (platící pro $a \mid b$) nad námi definovanými „přirozenými čísly“.

### Síla a moc unifikace

Budeme pracovat s řetězci složených ze znaků a z proměnných, které budou ohraničené složenými závorkami.

**Definice.** (Dosazení za proměnnou) *Dosazením* řetězce $b$ za proměnnou $A$ v řetězci $a$ rozumíme, že všechny instance dané proměnné $A$ v řetězci $a$ nahradíme řetězcem $b$.

Nad těmito řetězci si můžeme definovat unifikaci dvou řetězců.

**Definice.** (Unifikace) Mějme nějaké tři řetězce $A$, $B$, $C$. Řetězec $C$ nazveme *unifikací* řetězců $A$ a $B$, pokud existuje dosazení do řetězců $A$, $B$ takové, že vznikne $C$.

**Příklad.** Unifikujte řetězce $A$ =„Moje jméno je {Jméno}“ a $B$ =„{Podmět} je {Předmět}“.

*Řešení.* Jejich unifikací je „Moje jméno je {X}“, přičemž jsme použili dosazení Jméno = „{X}“, Předmět = „{X}“, Podmět = „Moje jméno“.

**Příklad.** Je „Moje jméno je Karel“ unifikací řetězců $A$, $B$ z předchozího příkladu?

*Řešení.* Ano, je. Funguje dosazení Jméno = „Karel“, Předmět = „Karel“, Podmět = „Moje jméno“.

**Úloha.** Existují nějaké tři řetězce, které jsou sobě navzájem unifikací?

**Příklad.** Unifikujte řetězce „A({A})“ a „A(a)B(c)“.

*Řešení.* Hledané dosazení A = „a)B(c“.

Může se nám stát, že dva řetězce unifikovat nejdou, například „A{X}“ a „B{X}“. V takovém případě řekneme, že unifikace *selhala*.

Můžeme mít řetězec s dvěma výskyty jedné proměnné, např. „{Pole}{Pole}“. Pak pokud dosadíme Pole = „a“, dostaneme „aa“. Je však dobré si uvědomit, že proměnné v jiných řetězcích jsou na sobě nezávislé. Tedy unifikace „{X}{A}“ a „{A}{X}“ může být „{H}{Y}“.

Zavedeme si dva nové pojmy: *nejobecnější unifikaci* a *unifikaci zachovávající uzávorkování*. Ideou prvního je, že při unifikaci chceme ztratit co možná nejméně informaci, tj. dosadit do proměnných co nejméně znaků. Dokonce existuje algoritmus, který nám umožní získat tuto vždy unifikaci získat, v Prologu je pak implementován za nás.

**Definice.** (Nejobecnější unifikace) Mějme dva řetězce $A$ a $B$ a nechť $S$ je množina všech řetězců, které mohou vzniknout unifikací. *Nejobecnější unifikace* je taková unifikace, že všechny řetězce v $S$ lze získat dosazením do této unifikace.

Současná definice unifikace, viz příklad, nám umožňuje dosazovat tak, že nedodržujeme uzávorkování, unifikace zachovávající uzávorkování pak tento problém řeší zpřísněním, jinými slovy navíc požaduje,

(1) aby do proměnných šlo dosazovat nové závorky pouze pokud jsou uzavřené,
(2) a aby čárky bylo možné dosazovat, pouze pokud jsou v závorkách.

**Úmluva.** Nadále budeme uvažovat jen nejobecnější a závorkování zachovávající unifikace.

Je důležité si uvědomit, že unifikaci provádíme na formálních řetězcích a vůbec nás nezajímá, co ve skutečnosti znamenají. Obecně nás tedy zajímá syntaxe, ale ne sémantika.

**Příklad.** Unifikujte řetězce „A({A})“ a „A(a)B(c)“.

*Řešení.* Taková unifikace neexistuje.

### Plnou parou do Prologu

Nyní nadešel první čas na lekci Prologu. Prolog má hodně dialektů, ale v příspěvku budeme používat SWI-Prolog[2].

Otevřeme-li si danou stránku. Najdeme dvě okna, ve kterých lze psát. V levém píšeme samotný program (tedy to co platí) a v pravém píšeme dotazy.

Jako první si zkusíme napsat jednoduchý program, kterého se budeme dotazovat na to, zda nějaké prasátko miluje nějaké jiné.

```
miluje(krkovička, šunka).
miluje(gulášek, šunka).
miluje(šunka, krkovička).
miluje(šunka, kotletka).
```

[2]Online verzi naleznete na *swish.swi-prolog.org*.

Nyní už máme jednoduchý program, na který můžeme činit dotazy. Můžeme se například zeptat, zda Guláškovi se líbí Šunka.

(1) Zadáme-li dotaz `miluje(krkovička, šunka).`, dostaneme odpověď `true;`.
(2) Zadáme-li dotaz `miluje(krkovička, kotletka).`, dostaneme odpověď `false;`.

Ve stručnosti se podívejme na to, jak cca Prolog funguje. V Prologu relacím neříkáme relace, ale *predikáty*.

Pokud Prologu zadáme nějaký dotaz, třeba `miluje(krkovička, šunka).`, pokusí se ho splnit – tj. nalézt nějaký predikát v programu, se kterým se dokáže unifikovat. Pokud to zvládne, vypíše `true`, jinak `false`. Pokud jsme vložili dotaz s proměnnou, vrátí se dosazení do těchto proměnných, stane-li se tak, nevypíše se `true`. Může se vypsat více řešení a jako poslední vypsané řešení se vždy vypíše `false`.

Prolog zkouší unifikovat predikáty v pořadí, ve kterém jsme je do programu napsali. Dejme si pozor: proměnné v Prologu se píšou velkými písmeny a musí být odděleny mezerou, případně znakem, který není písmenem, třeba závorkami nebo čárkou.

Tedy můžeme mít následující predikát: `miluje(A, šunka).`

**Příklad.** Zamyslete se, co program vypíše, pokud mu zadáme dotaz

```
miluje(A,šunka).
```

*Řešení.*

```
miluje(krkovička, šunka).
miluje(gulášek, šunka).
```

### Rekurze v Prologu

V Prologu můžeme psát predikáty, které závisí na jiných predikátech. Můžeme třeba napsat predikát

```
milostný_kruh(A,B,C) :- miluje(A,B), miluje(B,C), miluje(C,A).
```

Čárka znamená logické *a*, zatímco středník logické *nebo*.

**Příklad.** Jak dopadne dotaz `milostný_kruh(krkovička, šunka, kotletka).`?

*Řešení.* Selže. Jako první se program pokusí splnit `miluje(krkovička, šunka)`, což se mu podaří. Poté se pokusí splnit `miluje(šunka, kotletka)`, což se mu též podaří. Nakonec se pokusí splnit `miluje(kotletka, šunka)`, ten ale nejde s unifikovat s žádným predikátem v programu. Tedy program selže.

Ve skutečnosti vyhodnocení funguje trochu jinak. Pokud se Prologu nepodaří nějaký predikát splnit, vrátí se o krok zpět, a tedy zkusí splnit predikát `miluje(šunka,`

`kotletka)`, ale jiným způsobem. Například pokud bychom měli dále napsaný predikát `miluje(šunka, A)`, tak se mu podaří unifikovat a pokračuje dál.

Zaveďme si symbol pro unifikaci v Prologu: „=“ (tj. píšeme $A = B$). Dejme si ale pozor, nejde o matematické „rovná se“, ani o programátorské dosazení! Prolog se pokusí $A = B$ unifikovat, a pokud se mu to podaří, dosadí výsledek této unifikace za obě proměnné.

V Prologu se v predikátu lze odkazovat i sám na sebe, jinými slovy máme k dispozici rekurzi. Můžeme proto definovat „přirozená čísla“:

```
succ(0).
succ(A) :- A = succ(B)
```

**Příklad.** (Definice sčítání v Prologu)

```
add(0,B,B).
add(A,B,C) :- A = succ(A'), add(A',succ(B), C).
```

### Úlohy

Následující úlohy jsou převzaty ze sbírky Ninety-Nine Prolog Problems. V úlohách se vám také bude hodit definice *listu*, kterou naleznete v dokumentaci SWI-Prologu.

**Úloha 1.** Najděte předposlední prvek listu.

**Úloha 2.** Zkuste otočit list.

**Úloha 3.** Napište predikát zjišťující, zda číslo je prvočíslo.

**Úloha 4.** Jste převozník a vezete kozu, vlka, zelí. Bez vaší přítomnosti koza sní zelí a vlk kozu. Vaším cílem je převézt všechny přes řeku, ale do bárky se kromě vás vejde vždy jen jedna další věc. Jak to uděláte? Zkuste navrhnout jak problém řešit v Prologu.

**Úloha 5.** Určitě znáte Einsteinovu hádanku. Jak byste takový problém řešili v Prologu?

**Úloha 6.** Navrhněte reprezentaci grafu v Prologu. Napište program v Prologu, kterému zadáte vrchol a on vám vrátí všechny kružnice, na kterých leží.

**Úloha 7.** Navrhněte solver sudoku.

### Literatura a zdroje


[1] Rudolf Kryl: *Skripta P* , *https://ksvi.mff.cuni.cz/~kryl/prolog.pdf*.

[2] Patrick Blackburn, Johan Boss, Kristina Striegnitz: *Learn Prolog Now*, *https://www.let.rug.nl/bos/lpn//*.

[3] Werner Hett: *Ninety-Nine Prolog Problems*, *https://www.ic.unicamp.br/~meidanis/courses/mc336/2009s2/prolog/problemas/*.

# Úvod do teorie grafů

Klárka Grinerová

Abstrakt. Tečky, čárky, ale morseovka to není. Jsou to grafy. Můžeme s jejich pomocí popsat dopravní síť nebo třeba rodokmen. Podíváme se, co jsou takové grafy zač a jaké druhy grafů můžeme potkat. Mrkneme také na nějaké jejich vlastnosti, budeme v grafech hledat cesty a kreslit tahy a konečně si pohrajeme se spoustou úložek.

## A co že je to ten graf?

Graf je velmi užitečná kombinatorická struktura, s jejíž pomocí můžeme snadno popsat velké množství problémů. Často nám grafy také mohou pomoct formulovat naše řešení nebo formálně popsat nějakou situaci. Pojďme se tedy společně podívat, co jsou grafy zač.

**Definice.** *Graf* $G$ je uspořádaná dvojice $G = (V, E)$, kde $V$ je neprázdná množina vrcholů a $E \subseteq \binom{V}{2}$ je množina hran.

**Definice.** Dva vrcholy $u$ a $v$ jsou *sousední*, pokud $\{u, v\} \in E$, tedy pokud mezi nimi vede hrana.

Grafům můžeme přiřadit mnoho dalších atributů – hrany můžeme orientovat, tedy udělat z nich šipku z jednoho vrcholu do druhého, můžeme jednotlivým vrcholům a hranám přiřazovat číselnou váhu nebo barvu. Můžeme také dovolit, aby hrana vedla z vrcholu zpátky do stejného vrcholu, tedy tvořila smyčku, nebo aby mezi dvěma vrcholy vedlo více hran. Takové grafy ale necháme na jindy, v této přednášce budeme grafem vždy myslet neprázdnou množinu vrcholů, kde mezi každou dvojicí vrcholů vede nejvýše jedna hrana a každá hrana vede mezi dvěma různými vrcholy.

**Definice.** O vrcholu $v$ řekneme, že má *stupeň* $\deg(v) = d$, pokud z něj vede právě $d$ hran.

**Definice.** Graf je *regulární*, pokud všechny jeho vrcholy mají stejný stupeň. Pokud má každý stupeň vrchol $d$, říkáme, že je graf *$d$-regulární*.

**Věta.** (Princip sudosti) $\sum_{v \in V} \deg(v) = 2 \cdot |E|$.

**Věta.** (Handshaking lemma) *Libovolný graf obsahuje sudý počet vrcholů lichého stupně.*

**Cvičení.** Ukažte, že $k$-regulární graf má sudé $k$ nebo $|V|$.

**Cvičení.** Ukažte, že pokud má $2k$-regulární graf sudý počet hran, tak buď $k$ nebo $|V|$ je sudé.

**Definice.** Pro graf $G = (V, E)$ nazveme $\overline{G} = (V, \overline{E})$ *doplněk grafu*, kde pro každou dvojici vrcholů $u, v$ platí $\{u, v\} \in E$, právě když $\{u, v\} \notin \overline{E}$.

**Definice.** Graf $G' = (V', E')$ se nazývá *podgrafem* $G = (V, E)$, pokud platí $V' \subseteq V$ a $E' \subseteq E$.

V běžné řeči tedy doplněk grafu obsahuje přesně ty hrany, které nebyly v původním grafu. Podgraf je potom původní graf, ze kterého jsme odebrali libovolný počet hran a vrcholů (jen platí, že pokud odebereme vrchol, odebereme také všechny hrany, ve kterých se tento vrchol vyskytoval).

**Definice.** *Cesta* v grafu je konečná posloupnost různých vrcholů taková, že mezi každými dvěma po sobě jdoucími vrcholy vede hrana. Pokud dovolíme na cestě opakování vrcholů, ale ne hran, dostáváme *tah*. Pokud dovolíme opakovat i hrany, dostáváme *sled*. Cesta, sled nebo tah jsou *uzavřené*, pokud je poslední vrchol zároveň prvním vrcholem.

**Cvičení.** Dokažte, že libovolné dvě nejdelší cesty v souvislém grafu mají společný vrchol.

### A jaké že grafy známe?

Aby se nám o grafech lépe mluvilo, podíváme se na některé jejich specifické typy a na vlastnosti takových grafů.

**Definice.** *Cyklus* nebo také *kružnice* je uzavřená cesta. Obvykle se značí jako $C_n$, kde $n$ je počet vrcholů.

**Definice.** O grafu řekneme, že je *klika* nebo že je *úplný*, pokud mezi každou dvojicí vrcholů vede hrana. Obvykle se značí $K_n$, kde $n$ je počet vrcholů.

**Definice.** Graf je *$n$-partitní*, pokud dokážeme jeho vrcholy rozdělit na $n$ disjunktních množin tak, že každá hrana vede mezi vrcholy v různých množinách. Pro $n = 2$ se graf nazývá *bipartitní*, pro $n = 3$ pak *tripartitní*.

**Definice.** *Úplný bipartitní* graf je takový graf, kde mezi každou dvojicí vrcholů z různých partit vede hrana.

**Cvičení.** Existuje bipartitní graf s alespoň 5 vrcholy, jehož doplněk je také bipartitní?

### A jak moc je takový graf souvislý?

V této části přednášky nás bude zajímat, jak těžké je nějaký graf rozdělit na víc částí. Nejprve ale něco málo ke značení. Graf $G \setminus v$ vznikne z grafu $G$ odebráním vrcholu $v$ a veškerých hran vedoucích do vrcholu $v$. Graf $G \setminus e$ vznikne z grafu $G$ odebráním hrany $e$.

**Definice.** Graf je *souvislý*, pokud mezi každými dvěma vrcholy existuje cesta. Souvislé části nesouvislého grafu se nazývají *komponenty souvislosti*.

**Cvičení.** Dokažte, že každý souvislý graf na $n \geq 3$ vrcholech obsahuje dva vrcholy $u$ a $v$ takové, že všechny tři grafy $G \setminus u$, $G \setminus v$ a $G \setminus \{u, v\}$ jsou souvislé.

**Definice.** *Hranová souvislost* grafu $\kappa_e(G)$ je minimální počet hran, po jejichž odebrání se graf $G$ stane nesouvislým. Graf je hranově $k$-souvislý, pokud $\kappa_e(G) \geq k$.

**Cvičení.** Je každý souvislý graf se sudými stupni hranově 2-souvislý?

**Definice.** *Vrcholová souvislost* grafu $\kappa_v(G)$ je minimální počet vrcholů, po jejichž odebrání se graf $G$ stane nesouvislým. Pokud $\kappa_v(G) \geq k$, graf je vrcholově $k$-souvislý.

**Cvičení.** Je každý souvislý graf se sudými stupni vrcholově 2-souvislý?

### A co nějaké zajímavé grafy?

Každý z nás se někdy nejspíš snažil nakreslit nějaký obrázek jedním tahem. Někdy se nám to podařilo, někdy ne a někdy se nám to ani podařit nemohlo.

**Definice.** Uzavřený tah je *eulerovský*, pokud obsahuje všechny hrany grafu a graf je *eulerovský*, pokud má uzavřený eulerovský tah.

V překladu to znamená, že graf je eulerovský, pokud jej můžeme nakreslit jedním tahem tak, že začneme a skončíme v jednom vrcholu. A dál se podíváme, jak snadno určit, že je graf eulerovský.

**Cvičení.** Ukažte, že každý graf, ve kterém mají všechny vrcholy stupeň alespoň 2, obsahuje kružnici.

**Cvičení.** Dokažte, že hrany každého eulerovského grafu lze rozložit na disjunktní sjednocení kružnic.

**Věta.** *Graf $G$ je eulerovský právě tehdy, když je souvislý a každý jeho vrchol má sudý stupeň.*

*Důkaz.* Pokud v grafu existuje eulerovský uzavřený tah, graf je určitě souvislý a každý jeho vrchol má sudý stupeň, jelikož libovolný výskyt vrcholu v tahu znamená, že do takového vrcholu po nějaké hraně vejdeme a po nějaké hraně odejdeme. Jinak máme graf $G$ s vrcholy sudých stupňů a ukážeme, že má eulerovský tah. Z předchozího cvičení víme, že graf lze rozložit na disjunktní kružnice. Takové kružnice pak můžeme díky souvislosti pospojovat do uzavřeného eulerovského tahu. □

### Úlohy

**Úloha 1.** Ukažte, že každý graf s $m$ hranami má bipartitní podgraf s alespoň $\frac{m}{2}$ hranami.

**Úloha 2.** Ukažte, že každý graf na alespoň 2 vrcholech má nejméně 2 vrcholy stejného stupně.

**Úloha 3.** Pro každá dvě přirozená čísla $k$, $n$ taková, že $k < n$ a součin $kn$ je sudý, najděte příklad $k$-regulárního grafu na $n$ vrcholech.

**Úloha 4.** Dokažte, že graf je bipartitní právě tehdy, když neobsahuje cyklus liché délky.

**Úloha 5.** Na seznamovačkách se účastníci rozdělí do šestičlenných týmů. Každí dva účastníci se buď navzájem znají, nebo neznají. Dokažte, že v každém týmu je trojice, kde se všichni 3 účastníci navzájem znají nebo se všichni 3 navzájem neznají.

**Úloha 6.** Máme graf na $n$ vrcholech, který má $k$ komponent. Určete nejmenší a největší možný počet hran tohoto grafu v závislosti na $k$ a $n$.

**Úloha 7.** Najděte příklad grafu $G$, ve kterém lze odebrat vrchol tak, že hranová souvislost $G$ vzroste o libovolně velké předem dané číslo.

**Úloha 8.** Najděte příklad grafu $G$, ve kterém lze odebrat vrchol tak, aby vrcholová souvislost $G$ vzrostla o libovolně velké předem dané číslo. O kolik může vrcholová souvislost klesnout po odebrání vrcholu?

**Úloha 9.** Ukažte, že pro každé $k \geq 2$ je každý $k$-regulární souvislý bipartitiní graf vrcholově 2-souvislý.

**Úloha 10.** Je pro $k \geq 2$ každý $k$-regulární souvislý graf vrcholově 2-souvislý?

**Úloha 11.** Pro libovolnou dvojici přirozených čísel $k$ a $\ell$, kde $\ell \leq k$, nalezněte graf $G$, který splňuje $\kappa_e(G) = k$ a $\kappa_v(G) = \ell$.

**Úloha 12.** Předpokládejme, že ve vesnici má každý člověk sudý počet přátel (přátelství je vzájemné). Každý může od svého přítele buď získat minci, nebo mu dát minci. Ukažte, že si můžou předat mince tak, aby každý měl na konci tolik, s kolika začínal.

**Úloha 13.** Určete, kolik kružnic obsahuje úplný graf na $n$ vrcholech.

**Úloha 14.** Na soustředění je $2n + 1$ účastníků. Pro každou podmnožinu nejvýše $n$ lidí najdeme účastníka mimo tuto podmnožinu, který zná všechny lidi v této podmnožině. Dokažte, že existuje člověk, který zná všechny ostatní.

## Návody

**1.** Rozděluj vrcholy do dvou skupin, aby se využila aspoň polovina hran.

**2.** Rozmysli si, jaké všechny stupně mohou být v grafu na $n$ vrcholech.

**3.** Najdi konstrukci pro sudá $k$, rozšiř pro lichá $k$.

**4.** Zkus hladově rozdělovat vrcholy do dvou partit.

**5.** Jeden účastník mezi zbylými 5 určitě alespoň 3 (ne)zná, podívej se na vztah mezi těmito třemi účastníky.

**6.** Uvaž každou komponentu. Kolik nejméně musí mít hran, aby byla souvislá, a kolik nejvýše může mít hran?

**7.** Uvaž, co se stane, pokud ke klice připojíš další vrchol jednou nebo více hranami.

**8.** Opět uvaž, co se stane, pokud ke klice připojíš další vrchol.

**9.** Pro spor uvaž bipartitní graf, který je 1-souvislý, a dokaž, že není regulární.

**10.** Najdi protipříklad, hledej konstrukci pro sudá $k > 2$ a poté pro lichá $k$.

**11.** Uvaž úplné grafy na $k + 1$ vrcholech.

**12.** Uvaž, co dělat s eulerovským tahem.

**13.** Spočítej kružnice jednotlivých délek.

**14.** Postupně přehazuj lidi ze dvou skupin a jednoho měj uprostřed a dívej se, co se děje.

## Literatura a zdroje

[1] Kuba Svoboda: *Tématické grafové úlohy*, Horní Lysečiny, 2018.
[2] *Sbírka řešených úloh*, *https://matematika.reseneulohy.cz/cs/matematika/kombinatorika*.

