Diskrétní matematika pro matematiky — verze 2025

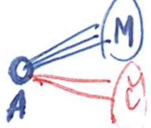
Intro: – co je DM, účel kursu, přednáška + cvičení, nahrávky + stream → GDPR
- přednáška → zkouška
- cvičení → zápočet – nutno před zkouškou
- https://mj.ucw.cz/vyuka/dm

zpočátku neformální, ale precizní; později doplníme formalismus

PTEJTE SE!

Matfyzáci v tramvaji: 6 lidí, relace "znát se" (symetrická) → $\exists \Delta$ nebo Δ } vizualizace (graf)

Řešení:



$|M| + |\bar{C}| = 5 \Rightarrow |M| \geq 3 \vee |\bar{C}| \geq 3$ (obráceno) → symetricky

buď mezi M je | ⇒ Δ s A

nebo samé | ⇒ Δ uvnitř M

Souvislosti: Ramseyovy věty, "neexistuje dokonalý chaos"

Nekonečně mnoho prvočísel (à la Euklides) – důkaz sporem
- kdyby jich bylo konečně mnoho, můžeme je vyjmenovat: $p_1 < p_2 < \ldots < p_n$
- nyní uvažme $x = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$
  - $x > p_n \Rightarrow x \neq p_i$ pro všechna $i \Rightarrow x$ není prvočíslo
  - tedy $\exists i : p_i \mid x$ … to ale není možné, protože $x \bmod p_i = 1$ ↯

Součet $S_n := 1 + 2 + \_\_ + n$ … značení: $S_n = \sum_{i=1}^{n} i$ ← aritmetická řada (spec. případ)

(definiční rovnost) ← co je $\mathbb{N}$?

- okrajové případy: $S_0 = 0$, $S_1 = 1$
- přeuspořádání:

$$\begin{aligned} S_n &= 1 + 2 + \_\_ + (n-1) + n \\ S_n &= n + (n-1) + \_\_ + 2 + 1 \\ \hline 2S_n &= (n+1) + \_\_ + (n+1) = \frac{n(n+1)}{2} = \frac{n^2+n}{2} \end{aligned}$$

- můžeme dokázat indukcí … obecný princip: $\varphi(0) \;\&\; (\forall n(\underbrace{\varphi(n)}_{\text{indukční předpoklad}} \Rightarrow \varphi(n+1))) \Rightarrow \forall n\, \varphi(n)$ (indukční krok)
  - $\varphi(n)$: $\underbrace{1 + \_\_ + n}_{S_n} = \frac{n(n+1)}{2}$
  - $\varphi(0)$: $0 = \frac{0 \cdot 1}{2}$ ✓
  - $n \to n+1$: víme $S_n = \frac{n(n+1)}{2}$, chceme $S_{n+1} = \frac{(n+1)(n+2)}{2}$

$$S_{n+1} = \underbrace{S_n}_{\frac{n(n+1)}{2}} + (n+1) = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}$$

Q.E.D.

Součet $g_n := q^0 + q^1 + \_ + q^{n-1}$ ← geometrická řada

- pokus: $q = 10$

$$\underset{1}{10^0} + \underset{10}{10^1} + \underset{100}{10^2} + \_\_ + \underset{1\underbrace{0\_\_0}_{n-1}}{10^{n-1}} = \underbrace{1\_\_1}_{n} = \frac{\overbrace{9\_\_9}^{n}}{9} = \frac{10^n - 1}{9}$$

- pro $q = 3$ trojková soustava … $\frac{3^n - 1}{2}$
- hypotéza: $g_n = \frac{q^n - 1}{q - 1}$ … pokud $q \neq 1$ … jinak $g_n = n$

- můžeme dokázat indukcí:
  - $g_0 = 0 = \frac{q^0-1}{q-1} = 0$ ✓
  - $n \to n+1$: $g_{n+1} = g_n + q^n = \frac{q^n-1}{q-1} + q^n = \frac{q^n-1+\overbrace{q^n(q-1)}^{q^{n+1}-q^n}}{q-1} = \frac{q^{n+1}-1}{q-1}$ ✓

jiný způsob:
$g_n = q^0 + q^1 + \dots + q^{n-1}$
$q \cdot g_n = q^1 + q^2 + \dots + q^n$
$\Rightarrow (q-1)g_n = q^n - 1$

