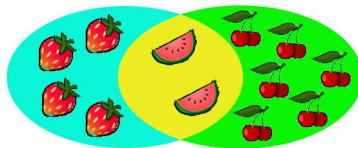


2 Množiny a množinové operace

V přehledu matematických formalismů informatiky se v této lekci zaměříme na první základní „datový typ“ matematiky, tj. na množiny. O množinách jste sice zajisté slyšeli už na základní škole, ale podstatou našeho předmětu je uvést povětšinou neformálně známé pojmy na patřičnou formální úroveň nutnou pro teoretické základy informatiky.



Stručný přehled lekce

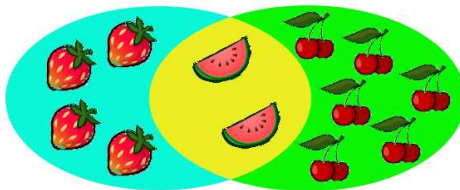
- * Uvedení množin a operací množinového kalkulu.
- * Uspořádané k -tice a kartézský součin.
- * Porovnávání a určení množin. Princip inkluze a exkluze.
- * Relace a funkce mezi množinami.

2.1 Pojem množiny

Co je vlastně množina? □

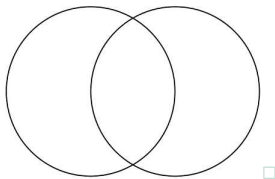
Na tuto otázku bohužel není zcela jednoduchá odpověď. . .

- Naivní pohled: „*Množina je soubor prvků a je svými prvky plně určena.*“ □



- Příklady zápisu množin \emptyset , $\{a, b\}$, $\{b, a\}$, $\{a, b, a\}$, $\{\{a, b\}\}$, $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$, $\{x \mid x \text{ je liché přirozené číslo}\}$.

Co je ale pak prvek?



Tady pozor, pojem **prvku** sám o sobě nemá matematický význam, svého významu totiž nabývá pouze ve spojení „**být prvkem množiny**“. Prvky množiny tak může být cokoli, mimo jiné i další množiny. □

Relativitu významu vztahu „prvek–množina“ si můžeme přiblížit třeba na vztahu „**podřízený–nadřízený**“ z běžného pracovního života. Tam také nemá smysl jen říkat, že je někdo podřízeným, aniž řekneme také jeho nadřízeného. Přitom i vedoucí je někomu ještě podřízený a naopak i ten poslední podřízený pracovník může být pánem třeba svého psa. Podobně je tomu s množinou jako „**nadřízenou**“ svých prvků. □

Ale přece jenom... v dobře definovaném kontextu lze (omezeně) mluvit o prvcích jako **samostatných entitách**. Formálně se například jedná o **prvky** pevně dané nosné množiny.

Zápis množiny

Značení množin a jejich prvků:

- $x \in M$ „ x je *prvkem* množiny M “,
- \emptyset je *prázdná* množina $\{\}$. \square

Některé vlastnosti vztahu „být prvkem“ jsou

- $a \in \{a, b\}$, $a \notin \{\{a, b\}\}$, $\{a, b\} \in \{\{a, b\}\}$, $\square a \notin \emptyset$, $\emptyset \in \{\emptyset\}$, $\emptyset \notin \emptyset$, \square
- **rovnost** množin dle prvků $\{a, b\} = \{b, a\} = \{a, b, a\}$, $\{a, b\} \neq \{\{a, b\}\}$. \square

Značení: Počet prvků (*mohutnost*) množiny A zapisujeme $|A|$.

- $|\emptyset| = 0$, $|\{\emptyset\}| = 1$, $|\{a, b, c\}| = 3$, $|\{\{a, b\}, c\}| = 2$.

Jednoduché srovnání množin

Vztah „být prvkem množiny“ nám přirozeně podává i způsob porovnávání množin mezi sebou. Jedná se o klíčovou část, čili hlavní nástroj teorie množin.

Definice: Množina A je *podmnožinou* množiny B , právě když každý prvek A je prvkem B . Píšeme $A \subseteq B$ nebo obráceně $B \supseteq A$.