# Monovarianty

Vít Hanika

Abstrakt. Na přednášce budeme hledat monovarianty a algoritmy, při kterých je nějaká veličina monovariantem.

Monovariantem (česky poloměnkou) nazýváme veličinu, která se v čase mění pouze na jednu stranu, tj. buď stále klesá, a nebo stále stoupá. A pokud takovou veličinu najdeme a ukážeme, že takto může postupovat jen konečně dlouho, pak můžeme říct, že nějaký proces, který s tím monovariantem hýbe, musí časem skončit. Ukázka níže:

**Příklad.** V každém poli tabulky $n \times n$ je napsané celé číslo. V každém kroku můžeme změnit znaménka u všech čísel v některém řádku či sloupci. Ukažte, že lze dosáhnout stavu, kdy bude součet čísel v každém řádku a sloupci nezáporný.

*Řešení.* Všimneme si, že když změníme všechna znaménka v nějakém řádku či sloupci se záporným součtem, zvětší se součet čísel v celé tabulce, a to alespoň o 1. A protože součet celé tabulky může být jen omezeně velký, po konečném počtu kroků už nebudeme moci najít další záporný řádek ani sloupec.

## Úlohy

**Úloha 1.** Kámen rád cestuje, a tak vždy cestuje pouze do města nejvzdálenějšího od jeho aktuálního města. Pokud se ze svého druhého města nevrátil do počátečního, ukažte, že se tam nevrátí už nikdy.

**Úloha 2.** 2013 lidí je rozmístěno v 100 pokojích. Každou minutu někdo přejde z jedné místnosti do jiné, kde je alespoň tolik lidí jako v té původní. Ukažte, že v konečném čase budou všichni v jedné místnosti.

**Úloha 3.** V řadě je 100 mincí, na každé je buď panna nebo orlomut. Každý rok přijde Voldemut a otočí nějakou minci, na které je panna, a poté kolik chce mincí napravo od ní. Ukažte, že nehledě na to, jak hraje, budou v konečném čase na všech mincích orlomuti.

**Úloha 4.** Na několika políčkách nekonečného pásku je kladný počet žetonů. V každém kroku vezmeme dva žetony, které byly na stejném políčku, jeden posuneme o 1

pole směrem doprava a druhý o 1 doleva. Ukažte, že nikdy nemůžeme získat původní rozložení.

**Úloha 5.** V zemi s $n$ státy je každý stát buď monarchie nebo demokracie. Každý rok jedna ze zemí, která má více sousedů s jiným státním zřízením než se stejným, změní svoje státní zřízení. Ukažte, že takto mohou postupovat jen konečně mnoho let.

**Úloha 6.** V 123 místnostech je rozmístěno 1000 mužů a 1000 žen. Každou minutu přejde buď nějaká žena z místnosti s více ženami než muži do místnosti s více muži než ženami, nebo nějaký muž z místnosti s více muži než ženami do místnosti s více ženami než muži. Ukažte, že se časem nikdo nebude moci pohnout.

**Úloha 7.** Mějme graf s $v$ vrcholy a $e$ hranami. Ukažte, že existuje podgraf, který má stupeň každého vrcholu alespoň $\frac{e}{v}$.

**Úloha 8.** Vrcholy $n$-úhelníku jsou očíslované reálnými čísly. Nechť $a$, $b$, $c$, $d$ jsou 4 sousední čísla. Pokud $(a-d)(b-c) < 0$, můžeme vyměnit $b$ a $c$. Může být tato operace prováděna nekonečně dlouho?

**Úloha 9.** Mějme balíček s kartami očíslovanými $1, 2, \ldots, n$. Vždy, když je nahoře karta $k$, otočíme pořadí vrchních $k$ karet. Ukažte, že časem bude nahoře karta s číslem 1.

**Úloha 10.** Na tabuli je několik přirozených čísel. V jednom kroku můžeme vzít dvě čísla taková, že ani jedno není násobkem druhého, a nahradit je jejich největším společným dělitelem a nejmenším společným násobkem. Ukažte, že proces nemůže pokračovat do nekonečna. (St. Petersburg 1996)

**Úloha 11.** Mějme $n$ přepínačů v řadě. Každý je otočený buď na sever, západ, jih, nebo východ. Pokud tři po sobě jdoucí přepínače ukazují různými směry, můžeme je otočit do čtvrtého směru. Ukažte, že se proces zastaví. (BAMO 2006-5)

**Úloha 12.** (zdlouhavá) Mějme šestiúhelník s nezáporným celým číslem v každém vrcholu, přičemž součet všech šesti čísel je 2019. Kdykoliv můžeme nahradit některé z čísel absolutní hodnotou rozdílu čísel v sousedních vrcholech. Dokažte, že lze dosáhnout stavu, kdy jsou ve všech vrcholech nuly. (USAMO 2003)

**Úloha 13.** Fyzik objevil novou částici, *imon*, když jich pár našel ve své laboratoři. Některé dvojice *imonů* jsou spolu provázané. Fyzik se už s nimi naučil provádět dva druhy operací. Vždy umí provést jednu z následujících operací:

(1) Odebrat nějaký *imon* s lichým počtem sousedů.
(2) Zdvojnásobit počet *imonů* v laboratoři tak, že pro každý *imon I* vytvoří druhý *imon I'*, který je s ním provázaný a nově vzniklé *imony I'* a *J'* jsou provázané právě tehdy, pokud jejich originály *I* a *J* byly provázané.

Ukažte, že umí docílit stavu, kde nejsou žádné *imony* provázané.

(IMO Shortlist 2013)

**Úloha 14.** V nekonečné čtvercové mřížce si vybereme horizontální přímku a poté na políčka pod ni umístíme, kolik chceme kamenů, maximálně jeden na políčko. Kterýkoliv kámen může přeskočit jiný kámen, se kterým sousedí hranou, sebrat ho a skočit hned za něj. Ukažte, že v konečném počtu tahů se žádný kámen nedostane na páté políčko nad horizontální přímkou (aby mezi ním a přímkou byla 4 políčka).

### Hledané monovarianty

Zde jsou příklady monovariantů, kterými jdou úlohy rozlousknout. Rozhodně však nejsou jediné :).

**1.** Délka posledního uraženého úseku.

**2.** Součet čtverců počtu lidí v jednotlivých místnostech.

**3.** Posloupnost orlomutů a panen interpretovaná jako číslo ve dvojkové soustavě.

**4.** Součet vzdáleností všech dvojic žetonů.

**5.** Počet dvojic sousedních zemí, které mají stejné státní zřízení.

**6.** Rozdíly (v absolutních hodnotách) počtů mužů a žen v jednotlivých místnostech.

**7.** Zkus začít s celým grafem, odebírat vrcholy a sledovat $\frac{e}{v}$.

**8.** Součet čtverců rozdílů sousedních čísel.

**9.** Dvojková soustava, kde na pozici $i$ je jednička, právě když je $i$-tá karta odshora $i$.

**10.** Součet čísel na tabuli.

**11.** Součet $\sqrt{i}$ takových, že na pozicích $i$ a $i+1$ jsou stejně orientované přepínače (ve skutečnosti se dá mimo jiné použít jakákoliv konkávní kladná funkce, nejen odmocnina).

**12.** Maximum všech čísel (je ho potřeba trochu nutit do zmenšování se :)).

**13.** Chromatické číslo[1] grafu.

**14.** Každému políčku přiřaďte hodnotu $a^x$, kde $x$ je jeho manhattanská vzdálenost od cíleného políčka, a $a = \frac{\sqrt{5}-1}{2}$. Monovariant je součet hodnot všech políček, na kterých je kámen.

### Poděkování

Děkuji *Martinu Töpferovi*, z jehož příspěvku na soustředění v Mentaurově jsem přebral spoustu úloh.

### Literatura a zdroje

[1] Viki Němeček: *Monovarianty*, Paseky, 2018.
[2] Jenya Soprunova: *Advanced Problem Solving – Monovariants*, *https://www.math.kent.edu/~soprunova/64091f16/monovariants16.pdf*.

[1] Graf je $k$-obarvitelný, pokud jde obarvit $k$ barvami tak, aby žádné dva vrcholy stejné barvy nesousedily. Jeho chromatické číslo je nejmenší takové $k$.

# Hales–Jewett

Lenka Kopfová

Abstrakt. Asi každý už někdy narazil na hru Tic-tac-toe, která připomíná piškvorky na hrací ploše $3 \times 3$. Hra ale vždy skončí remízou, pokud hráči hrají optimálně, a tak nějak není moc zajímavá. Co by se ale stalo, pokud by hráči hráli na nějaké obecnější krychli větší dimenze a jejich společným cílem by bylo nikdy nevytvořit jednobarevnou přímku?

### Základní pojmy:

Označme si $A$ množinu celých čísel $\{0, 1, \ldots, a-1\}$. Její $k$-té kartézské mocnině $A^k$ budeme říkat $k$-rozměrná *krychle* nad $A$. Každý bod $x \in A^k$ pak můžeme popsat $k$-znakovým *řetězcem* nad abecedou $A$. Pokud do abecedy přidáme ještě symbol $*$ (*žolík*), můžeme se na řetězec $\alpha \in (A \cup \{*\})^k$ dívat jako na funkci $\alpha : A \to A^k$ takovou, že $\alpha(t)$ je slovo vzniklé ze slova $\alpha$ nahrazením všech výskytů hvězdičky hodnotou $t$. Takovému slovu (a také příslušné funkci) budeme říkat *šablona*. Podobně si zavedeme *multišablonu*: to je slovo s více druhy hvězdiček $*_1, \ldots, *_\ell$ a odpovídá mu funkce $\alpha(t_1, \ldots, t_\ell) : A^\ell \to A^k$ dosazující $t_i$ na místo $*_i$.

V krychli $A^k$ nás budou zajímat *kombinatorické přímky*. Každá přímka je jednoznačně určena nějakou šablonou $\alpha$ a obsahuje body $L_\alpha = \{\alpha(0), \ldots, \alpha(t-1)\}$. Jinými slovy $L_\alpha = \alpha[A]$, takže šablona vlastně funguje jako vnoření kanonické přímky $\{0, \ldots, a-1\}$ do krychle. Podobně můžeme zavést kombinatorické roviny a obecně $\ell$-dimenzionální podkrychle. Každá taková je určena multišablonou $\alpha$ s $\ell$ druhy hvězdiček a obsahuje body $\alpha[A^\ell]$, čili je to opět vnoření krychle $A^\ell$ do $A^k$.

**Cvičení.** Kolik existuje kombinatorických přímek v $A^k$? A rovin?

### Hales-Jewett

**Věta.** (Hales-Jewett) *Pro každé $a$ (délka hrany krychle) a $b$ (počet barev) existuje $N = \mathrm{HJ}(b, a)$ takové, že obarvíme-li body krychle $A^N$ pomocí $b$ barev, vždy existuje jednobarevná kombinatorická přímka.*

**Úloha.** Dokažte, že $\mathrm{HJ}(b, 2) \leq b$.

**Úloha.** Dokažte, že $\mathrm{HJ}(b, 2) \geq b$.

*Důkaz.* Fixujeme počet barev $b$ a budeme postupovat indukcí podle $a$. Pro $a = 1$ je tvrzení věty triviální, zbytek večera věnujeme indukčnímu kroku: již máme $n = \mathrm{HJ}(b, a)$, chceme nalézt (a hlavně ukázat, že existuje) $N = \mathrm{HJ}(b, a + 1)$.

Kam míříme: Potřebujeme si pořídit krychli s o jedničku kratší hranou, abychom mohli použít indukci. Proto ze zadané krychle „sloupneme slupku“ (odstraníme všechny body, jejichž některá souřadnice je nulová) a aplikujeme indukční předpoklad na oloupanou krychli. Indukce nám najde jednobarevnou přímku délky $a$, my ji potřebujeme rozšířit na přímku délky $a+1$. To samozřejmě obecně nemusí jít, proto předem zařídíme, aby byla slupka obarvena stejně jako body, které leží „těsně pod ní“. To zajistíme tak, že místo celé původní krychle budeme loupat nějakou její vhodnou podkrychli. Na to se nám bude hodit následující pomocné tvrzení.

**Definice.** Body $x, y \in A^n$ nazveme *sousední*, pokud pro každou souřadnici $i$ platí, že buď $x_i = y_i$ nebo $\{x_i, y_i\} = \{0, 1\}$.

O obarvení $\chi'$ $n$-rozměrné podkrychle $\alpha[A^n]$ budeme říkat, že je *konzistentní*, pokud pro každé dva sousední body $x, y \in A^n$ platí, že $\chi'(\alpha(x)) = \chi'(\alpha(y))$.

**Tvrzení.** (klíčové) *Existuje $N$ takové, že pro každé obarvení $\chi : A^N \to [b]$ existuje podkrychle $\alpha[A^n] \subseteq A^N$ obarvená konzistentně.*

Než tvrzení dokážeme (a ukážeme, kolik musí být $N$), rozmyslíme si, jak ho použít ke kýženému indukčnímu kroku.

Nastavíme $N$ podle tvrzení. Nepřítel nám zadá nějaké obarvení $\chi : A^N \to [b]$. My podle tvrzení nalezneme podkrychli $\alpha[A^n]$ obarvenou konzistentně a, jak za chvíli ukážeme, najdeme jednobarevnou přímku v této podkrychli. Jelikož každá taková přímka je současně jednobarevnou přímkou v $A^N$, indukční krok bude hotov. Všimněme si, že se stačí omezit na samotnou $A^n$ a vůbec neuvažovat její vnoření do velké krychle (vnoření určuje obarvení krychle $A^n$ a překládá přímky v $A^n$ na stejně obarvené přímky v $A^N$).

Máme tedy krychli $A^n$ a nějaké její konzistentní obarvení. Tuto krychli omezíme na $\{1, \ldots, a\}^n$ („oloupeme ji“) a použijeme na ni indukční předpoklad (v souřadnicích posunutých o 1, ale to je pouze formální rozdíl). Indukce nám zaručuje existenci jednobarevné přímky $L_\beta = \{\beta(1), \ldots, \beta(a)\}$ v oloupané krychli. Bod $\beta(0)$ ovšem musí mít stejnou barvu jako $\beta(1)$, protože tyto dva body se mohou lišit pouze změnou nulových souřadnic na jedničky, takže jsou sousední. Nyní stačí použít konzistenci obarvení a získat tak jednobarevnou přímku v celé krychli $A^n$. □

*Důkaz.* (klíčového tvrzení) Multišablonu $\alpha$, která určuje hledanou podkrychli, budeme hledat ve speciálním tvaru. Bude se skládat z bloků $\alpha_1, \ldots, \alpha_n$ položených za sebe, přičemž blok $\alpha_i$ bude mít délku $N_i$ a budou se v něm nacházet výhradně hvězdičky $i$-tého typu (a konkrétní hodnoty souřadnic). Parametry $N_i$ přitom nastavíme následovně:

$$N_1 = b^{a^n}, \qquad N_i = b^{a^{\left(n+\sum_{j=1}^{i-1} N_j\right)}}.$$

Hledaná dimenze $N$ pak bude přirozeně součet $N_1 + \cdots + N_n$.

Dostali jsme tedy nějaké obarvení $\chi : A^N \to [b]$ a chceme sestrojit bloky $\alpha_1, \ldots, \alpha_n$ hledané multišablony. Budeme je konstruovat zpětnou indukcí. Začneme prázdnou posloupností bloků. Když pak budeme mít hotové bloky $\alpha_{i+1}, \ldots, \alpha_n$ a budeme chtít sestrojit blok $\alpha_i$, budeme postupovat následovně. Označíme si $M = N_1 + \cdots + N_{i-1}$ a uvážíme funkce $\chi_0, \ldots, \chi_{N_i} : A^{M+n-i} \to [b]$ definované takto:

$$\chi_t\Big(x_1 \ldots x_M y_{i+1} \ldots y_n\Big) = \chi\Big(x_1 \ldots x_M 0^t 1^{N_i - t} \alpha_{i+1}(y_{i+1}) \ldots \alpha_n(y_n)\Big).$$

(Funkce $\chi_t$ popisuje barvy nějakých bodů z $A^N$ vybraných tak, že na ještě nepoužitých souřadnicích vystřídáme všechny kombinace hodnot, v $i$-té souřadnici vždy použijeme nějakou kombinaci $N_i$ nul a jedniček a ve zbývajících souřadnicích dosazujeme podle už sestrojených bloků.)

Všimneme si, že možných funkcí z $A^{M+n-i}$ do $[b]$ je pouze $b^{a^{M+n-i}} \leq b^{a^{M+n}} = N_i$, takže podle Dirichletova principu musí existovat $k, \ell$ taková, že $\chi_k = \chi_\ell$ a $k < \ell$. Obarvení $\chi_k$ odpovídá nastavení $\alpha_i = 0^k 1^{N_i - k}$, obarvení $\chi_\ell$ pak $\alpha_i = 0^\ell 1^{N_i - \ell}$. Zvolíme tedy $\alpha_i = 0^k *_i^{\ell-k} 1^\ell$, což souhlasí s obojím, a pokračujeme předchozím blokem.

(Na volbě čísel $N_i$ samozřejmě není zhola nic magického, čísla jsou nastavena přesně tak, aby právě použitý holubníkový argument fungoval, a nejsou potřeba nikde jinde.)

Takto sestrojená multišablona $\alpha = \alpha_1 \ldots \alpha_n$ opravdu určuje nějakou $n$-rozměrnou podkrychli. Zbývá si uvědomit, že je skutečně obarvena konzistentně. Můžeme si uvědomit, že konzistenci stačí ověřit pro dvojici sousedních bodů, které se liší pouze v jedné souřadnici. Uvažujme tedy nějaké dva sousední body $x, y \in A^n$ takové, že pro právě jedno $i$ platí $x_i = 0$, zatímco $y_i = 1$. V podkrychli tedy vystupují jako $\alpha(x)$ a $\alpha(y)$. Pro jejich obarvení platí ($k$, $\ell$ a $M$ si vypůjčíme z kroku, v němž jsme určovali $\alpha_i$):

$$\begin{aligned}
\chi(\alpha(x)) &= \chi\Big(\alpha_1(x_1) \ldots \alpha_{i-1}(x_{i-1}) \alpha_i(0) \alpha_{i+1}(x_{i+1}) \ldots \alpha_n(x_n)\Big) \\
&= \chi\Big(z_1 \ldots z_M 0^k 0^{\ell-k} 1^\ell \alpha_{i+1}(x_{i+1}) \ldots \alpha_n(x_n)\Big) \text{ pro nějaká } z_1, \ldots, z_M \\
&= \chi_k\Big(z_1 \ldots z_M y_{i+1} \ldots y_n\Big) \\
&= \chi_\ell\Big(z_1 \ldots z_M y_{i+1} \ldots y_n\Big) \\
&= \chi\Big(z_1 \ldots z_M 0^k 1^{\ell-k} 1^\ell \alpha_{i+1}(x_{i+1}) \ldots \alpha_n(x_n)\Big) \\
&= \chi\Big(\alpha_1(y_1) \ldots \alpha_{i-1}(y_{i-1}) \alpha_i(1) \alpha_{i+1}(y_{i+1}) \ldots \alpha_n(y_n)\Big) \\
&= \chi(\alpha(y)).
\end{aligned}$$

□

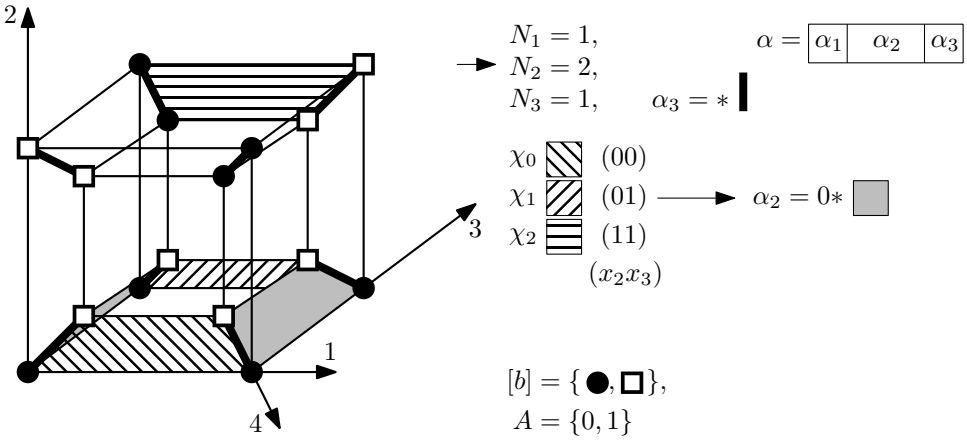
## Intuice

Ještě trocha geometrické intuice: Když máme hotové $\alpha_{i+1}, \ldots, \alpha_n$, každé nastavení zbývajících souřadnic (prvních $M + N_i$) určuje jednu $(n-i)$-rozměrnou podkrychli

v $A^N$. Každá volba $t$ pak odpovídá tomu, že si ze všech těchto podkrychlí vybereme ty, které mají v souřadnicích patřících do $i$-tého bloku správnou kombinaci nul a jedniček. Navíc si tyto podkrychle uspořádáme lexikograficky do posloupnosti $C_t$. Funkce $\chi_t$ pak není nic jiného než průmět obarvení $\chi$ celé krychle na obarvení posloupnosti $C_t$.

