Aritmetika a algebra I

Literatura k předmětu:

[BeDla] Dlab V., Bečvář J.: *Od aritmetiky k abstraktní algebře.* Serifa, Praha, 2016. 2. vyd.: ČVUT, 2022. (k dostání za 400 Kč přímo u mne, v knihkupectvích za cca 550 Kč)

[Be] Bečvář J.: *Lineární algebra.* Matfyzpress, Praha, 2019. (pouze po stranu 60)
knižní podoba v nakladatelství MatfyzPress (přímo v karlínské budově, na vrátnici Vás nasměrují)

Podmínky udělení zápočtu:

1. úspěšné napsání průběžného testíku v semestru,
2. samostatné vypracovávání domácích úkolů v průběhu semestru (bude ověřeno u závěrečného testíku, kde se předkládá portfolio),
3. úspěšné napsání závěrečného testíku ve zkouškovém období (příklady pokrývající celý semestr).

Požadavky ke zkoušce:
Zkouška je zaměřena teoreticky, požaduje se dobrá znalost teorie v rozsahu probíraném na seminářích (včetně úloh zadávaných k samostatnému rozmyšlení). Klíčem k úspěchu je znát definice (i proč vypadají právě takto), důkazy a odvození, principy, proč co platí.

Není dobrý nápad se učit látku zpaměti, důraz je kladen na porozumění.

Zápočet a zkouška

S sebou:

- portfolio (vyřešené úlohy označené hvězdičkou z tohoto souboru; poznámky a shrnutí teorie není potřeba opisovat),
- samostatný kalkulátor (nikoli v mobilu),
- něco na psaní (pouze propiska; nikoli papíry, ty rozdávám).

Na zkoušce je zadán testík obsahující příklady (podobné těm z tohoto souboru), při jeho zadávání se odevzdává portfolio. Portfolio po prohlédnutí vracím.

Portfolio + úspěšný testík z příkladů = zápočet.

Ihned či na kterémkoli dalším termínu lze psát teoretickou část (důkazy vět, definice, ...). Na základě tohoto testíku se uděluje hodnocení zkoušky.

Na oba tyto testíky zpravidla navazuje rozhovor nad vypracovanými úlohami a otázkami.

Do portfolia je třeba vypracovat úlohy označené hvězdičkou.

Ostatní úlohy se do portfolia psát nemusejí (buď jsou to věci k rozmyšlení nebo jsou nepovinné pro zájemce).

Osnova předmětu

1. Definice, věta, důkaz. Typy důkazů vět ve tvaru implikace: přímý, nepřímý, sporem. Poznámka k rozdílu mezi rovnicí a rovností. $a^n \pm b^n$, součet prvních n členů geometrické posloupnosti.

2. Mohutnost (kardinalita) množiny, množiny konečné, spočetné a nejvýše spočetné, $|\mathbb{N}| = \aleph_0$, charakterizace nekonečných množin pomocí vlastních podmnožin. Mohutnost jednotlivých číselných oborů: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

3. Úvod do algebraických struktur. Zákon komutativní, asociativní, distributivní. Binární operace.
   - Algebraické struktury s jednou binární operací: grupoid, pologrupa, monoid, grupa. Grupa: motivace, definice, příklady (číselné grupy, translace, matice, ...).
   - Algebraické struktury se dvěma binárními operacemi: pole, těleso; příklady pole ($\mathbb{R}, \mathbb{C}, \mathbb{Z}_p$); počítání v tělese, charakteristika tělesa. Okruh, obor integrity; motivace, příklady.

4. Zobrazení a funkce. Definice zobrazení, injekce, surjekce, bijekce, graf zobrazení. Rozklad zobrazení na surjekci a injekci. Transformace a permutace množiny.

5. Binární relace. Uspořádaná a neuspořádaná dvojice, kartézský součin, n-tá kartézská mocnina množiny. Relace z množiny do množiny, relace v množině, kartézský graf. Příklady relací. Skládání relací, relace inverzní, $(R_1 \circ R_2)^{-1} = R_2^{-1} \circ R_1^{-1}$, asociativita skládání relací (tedy i zobrazení a funkcí).
   Ekvivalence: relace reflexivní, symetrická, tranzitivní, relace ekvivalence na množině, rozklad množiny, třída (blok) ekvivalence, faktorová množina; ekvivalence na množině indukuje její rozklad a rozklad definuje ekvivalenci.
   Uspořádání: relace antisymetrická, množina uspořádaná částečně, úplně (lineárně), dichotomie. Lexikografické uspořádání. Hasseův diagram, svaz dělitelů; prvek nejmenší, největší, minimální, maximální.

6. Permutace. Skládání (součin) permutací, inverzní permutace. Rozklad na nezávislé cykly, transpozice. Inverze, znaménko (znaménko součinu permutací je součinem jejich znamének, transpozice je lichá, výpočet pomocí počtu nezávislých cyklů). Umocňování permutací.

7. Přirozená čísla, zavedení genetickou metodou, čísla von Neumannova. Zavedení sčítání a násobení přirozených čísel. Princip matematické indukce a princip dobrého uspořádání, ekvivalence těchto principů. Důkaz matematickou indukcí. Součty mocnin přirozených čísel.

8. Dělení se zbytkem, eukleidovské dělení a jeho aplikace (převod mezi pozičními číselnými soustavami o různém základu, násobení čísel zapsaných římskými číslicemi). Eukleidův algoritmus, věta Bézoutova, aplikace Bézoutovy věty na řešení lineární diofantické rovnice.
   Důsledky Bézoutovy věty: Gaussova věta a Eukleidovo lémma, Základní věta aritmetiky.
   Malá Fermatova věta. Porovnání Malé Fermatovy věty a věty Bézoutovy.
   Vyjádření NSD a nsn pomocí součinu mocnin prvočísel.

9. Řetězové zlomky. Vyjádření racionálních čísel řetězovými zlomky, rozvoj iracionálního čísla do řetězového zlomku, souvislost s Eukleidovým algoritmem. Konvergenty a jejich efektivní výpočet pomocí rekurentních formulí. Pozorování chování posloupnosti konvergentů (střídavě jsou větší a menší než přesná hodnota řetězového zlomku). Řešení lineární diofantické rovnice pomocí řetězových zlomků.

10. Dělitelnost. Dělitel, násobek, největší společný dělitel, nejmenší společný násobek, čísla nesoudělná. Hasseovy diagramy, svaz všech dělitelů. Základní kritéria dělitelnosti, odvození.

11. Prvočísla. Eukleidova věta o nekonečném počtu prvočísel. Eratosthenovo síto.
    Mersennova a Fermatova čísla, počet cifer. Matijasevičova parabola. Mersennova čísla a prvočísla, sudá dokonalá čísla, vztah mezi nimi: věta Eukleidova a Eulerova. Fermatova čísla a jejich vlastnosti, věta o konstruovatelnosti pravidelných n-úhelníků pomocí pravítka a kružítka.

12. Konstrukce aditivní grupy celých čísel.

1 Definice, věta, důkaz

Definice:

- pozor: netvrdíme, že *čtverec je čtyřúhelník takový, že...*, ale měly by se vyskytnout výrazy typu: *říkáme, že...*; *nazýváme*; *označujeme*; ...
- definice musí definovaný pojem skutečně charakterizovat
- definice by neměla obsahovat nadbytečné podmínky, předpoklady, ...

Věty (matematické): pozor: není-li pravdivost výroku dokázána, nejedná se o matematickou větu (může se jednat o hypotézu).

V matematice máme zpravidla věty ve tvaru:

- **elementárního výroku** (např. $\sqrt{2}$ je iracionální číslo),
- **implikace** (např. $\forall a, b, c \in \mathbb{R} : \ a = b \implies ac = bc$),
- **ekvivalence** (např. $\forall a, b \in \mathbb{R} : \ a^2 + b^2 = 0 \iff (a = 0 \wedge b = 0)$).

Důkazy vět ve tvaru ekvivalence:

- Jak dokazujeme ekvivalenci $A \iff B$? Dokážeme $(A \implies B) \wedge (B \implies A)$.
- Jak dokazujeme ekvivalenci tří výroků A, B, C? Stačí dokázat „kolečko“, tj. dokážeme

$$(A \implies B) \wedge (B \implies C) \wedge (C \implies A).$$

Důkazy vět ve tvaru implikace:
Typy důkazů vět ve tvaru implikace, tj. ve tvaru $A \implies B$:

- přímý: $A \implies B_1$, $B_1 \implies B_2$, $B_2 \implies B_3$, ..., $B_n \implies B$
- nepřímý: je to vlastně přímý důkaz obměněné implikace: $\neg B \implies \neg A$. Vychází z toho, že implikace je s ní ekvivalentní:

$$(A \implies B) \iff (\neg B \implies \neg A)$$

- sporem: místo $A \implies B$ dokazujeme $\neg(A \wedge \neg B)$, neboť platí

$$(A \implies B) \iff \neg(A \wedge \neg B)$$

  Předpokládáme tedy A a to, že neplatí tvrzení, tj. $\neg B$. Typický začátek důkazu sporem je: *kdyby neplatilo B, tak by ...*

Pokud A neplatí, je $A \implies B$ splněno automaticky, nemusíme nic dokazovat.

Příklad důkazu sporem: *Jestliže má posloupnost $\{a_n\}$ limitu, pak je tato limita právě jedna.*
Důkaz sporem: Kdyby neplatilo B, tj. kdyby měla posloupnost více limit, tak by měla aspoň dvě různé limity, ozn. je a a b, tj. ... $a - \varepsilon < a_n < a + \varepsilon$ a $b - \varepsilon < a_n < b + \varepsilon$. Bez újmy na obecnosti nechť např. je $a < b$. Pak z předpokladu A a negace $\neg B$ plyne (po úvahách a úpravách):

$$a_n < a + \varepsilon < b - \varepsilon < a_n \,,$$

tj. $a_n < a_n$, což není možné; říkáme, že jsme došli ke sporu. Neplatí tedy $A \wedge \neg B$, tj. platí $\neg(A \wedge \neg B)$, což je ekvivalentní s $A \implies B$, takže je tato implikace dokázána. □

Poznámka k rozdílu mezi rovnicí a rovností $L(x) = P(x)$
(pro jednoduchost uvažujeme jednu neznámou / proměnnou):

- rovnice: úloha najít všechna x z dané množiny taková, aby $L(x) = P(x)$,
- rovnost: výrok, že pro všechna x z dané množiny platí: $L(x) = P(x)$.

1.1 Typy důkazů :-)

- Důkaz přenecháním: „Důkaz přenecháváme čtenáři jako snadné cvičení.“
- Důkaz vypuštěním: „Čtenář si snadno doplní detaily.“
- Důkaz odkladem: „Toto si dokážeme v jedné z příštích přednášek.“
- Důkaz zastrašováním: „Pokud nebudete věřit, že to platí, tak zkoušku neuděláte.“
- Důkaz pokušením: „Přesvědčte se, že to platí!“
- Důkaz odkazem na nedostupnou literaturu: Autor cituje jednoduchý důsledek věty uvedené v soukromých zápiscích Slovinské filologické společnosti z roku 1883.
- Důkaz přijetím: „Chce se po nás, abychom to dokázali, proto to platí.“
  „Měli jsme to dokázat jako cvičení, takže to platí.“
- Důkaz rychlokurzem: „Nemáme čas to tu dokazovat.“
- Důkaz soucitem: „Ušetřím vás zbytečných detailů a přejdu rovnou k hlavnímu důsledku.“
- Důkaz zjevností: „Důkaz je tak jasný, že není třeba ho zmiňovat.“
- Důkaz obecným souhlasem: „Všichni pro…?“
- Důkaz předpokladem: „Budeme předpokládat, že je to pravda.“
- Důkaz představivostí: „Představme si, že je to pravda.“
- Důkaz odkazem na chystané dílo: Odkaz je obyčejně na chystané dílo autora, které často není tak chystané, jak se zprvu zdálo.
- Důkaz nutností: „Raději by to mělo platit, jinak se celá struktura matematiky zhroutí.“
- Důkaz definicí: „Definujeme, že platí...“
- Důkaz nedostatkem zájmu: „Chce to opravdu někdo vidět?“
- Důkaz bulharskou konstantou: „Nechť c je takové číslo, aby důkaz fungoval.“
- Důkaz redukcí: „Tento důkaz se zjednoduší na $1 + 1 = 2$.“
- Důkaz podvodem: „Teď se všichni otočte…“

2 Množiny

Jak je tomu s definicí množiny? Množina je tzv. *primitivní pojem*, je to tedy cokoli, co vyhovuje axiómům teorie množin. S axiómy teorie množin (existuje několik různých přístupů) se seznámíme v 5. ročníku.

Axiómaticky budovaná teorie je založena na souboru axiómů, které vypovídají něco o vlastnostech jinak nespecifikovaných a nedefinovaných pojmů, tzv. *primitivních pojmů*. Například v planimetrii jsou primitivními pojmy *bod* a *přímka*.

Výhoda axiómatického přístupu k matematice: za primitivní pojmy lze dosadit cokoli, co vyhovuje podmínkám (axiómům). Matematika se tak stává abstraktní, tj. nemá konkrétní obsah.

S nadsázkou a humorem lze říci: matematika budovaná axiómaticky je o ničem, což je moc dobře.