Říkáme také, že se jedná o *inkluzi*. \square

- Platí $\{a\} \subseteq \{a\} \subseteq \{a, b\} \not\subseteq \{\{a, b\}\}$, $\emptyset \subseteq \{\emptyset\}$,
- $A \subsetneq B$ právě když $A \subseteq B$ a $A \neq B$ (A je *vlastní* podmnožinou B). \square

Z naivní definice množiny pak přímo vyplývá následující:

Definice: Dvě množiny jsou si *rovny* $A = B$ právě když $A \subseteq B$ a $B \subseteq A$.

- Podle naivní definice jsou totiž množiny A a B stejné, mají-li stejné prvky. \square
- Důkaz rovnosti množin $A = B$ má obvykle *dvě části*:
Odděleně se dokáží inkluze $A \subseteq B$ a $B \subseteq A$.

Ukázky nekonečných množin

Značení: Běžné číselné množiny v matematice jsou následující

- * $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ je množina přirozených čísel,
- * $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$ je množina celých čísel,
- * $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$ je množina celých kladných čísel,
- * \mathbb{Q} je množina racionálních čísel (zlomků).
- * \mathbb{R} je množina reálných čísel. \square

Tyto uvedené číselné množiny jsou vesměs *nekonečné*, na rozdíl od konečných množin uvažovaných v předchozím „naivním“ pohledu. \square

Pojem nekonečné množiny se přímo v matematice objevil až teprve v 19. století a brzy se s ním spojilo několik *paradoxů* ukazujících, že naivní pohled na teorii množin pro nekonečné množiny *nedostačuje*. My se k problematice nekonečných množin, Kantorově větě a Russelovu paradoxu vrátíme v závěru našeho předmětu v Lekci 11.

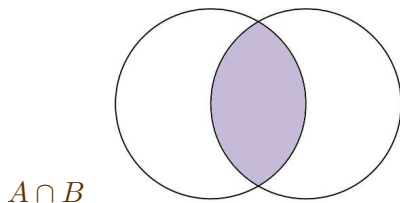
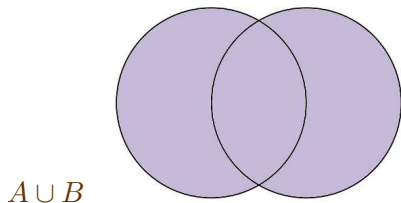
2.2 Množinové operace

Sjednocení a průnik

Definice 2.1. Sjednocení \cup a průnik \cap dvou množin A, B definujeme

$$A \cup B = \{x \mid x \in A \text{ nebo } x \in B\} \square,$$

$$A \cap B = \{x \mid x \in A \text{ a současně } x \in B\} . \square$$



- Příklady $\{a, b, c\} \cup \{a, d\} = \{a, b, c, d\}$, $\{a, b, c\} \cap \{a, d\} = \{a\}$.

Sjednocení a průnik

$$A \cup B = \{x \mid x \in A \text{ nebo } x \in B\},$$

$$A \cap B = \{x \mid x \in A \text{ a současně } x \in B\}.$$

- Vždy platí „distributivita“ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
a $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ \square
- a také „asociativita“ $A \cap (B \cap C) = (A \cap B) \cap C$ (stejně pro \cup)
a „komutativita“ $A \cap B = B \cap A$ (stejně pro \cup). \square

Definice: Pro libovolný počet množin indexovaných pomocí I rozšířeně

$$\bigcup_{i \in I} A_i = \{x \mid x \in A_i \text{ pro nějaké } i \in I\} \square,$$

$$\bigcap_{i \in I} A_i = \{x \mid x \in A_i \text{ pro každé } i \in I\} \square$$

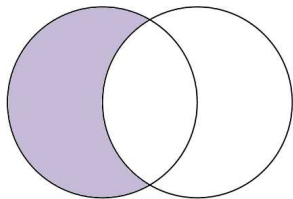
- Necht' $A_i = \{2 \cdot i\}$ pro každé $i \in \mathbb{N}$. Pak $\bigcup_{i \in \mathbb{N}} A_i$ je množina všech sudých přirozených čísel. \square
- Necht' $B_i = \{x \mid x \in \mathbb{N}, x \geq i\}$ pro každé $i \in \mathbb{N}$. Pak $\bigcap_{i \in \mathbb{N}} B_i = \emptyset$.