Jelikož je těchto posloupností dostatečně mnoho, existují $C_k$ a $C_\ell$ obarvené stejně. Každá krychle z $C_k$ přitom vznikne posunutím odpovídající krychle z $C_\ell$ o jedničku v souřadnicích, ve kterých se předepsané nuly a jedničky liší. Pokud přidáme ještě dalších $a-2$ posunutí o ostatní hodnoty, vytvoříme tím krychli o jedničku vyšší dimenze a jelikož první dvě posunutí byla obarvena stejně, je tato nová krychle v $i$-té dimenzi obarvena konzistentně. Takovou krychli ovšem máme pro libovolné nastavení předchozích $M$ souřadnic, takže v dalším kroku můžeme přidat konzistenci v $(i-1)$-ní dimenzi a tak dále.

Dobře je to vidět na následujícím obrázku. Aby se nám vešel do čtyř dimenzí, zvolili jsme (nerealisticky) $n=3$, $N_1=1$, $N_2=2$ a $N_3=1$ a také nejjednodušší možný případ $b=2$, $a=2$. Zastavili jsme se v okamžiku, kdy $\alpha_3$ už je určeno a chceme najít $\alpha_2$. Tlusté hrany jsou všechny 1-dimenzionální krychle vytvořené posunutím šablony $\alpha_3$. Ty z nich, které spadají do $C_0$ (resp. barví je $\chi_0$), jsme si označili šrafovaně zleva nahoru doprava dolů. Podobně $C_1$ šrafovaně zprava nahoru doleva dolů a $C_2$ šrafovaně vodorovně. Nyní si všimneme, že konfigurace $\chi_0$ a $\chi_1$ jsou obarveny stejně, takže zvolíme $\alpha_2 = 0*_2$. Tím se nám každá krychle v $C_0$ spojí s odpovídající krychlí v $C_1$ do šedé krychle o jedničku větší dimenze (pokud by bylo $a>2$, přibrala by ještě další svá posunutí, ale ta nejsou zajímavá, protože se jich konzistence netýká). Všechny takové krychle (v našem případě jsou dvě) pak postupují do dalšího kroku indukce.



### Důsledky

**Důsledek.** (Van der Waerdenova věta) *Pro každé $t$ (délka posloupnosti) a $b$ (počet barev) existuje $N$ takové, že v libovolném obarvení množiny $[N]$ pomocí $b$ barev existuje jednobarevná aritmetická posloupnost délky $t$.*

Můžeme dokázat i obecnější verzi pracující v $d$-rozměrném prostoru. Místo aritmetických posloupností pak budeme hledat *homotetické kopie* nějaké konečné množiny $H \subset \mathbb{N}^d$, což budou množiny ve tvaru $v_0 + \lambda H$ pro $v_0 \in \mathbb{N}^d$, $\lambda \in \mathbb{N}^+$.

**Věta.** (Gallai-Witt) *Pro každé $d$ (dimenze) a konečnou množinu $H \subset \mathbb{N}^d$ platí, že v libovolném obarvení prostoru $\mathbb{N}^d$ pomocí $b$ barev existuje jednobarevná homotetická kopie množiny $H = \{v_1, \dots, v_a\}$ (homotetická kopie $H$ je množina tvaru $\{a_0 + \lambda v_1, a_0 + \lambda v_2, \dots, a_0 + \lambda v_k\}$ pro nějaké $a_0 \in \mathbb{N}^d$ a $\lambda \in \mathbb{N}^+$).*

Teď už pouze dodáme, že bychom mohli dokonce místo celého prostoru barvit jen nějaký omezený podprostor $[N]^d$ a najít jednobarevnou kopii $H$ i tam. Jeho velikost $N$ by pak samozřejmě závisela na velikosti $H$ a počtu použitých barev (a příslušných Hales-Jewettových čísel).

**Úloha.** Dokažte, že $H(3, 2) = 4$.

Následující věta je ještě obecnější verze Hales-Jewetta. Někdy se jí říká také hustotní Hales-Jewett a pro její složitost si ji nebudeme dokazovat.

**Věta.** (Fürstenberg-Katznelson) *Pro každé $a$ a každé $\varepsilon \in (0, 1]$ existuje $N$ takové, že každá množina bodů $M \subseteq [a]^N$ splňující $|M| \geq \varepsilon a^N$ už nutně obsahuje nějakou kombinatorickou přímku.*

**Úloha.** Dokažte, že z Gallai-Witta plyne Van der Waerden.

**Úloha.** Dokažte, že z Hales-Jewetta plyne Galai-Witt.

**Úloha.** Dokažte, že z Fürstenberg-Katznelsona plyne Hales-Jewett.

### Literatura a zdroje

Příspěvek je z většiny převzat od Martina Mareše, za což bych mu chtěla poděkovat.

[1] Martin Mareš: *Hales-Jewettova věta*, *http://mj.ucw.cz/papers/hjt.pdf*.
[2] Stasys Jukna: *Extremal Combinatorics*.
[3] Vít Jelínek: *Kombinatorika a grafy 3*, MFF UK, 2021.

# Hrátky s polynomy

Magdaléna Mišinová

Abstrakt. Ukážeme si dva poměrně odlišné pohledy na polynomy a možná zbyde čas i na nějakou úlohu.

## Úvod

Když se v úloze objeví polynom, bývá dobrým zvykem zadat, z jaké množiny jsou jeho koeficienty. Většinou se jedná o množinu $\mathbb{Z}$ nebo $\mathbb{R}$, může to být ale i jiná. Aby dávalo smysl koeficienty z dané množiny brát, je potřeba v ní umět sčítat a násobit. Takovým strukturám se říká *okruhy*. Kromě již zmíněných je to třeba $\mathbb{Z}_n$ pro $n \in \mathbb{N}$, $\mathbb{Q}$ nebo $\mathbb{C}$. Obecný okruh budeme značit $R$, od anglického *ring*. Pokud v okruhu navíc můžeme dělit libovolným nenulovým prvkem, říkáme mu *těleso*. Tělesa jsou například $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ i $\mathbb{Z}_p$ pro $p$ prvočíslo, ale $\mathbb{Z}$ už těleso není.

**Definice.** Je-li $R$ okruh, pak *polynomem nad* $R$ myslíme výraz $a_0+a_1x+\cdots+a_nx^n$ pro $a_i \in R$. Množinu všech polynomů nad $R$ v proměnné $x$ značíme $R[x]$.

**Definice.** O $\alpha \in R$ řekneme, že je *kořenem* polynomu $p$, pokud $p(\alpha) = 0$.

**Definice.** Je-li $p \in R[x]$ polynom $p(x) = a_0 + \cdots + a_nx^n$ a $a_n \neq 0$, pak $n$ nazveme *stupněm* $p$. Zapisujeme $\deg(p) = n$. Speciálně definujeme $\deg(0) = -\infty$.

**Definice.** Je-li $p \in R[x]$ polynom $p(x) = a_0 + \cdots + a_nx^n$ a $a_n = 1$, nazveme $p$ *monickým* polynomem.

Polynomy můžeme sčítat nebo násobit mezi sebou, takže rovněž tvoří okruh.

### Polynomy a jejich kořeny

V této části budeme zkoumat polynomy pomocí jejich algebraických vlastností, z nichž nejdůležitější je ta, kde mají kořeny. Začneme tvrzením, které dost možná znáte:

**Tvrzení.** (Viètovy vztahy) *Nechť $R$ je okruh, $p \in R[x]$ a $p = a_0+a_1x+\cdots+a_nx^n$ má kořeny $r_1, \ldots, r_n$. Potom pro všechna $k \in \{1, 2, \ldots, n\}$ platí*

$$(-1)^k \cdot \frac{a_{n-k}}{a_n} = \sum_{\{i_1,\ldots,i_k\}\subseteq\{1,\ldots,n\}} r_{i_1} r_{i_2} \cdots r_{i_k}.$$

Následující tvrzení využívá toho, že funkce určená polynomem je velmi hezká.

**Tvrzení.** *Nechť $a < b$ jsou reálná čísla a $p \in \mathbb{R}[x]$. Pokud $p(a)p(b) < 0$, existuje kořen $p$ mezi $a$ a $b$.*

**Důsledek.** *Polynom nad reálnými čísly lichého stupně má kořen.*

**Úloha 1.** Alice a Bob hrají hru s polynomem stupně alespoň 4:

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

Střídají se v tazích, přičemž v jednom tahu vyplní nějaké reálné číslo do některého z dosud prázdných čtverečků. Alice vyhraje, pokud polynom na konci nebude mít žádné reálné kořeny, Bob vyhraje v opačném případě. Rozhodněte, kdo má vítěznou strategii.

**Úloha 2.** Je dáno sudé přirozené číslo $n$ a reálná čísla $c_1, c_2, \ldots, c_{n-1}$ splňující

$$\sum_{i=1}^{n-1} |c_i - 1| < 1.$$

Dokažte, že polynom

$$2x^n - c_{n-1}x^{n-1} + c_{n-2}x^{n-2} - \cdots - c_1x^1 + 2$$

nemá žádné reálné kořeny. (USA TST 2014)

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

To znamená, že každý polynom se nad $\mathbb{C}$ rozkládá na lineární činitele, tj. každý polynom lze zapsat jako $a_0 \cdot (x - r_1)(x - r_2)\cdots(x - r_n)$, kde $n$ je stupeň tohoto polynomu, $a_0$ a $r_i$ pro $i \in \{1, \ldots, n\}$ jsou komplexní čísla. To je jeden z důvodů, proč se občas hodí uvažovat polynom nad komplexními čísly, i když ho máme zadaný nad něčím jiným, třeba nad $\mathbb{Z}$ nebo $\mathbb{R}$.

### Polynomy a teorie čísel

V této části se budeme zabývat vlastnostmi polynomů, které jsou analogií vlastností celých čísel.

**Definice.** Nechť $p, q \in R[x]$. Pokud $p = qr$ pro nějaké $r \in R[x]$, pak říkáme, že $q$ *dělí* $p$, a zapisujeme stejně jako u čísel: $q \mid p$.

**Definice.** Nechť $p, q, r \in R[x]$. Pokud $r \mid p - q$, píšeme $p \equiv q \pmod{r}$.

Nad tělesy se dělení polynomů chová obzvláště dobře.

**Tvrzení.** (dělení se zbytkem) *Pro $u, v \in F[x], v \neq 0$ existují polynomy $q, r \in F[x]$ takové, že $u = qv + r$ a $\deg(r) < \deg(v)$.*

**Tvrzení.** *Prvek $\alpha \in F$ je kořenem $p(x) \in F[x]$, právě když $x - \alpha \mid p(x)$.*

**Důsledek.** *Polynom $p \in F[x]$ stupně $n \geq 0$ má nejvýše $n$ kořenů.*

**Důsledek.** *Pokud se dva polynomy stupně nejvýše $n$ shodují v alespoň $n + 1$ bodech, jsou už nutně stejné.*

**Úloha 3.** Rozmyslete si, že předchozí dvě tvrzení platí i pro $\mathbb{Z}[x]$, pokud se v dělení se zbytkem přidá podmínka, že $v$ je monický.

**Úloha 4.** Najděte polynom $p \notin \mathbb{Z}[x]$ takový, že $p(x) \in \mathbb{Z}$ pro všechna $x \in \mathbb{Z}$.

**Úloha 5.** (Bézoutova věta) Definujme největšího společného dělitele polynomů nad tělesem stejně jako pro celá čísla. Dokažte, že pro libovolné $p, q \in F[x]$ existují $a, b \in F[x]$ takové, že $\mathrm{NSD}(p(x), q(x)) = a(x)p(x) + b(x)q(x)$.

**Úloha 6.** Dokažte, že pokud $p \in \mathbb{Z}[x]$ nabývá hodnoty $-1$ ve třech různých celých číslech, pak $p$ nemá celočíselný kořen.

Bezesporu nejdůležitější je následující tvrzení:

**Tvrzení.** *Pokud $a \neq b \in \mathbb{Z}$ a $p \in \mathbb{Z}[x]$, pak platí $a - b \mid p(a) - p(b)$ (dělitelnost je obyčejná dělitelnost celých čísel).*

Alternativně lze totéž říct i pomocí kongruencí:

**Tvrzení.** *Polynomy s celočíselnými koeficienty jsou periodické* (mod $n$) *pro libovolné přirozené $n$, tj. $p(x + n) \equiv p(x) \pmod{n}$ pro všechna celá $x$.*

Pokud se v úloze vyskytují polynomy a dělitelnost, tak se vám nejspíš alespoň jednou bude dané tvrzení hodit.

**Úloha 7.** Ukažte, že pro libovolný monický polynom $p \in \mathbb{Z}[x]$ se stupněm alespoň 2 existuje nekonečná rostoucí posloupnost celých čísel $(x_n)$ taková, že $p(x_n) \mid p(x_{n+1})$.

Celkem dost se toho dá říct i o racionálních kořenech celočíselných polynomů, a to především díky následujícímu tvrzení:

**Tvrzení.** (Věta o racionálních kořenech) *Pokud* $\mathrm{NSD}(p, q) = 1$ *a $x = \frac{p}{q}$ je kořenem celočíselného polynomu $f(x) = a_n x^n + \cdots + a_0$, pak platí $p \mid a_0$, $q \mid a_n$.*

**Důsledek.** *Všechny racionální kořeny monického polynomu ze $\mathbb{Z}[x]$ jsou celé.*

Obecně jsou úlohy, které tvrdí něco o souvislostech mezi polynomy a prvočísly, velmi těžké (většina z nich stále zůstává bez odpovědi). Následující tvrzení poskytuje drobný, ale zase velmi užitečný vhled do této problematiky:

**Tvrzení.** (Schurova věta) *Je dán polynom $p \in \mathbb{Z}[x]$. Pokud je pouze konečně mnoho prvočísel, která dělí $p(x)$ pro nějaké $x \in \mathbb{Z}$, je $p$ konstantní polynom.*

**Úloha 8.** Existuje polynom sudého stupně s lichými koeficienty, který má racionální kořen? (MKS 34–6–4)

**Úloha 9.** Dokažte, že pokud $ax^3 + bx^2 + cx + d \in \mathbb{Z}[x]$ a $ad$ je liché, zatímco $bc$ je sudé, potom nemůžou být všechny kořeny tohoto polynomu racionální.

**Úloha 10.** Pokud $p \in \mathbb{Z}[x], a, b, c \in \mathbb{Z}$, tak $p(a) = b, p(b) = c, p(c) = a$ nastane jedině pokud $a = b = c$.

**Úloha 11.** Jsou-li $p, q \in \mathbb{Z}[x]$ nesoudělné, monické polynomy, pak posloupnost $a_n = \mathrm{NSD}(p(n), q(n))$ je periodická.

**Úloha 12.** Mějme $p \in \mathbb{Z}[x]$ se stupněm alespoň dva. Ukažte, že potom existuje dvojice přirozených čísel $(m, n)$ taková, že kongruence $p(x) \equiv m \pmod{n}$ nemá celočíselné řešení.

### Ireducibilita

Podobně jako nám rozklad na prvočísla může ledacos prozradit o celých číslech, tak se i u polynomů občas vyplatí zkoumat rozklady na součin. Obdobou prvočísel se pak stávají tzv. ireducibilní polynomy.

**Definice.** O polynomu $p \in R[x]$ řekneme, že je *ireducibilní nad* $R[x]$, pokud ho nelze napsat jako součin dvou nekonstantních polynomů z $R[x]$.

**Pozor:** je vždycky nutné uvádět, nad jakým okruhem myslíme ireducibilitu! Například díky základní větě algebry jsou ireducibilní polynomy nad $\mathbb{C}[x]$ právě ty se stupněm nejvýše jedna, zatímco ireducibilní polynomy nad $\mathbb{Z}[x]$ tvoří mnohem komplikovanější strukturu. Následující tvrzení však ukazuje, že ne vždy je rozdíl tak drastický.

**Tvrzení.** (Gaussova věta) *Polynom $p(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ je ireducibilní nad $\mathbb{Z}[x]$ právě tehdy, je-li ireducibilní nad $\mathbb{Q}[x]$.*

Obecně je ireducibilitu nějakého polynomu poměrně obtížné dokázat. Následující tvrzení ale ukazuje, jak lze šikovně použít $\mathbb{Z}_p[x]$.

**Tvrzení.** (Eisensteinovo kritérium) *Mějme polynom $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ a prvočíslo $p$, které splňují:*

(1) $p \nmid a_n$,
(2) $p \mid a_i$ *pro* $i = 0, \ldots, n-1$,
(3) $p^2 \nmid a_0$.

*Pak je $f$ ireducibilní nad $\mathbb{Z}[x]$.*

**Úloha 13.** Které z následujících polynomů jsou ireducibilní nad $\mathbb{Q}[x]$?

$$x^4 + 2x + 2, \quad x^4 + 18x^2 + 24, \quad x^3 - 9, \quad x^3 + x^2 + x + 1, \quad x^4 + 1, \quad x^4 + 4.$$

**Úloha 14.** Pro prvočíslo $p$ dokažte, že je $x^{p-1} + x^{p-2} + \cdots + 1$ ireducibilní nad $\mathbb{Q}[x]$.

**Úloha 15.** Pro $n > 1$ ukažte, že je $x^n + 5x^{n-1} + 3$ ireducibilní nad $\mathbb{Z}[x]$.

(IMO 1993–1)

**Úloha 16.** Nechť $p \in \mathbb{Z}[x]$ splňuje $p(x) = a_n x^n + \cdots + a_1 x + a_0$, kde $|a_0|$ je prvočíslo a $|a_0| > |a_1| + \cdots + |a_n|$. Dokažte, že $p$ je ireducibilní.

**Úloha 17.** Jsou-li $f, g \in \mathbb{Z}[x]$ dva monické polynomy ireducibilní nad $\mathbb{Z}[x]$, pro které navíc mají čísla $f(n)$ a $g(n)$ shodné množiny prvočíselných dělitelů pro všechna dost velká $n$, pak nutně platí $f = g$.

### Úlohy na procvičení

**Úloha 18.** Je dán polynom $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + 1 \in \mathbb{Z}[x]$ s nezápornými koeficienty, který navíc splňuje $a_i = a_{n-i}$ pro všechna $i$. Dokažte, že existuje nekonečně mnoho dvojic celých čísel $x < y$, které splňují $x \mid p(y)$ a $y \mid p(x)$.
(iKS 2–N5)

**Úloha 19.** Pro daná celá čísla $a, b, c$ jsou čísla $\frac{a}{b} + \frac{b}{c} + \frac{c}{a}$ i $\frac{b}{a} + \frac{c}{b} + \frac{a}{c}$ celá. Dokažte $|a| = |b| = |c|$.

**Úloha 20.** Definujme posloupnost $(x_n)$ jako $x_0 = 0$, $x_{n+1} = p(x_n)$ pro $p \in \mathbb{Z}[x]$. Ukažte, že pokud $x_n = 0$ pro nějaké $n > 0$, pak $x_1 x_2 = 0$. (Putnam 2000)

**Úloha 21.** Je dán polynom $p \in \mathbb{Z}[x]$ takový, že $p(n) > n$. Definujme posloupnost $(x_n)$ jako $x_0 = 0$, $x_{n+1} = p(x_n)$. Dokažte, že pokud pro každé $m \in \mathbb{N}$ obsahuje tato posloupnost nějaký násobek $m$, pak platí $p(x) = x + 1$. (Írán TST 2004)

**Úloha 22.** Je-li $p \in \mathbb{Z}[x]$ nekonstantní, pak polynom $p^k(x) - x$ má nejvýše $\deg(p)$ kořenů ($p^k$ značí $k$-násobné složení). (IMO 2006–5)

**Úloha 23.** Mějme funkci $f : \mathbb{Z} \to \mathbb{R}$ takovou, že $|f(n)| < p(n)$ pro nějaký polynom $p$ a $k - l \mid f(k) - f(l)$ pro všechna různá celá $k$, $l$. Dokažte, že existuje polynom $q \in \mathbb{R}[x]$ takový, že $f(k) = q(k)$ pro všechna $k \in \mathbb{Z}$. (MKS 34–6–8)

**Úloha 24.** Buď $a, b, c, d, e, f \in \mathbb{N}$ a $S = a + b + c + d + e + f$. Platí-li $S \mid abc + def$ a $S \mid ab + bc + ca - de - ef - fd$, dokažte, že $S$ musí být složené.
(IMO SL 2005–N3)

### Návody

**1.** Vyhraje Bob. Stačí řešit několik posledních tahů.

**2.** Těžká část úlohy je ukázat, že polynom je kladný pro kladná čísla. Rozděl je podle toho, zda jsou větší či menší než 1.

