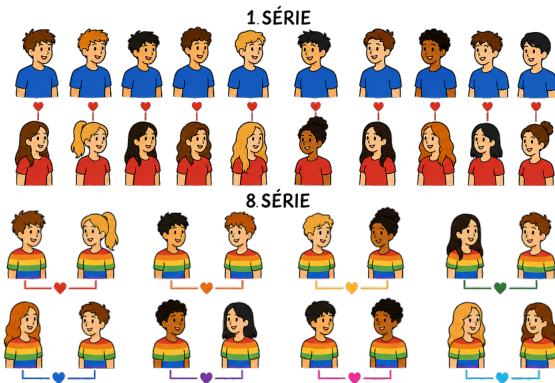


Diskrétní matematika

V 1. sérii reality show *Are you the one?* byla skupina 10 žen a 10 mužů tajně spárována do „optimálních“ dvojic. Soutěžící měli za cíl toto optimální párování odhalit a tak vyhrát 1 000 000 \$.

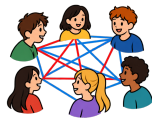
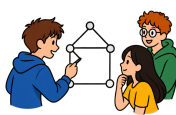
V 8. sérii bylo jen 16 soutěžících, ale nezáleželo na pohlaví, tedy optimální dvojici mohli tvořit i dva muži nebo dvě ženy.

Je v 8. sérii možných párování více nebo méně než v 1. sérii?



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.

„Počítá se to přes permutace, kombinace nebo variace?“ „ 10^2 možností je asi málo, a 10^{10} mi přijde moc, žejo?“

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

... nestačí odpovědět jen: „Párování je 3 628 800 a v 8. sérii jich bylo víc než v 1.“ — což ani není celé pravda.

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*).

Vloni bylo HOMONOLO 1. – 5. prosince 2025 (po – pá), letos je o týden později. Na který pátek je třeba zajistit náhradu přednášky?

Rok 2026 je nepřestupný, má 365 dní. $365 = 350 + 14 + 1$, což je 52 týdnů a *jeden* den navíc. 5. prosince 2026 bude v sobotu.

Suplování je třeba zajistit na následující pátek 11. prosince.

Nezajímal nás celočíselný podíl z 365 po dělení 7, ale *zbytek*.

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.

Modulární aritmetika

Použití: Cyklicky opakované události, například $\text{mod } 60$ pro minuty v hodině, $\text{mod } 24$ pro hodiny během dne, ...

Caesarova šifra: šifrování: $x \rightarrow x + 3 \pmod{26}$



Y Z A B C D E F G

dešifrování: $x \rightarrow x - 3 \pmod{26}$

Geocaching

Decryption Key

A	B	C	D	E	F	G	H	I	J	K	L	M
---	---	---	---	---	---	---	---	---	---	---	---	---

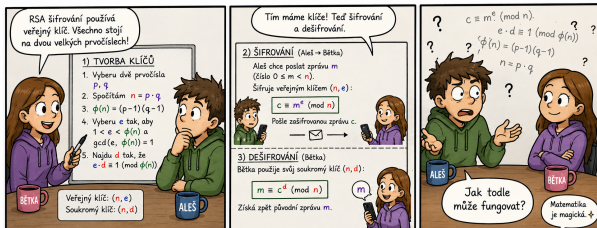
N|O|P|Q|R|S|T|U|V|W|X|Y|Z

$$x \rightarrow x + 13 \pmod{26}$$

Malá Fermatova věta:

Pro každé prvočíslo p a každé celé číslo a platí $a^p \equiv a \pmod{p}$.

RSA: šifrování s veřejným klíčem, elektronický podpis, <https://>



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 $\pmod{4}$:

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

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

Podobně pro $\pmod{8}$:

$$(4k)^2 = 16k^2 \equiv 0$$

$$(4k+2)^2 = 16(k^2+k) + 4 \equiv 4$$

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

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 výroků, 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: $\forall b \in \mathbb{Z}: 1|b$.

Důkaz: Podle definice $a|b \Leftrightarrow \exists c \in \mathbb{Z}: b = ac$,

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 $\exists c: a - b = cn$.

Podobně $\exists c': a' - b' = c'n$. Chceme $\exists d: aa' - bb' = dn$.

$$\begin{aligned} aa' - bb' &= aa' - ab' + ab' - bb' = a(a' - b') + (a - b)b' = \\ &= ac'n + cnb' = (ac' + cb')n, \text{ čili } aa' - bb' = dn \text{ pro } d = ac' + cb'. \end{aligned}$$

Další pozorování zkuste sami doma nebo se zeptejte na cvičeníh.

Co už může být a co určitě není důkaz?

Pozorování Pro každé celé n platí $3|n^3 - n$.

Důkaz 1: Jde o pozorování, u něho není nikdy co dokazovat.

Důkaz 2: Všimneme si, že $n^3 - n = n(n^2 - 1) = (n - 1)n(n + 1)$, což je součin tří po sobě jdoucích čísel a jedno z nich je dělitelné 3. $3|n$ pro $n \equiv 0 \pmod{3}$, $3|(n - 1)$ pro $n \equiv 1$ a $3|(n + 1)$ pro $n \equiv 2$.