Mohutnost (kardinalita) množiny
Říkáme, že množiny A a B mají stejnou mohutnost, existuje-li bijekce množiny A na množinu B. (samozřejmě pak také existuje bijekce množiny B na množinu A, je to inverzní zobrazení k původní bijekci)

bijekce – vzájemně jednoznačné zobrazení, tj. zobrazení, které je zároveň prosté (*injektivní*) a na (*surjektivní*).

Jak si představit mohutnost množiny intuitivně? U konečné množiny jako počet jejích prvků. U nekonečné to začne být skutečně zajímavé, lze například dokázat, že

$$|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| \ < \ |\mathbb{R}| = |\mathbb{C}| \ .$$

Mohutnost množiny A značíme $|A|$. Mohutnost množiny $\mathbb{N}$ značíme $\aleph_0$, čteme *alef nula* (alef je první písmeno hebrejské abecedy). O množinách, které mají mohutnost $\aleph_0$ (neboli stejnou mohutnost, jako množina přirozených čísel), říkáme, že jsou *spočetné*. Množiny, které jsou buď konečné, nebo spočetné, nazýváme *nejvýše spočetné*.

Příklady spočetných množin:

- množina všech přirozených čísel větších než milion $\{10^6+1, 10^6+2, 10^6+3, 10^6+4, ...\}$,
- množina všech uspořádaných dvojic přirozených čísel $\mathbb{N}^2$,
- množina všech uspořádaných trojic přirozených čísel $\mathbb{N}^3$,
- množina všech prvočísel $\mathbb{P}$,
- množina všech kladných sudých čísel $2\mathbb{N}$,
- množina všech celočíselných násobků sedmnácti $17\mathbb{Z}$,
- množina všech uspořádaných n-tic racionálních čísel $\mathbb{Q}^n$.

Příklady nespočetných množin:

- množina všech uspořádaných n-tic reálných čísel $\mathbb{R}^n$.
- množina všech komplexních čísel $\mathbb{C}$,
- množina všech uspořádaných n-tic komplexních čísel $\mathbb{C}^n$,
- množina všech funkcí $\{f : \mathbb{R} \to \mathbb{R}\}$.

Pozor: množina všech funkcí $\{f : \mathbb{R} \to \mathbb{R}\}$ má mohutnost ostře větší než $|\mathbb{R}|$.

Charakterizace nekonečných množin:
Pro nekonečnou množinu je charakteristické, že existuje nějaká její vlastní[1] podmnožina, s níž je celá množina ekvivalentní.

- Všimněte si, že nekonečnou množinu od konečné odlišuje tato vlastnost: nekonečná množina obsahuje vlastní podmnožinu, která je s ní ekvivalentní (tj. mají stejnou mohutnost, tj. existuje mezi nimi bijekce). U konečných množin už tohle neplatí. Takto definoval nekonečnou množinu Richard Dedekind, viz [BeDla], str. 26 nahoře:

  Řekneme, že množina M je nekonečná, jestliže existuje injektivní (neboli prosté) zobrazení $f : M \to M$ takové, že $f(M) \neq M$.

- Probádejte definici kartézské mocniny. Zpočátku to vypadá jednoduše: $A^2 := A \times A$, dále $A^3 := A \times A \times A$, ...
  Dohodneme-li se, že místo $[a]$ budeme psát pouze samotný prvek a, můžeme dodefinovat $A^1 := A$.
  Proč však (pouze pro $A \neq \emptyset$) dodefinováváme $A^0 := \{\emptyset\}$? Bude pak platit, že

$$A^m \times A^n = A^{m+n} \, ?$$

  Konkrétně: bude $A^n \times A^0 = A^n$?

2.1 Mohutnost číselných oborů

Jak ukážeme, že množiny $\mathbb{Z}, \mathbb{Q}$ jsou spočetné? Stačí zkonstruovat bijekci těchto množin na množinu $\mathbb{N}$ (jednoduše řečeno: stačí ukázat, že lze všechny prvky těchto množin očíslovat přirozenými čísly).

$\mathbb{Z}$ je spočetná množina: $0 \mapsto 1$, $1 \mapsto 2$, $-1 \mapsto 3$, $2 \mapsto 4$, $-2 \mapsto 5$, $3 \mapsto 6$, $-3 \mapsto 7$, $4 \mapsto 8$, $-4 \mapsto 9$, ...

Zkonstruovali jsme tedy bijekci mezi množinami $\mathbb{N}$ a $\mathbb{Z}$, mají tedy stejnou mohutnost, tj.

$$|\mathbb{N}| = |\mathbb{Z}| \ .$$

$\mathbb{Q}$ je spočetná množina: stačí ukázat, že množina kladných zlomků je spočetná.

[1] Vlastní podmnožina množiny A – takto se nazývá podmnožina množiny A, která není rovna celé množině A.

$$\begin{array}{llllll}
\frac{1}{1}\,(1) & \frac{1}{2}\,(2) & \frac{1}{3}\,(4) & \frac{1}{4}\,(7) & \frac{1}{5}\,(11) & \frac{1}{6}\,(16) & \ldots \\
\frac{2}{1}\,(3) & \frac{2}{2}\,(5) & \frac{2}{3}\,(8) & \frac{2}{4}\,(12) & \frac{2}{5}\,(17) & \frac{2}{6}\,(23) & \ldots \\
\frac{3}{1}\,(6) & \frac{3}{2}\,(9) & \frac{3}{3}\,(13) & \frac{3}{4}\,(18) & \frac{3}{5}\,(24) & \frac{3}{6}\,(31) & \ldots \\
\frac{4}{1}\,(10) & \frac{4}{2}\,(14) & \frac{4}{3}\,(19) & \frac{4}{4}\,(25) & \frac{4}{5}\,(32) & \frac{4}{6}\,(40) & \ldots \\
\frac{5}{1}\,(15) & \frac{5}{2}\,(20) & \frac{5}{3}\,(26) & \frac{5}{4}\,(33) & \frac{5}{5}\,(41) & \frac{5}{6}\,(50) & \ldots \\
\frac{6}{1}\,(21) & \frac{6}{2}\,(27) & \frac{6}{3}\,(34) & \frac{6}{4}\,(42) & \frac{6}{5}\,(51) & \frac{6}{6}\,(61) & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots
\end{array}$$

Číslování jednotlivých zlomků probíhá ve směru vedlejší diagonály. Je zřejmé, že stejně bychom postupovali u množiny všech uspořádaných dvojic přirozených čísel – její prvky by šlo očíslovat přirozenými čísly stejným způsobem, tj. $|\mathbb{N}| = |\mathbb{N}^2|$.

Pokud bychom chtěli číslovat nejen kladné, ale i záporné zlomky, tak bychom výše uvedený postup snadno modifikovali (podobně jako u číslování celých čísel): $0 \mapsto 1$, $\frac{1}{1} \mapsto 2$, $-\frac{1}{1} \mapsto 3$, $\frac{1}{2} \mapsto 4$, $-\frac{1}{2} \mapsto 5$, $\frac{2}{1} \mapsto 6$, $-\frac{2}{1} \mapsto 7$, $\frac{1}{3} \mapsto 8$, $-\frac{1}{3} \mapsto 9$, ..., tj.

$$|\mathbb{N}| = |\mathbb{Q}| \ .$$

Pro přehled:

$$\aleph_0 = |\mathbb{N}| = |\mathbb{P}| = |3\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| = |\mathbb{A}| \ ,$$

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{A} \subseteq \mathbb{R} \subseteq \mathbb{C} \, .$$

Rozklady $\mathbb{R}$:

$$\mathbb{R} = \mathbb{A} \cup \mathbb{T} \, , \qquad \mathbb{R} = \mathbb{Q} \cup \mathbb{I} \, .$$

Pomocí *Cantorovy diagonální metody* lze dokázat, že množina reálných čísel není spočetná; říkáme, že má *mohutnost kontinua* $\mathfrak{c}$.

$$\mathfrak{c} = |\mathbb{R}| = |\mathbb{C}| = |\mathbb{T}| = |\mathbb{I}| = |\langle 0, 1 \rangle| \ .$$

- $\mathbb{P}$ – množina všech prvočísel,
- $\mathbb{A}$ – čísla algebraická (reálné kořeny polynomů s celočíselnými[2] koeficienty),
- $\mathbb{T}$ – čísla transcendentní (nejsou kořenem polynomu s celočíselnými koeficienty),
- $\mathbb{I}$ – čísla iracionální.

Množiny větší mohutnosti lze zkonstruovat snadno, lze vzít např. potenční množinu[3], tj. systém všech podmnožin dané množiny. Lze ukázat, že má vždy větší mohutnost než původní množina.

[2] Ekvivalentní je požadovat polynomy s racionálními koeficienty. Stačí si představit racionální koeficienty ve tvaru zlomků a vynásobit tento polynom nejmenším společným násobkem jmenovatelů.

[3] Kolik podmnožin má dvouprvková množina? A kolik podmnožin má tříprvková množina? Je třeba zahrnout i prázdnou množinu i celou samotnou množinu. Potenční množinu množiny A značíme $P(A)$ nebo 2^A. Proč?

2.2 Mohutnost $\mathbb{R}$ – zajímavosti

- 29. listopadu 1873 napsal Georg Cantor Richardu Dedekindovi dopis:

  Rád bych Vám položil otázku, která má pro mne jistý teoretický význam, nemohu však na ni nalézt odpověď. Možná na ni můžete odpovědět a byl byste tak laskav a napsal mi o ní. Zní takto: mějme množinu všech přirozených čísel n a označme ji $\mathbb{N}$. Uvažujme dále množinu všech kladných reálných čísel x a označme ji $\mathbb{R}$. Otázka potom zní: lze $\mathbb{N}$ spárovat s $\mathbb{R}$ tak, že každému prvku jedné množiny odpovídá právě jeden prvek druhé množiny? Na první pohled si člověk řekne: „Ne, to možné není, neboť $\mathbb{N}$ sestává z diskrétních prvků a $\mathbb{R}$ je kontinuum.“ Tento argument však nic nedokazuje. A i když tuším, že $\mathbb{N}$ a $\mathbb{R}$ takto spárovat nelze, stále nemohu najít důvod. A to mě trápí; možná je to velmi jednoduché.

- Již 7. prosince 1873 napsal Georg Cantor Richardu Dedekindovi další dopis:

  Nedávno jsem měl čas rozpracovat trochu podrobněji hypotézu, o níž jsem se Vám zmínil; až dnes jsem přesvědčen, že jsem tuto záležitost dokončil. Kdybych se mýlil, nenašel bych shovívavějšího soudce než Vás. Dovoluji si Vám tedy předložit k posouzení to, co jsem napsal, v celé neúplnosti prvního návrhu.

- G. Cantor ukázal, že neexistuje bijekce mezi množinami $\mathbb{N}$ a $\mathbb{R}$. 7. prosince 1873 se tedy zrodila teorie množin...

- G. Cantor předložil dokonce dva důkazy nespočetnosti $\mathbb{R}$, druhý z nich je slavnou *Cantorovou diagonální metodou*.

- Množina reálných čísel v otevřeném intervalu $(0, 1)$ se stala první nekonečnou množinou, o níž bylo dokázáno, že je „početnější“ než $\mathbb{N}$, tedy že má větší mohutnost (neboli že je nespočetná).

- **Důkaz** bychom mohli provést také takto (opět sporem):

  Předpokládejme, že body otevřeného intervalu $(0, 1)$ lze seřadit do posloupnosti a_1, a_2, a_3, ...
  Pokryjme a_1 intervalem délky $\frac{1}{10}$, a_2 intervalem délky $\frac{1}{10^2}$, a_3 intervalem délky $\frac{1}{10^3}$, ...
  Všechny prvky intervalu $(0, 1)$ jsou tedy těmito intervaly pokryty, je tedy pokryt (připouští se jejich překrývání) celý interval $(0, 1)$. Jenže:

  – délka intervalu $(0, 1)$ je 1,

  – součet délek interválků, které jej pokrývají, je však ostře menší:

$$\frac{1}{10} + \frac{1}{10^2} + \frac{1}{10^3} + ... = \frac{\frac{1}{10}}{1 - \frac{1}{10}} = \frac{1}{9} \;<\; |(0, 1)| = 1\,.$$

  Dostáváme tak spor; body otevřeného intervalu $(0, 1)$ tedy nelze seřadit do posloupnosti.

Hypotéza kontinua

Vzniká otázka, zda mezi mohutností množiny přirozených čísel ($\aleph_0$) a mezi mohutností množiny reálných čísel (mohutnost kontinua $\mathfrak{c}$) existuje ještě nějaká další mohutnost.

- 1882 zformuloval Georg Cantor hypotézu, že žádná taková mohutnost neexistuje; této hypotéze se říká *hypotéza kontinua*.

- 1940 dokázal Kurt Gödel, že tuto hypotézu nelze v rámci teorie množin vyvrátit.

- 1963 dokázal Paul Cohen, že tuto hypotézu nelze v rámci teorie množin dokázat.

Hypotéza kontinua je tedy na axiomech teorie množin (Zermelo-Fraenkelův systém axiómů) ***nezávislá***.

Formulace hypotézy kontinua

Existuje celá řada ekvivalentních formulací hypotézy kontinua.

- Mohutnost množiny všech reálných čísel (tj. *mohutnost kontinua*) je nejmenší nespočetnou mohutností.
- $2^{\aleph_0} = \aleph_1$

3 Algebraické struktury

3.1 Algebraické struktury s jednou binární operací

1. * Ukažte, že algebraické struktury $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ jsou komutativní grupy.