**5.** Děl se zbytkem.

**6.** $p(x) = (x - a)(x - b)(x - c)q(x) - 1$ pro $q \in \mathbb{Z}[x]$.

**8.** Nula je sudá, součet lichých čísel je ...

**9.** Ukaž sporem pomocí věty o racionálních kořenech.

**10.** $a - b \mid p(a) - p(b)$.

**11.** Z Bézouta $ap + bq = N$ pro nějaké přirozené $N$. Dokaž $a_{n+N} = a_n$.

**12.** Kdyby tomu tak nebylo, musí $p(x), \ldots, p(x+n-1)$ dávat různé zbytky po dělení $n$ pro libovolné $x$. Zvol $n = p(x+1) - p(x) > 2$.

**14.** Posuň se o jedničku.

**15.** Zkus trochu zobecnit Eisensteina.

**16.** Ukažte, že absolutní hodnota všech komplexních kořenů $p$ je větší než 1.

**17.** Ireducibilita a různost vynucují nesoudělnost, pak Bézout a Schur dokončí oslavu.

**18.** Funguje-li dvojice $(x, y)$, pak funguje i $\left(y, \frac{P(x)}{y}\right)$.

**19.** Vezmi polynom s kořeny $\frac{a}{b}, \frac{b}{c}, \frac{c}{a}$ a na něj aplikuj větu o racionálních kořenech.

**20.** Když $x_1 = 0$, je všechno jasné, jinak využij $x - y \mid p(x) - p(y)$.

**21.** $x - y \mid p(x) - p(y)$.

**22.** Jsou-li $x, y$ kořeny, pak platí $|x - y| = |p(x) - p(y)|$. Případně zkus použít předchozí úlohu k tomu, aby ti stačilo vyřešit jen případ $k = 2$.

**23.** Pomocí toho, že $\mathrm{NSN}(n, n-1, \ldots, n-d) > kn^{d+1}$ pro nějakou konstantu $k > 0$, dokaž, že se hodnoty $f$ shodují s vhodným polynomem.

**24.** Zkoumej polynom $(x+a)(x+b)(x+c) - (x-d)(x-e)(x-f)$.

### Literatura a zdroje

Čerpala jsem především z příspěvku *Danila Koževnikova*, kterému bych tímto chtěla poděkovat

[1] Danil Koževnikov: *Aritmetické vlastnosti polynomů*, Sklené, 2019.
[2] Yufei Zhao: *Integer Polynomials*, MOP, 2007.
[3] Alexander Remorov: *Polynomials*, Canadian MO trianing camp, 2011.

# Nerovnosti bez kladiv

Magdaléna Mišinová

Abstrakt. Říká se, že nerovnosti už vyšly z módy. Není to ale úplně pravda, jen často nejdou vyřešit tak, že v nich poznáme speciální případ nějaké známé nerovnosti. V této přednášce si ukážeme několik úloh s nerovnostmi, které se v olympiádě v posledních letech objevily, na něž spíš než velká kladiva použijeme dobré nápady.

Úlohy, u nichž je uveden zdroj, jsou „ty“ úlohy, které si chceme předvést. Zbytek jsou spíše návodná cvičení, která by měla rozkouskovat myšlenky v oněch hlavních úlohách. Někdy se jedná přímo o součást řešení, jindy o podobnou, ale jednodušší úlohu.

### Různé

**Cvičení 1.** Nechť $a_1, \ldots, a_n$ jsou nenulová reálná čísla a $\sum_{i=1}^{n} a_i = 0$. Dokažte, že $\sum_{i<j} a_i a_j < 0$.

**Cvičení 2.** Nechť $c \in \mathbb{R}^+$ a pro reálná čísla $a_1, \ldots, a_n$ platí $|a_i| \geq c$. Dokažte, že

$$\sum_{i,j,\, |a_i - a_j| < 2c} a_i a_j \geq 0.$$

**Úloha 3.** Nechť $n \geq 2$ je přirozené číslo a $a_1, \ldots, a_n$ jsou reálná čísla splňující $a_1 + \cdots + a_n = 0$. Označíme jako $A$ množinu $\{(i,j) | 1 \leq i < j \leq n, |a_i - a_j| \geq 1\}$. Dokažte, že pokud je $A$ neprázdná, pak platí $\sum_{(i,j)\in A} a_i a_j < 0$. (ISL 2019 A4)

**Cvičení 4.** (Rozklad na součin) Rozhodněte, pro která $x$ platí

(1) $x(x+2) \geq -1$,
(2) $x(x+1) \geq -\frac{1}{4}$,
(3) $2x(x-1) \geq 1$,
(4) $x(x+1) \leq \frac{1}{3}$.

**Cvičení 5.** Jsou dána reálná čísla $x$ a $y$, pro něž platí $xy = -1$ a $x^2 + y^2 = 6$. Určete všechny možné hodnoty $x + y$.

**Úloha 6.** Jsou dána reálná čísla $a$, $b$, $c$ splňující $a + b + c = a^2 + b^2 + c^2 = 1$. Dokažte, že $-\frac{1}{4} \leq ab \leq \frac{4}{9}$. (CNMO 2020)

### Rozděl a odhaduj

**Cvičení 7.** Nechť reálná čísla $a_1 \geq a_2 \geq \cdots \geq a_k \geq 0$ a $b_1 \geq b_2 \geq \cdots \geq b_\ell \geq 0$ splňují $\sum_{i=1}^{k} a_i = \sum_{i=1}^{\ell} b_i$. Dokažte, že platí

$$\sum_{i=1}^{k} a_i^2 + \sum_{i=1}^{\ell} b_i^2 \leq (k+\ell) a_1 b_1.$$

**Úloha 8.** Nechť $u_1, \ldots, u_{2019}$ jsou reálná čísla splňující $u_1 + \cdots + u_{2019} = 0$, $u_1^2 + \cdots + u_{2019}^2 = 1$. Označme $a = \min\{u_1, \ldots, u_{2019}\}$ a $b = \max\{u_1, \ldots, u_{2019}\}$. Dokažte, že $ab \leq -\frac{1}{2019}$. (ISL 2019 A2)

**Úloha 9.** Posloupnost reálných čísel $x_0, \ldots, x_{100}$ nazveme *prasečí*, pokud splňuje

(1) $x_0 = 0$,
(2) $1 \leq x_i - x_{i-1} \leq 2$ pro každé $i$, $1 \leq i \leq 100$.

Najděte největší přirozené $k \leq 100$ takové, že pro libovolnou prasečí posloupnost platí

$$x_k + \cdots + x_{100} \geq x_0 + x_1 + \cdots + x_{k-1}.$$

(CGMO 2022 P1)

**Cvičení 10.** (Teleskopické) Dokažte následující nerovnosti:

(1) $\sum_{i=1}^{n} \frac{1}{i^2} \leq 2 - \frac{1}{n}$,
(2) $\sum_{i=1}^{n} \frac{1}{2\sqrt{i}} \leq \sqrt{n}$.

**Úloha 11.** Dokažte, že pro libovolná čísla $a_1, \ldots, a_n \in [1, 2]$ platí

$$\sum_{i=1}^{n} \frac{a_i^2}{(a_1 + a_2 + \cdots + a_i)^2} < 5.$$

**Cvičení 12.** Rozmyslete si, jak se předchozí úloha změní, pokud interval $[1, 2]$ nahradíme intervalem $\left[2^k, 2^{k+1}\right]$ pro nějaké přirozené $k$.

**Úloha 13.** Jsou dána dvě přirozená čísla $n$ a $k$. Dokažte, že pro libovolná čísla $a_1, \ldots a_n \in \left[1, 2^k\right]$ platí

$$\sum_{i=1}^{n} \frac{a_i}{\sqrt{a_1^2 + \cdots + a_i^2}} \leq 4\sqrt{kn}.$$

(ISL 2020 A7)

### Návody

**1.** Uvažuj $(\sum_{i=1}^{n} a_i)^2$.

**2.** Uvědom si, jaké dvojice čísel splňují podmínku v sumě.

**3.** Převeď problém na množinu, kde nevyžaduješ ostrou nerovnost mezi indexy a díváš se na malé vzdálenosti místo velkých.

**4.** Převeď to na jednu stranu a rozlož na součin.

**6.** Ukaž, že $ab = c(c-1)$.

**7.** Odhadni každou sumu pomocí ne nutně těsných odhadů.

**8.** Rozděl čísla na kladná a záporná.

**9.** Pro velká čísla použij dolní odhad rozdílů, pro malá ten horní.

**10.** Odhadni to pomocí jiného součtu, který se nechá „zteleskopovat“.

**11.** Odhadni jmenovatel každého členu zdola a čitatel shora.

**12.** Nijak.

**13.** Kromě předchozích úloh a cvičení může pomoci nerovnost mezi kvadratickým a aritmetickým průměrem.

### Literatura a zdroje

[1] *http://https://artofproblemsolving.com/community*.

# Úvod do lineární algebry

Vendula Onderková

Abstrakt. Cílem příspěvku je seznámit čtenáře se základními pojmy lineární algebry.

## Matice

**Definice.** *Reálnou maticí $A$ typu $m \times n$* rozumíme obdélníkové schéma s $m$ řádky a $n$ sloupci. Značením $a_{ij}$ rozumíme prvek na $i$-tém řádku a $j$-tém sloupci. Zápisem $A = (a_{ij})_{n\times m}$ rozumíme matici $A$ typu $n \times m$, která má na pozici $(i, j)$ (tedy na $i$-tém řádku a $j$-tém sloupci) prvek $a_{ij}$.

**Definice.** *Vektorem* rozumíme matici typu $n \times 1$. Vektor také můžeme chápat jako veličinu určenou velikostí a směrem.

**Definice.** *Skalár* je veličina určená svou velikostí. Většinou se jedná o reálné či komplexní číslo.

**Definice.** Nechť $A = (a_{ij})_{m\times n}$ je reálná matice, potom matici $B = (b_{ij})_{n\times m}$ nazveme *transponovanou maticí* k matici $A$, pokud pro každé $i$, $j$ platí $a_{ij} = b_{ji}$. Značíme ji $A^T$.

**Definice.** *Jednotkovou maticí typu $n \times n$* rozumíme matici, která má na hlavní diagonále jedničky a jejíž prvky mimo hlavní diagonálu jsou rovny 0.

**Definice.** (Sčítání matic) Nechť $A = (a_{ij})_{m\times n}$ a $B = (b_{ij})_{m\times n}$, pak pro matici $C = (c_{ij})_{m\times n}$ platí $A + B = C$, pokud pro každé $i, j$ platí $c_{ij} = a_{ij} + b_{ij}$.

**Definice.** (Násobení skalárem) Nechť $A = (a_{ij})_{m\times n}$ je matice typu $m \times n$ a $t \in \mathbb{R}$, potom $tA = (t \cdot a_{ij})_{m\times n}$.

**Definice.** (Násobení dvou matic) Nechť $A$ je matice typu $m \times n$, $B$ je matice typu $n \times p$. Potom *součinem matic* $A \cdot B$ rozumíme matici $C$ typu $m \times p$ takovou, že $c_{ij} = \sum_{k=1}^{n} a_{ik} \cdot b_{kj}$.

**Definice.** (Násobení matic s vektorem) Nechť $A = (\mathbf{a}_1 \mid \mathbf{a}_2 \mid \cdots \mid \mathbf{a}_n)$ je matice typu $m \times n$, kde $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n$ jsou sloupcové vektory matice a $\mathbf{x} = (x_1, x_2, \ldots, x_n)^T$ je $n$-složkový vektor. Potom $A \cdot \mathbf{x} = x_1 \cdot \mathbf{a}_1 + x_2 \cdot \mathbf{a}_2 + \cdots + x_n \cdot \mathbf{a}_n$.

**Úloha 1.** Nechť

$$A = \begin{pmatrix} 5 & 9 & 4 \\ 3 & 11 & 7 \\ 8 & 10 & 7 \end{pmatrix}, \qquad B = \begin{pmatrix} 4 & 3 & 4 \\ 5 & 2 & 6 \\ -8 & 6 & -5 \end{pmatrix}, \qquad C = \begin{pmatrix} 3 \\ 5 \\ 2 \end{pmatrix}, \qquad D = \begin{pmatrix} 2 \\ 0 \\ 6 \end{pmatrix}.$$

Spočítejte $A \cdot B$, $B \cdot A$, $A + B$, $B + A$, $C^T \cdot D$, $D \cdot C^T$, $A \cdot C$, $C^T \cdot A$, $B \cdot C$, $B \cdot A$, $C + D$.

**Úloha 2.** Procvičte si násobení matic:

a) $\begin{pmatrix} 1 & 1 \\ 2 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 3 \\ 3 & 2 \end{pmatrix}$, b) $\begin{pmatrix} 5 & 2 \\ 1 & 3 \\ 4 & 3 \\ 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 2 & 0 \\ 3 & 2 & 1 & 4 \end{pmatrix}$, c) $\begin{pmatrix} 4 & 0 & 1 \\ 2 & 1 & 4 \\ 3 & 5 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}$.

**Cvičení.** Co musí matice $A$, $B$ splňovat, aby byly definované součiny $A \cdot B$ a zároveň i $A \cdot B$? Najděte nějaké matice, pro které $A \cdot B = B \cdot A$.

### Gaussova eliminace

Častokrát potřebujeme při řešení různých úloh převést matici do takzvaného *řádkově odstupňovaného tvaru*, tedy do matice, kdy je každý následující řádek kratší než předchozí. Pro tento účel používáme metodu, která se nazývá *Gaussova eliminace*.

**Definice.** *Elementárními řádkovými úpravami* rozumíme následující typy úprav:

(i) Prohození $i$-tého řádku s $j$-tým řádkem.
(ii) Přičtení $k$-násobku $i$-tého řádku k $j$-tému řádku, kde $k$ je nenulové číslo.
(iii) Vynásobení $i$-tého řádku nenulovým číslem.

**Poznámka.** Obdobným způsobem definujeme i elementární sloupcové úpravy.

Pro eliminaci jednoho sloupce využijeme následující postup:

(1) Najdeme první nenulový sloupec, nechť je jeho index $k$.
(2) Podíváme se na prvek $a_{1k}$, pokud je roven 0, najdeme první řádek, který má v $k$-tém sloupci nenulový prvek. Prohodíme tento řádek s prvním řádkem.
(3) Ke každému řádku, kde $a_{ik} \neq 0$ přičteme $(-a_{ik}/a_{1k})$-násobek prvního řádku, dokud není prvek $a_{1k}$ jediný nenulový prvek v $k$-tém řádku.
(4) Celý proces zopakujeme pro matici bez prvního řádku.

### Soustavy lineárních rovnice

Matice můžeme využívat ke zjednodušení zápisu a výpočtu lineárních rovnic:

$$\begin{aligned} x_1 + 2x_2 + 2x_3 &= 3, \\ x_1 + 3x_2 + 3x_3 &= 4, \\ -3x_1 - 2x_2 + x_3 &= 4. \end{aligned}$$

Přepíšeme levou stranu soustavy jako součin matice $A$ s vektorem $\mathbf{x} = (x_1, x_2, x_3)^T$:

$$\begin{pmatrix} 1 & 2 & 2 \\ 1 & 3 & 3 \\ -3 & -2 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 3 \\ 4 \\ 4 \end{pmatrix}.$$

Pro výpočty pak používáme zápis, kterému se říká *rozšířená matice* soustavy:

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

**Úloha 3.** Vyřešte:

$$\begin{aligned} 1x_1 + 2x_2 + x_3 + 2x_4 &= 7, \\ 3x_1 - 2x_2 - x_3 - 2x_4 &= 9, \\ -x_1 + x_2 + 2x_3 - 2x_4 &= 5, \\ 3x_2 - x_1 + 2x_3 - x_4 &= 6. \end{aligned}$$

### Tělesa

**Definice.** *Tělesem* $T$ rozumíme množinu $T$ spolu s binárními operacemi $+$, $\cdot$ splňující následující axiomy:

(1) Pro každé $a, b, c \in T$ platí $(a + b) + c = a + (b + c)$.
(2) Existuje prvek $0 \in T$ takový, že pro každé $a \in T$ platí $a + 0 = a$.
(3) Pro každé $a \in T$ existuje prvek $(-a) \in T$ takový, že platí $a + (-a) = 0$.
(4) Pro každé $a, b \in T$ platí $a + b = b + a$.
(5) Pro každé $a, b, c \in T$ platí $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
(6) Existuje prvek $1 \in T$ takový, že pro každé $a \in T$ platí $a \cdot 1 = a$.
(7) Pro každé $0 \neq a \in T$ existuje prvek $a^{-1} \in T$ takový, že platí $a \cdot a^{-1} = 1$.
(8) Pro každé $a, b, c \in T$ platí $(a + b) \cdot c = a \cdot c + b \cdot c$.
(9) Množina $T$ obsahuje alespoň dva prvky.

Tělesa jsou pojmem hojně využívaným v lineární algebře a existuje spousta různých typů těles. Například $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ jsou tělesa. Naopak $\mathbb{N}$, $\mathbb{Z}$ tělesy nejsou, jelikož nesplňují existenci inverzního prvku. Jelikož ovšem mnohdy chceme počítat i s tělesy, která jsou celočíselná, zavádíme tělesa typu $\mathbb{Z}_p$, kde $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ a binární operace $+$, $\cdot$ jsou prováděny modulo $p$.

**Cvičení.** Ověřte, že takto zavedená tělesa splňují všechny axiomy.

**Úloha 4.** V tělesech $\mathbb{Z}_{11}$ a $\mathbb{Z}_{19}$ najděte ke každému prvku jeho inverzní prvek.

**Úloha 5.** Nechť $\mathbf{u} = (1, 4, 5, 6)^T$, $\mathbf{v} = (2, 4, 3, 5)^T$, $\mathbf{w} = (4, 2, 1, 3)^T$. Spočítejte $\mathbf{u}^T \cdot \mathbf{v}$, $\mathbf{w}^T \cdot \mathbf{v}$, $\mathbf{v} \cdot \mathbf{u}^T$, $\mathbf{w}^T \cdot \mathbf{u}$, $\mathbf{v} \cdot \mathbf{w}^T$ nad tělesy $\mathbb{R}$, $\mathbb{Z}_7$, $\mathbb{Z}_{11}$, $\mathbb{Z}_{13}$.

**Úloha 6.** Znovu spočítejte úlohu 2, ale nad tělesy $\mathbb{Z}_7$, $\mathbb{Z}_{11}$.

### Vektorové prostory

**Definice.** Nechť $T$ je těleso. Potom nazveme *vektorovým prostorem $V$ nad tělesem $T$* množinu $V$ spolu s binárními operacemi sčítání $+$ na $V$ (kde $+$ je zobrazení $V \times V \to V$) a násobení skalárem $\cdot$ (kde $\cdot$ je zobrazení $T \times V \to V$), splňujícími následující axiomy:

(1) Pro každé $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ platí $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$.
(2) Pro každé $\mathbf{u}, \mathbf{v} \in V$ platí $\mathbf{v} + \mathbf{u} = \mathbf{u} + \mathbf{v}$.
(3) Existuje prvek $\mathbf{0} \in V$ takový, že pro každé $\mathbf{v} \in V$ platí $\mathbf{v} + \mathbf{0} = \mathbf{v}$.
(4) Pro každé $\mathbf{v} \in V$ existuje prvek $(-\mathbf{v}) \in V$ takový, že platí $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$.
(5) Pro každé $\mathbf{v} \in V$ a každé $a, b \in T$ platí $(a \cdot b) \cdot \mathbf{v} = a \cdot (b \cdot \mathbf{v})$.
(6) Pro každé $\mathbf{v} \in V$ platí $1 \cdot \mathbf{v} = \mathbf{v}$.
(7) Pro každé $\mathbf{u}, \mathbf{v} \in V$ a $a \in T$ platí $a \cdot (\mathbf{u} + \mathbf{v}) = a \cdot \mathbf{u} + a \cdot \mathbf{v}$.
(8) Pro každé $\mathbf{v} \in V$ a $a, b \in T$ platí $(a + b) \cdot \mathbf{v} = a \cdot \mathbf{v} + b \cdot \mathbf{v}$.

**Definice.** Nechť $V$ je vektorový prostor nad $T$, pak vektorový prostor $U$ nad $T$ nazveme *podprostorem* vektorového prostoru $V$, pokud $U \subset V$ a shoduje se s $V$ v příslušných operacích $+$, $\cdot$.

**Tvrzení.** *Je-li $V$ vektorový prostor, pak $U \subset V$ je podprostorem právě tehdy, když je uzavřená na operace násobení a sčítání.*

### Lineární (ne)závislost

**Definice.** Nechť $V$ je vektorový prostor nad tělesem $T$, $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k \in V$ a $t_1, t_2, \ldots, t_k \in T$, potom vektor

$$t_1\mathbf{v}_1 + t_2\mathbf{v}_2 + \cdots + t_k\mathbf{v}_k$$

nazveme *lineární kombinací* vektorů $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$.

**Definice.** Nechť $V$ je vektorový prostor nad $T$ a $X \subset V$, potom *lineárním obalem množiny $X$* rozumíme množinu všech lineárních kombinací prvků $X$. Značíme ji $\mathrm{LO}\, X$.

**Tvrzení.** *Lineární obal množiny $X \subseteq V$ tvoří podprostor.*

**Definice.** Nechť $V$ je vektorový prostor nad $T$ a $X \subset V$, potom množinu $X$ nazveme *množinou generátorů $V$*, pokud lze každý prvek $\mathbf{v} \in V$ zapsat jako lineární kombinace prvků $X$.