- trik: jelikož se jedná o rovnost polynomů, stačí, když platí pro dost různých q (my jich máme ∞)

Součet $\square_n := 1^2 + 2^2 + \dots + n^2$

- malé případy: $\square_0 = 0$, $\square_1 = 1$, $\square_2 = 5$, $\square_3 = 14$ … pattern?
- hypotéza: je to kubický polynom, tedy $\square_n = ax^3 + bx^2 + cx + d$ pro nějaké a, b, c, d
- pak: $\square_0 = 0 \Rightarrow d = 0$

$\square_1 = 1 \Rightarrow a + b + c = 1$ $\to c = \frac{1}{6}$

$\square_2 = 5 \Rightarrow 8a + 4b + 2c = 5$ $\to 6a + 2b = 3$ $\to b = 1/2$

$\square_3 = 14 \Rightarrow 27a + 9b + 3c = 14$ $\to 24a + 6b = 11$

$6a = 2 \to a = \frac{1}{3}$

- mělo by tedy být $\square_n = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n = \frac{n(n+\frac{1}{2})(n+1)}{3}$
- ověříme indukcí (D.Ú.)

Platíme pomocí 3Kč a 5Kč – které částky jdou zaplatit?

"indukce s prefixem"

0	✓	8	✓
1	✗	9	✓
2	✗	10	✓
3	✓	11	✓
4	✗	12	✓
5	✓	13	✓
6	✓	14	✓
7	✗	15	✓

⋮ atd.

od 11 dál můžeme indukovat

Princip: $\varphi(n_0) \,\&\, (\forall n \geq n_0 : \varphi(n) \Rightarrow \varphi(n+1))$
$\Rightarrow \forall n \geq n_0\ \varphi(n)$

- $\varphi(n) =$ "pro 8 až n to jde"
  $n_0 = 10$

Existence zápisů ve dvojkové soustavě – každé $n \geq 0$ jde zapsat jako součet různých mocnin dvojky

Silná indukce: $\varphi(0) \,\&\, (\forall n\ (\forall k < n\ \varphi(k)) \Rightarrow \varphi(n)) \Rightarrow \forall n\ \varphi(n)$

- $\varphi(n) =$ "n lze zapsat"
- $\varphi(0)$ ✓ (prázdný součet)
- n: nechť 2^i je nejvyšší mocnina 2 menší rovná n
  $n' := n - 2^i$ … $n' < n \Rightarrow \varphi(n')$ platí … vezmeme zápis n' a přičteme 2^i

nemůže ale obsahovat 2^i? když by ano, pak $n' \geq 2^i$ a tedy $n \geq 2^i + 2^i = 2^{i+1}$ $\Rightarrow 2^i$ nebyla největší

- zesílení úvahy: zápis existuje právě jeden (až na pořadí sčítanců)
  - každý zápis n musí obsahovat 2^i, neboť $2^0 + \dots + 2^{i-1} = 2^i - 1 < n$
  - stačí využít jednoznačnost zápisu n' z IP

Dělitelnost $a \backslash b \equiv \exists c: b = ac$

👁 $1 \backslash b$ pro všechna b
$a \backslash 0$ pro všechna a ($0 \backslash 0$ platí)
$-3 \backslash 6$ ... obecně funguje pro $\mathbb{Z}$

$a \backslash b \Leftrightarrow a \bmod b = 0$

Kongruence $a \equiv b \pmod{n} \Leftrightarrow n \backslash a-b \Leftrightarrow a \bmod n = b \bmod n$

"chová se jako rovnost" – $a \equiv a$, $a \equiv b \Leftrightarrow b \equiv a$, $a \equiv b$ & $b \equiv c \Rightarrow a \equiv c$ (R, S, T)

$a \equiv a'$, $b \equiv b'$ $\Leftrightarrow$ $a+b \equiv a'+b'$ ... sečteme kongruence nebo vyměníme výraz za kongruentní