Množinový rozdíl

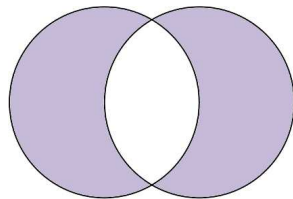
Definice 2.2. **Rozdíl** \setminus a **symetrický rozdíl** Δ dvou množin A, B definujeme

$$A \setminus B = \{x \mid x \in A \text{ a současně } x \notin B\} \square,$$

$$A \Delta B = (A \setminus B) \cup (B \setminus A). \square$$



$A \setminus B$



$A \Delta B$

- Příklady $\{a, b, c\} \setminus \{a, b, d\} = \{c\}$, $\{a, b, c\} \Delta \{a, b, d\} = \{c, d\}$. \square
- Vždy platí například $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$ apod. \square

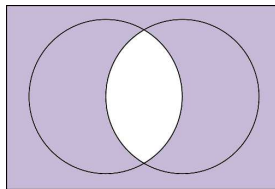
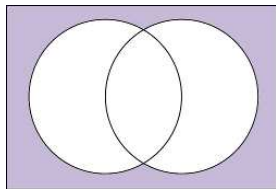
Definice: Pro libovolný počet množin indexovaných pomocí **konečné** I

$$\Delta_{i \in I} A_i = \{x \mid x \in A_i \text{ pro lichý počet } i \in I\}.$$

Doplňěk k množině

Definice: Necht' $A \subseteq M$. *Doplňkem* A *vzhledem k* M je množina $\overline{A} = M \setminus A$.

- Jedná se o poněkud specifickou operaci, která **musí být vztažena** vzhledem k **nosné množině** M !
Je-li $M = \{a, b, c\}$, pak $\overline{\{a, b\}} = \{c\}$. Je-li $M = \{a, b\}$, pak $\overline{\{a, b\}} = \emptyset$. \square
- Vždy pro $A \subseteq M$ platí $\overline{\overline{A}} = A$ („dvojitý“ doplňěk). \square
- Vždy pro $A, B \subseteq M$ platí $\overline{A \cup B} = \overline{A} \cap \overline{B}$ a $\overline{A \cap B} = \overline{A} \cup \overline{B}$.
(Viz Vennovy diagramy.)



Potenční množina

Definice 2.3. Potenční množina množiny A , neboli množina všech podmnožin, je definovaná vztahem

$$2^A = \{B \mid B \subseteq A\}.$$

-
- Platí například $2^{\{a,b\}} = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$,
 - $2^\emptyset = \{\emptyset\}$, $2^{\{\emptyset, \{\emptyset\}\}} = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$, □

Věta 2.4. Počet prvků potenční množiny splňuje $|2^A| = 2^{|A|}$. □

Důkaz: Důkaz jen stručně naznačíme (pro přesnější zápis důkazu by se použila matematická indukce z Lekce 3).

Jak vybereme jednu podmnožinu $B \subseteq A$? Například tak, že pro každý z $|A|$ prvků množiny A se nezávisle rozhodneme, zda jej zařadíme do B nebo ne. To jsou dvě možnosti pro výběr každého prvku $b \in A$ a podle principu nezávislých výběrů je celkový počet různých podmnožin množiny A roven

$$|2^A| = 2 \cdot 2 \cdot \dots \cdot 2 = 2^{|A|}.$$

□

2.3 Kartézský součin

Definice: *Uspořádaná dvojice* (a, b) je zadána množinou $\{\{a\}, \{a, b\}\}$. □

Fakt: Platí $(a, b) = (c, d)$ právě když $a = c$ a současně $b = d$. □

- Co je dle definice (a, a) ? □ $(a, a) = \{\{a\}, \{a, a\}\} = \{\{a\}, \{a\}\} = \{\{a\}\}$. □

Definice 2.5. Kartézský součin dvou množin A, B definujeme jako množinu všech uspořádaných dvojic ze složek z A a B

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

□

- Příklady $\{a, b\} \times \{a\} = \{(a, a), (b, a)\}$,
 $\{c, d\} \times \{a, b\} = \{(c, a), (c, b), (d, a), (d, b)\}$. □
- Platí $\emptyset \times X = \emptyset = X \times \emptyset$ pro každou množinu X . □
- Jednoduchá mnemotechnická pomůcka říká $|A \times B| = |A| \cdot |B|$.