**Úloha 7.** Vyjádřete vektor $(3, 2, 1)^T$ jako lineární kombinaci vektorů v prostorech $\mathbb{R}^3$, $\mathbb{Z}_5^3$:

a) $(1, 0, 3)^T$, $(1, 3, 2)^T$, $(2, 2, 3)^T$,
b) $(0, 3, 2)^T$, $(0, 2, 1)^T$, $(2, 1, 4)^T$.

**Úloha 8.** Určete, zda vektor $(5,1,4)^T \in \mathbb{Z}_7^3$ nad $\mathbb{Z}_7$ náleží do lineárního obalu vektorů:

a) $(1,1,3)^T$, $(1,2,6)^T \in \mathbb{Z}_7^3$ nad $\mathbb{Z}_7$,
b) $(1,0,1)^T$, $(2,3,4)^T$, $(2,1,3)^T \in \mathbb{Z}_7^3$ nad $\mathbb{Z}_7$,
c) $(4,1,5)^T$, $(1,2,3)^T \in \mathbb{Z}_7^3$ nad $\mathbb{Z}_7$.

**Definice.** Posloupnost $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$ nazveme *lineárně závislou*, pokud existuje vektor $\mathbf{v}_i$, kde $i \in \{1,2,\ldots,k\}$, který lze zapsat jako lineární kombinaci zbývajících vektorů. V opačném případě nazveme posloupnost *lineárně nezávislou*.

**Tvrzení.** *Posloupnost vektorů $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$ je lineárně nezávislá právě tehdy, když lze nulový vektor vyjádřit jako lineární kombinaci těchto vektorů pouze triviálním způsobem (tedy $0 \cdot \mathbf{v}_1 + 0 \cdot \mathbf{v}_2 + \cdots + 0 \cdot \mathbf{v}_k = \mathbf{0}$).*

**Příklad.** Zjistěte, zda je v prostoru $\mathbb{R}^4$ posloupnost $(3,4,1,0)^T$, $(3,1,3,-2)^T$, $(2,1,-4,3)^T$ lineárně nezávislá.

*Řešení.* Chceme zjistit, zda má následující rovnice právě jedno řešení:

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

Tuto rovnici můžeme přepsat jako homogenní soustavu:

$$\begin{pmatrix} 3 & 3 & 2 \\ 4 & 1 & 1 \\ 1 & 3 & -4 \\ 0 & -2 & 3 \end{pmatrix}.$$

Po provedení Gaussovy eliminace dostaneme

$$\begin{pmatrix} 3 & 3 & 2 \\ 0 & 9 & 5 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Zpětným dosazením zjistíme, že má rovnice opravdu právě jedno řešení, a tedy je soustava lineárně nezávislá.

**Úloha 9.** Zjistěte, zda jsou následující posloupnosti vektorů lineárně nezávislé:

a) $(3,4,2)^T, (1,2,4)^T, (2,3,0)^T$ v prostoru $\mathbb{Z}_5^3$ nad $\mathbb{Z}_5$,
b) $(3,2,3,1,0)^T$, $(5,4,5,5,1)^T$, $(2,1,3,3,2)^T$, $(1,4,2,4,2)^T$, $(1,1,0,4,1)^T$, $(1,6,1,6,2)^T$ v prostoru $\mathbb{Z}_7^5$ nad $\mathbb{Z}_7$,
c) $(1,0,1,1,0,0)^T, (0,1,1,1,1,0)^T, (0,1,1,1,1,0)^T, (1,0,1,1,0,1)^T$ v prostoru $\mathbb{Z}_2^6$ nad $\mathbb{Z}_2$.

**Úloha 10.** Zjistěte, zda jsou následující posloupnosti vektorů v prostoru reálných funkcí lineárně nezávislé:

(1) $\sin x$, $\cos x$,
(2) $x^2 + 2x + 1$, $x^2$, $1$,
(3) $x^2$, $x^3 + 2$, $x^3 + x - 5$, $4x$, $3$.

**Definice.** Nechť $V$ je vektorový prostor nad $T$, potom posloupnost vektorů $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$ nazveme *bází* vektorového prostoru $V$, pokud je lineárně nezávislá a množina $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ generuje celý prostor $V$.

**Definice.** *Dimenzí* vektorového prostoru $V$ rozumíme počet vektorů jeho báze.

**Úloha 11.** Vyberte největší lineárně nezávislou posloupnost z posloupnosti vektorů $(1,0,1)^T$, $(1,1,1)^T$, $(1,1,0)^T$, $(0,1,1)^T$, $(0,1,0)^T$ v prostoru $\mathbb{Z}_2^3$ nad tělesem $\mathbb{Z}_2$ a určete velikost dimenze prostoru, který generuje.

**Úloha 12.** Najděte alespoň dvě různé báze prostorů $\mathbb{R}^4$, $\mathbb{Z}_3^5$, $\mathbb{Z}_4^4$.

**Úloha 13.** Jakou dimenzi mají prostory generované množinami vektorů v úloze 9?

**Cvičení.** Rozmyslete si, jaká je maximální dimenze prostoru generovaného čtyřsložkovými vektory.

**Cvičení.** Nechť $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k)$ je posloupnost $n$-složkových vektorů vektorového prostoru $V$ nad $T$. Dokažte, že je lineárně nezávislá právě tehdy, když lze každý $n$-složkový vektor vyjádřit jako lineární kombinaci $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ nejvýš jedním způsobem.

### Hodnost matice

**Definice.** *Hodností matice* rozumíme počet nenulových řádků matice $C$ v *řádkově odstupňovaném tvaru*, která vznikne z matice $A$ Gaussovou eliminací. Značí se $r(A)$ nebo také $\operatorname{rank}(A)$.

Prvním nenulovým prvkům zleva v řádcích matice v odstupňovaném tvaru říkáme *pivoti*. Sloupcům, které obsahují pivota, říkáme sloupce *bázové*. Hodnost je tedy jinak řečeno rovna počtu pivotů či počtu bázových sloupců.

**Definice.** *Sloupcovým (resp. řádkovým) prostorem matice $A$* rozumíme prostor generovaný sloupci (resp. řádky) matice $A$. Značíme jej $\operatorname{Im} A$ (resp. $\operatorname{Im} A^T$).

Každá matice $A$ typu $m \times n$ určuje zobrazení z prostoru $n$-složkových vektorů do prostoru $m$-složkových vektorů. Taková zobrazení definujeme předpisem

$$f_A(\mathbf{x}) = A\mathbf{x},$$

kde $\mathbf{x}$ je nějaký $n$-složkový vektor. Podíváme-li se na násobení matice s vektorem tzv. *sloupcovým pohledem*, vidíme, že každý obraz vektoru $\mathbf{x}$ je vlastně lineární kombinací

sloupců matice $A$. Tedy sloupcový prostor matice $A$ je zároveň oborem hodnot (neboli obrazem) zobrazení daného maticí $A$. Odtud taky z anglického „image“ máme označení $\operatorname{Im} A$.

**Definice.** (Trochu jiná definice hodnosti) *Hodností matice $A$* rozumíme dimenzi řádkového (sloupcového) prostoru matice $A$.

**Tvrzení.** *Řádkové ani sloupcové úpravy nemění lineární nezávislost řádkových ani sloupcových vektorů matice.*

**Úloha 14.** Spočítejte hodnosti následujících matic nad tělesy $\mathbb{R}$, $\mathbb{Z}_7$, $\mathbb{Z}_{11}$, $\mathbb{Z}_{13}$:

$$A = \begin{pmatrix} 1 & 1 & 5 & 2 \\ 2 & 4 & 2 & 2 \\ 1 & 2 & 3 & 3 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 & 2 \\ 2 & 1 & 1 \\ 3 & 1 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad C = \begin{pmatrix} 2 & 5 \\ 2 & 4 \\ 1 & 5 \\ 4 & 5 \end{pmatrix}.$$

**Úloha 15.** V závislosti na parametru $a, \in \mathbb{R}$ určete hodnosti matic:

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 1 \\ a & 1 & 3 \end{pmatrix}, \qquad B = \begin{pmatrix} a+2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 3 & 0 \end{pmatrix}.$$

**Tvrzení.** *Nechť $A$ je matice typu $m \times n$ a $B$ je matice typu $n \times p$, potom*

$$\operatorname{rank}(AB) \leq \min\big(\operatorname{rank}(A), \operatorname{rank}(B)\big).$$

### Determinant

**Definice.** *Determinant* čtvercové matice řádu $n$ značíme $\det(A)$ a definujeme následujícím rekurzivním způsobem:

(1) Pro matici řádu 1 je determinant roven jejímu jedinému prvku.
(2) Pro matice řádu $n \geq 2$ definujeme determinant pro libovolné $j \in \{1, 2, \ldots, n\}$ předpisem

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det(M_{ij}),$$

kde $M_{ij}$ je matice řádu $n-1$, která vznikne z matice $A$ vynecháním $i$-tého řádku a $j$-tého sloupce.

Jak jsme si již zmínili, matice určují nějaké zobrazení. Determinant nám pak říká, jak takovéto zobrazení mění objem $n$-rozměrného rovnoběžnostěnu. Konkrétně absolutní hodnota determinantu nám udává, kolikrát se tento objem změní. Znaménko determinantu nám potom určuje, zda se změní „orientace“ tohoto tělesa v prostoru.

**Příklad.** Spočítejte determinant matice

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 2 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

*Řešení.* Na výběru sloupce, podle kterého rozvoj povedeme, nezáleží. Bývá ovšem výhodné vybírat si sloupec tak, aby měl co nejvíce nul, jelikož nám to dosti zjednoduší počítání. Rozvíjejme tedy podle druhého sloupce, potom dostáváme:

$$\det(A) = 0\cdot(-1)^{1+2}\cdot\det\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} + 1\cdot(-1)^{2+2}\cdot\det\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + 1\cdot(-1)^{3+2}\cdot\det\begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}.$$

Opět provedeme rozvoje, nyní například podle prvních sloupců, a po mírných úpravách dostáváme:

$$\begin{aligned} \det(A) = (-1)^{1+1}\cdot\det(1) + (-1)^{2+1}\cdot\det(1) - \\ - \Big((-1)^{1+1}\cdot\det(1) + 2\cdot(-1)^{2+1}\cdot\det(1)\Big). \end{aligned}$$

Tedy vidíme, že $\det(A) = 1$.

**Úloha 16.** Spočítejte determinanty následujících matic:

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

Pro menší matice existují jednodušší vzorečky pro výpočet determinantu:

**Tvrzení.** (Sarrusovo pravidlo) *Nechť $A = (a_{ij})_{3\times 3}$, potom*

$$\det(A) = a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} + a_{31}a_{12}a_{23} - a_{13}a_{22}a_{31} - a_{23}a_{32}a_{11} - a_{33}a_{12}a_{12}.$$

### Literatura a zdroje


[1] Libor Barto, Jiří Tůma: *Lineární algebra.*
[2] Anna Marie Minarovičová: *Úvod do lineární algebry*, Mrtník, 2023.
[3] Martin „E.T.“ Sýkora: *Matice ze všech stran*, Zásada, 2017.

# Intuicionistická logika

Daniel Perout

Abstrakt. Příspěvek je úvodem do intuicionistické logiky jako zástupce neklasických logik. Zopakuje sémantiku klasické logiky a tabulkovou metodu, poté představí intuicionistickou logiku, Heytingovu interpretaci významu jejích formulí a intuicionistickou kripkovskou sémantiku.

## Proč potřebujeme logiku

**Příklad.** (Berryho paradox) Existuje nejmenší přirozené číslo takové, že se nedá popsat méně než třinácti slovy?

**Příklad.** (Paradox holiče ze Sevilly) Holič v Seville holí právě ty její obyvatele, kteří se sami neholí. Holí holič sám sebe?

Výše uvedené příklady nám ukazují, že existují výrazy přirozeného jazyka, které by nám dělaly problémy, pokud bychom je přijali do matematiky. Mimo jiné právě takové paradoxy inspirovaly v 19. století k vybudování nové oblasti matematiky – logiky.

Cílem logiky by mělo být korektně formalizovat naše uvažování. Některá pravidla se nabízejí sama a není okolo nich žádná kontroverze, např. pokud platí tvrzení typu „$A$ a $B$“, pak by mělo platit i tvrzení typu „$B$ a $A$“. Ovšem existují i principy, o jejichž platnosti se logici desítky let přeli a které postupně vedly k vytvoření tzv. *neklasických logik*.

## Vyrábíme výrokovou logiku

Nejprve si vybudujme formální logický arzenál. Nebudeme už pracovat s větami či jinými strukturami přirozeného jazyka, ale s formulemi, které náš přirozený jazyk abstrahují. Zabývat se přitom budeme *výrokovými formulemi*, které zachycují pouze vztahy mezi výroky, ale nic neříkají o objektech, jejich vlastnostech ani vztazích (na to bychom potřebovali silnější logiku (predikátovou)).

Neformálně si formuli představme jako správně utvořený výraz skládající se z *výrokových atomů*, závorek a logických spojek, tj. negace $\neg$, konjunkce $\wedge$, disjunkce $\vee$ a implikace $\rightarrow$.

Častým trikem při definování pojmů je tzv. rekurentní definice, tedy že neřekneme, co daný objekt je, ale jen že patří do dané množiny, kterou sestrojíme pomocí rekurze. Tedy správná odpověď na otázku, co je formule, je, že jde o prvek množiny formulí.

**Definice.** (Formule) Nechť je dána množina atomů At. Množinou formulí Fle rozumíme nejmenší množinu splňující:

(i) každý atom je formule;
(ii) je-li $A$ formule, pak i $\neg A$ je formule;
(iii) jsou-li $A$ a $B$ formule, pak i $A \wedge B$, $A \vee B$ a $A \to B$ jsou formule.

Proč je dobré si definovat formule takto? Umožní nám to systematicky postupovat při důkazech, ve kterých je potřeba využít strukturu formulí. Máme-li totiž nějakou vlastnost definovanou pro atomy, většinou se dá rozšířit na všechny formule. Atomy proto můžeme chápat jako jisté počáteční podmínky, které stačí nastavit a určí nám už stav celého systému. Příklady uvidíme v další kapitole.

### Klasická sémantika

Představme nyní tzv. *klasickou logiku*, kterou používáme nejčastěji a většinou bez pomyšlení, že by mohla nebýt jedinou. V této logice každé formuli přiřazujeme pravdivostní hodnotu (pravda nebo nepravda) a význam formulí je potom zcela určen jejich pravdivostní hodnotou. Formálně si přiřazení pravdivostní hodnoty zadefinujme níže.

**Definice.** (Ohodnocení) *Ohodnocením atomů* rozumíme libovolné zobrazení $v_{\mathrm{At}}$ z množiny atomů do množiny $\{0, 1\}$.

Je-li dáno ohodnocení atomů $v_{\mathrm{At}}$, *ohodnocením* (formulí) rozumíme zobrazení $v$ z množiny formulí do množiny $\{0, 1\}$, které pro každé formule $A$, $B$ splňuje:

(i) je-li $A$ atom, pak $v(A) = v_{\mathrm{At}}(A)$;
(ii) $v(\neg A) = 1$, právě když $v(A) = 0$;
(iii) $v(A \wedge B) = 1$, právě když $v(A) = 1$ a $v(B) = 1$;
(iv) $v(A \vee B) = 1$, právě když $v(A) = 1$ nebo $v(B) = 1$;
(v) $v(A \to B) = 1$, právě když $v(A) = 0$ nebo $v(B) = 1$.

**Definice.** ((Klasická) tautologie) Formule je *(klasickou) tautologií*, pokud je platná při každém ohodnocení.

Jak zjistíme, zda je formule tautologií? Můžeme si vypsat všechna ohodnocení a ověřit, že při každém je formule splněná. Stačí nám přitom ohodnocovat pouze atomy, které se ve formuli vyskytují. Standardním nástrojem pro takové ověřování jsou tabulky.

**Příklad.** Určete, zda je $A = (p \to q) \to (\neg q \to \neg p)$ tautologie.

*Řešení.*

| $p$ | $q$ | $\neg p$ | $\neg q$ | $p \to q$ | $\neg q \to \neg p$ | $A$ |
|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 1 |
| 0 | 1 | 1 | 0 | 1 | 1 | 1 |
| 0 | 0 | 1 | 1 | 1 | 1 | 1 |

**Úloha.** Které z formulí

(1) $p$, (2) $p \vee p$, (3) $p \wedge p$,
(4) $p \to p$, (5) $p \wedge \neg p$, (6) $\neg p \to p$,
(7) $p \to (\neg p \to p)$

jsou tautologie?

#### Není naše logika moc silná?

Protože má v klasické logice každá formule pravdivostní hodnotu (stačí jen najít, jaká je), můžeme dělat úvahy jako např. důkaz sporem (tj. pokud dojdeme ke sporu při předpokladu opaku, tak musí formule platit) nebo rozdělením na případy (daná formule buď platí nebo neplatí, tedy pokud z obojího dokážeme, co chceme, pak výsledek platí).

**Příklad.** (Zákon vyloučení třetího) Dokažte, že $A \vee \neg A$ je tautologie.

Je ale možné argumentovat, že takový přístup k formalizaci uvažování není přirozený, můžeme totiž např. zaručovat existenci objektů jen z toho důvodu, že jejich neexistence by vedla k rozporu v naší logice.

**Příklad.** (Motivační) Dokažte existenci dvou iracionálních čísel $a$, $b$, pro která platí, že $a^b$ je racionální číslo.

*Řešení.* Situaci rozdělíme na dva případy: buď je $\sqrt{2}^{\sqrt{2}}$ racionální nebo iracionální číslo. V prvním případě jsme hotovi (neboť $a = b = \sqrt{2}$ a $\sqrt{2}$ je, jak známo, iracionální). V druhém případě položíme $a = \sqrt{2}^{\sqrt{2}}$ a $b = \sqrt{2}$, dostáváme

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = 2,$$

takže jsme též hotovi.

Všimněte si, že v důkazu jsme čísla $a$, $b$ *nezkonstruovali*, ale jen jsme pomocí logiky zaručili, že nějaká taková čísla jsou. O jaká čísla ale jde, nemáme vůbec ponětí.

Pokud chceme význam formulí chápat tak, aby zákony jako vyloučení třetího nebyly (všeobecně) platné, musíme se vydat cestou jiné logiky.

### Intuicionistická logika a Heytingova interpretace

Intuicionismus (nebo také konstruktivismus) je matematický filozofický směr, který vnímá matematiku pouze jako konstruktivní duševní úsilí a odmítá ji redukovat na pouhou manipulaci se symboly. Jedním z jeho principů je, že abychom ukázali existenci nějakého objektu, musíme daný objekt zkonstruovat a poukázat na něj, tedy nestačí jen dojít ke sporu s jeho neexistencí.

Intuicionistická logika se pak snaží formalizovat myšlenky intuicionismu v logice (což už sám o sobě je trochu protimluv), jinými slovy vytvořit formální rámec, v němž bychom mohli provozovat matematiku rigorózně a zároveň i v intuicionistickém duchu.

Dobrou intuici pro intuicionistickou logiku navozuje tzv. důkazová interpretace, kterou navrhl Arend Heyting v roce 1934. Pracujeme v ní s důkazy, které postupně budujeme od podformulí k celé formuli.

(i) Pokud chceme dokázat tvrzení $A \wedge B$, musíme dokázat tvrzení $A$ a dokázat tvrzení $B$
(ii) Pokud chceme dokázat tvrzení $A \vee B$, musíme ukázat na jedno z tvrzení $A$ nebo $B$ a to dokázat.
(iii) Pokud chceme dokázat tvrzení $A \to B$, pak z každého důkazu $A$ musíme umět vyrobit důkaz $B$.
(iv) Pokud chceme dokázat tvrzení $\neg A$, pak z každého důkazu $A$ musíme odvodit spor.

**Příklad.** Zdůvodněte, že tvrzení $(A \wedge B) \to A$ je intuicionisticky platné.

**Příklad.** Zdůvodněte, že tvrzení $A \vee \neg A$ není intuicionisticky platné.

### Intuicionistická sémantika

Chceme-li formálně vyjádřit intuicionistický význam formulí, nevystačíme si s prostým ohodnocením pravdou a nepravdou, budeme vyžadovat složitější modely.

Jedním z moderních způsobů, jak zachycovat sémantiku neklasických logik, jsou tzv. Kripkovské modely. Stále budeme ohodnocovat formule (určovat, zda platí nebo neplatí), ale toto ohodnocení budeme provádět paralelně v několika *možných světech*, které se navzájem mohou nějak ovlivňovat přes *relaci dosažitelnosti*. Formálně pak možné světy tvoří vrcholy určitého grafu a relace dosažitelnosti budou jeho hrany.

V intuicionismu si můžeme představovat, že každý možný svět je souhrnem znalostí, které má matematik k dispozici – ve všech z něj dosažitelných světech má tyto znalosti také, a pokud v žádném světě dosažitelném z nějakého světa tvrzení neplatí, pak může v tomto světě usoudit jeho negaci.

**Definice.** (Kripkovský rámec) Dvojici $(V, \leq)$ nazveme *kripkovským rámcem*, je-li $(V, \leq)$ orientovaný graf, ve kterém platí:

(i) (*reflexivita*) každý vrchol $x$ je spojen hranou sám se sebou, tj. $x \leq x$;
(ii) (*tranzitivita*) pokud pro tři vrcholy platí, že jestli $x$ a $y$ jsou spojeny hranou a $y$ a $z$ jsou spojeny hranou, pak i $x$ a $z$ jsou spojeny hranou, tj.

$$x \leq y \wedge y \leq z \implies x \leq z.$$

Pokud pro dva vrcholy platí $x \leq y$, řekneme, že $y$ je *dosažitelný* z $x$.