Důkaz 3: Pro $n = 0$ je $0^3 - 0 = 0$ dělitelné 3, pro $n = 1$ je $1^3 - 1 = 0$ dělitelné 3, pro $n = 2$ je $2^3 - 2 = 8 - 2 = 6$ dělitelné 3, pro ostatní čísla je to podobné, jen u záporných bude navíc mínus.

Důkaz 4: Rozebereme případy (ve všech je $k \in \mathbb{Z}$):

- ▶ když $n = 3k$, pak $n^3 - n = (3k)^3 - 3k = 3(9k^3 - k)$,
- ▶ když $n = 3k + 1$, pak $n^3 - n = 3k(3k + 1)(3k + 2)$,
- ▶ když $n = 3k + 2$, pak $n^3 - n = 3(k + 1)(3k + 1)(3k + 2)$.

Ve všech případech máme $3|n^3 - n$, a ty pokrývají všechna celá n .

Důkaz 5: Označíme $n = 3k + l$, $l \in \{0, 1, 2\}$, pak $n^3 - n = (3k + l)^3 - (3k + l) = 3(9k^3 + 9k^2l + 3kl^2 - k) + l^3 - l$, přičemž $3|l^3 - l$ pro $l \in \{0, 1, 2\}$, jak jsme ukázali v důkazu 3.

Problém „jedničkových čísel“

Existuje n takové, že 2 025, 2 026 nebo 2 027 dělí $J_n = \underbrace{11 \dots 1}_{n \times}$?

Vidíme, že každé J_n je liché, tedy 2 026 nikdy nedělí J_n .

Podobně žádné J_n nekončí 0 ani 5, a tak ani 2 025 nedělí žádné J_n .

Co si ale počneme s 2 027? ▶

Vyzkoušíme menší hodnoty dělitele d . Můžeme vynechat sudá čísla a násobky pěti, a místo $d = 2\,027$ zkusíme $d = 1, 3, 7, 9, 11, 13, \dots$

d	J_n	d	J_n	d	J_n	
1	1	7	111 111	11	111 111	$111\,111 =$
3	111	9	111 111 111	13	111 111	$= 111 \cdot 1\,001$
						$= 111 \cdot 7 \cdot 11 \cdot 13$

Hypotéza: Pro každé d , které není násobkem 2 ani 5, J_n existuje. Zbytek po dělení d nabývá jen d hodnot, proto podle *Dirichletova principu* z $d + 1$ čísel $J_1, \dots, J_{d+1}$ mají alespoň dvě stejný zbytek.

Čili $\exists i, j \in \{1, \dots, d + 1\}, i > j: J_i \equiv J_j \pmod{d}$.

Potom $d \mid J_i - J_j$, přičemž $J_i - J_j = \underbrace{11 \dots 1}_{(i-j) \times} \underbrace{00 \dots 0}_{j \times} = J_{i-j} \cdot 10^j$.

Protože $2 \nmid d$, $5 \nmid d$, musí $d \mid J_{i-j}$.

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 $x_1 + x_2 + \dots + x_n = m$. Kdyby v každé přihrádce byl nejvýš jeden předmět, měli bychom $x_1 + x_2 + \dots + x_n \leq n$, 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 $f : A \rightarrow B$, kde *být prosté* znamená: $x \neq y \Rightarrow f(x) \neq f(y)$.

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



Johann Peter
Gustav Lejeune
Dirichlet
1805 – 1859

[Obr. Wikipedie]

Celočíselné kořeny polynomů

Kořeny kvadratického polynomu $f(x) = ax^2 + bx + c$ lze spočítat známým vzorcem $x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$; pro kořeny polynomu 3. stupně máme Cardanovy vzorce, pro 4. Ferrariho metodu. Pro obecný polynom 5. a vyššího stupně, např. pro $x^5 - x - 1$, žádné vzorce existovat nemohou, jak dokázal roku 1830 Évariste Galois.

Celočíselné kořeny polynomu libovolného stupně s celočíselnými koeficienty lze nalézt snadno:

Mějme $f(x) = a_n x^n + \dots + a_1 x + a_0$. Je-li $a_0 = 0$, je 0 kořenem f , a vydělením $(x - 0)$ se sníží stupeň na $a_n x^{n-1} + \dots + a_2 x + a_1$.

Pro $a_0 \neq 0$ jako např. v $f(x) = 4x^5 - 12x^4 - 5x^3 + 15x^2 + x - 3$ a celočíselný kořen x platí, že $f(x) = 0 \equiv a_0 \pmod{x}$, protože z ostatních členů $a_n x^n, \dots, a_1 x$ lze x vytknout.

Každý celočíselný kořen x polynomu $f(x)$ je proto dělitelem a_0 .

Např. pro $a_0 = -3$ máme dělitele 3, 1, -1 a -3. Dosazením do daného $f(x)$ zjistíme, že jen 3, 1 a -1 jsou jeho celočíselné kořeny.

Lze tento postup rozšířit i pro racionální kořeny?