   [není třeba to podrobně rozepisovat, stačí si uvědomit splnění jednotlivých axiómů]

2. * Rozhodněte, zda následující množiny s předepsanou operací tvoří komutativní grupu. Opět není potřeba to podrobně rozepisovat, stačí si splnění jednotlivých axiómů uvědomit.

   $$(\mathbb{Z}, \cdot) \qquad (\mathbb{Q}, \cdot) \qquad (\mathbb{Q} \setminus \{0\}, \cdot) \qquad (\mathbb{R} \setminus \{0\}, \cdot) \qquad (\mathbb{C} \setminus \{0\}, \cdot)$$

   [$\mathbb{Z}$ ne (inv. prvky), $\mathbb{Q}$ ne (inv. prvek k 0), ostatní ano]

3. * Rozhodněte, zda množina $\mathbb{R}^3 = \{(a, b, c);\, a, b, c \in \mathbb{R}\}$ všech uspořádaných trojic reálných čísel s operací sčítání trojic po složkách, tj.

   $$\forall a, b, c, d, e, f \in \mathbb{R} \quad \text{definujeme} \quad (a, b, c) + (d, e, f) = (a + d, b + e, c + f),$$

   tvoří komutativní grupu.

   [ano, tvoří komutativní grupu, obecně $(\mathbb{R}^n, +)$ tvoří kom. grupu]

4. * Rozhodněte, jakou algebraickou strukturu tvoří $(G, \circ)$.

   a) $G = \mathbb{Z}$, $a \circ b = a + 2b$
   b) $G = \mathbb{Q}$, $a \circ b = a + b + 1$
   c) $G = \mathbb{R}^+$, $a \circ b = \ln(a \cdot b)$
   d) $G = \mathbb{Z}$, $a \circ b = (a - b)^2$
   e) $G = \{u + v\sqrt{3}; u, v \in \mathbb{Z}\}$, $a \circ b = a + b$
   f) $G = \{u + v\sqrt{3}; u, v \in \mathbb{Z}\}$, $a \circ b = a \cdot b$
   g) $G = 4\mathbb{Z} = \{4n; n \in \mathbb{Z}\}$, $a \circ b = a + b$

[a) grupoid, b) kom. grupa ($n = -1$), c) $\circ$ není operace na $\mathbb{R}^+$ ($a = b = \frac{1}{2}$)]

[d) kom. grupoid, e) kom. grupa, f) kom.monoid (inv. prvek k 0), g) kom. grupa]

5. * Rozhodněte, zda množina všech
   a) posunutí v rovině;
   b) otočení v rovině kolem jednoho pevně daného bodu S;
   společně s operací skládání tvoří grupu. V kladném případě rozhodněte, zda je tato grupa komutativní.

   [a) kom. grupa, b) kom. grupa]

Názvy prvků v algebraických strukturách:

obecně:	neutrální prvek n,	inverzní prvek a^{-1}
aditivně:	nulový prvek 0 či o,	opačný prvek $-a$
multiplikativně:	jednotkový prvek 1 či e,	inverzní prvek a^{-1}

3.2 Algebraické struktury se dvěma binárními operacemi

1. Nahlédněte do učebnice *Lineární algebra.* a zopakujte si definici *tělesa* (def. 2.1 na str. 18), *pole* (neboli komutativního tělesa) a definici *grupy* (def. 5.1a a 5.1b na str. 45).
   Dále si zopakujte definici *okruhu* (def. 3.1 na str. 27) a *oboru integrity* (def. 3.2 na str. 28).

2. * Rozhodněte, o jakou algebraickou strukturu se jedná.
   a) $(\mathbb{N}, +, \cdot)$ b) $(\mathbb{Z}, +, \cdot)$ c) $(\mathbb{Q}, +, \cdot)$ d) $(\mathbb{R}, +, \cdot)$ e) $(\mathbb{C}, +, \cdot)$ f) $(\mathbb{Z}_p, +, \cdot)$, $p \in \mathbb{P}$
   g) $(\mathbb{Z}_n, +, \cdot)$, $n \in \mathbb{N} \setminus \mathbb{P}$, $n > 1$

   [a) není ani okruh (chybí nulový prvek a opačné prvky), b) kom. okruh s jednotkovým prvkem, dokonce obor integrity, c) pole, d) pole, e) pole, f) pole, g) kom. okruh s jednotkovým prvkem]

3. * Ukažte, že každé pole je automaticky také oborem integrity.

   [Pole a obor integrity mají společné všechny axiomy kromě jediného: axiom existence inverzních prvků u pole je u oboru integrity nahrazen axiomem neexistence netriviálních dělitelů nuly. Stačí tedy ukázat, že v poli nemohou existovat netriviální dělitelé nuly. (využijte existence inverzních prvků)]

4. * Rozhodněte, zda je $(\mathbb{Z}[x], +, \cdot)$ (polynomy s celočíselnými koeficienty) oborem integrity.
   Podobně rozhodněte (není třeba rozepisovat, stačí si to uvědomit), zda jsou struktury $(\mathbb{Q}[x], +, \cdot)$, $(\mathbb{R}[x], +, \cdot)$, $(\mathbb{C}[x], +, \cdot)$ oborem integrity.

4 Zobrazení, funkce

4.1 Terminologie

1. Zopakujte si definici zobrazení. Čerpejte ze střední školy i z matematické analýzy.

   - Říkáme, že relace[4] $f \subseteq A \times B$ je zobrazením z množiny A do množiny B, je-li

     $$\forall x \in A\ \forall y_1, y_2 \in B\colon \quad (x, y_1) \in f \wedge (x, y_2) \in f \implies y_1 = y_2\,.$$

     Je-li f zobrazení, píšeme zpravidla místo $(x, y) \in f$ stručnější a názornější $y = f(x)$. Tento zápis je možný, neboť y je daným $x \in D_f$ určeno jednoznačně; u relace tomu tak být nemusí, proto je tento zápis vyhrazen pouze zobrazením a funkcím.

     Definičním oborem rozumíme množinu $D_f = \{x \in A\colon \exists y \in B\colon (x, y) \in f\}$.
     Oborem hodnot rozumíme množinu $H_f = \{y \in B\colon \exists x \in A\colon (x, y) \in f\}$.
     Všimněme si, že pomocí stručné notace lze psát $H_f = \{f(x)\colon x \in D_f\}$.
   - Říkáme, že relace $f \subseteq A \times B$ je zobrazením množiny A do množiny B, jestliže

     $$\forall x \in A\ \exists!\, y \in B;\ (x, y) \in f.$$

     Definičním oborem je v tomto případě přímo množina A. Je-li f zobrazení množiny A do množiny B, můžeme tento fakt stručně zapisovat takto: $f\colon A \to B$.

     Pokud by takové y existovalo nejvýše jedno (nikoli tedy nutně právě jedno), tak bychom obdrželi definici zobrazení z A do B.

2. Terminologická perlička – všimněme si, že se rozlišuje:

   - Zobrazení *množiny* A do množiny B: zde se zobrazuje každý prvek množiny A. Definice definičního oboru je v tomto případě snadná: je to samotná množina A.
     Zápis $A \to B$ označuje právě zobrazení množiny A do množiny B.
   - Zobrazení *z množiny* A do množiny B: zde se zobrazuje ne nutně každý prvek množiny A.

   Proč ta dvojznačnost, tj. proč nedefinujeme např. pouze zobrazení množiny A do množiny B? Tento přístup je oblíbený na SŠ, definice D_f je velmi jednoduchá, také některé další formulace mohou vypadat přehledněji.

   Ale: hovoří se například o reálných funkcích (jejich obor hodnot je neprázdnou podmnožinou[5] množiny $\mathbb{R}$) jedné reálné proměnné (jejich definiční obor je neprázdnou podmnožinou $\mathbb{R}$),[6]

[4] Relace budeme definovat později. Můžeme si je však snadno představit už teď: binární relací f z množiny A do množiny B rozumíme libovolnou množinu uspořádaných dvojic, jejichž první složku tvoří prvek množiny A a druhou složku tvoří prvek množiny B.
Je-li $A = \{a_1, a_2\}$, $B = \{b_1, b_2, b_3\}$, pak jsou příklady binárních relací z množiny A do množiny B třeba takovéto množiny uspořádaných dvojic: $\{(a_2, b_1)\}$, $\{(a_2, b_1), (a_2, b_2), (a_2, b_3)\}$, $\{(a_1, b_3), (a_3, b_2)\}$.

[5] Rozumíme tím podmnožinu vlastní či nevlastní. Říkáme, že množina A je *vlastní podmnožinou* množiny M, je-li její podmnožinou (tj. $A \subseteq M$), zároveň je však různá od samotné M (tj. $A \neq M$); píšeme $A \subset M$, případně výrazněji $A \subsetneq M$ (o obou těchto zápisech hovoříme jako o ostré inkluzi).
Říkáme, že množina A je *nevlastní podmnožinou* množiny M, je-li její podmnožinou; píšeme $A \subseteq M$. Jinými slovy: množina A je *nevlastní podmnožinou* (většinou říkáme jen *je podmnožinou*) množiny M, je-li buď $A = M$, nebo $A \subset M$.

[6] Jedná se tedy o funkce, jejichž definiční obor je buď celé $\mathbb{R}$, nebo jakákoli neprázdná podmnožina $\mathbb{R}$ a obor hodnot je buď celé $\mathbb{R}$, nebo jakákoli neprázdná podmnožina $\mathbb{R}$.

stručně o funkcích „z $\mathbb{R}$ do $\mathbb{R}$“. Není tedy nutné, aby byl definiční obor roven celé množině $\mathbb{R}$ (např. $y = \frac{1}{x}$), nebo obor hodnot roven celé množině $\mathbb{R}$ (např. $y = \sin x$).

3. Pozor: z definice zobrazení množiny A do množiny B plyne, že součástí zadání takového zobrazení (a samozřejmě i funkce) je množina, na níž je toto zobrazení definováno. Například $y = \frac{1}{x}$ na intervalu $(0, +\infty)$ a $y = \frac{1}{x}$ na množině $\mathbb{R} \setminus \{0\}$ jsou různé funkce.

   V této souvislosti také upozorněme na problémy, které přináší „definice“ zobrazení (či funkce) jako nějakého *předpisu*, např.:

   - samotný předpis nestačí, je nutno zadat množinu, na níž tento předpis budeme uvažovat;
   - funkce mohou být zadány i jinak, nejen nějakým předpisem (např. tabulkou hodnot).

4. * V této souvislosti uvažte, co znamená formulace, která se objevuje v některých sbírkách úloh: *Určete definiční obor následujících funkcí...* Pokuste se navrhnout lepší formulaci.

5. Jaký je rozdíl mezi funkcí a zobrazením?

   - Předně: funkce je speciálním případem zobrazení, každá funkce je tedy zobrazením.

     Funkcí zpravidla nazýváme takové zobrazení,
     jehož obor hodnot je podmnožinou nějaké číselné množiny.

   - Proč jsou zobrazení, jejichž hodnoty jsou čísla, tak důležitá? *Lze s nimi počítat.* Např. součet funkcí f a g (na neprázdném průniku jejich definičních oborů) je definován pomocí součtu funkčních hodnot (tj. pomocí součtu obrazů):

     $$(f + g)(x) := f(x) + g(x).$$

     Jelikož jsou obrazy čísla, je definován jejich součet (a další operace s nimi).

     Počítat lze i s jinými objekty, než jen s čísly. Hovoříme tedy také např. o vektorových funkcích (obrazy jsou vektory), maticových funkcích (obrazy jsou matice) a podobně.

4.2 Vlastnosti zobrazení

1. Zopakujte si definici injekce, surjekce, bijekce.

   Říkáme, že zobrazení f z množiny A do množiny B je:

   - injektivní (prosté), je-li $\forall x_1, x_2 \in D_f\colon \quad x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$;
   - surjektivní (zobrazením na množinu B), jestliže $\forall y \in B\ \exists x \in A;\ y = f(x)$;
   - bijektivní (vzájemně jednoznačné), je-li zároveň injektivní a surjektivní.

2. Alternativní charakterizace:

   - Jednoduchá charakterizace injekce: také f^{-1} je zobrazení.
   - Injekci lze definovat i takto (viz obměněná implikace: $(A \implies B) \iff (\neg B \implies \neg A)$):

     $$\forall x_1, x_2 \in D_f\colon \quad f(x_1) = f(x_2) \implies x_1 = x_2\,.$$

   - Jednoduchá charakterizace surjekce: $H_f = B$.

3. * Rozmyslete si, že pro každá dvě zobrazení $f : A \to B$ a $g : B \to C$ platí:

- Je-li složení zobrazení $g \circ f$ (vlastně to znamená $g(f)$) injektivní, pak je f injektivní.
- Je-li $g \circ f$ surjektivní (tj. zobrazení *na*), pak je g surjektivní.

[návod: nakreslete si množiny A, B, C s několika prvky a pozorujte obrázek]

Rozklad zobrazení na surjekci a injekci

1. * Rozložte následující funkce na surjekci a injekci.
   a) $y = x^2$ na $\mathbb{R}$, b) $y = \operatorname{sgn} x$ na $\mathbb{R}$, c) $y = \dfrac{1}{x}$ na $\mathbb{R}\setminus\{0\}$, d) $y = \operatorname{tg} x$ na $\mathbb{R}\setminus\{\frac{\pi}{2}+k\pi, k \in \mathbb{Z}\}$

5 Binární relace

Definice: Množina $R \subseteq A \times B$ se nazývá binární relací z množiny A do množiny B.
Je-li $A = B$, říkáme, že R je (binární) relací v množině A.
Jednotkovou (binární) relací v množině A rozumíme relaci $E(A) = \{(a, a) \colon a \in A\}$.
Poznamenejme, že i prázdná množina může být relací.