Skládání součinu

Definice: Pro $k \in \mathbb{N}, k > 0$ definujeme *uspořádanou k -tici* (a_1, \dots, a_k) ind.

- $(a_1) = a_1,$
- $(a_1, a_2, \dots, a_i, a_{i+1}) = ((a_1, a_2, \dots, a_i), a_{i+1}). \square$

Fakt: Platí $(a_1, \dots, a_k) = (b_1, \dots, b_k)$ právě když $a_i = b_i$ pro každé $1 \leq i \leq k$ \square

Definice *kartézského součinu* více množin: Pro každé $k \in \mathbb{N}$ definujeme

$$A_1 \times A_2 \times \dots \times A_k = \{(a_1, a_2, \dots, a_k) \mid a_i \in A_i \text{ pro každé } 1 \leq i \leq k\}. \square$$

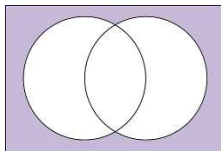
- Například $\mathbb{Z}^3 = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} = \{(i, j, k) \mid i, j, k \in \mathbb{Z}\}.$
- Co je A^0 ? $\square \quad \{\emptyset\}$, neboť jediná uspořádaná 0-tice je právě prázdná \emptyset .

Poznámka: Podle uvedené definice *není kartézský součin asociativní*, tj. obecně nemusí platit, že $A \times (B \times C) = (A \times B) \times C. \square$

V matematické praxi je někdy výhodnější uvažovat upravenou definici, podle níž součin *asociativní je*. Pro účely této přednášky není podstatné, k jaké definici se přikloníme. Prezentované definice a věty „fungují“ pro obě varianty.

2.4 Porovnávání a určení množin

Věta 2.6. Pro každé dvě množiny $A, B \subseteq M$ platí $\overline{A \cup B} = \overline{A} \cap \overline{B}$. \square



Důkaz v obou směrech rovnosti (viz ilustrační obrázek).

• $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$: \square

- * Pro $x \in M$ platí $x \in \overline{A \cup B}$, právě když $x \notin A \cup B$, neboli když zároveň $x \notin A$ a $x \notin B$.
- * To znamená $x \in \overline{A}$ a zároveň $x \in \overline{B}$, z čehož vyplývá požadované $x \in \overline{A} \cap \overline{B}$. \square

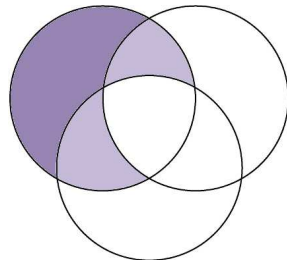
• $\overline{A \cup B} \supseteq \overline{A} \cap \overline{B}$:

- * Pro $x \in M$ platí $x \in \overline{A} \cap \overline{B}$, právě když $x \in \overline{A}$ a zároveň $x \in \overline{B}$, neboli když zároveň $x \notin A$ a $x \notin B$. \square
- * To znamená $x \notin A \cup B$, z čehož vyplývá požadované $x \in \overline{A \cup B}$.

\square

Věta 2.7. Pro každé tři množiny A, B, C platí

$$A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C). \square$$



Důkaz (viz ilustrační obrázek). \square

- $A \setminus (B \cap C) \subseteq (A \setminus B) \cup (A \setminus C)$:
 - * Je-li $x \in A \setminus (B \cap C)$, pak $x \in A$ a zároveň $x \notin (B \cap C)$, neboli $x \notin B$ nebo $x \notin C$.
 - * Pro první možnost máme $x \in (A \setminus B)$, pro druhou $x \in (A \setminus C)$. \square
- Naopak $A \setminus (B \cap C) \supseteq (A \setminus B) \cup (A \setminus C)$:
 - * Je-li $x \in (A \setminus B) \cup (A \setminus C)$, pak $x \in (A \setminus B)$ nebo $x \in (A \setminus C)$.
 - * Pro první možnost máme $x \in A$ a zároveň $x \notin B$, z čehož plyne $x \in A$ a zároveň $x \notin (B \cap C)$, a tudíž $x \in A \setminus (B \cap C)$. \square
 - * Druhá možnost je analogická.

