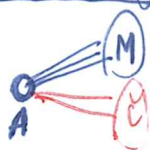


Intro: - co je DM, účel kursu, přednáška + cvičení, nahrávky + stream

- <https://uj.uan.cz/vyuka/dm>

Matfyzáci v trávě: 6 lidí, telace "znát se" (symetrické) → $\exists \Delta$ nebo Δ } vizualizace (graf)
 PTEJE SE?

Řešení:



$$|M| + |C| = 5 \Rightarrow |M| \geq 3 \vee |C| \geq 3 \text{ (obutěnou)}$$

bud' mezi M je $\Delta \Rightarrow \Delta$ s A
 nebo samé $\Delta \Rightarrow \Delta$ uvnitř M

Souvislosti: Ramseyovy věty, "neexistuje dokonalý chaos"

Nekonečně mnoho prvočísel (à la Euklides) - důkaz sporem

- kdyby jich bylo konečně mnoho, můžeme je vyjmenovat: $p_1 < p_2 < \dots < p_n$

- nyní uvažme $x = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$

• $x > p_n \Rightarrow x \neq p_i$ 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 $S_n = 1 + 2 + \dots + n$... značení: $S_n = \sum_{i=1}^n i$ ← aritmetická řada (spec. případ)

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

- přeuspořádání: $S_n = 1 + 2 + \dots + (n-1) + n$

$$S_n = n + (n-1) + \dots + 2 + 1$$

$$2S_n = (n-1) + \dots + (n-1) + (n-1) = \frac{n(n-1)}{2} = \frac{n^2 - n}{2}$$

- můžeme dokázat indukci ... obecný princip: $\varphi(0) \& (\forall n (\varphi(n) \Rightarrow \varphi(n+1))) \Rightarrow \forall n \varphi(n)$

$$\varphi(n): \underbrace{1 + \dots + n}_{S_n} = \frac{n(n+1)}{2}$$

indukční předpoklad indukční krok

$$\varphi(0): 0 = \frac{0 \cdot 1}{2} \checkmark$$

$$n \rightarrow n+1: \text{víme } S_n = \frac{n(n+1)}{2}$$

$$\text{chceme } S_{n+1} = \frac{(n+1)(n+2)}{2}$$

$$S_{n+1} = S_n + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2} \text{ Q.E.D.}$$

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

- pokus: $q=10$

$$10^0 + 10^1 + 10^2 + \dots + 10^{n-1} = 1 + 10 + 100 + \dots + 10^{n-1} = \frac{10^n - 1}{9}$$

- 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 indukci:
- jiný způsob:
 $g_n = q^0 + q^1 + \dots + q^{n-1}$
 $q \cdot g_n = q^1 + q^2 + \dots + q^n$
 $\Rightarrow (q-1)g_n = q^n - 1$
- $g_0 = 0 = \frac{q^0 - 1}{q - 1} = 0 \checkmark$
- $n \rightarrow n+1: g_{n+1} = g_n + q^n = \frac{q^n - 1}{q - 1} + q^n = \frac{q^n - 1 + q^n(q - 1)}{q - 1} = \frac{q^{n+1} - 1}{q - 1} \checkmark$
- trik: jelikož se jedná o rovnost polynomů, stačí, když platí pro dost různých q (můžeme si vybrat)

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

- malé případy: $\square_0 = 0, \square_1 = 1, \square_2 = 5, \square_3 = 14 \dots$ pattern?
- hypotéza: je to kubický polynom, tedy $\square_n = an^3 + bn^2 + cn + d$ pro nějaké a, b, c, d
- pak: $\square_0 = 0 \Rightarrow d = 0$
- $\square_1 = 1 \Rightarrow a + b + c = 1$
 $\square_2 = 5 \Rightarrow 8a + 4b + 2c = 5$
 $\square_3 = 14 \Rightarrow 27a + 9b + 3c = 14$
- $\xrightarrow{c = \frac{1}{6}}$
 $\xrightarrow{b = 1/2}$
 $\xrightarrow{6a + 2b = 3}$
 $\xrightarrow{24a + 6b = 11}$
 $\xrightarrow{6a = 2 \rightarrow a = \frac{1}{3}}$
- mělo by tedy být $\square_n = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n = \frac{n(n+1)(n+2)}{6}$
- ověříme indukci (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 ✓

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 ať n to jde"
 $n_0 = 10$

Existence zápisů ve dvojkové soustavě - každé $n \geq 0$ jde zaplat 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 zaplat"
 - $\varphi(0) \checkmark$ (prázdný součet)
 - n : nechť 2^i je nejvyšší mocnina 2 menší rovná n
 $n' = n - 2^i \dots n' < n \Rightarrow \varphi(n')$ platí ... vezmeme zápis n' a přičteme 2^i
- zesílení úvahy: zápis existuje právě jeden (ať 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 $n' \in \mathbb{P}$
- neumíže ale obsahovat 2^i ?
kdyby ano, pak $n' \geq 2^i$
a tedy $n \geq 2^i + 2^i = 2^{i+1}$
 $\Rightarrow 2^i$ nebyla největší