1. * Zapište relaci „=“ na množině $\mathbb{N}$ jako množinu uspořádaných dvojic. Rozhodněte, zda se nějak liší od jednotkové relace $E(\mathbb{N})$ a nakreslete její graf.
2. * Zapište relaci „$\leq$“ na množině $\mathbb{N}$ jako množinu uspořádaných dvojic. Nakreslete její graf.
3. * Máme-li zakreslen graf relace $R \subseteq A \times B$, kde A, B jsou číselné množiny, jak potom získáme graf relace R^{-1} k ní inverzní?

Definice: Binární relace R v množině A (tj. $R \subseteq A \times A$) se nazývá:

- *reflexivní*, jestliže $\forall x \in A$: $\quad xRx$
- *symetrická*, jestliže $\forall x, y \in A$: $\quad xRy \implies yRx$
- *tranzitivní*, jestliže $\forall x, y, z \in A$: $\quad xRy \wedge yRz \implies xRz$
- *antisymetrická*, jestliže $\forall x, y \in A$: $\quad xRy \wedge yRx \implies x = y$
- *antireflexivní*, jestliže $\forall x \in A$: $\quad \neg\,(xRx)$

Říkáme, že relace R v množině A je *relací ekvivalence*, je-li reflexivní, symetrická a tranzitivní.

Říkáme, že relace R v množině A je *(částečným) uspořádáním*, je-li reflexivní, antisymetrická a tranzitivní. Ještě můžeme rozlišovat ostré a neostré uspořádání:

- *neostré uspořádání* – tak se nazývá relace, která je reflexivní, antisymetrická a tranzitivní;
- *ostré uspořádání* – tak se nazývá relace, která je antireflexivní, antisymetrická a tranzitivní.

Je-li v množině A dána relace uspořádání R, pak uspořádanou dvojici (A, R) nazýváme uspořádanou množinou.

Není těžké si rozmyslet, že relace $R \subseteq A \times A$ je:

- reflexivní $\iff$ $E(A) \subseteq R$,
- symetrická $\iff$ $R \subseteq R^{-1}$ $\iff$ $R = R^{-1}$

Rozklady množiny

1. * Provokace: uvažujme dvouprvkovou množinu $M_2 = \{a, b\}$. Kolik rozkladů je možno vytvořit? Dva: $M_2 = \{a, b\}$ a $M_2 = \{a\} \cup \{b\}$.
   U tříprvkové množiny $M_3 = \{a, b, c\}$ je rozkladů už pět:

   $M_3 = \{a, b, c\}$ $M_3 = \{a, b\} \cup \{c\}$ $M_3 = \{a, c\} \cup \{b\}$ $M_3 = \{b, c\} \cup \{a\}$ $M_3 = \{a\} \cup \{b\} \cup \{c\}$

   Kolik jich má čtyřprvková množina $M_4 = \{a, b, c, d\}$? [15]

2. A pro labužníky: lze to nějak rozumně zobecnit na M_n? Ano. Označme $b(n)$ počet všech rozkladů n-prvkové množiny M_n. Ukažte, že

$$b(n+1) = 1 + \binom{n}{1} b(1) + \binom{n}{2} b(2) + \binom{n}{3} b(3) + \cdots + \binom{n}{n} b(n)\,.$$

   [vypište si jednotlivé možnosti, seřaďte je do vhodných skupinek]

3. Terminologická perlička 1: číslům $b(n)$ říkáme Bellova čísla. Podaří se Vám pomocí Pythonu najít $b(4), b(5), b(6)$?
   [$b(0) = 1$, $b(1) = 1$, $b(2) = 2$, $b(3) = 5$, $b(4) = 15$, $b(5) = 52$, $b(6) = 203$, $b(7) = 877$, $b(8) = 4\,140$, $b(9) = 21\,147$, ...]

4. Bellova čísla: viz též [BeDla], str. 31. Na str. 32 je vypsáno několik prvních členů Bellovy posloupnosti; poslední z nich je 5 832 742 205 057. Jakou hodnotu má člen po něm bezprostředně následující? Podaří se Vám to zjistit pomocí Pythonu?

5. Terminologická perlička 2: rozklad množiny M indukovaný relací ekvivalence $\sim$ se též nazývá *faktorová množina* množiny M podle ekvivalence $\sim$, píšeme $A/\!\sim$.

Ekvivalence

1. Všimněme si, že počítání modulo n je vlastně počítání s třídami ekvivalence. Množinu celých čísel rozloží relace ekvivalence „mít stejný zbytek po dělení 5“ na právě n tříd, stručně je označujeme postupně $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \ldots, \overline{n-1}$, nebo ještě stručněji jen pomocí jejich reprezentantů: $0, 1, 2, 3, \ldots, n-1$. Je třeba si uvědomit, že např. 0 není číslem nula, ale třídou obsahující násobky čísla n, tj. množinou $\{k \cdot n, k \in \mathbb{Z}\}$, značíme ji buď $n\mathbb{Z}$, nebo $\overline{0}$; podobně
   - 1 není číslem jedna, ale třídou $\{1 + k \cdot n, k \in \mathbb{Z}\}$, značíme ji $1 + n\mathbb{Z}$, nebo $\overline{1}$,
   - 2 není číslem dva, ale třídou $\{2 + k \cdot n, k \in \mathbb{Z}\}$, značíme ji $2 + n\mathbb{Z}$, nebo $\overline{2}$,
   - ...,

- $n-1$ není číslem $n-1$, ale třídou $\{(n-1)+k\cdot n, k\in\mathbb{Z}\}$, značíme ji $(n-1)+n\mathbb{Z}$, nebo také $\overline{n-1}$.

2. * Na semináři jsme uváděli několik příkladů relací ekvivalence, které se týkaly školské matematiky. Najdete nějaké další příklady? Např.:
   - jaký je vztah mezi orientovanou úsečkou a vektorem,
   - jaký je vztah mezi zlomky $\frac{2}{3}, \frac{4}{6}, \frac{6}{9}, \frac{8}{12}, \ldots$

3. * Filoména ráda popisuje okolní svět pomocí matematiky. Tentokrát si vzala na paškál své čtyři spolužáky: Pepíčka, Máničku, Celestýna a Andělína. Všimla si, že někteří z nich si spolu povídají natolik, že novinku stačí říci jen jednomu z nich a brzy o tom ví i ten druhý. Situace se má takto: Celestýn si hodně povídá s Máničkou; Andělín si hodně povídá s Pepíčkem. Filoména tedy definovala množinu $M=\{P,M,C,A\}$ a její prvky uspořádala do podmnožin $M_1=\{C,M\}$ a $M_2=\{A,P\}$.
   Rozhodněte, zda tímto Filoména definovala na množině M svých spolužáků relaci ekvivalence.

Částečné uspořádání

1. Pro připomenutí: Binární relace na množině M, která je reflexivní, antisymetrická a tranzitivní, se nazývá *částečné uspořádání* na množině M (někdy jen stručně *uspořádání* na množině M).

   Částečně uspořádanou množinou rozumíme dvojici $(M,\preceq)$, kde M je množina a $\preceq$ je částečné uspořádání na této množině. Často stručně hovoříme jen o *uspořádané množině* tj. příslovce „částečně“ vynecháváme.

   Je-li částečné uspořádání $\preceq$ na M navíc *dichotomické*, tj.

   $$\forall\, a,b\in M:\quad a\preceq b\ \vee\ b\preceq a\,,$$

   říkáme, že je toto uspořádání *úplné* (nebo také *lineární*).

   Všimněme si, že dichotomie je vlastně podmínkou vyjadřující požadavek, že každé dva prvky jsou *porovnatelné*. Odtud také plyne název tohoto uspořádání: „úplné“.

2. * Uvažujme systém $\mathcal{P}(M)$ všech podmnožin[7] neprázdné konečné množiny M. Určete, jakou má potenční množina $\mathcal{P}(M)$ mohutnost. [*Návod: sečtěte vhodná kombinační čísla...*]

3. * Ukažte, že je-li M neprázdná konečná množina, potom je relace $\subseteq$ na $\mathcal{P}(M)$ částečným uspořádáním.
   Je nutný předpoklad, aby množina M byla: a) neprázdná; b) konečná?

   [*Ověříme R, A, T, případně i ukážeme, že usp. není úplné: $M=\{a,b\}$, $\{a\}$ a $\{b\}$ jsou neporovnatelné, neboť neplatí $\{a\}\subseteq\{b\}$ ani $\{b\}\subseteq\{a\}$.*]

4. **Definice:** Říkáme, že prvek $a\in M$ uspořádané množiny $(M,\leq)$ je

   - největší, pokud je $\forall b\in M$: $b\leq a$,
   - nejmenší, pokud je $\forall b\in M$: $a\leq b$,
   - maximální, pokud neexistuje žádné $b\in M$ takové, že $a<b$,
   - minimální, pokud neexistuje žádné $b\in M$ takové, že $b<a$.

[7] Tzv. *potenční množina*.

5. * Znázorněte svaz všech dělitelů čísla 200 pomocí Hasseova diagramu.

6. * Znázorněte svaz všech dělitelů čísla 360 pomocí Hasseova diagramu.

   [*Rovnoběžnostěn..., prvočísla z rozkladu jsou totiž tři:* $2, 3, 5$.]

7. * Rozhodněte, zda množina s danou relací je uspořádána částečně či lineárně.

   $$(\mathbb{N}, \leq) \quad (\mathbb{R}, \leq) \quad (\mathbb{N}, |) \quad (\mathbb{N} \setminus \{1\}, |)$$

   Relace $|$ je na $\mathbb{Z}$ definována takto: říkáme, že a dělí b, píšeme $a|b$, existuje-li $q \in \mathbb{Z}$ takové, že $b = q \cdot a$.
   Ve všech případech najděte, pokud existují, největší a nejmenší prvky i minimální a maximální prvky.

   [$(\mathbb{N}, \leq)$ *lineárně, min.=nejm.=1, max. a nejv. neex.;* $(\mathbb{R}, \leq)$ *lineárně, min., nejm., max. a nejv.: neex.;* $(\mathbb{N}, |)$ *částečně, min.=nejm.=1, max. a nejv. neex.;* $(\mathbb{N}\setminus\{1\}, |)$ *částečně, min.: všechna prvočísla, nejm. neex, max. a nejv. neex.*]

8. * Je množina všech uspořádaných trojic přirozených čísel uspořádána lexikografickým uspořádáním úplně, nebo pouze částečně?

   [*úplně*]

9. * Kratičce zapřemýšlejte: lze nějak rozumně definovat standardní úplné uspořádání na $\mathbb{C}$ (analogické úplnému uspořádání množiny $\mathbb{R}$)? Zvažte například, co by byly kladné prvky ($1-i$, nebo $i-1$?), či které komplexní číslo by bylo větší: $1-i$, nebo $i-1$?

6 Permutace

Kompletní teorie k tématu permutace je v knize Bečvář J.: *Lineární algebra* na stranách 51 – 60.

1. K dané permutaci P určete permutaci P^{-1}.

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 9 & 8 & 6 & 5 & 7 & 2 & 1 & 4 \end{pmatrix}$$

   Jak na to? Stačí zaměnit obrazy za vzory, tj. zaměnit první a druhý řádek:

$$P^{-1} = \begin{pmatrix} 3 & 9 & 8 & 6 & 5 & 7 & 2 & 1 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}.$$

   A je dobrým zvykem vše uspořádat:

$$P^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 7 & 1 & 9 & 5 & 4 & 6 & 3 & 2 \end{pmatrix}.$$

2. * Skládání zobrazení obecně není komutativní. Stejně tak je tomu se skládáním permutací. Vypočtěte $P \circ Q$ a $Q \circ P$.

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \qquad Q = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

3. * Určete počet inverzí dané permutace a její znaménko a určete permutaci k ní inverzní.

   a)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 1 & 4 & 5 & 8 & 3 & 9 & 6 & 7 \end{pmatrix}$$

   [Počet inverzí: $\operatorname{in} P = 8$, znaménko: $\operatorname{sgn} P = (-1)^8 = 1$, sudá permutace.]

   b)

$$Q = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 7 & 1 & 9 & 5 & 4 & 6 & 3 & 2 \end{pmatrix}$$

   [Počet inverzí: $\operatorname{in} P = 26$, znaménko: $\operatorname{sgn} P = (-1)^{26} = 1$, sudá permutace.]

4. * Rozložte permutaci P na nezávislé cykly.

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 1 & 9 & 8 & 2 & 4 & 6 & 7 \end{pmatrix}$$

5. * Najděte permutaci P^{-1}.

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 1 & 9 & 8 & 2 & 4 & 6 & 7 \end{pmatrix}$$

6. * Cyklus $(2, 4, 3, 5)$ zapište jako permutaci (dvouřádková notace). Je zřejmé, že obrazem 1 bude 1. Tuto permutaci umocněte na druhou (tj. vypočtěte $P^2 = P \circ P$) a na třetí (tj. vypočtěte $P^3 = P \circ P \circ P$). Obě permutace P^2 i P^3 rozložte na nezávislé cykly. Jak se tyto cykly liší?

7. * Všimněme si: každý cyklus lze zapsat pouze pomocí transpozic. Například:

$$(1, 3, 2, 7, 5) = (1, 5)(1, 7)(1, 2)(1, 3).$$

   Ověřte, že tato rovnost skutečně platí; postupujte tak, že transpozice na pravé straně složíte.