\square

Charakteristický vektor (pod)množiny

V případech, kdy všechny uvažované množiny jsou podmnožinami nějaké konečné *nosné množiny* X , což není neobvyklé v programátorských aplikacích, s výhodou využijeme následující reprezentaci množin.

Definice: Mějme nosnou množinu $X = \{x_1, x_2, \dots, x_n\}$. Pro $A \subseteq X$ definujeme *charakteristický vektor* χ_A jako

$$\chi_A = (c_1, c_2, \dots, c_n), \text{ kde } c_i = 1 \text{ pro } x_i \in A \text{ a } c_i = 0 \text{ jinak. } \square$$

- Platí $A = B$ právě když $\chi_A = \chi_B$.
- Množinové operace jsou realizovány „bitovými funkcemi“
sjednocení \sim OR, průnik \sim AND, symetrický rozdíl \sim XOR.

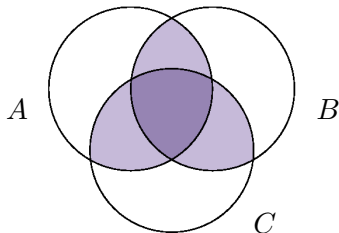
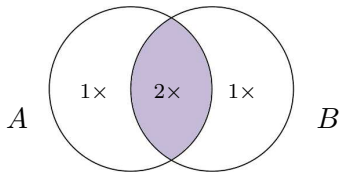
Princip inkluze a exkluze

Tento důležitý a zajímavý kombinatorický princip je někdy také nazýván „princip zapojení a vypojení“.

Věta 2.8. Počet prvků ve sjednocení dvou či tří množin spočítáme:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \square$$



Všimněte si, že větu lze stejně tak využít k výpočtu počtu prvků v průniku množin...

Příklad 2.9. Z 1000 televizí jich při první kontrole na výrobní lince má 5 vadnou obrazovku, 10 je poškrábaných a 12 má jinou vadu. Přitom 3 televize mají současně všechny tři vady a 4 jiné jsou poškrábané a mají jinou vadu.

Kolik televizí je celkem vadných? □

Řešení: Dosazením $|A| = 5$, $|B| = 10$, $|C| = 12$, $|A \cap B \cap C| = 3$, $|A \cap B| = 3 + 0$, $|A \cap C| = 3 + 0$, $|B \cap C| = 3 + 4$ do Věty 2.8 zjistíme výsledek 17. □

Poznámka. Jen stručně, bez důkazu a bližšího vysvětlení, si uvedeme **obecnou formu principu inkluze a exkluze**:

$$\left| \bigcup_{j=1}^n A_j \right| = \sum_{\emptyset \neq I \subseteq \{1, \dots, n\}} (-1)^{|I|-1} \cdot \left| \bigcap_{i \in I} A_i \right|$$

(Jeho znalost nebude v předmětu vyžadována.)

2.5 Relace a funkce

Vedle množin jsou dalším důležitým základním „datovým typem“ matematiky relace, které nyní zavedeme a kterým vzhledem k jejich mnohotvárnému použití v informatice věnujeme významnou pozornost i v příštích lekcích.

Definice 2.10. Relace mezi množinami A_1, A_2, \dots, A_k , pro $k \in \mathbb{N}$, je **libovolná** podmnožina kartézského součinu

$$R \subseteq A_1 \times A_2 \times \dots \times A_k. \square$$

Pokud $A_1 = A_2 = \dots = A_k = A$, hovoříme o **k -ární relaci R na A** . \square

Příklady relací.