**Definice.** (Kripkovský model) Trojici $(V, \leq, \Vdash)$ nazveme *kripkovským modelem*, je-li $(V, \leq)$ kripkovským rámcem a $\Vdash$ je binární relace na množině $V \times \mathrm{Fle}$, kde pro každý vrchol $x \in V$ a každé dvě formule $A, B \in \mathrm{Fle}$ platí

(i) (podmínka perzistence) je-li $p$ atom splňující $x \Vdash p$, pak pro každý dosažitelný vrchol $y$ z $x$ platí $y \Vdash p$;
(ii) $x \Vdash A \wedge B$ právě tehdy, když $x \Vdash A$ a $x \Vdash B$;
(iii) $x \Vdash A \vee B$ právě tehdy, když $x \Vdash A$ nebo $x \Vdash B$;
(iv) $x \Vdash A \to B$ právě tehdy, když pro každý dosažitelný vrchol $y$ z $x$ platí, že pokud $y \Vdash A$, pak i $y \Vdash B$;
(v) $x \Vdash \neg A$ právě tehdy, když pro každý dosažitelný vrchol $y$ z $x$ platí $y \nVdash A$.

O formuli $A$ řekneme, že *platí* ve vrcholu $x$, pokud $x \Vdash A$.

Relaci $\Vdash$ též můžeme nazvat jako ohodnocení, v intuicionistickém logice ale záleží na světě, ve kterém formule ohodnocujeme.

**Cvičení.** Platí pro libovolnou formuli $A$ a libovolný vrchol $x$ libovolného modelu následující implikace?

(i) $x \Vdash \neg A \implies x \nVdash A$,
(ii) $x \nVdash A \implies x \Vdash \neg A$.

**Definice.** (Intuicionistická tautologie) Formuli $A$ nazveme *intuicionistickou tautologií*, pokud pro každý vrchol $x$ každého kripkovského modelu $(V, \leq, \Vdash)$ platí $x \Vdash A$.

**Příklad.** Zdůvodněte, že pro libovolnou formuli $A$ je $A \to A$ intuicionistická tautologie.

*Řešení.* Ať je dán $(V, \leq, \Vdash)$ a vrchol $x \in V$. Uvažme libovolný vrchol $y$ dosažitelný z $x$, v něm zřejmě platí, že pokud $y \Vdash A$, pak $y \Vdash A$. Tedy z definice platnosti implikace $x \Vdash A \to A$.

**Věta.** (O perzistenci formulí) *Podmínka perzistence z definice kripkovského modelu platí pro libovolnou formuli (tj. nejen pro atomy).*

**Věta.** *Každá intuicionistická tautologie je i klasickou tautologií.*

*Důkaz.* (skeč) Rozmyslete si, že pokud formule není klasickou tautologií, pak umíte sestrojit jednoprvkový model, který bude (intuicionistickým) protipříkladem. □

### Úlohy

V následujících úlohách jsou $A$ a $B$ dané formule a $p$ je atom.

**Úloha 1.** Zdůvodněte, že $(A \wedge B) \to A$ a $(A \wedge B) \to B$ jsou intuicionistické tautologie.

**Úloha 2.** Zdůvodněte, že $A \to (A \vee B)$ a $B \to (A \vee B)$ jsou intuicionistické tautologie.

**Úloha 3.** Sestrojte protipříklad k formuli $\neg\neg p \to p$.

**Úloha 4.** Sestrojte protipříklad k formuli $p \vee \neg p$.

**Úloha 5.** Rozhodněte, zda je formule $A \to \neg\neg A$ intucionistickou tautologií.

### Návody

**1.** Uvaž libovolný vrchol a argumentuj o libovolném z něj dosažitelném vrcholu. Využij toho, že pokud ve vrcholu platí konjunkce, musí tam platit oba z konjunktů.

**2.** Pokud ve vrcholu platí nějaký z disjunktů, musí tam platit disjunkce.

**3.** Stačí ti dvouprvkový model, ve kterém v jednom vrcholu bude $p$ ohodnoceno kladně a v druhém záporně.

**4.** Můžeš zrecyklovat model z předchozí úlohy.

**5.** Najdi kritérium platnosti formule $\neg\neg A$ a využij větu o perzistenci formulí.

### Literatura a zdroje


[1] Vítězslav Švejdar: *Neúplnost a Gödelovy věty*, Filozofická fakulta UK, 2022/2023.

[2] Vítězslav Švejdar: *Logika – neúplnost, složitost a nutnost*, Academia, 2002, *http://www1.cuni.cz/~svejdar/?s=book*.

[3] Dirk van Dalen: *Intuicionistic logic*, *https://ulrikbuchholtz.dk/80-518-818/vanDalen-2001.pdf*. In *The Blackwell Guide to Philosophical Logic*, Blackwell Publishers, 2001.

[4] Anša Vernerová: *Neklasické logiky*, seriál MKS, 2006/2007.

# Teleskopické součty a součiny

Daniel Perout

Abstrakt. Příspěvek se zabývá metodou teleskopických součtů a součinů a obsahuje několik příkladů na její procvičení.

Princip teleskopických součtů a součinů je založen na vhodném prodloužení výrazu, který následně upravíme tak, že dostaneme mnohem jednodušší výraz než před „prodloužením“. Ač se to na první pohled může zdát zvláštní, tato technika nám usnadní řešení řady příkladů.

**Úmluva.** V celém příspěvku budeme počítat s $n > 1$.

Při metodě teleskopických součtů se obvykle snažíme každý ze sčítanců přepsat ve tvaru rozdílu tak, že většina členů takto upraveného součtu se nakonec navzájem odečte.

**Příklad.** Určete hodnotu výrazu $\dfrac{1}{1\cdot 2}+\dfrac{1}{2\cdot 3}+\cdots+\dfrac{1}{n\cdot(n+1)}$.

**Příklad.** Určete hodnotu výrazu $1!\cdot 1+2!\cdot 2+\cdots+n!\cdot n$.

Při teleskopických součinech chceme jednotlivé činitele upravit tak, aby se jich co nejvíc zkrátilo a zůstal nám pouze jednoduchý výraz.

**Příklad.** Dokažte, že $\left(1+\dfrac{1}{1\cdot 3}\right)\cdot\left(1+\dfrac{1}{2\cdot 4}\right)\cdots\left(1+\dfrac{1}{(n-1)\cdot(n+1)}\right)<2$.

**Příklad.** Dokažte, že $\left(1-\dfrac{1}{4}\right)\cdot\left(1-\dfrac{1}{9}\right)\cdots\left(1-\dfrac{1}{n^2}\right)=\dfrac{n+1}{2n}$.

### Úlohy

**Úloha 1.** Určete hodnotu $\dfrac{1}{1\cdot 2\cdot 3}+\dfrac{1}{2\cdot 3\cdot 4}+\cdots+\dfrac{1}{n\cdot(n+1)\cdot(n+2)}$.

**Úloha 2.** Dokažte, že platí $\dfrac{1}{2^2}+\dfrac{1}{3^2}+\cdots+\dfrac{1}{n^2}<1$.

**Úloha 3.** Dokažte, že platí $\dfrac{1}{\sqrt{1}+\sqrt{2}}+\dfrac{1}{\sqrt{2}+\sqrt{3}}+\cdots+\dfrac{1}{\sqrt{99}+\sqrt{100}}=9$.

**Úloha 4.** Dokažte, že platí $1+\dfrac{1}{1+2}+\dfrac{1}{1+2+3}+\cdots+\dfrac{1}{1+2+\cdots+n}<2$.

**Úloha 5.** Dokažte, že platí $\dfrac{1}{2}+\dfrac{3}{2\cdot 4}+\dfrac{5}{2\cdot 4\cdot 6}+\cdots+\dfrac{2n-1}{2\cdot 4\cdots 2n}+\cdots=1$.

**Úloha 6.** Dokažte, že platí $\dfrac{1}{1\cdot 5}+\dfrac{1}{3\cdot 7}+\cdots+\dfrac{1}{(2n-1)\cdot(2n+3)}<\dfrac{1}{3}$.

**Úloha 7.** Dokažte, že platí

$$\left(1+\frac{1}{2}-\frac{1}{4}-\frac{1}{8}\right)\left(1+\frac{1}{3}-\frac{1}{9}-\frac{1}{27}\right)\cdots\left(1+\frac{1}{n}-\frac{1}{n^2}-\frac{1}{n^3}\right)=\frac{(n+1)^2}{4n}.$$

**Úloha 8.** Dokažte, že platí

$$\frac{3}{1!+2!+3!}+\frac{4}{2!+3!+4!}+\cdots+\frac{2019}{2017!+2018!+2019!}<\frac{1}{2}.$$

**Úloha 9.** Určete hodnotu $\sqrt{1+1+\dfrac{1}{4}}+\sqrt{1+\dfrac{1}{4}+\dfrac{1}{9}}+\cdots+\sqrt{1+\dfrac{1}{n^2}+\dfrac{1}{(n+1)^2}}$.

**Úloha 10.** Zjednodušte

$$\frac{1}{2\cdot\sqrt{1}+1\cdot\sqrt{2}}+\frac{1}{3\cdot\sqrt{2}+2\cdot\sqrt{3}}+\cdots+\frac{1}{(n+1)\cdot\sqrt{n}+n\cdot\sqrt{n+1}}.$$

**Úloha 11.** Dokažte, že platí $\dfrac{1}{2}\cdot\dfrac{3}{4}\cdots\dfrac{99}{100}<\dfrac{1}{10}$.

**Úloha 12.** Dokažte, že platí $\dfrac{2^3+1}{2^3-1}\cdot\dfrac{3^3+1}{3^3-1}\cdots\dfrac{n^3+1}{n^3-1}<\dfrac{3}{2}$.

**Úloha 13.** Dokažte, že platí $\left(1-\dfrac{1}{8}\right)\cdot\left(1-\dfrac{1}{27}\right)\cdots\left(1-\dfrac{1}{n^3}\right)>\dfrac{1}{2}$.

**Úloha 14.** Určete hodnotu $\displaystyle\sum_{n=2}^{\infty}\frac{F_n}{F_{n-1}\cdot F_{n+1}}$, kde $F_n$ značí $n$-té Fibonacciho číslo.

**Úloha 15.** Určete hodnotu $\displaystyle\sum_{n=2}^{\infty}\frac{1}{F_{n-1}\cdot F_{n+1}}$.

**Úloha 16.** Dokažte, že platí $\dfrac{2^{2m}}{2\sqrt{m}}\le\binom{2m}{m}\le\dfrac{2^{2m}}{\sqrt{2m}}$.

### Návody

**1.** Rozlož zlomek $\frac{1}{(n-1)n(n+1)}$ na $\frac{1/2}{n-1} - \frac{1}{n} + \frac{1/2}{n+1}$.

**2.** Uvědom si, že $\frac{1}{n^2} < \frac{1}{n(n-1)}$.

**3.** Usměrni zlomky.

**4.** Použij vzorec pro součet čísel od 1 do $n$.

**5.** Neformálně: využij toho, že každý člen nekonečné řady (kromě prvního) má levého a pravého souseda, kde se může něco pochálovat. Formálně: najdi vzorec pro částečný součet a ukaž, že limita součtů je 1 pro $n \to \infty$.

**6.** Rozlož na parciální zlomky.

**7.** Převeď na společného jmenovatele a rozlož čitatel

$$n^3 + n^2 - n - 1 = (n^2 - 1)(n + 1) = (n + 1)^2(n - 1).$$

**8.** Rozlož zlomek $\frac{k+2}{k!+(k+1)!+(k+2)!} = \frac{1}{k!(k+2)} = \frac{k+2-1}{(k+2)!}$.

**9.** Převeď na společného jmenovatele a čitatel rozlož na čtverec.

**10.** Převeď do tvaru $\frac{1}{\sqrt{n}\cdot\sqrt{n+1}\cdot\left(\sqrt{n}+\sqrt{n+1}\right)}$ a zkus vhodně usměrnit.

**11.** Vezmi si velmi podobný a o trochu vetší výraz, který by se se zadaným výrazem mohl zkrátit, konkrétně $\frac{2}{3} \cdot \frac{4}{5} \cdots \frac{100}{101}$. Zkus zkoumat jejich součin.

**12.** Rozlož čitatele a jmenovatele podle vzorců $a^3 - b^3$ a $a^3 + b^3$. Poté si uvědom, že platí $n^2 + n + 1 = (n + 1)^2 - (n + 1) + 1$.

**13.** Buď si uvědom, že už jsme to dokázali, nebo to rozlož a zkus něco „zapomenout“.

**14.** Rozlož na parciální zlomky.

**15.** Rozlož na parciální zlomky.

**16.** Odhadni zvlášť shora a zvlášť zdola. Vhodně vytkni $2^{2m}$ z $\binom{2m}{m}$ tak, aby zbyl výraz podobný výrazu z poslední úlohy.

### Literatura a zdroje

Tento příspěvek je pouze stylisticky upravený příspěvek Fíly Čermáka, jehož příspěvek je z velké části převzatý z přednášek Adély Kostelecké a Aničky Mlezivové. Všem zmíněným bych tímto chtěl poděkovat.

[1] Filip Čermák: *Teleskopické součty a součiny*, Zásada, 2021.
[2] Anna Mlezivová: *Teleskopické součty a součiny*, Branná, 2019.
[3] Adéla Kostelecká: *Teleskopické součty a součiny*, Lipová-lázně, 2016.
[4] Jaroslav Švrček: *O teleskopických součtech a součinech*, *https://is.muni.cz/el/1431/jaro2010/MA572/um/didmat2.pdf*.
[5] Brilliant: *Telescoping Series – Sum*, *https://brilliant.org/wiki/telescoping-series/*.
[6] Martin Balko: *Přednáška z Kombinatoriky a grafů 1*, MFF UK, 2018/2019.

# Extremální princip

Martin Raška

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

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

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

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

Nyní se můžeme pustit do samostatného počítání.

### Příklady

**Příklad 1.** Lenka dokázala, že prvočísel je konečně mnoho. Ukažte, že se spletla.

**Příklad 2.** Rozárka žije v kraji, kde jsou města vystavena v takových rozestupech, že trojúhelník s vrcholy v libovolných třech městech má rozlohu menší než Zimbabwe. Ukažte, že všechna města se vejdou na plochu menší, než má Mongolsko.[1]

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

[1] Poradím, že Zimbabwe má rozlohu 390 580 km$^2$ a Mongolsko 1 566 500 km$^2$.

**Příklad 4.** V Přerovském království navrhli leteckou dopravu tak, že mezi každými dvěma městy existují letecké linky právě jedním ze dvou směrů. Ukažte, že existuje město, do kterého se dá z každého města dostat nanejvýš s jedním přestupem.

**Příklad 5.** Na Helčině oslavě narozenin se každý pohádal s nejvýše třemi lidmi. Je možné účastníky slavnosti rozdělit do dvou skupin tak, aby každý měl ve své skupině nejvýše jednoho jiného člověka, se kterým se pohádal?

**Příklad 6.** Jindřichův Hradec se dělí na obydlené a neobydlené části. Jindrovi se zdálo, že spojíme-li úsečkou dvě obydlené části, bude tato úsečka obsahovat i neobydlenou část a naopak. Ukažte, že pak všechny části leží na přímce. Části vesnice považujeme za body a předpokládáme, že jich je konečně mnoho.

**Příklad 7.** Barbora si na zahrádce stoupla ke čtverečkovanému záhonu $n \times n$ a rozestavila na něj květináče s chryzantémami. Potom přišel Lucian a všiml si, že kdykoli máme v záhonu prázdný čtvereček, tak v řádku a sloupci, které daný čtvereček obsahují, je dohromady alespoň $n$ chryzantém. Dokažte, že Barbora rozestavila alespoň $\frac{n^2}{2}$ chryzantém.

**Příklad 8.** Martin si do sešitu nakreslil konečně mnoho bodů. Přišli k němu Štěpán s Tomášem a všimli si, že každá přímka, která prochází skrz dva body, prochází i nějakým třetím bodem. Ukažte, že všechny body leží v jedné přímce.

**Příklad 9.** V Praze je $n$ hradů a $n$ studen takových, že žádné tři stavby neleží na jedné přímce. Johana s Viki se shodly, že by bylo vhodné každý hrad spojit s jednou studnou přímou cestou aniž by se cesty křížily. Je možné to provést?

**Úloha 10.** Pomozte Aličce najít všechna kladná řešení dané soustavy rovnic:

$$x_1 + x_2 = x_3^2, \quad x_2 + x_3 = x_4^2,$$
$$x_3 + x_4 = x_1^2, \quad x_4 + x_1 = x_2^2.$$

**Příklad 11.** Marek tvrdí, že každý mnohostěn má alespoň dvě stěny se stejným počtem hran. Ivan mu to ale odmítá věřit. Kdo z chlapců má pravdu?

**Příklad 12.** Po drtivém útoku Liberce na americký Pentagon byla podstava této budovy zdeformována do tvaru obecného konvexního pětiúhelníku. Markéta ukázala, že i tak z ní jde vybrat tři úhlopříčky, z nichž lze vytvořit trojúhelník. Ukažte to taky!

**Příklad 13.** Markéta, Jan a jejich pět kamarádů sedí kolem kruhového stolu. Každý před sebou má pohár s mlékem. Dohromady mají mléka tři litry. Nejdřív první z nich vstane a rozdělí své mléko rovnoměrně mezi ostatní. Pak postupně proti směru hodinových ručiček totéž udělají i zbývající spolusedící. Když skončí, má každý z nich tolik mléka, kolik měl na začátku. Kolik to je?

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

**Úloha 15.** Patrik si vzal svých šest oblíbených kruhů a nakreslil je tak, aby se všechny protínaly v alespoň jednom společném bodě. Ukažte, že jeden z těchto kruhů obsahuje střed dalšího kruhu.

**Příklad 16.** Verča s Erikem hráli 3D šachy a přitom je napadla otázka, kolik nejméně věží je potřeba, aby ohrožovaly všechna políčka šachovnice $n \times n \times n$. Kolik to je?

**Úloha 17.** David si do notýsku napsal kladná čísla taková, že součet součinů všech jejich dvojic byl roven jedné. Dominik se pak rozhodl, že ho poškádlí a jedno číslo škrtne. Ukažte, že může škrtnout takové, aby součet zbylých čísel byl menší než $\sqrt{2}$.

### Návody

**1.** To zvládneš!

**2.** Vezmi si trojúhelník s největším obsahem a kresli si :).

**3.** Řešení minimalizující $a^2 + b^2$.

**4.** Vezmi si město s nejvíce příchozími linkami.

**5.** Uvažuj rozdělení minimalizující celkový počet rozhádaných dvojic, kde oba z dvojice jsou ve stejné skupině.

**6.** Co kdyby existoval trojúhelník, jehož vrcholy jsou všechny (ne)obydlené?

**7.** Uvažuj řádek/sloupec s nejmenším počtem chryzantém.

**8.** Dvojice (přímka, bod mimo ní) minimalizující vzdálenost mezi nimi.

**9.** Uvažuj párování s nejmenším součtem délek.

**10.** Odhadni nejmenší a největší z čísel.

**11.** Uvaž stěnu s nejvíce hranami.

**12.** Uvaž nejdelší diagonálu a vzpomeň si na příklad 9.

**13.** Uvažuj u každého člověka objem mléka těsně předtím než ho rozdělil. Ukaž, že tato velikost je pro všechny stejná.

**14.** Skoro jako bych podobnou úlohu už někde viděl.

**15.** Spoj si společný bod se středy kružnic a minimalizuj úhel.

**16.** Vyjde $\frac{n^2}{2}$ pro $n$ sudé, $\frac{n^2+1}{2}$ pro $n$ liché. Pro důkaz odhadu uvažuj rovinu (rovnoběžnou s nějakou stěnou krychle) obsahující nejméně věží a odhaduj.

**17.** Vezmi si největší číslo a odhadni druhou mocninu součtu ostatních.

### Literatura a zdroje

Tento příspěvek je téměř kopií příspěvku Martina Rašky z jarního soustředění 2019, který je téměř kopií příspěvku Martina Sýkory z jarního soustředění 2017, za což bych jim oběma tímto chtěl poděkovat.

[1] Arthur Engel: *Problem-Solving Strategies*, Springer, 1997.

[2] Alča Skálová: *Extremální princip*, Blansko-Obůrka, 2011.

# Geometrické podvádění

Martin Raška

Abstrakt. Chtěli jste někdy zjistit, jak vychází řešení geometrické úlohy, ale nemuset při tom přemýšlet? Rádi si kreslíte čáry a kolečka, ale na papíře to vypadá moc nakřivo? Pak je tato přednáška právě pro vás! Ukážeme si, jaké triky se dají dělat s Geogebrou a jak s její pomocí řešit geometrické úlohy, pokud opravovatele nezajímá postup.