   Obecně:

$$(a_1, a_2, a_3, \ldots, a_{r-1}, a_r) = (a_1, a_r)(a_1, a_{r-1}) \ldots (a_1, a_4)(a_1, a_3)(a_1, a_2).$$

   Umíme-li rozložit na transpozice každý cyklus, můžeme rozložit na transpozice každou permutaci: stačí tuto permutaci rozložit na nezávislé cykly a každý z těchto cyklů rozložit na transpozice.

8. * Určete počet inverzí dané permutace a její znaménko, rozložte ji na nezávislé cykly, určete její znaménko, rozložte ji na transpozice, určete permutaci k ní inverzní.

   a)

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 9 & 8 & 6 & 5 & 7 & 2 & 1 & 4 \end{pmatrix}$$

   [Počet inverzí: $\operatorname{in} P = 26$, znaménko: $\operatorname{sgn} P = (-1)^{26} = 1$, rozklad na nezávislé cykly: $(1, 3, 8)(2, 9, 4, 6, 7)(5)$, rozklad na transpozice: $(1, 8)(1, 3)(2, 7)(2, 6)(2, 4)(2, 9)$.]

   b)

$$Q = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 7 & 1 & 9 & 5 & 4 & 6 & 3 & 2 \end{pmatrix}$$

   [Počet inverzí: $\operatorname{in} P = 26$, znaménko: $\operatorname{sgn} P = (-1)^{26} = 1$, rozklad na nezávislé cykly: $(1, 8, 3)(2, 7, 6, 4, 9)(5)$.]

   c)

$$R = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 7 & 8 & 9 & 4 & 3 & 2 & 1 & 5 \end{pmatrix}$$

   [Počet inverzí: $\operatorname{in} P = 26$, znaménko: $\operatorname{sgn} P = (-1)^{26} = 1$, rozklad na nezávislé cykly: $(1, 6, 3, 8)(2, 7)(4, 9, 5)$.]

9. * Určete počet inverzí dané permutace a její znaménko, rozložte ji na nezávislé cykly, umocněte ji na 11, určete její znaménko, rozložte ji na transpozice, určete permutaci k ní inverzní.

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 1 & 7 & 2 & 4 & 3 & 6 & 9 & 10 & 8 \end{pmatrix}$$

[Počet inverzí: $\operatorname{in} P = 11$, znaménko: $\operatorname{sgn} P = (-1)^{11} = -1$, rozklad na nezávislé cykly: $(1,5,4,2)(3,7,6)(8,9,10)$, tj. $\operatorname{sgn} P = (-1)^{10-3} = -1$. $P^{11} = (1,2,4,5)(3,6,7)(8,10,9)$]

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 1 & 5 & 4 & 8 & 9 & 6 & 2 & 10 & 7 \end{pmatrix}$$

[Počet inverzí: $\operatorname{in} P = 13$, znaménko: $\operatorname{sgn} P = (-1)^{13} = -1$, rozklad na nezávislé cykly: $(1,3,5,8,2)(4)(6,9,10,7)$, tj. $\operatorname{sgn} P = (-1)^{10-3} = -1$. $P^{11} = (1,3,5,8,2)(6,7,10,9)$.]

10. * Umocněte permutace z úlohy 8:
    - najděte permutace Q^7 a Q^{47},
    - najděte permutace R^7 a R^{47}.

Umocňování permutací

Pokud by chtěl někdo umocňovat permutace, stačí k tomu následující pozorování:

- Umocnit permutaci P na k-tou znamená složit ji samu se sebou k-krát, tj. např.:

$$P^1 = P, \qquad P^2 = P \cdot P, \qquad P^3 = P \cdot P \cdot P, \qquad P^4 = P \cdot P \cdot P \cdot P, \ldots$$

- Snadno se umocňuje cyklus. Př.: Je-li $C = (1,3,2,5)$, vypočtěte samostatně C^2, C^3, C^4, C^5.
- V předchozím příkladu pozorujme: umocněním cyklu délky k na k-tou dostaneme identickou permutaci.
- Nezávislé cykly jsou skutečně nezávislé: lze je umocňovat zvlášť.

- **Příklad:** Vypočtěte P^{10}, je-li $P = (2,3,7,4)\,(1,6,5)$.
  Návod:

$$P^{10} = \big((2,3,7,4)\,(1,6,5)\big)^{10} = (2,3,7,4)^{10}\,(1,6,5)^{10} =$$
$$(2,3,7,4)^4\,(2,3,7,4)^4\,(2,3,7,4)^2 \quad (1,6,5)^3\,(1,6,5)^3\,(1,6,5)^3\,(1,6,5)^1 =$$
$$\mathrm{id}\cdot\mathrm{id}\cdot(2,3,7,4)^2 \quad \mathrm{id}\cdot\mathrm{id}\cdot\mathrm{id}\cdot(1,6,5) =$$
$$(2,3,7,4)^2\cdot(1,6,5) \;=\; (2,7)(3,4)\cdot(1,6,5)\,.$$

- Vypočtěte P^{123} a P^{2025} pro permutaci P z předchozího příkladu.

Testík

Zopakujte si vše až po permutace (včetně permutací) a vypracujte samostatně následující testík (je na cca 75 minut).

Termín skutečného testíku: 3. prosince 2025

7 Testík I (ukázková verze)

čas: 75 minut

1. * Na jaké výrokové formuli je založen důkaz sporem?

2. * Rozhodněte, zda množina s danou relací je uspořádána částečně či lineárně.

$$(\mathbb{N} \setminus \{1\}, |)$$

   Najděte všechny minimální a maximální prvky, největší a nejmenší prvek (pokud existují).

3. * Rozhodněte, zda je relace *mít stejnou paritu* (sudost, lichost) na množině celých čísel relací ekvivalence.

4. * Ukažte, že pro každou relaci R na množině M platí: $(R^{-1})^{-1} = R$.

5. * Rozhodněte, jakou algebraickou strukturu tvoří $(\mathbb{Q}, \oplus, \odot)$.

$$\forall a, b \in \mathbb{Q}: \quad a \oplus b = a + b - \frac{1}{2}, \qquad a \odot b = a - 2ab + b\,.$$

6. * Rozhodněte, jakou algebraickou strukturu tvoří $(\mathbb{Q} \setminus \{0\}, \circ)$.

$$\forall a, b \in \mathbb{Q} \setminus \{0\}: \quad a \circ b = \frac{1}{a} + \frac{1}{b}\,.$$

7. * Znázorněte svaz všech dělitelů čísla 200.

8. * a) Danou permutaci P rozložte na nezávislé cykly i na transpozice a určete její znaménko. K dané permutaci P určete permutaci P^{-1}.

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 8 & 6 & 4 & 1 & 5 & 3 & 2 \end{pmatrix}$$

   b) Permutaci P z bodu a) umocněte na 2025.

   c) Určete znaménko permutace $Q = (1, 3, 5, 4, 7, 2) \cdot (4, 7, 5) \cdot (6, 2, 7, 8)$.

8 Genetická metoda a přirozená čísla

8.1 Genetická metoda

Ve formálním axiomatickém systému jsou primitivní pojmy specifikovány pouze pomocí vztahů (axiomů), čímž dostaneme soustavu *abstraktních* objektů. Při tomto postupu však nemusí být zřejmé, že je soustava axiomů konzistentní. Je tedy třeba ověřit, zda soustava výchozích objektů není prázdná. To je možno provést konstruktivně.

Dostáváme se tak k další metodě, která je hojně využívána k výstavbě matematických teorií. Upozornil na ni David Hilbert ve svém článku *Über den Zahlbegriff*, Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 8 (1900), 180–184. Jedná se o *genetickou metodu*, která vychází z prvotních přítomných objektů, z nichž se danými procedurami vytvářejí všechny další objekty. Odpadá tak problém jejich existence, neboť za existující objekty se považují právě ty, které lze zkonstruovat.

Na genetickou metodu se můžeme dívat jako na protipól metody axiomatické. Na počátku každé teorie totiž stojí prvotní objekty a jejich vlastnosti. Zatímco v axiomatické metodě vycházíme z vlastností (axiomů), které popisují blíže neurčené objekty, v genetické metodě nejprve vytvoříme objekty pomocí zvolených procedur. Zkonstruované objekty jsou navíc často názornější, než soustava objektů čistě *abstraktních*, tj. určených pouze tím, že vyhovují dané soustavě axiomů.

Pro některé směry (intuicionizmus, konstruktivizmus) se genetická metoda stala základní metodou. Při budování matematické teorie pak nemusíme na začátku předpokládat existenci jisté dané množiny objektů, které vyhovují daným podmínkám (axiomům).

Myslím, že budování některých matematických teorií genetickou metodou může být inspirací i pro vyučování matematice. Považuji za příjemnější si objekty svého zkoumání sestrojit, než je mít určeny zdánlivě arbitrární soustavou podmínek. Navíc je také lépe patrné, jakými objekty byly tyto podmínky inspirovány; zajímavé je také sledovat samotný postup formalizace objektů. Po získání zkušeností v dané teorii je pak snazší přejít k její formalizaci axiomatickou metodou.

8.2 Zavedení přirozených čísel

Ilustrujme použití genetické metody na známém postupu zavedení přirozených čísel. Mějme jeden prvotní objekt, označme jej například 0, a proceduru $'$, která z každého objektu n vytvoří (jeden) další objekt n' (jeho následníka). Dostáváme tak objekty:

$$0, \quad 0', \quad 0'', \quad 0''', \quad 0'''', \quad 0''''', \quad \ldots$$

Tento postup můžeme shrnout do tří kroků:

1. 0 je přirozené číslo.
2. Je-li n přirozené číslo, pak také n' je přirozené číslo.
3. Přirozenými čísly jsou pouze objekty vytvořené v krocích 1 a 2.

V této induktivní definici ještě chybí explicitní vyjádření předpokladu různosti objektů, které byly vytvořeny různými způsoby. V každém kroku totiž chceme vygenerovat nový prvek. Induktivně tak zavedeme nový predikát $=$ pomocí následujících podmínek.

4. Pro každé přirozené číslo n platí, že $n' \neq 0$.
5. Pro každá přirozená čísla m, n platí $m' = n'$ právě tehdy, když $m = n$.

Vidíme, jak se opakováním základní procedury $'$ vytvářejí z prvotního objektu všechny další objekty. Tyto objekty bychom však vytvářeli zbytečně, kdybychom neměli možnost o nich získávat pravdivá tvrzení. K tomu nám poslouží zavedení dalších predikátů a zejména operací. Predikát $<$ lze zavést snadno: procedurou $'$ je přirozeně dáno uspořádání přirozených čísel. Operaci $+$ zavedeme pomocí rekurze:

a) $n + 0 = n$ pro každé přirozené číslo n,

b) $(n + m)' = n + m'$ pro každá dvě přirozená čísla m, n.

Nyní již lze dokázat komutativitu a asociativitu sčítání, zavést pomocí rekurze násobení (existuje jediná operace na $\mathbb{N}$ taková, že pro každá dvě $m, n \in \mathbb{N}$ platí: $n \cdot 0 = 0$, $n \cdot m' = n \cdot m + n$), dokázat asociativitu, komutativitu a distributivitu násobení, a následně odvozovat všechny podstatné věty aritmetiky přirozených čísel.

V konstrukci je také možno pokračovat, čímž vzniknou postupně čísla celá, racionální, reálná, komplexní. Významným a všeobecně uznávaným konstitutivním prvkem je zde *princip permanentnosti*[8], kdy při rozšiřování nějakého pojmu a při zobecňování požadujeme zachování co nejvíce vlastností původních objektů. Například při rozšiřování pojmu čísla vycházíme z požadavku zachování vlastností sčítání a násobení (komutativní, asociativní a distributivní zákon). Tyto vlastnosti jsou pak fixovány v axiomech komutativního tělesa (pole).

8.3 Poznámky k zavedení přirozených čísel

1. a) Uvažujme prvotní objekt 0 a vytvořeného následníka $0'$: v momentě, kdy příslušnou teorii teprve vytváříme, nemáme k dispozici numerační soustavu (způsob zápisu čísel, např. poziční desítkovou soustavu). Prvotní objekt sice (pro názornost) zpravidla nazýváme nulou (a o $0'$ pak budeme nejspíše hovořit jako o čísle jedna), můžeme jej však také nazývat číslem jedna (a $0'$ pak nejspíše nazveme „dva“).

   b) Názvy a označení však nejsou v tomto případě podstatné. Důležité je, zda bude prvotní objekt nulovým prvkem (tj. neutrálním prvkem vůči zavedené operaci sčítání), nebo jednotkovým prvkem. V případě volby 0 jako nulového prvku budou podmínky jednoznačně definující operaci sčítání následující:

   a) $n + 0 = n$ pro každé přirozené číslo n,

   b) $(n + k)' = n + k'$ pro každá dvě přirozená (nulou počínaje) čísla k, n.

   Pokud bychom k tomuto vytvářeli alternativní teorii a zvolili za prvotní objekt místo 0 objekt $0'$ (označme jej 1), bylo by potřeba podmínky z definice sčítání upravit:

   a) $n + 1 = n'$ pro každé přirozené číslo n,

   b) $(n + k)' = n + k'$ pro každá dvě přirozená (jedničkou počínaje) čísla k, n.

[8] Jako první jej zformuloval německý matematik Hermann Hankel (1839–1873) roku 1867 v práci *Prinzip der Permanenz der formalen Gesetze*.