Racionální kořeny polynomů

Jsou-li koeficienty racionální, lze je vynásobit nejmenším společným násobkem jmenovatelů, a tak *bez újmy na obecnosti* (zkr. *búno*) můžeme předpokládat, že polynom $f(x) = \sum_{i=0}^n a_i x^i$ má celočíselné koeficienty, stejně jako v předchozím případě.

Předpokládejme, že $x = \frac{p}{q}$ s nesoudělnými p a q je racionální kořen polynomu f , t.j. $f\left(\frac{p}{q}\right) = \sum_{i=0}^n a_i \left(\frac{p}{q}\right)^i = 0$.

Vynásobením obou stran q^n dostaneme rovnici $\sum_{i=0}^n a_i p^i q^{n-i} = 0$,

a podle ní omezíme možnosti pro p a q , podobně jako u $x \in \mathbb{Z}$.

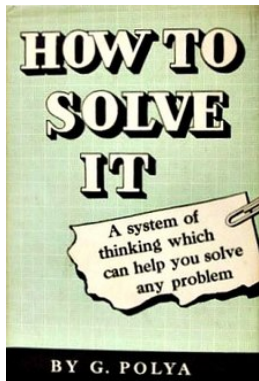
Pro nesoudělná p, q platí: $\forall a \in \mathbb{Z}: p|aq \Rightarrow p|a$, a také $q|ap \Rightarrow q|a$.

Při počítání *mod* p dostaneme u posledního členu: $p|a_0 q^n \Rightarrow p|a_0$.

Při počítání *mod* q dostaneme u prvního členu: $q|a_n p^n \Rightarrow q|a_n$.

Např. pro náš polynom $f(x) = 4x^5 - 12x^4 - 5x^3 + 15x^2 + x - 3$ je $p \in \{\pm 1, \pm 3\}$ a $q \in \{\pm 1, \pm 2, \pm 4\}$, a dosazením zjistíme, že kromě celočíselných kořenů $3, 1, -1$, má i racionální $\frac{1}{2}$, $-\frac{1}{2}$ a jiné už ne.

Jak to řešit?



1. vydání, Princeton
Univ. Press, 1945



George Pólya
1887–1985



1. české vydání,
Matfyzpress, 2016

JAK ŘEŠIT MATEMATICKOU ÚLOHU

POROZUMĚNÍ ÚLOZE

Za první.

Musíte porozumět úloze.

Co je zde neznámá? Jaké jsou údaje? Jaké jsou podmínky?

Je možné vyhovět podmínkám? Jsou podmínky dostatečné pro určení neznámé? Nebo jsou nedostačující? Nebo nadbytečné? Nebo obsahují rozpor?

Nakreslete si obrázek. Zaveďte vhodné označení.

Oddělte od sebe různé podmínky. Umíte je zapsat?

NAVRŽENÍ PLÁNU ŘEŠENÍ

Za druhé.

Najděte souvislosti mezi údaji a neznámou.

Už jste viděli úlohu předtím? Nebo jste ji viděli v trochu jiném tvaru?

Znáte nějakou příbuznou/podobnou úlohu? Znáte nějakou větu, která by mohla být užitečná?

Možná budete muset vyřešit pomocné úlohy, pokud bezprostřední souvislost nelze najít. Nakonec budete muset sestavit *plán* řešení.

Podívejte se na neznámou! A zkuste přemýšlet o všeobecně známé úloze mající tutéž nebo podobnou neznámou.

Tady je úloha příbuzná té vaší, která již byla vyřešena. Můžete ji využít? Můžete využít její výsledek? Můžete použít její metodu?

Uměli byste zavést nějaký pomocný prvek, abyste takové využití umožnili? Umíte úlohu přeformulovat? Můžete ji přeformulovat ještě jednou?

Vraťte se k definicím.

Jestliže nemůžete vyřešit předloženou úlohu, pokuste se vyřešit nějakou příbuznou úlohu. Umíte si představit nějakou přístupnější příbuznou úlohu? Nebo obecnější úlohu? Speciálnější úlohu? Analogickou úlohu? Umíte vyřešit aspoň část úlohy? Uvažujte pouze část z daných podmínek a vynechejte jejich další části. Nakolik je pak neznámá určena, a jak se může měnit? Umíte odvodit něco užitečného z daných údajů? Umíte si představit jiné údaje, vhodné pro určení neznámé? Můžete změnit neznámou nebo údaje, nebo v případě nutnosti obojí tak, že nová neznámá a nové údaje mají k sobě blíže?

Využili jste všechny údaje? Využili jste všechny podmínky? Vzali jste v úvahu všechny podstatné pojmy použité v úloze?

REALIZACE PLÁNU

Za třetí.

Realizujte svůj plán.

Při realizaci vašeho plánu řešení *překontrolujte každý krok.*

Vidíte jasně, že tento krok je správný? Umíte dokázat, že je správný?

POHLED ZPĚT

Za čtvrté.

Přezkoušejte nalezené řešení.

Umíte *překontrolovat výsledek*? Umíte zkontrolovat důkaz?

Umíte stejný výsledek získat jinak? Vidíte to na první pohled?

Umíte použít výsledek nebo metodu na vyřešení jiné úlohy?