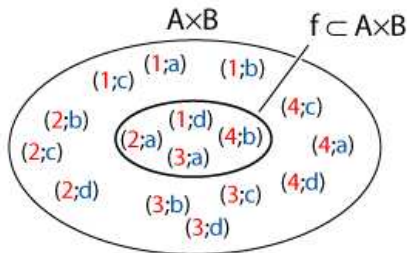
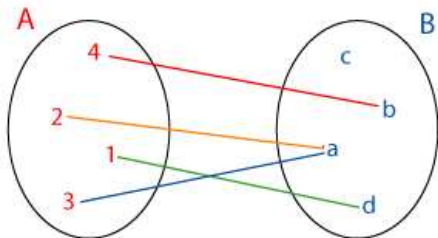
- $\{(1, a), (2, a), (2, b)\}$ je relace mezi $\{1, 2, 3\}$ a $\{a, b\}$.
- $\{(i, 2 \cdot i) \mid i \in \mathbb{N}\}$ je **binární** relace na \mathbb{N} . \square
- $\{(i, j, i + j) \mid i, j \in \mathbb{N}\}$ je **ternární** relace na \mathbb{N} .
- $\{3 \cdot i \mid i \in \mathbb{N}\}$ je **unární** relace na \mathbb{N} . \square
- Jaký význam vlastně mají unární a nulární relace na A ?

Funkce mezi množinami

Definice 2.11. (Totální) funkce z množiny A do množiny B je relace f mezi A a B taková, že pro každé $x \in A$ existuje **právě jedno** $y \in B$ takové, že $(x, y) \in f$. \square

Množina A se nazývá **definiční obor** a množina B **obor hodnot** funkce f .

Neformálně řečeno, ve funkci f je každé „vstupní“ hodnotě x přiřazena **jednoznačně** „výstupní“ hodnota y . (V obecné relaci počty „přiřazených“ dvojic neomezujeme. . .)



Značení: Místo $(x, y) \in f$ píšeme obvykle $f(x) = y$.

Zápis $f : A \rightarrow B$ říká, že f je funkce s def. oborem A a oborem hodnot B . □

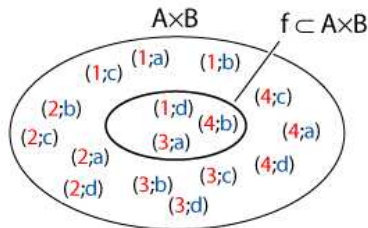
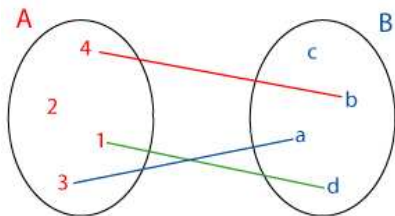
Funkcím se také říká *zobrazení*.

Příklady funkcí jsou třeba následující.

- Definujeme funkci $f : \mathbb{N} \rightarrow \mathbb{N}$ předpisem $f(x) = x + 8$.
Pak $f = \{(x, x + 8) \mid x \in \mathbb{N}\}$. □
- Definujeme funkci $plus : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ předpisem $plus(i, j) = i + j$.
Pak $plus = \{(i, j, i + j) \mid i, j \in \mathbb{N}\}$.

Parciální (částečné) funkce

Definice: Pokud naši Definici 2.11 upravíme tak, že požadujeme pro každé $x \in A$ **nejvýše jedno** $y \in B$ takové, že $(x, y) \in f$, obdržíme definici **parciální funkce** z A do B . \square



V parciální funkci f nemusí být pro některé „vstupní“ hodnoty x funkční hodnota definována (viz například $f(2)$ v uvedeném obrázku).

Pro **nedefinovanou** hodnotu používáme znak \perp .

Následuje několik příkladů parciálních funkcí.

- Definujeme parciální funkci $f : \mathbb{Z} \rightarrow \mathbb{N}$ předpisem

$$f(x) = \begin{cases} 3 + x & \text{jestliže } x \geq 0, \\ \perp & \text{jinak.} \end{cases}$$

Tj. $f = \{(x, 3 + x) \mid x \in \mathbb{N}\}$. \square

- Také funkce $f : \mathbb{R} \rightarrow \mathbb{R}$ daná běžným analytickým předpisem

$$f(x) = \log x$$

je jen parciální – není definována pro $x \leq 0$. \square

- Co je relace, přiřazující lidem v ČR jejich (česká) rodná čísla?