2. Von Neumannova čísla lze vytvářet snadno:

```
# von Neumannova cisla (od nuly)
c = []
for i in range(5):
    print(len(c), c)
    c = c + [c]
```

9 Součty přirozených čísel

1. Zopakujte si jednoduchý trik malého Gausse umožňující snadno sečíst prvních n přirozených čísel.

$$S_1(n) = 1 + 2 + 3 + 4 + \cdots + (n-2) + (n-1) + n$$

Všimněme si, že součet prvního a posledního členu je $n+1$, druhého a předposledního je také $n+1$. Takto pokračujeme ve vytváření součtů rovných stále $n+1$, až vyčerpáme všechna sčítaná čísla (je-li n sudé), případně až zbude jediné číslo ($\frac{n+1}{2}$, tj. „to uprostřed“, je-li n liché).

Součet $S_1(n)$ pak bude roven $(n+1) \cdot \frac{n}{2}$ (pro n sudé), resp. pro n liché: $(n+1) \cdot \frac{n-1}{2} + \frac{n+1}{2} = (n+1) \cdot \left(\frac{n-1}{2} + \frac{1}{2}\right) = (n+1) \cdot \frac{n}{2}$. Můžeme tedy psát jednotně pro n sudá i lichá:

$$S_1(n) = \frac{n}{2} \cdot (n+1)\,.$$

2. * Odvoďte z předchozího vztahu pro $S_1(n)$ vzorec pro součet prvních n členů obecné aritmetické posloupnosti zadané vzorcem $a_n = a_1 + (n-1)d$.

Návod: $s_n = a_1 + a_2 + \cdots + a_n = a_1 + (a_1 + d) + (a_1 + 2d) + (a_1 + 3d) + \cdots + (a_1 + (n-1)d) = \ldots$

3. * Odvoďte ze vztahu pro $S_2(n) = 1^2 + 2^2 + 3^2 + \cdots + (n-1)^2 + n^2$ (odvozen na přednášce) vzorec pro součet

$$S_3(n) = 1^3 + 2^3 + 3^3 + \cdots + (n-1)^3 + n^3 = \frac{1}{4} n^2 (n+1)^2\,.$$

4. * Dokažte, že pro všechna $n \in \mathbb{N}$ platí:

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = (1 + 2 + 3 + \cdots + n)^2\,.$$

10 Eukleidův algoritmus

Funkci vracející největšího společného dělitele dvou zadaných celých čísel vypočteného pomocí Eukleidova algoritmu je snadné naprogramovat. (Operátor `%` vypočítá zbytek po dělení.)

Zde je klasická verze:

```
def NSD(a, b):
    while b != 0:
        a, b = b, a % b
    return a
```

A zde pomocí rekurze (což je ještě jednodušší):

```
def NSDr(a, b):
    if b == 0:
        return a
    return NSDr(b, a % b)
```

1. * Pomocí Eukleidova algoritmu najděte největší společný dělitel čísel a a b.
   a) $a = 204$, $b = 54$, b) $a = 353\,623$, $b = 244\,571$, c) $a = 8\,483$, $b = 8\,313$.

2. * Dokažte, že největší společný dělitel čísel $2\,878\,325$ a $2\,878\,322$ nemůže být větší než 3.

3. * Ukažte pomocí rozkladů na součin prvočísel, že pro každé $a, b \in \mathbb{N}$ platí

$$a \cdot b = \mathrm{NSD}(a, b) \cdot \mathrm{nsn}(a, b)\,.$$

4. Všimněte si: posloupnost zbytků v Eukleidově algoritmu je ostře klesající. Tento algoritmus tedy nutně končí po konečně mnoha krocích.

   Navíc „postupným odečítáním“, které je ideovým základem Eukleidova algoritmu, se nakonec dostaneme k největšímu společnému děliteli d. Nutně se tedy po konečně mnoha krocích dostaneme k řádku, který vypadá takto (předposlední řádek):

$$a_i = b_i \cdot q_i + d\,.$$

   Jelikož je d největším společným dělitelem čísel a_i, b_i, dělí d číslo b_i, zbytek po dělení tedy bude nutně nula.

$$b_i = q_{i+1} d + 0$$

5. Pozorujme, jak „rychlý “ je Eukleidův algoritmus.

   Zde algoritmus končí poměrně rychle, neboť jsou celočíselné podíly velké (3, 7, 15).

$$\begin{aligned} 333 &= 106 \cdot 3 + 15 \\ 106 &= 15 \cdot 7 + 1 \\ 15 &= 1 \cdot 15 + 0 \end{aligned}$$

Nejhorší scénář nastane, když budou podíly nejmenší možné, tj. vždy rovny jedné. Tehdy bude Eukleidův algoritmus probíhat nejdéle, tj. v nejvíce krocích.

$$\begin{aligned} 55 &= 34 \cdot 1 + 21 \\ 34 &= 21 \cdot 1 + 13 \\ 21 &= 13 \cdot 1 + 8 \\ 13 &= 8 \cdot 1 + 5 \\ 8 &= 5 \cdot 1 + 3 \\ 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 2 + 0 \end{aligned}$$

Všimněme si, že každý řádek můžeme interpretovat tak, že postupně každé číslo je součtem předcházejících dvou a začíná členy 1 a 2, $(3 = 2+1, \ldots)$, takže tvoří Fibonacciho posloupnost.

6. * Na základě předchozího pozorování dokažte, že každé dva po sobě jdoucí členy Fibonacciho posloupnosti (počínaje $2, 3, \ldots$) jsou nesoudělné.

   [pozorujte předposlední řádek v předchozím příkladě: $3 = 2 \cdot 1 + 1$
   uvažte, že F_{n+1}, F_n jsou nesoudělná, je-li $\mathrm{NSD}(F_{n+1}, F_n) = 1$]

7. * Zvažte, zda platí silnější tvrzení, že každá dvě různá Fibonacciho čísla větší než 2 jsou nesoudělná.

   [neplatí, stačí protipříklad: 55 a 5]

Fibonacciho posloupnost pro zájemce

8. Hezké pozorování pro zájemce: členy Fibonacciho posloupnosti $\{F_n\}_{n=0}^{+\infty}$ zadané rekurentně

$$F_0 = 0, \quad F_1 = 1, \qquad F_n = F_{n-1} + F_{n-2} \ \text{ pro } n > 1,$$

   lze počítat pomocí násobení maticí

$$F = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

   neboť červeně vyznačené prvky zajistí sčítání $F_{n-1} + F_{n-2}$:

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} F_{n-2} \\ F_{n-1} \end{pmatrix} = \begin{pmatrix} F_{n-1} \\ F_{n-2} + F_{n-1} \end{pmatrix} = \begin{pmatrix} F_{n-1} \\ F_n \end{pmatrix}.$$

   Skutečně, postupným násobením vektoru $\vec{u} = \begin{pmatrix} F_0 \\ F_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ maticí F dostaneme:

$$\vec{u} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$F \cdot \vec{u} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$F^2 \cdot \vec{u} = F \cdot (F \cdot \vec{u}) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

$$F^3 \cdot \vec{u} = F \cdot (F^2 \cdot \vec{u}) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$$

$$F^4 \cdot \vec{u} = F \cdot (F^3 \cdot \vec{u}) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 3 \\ 5 \end{pmatrix}$$

$$F^5 \cdot \vec{u} = F \cdot (F^4 \cdot \vec{u}) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 5 \end{pmatrix} = \begin{pmatrix} 5 \\ 8 \end{pmatrix}$$

Obecně pro $n \in \mathbb{N}_0$:

$$F^n \cdot \vec{u} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} F_n \\ F_{n+1} \end{pmatrix} .$$

Kdybychom uměli snadno počítat mocniny matice F, tj. F^n, dostali bychom vzorec pro n-tý člen Fibonacciho posloupnosti F_n. To se však pohodlně provede pomocí Jordanova kanonického tvaru J_F (což je diagonální matice, tu je snadné umocnit – stačí umocnit prvky na diagonále), který bude probírán až v Lineární algebře II, tj. příští semestr.

Komu by to náhodou nedalo spát: pokud $F = PJ_FP^{-1}$, kde P je nějaká regulární matice, tak $F^n = PJ_F^nP^{-1}$, tj. stačí umocnit pouze diagonální matici J_F.

11 Bézoutova věta

1. * Dokažte pomocí Bézoutovy věty následující tvrzení.

   - Čísla $6k + 5$ a $9k + 7$ jsou nesoudělná pro každé $k \in \mathbb{Z}$.
   - Čísla $3n + 2$ a $2n + 1$ jsou nesoudělná pro každé $n \in \mathbb{Z}$.

   [nesoudělná čísla mají NSD = 1]

2. Bézoutova věta umožňuje řešit lineární diofantickou rovnici, tj. rovnici

   $$ax + by = c\,,$$

   jsou-li koeficienty rovnice a, b, c celá čísla a řešení hledáme opět v oboru celých čísel. Nutnou a postačující podmínkou existence řešení je, aby $\mathrm{NSD}(a, b)$ dělil c, tj.

   $$\boxed{\mathrm{NSD}(a, b) \mid c\,.}$$

   Kdyby tato podmínka nebyla splněna, tak je možno snadno vidět, že by diofantická rovnice nemohla mít v $\mathbb{Z}$ řešení. Např. rovnice

   $$15x + 24y = 1$$

   nemá v $\mathbb{Z}$ řešení, protože na levé straně můžeme vytknout trojku:

   $$3 \cdot (5x + 8y) = 3 \cdot (\text{nějaké celé číslo}) \neq 1\,.$$

3. Aplikace Bézoutovy věty na řešení lineární diofantické rovnice je přímočará v případě, že $c = 1$, tj. řešíme-li rovnici tvaru $ax + by = 1$. Pokud by na pravé straně bylo číslo různé od jedné, řešení je snadné najít:

- najdeme nějaké jedno řešení $[x_0, y_0]$ rovnice $ax + by = 1$,
- uvědomíme si, že $[cx_0, cy_0]$ je řešením rovnice $ax + by = c$, neboť

$$a \cdot (cx_0) + b \cdot (cy_0) = c \cdot (ax_0 + by_0) = c \cdot 1 = c\,.$$

4. * Pomocí Bézoutovy věty najděte nějaké jedno řešení následujících diofantických rovnic.

   a) $13\,x + 17\,y = 1$ b) $26\,x + 34\,y = 2$ c) $13\,x + 17\,y = 4$
   d) $7\,x + 26\,y = 1$ e) $18\,x + 23\,y = 1$

5. Pozorujme, jak by vypadala další řešení dané lineární diofantické rovnice $ax + by = c$, je-li jedno řešení $[x_0, y_0]$. Je zřejmé, že:

$$a \cdot b + b \cdot (-a) = 0\,,$$

   případně po vynásobení celým číslem n:

$$a \cdot (nb) + b \cdot (-na) = 0\,,$$

   takže $[nb, -na]$ je pro každé $n \in \mathbb{Z}$ řešením příslušné homogenní rovnice $ax + by = 0$. A tak vidíme, že pro každé $n \in \mathbb{Z}$ jsou

$$\boxed{x = x_0 + nb\,, \quad y = y_0 - na\,,}$$

   také řešením zadané lineární diofantické rovnice $ax + by = c$, neboť

$$ax + by = a \cdot (x_0 + nb) + b \cdot (y_0 - na) = ax_0 + anb + by_0 - bna = c + 0 = c\,.$$

   Lze ukázat, že v tomto tvaru jsou už všechna řešení dané lineární diofantické rovnice $ax+by = c$.

6. * Zapište *všechna* řešení lineárních diofantických rovnic z bodu 4.

12 Zápis čísel v pozičních soustavách

1. Převod zápisu čísla v poziční soustavě o základu n na zápis v poziční desítkové soustavě je snadný, stačí interpretovat, co znamená zápis čísla v poziční soustavě. Pozorujme např. zápis čísla ve trojkové soustavě:

$$210211_3 = 2 \cdot 3^5 + 1 \cdot 3^4 + 0 \cdot 3^3 + 2 \cdot 3^2 + 1 \cdot 3^1 + 1 \cdot 3^0 = 589_{10}$$

2. Převod zápisu čísla v poziční desítkové soustavě na zápis v poziční soustavě o základu n je zábavnější. Pozorujme číslo 5 172.

$$\begin{aligned} 5172 : 10 &= 517, \quad \text{zbytek } 2 \\ 517 : 10 &= 51, \quad \text{zbytek } 7 \\ 51 : 10 &= 5, \quad \text{zbytek } 1 \\ 5 : 10 &= 0, \quad \text{zbytek } 5 \end{aligned}$$

   Vidíme, že cifry čísla 5172 jsou rovny zbytkům po dělení desítkou.

Kdybychom chtěli číslo 5172 zapsat v poziční soustavě o základu 5, tak bychom mohli opět aplikovat analogický postup a pozorovat zbytky po dělení pěti:

$$\begin{aligned} 5172 : 5 &= 1034, \quad \text{zbytek } 2 \\ 1034 : 5 &= 206, \quad \text{zbytek } 4 \\ 206 : 5 &= 41, \quad \text{zbytek } 1 \\ 41 : 5 &= 8, \quad \text{zbytek } 1 \\ 8 : 5 &= 1, \quad \text{zbytek } 3 \\ 1 : 5 &= 0, \quad \text{zbytek } 1 \end{aligned}$$

Skutečně, $5172_{10} = 131142_5$.

Jednotlivé řádky v uvedeném postupu se nazývají *eukleidovské dělení*. Převod mezi číselnými soustavami je tedy založen na opakovaném užití eukleidovského dělení.