Dělitelnost

$a \setminus b \equiv \exists c: b = ac$  $1 \setminus b$ pro všechna b
 $a \setminus 0$ pro všechna a (0/0 platí)
 $-3 \setminus 6 \dots$ obecně funguje pro $\mathbb{Z}$

(3)

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

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

"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 vynásobíme výraz
za kongruentní

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

$$\Rightarrow ab \equiv a'b' \text{ --- ale pozor, tady } \Leftarrow \text{ obecně neplatí!}$$

modulo 4: $2 \cdot 2 \equiv 2 \cdot 4$, ale $2 \not\equiv 4$

↓
představa
ciferníku hodin

Skoumáme $n^2 \bmod 4$

→ pro n sudé je $4 \setminus n^2$

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

n	n^2	$n^2 \bmod 4$	$\bmod 8$
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

• lze indukovat

• nebo také $(2n)^2 \equiv 4n^2 \equiv 0 \cdot n^2 \equiv 0$

$$(2n+1)^2 \equiv 4n^2 + 4n + 1 \equiv 0 + 0 + 1 \equiv 1$$

• co mod 8? $(2n+1)^2 \equiv 4n^2 + 4n + 1 \equiv 0 + 1$

$4n(n+1)$
sude

Celočíslné kořeny polynomů

uvažujme $f(x) = 4x^5 - 12x^4 - 5x^3 + 15x^2 + x - 3 \dots$ jaké má kořeny?

... to je obecně těžké (Galoisova věta), ale celočíslné jdou najít snadno

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

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

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

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

$$\text{z toho } a_0 \equiv 0 \pmod{x}$$

Díjnými slovy $x \setminus a_0$

... takže stačí prozkoumat konečné mnoho dělitelů a_0

V našem případě $a_0 = -3 \dots$ 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)

(4)

Nechť $\sum_i a_i (\frac{p}{q})^i = 0$... vynásobíme obe strany $q^n \rightarrow \sum_i a_i p^i q^{n-i} = 0$

Nyní mod p : $p \nmid a_0$
 mod q : $q \nmid a_n$ } konečně mnoho kandidátů
 V našem případě: $p \in \{\pm 1, \pm 3\}$, $q \in \{\pm 1, \pm 2, \pm 4\}$
 Funguje $\frac{1}{2}$ a $-\frac{1}{2}$... a to už je 5 kořenů
 $\Rightarrow$ jsou všechny reálné

Jedničkova čísla (a.k.a. repunits)

$J_n = \underbrace{1 \dots 1}_n$... platí pro nějaké n : $2017 \mid J_n$?

• zobecníme pro dělitelnost jakýmkoliv m

• malé případy:

m	J_n	m	J_n	m	J_n
1	1	6	x	11	11
2	x	7	111 111 = 111 · 1001	13	111111
3	111	8	x	17	?
4	x	9	111 111 111		
5	x	10	x		

4 pokud je m dělitelné 2 nebo 5, evidentně to nejde

• hypotéza: pro všechna ostatní n to jde

• uvažujeme všechna $J_n \bmod m$... konečně mnoho zbytků $\Rightarrow$ princip holubníku

takže $\exists i > j: J_i \equiv J_j \pmod{m}$

$$\Rightarrow J_i - J_j \equiv 0 \pmod{m}$$

číslo tvaru $\underbrace{1 \dots 1}_{i-j} \underbrace{0 \dots 0}_j = J_{i-j} \cdot 10^j$

} jelikož m není dělitelné 2 ani 5, máme $m \mid J_{i-j}$ $\square$

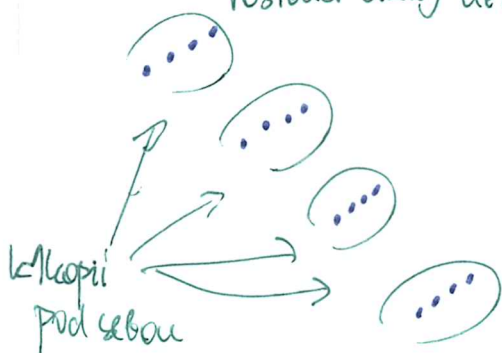
Monotónní ^{pod}postoupnosti

Dostaneme posloupnost $x_1 \sim x_n \in \mathbb{R}$ různých čísel

Jak dlouhá rostoucí/klesající vybraná podpostoupnost v ní musí být?

Pokus o konstrukci dlouhé posl. bez dlouhých monotónních pp.:

rostoucí úseky délky $r-1$



- neobsahuje rostoucí pp. délky r
 - ani klesající pp. délky k
 - má celkem $n = (r-1)(k-1) + 1$ prvků
- Ukažeme, že je nejdelší možná.

