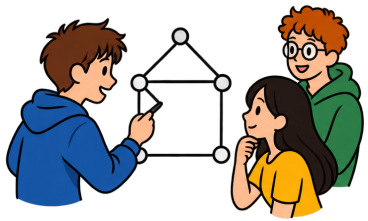
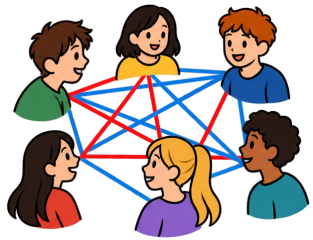
Diskrétní matematika

Do našeho kurzu patří kombinatorika, diskrétní pravděpodobnost, teorie grafů, relace, částečná uspořádání, Ramseyova teorie . . .



— *zabývají se zejména objekty vystavěnými z konečných množin.*

Příbuzné obory: teorie množin, logika, teorie čísel, výpočetní složitost, matematické struktury, obecná algebra . . .

Naučíme se porozumět zadání úloh, popsat je pomocí matematických pojmů a s použitím vhodné symboliky.

Budeme nejen hledat jejich řešení, ale hlavně se učit *odůvodňovat*, že je řešení správné. Budeme také hledat různé cesty k řešení.

Z jednoduchých a konkrétních pojmů budeme budovat pojmy a vztahy složitější a obecnější — abstraktnější.

Celočíselná a modulární aritmetika

Jednodušší než množiny jsou přirozená a celá čísla
(nezajímá nás obsah konečných množin, ale jen jejich velikosti).

Definice: Pro celá čísla a a b, říkáme, že a *dělí* b (beze zbytku), právě když existuje celé číslo c takové, že $b = ac$. Značíme $a|b$.

Stručněji: Pro $a, b \in \mathbb{Z}$: a *dělí* $b \Leftrightarrow \exists c \in \mathbb{Z}$: $b = ac$, značíme $a|b$.

$\mathbb{Z}$ znamená množinu celých čísel (z něm. *Zahlen*),
podobně $\mathbb{N}$ množinu přirozených čísel (z lat. *numero, naturalis*).

365 a 1 mají stejný zbytek po dělení 7 — tato vlastnost má jméno:

Definice: Pro celá čísla a, b a n, kde $n \geq 2$, říkáme, že a *je kongruentní s* b *modulo* n, pokud rozdíl čísel a a b je beze zbytku dělitelný n. Formálně zapsáno: $n|(a - b)$.
Značení: „a je kongruentní s b modulo n“: $a \equiv b \pmod{n}$.

Ukázky: $365 \equiv 1 \pmod{7}$, $1 \equiv 365 \pmod{7}$, $29 \equiv 365 \pmod{7}$.
Výraz $a \equiv 1 \pmod{2}$ znamená, že a je liché.

K definicím a značení

Definice: Pro celá čísla a, b a n, kde $n \geq 2$, říkáme, že *a je kongruentní s b modulo n*, pokud rozdíl čísel a a b je beze zbytku dělitelný n. Formálně zapsáno: $n|(a-b)$.
Značení: „a je kongruentní s b modulo n“: $a \equiv b \pmod{n}$.

Definice se *nedokazují*, jen je třeba vždy ověřit, zdali si objekt uvažovaný *název* zaslouží. Podobně značení zavádí nový *symbol*. Název ani symbol by se neměly plést s již zavedenými pojmy.

V definicích využíváme jednodušší nebo dříve zavedené pojmy, zde např. „celá čísla“, „rozdíl“, „dělí beze zbytku“ ...
Můžeme se ptát, jak jsou definovány tyto jednodušší pojmy, atd., atd., až dojdeme k elementárním objektům z teorie množin, které se už dále nedefinují: prvek, množina, třída a relace náležení.

V tomto kurzu budeme vycházet ze středoškolské představy přirozených, racionálních a reálných čísel, konečných množin a základních početních a množinových operací.

Jaký zbytek má n^2 při dělení 4, resp. 8?

n	n^2	$n^2 \bmod 4$	$n^2 \bmod 8$
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
8	64	0	0
9	81	1	1

Z tabulky se zdá, že
pro sudé n je $n^2 \equiv 0 \pmod 4$ a
pro liché n je $n^2 \equiv 1 \pmod 4$.

Vskutku, pro $(\mathrm{mod}\ 4)$:

$$(2k)^2 = 4k^2 \equiv 0$$
$$(2k+1)^2 = 4(k^2+k)+1 \equiv 1$$

Podobně pro $(\mathrm{mod}\ 8)$:

$$(4k)^2 = 16k^2 \equiv 0$$
$$(4k+2)^2 = 16(k^2+k)+4 \equiv 4$$
$$(2k+1)^2 = 4\underbrace{(k^2+k)}_{\text{sudé}}+1 \equiv 1$$

Jednoduchá pozorování z celočíselné aritmetiky

Pozorování: Pro dělitelnost platí:
$1|b$ pro všechna $b \in \mathbb{Z}$,
$a|0$ pro všechna $a \in \mathbb{Z}$ včetně 0, t.j. $0|0$,
$n|b \Leftrightarrow b \equiv 0 \pmod{n}$ pro všechna $b, n \in \mathbb{Z}, n \geq 2$.