$\Leftrightarrow$ $a-b \equiv a'-b'$

$\Rightarrow$ $ab \equiv a'b'$ ... ale pozor, tady $\Leftarrow$ obecně neplatí!
modulo 4: $2 \cdot 2 \equiv 2 \cdot 4$, ale $2 \not\equiv 4$

představa ciferníku hodin

Zkoumáme $n^2 \bmod 4$

n	n^2	$n^2 \bmod 4$	mod 8
0	0	0	0
1	1	1	1
2	4	0	4
3	9	1	1
4	16	0	0
5	25	1	1
6	36	0	4
7	49	1	1

→ pro n sudé je $4 \backslash n^2$
pro n liché je $n^2 \bmod 4 = 1$ ... tedy $\left.\begin{array}{l} n^2 \equiv 0 \\ n^2 \equiv 1 \end{array}\right\}$ mod 4

- lze indukovat
- nebo takto $(2n)^2 \equiv 4n^2 \equiv 0 \cdot n^2 \equiv 0$
  $(2n+1)^2 \equiv 4n^2 + 4n + 1 \equiv 0 + 0 + 1 \equiv 1$
- co mod 8? $(2n+1)^2 \equiv \underbrace{4n^2+4n}_{4\underbrace{n(n+1)}_{\text{sudé}}} + 1 \equiv 0 + 1$

Celočíselné kořeny polynomů

uvažujme $f(x) = 4x^5 - 12x^4 - 5x^3 + 15x^2 + x - 3$ ... jaké má kořeny?
... to je obecně těžké (Galoisova věta), ale celočíselné jdou najít snadno

Obecně: nechť $f(x) = \sum_{i=0}^{n} a_i x^i$ je polynom s celočíselnými koeficienty $a_0 - a_n$

Pokud x je kořen: $\sum_{i=0}^{n} a_i x^i = 0$ ... uvažme mod $|x|$

$x \neq 0$ } $x=0$ se pozná snadno ($a_0 = 0$)

↳ $\underbrace{a_0 x^0}_{1} + \underbrace{a_1 x^1 + \ldots + a_n x^n}_{\text{jsou dělitelné } x, \text{ tedy } \equiv 0} \equiv a_0$

Z toho $a_0 \equiv 0 \pmod{x}$
Jinými slovy $x \backslash a_0$

... takže stačí prozkoumat konečně mnoho dělitelů a_0

V našem případě $a_0 = -3$ ... kandidáti jsou
$+1$ ✓ $4 - 12 - 5 + 15 + 1 - 3 = 0$
-1 ✓ $-4 - 12 + 5 + 15 - 1 - 3 = 0$
$+3$ ✓
-3 ✗

Vylepšení: racionální kořeny (pro celočíselné koeficienty)

Nechť $\sum_i a_i \left(\frac{p}{q}\right)^i = 0$ … vynásobíme obě strany q^n → $\sum_i a_i p^i q^{n-i} = 0$

Nyní mod p: $p \setminus a_0$
mod q: $q \setminus a_n$ } konečně mnoho kandidátů

V našem případě: $p \in \{\pm 1, \pm 3\}$, $q \in \{\pm 1, \pm 2, \pm 4\}$

Funguje $1/2$ a $-1/2$ … a to už je 5 kořenů
⇒ jsou to všechny reálné

Jedničková čísla (a.k.a. repunits)

$J_n = \underbrace{1 \dots 1}_{n}$ … platí pro nějaké n: $2017 \setminus J_n$?

- zobecníme pro dělitelnost jakýmkoliv m
- malé případy:

m	J_n
1	1
2	×
3	111
4	×
5	×
6	×
7	111 111 = 111 · 1001 ($7 \cdot 11 \cdot 13$)
8	×
9	111 111 111
10	×
11	11
13	111111
17	?