Jak se buduje matematika

- definice objektů matematického světa

$\left\{ \begin{array}{l} \text{pomocí jednoduchších objektů} \\ \text{pomocí axiomů} \end{array} \right\}$ třeba přiroz. čísla
 např. u množin

přiroz. čísla
 $\downarrow$
 celá čísla
 $\downarrow$
 dělitelnost
 $\downarrow$
 prvočísla

- uplatníme tvrzení (hypotézy) a zvažujeme, jestli platí

věta lemma pozorování

- může se také stát, že tvrzení je nerozhodnutelné

o pravdivosti nás přesvědčí důkaz

idea: je to postupnost kroků (konечná?)
 každý plyne buď přímo z definic/axiomů
 nebo z předchozích kroků
 "triviálním způsobem"

pořádně
 viz
 logika

Matematická notace

- pro čísla: $\lceil x \rceil$ horní celá část (zaokrouhlení nahoru)
 $\lfloor x \rfloor$ dolní celá část (zaokrouhlení dolů)

např. $\lceil 1.35 \rceil = 2$ $\lfloor 1 \rfloor = \lfloor 1.1 \rfloor = 1$
 $\lceil 1.35 \rceil = 2$
 $\lfloor -1.35 \rfloor = -2$

- "tri tečky": $x_1 + x_2 + \dots + x_n$
 (nebo "—") $1 + 2 + \dots + n$

$2 + 4 + \dots + n$ } nejasné - sudá, nebo 2^k ?
 $2^1 + 2^2 + \dots + 2^k$

důvod: chceme, aby platilo

$$\sum_{i=1}^n f(i) = \left(\sum_{i=1}^{n-1} f(i) \right) + f(n) \quad \text{i pro } n=1$$

- Suma: $\sum_{i=1}^n x_i = x_1 + x_2 + \dots + x_n$

$$\sum_{1 \leq i \leq n} i^2$$

$$\sum_{i \in \{1, \dots, n\}} \frac{1}{i} \quad \text{\& i prvočíslo}$$

pozor: průběžná suma $\sum_{i=1}^0 i = 0$

nebo $\sum_{0 \leq i \leq 1} i = 0$
 & i prvočíslo

→ analogický produkt $\prod_{i=1}^n i = 1 \cdot 2 \cdot \dots \cdot n$

též značíme $n!$ (faktoriál)
 průběžný produkt $= 1$

- množiny:

- $\{1, 3, 7\} = \{7, 1, 3, 1, 1\}$

- $\{\} = \emptyset$ } pozor: $\{\emptyset\} \neq \emptyset$

- $\{5, \emptyset\}$

- $\{\emptyset, \{1\}\}$

- $|A| := \# \text{ prvků (konечné) množiny}$

- $\mathbb{N}$ - pro nás včetně 0

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

- operace s množinami:

- $x \in A$

je prvkem

- $A \subseteq B \equiv \forall a \in A: a \in B$ je podmnožinou

- $A \cap B := \{a \in A \mid a \in B\}$ průnik

- $A \cup B$

sjednocení

- $A \setminus B := \{a \in A \mid a \notin B\}$ rozdíl

- $A \Delta B := (A \cup B) \setminus (A \cap B)$ symetrický rozdíl

- $2^A = \mathcal{P}(A) := \{B \mid B \subseteq A\}$ potence

- $\{x \in A \mid \varphi(x)\}$ výběr podmnožiny

- $\{x^2 \mid x \in A\}$ nahrazení prvků jinými

Věta (Erdős-Šzekeresová): Postoupnost délek (alespoň) $(r-1)(k-1)+1$ obsahuje rostoucí pp. délky r nebo klesající pp. délky k

(5)

Dle: pro $x_1 \dots x_n$

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

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

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

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

Přidávky

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

KOMBINATORIKA

- KOLIK JE OBJEKTŮ DANÉHO DRUHU?

Příklady:

- ① # slov o 8 písmenech z $\{a-z\} = 26^8 \leftarrow 26 \text{ znaki Angl. abecedy} \leftarrow 2 \text{ písmenka} \leftarrow \begin{matrix} 26 \\ \boxed{\begin{matrix} \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{matrix}} \end{matrix} \leftarrow \text{pak pokračujeme indukci}$
- ② ... všechna písmena různá: $26 \cdot 25 \cdot 24 \cdot \dots \cdot 19 = 26^{\underline{8}}$
 $\underbrace{\hspace{10em}}_{8 \text{ členů}}$
- ③ # přesmyček slova KRUTOVLADCE = $11^{\underline{11}} = 11!$ $\leftarrow$ jiný krásný příklad: ZPRACHNIVĚLOST
 či ZUBOLEKARSTVI (nejdelší roztomilá bez opakování)
- ④ # přesmyček slova JEZEVEC ... nejdrůbež JEZEVEC = $7!$
 • 3! = 6 způsobů, jak E-čka očíslovat $\Rightarrow$ #přesmyček $\cdot 3! = 7!$
 $\Rightarrow$ #přesmyček = $\frac{7!}{3!}$

$\hookrightarrow$ technika počítání dvěma způsoby