*Hmm, ale ony všechny soutěže chtějí nějaké otravné postupy a důkazy ... Skoro jako by chtěli, aby jim řešitelé přemýšleli ... Kéž by tak existovala nějaká soutěž, kde stačí výsledek zaokrouhlený na* 5 *desetinných míst ... Ajooo, ještě že máme MathRace!*

**Úloha.** Uvažujme pravidelný 2021-úhelník s délkou strany rovnou jedné. Nechť $A$, $B$, $C$, $D$, $E$ je pět libovolných po sobě jdoucích vrcholů. Označme průsečík přímek $AB$ a $DE$ jako $X$. Jaká je délka úsečky $CX$? (MathRace 2021–31)

**Úloha.** Pata výšky pravoúhlého trojúhelníka o obsahu 1 dělí přeponu v poměru $3 : 1$. Určete obsah pravoúhlého rovnoramenného trojúhelníku, který má stejnou délku přepony. (MathRace 2020–28)

### Prostě to zkonstruuj!

**Úloha 1.** Máme tětivový lichoběžník $ABCD$. Víme, že velikost úhlu $ABC$ je $63°$ a velikost úhlu $DAC$ činí $21°$. Označme si průsečík úhlopříček v našem lichoběžníku jako $S$. Kolik stupňů měří úhel $BSC$? (MathRace 2021–11)

**Úloha 2.** V roce 2093 se znovu začaly stavět Brněnské hradby. Extravagantní architekt navrhl stavbu ve tvaru pravidelného 2021-úhelníku s délkou strany 8. Bylo ovšem navíc potřeba ohradit oblast bývalého Hlavního nádraží, ze které se v té době stalo zvrhlé a divoké území nepřístupné běžným lidem. Proto kolem něj architekt postavil trojúhelník následujícím způsobem: nechť $A$, $B$, $C$ jsou tři po sobě jdoucí body pravidelného 2021-úhelníka. Uvažujme body $X$, $Z$ ležící na polopřímkách opačných k polopřímkám $BA$, $CB$. Navíc $|BX| = 1645$ a $|CZ| = 1782$. Jaká je vzdálenost $|XZ|$? (MathRace 2021–1)

**Úloha 3.** Tětivový čtyřúhelník $ABCD$ splňuje $|\sphericalangle DAC| = |\sphericalangle ADB|$, $|AB| = 13$, $|BC| = 4$ a $|AD| = 14$. Určete velikost úsečky $AC$. (MathRace 2021–18)

**Úloha 4.** Máme trojúhelník se stranami $a$, $b$, $c$, pro které platí $5(a+b+c)(a+b-c) = 12ab$. Určete velikost v radiánech úhlu naproti straně $c$. (MathRace 2020–43)

**Úloha 5.** Je dána kružnice $k$. Body $L$ a $M$ vytnou na kružnici $k$ tětivu délky 28. Kružnice $l$ a $m$ mají vnitřní dotyk s kružnicí $k$ v bodech $L$ a $M$, přičemž kružnice $l$ a $m$ mají menší poloměr než $k$. Na kružnicích $l$ a $m$ jsme zvolili body $A$ a $B$ takové, že existuje bod $C$ ležící v průniku úseček $AB$ a $LM$. Jaká je největší možná hodnota $|AC| \cdot |BC|$? (MathRace 2021–28)

**Úloha 6.** Mějme tětivový čtyřúhelník $ABCD$ takový, že se polopřímky $AD$, $BC$ protínají. Označme průsečík polopřímek $AD$ a $BC$ jako $E$. Platí, že $|AB| = 1$, $|\sphericalangle CAB| = \frac{1}{2022}^\circ$, $|\sphericalangle DBA| = \frac{20219}{2022}^\circ$ a $|\sphericalangle AEB| = 10^\circ$. Určete délku poloměru kružnice opsané čtyřúhelníku $ABCD$. (MathRace 2022–24)

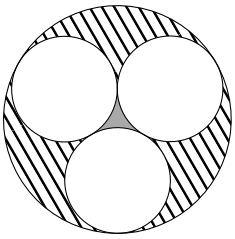
**Zkus si něčeho všimnout!**

**Úloha 7.** V kartézské souřadné soustavě je dán trojúhelník $ABC$, kde $A = [0,0]$, $B = [1,0]$ a $C = [\frac{1}{2}, \frac{\sqrt{3}}{2}]$. Nalezněte vnitřní bod $X$ trojúhelníka $ABC$ takový, že obsahy trojúhelníků $ACX$, $ABX$ a $BCX$ budou v poměru $1:2:3$. Jako výsledek zadejte součin $x$-ové a $y$-ové souřadnice bodu $X$. (MathRace 2022–16)

**Úloha 8.** V rovině jsou dány tři kružnice po řadě se středy $R$, $S$, $T$ a poloměry $r$, $s$, $t$, z nichž každé dvě se dotýkají. Nalezněte $|\sphericalangle RTS|$ v radiánech, jestliže platí $r+s+t = \frac{2rs}{t}$. (MathRace 2022–39)

**Úloha 9.** Kuba si nakreslil na zem tečnový čtyřúhelník $ABCD$, jehož strana $AB$ má délku 16 a kružnice vepsaná $k$ má střed $I$. Pak přišel Kuba a protl úsečky $BI$, $CI$, $DI$ s $k$ v bodech po řadě $B_0$, $C_0$, $D_0$. Tečna v bodě $B_0$ ke $k$ protíná strany $AB$, $BC$ po řadě v bodech $B_1$, $B_2$. Obdobně tečna v $C_0$ protíná strany $BC$, $CD$ v bodech $C_1$, $C_2$ a tečna v $D_0$ protíná strany $CD$, $DA$ v bodech $D_1$, $D_2$. Kubové si pak všimli, že obvody trojúhelníků $BB_1B_2$, $CC_1C_2$ a $DD_1D_2$ jsou po řadě 17, 20 a 13. Jak dlouhá je strana $AD$? (MathRace 2022–36)

**Úloha 10.** Na obrázku se nachází tři kružnice s poloměrem 1, které se navzájem dotýkají, a jedna kružnice, která se dotýká každé z nich. Jaký je poměr obsahů šrafované a plné oblasti?



(MathRace 2021–35)

### Fígle a tříčky

**Úloha 11.** Sluneční soustava je podobná té naší, Sluneční soustavě. Země obíhá kolem Slunce a Měsíc kolem Země, ale Měsíc je ve dvakrát větší vzdálenosti od Země než Země od Slunce. Měsíc oběhne celou Zemi za jeden měsíc, Země oběhne Slunce za dvanáct měsíců. Měsíc obíhá Zemi po směru hodinových ručiček, zatímco Země obíhá Slunce proti směru. Kolikrát za dvanáct měsíců tvoří Země, Měsíc a Slunce pravoúhlý trojúhelník? (MathRace 2021–12)

**Úloha 12.** V Hloupětíně je vyhlášený italský zmrzlinář. Jeho zmrzlina se skládá z koule o poloměru 5 cm a kornoutu ve tvaru kužele, který se koule dotýká (tzn. povrchové úsečky kužele, které začínají ve vrcholu kužele a končí v bodě dotyku, jsou tečny ke kouli, a základna kužele je kruh vymezen dotykovou kružnicí). Výška celé zmrzliny je 18 cm. Určete objem kužele vymezeného kornoutem.

(MathRace 2021–30)

**Úloha 13.** Najděte všechny pravoúhlé trojúhelníky ABC s celočíselnými délkami stran $|AB| > |AC| > |BC|$ a obsahem nejvýše 100, pro které lze číslo $\operatorname{tg}(|\sphericalangle BAC|)$ vyjádřit jako podíl dvou přirozených čísel lišících se o 7. Jako řešení zadejte součet všech obvodů těchto trojúhelníků. (MathRace 2022–15)

**Úloha 14.** V rovině je dán čtverec o délce strany 1. Opišme mu pravidelný osmiúhelník tak, aby každý vrchol čtverce byl středem každé druhé strany osmiúhelníka. Osmiúhelníku stejným způsobem opišme pravidelný šestnáctiúhelník, tomu pravidelný dvaatřicetiúhelník a tímto způsobem pokračujme do nekonečna. Jaký je nejmenší poloměr kružnice se středem v průsečíku úhlopříček čtverce, do které se všechny takto vytvořené $2n$-úhelníky vejdou? (MathRace 2021–40)

### Návody

**1.** Zvol si jeden bod pohyblivě a zkonstruuj, co zvládneš. Pak hýbej, aby vše sedělo!

**2.** Prostě to zkonstruuj!

**3.** Zvol si například $D$ pohyblivě ve správné vzdálenosti od $A$, dokresli zbytek a hýbej.

**4.** Hýbej, dokud to nebude dost přesně!

**5.** Zkontruuj a hýbej!

**6.** Zvol si volně například $C$, a pak dohýbej, aby $\sphericalangle AEB$ vycházel.

**7.** Pokud nechceš hýbat bez rozmyslu (což jde taky!), zkus si všimnout, kde jsou poměry konstantní.

**8.** Zkus hýbat s poloměrem $t$ a ostatní mít fixní.

**9.** Všimni si, kde musí ležet $I$, pokud má platit vztah pro první obvod.

**10.** Středy menších kružnic tvoří rovnostranný trojúhelník.

**11.** Udělej si pomocí posuvníků simulaci a počítej :)

**12.** Prostě to zkonstruuj! (Ale ve 3D :O)

**13.** S dobrými posuvníky to jde rychle. Nezapomeň na nezkrácené zlomky ;)

**14.** Pokud nechceš umřít, tipni si výsledek. Jakou dobrou konstantu by tak řešení mohlo obsahovat?

### Výsledky

**1.** $\frac{10332}{123}$.

**2.** $4 \cdot 7.2549055 \cdot 5$.

**3.** $7 \cdot \cos(0) \cdot \frac{6}{14} \cdot 5$.

**4.** $\frac{8559}{6250}$.

**5.** $(5 \cdot 9 - 2^5 + 1)(-8 + 7 \cdot 6 - 5 \cdot 4)$.

**6.** $\frac{119254}{23056} \cdot \frac{161392}{1669556}$.

**7.** $\frac{12.31744}{128}$.

**8.** $6.72539^2 - 43.9999106521$.

**9.** $16.52 \cdot 20 \cdot 12 \cdot 15 - 31 \cdot 2 \cdot 137 \cdot 7$.

**10.** $30 + \frac{10}{9+\frac{1}{1+\frac{1}{24.1}}} + 0.00009$.

**11.** $9^3 - 8^3 - 165$.

**12.** $\frac{5189}{21} - 0.00046\overline{809523}$.

**13.** $2 \cdot 7 \cdot 19 - 76$.

**14.** $\frac{3927}{5000}$.

### Literatura a zdroje

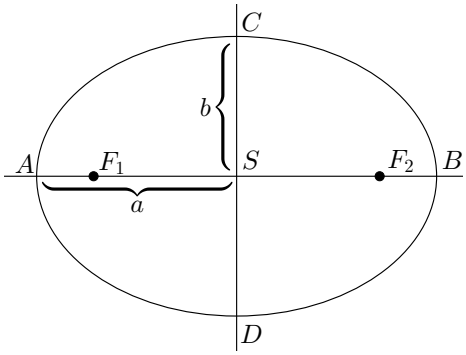
Čerpal jsem z vlastních životních zkušeností a ze stránek soutěže MathRace: *http://brkos.math.muni.cz/mathrace/*.

# Kuželosečky

Matouš Šafránek

Abstrakt. Podíváme se, co všechno můžeme zjistit o kuželosečkách i bez analytické a projektivní geometrie. Ukážeme si trojí definici, základní vlastnosti a spoustu úloh.

**Definice.** *Elipsa* je množina všech bodů v rovině, které mají od dvou daných bodů $F_1$, $F_2$ (ohnisek) konstantní součet vzdáleností.

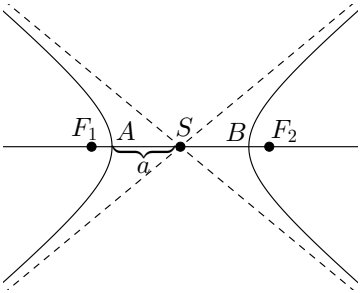



Elipsa je zřejmě souměrná podle přímky $F_1F_2$ a podle osy úsečky $F_1F_2$. Těmto přímkám říkáme *hlavní* a *vedlejší* osa. Někdy tak říkáme jen úsečkám, která na těch přímkách elipsa vymezí. Pak má smysl zavést délku hlavní a vedlejší osy, typicky se však používají jejich poloviny, *délka hlavní poloosy* značená $a$ a *délka vedlejší poloosy* značená $b$.

**Cvičení.** Konstantní součet vzdáleností bodů elipsy od ohnisek je roven $2a$.

**Cvičení.** Kružnice je speciální případ elipsy, když jsou ohniska totožná. Poloměr má $a$.

**Definice.** *Hyperbola* je množina všech bodů v rovině, které mají od dvou daných různých bodů $F_1$, $F_2$ (ohnisek) konstantní rozdíl vzdáleností (v absolutní hodnotě).




Podobně jako u elipsy má hyperbola osy a má konstantní rozdíl vzdáleností bodů od ohnisek, který je roven $2a$. Vedlejší (polo)osu nebudeme řešit.

Hyperbola má dvě *asymptoty*, přímky, ke kterým je tím blíž čím dál je od středu, ale nikdy se jich nedotkne.

**Definice.** *Parabola* je množina všech bodů v rovině, které mají od dané přímky $d$ (řídicí přímky) a bodu $F$ (ohniska) mimo ni stejnou vzdálenost.

### Jednotné definice

Teď zjistíme, proč se jim říká kuželosečky. Na chvíli se podíváme do prostorové geometrie.

**Definice.** *Rotační kuželovou plochu* vykreslí přímka, když se otáčí okolo různoběžky. Dále jí budeme říkat prostě *kužel*.

**Věta.** (Quételetova-Dandelinova) *Řez kužele rovinou neprocházející vrcholem je elipsa, parabola nebo hyperbola.*

**Věta.** (dodatek) *Množina všech bodů v rovině, které mají od daného bodu $F$ (ohniska) a dané přímky $d$ (řídicí přímky) konstantní poměr vzdáleností, je kuželosečka.*

Pokud je poměr menší než 1 (blíž k bodu), je to elipsa. Pokud je větší (dál od bodu), je to hyperbola. Pro parabolu jsme žádnou novou definici nezískali. Pokud je poměr 1, je tato definice stejná jako původní definice paraboly.

**Poznámka.** Degenerovaným případům, když rovina protíná kužel ve vrcholu, říkáme singulární kuželosečky. Ty nejsou moc zajímavé. Naopak se v nich některá tvrzení rozbíjí. Ostatní definice mají také degenerované případy, například když je $2a = |F_1F_2|$. Až na následující cvičení je už nebudeme řešit.

**Cvičení.** Rozmyslete si, jak můžou vypadat singulární kuželosečky. Pomocí toho se dá ukázat, že když kuželosečka není singulární, může s ní mít přímka nejvýš dva společné body.

**Cvičení.** Jaký je řez válcové plochy?

Elipsa a hyperbola mají spoustu „opačných“ vlastností. Obyčejně u jedné uvažujeme směr k ohnisku a u druhé od ohniska. Parabola je něco mezi nimi. Často na

ni můžeme koukat jako na elipsu, která má druhé ohnisko nekonečně daleko na ose směrem dovnitř, anebo na hyperbolu, která má druhé ohnisko nekonečně daleko na ose směrem ven.

Sice musíme dávat pozor na to, že tahle úvaha není vždy automaticky funkční, ale v úlohách si například odpouštíme formulaci pro parabolu.

**Věta.** *Na kuželosečce $k$ s ohnisky $F_1$, $F_2$ leží bod $T$. Tečna ke $k$ v bodě $T$ je osa úhlu $F_1TF_2$.*

U elipsy to je vnější úhel, u hyperboly vnitřní. Rozmyslete si (ukážeme si), jak je to u paraboly. Toto znamená, že když něco vyjde z ohniska elipsy kterýmkoliv směrem a o elipsu se to odrazí, dorazí to do druhého ohniska (a to za konstantní dobu). Tato vlastnost se používá hlavně s vlnami (zvukovými nebo světelnými), viz třeba eliptické šeptající galerie, posluchárny na Matfyzu (no, možná), parabolické antény a reflektory.

### Na rozehřátí

**Úloha 1.** Jaká je množina středů všech kružnic, které se vnějškem dotýkají

(1) dvou kružnic mimo sebe?
(2) dvou kružnic v sobě?
(3) kružnice a přímky mimo ni?

**Úloha 2.** Na elipse s ohnisky $F_1$, $F_2$ leží dva různé body $E_1, E_2$. Ukažte, že existuje hyperbola s ohnisky $E_1, E_2$, na které leží body $F_1$, $F_2$.

**Úloha 3.** Protíná se hyperbola a elipsa se stejnými dvěma ohnisky. Ukažte, že jsou na sebe kolmé neboli že jsou na sebe v každém průsečíku kolmé jejich tečny.

### Základní tvrzení

**Úloha 4.** Kuželosečka má ohniska $F_1$, $F_2$. Ukažte, že množina zrcadlových obrazů bodu $F_2$ podle všech tečen je kružnice se středem v $F_1$. U paraboly ukažte, že je to řídicí přímka.

**Úloha 5.** Jaká je množina pat kolmic z ohnisek na všechny tečny?

**Úloha 6.** Na elipse s ohnisky $F_1$, $F_2$ leží body $S$, $T$. Tečny v $S$ a $T$ se protnou v bodě $P$. Ukažte, že platí $\sphericalangle SPF_1 = \sphericalangle F_2PT$.[1]

**Úloha 7.** V kuželosečce s ohnisky $F_1$, $F_2$ prochází ohniskem $F_1$ tětiva $ST$. Tečny v $S$ a $T$ se protnou v bodě $P$. Ukažte, že kružnice vepsaná, resp. připsaná (u elipsy, resp. hyperboly) trojúhelníku $F_2ST$ má střed $P$ a strany $ST$ se dotýká v bodě $F_1$.

**Úloha 8.** Na kuželosečce s ohnisky $F_1$, $F_2$ leží body $S$, $T$. Tečny v $S$ a $T$ se protnou v bodě $P$. Ukažte, že $P$ leží na ose úhlu $SF_1T$.

[1] Platí i pro zbylé kuželosečky, akorát se pokaždé musí vzít orientovaný úhel mezi tečnou a spojnicí s ohniskem.

### Další úlohy

**Úloha 9.** Trojúhelníky $ABC$, $ABD$ mají stejně dlouhé obvody. Osy vnitřních úhlů $CAD$ a $CBD$ se protnou v bodě $P$. Dokažte, že $|\sphericalangle APC| = |\sphericalangle BPD|$.

(Rumunské výběrko 2015)

**Úloha 10.** Na parabole s ohniskem $F$ leží body $S$, $T$. Jejich kolmé průměty na řídicí přímku označíme $S'$,$T'$. Tečny v $S$ a $T$ se protnou v bodě $P$. Dokažte, že je $P$ opsiště trojúhelníku $FS'T'$.

**Úloha 11.** Na kuželosečce s ohnisky $F_1$, $F_2$ leží body $S$, $T$. Tečny v $S$ a $T$ se protnou v bodě $P$. Ukažte, že má čtyřúhelník $F_1SF_2T$ kružnici vepsanou nebo připsanou[2] a ta má za střed $P$.

**Úloha 12.** Je dán trojúhelník $ABC$ a bod $F_1$, který neleží na žádné ze stran (za strany považujeme celé přímky). Sestrojte bod $F_2$ takový, že existuje kuželosečka s ohnisky $F_1$, $F_2$, která se dotýká všech stran trojúhelníka. Pro jaké polohy bodu $F_1$ to bude parabola?

Mimochodem, poznáváte tuto dvojici bodů?

**Úloha 13.** Dokažte, že množina bodů, které vidí parabolu pod pravým úhlem[3], je řídicí přímka.

**Úloha 14.** Do $2n$-úhelníku je vepsána elipsa. Obarvěme strany mnohoúhelníku střídavě bíle a černě. Dokažte, že součet úhlů, pod kterými jsou z ohniska vidět bílé strany, je roven $180°$.

**Úloha 15.** Znáte ohniska kuželosečky a délku hlavní poloosy. Máte daný bod $B$ mimo kuželosečku. Sestrojte tečny ke kuželosečce vedoucí tímto bodem.

**Úloha 16.** Na parabole s ohniskem $F$ a osou $o$ leží bod $T$. Tečna v $T$ protne osu $o$ v bodě $M$, normála (kolmice na tečnu) v $T$ protne osu $o$ v bodě $N$. Dokažte, že je $F$ střed úsečky $MN$. Je-li dále $P$ kolmý průmět $T$ na $o$, dokažte, že je vrchol paraboly střed úsečky $MP$ a že úsečka $NP$ má pevnou délku nehledě na polohu bodu $T$.

**Úloha 17.** Jsou dány dvě různé elipsy se společným ohniskem. Dokažte, že mají nejvýše dva společné body. Proč to neplatí s hyperbolami? (IMC 2008, rozšířeno)

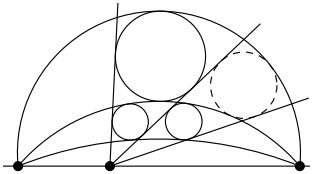
**Úloha 18.** Dokažte, že množina bodů, které vidí elipsu pod pravým úhlem, je kružnice. Platí to i pro hyperbolu?

**Úloha 19.** Je dána parabola. Dokažte, že množina bodů, ve kterých se dvě tečny k parabole protínají pod pevným úhlem $\alpha$, kde $\alpha \in (0°, 90°)$, je hyperbola se stejným ohniskem a řídicí přímkou.