3. * Pomocí eukleidovského dělení převeďte zápisy čísel v poziční desítkové soustavě na zápisy v požadovaných číselných soustavách.

   a) $132_{10} = \ ?_5$ b) $876_{10} = \ ?_2$ c) $876_{10} = \ ?_4$ d) $876_{10} = \ ?_8$

4. Všimněte si, že převádět mezi soustavami o základech $2, 2^2, 2^3$ je snadné, stačí převést v zápisu ve dvojkové soustavě dvojice cifer (při převodu do čtyřkové soustavy), resp. trojice cifer (při převodu do osmičkové soustavy); postupujeme odzadu – od jednotek. Například:

   $$1101101100_2 = 31230_4 = 1554_8.$$

5. Pokud bychom chtěli převádět z poziční soustavy o libovolném základu do soustavy o libovolném jiném základu, kód by nemusel být nijak složitý. Výhodné je mít jako mezistupeň poziční desítkovou soustavu (pro výpočty pak lze použít vestavěných operátorů, např. celočíselné dělení a zbytek po dělení). V následující funkci jsou tedy pěkně vidět oba postupy: převod do i z desítkové soustavy.

```
# prevod cisla o zakladu zaklad1 na cislo o zakladu zaklad2
# funguje pouze pro prirozena cisla
# jednotlive cifry reprezentovany prvky seznamu

def prevod(cislo1, zaklad1, zaklad2):
    # prevod cisla1 o zakladu zaklad1 na d v 10kove soustave
    d = 0
    for i in cislo1:
        d = d * zaklad1 + i
    # prevod d z 10kove soustavy na cislo2 o zakladu zaklad2
    cislo2 = []
    while d > 0:
        cislo2.insert(0, d % zaklad2)
        d = d // zaklad2
    return cislo2
```

`//` ... celočíselné dělení,
`%` ... zbytek po dělení,
metoda `insert(i, prvek)` vloží `prvek` do seznamu na `i`-tou pozici (indexováno od nuly)

Uvedený algoritmus můžeme otestovat, převeďme například číslo 2414_5 v soustavě o základu 5 do trojkové soustavy.

```
c = [2, 4, 1, 4] # cislo v 5kove soustave
print(prevod(c, 5, 3))
```

Výstupem je `[1, 1, 1, 0, 2, 2]`, takže $2414_5 = 111022_3$ (obě tato čísla jsou rovna 359_{10}).

13 Řetězové zlomky

1. * Najděte racionální číslo, jehož řetězový zlomek je

$$[1; 1, 2, 1, 3, 1, 2]\,.$$

   Vypočtěte všechny konvergenty tohoto řetězového zlomku.

2. * Rozviňte do řetězového zlomku číslo $\frac{184}{106}$.

3. Pozorujte jednoduchý prográmek, který vypíše prvních n článků řetězového zlomku čísla x.

```
# Retezovy zlomek zadaneho iracionalniho cisla x
# prvnich n clanku

import math

x = math.e
pocet_clanku = 10

print(x)

q = []      # retezovy zlomek

for k in range(pocet_clanku):
    q.append( int(x) )
    x = 1 / ( x - int(x) )

print(q)
```

4. * Řetězový zlomek iracionálního čísla α je nekonečný, tj. $\alpha = [q_0; q_1, q_2, q_3, q_4, q_5, \dots]$. S pomocí kalkulátoru lze jeho články q_i hledat velmi snadno, stačí stále opakovat tutéž sekvenci:

   a) odečtu celou část, kterou zaznamenám (to je totiž q_i),
   b) ze zbylého čísla (menšího než jedna) vypočtu převrácenou hodnotu (ta už je > 1).

   Vypočtěte prvních sedm článků (tj. čísla q_i pro $i = 1, 2, \dots, 7$) řetězových zlomků následujících iracionálních čísel:

$$\varphi = \frac{1+\sqrt{5}}{2} \qquad e \qquad \pi \qquad \sqrt{3} \qquad \sqrt{5}\,.$$

   U čísel φ (tzv. zlatý řez), π a e také vypočtěte prvních sedm konvergentů $\frac{A_i}{B_i}$, $i = 1, 2, \dots, 7$.

   [$\varphi = [1; 1, 1, 1, 1, 1, 1, \dots]$, konvergenty: $1/1, 2/1, 3/2, 5/3, 8/5, 13/8, 21/13$

   $e = [2; 1, 2, 1, 1, 4, 1, \dots]$, konvergenty: $2/1, 3/1, 8/3, 11/4, 19/7, 87/32, 106/39$

   $\pi = [3; 7, 15, 1, 292, 1, 1, \dots]$, konvergenty: $3/1, 22/7, 333/106, 355/113, 103\,993/33\,102, \dots$

   $\sqrt{3} = [1; 1, 2, 1, 2, 1, 2, \dots]$, konvergenty: $1/1, 2/1, 5/3, 7/4, 19/11, 26/15, 71/41$

   $\sqrt{5} = [2; 4, 4, 4, 4, 4, 4, \dots]$, konvergenty: $2/1, 9/4, 38/17, 161/72, 682/305, 2889/1292, 12238/5473$]

5. * U čísla e doporučuji vypočítat mnohem více článků. Vynikne tak struktura (ve starších knihách se jí říká „výtvarné zákony“) tohoto nekonečného řetězového zlomku.

6. Pozorujme větu „o cikcaku“ na konvergentech řetězového zlomku, který je rozvojem čísla π:

$$\begin{aligned}
3/1 &= 3,0 && < \pi \\
22/7 &= 3,14|2857142857143 && > \pi \\
333/106 &= 3,1415|09433962264 && < \pi \\
355/113 &= 3,141592|9203539825 && > \pi \\
103\,993/33\,102 &= 3,141592653|0119025 && < \pi \\
104\,348/33\,215 &= 3,141592653|921421 && > \pi \\
208\,341/66\,317 &= 3,141592653|4674368 && < \pi \\
312\,689/99\,532 &= 3,141592653|6189365 && > \pi \\
833\,719/265\,381 &= 3,14159265358|1078 && < \pi
\end{aligned}$$

   Pro porovnání: $\pi = 3,141592653589793\dots$

7. Poznámka ke konvergentům čísla φ (tj. zlatého řezu): Fibonacciova posloupnost je zadána rekurentně:

$$F_1 = F_2 = 1, \quad F_{n+2} = F_{n+1} + F_n$$

   pro všechna $n \in \mathbb{N}$. Lze ukázat, že tuto posloupnost zadanou rekurentně lze také snadno zadat vzorcem: $F_n = \dfrac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}$. Tento vztah lze zapsat pomocí čísla $\varphi = \dfrac{1+\sqrt{5}}{2}$ (φ také nazýváme zlatý řez):

$$F_n = \frac{\varphi^n - (-\varphi)^{-n}}{\sqrt{5}}\,.$$

8. * Pomocí řetězových zlomků najděte nějaké jedno řešení následujících diofantických rovnic.

   a) $13\,x + 17\,y = 1$ b) $26\,x + 34\,y = 2$ c) $13\,x + 17\,y = 4$
   d) $7\,x + 26\,y = 1$ e) $18\,x + 23\,y = 1$

9. * Vypočtěte následující součin matic.

$$\begin{pmatrix} 1 & q_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_3 \end{pmatrix}$$

   Jak to souvisí s řetězovými zlomky?

14 Kritéria dělitelnosti

Předně si všimněme rozkladů čísel blízkých mocninám desítky (budeme počítat v poziční desítkové soustavě).

98	$2 \cdot 7 \cdot 7$	998	$2 \cdot 499$
99	$3 \cdot 3 \cdot 11$	999	$3 \cdot 3 \cdot 3 \cdot 37$
101	101	1001	$7 \cdot 11 \cdot 13$
102	$2 \cdot 3 \cdot 17$	1002	$2 \cdot 3 \cdot 167$

Uvažujme přirozené číslo a se zápisem v poziční desítkové soustavě: $a_n a_{n-1} \dots a_3 a_2 a_1 a_0$, tj.

$$a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_3 10^3 + a_2 10^2 + a_1 10 + a_0.$$

1. **Kritérium dělitelnosti 9**
   Jestliže je ciferný součet $a_n + a_{n-1} + \cdots + a_3 + a_2 + a_1 + a_0$ dělitelný 9, pak je číslem 9 dělitelné také a.
   Odvození: Jelikož je $10^k \equiv 1 \mod 9$ pro každé $k \in \mathbb{N}$, platí:

$$a \equiv a_n \cdot 1 + a_{n-1} \cdot 1 + \cdots + a_3 \cdot 1 + a_2 \cdot 1 + a_1 \cdot 1 + a_0 \mod 9\,,$$

   odkud již dostáváme požadované tvrzení.

2. * Na základě bodu 1 odvoďte kritérium dělitelnosti 3.

3. * Ukažte, že všechna čísla tvaru $10^{2k+1} + 1$, $k \in \mathbb{N}_0$ jsou dělitelná 11.

4. * Ukažte, že pro každé $k \in \mathbb{N}$ je $10^{2k} \equiv 1 \mod 11$.

5. **Kritérium dělitelnosti 11**
   Jestliže je rozdíl součtů cifer na sudých a lichých pozicích dělitelný 11, pak je číslem 11 dělitelné také a.
   Odvození: Jelikož je pro každé $k \in \mathbb{N}$:

$$10^{2k} \equiv 1 \mod 11 \quad \text{a} \quad 10^{2k+1} \equiv -1 \mod 11\,,$$

   platí:

$$a \equiv \sum_{j \text{ sudá}} a_j - \sum_{j \text{ lichá}} a_j \mod 11\,,$$

   odkud již dostáváme požadované tvrzení.

   Pozor, v následujících kritériích jde spíše o usnadnění rozhodování o dělitelnosti, čísla lze totiž uvedenými postupy podstatně zmenšit. Nejedná se o kompletní kritéria, která by byla tak pěkná, jako u 3, 9, 11.

6. * **1. kritérium dělitelnosti 7**
   Jelikož je $100 \equiv 2 \mod 7$, platí

   $$a \equiv a_1 \cdot 10 + a_0 + 2 \cdot (a_n \cdot 10^{n-2} + a_{n-1} \cdot 10^{n-3} + \cdots + a_3 \cdot 10 + a_2) \mod 7\,,$$

   což vede při opakovaném použití k relativně snadnému rozhodování o dělitelnosti sedmi.

7. * **2. kritérium dělitelnosti 7**
   Odvoďte jiné kritérium dělitelnosti 7, využijte přitom rovnost $1\,000 \equiv -1 \mod 7$.

8. * Naznačte, jak si usnadnit rozhodování o dělitelnosti číslem: 13, 17, 27, 37, 167, 499. Proč právě tato čísla?

9. * Pomocí odvozených kritérií prošetřete dělitelnost čísel $2\,838\,997\,161$ a $1\,416\,659\,583\,339$. Najděte všechny dělitele.

15 Malá Fermatova věta

1. Připomeňme si znění Malé Fermatovy věty: Je-li p prvočíslo, pak pro každé $a \in \mathbb{Z}$:

   $$a^p \equiv a \qquad \mod p\,.$$

2. * Dokažte, že na $\mathbb{Z}$ platí: je-li $a \equiv c \mod n$, pak $a^b \equiv c^b \mod n$.
   Návod: pozorujte např. tento výpočet (kongruence jsou modulo 3): jelikož je $7 \equiv 1$, tak je $7 = 1 + 3k$ pro nějaké $k \in \mathbb{Z}$ a lze psát:

   $$7^4 = (1 + 3k)^4 = 1^4 + 3N \equiv 1^4\,,$$

   přičemž poslední rovnost je na základě binomické věty.

3. Pozorujme, co se děje pro $p = 3$:
   $0^3 = 0$, $1^3 = 1$, $2^3 = 8 \equiv 2$, $3^3 = 27 \equiv 0 \equiv 3$, $4^3 = 64 \equiv 4$, $5^3 = 125 \equiv 5$, $6^3 = 216 \equiv 0 \equiv 6$, $7^3 = 343 \equiv 1 \equiv 7$, ...

4. Všimněme si, že není potřeba v předchozím příkladě pokračovat dále. Obecně stačí provádět testování Fermatovy věty pro hodnoty $a = 0, 1, 2, \ldots, p-1$. Pro ostatní a už platnost vyplývá ze vztahu

   $$a \equiv c \quad \Longrightarrow \quad a^b \equiv c^b\,.$$

   Takže např. při $p = 3$ stačí Malou Fermatovu větu ($a^3 \equiv a \mod 3$) ilustrovat pro $a = 0, 1, 2$.

   - Pro $a = 3$ to totiž nutně dopadne jako pro $a = 0$ (neboť $3^3 \equiv 0^3$),
   - pro $a = 4$ to totiž nutně dopadne jako pro $a = 1$ (neboť $4^3 \equiv 1^3$),
   - pro $a = 5$ to totiž nutně dopadne jako pro $a = 2$ (neboť $5^3 \equiv 2^3$),
   - pro $a = 6$ to totiž nutně dopadne jako pro $a = 0$ (neboť $6^3 \equiv 0^3$),
   - pro $a = 7$ to totiž nutně dopadne jako pro $a = 1$ (neboť $7^3 \equiv 1^3$),
     ...