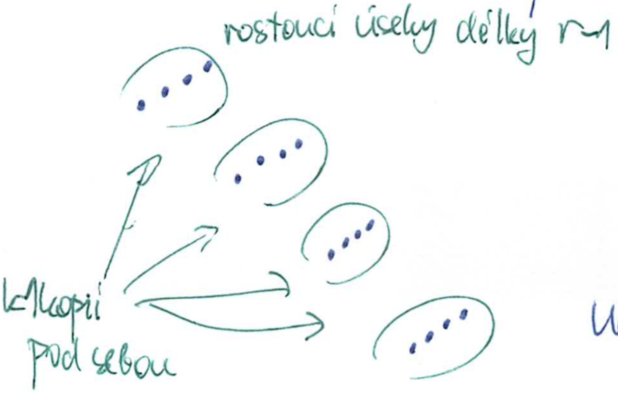
pokud je m dělitelné 2 nebo 5, evidentně to nejde

- hypotéza: pro všechna ostatní n to jde
- uvažujme všechna J_n mod m … konečně mnoho zbytků ⇒ princip holubníku
  takže $\exists i > j: J_i \equiv J_j \pmod m$
  $\Rightarrow \underbrace{J_i - J_j}_{\text{číslo tvaru } \underbrace{1 \_\_ 1}_{i-j} \underbrace{0 \_\_ 0}_{j}} \equiv 0 \pmod m$

  číslo tvaru $\underbrace{1 \_\_ 1}_{i-j}\underbrace{0 \_\_ 0}_{j} = J_{i-j} \cdot 10^j$ } jelikož m není dělitelné 2 ani 5, máme $m \setminus J_{i-j}$ □

Monotónní podposloupnosti

Dostaneme posloupnost $x_1 - x_n \in \mathbb{R}$ různých čísel
Jak dlouhá rostoucí/klesající vybraná podposloupnost v ní musí být?
Pokus o konstrukci dlouhé posl. bez dlouhých monotónních pp.:



- neobsahuje rostoucí pp. délky r
- ani klesající pp délky k
- má celkem $n = (r-1)(k-1)$ prvků

Ukážeme, že je nejdelší možná.

Věta (Erdősova–Szekeresova): Posloupnost délky (alespoň) $(r-1)(k-1)+1$ obsahuje rostoucí pp. délky r nebo klesající pp. délky k

Dk: pro $x_1 - x_n$

def. (a_i, b_i), kde $a_i :=$ délka nejdelší rostoucí pp končící prvkem x_i
$b_i :=$ — " — klesající — " —

Sporem: pokud $\nexists$ dost dlouhá pp., je vždy $1 \le a_i \le r-1$, $1 \le b_i \le k-1$
$\Rightarrow (r-1)(k-1)$ možných hodnot dvojice, ale $n > (r-1)(k-1)$

Tedy podle principu holubníku $\exists\, i,j:\ i<j,\ (a_i, b_i) = (a_j, b_j)$

To ale není možné: Buď $x_i < x_j$, ale pak $a_j \ge a_i + 1$
nebo $x_i > x_j$, — " — $b_j \ge b_i + 1$ ↯

Přídavky

- Neexistují dvě mocniny 2 lišící se jen pořadím cifer.
- Wilsonova věta: n je prvočíslo $\Leftrightarrow$ $(n-1)!+1$ je dělitelné n
- Čínská zbytková věta (důkaz holubníkem)
- 3 domečky a 3 studny

KOMBINATORIKA

– KOLIK JE OBJEKTŮ DANÉHO DRUHU?

Příklady:

26 znaků angl. abecedy

1. # slov o 8 písmenech z $\{a - z\} = 26^8$ ← 2 písmenka:  pak pokračujeme indukcí
2. … všechna písmena různá: $\underbrace{26 \cdot 25 \cdot 24 \cdot \ldots \cdot 19}_{8 \text{ členů}} = 26^{\underline{8}}$

jiný krutý příklad: ZPRACHNIVĚLOST či ZUBOLÉKAŘSTVÍ (nejdelší rozumná) bez opak.
2 znaky

3. # přesmyček slova KRUTOVLADCE $= 11^{\underline{11}} = 11!$ ←
4. # přesmyček slova JEZEVEC … nejdříve $JE_1ZE_2VE_3C = 7!$
   - $3! = 6$ způsobů, jak E-čka očíslovat $\rightarrow$ #přesmyček $\cdot\, 3! = 7!$
   $\Rightarrow$ #přesmyček $= \dfrac{7!}{3!}$

↳ technika počítání dvěma způsoby