[2] Tj. dotýká se všech jeho stran coby přímek. Vlastně to ani nemusí být čtyřúhelník, strany se mu můžou protínat.

[3] Tj. kde se dvě tečny té paraboly protínají pod pravým úhlem.

**Úloha 20.** Je dán svazek tří kružnic a svazek tří přímek. Průsečík přímek je na úsečce mezi průsečíky kružnic. V jedné polorovině od ní vzniknou čtyři chlívečky ohraničené vždy dvěma kružnicemi a dvěma přímkami. Dokažte, že pokud jde vepsat kružnice do třech chlívečků, jde to i do čtvrtého.



(IMO Shortlist 2010, přeformulováno)

## Návody

**1.** Středy daných kružnic jsou ohniska.

**3.** Využij, že jsou tečny osy úhlu.

**4.** Zrcadlový obraz už jsme použili v důkazu věty.

**5.** Použij předchozí úlohu. Pata kolmice je dvakrát blíž k ohnisku než zrcadlový obraz.

**6.** Překlop a najdi shodné trojúhelníky.

**7.** Střed získáš z os úhlů. Dotek překlápěním tečen.

**8.** Překlop $F_2$ podle tečen, získáš deltoid.

**10.** Je fakt jednoduchá. Kam se zobrazí ohnisko překlopením podle tečny?

**11.** Úloha 8.

**12.** Jde to například překlápěním přes tečny nebo pomocí úlohy 6. Takovým dvěma bodům se říká „kamarádi“ a pomocí tečných kuželoseček jde snadno dokázat některé jejich vlastnosti.

**13.** Překlápění.

**14.** Úloha 8.

**15.** Využij množinu pat kolmic z ohniska na tečny.

**16.** Shodné trojúhelníky.

**17.** Použij poměrovou definici kuželosečky.

**18.** Je to počítací úloha. Překlopením jako v úloze 6 získáš rovnost, která Ti pomůže. Dál jde třeba spočítat délku těžnice.

**19.** Jak zařídit pevný poměr vzdáleností, když na to máš pevný úhel? Dál ti může pomoct úloha 10.

**20.** V jakém bodě musí mít kružnice střed? A jaký musí mít poloměr? Použij poměrovou definici, všechno vychází stejně lineárně.

## Literatura a zdroje

Příspěvek je prakticky jen spojením dvou zdrojů. Děkuji autorům hlavně za nasbírané úlohy.

[1] David Hruška: *Kuželosečky*, Hojsova Stráž, 2016.

[2] Michal Janík: *Kuželosečky v olympiádní geometrii*, maturitní práce z deskriptivní geometrie, 2023.

# Cevova a Meneláova věta

Adéla Karolína Žáčková

Abstrakt. Častým problémem nejen v olympiádní geometrii, ale v geometrii celkově, je ukázat hezké vlastnosti nějakých objektů. Například, že tři body leží na jedné přímce nebo naopak, že se tři přímky protínají v jednom bodě. Právě s tímto nám napomáhají Cevova a Meneláova věta, které si v přednášce představíme a naučíme se je používat na lehčích i těžších příkladech.

Častými postupy v řešení geometrických úloh jsou dva následující: úhlím jak blbec, dokud nezvládnu vyjádřit nějak pěkně úhel, o který mi kráčí, a vyjadřuji si poměry jak blbec, dokud se nedostanu k něčemu pěknému. Cevova i Meneláova věta jsou věty založené na poměrech, proto se budeme věnovat spíše tomu druhému postupu (to ovšem neznamená, že se všem úhlům vyhneme). Pomocné ručičky nám pak mohou podat podobnost, mocnost bodu ke kružnici nebo sinová věta.

### Připomenutí

**Věta.** (Sinová) *Pro každý trojúhelník $\triangle ABC$ s vnitřními úhly označenými $\alpha$, $\beta$ a $\gamma$, stranami $a$, $b$, $c$ a poloměrem kružnice opsané $R$ platí*

$$\frac{a}{\sin\alpha} = \frac{b}{\sin\beta} = \frac{c}{\sin\gamma} = 2R.$$

**Lemma.** (O obsazích) *Na straně $BC$ trojúhelníka $ABC$ je zvolen bod $D$. Na úsečce $AD$ je zvolen bod $D'$. Dokažte, že*

$$\frac{S_{ABD'}}{S_{ACD'}} = \frac{|BD|}{|DC|}.$$

### Pod žhavým španělským sluncem

Někdy v jedenáctém století se na světlo světa dostala kniha s kouzelným názvem Kitab al-Istikmal (v překladu Kniha dokonalosti). Jak už její název (a také to, že o ní sem píšu) napovídá, byla to kniha matematiky, která obsahovala kromě slavných vět a tvrzení Eukleida, Archiméda a arabských učenců také větičky a tvrzení do té doby zůstávající v utajení. A právě mezi nimi se prvně objevila následující věta:

**Věta.** (Cevova) *V trojúhelníku $ABC$ jsou na stranách $BC$, $CA$, $AB$ postupně zvoleny body $D$, $E$, $F$. Pak se přímky $AD$, $BE$, $CF$ protínají v jednom bodě právě tehdy, když platí*

$$\frac{|BD|}{|DC|} \cdot \frac{|CE|}{|EA|} \cdot \frac{|AF|}{|FB|} = 1.$$

**Poznámka.** Věta platí, i když dva ze tří bodů $D$, $E$, $F$ leží na prodloužení stran místo uvnitř.

Velký matematik, který větu snad objevil jako první, král Zaragozy, měl ale nejspíš natolik obtížné jméno, že větu radši pojmenovali po jejím znovuobjeviteli, Italovi Giovannim Cevovi. (Přece jenom Abu Amir Yusuf ibn Ahmad ibn Hud se špatně pamatuje.)

### Triky pro řešení příkladů

(1) Uvědomte si, jakou větu, či její podobu budete chtít použít.
(2) Najděte si vhodný trojúhelník, ve kterém ji chcete uplatnit.
(3) Nebude-li snadno vykoukatelná, dopomozte si podobností, sinovou větou či mocností.

### A jde se na to!

**Úloha 1.** Pomocí Cevovy věty dokažte, že se

(i) těžnice,
(ii) osy úhlů,
(iii) výšky

v trojúhelníku protínají v jednom bodě.

**Úloha 2.** Na stranách $BC$, $CA$ trojúhelníku $ABC$ jsou dány body $D$, $E$ tak, že $|BD| : |DC| = |CE| : |EA| = 2$. Označme $X$ průsečík $AD$ a $BE$ a $F$ průsečík $CX$ a $AB$. Určete $|BF| : |FA|$.

**Úloha 3.** (Gergonnův bod) Kružnice vepsaná trojúhelníku $ABC$ se dotýká jeho stran $BC$, $CA$, $AB$ postupně v bodech $D$, $E$, $F$. Dokažte, že úsečky $AD$, $BE$, $CF$ se protínají v jednom bodě.

**Úloha 4.** Rovnoběžka se stranou $BC$ trojúhelníku $ABC$ protíná strany $AB$, $AC$ v bodech $X$, $Y$. Dokažte, že průsečík úseček $BY$, $CX$ leží na $A$-těžnici.

**Úloha 5.** Dokažte, že přímky spojující středy stran se středy odpovídajících výšek (tj. střed strany $BC$ se středem výšky na stranu $BC$ apod.) procházejí jedním bodem.

**Úloha 6.** Kružnice připsané trojúhelníku $ABC$ se dotýkají jeho stran $BC$, $CA$, $AB$ v bodech $T$, $U$, $V$. Dokažte, že přímky $AT$, $BU$, $CV$ procházejí jedním bodem.

**Lemma.** (O poměrech) *V trojúhelníku $ABC$ je na straně $BC$ zvolen bod $D$. Dokažte, že*

$$\frac{|BD|}{|DC|} = \frac{|AB| \sin \sphericalangle BAD}{|CA| \sin \sphericalangle CAD}.$$

**Věta.** (Cevova, trigonometrická verze) *Na stranách $BC$, $CA$, $AB$ trojúhelníku $ABC$ jsou dány body $D$, $E$, $F$. Pak se přímky $AD$, $BE$, $CF$ protínají v jednom bodě právě tehdy, když*

$$\frac{\sin \sphericalangle DAC}{\sin \sphericalangle BAD} \cdot \frac{\sin \sphericalangle EBA}{\sin \sphericalangle CBE} \cdot \frac{\sin \sphericalangle FCB}{\sin \sphericalangle ACF} = 1.$$

**Úloha 7.** (Isogonální kamarád) Na stranách $BC$, $CA$, $AB$ trojúhelníku $ABC$ jsou dány body $D$, $E$, $F$ tak, že úsečky $AD$, $BE$, $CF$ se protínají v jednom bodě. Přímky $AD$, $BE$, $CF$ zobrazíme podle příslušných os vnitřních úhlů trojúhelníku $ABC$. Dokažte, že vzniklé přímky opět procházejí jedním bodem (isogonálním kamarádem toho původního).

Body nazvané kamarádi mají sami o sobě spoustu zajímavých vlastností.[1] Zajímavým a užitečným faktem je kamarádství opsiště a ortocentra. Napadlo by vás, které body kamarádí samy se sebou?

**Úloha 8.** Je dán trojúhelník $ABC$ s výškami $AD$, $BE$, $CF$. Označme $M$, $N$, $P$ středy úseček $EF$, $FD$, $DE$. Dokažte, že přímky $AM$, $BN$, $CP$ procházejí jedním bodem.

### Ceva znovuobjevitel

Druhá věta, na kterou jsem vás už výše nalákala, je pojmenována po Meneláovi. Ovšem ne po tom, který měl za choť krásnou Helenu a vykonal mnohé hrdinské skutky v trojské válce, ale po Meneláovi Alexandrijském, řeckém matematikovi a astronomovi, jehož neopomenula ani výše zmíněná Kniha Dokonalosti a který se mimo jiné zabýval sférickou geometrií a geometrií trojúhelníka.

**Věta.** (Meneláova) *Je dán trojúhelník $ABC$. Body $D$, $E$, $F$ leží po řadě na přímkách $BC$, $CA$, $AB$ tak, že buď jeden z nich, nebo všechny tři leží vně trojúhelníku $ABC$. Pak body $D$, $E$, $F$ leží v přímce právě tehdy, když platí*

$$\frac{|AE|}{|EC|} \cdot \frac{|CD|}{|DB|} \cdot \frac{|BF|}{|FA|} = 1.$$

**Úloha 9.** V trojúhelníku $ABC$ označme $N$ střed těžnice $AM$ a $P$ bod na straně $AC$ takový, že $|AC| = 3|AP|$. Rozhodněte, zda body $B$, $N$, $P$ leží v přímce.

[1] Více o nich si můžete přečíst například v seriálu *Geometrie trojúhelníka*: *https://prase.cz/archive/36/serial.pdf*.

**Úloha 10.** Je dán trojúhelník $ABC$ s vepsištěm $I$. Osa úhlu u vrcholu $A$ protíná stranu $BC$ v bodě $D$. Pomocí délek stran vyjádřete hodnotu poměru $\frac{|AI|}{|ID|}$.

**Úloha 11.** (Van Aubelova věta) V trojúhelníku $ABC$ jsou na stranách $BC$, $CA$, $AB$ postupně zvoleny body $D$, $E$, $F$ tak, že přímky $AD$, $BE$, $CF$ se protínají v jednom bodě $X$. Dokažte, že pak

$$\frac{|AX|}{|XD|} = \frac{|AE|}{|EC|} + \frac{|AF|}{|FB|}.$$

**Úloha 12.** Kružnice vepsaná různostrannému trojúhelníku $ABC$ se dotýká jeho stran $BC$, $CA$, $AB$ postupně v bodech $D$, $E$, $F$. Uvnitř trojúhelníku $ABC$ je dán bod $X$ tak, že kružnice vepsaná trojúhelníku $BCX$ se dotýká $BC$ v $D$. Označme dále $Y$, $Z$ její body dotyku se stranami $XB$, $XC$. Dokažte, že přímky $EF$, $YZ$ a $BC$ procházejí jedním bodem.

**Úloha 13.** (Newton-Gauss line) Je dán konvexní čtyřúhelník $ABCD$, jehož protilehlé strany nejsou rovnoběžné. Označme $Q = BC \cap DA$ a $R = AB \cap CD$. Dále označme $X$, $Y$, $Z$ postupně středy úseček $AC$, $BD$, $QR$. Dokažte, že body $X$, $Y$, $Z$ leží na jedné přímce.

### Další úlohy

Pro řešení těchto úloh vám mohou být užiteční pomocníčci zmínění v prvním odstavci přednášky. Nebojte se věty, kterými se zabýváme, kombinovat nebo používat dvakrát, ony se neochodí ;).

**Úloha 14.** Na stranách $BC$, $CA$, $AB$ trojúhelníku $ABC$ jsou dány body $D$, $E$, $F$ tak, že úsečky $AD$, $BE$, $CF$ se protínají v jednom bodě. Kružnice opsaná trojúhelníku $DEF$ protne strany podruhé v bodech $D'$, $E'$, $F'$. Dokažte, že $AD'$, $BE'$, $CF'$ se také protnou v jednom bodě.

**Úloha 15.** Na přímce $p$ jsou dány body $A$, $Z$, $B$ v tomto pořadí, přičemž $Z$ není středem $AB$. Zvolme libovolně bod $X \notin p$ a poté libovolně zvolme bod $Y$ na úsečce $XZ$. Označme $D = AX \cap BY$ a $E = BX \cap AY$. Dostali jsme tak přímku $DE$, jejíž konstrukce závisí na zvolených bodech $X$, $Y$. Dokažte, že všechny takto zkonstruované přímky $DE$ procházejí jedním pevným bodem.

**Úloha 16.** Je dán trojúhelník $ABC$. Přímka skrz jeho těžiště $G$ protne strany $AB$, $AC$ v bodech $F$, $E$. Dokažte, že

$$\frac{|BF|}{|FA|} + \frac{|CE|}{|EA|} = 1.$$

**Úloha 17.** (Pascalova věta) Body $A$, $B$, $C$, $D$, $E$, $F$ leží na kružnici v libovolném pořadí. Nechť $L = AB \cap DE$, $M = BC \cap EF$, $N = CD \cap FA$. Dokažte, že $L$, $M$, $N$ leží na jedné přímce.

## Úlohy z olympiád

**Úloha 18.** V nerovnoramenném trojúhelníku $ABC$ protíná osa úsečky $BC$ kružnici jemu opsanou v bodech $M$ a $N$. Označme středy úseček $AM$ a $AN$ $K$, respektive $L$. Nechť kružnice $ABK$, respektive $ABL$ protínají $AC$ podruhé v bodech $D$, respektive $E$, kružnice $ACK$, respektive $ACL$ protínají $AB$ podruhé v bodech $F$, respektive $G$. Dokažte, že $DF$, $EG$ a $MN$ se protínají v jednom bodě.

(Turecko 2021 TST)

**Úloha 19.** Nechť $ABC$ je rovnoramenný trojúhelník s $|AB| = |AC|$. Kružnice vepsaná se dotýká stran $BC$ a $CA$ postupně v bodech $D$ a $E$. Bodem $B$ vedeme přímku různou od $BE$, která protne kružnici vepsanou v bodech $F$ a $G$. Nechť $BC$ protíná přímky $EF$ a $EG$ postupně v bodech $K$ a $L$. Dokažte, že $|DK| = |DL|$.

(MEMO 2008)

**Úloha 20.** Je dán trojúhelník $ABC$ a uvnitř něj bod $P$. Bodem $P$ prochází přímka $p$. Bod $A'$ dostaneme jako průsečík strany $BC$ a obrazu přímky $AP$ podle osy $p$. Analogicky dostaneme body $B'$ a $C'$. Dokažte, že body $A'$, $B'$, $C'$ leží na jedné přímce. (USAMO 2012)

**Úloha 21.** Nechť $AD$ je průměr kružnice opsané trojúhelníku $\triangle ABC$. Přímky vedené bodem $D$ rovnoběžné s $AB$ a $AC$ protínají $AC$ a $AB$ postupně v bodech $E$ a $F$. Průsečík $EF$ a $BC$ označme $G$. Dokažte, že $AD$ a $DG$ jsou na sebe kolmé.

(MEMO 2021)

**Úloha 22.** Nechť $\Omega$ je kružnice opsaná trojúhelníku $ABC$. Označme $S_b$ a $S_c$ postupně středy oblouků $AC$ a $AB$, které neobsahují třetí vrchol trojúhelníku. Označme $N_a$ střed oblouku $BAC$ (oblouk $BC$ obsahující bod $A$). Střed kružnice vepsané trojúhelníku $ABC$ označíme $I$. Nakonec ať $\omega_b$ značí kružnici, která se dotýká $AB$ a má vnitřní dotyk s kružnicí $\Omega$ v bodě $S_b$, a podobně ať $\omega_c$ značí kružnici, která se dotýká $AC$ a má vnitřní dotyk s kružnicí $\Omega$ v bodě $S_c$. Dokažte, že přímka $IN_a$ se s přímkou procházející průsečíky kružnic $\omega_b$ a $\omega_c$ protíná na kružnici $\Omega$.

(EGMO 2023)

### Návody

**3.** Využij, že strany jsou tečny ke kružnici. Pak znáš délky jednotlivých úseků.

**4.** Dokaž, že $\frac{|CY|}{|YA|} = \frac{|BX|}{|XA|}$. Pomůže ti stejnolehlost.

**5.** Uvědom si, že středy výšek leží na středních příčkách. Použij Cevovu větu na trojúhelník ze středních příček.

**6.** Vzpomeň si, že bod dotyku kružnice vepsané a připsané na téže straně jsou souměrné podle jejího středu. Využij znalost o dotecích kružnice vepsané.

**7.** Uvědom si, že přesně zde je krásně vidět trigonometrický tvar.

**8.** Dopočítej si záhadné úhly sinovkou (s využitím, že $M$, $N$, $P$ jsou středy) a využij trigonometrický tvar.

**9.** Použij Meneláovu větu v trojúhelníku $AMC$.

**10.** Využij, že osa úhlu dělí protější stranu v poměru přilehlých. Meneláovu větu použij z trojúhelníku ADC.

**11.** Meneláova věta v trojúhelníku $ACD$, použij i Cevovu.

**12.** Spočítej, kde protnou $EF$ a $YZ$ přímku $BC$.

**13.** Využij Meneláovu větu v trojúhelníku ze středních příček $ABQ$.

**14.** Použij mocnost bodů $A$, $B$, $C$ ke kružnici opsané trojúhelníku $DEF$.

**15.** Hlavní roli hraje trojúhelník $ABX$, pro který použijte Menealovu i Cevovu větu.

**16.** Vyjádři si oba zlomky z Menealovy věty pro přímku $EF$ a trojúhelníky $ABM$, resp. $ACM$, kde $M$ je střed $BC$ (označ si průsečík $EF$ a $BC$).

**17.** Prodluž sudé strany šestiúhelníku $ABCDEF$, a tím vytvoř trojúhelník $XYZ$. Pro ten pak napiš tři Menealovy věty pro tři různé přímky.

**19.** Označ si $X = CG \cap AB$ a použij Menealovu větu pro trojúhelník $XBC$ dvakrát – s body $E$, $G$, $L$ a s body $E$, $F$, $K$. Pak pomůže mocnost.

**20.** Vyjádři si poměry z Menealovy věty pomocí lemmatu o poměrech.

**21.** Označ si $X$ průsečík $BC$ a kolmice z $AD$. Pomocí Meneláovy věty dokaž, že $E$, $F$ a $X$ leží na jedné přímce. K tomu využij rovnoběžník a fakt, že $DX$ je tečna k opsané kružnici.

### Literatura a zdroje

Chtěla bych poděkovat Jáchymovi, jehož přednáška mi byla skvělým zdrojem i inspirací.

[1] Jáchym Solecký: *Cèvova a Menelaova věta*, Paseky, 2018.
[2] *Wikipedie*, *https://en.wikipedia.org/wiki/Ceva%27s_theorem*.

# Obsah

**RSA** (Natália Bátorová) . . . . . 3
**Ciferné součty** (Fíla Čermák) . . . . . 8
**Lineární algebra v kombinatorice** (Fíla Čermák) . . . . . 13
**Simsonova přímka** (Káťa Danilina) . . . . . 19
**Interpolace** (Matěj Doležálek) . . . . . 23
**Konečná tělesa a kde je najít** (Matěj Doležálek) . . . . . 27
**Prolog** (Vojta Gaďurek) . . . . . 33
**Úvod do teorie grafů** (Klárka Grinerová) . . . . . 39
**Monovarianty** (Vít Hanika) . . . . . 44
**Hales–Jewett** (Lenka Kopfová) . . . . . 47
**Hrátky s polynomy** (Magdaléna Mišinová) . . . . . 52
**Nerovnosti bez kladiv** (Magdaléna Mišinová) . . . . . 58
**Úvod do lineární algebry** (Vendula Onderková) . . . . . 61
**Intuicionistická logika** (Daniel Perout) . . . . . 69
**Teleskopické součty a součiny** (Daniel Perout) . . . . . 75
**Extremální princip** (Martin Raška) . . . . . 78
**Geometrické podvádění** (Martin Raška) . . . . . 81
**Kuželosečky** (Matouš Šafránek) . . . . . 85
**Cevova a Meneláova věta** (Adéla Karolína Žáčková) . . . . . 91