5. Pozorujme, co se děje pro různé hodnoty prvočísla p (kongruence jsou vždy modulo p).

   - $p = 3$: $0^3 = 0$, $1^3 = 1$, $2^3 = 8 \equiv 2$
   - $p = 5$: $0^5 = 0$, $1^5 = 1$, $2^5 = 32 \equiv 2$, $3^5 = 243 \equiv 3$, $4^5 = 1024 \equiv 4$
   - $p = 7$: $0^7 = 0$, $1^7 = 1$, $2^7 = 128 \equiv 2$, $3^7 = 2187 \equiv 87 \equiv 3$, $4^7 = 16\,384 \equiv 4$, $5^7 = 78\,125 \equiv 5$, $6^7 = 279\,936 \equiv -64 \equiv 6$

   Není-li však p prvočíslem, dostáváme např.:

   - $p = 4$: $0^4 = 0$, $1^4 = 1$, !!! $2^4 = 16 \equiv 0$, !!! $3^4 = 81 \equiv 1$
   - $p = 6$: $0^6 = 0$, $1^6 = 1$, !!! $2^6 = 64 \equiv 4$, $3^6 = 729 \equiv 3$, $4^6 = 4\,096 \equiv 4$, !!! $5^6 = 15\,625 \equiv 1$

Poznámky k dělitelnosti, prvočíslům, Mersennovým a Fermatovým číslům jsou zde v pdf.

16 Mersennova čísla a dokonalá čísla

Mersennova a Fermatova čísla jsou mimo jiné skvělou hračkou. Některé jejich vlastnosti lze poměrně snadno dokázat.

1. Známá Mersennova prvočísla: `https://www.mersenne.org/primes/`
2. * V následující tabulce pozorujte poslední cifry Mersennových čísel $M_n = 2^n - 1$.
   Pozorujte poslední cifry čísel 2^n pro $n = 1, 2, 3, \ldots, 8$.
   Jakou poslední cifru mohou Mersennova čísla mít?

1	1	26	67108863	51	2251799813685247
2	3	27	134217727	52	4503599627370495
3	7	28	268435455	53	9007199254740991
4	15	29	536870911	54	18014398509481983
5	31	30	1073741823	55	36028797018963967
6	63	31	2147483647	56	72057594037927935
7	127	32	4294967295	57	144115188075855871
8	255	33	8589934591	58	288230376151711743
9	511	34	17179869183	59	576460752303423487
10	1023	35	34359738367	60	1152921504606846975
11	2047	36	68719476735	61	2305843009213693951
12	4095	37	137438953471	62	4611686018427387903
13	8191	38	274877906943	63	9223372036854775807
14	16383	39	549755813887	64	18446744073709551615
15	32767	40	1099511627775	65	36893488147419103231
16	65535	41	2199023255551	66	73786976294838206463
17	131071	42	4398046511103	67	147573952589676412927
18	262143	43	8796093022207	68	295147905179352825855
19	524287	44	17592186044415	69	590295810358705651711
20	1048575	45	35184372088831	70	1180591620717411303423
21	2097151	46	70368744177663	71	2361183241434822606847
22	4194303	47	140737488355327	72	4722366482869645213695
23	8388607	48	281474976710655	73	9444732965739290427391
24	16777215	49	562949953421311	74	18889465931478580854783
25	33554431	50	1125899906842623	75	37778931862957161709567

3. * Pozorujte uvedená přirozená čísla, počet cifer v jejich zápisu v poziční desítkové soustavě a jejich dekadický logaritmus (tj. logaritmus o základu 10).

n	počet cifer	$\log n$
1	1	0
10	2	1
100	3	2
1000	4	3
10000	5	4
7	1	0,8451
58	2	1,7634
782	3	2,8932
3428	4	3,535

   Určete počet cifer (v poziční desítkové soustavě) čísel 5^3 a 3^{10}, vyjádřete jej pomocí dekadického logaritmu.

4. * Kolik cifer má Mersennovo číslo M_{127}? [Návod: užijte dekadického logaritmu. (39)]

5. * Ověřte pomocí logaritmů, že Mersennovo číslo $M_{82\,589\,933}$ má 24 862 048 cifer. Pro zajímavost můžete zkusit spustit kód v Pythonu, který to potvrdí:

```
print(len(str( 2**82589933 - 1 )))
```

6. * Pozorujme dokonalá čísla: 6, 28, 496, 8 128, 33 550 336, 8 589 869 056, 137 438 691 328. Poslední cifrou je vždy 6 nebo 8. Ukažte, že to platí pro všechna sudá dokonalá čísla, tj. čísla ve tvaru $2^{p-1} \cdot (2^p - 1)$.

7. * Pozorujme součty převrácených hodnot všech dělitelů dokonalých čísel:

$$6: \quad \frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{6}=2, \qquad\qquad 28: \quad \frac{1}{1}+\frac{1}{2}+\frac{1}{4}+\frac{1}{7}+\frac{1}{14}+\frac{1}{28}=2.$$

   Dokažte, že jsou takovéto součty rovny dvěma pro každé sudé dokonalé číslo.

8. Hledání dokonalých čísel hrubou silou není efektivní. Už najít čtvrté dokonalé číslo chvilku trvá.

```
def soucet_delitelu(n):
    soucet = 0
    for d in range(1, n):
        if n % d == 0:
            soucet = soucet + d
    return soucet

for n in range(2, 10**4):
    if soucet_delitelu(n) == n:
        print(n, end=", ")
```

   Efektivitu lze zvýšit hledáním dělitelů menších nebo rovných odmocnině prošetřovaného čísla. Přesto trvá nalezení pátého dokonalého čísla tímto postupem hodně dlouho (opravdu nedoporučuji).

```
def soucet_delitelu(n):
    soucet = 0
    odmoc = int( n**(1/2) )
    for d in range(1, odmoc+1):
        if n % d == 0:
            soucet  =  soucet  +  d  +  n // d
    if n == odmoc**2:   # odstranení duplicity u druhých mocnin
        soucet = soucet - odmoc
    return soucet

for n in range(2, 10**4):
    if  soucet_delitelu(n)  ==  2 * n:
        print(n, end=", ")
```

17 Fermatova čísla

1. Fermatova čísla jsou čísla tvaru

$$F_n = 2^{2^n} + 1\,.$$

Snadno vypočteme, že $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65\,537$, ... Všechna uvedená Fermatova čísla (tj. F_0 až F_4) jsou prvočísla. Fermat se tedy domníval, že všechna F_n, $n \in \mathbb{N}$ jsou prvočísla.

Leonhard Euler však našel dělitele čísla F_5: číslo 641. Dosud se nepodařilo najít žádné další Fermatovo prvočíslo. Buď o rozkladu daného F_n nevíme nic, nebo známe aspoň jednoho jeho netriviálního dělitele. U F_5 až F_{11} známe jejich kompletní rozklad na součin prvočísel.

U F_{12} sice známe netriviálního dělitele (je tedy číslem složeným), kompletní rozklad na součin prvočísel se však dosud nepodařilo najít.

Viz též `http://www.prothsearch.com/fermat.html`,
případně `http://www.fermatsearch.org/news.html`.

2. * Určete, kolik má číslo F_{12} cifer (v zápisu v poziční desítkové soustavě). Využijte dekadického logaritmu.

3. Pozorujme Fermatova čísla:

n	F_n
0	3
1	5
2	17
3	257
4	65537
5	4294967297
6	18446744073709551617
7	340282366920938463463374607431768211457
8	115792089237316195423570985008687907853269984665640564039457584007913129639937
9	13407807929942597099574024998205846127479365820592393377723561443721764030073546976801874298166903427690031858186486050853753882811946569946433649006084097
10	179769313486231590772930519078902473361797697894230657273430081157732675805500963132708477322407536021120113879871393357658789768814416622492847430639474124377767893424865485276302219601246094119453082952085006768838150682342462881473913110540827237163350510684586298239947245938479716304835356329624224137217

4. * Všimněme si, že pro $n \geq 2$ má F_n poslední cifru 7. Podaří se Vám ukázat, proč tomu tak je?

5. Fermatova čísla tedy rostou se vzrůstajícím n velmi rychle. Počet cifer F_n je pro $n = 0, 1, \ldots, 23$:
F_0 : 1 F_1 : 1 F_2 : 2 F_3 : 3 F_4 : 5 F_5 : 10 F_6 : 20 F_7 : 39 F_8 : 78
F_9 : 155 F_{10} : 309 F_{11} : 617 F_{12} : 1 234 F_{13} : 2 467 F_{14} : 4 933 F_{15} : 9 865
F_{16} : 19 729 F_{17} : 39 457 F_{18} : 78 914 F_{19} : 157 827 F_{20} : 315 653 F_{21} : 631 306
F_{22} : 1 262 612 F_{23} : 2 525 223 F_{24} : ?

6. * Kolik cifer má číslo F_{24}? [Návod: užijte logaritmů.]

7. **Eukleidova věta o nekonečném počtu prvočísel:** Máme-li dokázáno, že každá dvě různá Fermatova čísla F_m a F_n jsou nesoudělná (nemají tedy v rozkladu na součin prvočísel žádné společné prvočíslo), můžeme Eukleidovu větu o nekonečném počtu prvočísel dokázat snadno:

   označíme-li u každého F_k například jeho nejmenšího prvočíselného dělitele p_k, dostaneme nekonečnou posloupnost $\{p_k\}$ navzájem různých prvočísel (díky nesoudělnosti každých dvou různých Fermatových čísel).

8. * Dokažte, že pro všechna $n \geq 2$ platí: $F_n = F_0 F_1 \cdots F_{n-2} F_{n-1} + 2$.
9. * Pozorujme Fermatova čísla pro $n \geq 1$:

$$F_1 = 5 = 6 - 1, \quad F_2 = 17 = 18 - 1, \quad F_3 = 257 = 258 - 1.$$

Dokažte, že každé Fermatovo číslo F_n, $n \geq 1$, lze psát ve tvaru:

$$F_n = 6k - 1\,,$$

kde k je nějaké přirozené číslo.

10. * Pravidelné n-úhelníky, o nichž je známo, že jsou eukleidovsky (tj. pouze pomocí pravítka a kružítka) konstruovatelné, existují jen pro konečně mnoho *lichých* n. Určete jejich počet.

18 Základní pojmy dělitelnosti

1. Říkáme, že $a \in \mathbb{Z}$ je násobkem čísla $b \in \mathbb{Z}$, existuje-li $c \in \mathbb{Z}$ takové, že $a = bc$.
2. Říkáme, že $b \in \mathbb{Z}$ dělí číslo $a \in \mathbb{Z}$ (nebo také: $b \in \mathbb{Z}$ je dělitelem čísla $a \in \mathbb{Z}$), existuje-li $c \in \mathbb{Z}$ takové, že $a = bc$. Píšeme pak: $b \,|\, a$.
3. Říkáme, že prvky $a, b \in \mathbb{Z}$ jsou asociované, jestliže

$$a \,|\, b \quad \text{a} \quad b \,|\, a\,.$$

4. Všimněme si, že asociované prvky se chovají, co se týče dělitelnosti, stejně.
V $\mathbb{Z} \setminus \{0\}$ jsou asociované vždy prvky n a $-n$.
Předchozí dvě pozorování naznačují (obvyklou specifikací relace ekvivalence pomocí „mít něco společného“ a pomocí rozkladu), že relace *být asociovaný* je na $\mathbb{Z} \setminus \{0\}$ relací ekvivalence. Samotná množina $\mathbb{Z}\setminus\{0\}$ se tak rozpadne na třídy ekvivalence $\{n, -n;\ n \in \mathbb{N}\}$. Tuto faktorovou množinu (neboli množinu všech těchto tříd) lze ztotožnit s $\mathbb{N}$. To je jeden z důvodů, proč se dělitelnost na ZŠ zkoumá a může zkoumat právě v $\mathbb{N}$ (místo $\mathbb{Z}$).
5. Označme množinu všech dělitelů přirozeného čísla $n \in \mathbb{N}$ náležejících $\mathbb{N}$ symbolem $\mathbb{D}(n)$, definujeme tedy:

$$\mathbb{D}(n) := \{d \in \mathbb{N} :\ d \,|\, a\}\,.$$

6. Společným dělitelem nenulových celých čísel $a, b \in \mathbb{Z}$ rozumíme přirozené číslo $d \in \mathbb{N}$ takové, že $d \,|\, a$ a zároveň $d \,|\, b$.
7. Největším společným dělitelem nenulových celých čísel $a, b \in \mathbb{Z}$ rozumíme největší prvek množiny všech společných dělitelů čísel a a b. Značíme jej $\mathrm{NSD}(a, b)$.
8. Říkáme, že nenulová celá čísla $a, b \in \mathbb{Z}$ jsou nesoudělná, pokud jediným jejich společným dělitelem je číslo 1.
9. Pozorování: z definice nesoudělnosti ihned plyne, že nenulová celá čísla $a, b \in \mathbb{Z}$ jsou nesoudělná právě tehdy, když je $\mathrm{NSD}(a, b) = 1$.

10. Společným násobkem nenulových celých čísel $a, b \in \mathbb{Z}$ rozumíme přirozené číslo $d \in \mathbb{N}$ takové, že $a \mid d$ a zároveň $b \mid d$.

11. Nejmenším společným násobkem nenulových celých čísel $a, b \in \mathbb{Z}$ rozumíme nejmenší prvek množiny všech společných násobků čísel a a b. Značíme jej $\operatorname{nsn}(a, b)$.

12. Prvočíslem rozumíme takové přirozené číslo $p \in \mathbb{N}$, $p \neq 1$, jehož jedinými kladnými děliteli jsou čísla 1 a p.