Pozorování: Pro kongruenci modulo libovolné $n \geq 2$ platí:
$a \equiv a$ (tzv. *reflexivita*), $a \equiv b \Leftrightarrow b \equiv a$ (*symetrie*),
$(a \equiv b) \wedge (b \equiv c) \Rightarrow a \equiv c$ (*tranzitivita*).

Pozorování: Pro kongruenci $\pmod{n}$ platí: když $(a \equiv b) \wedge (a' \equiv b')$,
tak potom $a + a' \equiv b + b'$, $a - a' \equiv b - b'$ a také $aa' \equiv bb'$.

Pozor, obrácené implikace neplatí, například pro $\pmod{6}$:
$2 + 3 \equiv 0 + 5$ a také $2 \cdot 3 \equiv 0 \cdot 5$, ale $2 \not\equiv 0$ ani $3 \not\equiv 5$.

Platí však podobný vztah pro sčítání i odčítání:
$(a + a' \equiv b + b') \wedge (a' \equiv b') \Rightarrow a \equiv b$,
ale už ne pro násobení: $(aa' \equiv bb') \wedge (a' \equiv b') \not\Rightarrow a \equiv b$,
např. $(2 \cdot 3 \equiv 0 \cdot 3) \wedge (3 \equiv 3)$, ale $2 \not\equiv 0$.

K výrokům, větám, pozorováním . . . a k důkazům

Věty, pozorování, tvrzení a lemmata jsou *pravdivé* matematické výroky, jen se liší svou důležitostí (podle názoru mluvčího). *Výrok* je gramaticky správná věta v matematickém jazyce, u níž má smysl posuzovat, zda platí nebo ne. Výrok je pravdivý, když ho lze odvodit pomocí logických operací z výchozích předpokladů, tzv. *axiomů*. Tomuto odvození říkáme *důkaz*. Pokud lze naopak dokázat negaci výroku, je výrok nepravdivý.

V tomto kurzu budeme za axiomy považovat jednoduchá pravidla o číslech, množinách a souvisejících operacích, která známe ze střední školy, například komutativitu sčítání: $a + b = b + a$.

Jsou výroky, u kterých *nelze dokázat* jejich pravdivost ani nepravdivost. Příkladem je 5. Eukleidův postulát o rovnoběžkách. Někdy *jen nevíme*, zda je výrok pravdivý nebo zda ho lze dokázat. Věříme-li v jeho pravdivost, nazýváme ho *domněnka* či *hypotéza*. Třeba Velká Fermatova věta byla do roku 1994 „jen“ domněnkou.

Zpět k pozorováním a jejich důkazům

Pozorování je výrok, jehož důkaz je z hlediska mluvčího „tak jednoduchý, tak vidět, že ho není třeba ani zmínit“.

Pokud ho nevidíte, *NEBOJTE SE PŘIHLÁSIT A PTEJTE SE!*
Není to zbabělost nebo neschopnost, ale výraz odvahy
— pomůžete nejen sobě, ale často i ostatním.

Ukázky:
Pozorování: $\forall b \in \mathbb{Z}\colon 1|b$.
Důkaz: Podle definice $a|b \Leftrightarrow \exists c \in \mathbb{Z}\colon b = ac$,
Pro $a = 1$ stačí zvolit $c = b$, protože $b = 1 \cdot b$.

Pozorování: $(a \equiv b) \wedge (a' \equiv b') \Rightarrow (aa' \equiv bb') \pmod{n}$.
Důkaz: Z definice kongruence $n|a - b$, čili $\exists c\colon a - b = cn$.
Podobně $\exists c'\colon a' - b' = c'n$. Chceme $\exists d\colon aa' - bb' = dn$.
$aa' - bb' = aa' - ab' + ab' - bb' = a(a' - b') + (a - b)b' =$
$ac'n + cnb' = (ac' + cb')n$, čili $aa' - bb' = dn$ pro $d = ac' + cb'$.

Další pozorování zkuste sami doma nebo se zeptejte na cvičeních.

Dirichletův princip

Máme m předmětů a n přihrádek, kde $m > n$.
Každý předmět dáme do některé přihrádky.
Pak v některé jsou alespoň dva předměty.

Důkaz: Označme x_i počet předmětů v i-té přihrádce. Pak $x_1 + x_2 + \cdots + x_n = m$.
Kdyby v každé přihrádce byl nejvýš jeden předmět, měli bychom $x_1 + x_2 + \cdots + x_n \leq n$, což je spor s nerovností $n < m$.
Proto pro alespoň jedno i platí $x_i \geq 2$.

Stručnější formulace:
Pro konečné množiny A a B, kde $|A| > |B|$, neexistuje prosté zobrazení $f : A \to B$, kde *být prosté* znamená: $x \neq y \Rightarrow f(x) \neq f(y)$.

Johann Peter
Gustav Lejeune
Dirichlet
1805 – 1859

[Obr. Wikipedie]

angl. *pigeonhole principle* — princip holubníku; přihrádkový princip