

3 Vlastnosti celých čísel (dělitelnost, prvočísla) a Eukleidův algoritmus. Binární relace, zejména ekvivalence a uspořádání, a jejich reprezentace. Počítání modulo. (A4B01DMA)

3.1 Vlastnosti celých čísel

- celá čísla \mathbb{Z} se skládají z přirozených čísel, nuly a záporných celých čísel
- množina je uzavřena na operaci sčítání, odčítání a násobení

3.1.1 Dělitelnost

- **Definice:** Nechť $a, b \in \mathbb{Z}$. Řekneme, že a dělí b , značeno $a|b$, jestliže existuje $k \in \mathbb{Z}$ takové, že $b = k \cdot a$. V takovém případě říkáme, že a je faktor b a že b je násobek a . Také říkáme, že b je dělitelné číslem a . Pokud toto není pravda, tak píšeme $a \nmid b$.
- Číslo $d \in \mathbb{N}$ je **společný dělitel** (common divisor) čísel a, b , jestliže $d|a$ a $d|b$.
- **největší společný dělitel** (greatest common divisor), značeno $\gcd(a, b)$ je největší prvek množiny jejich společných dělitelů, pokud je alespoň jedno z a, b nenulové.
- Číslo $d \in \mathbb{N}$ je **společný násobek** (common multiple) čísel a, b , jestliže $a|d$ a $b|d$.
- **nejmenší společný násobek** (least common multiple), značeno $\text{lcm}(a, b)$ je nejmenší prvek množiny jejich společných násobků, pokud jsou obě a, b nenulové.
- $\text{lcm}(a, 0) = \text{lcm}(0, b) = 0$
- $\gcd(0, 0) = 0$
- $\text{lcm}(a, b) \cdot \gcd(a, b) = |a| \cdot |b|$
- čísla $a, b \in \mathbb{Z}$ jsou **nesoudělná**, jestliže $\gcd(a, b) = 1$

3.1.2 Prvočíslo

- je přirozené číslo, které je beze zbytku dělitelné **právě dvěma různými přirozenými čísly**, a to číslem **jedna** a **sebou samým** (tedy 1 není prvočíslo)
- Přirozená čísla různá od jedné, která nejsou prvočísla, se nazývají **složená čísla**.

3.1.3 Eukleidův algoritmus

Lze jím vypočítat **největšího společného dělitele** dvou přirozených čísel.

- **vychází z lemmatu**: Necht' $a, b \in \mathbb{N}$, necht' $q, r \in \mathbb{N}_0$ splňují $a = qb + r$ a $0 \leq r < b$. Pak platí následující: $d \in \mathbb{N}$ je společný dělitel a, b právě tehdy, když je to společný dělitel b, r .
- $\gcd(a, b) = \gcd(b, r)$
- opakovaně hledáme \gcd pro dvojici b, r místo a, b

3.1.3.1 příklad: Chceme najít $\gcd(408, 108)$

Máme $408 = 3 \cdot 108 + 84$ ($408 \bmod 108 = 84$), proto $\gcd(408, 108) = \gcd(108, 84)$.

Máme $108 = 1 \cdot 84 + 24$, proto $\gcd(408, 108) = \gcd(108, 84) = \gcd(84, 24)$.

Máme $84 = 3 \cdot 24 + 12$, proto $\gcd(408, 108) = \gcd(108, 84) = \gcd(84, 24) = \gcd(24, 12)$.

Máme $24 = 2 \cdot 12 + 0$, proto $\gcd(408, 108) = \gcd(108, 84) = \gcd(84, 24) = \gcd(24, 12) = \gcd(12, 0) = 12$.

3.2 Binární relace

Definice: Necht' A, B jsou množiny. Libovolná podmnožina $R \subseteq A \times B$ se nazývá relace z A do B . Jestliže $(a, b) \in R$, pak to značíme aRb a řekneme, že a je v relaci s b vzhledem k R . Jestliže $(a, b) \notin R$, pak řekneme, že a není v relaci s b vzhledem k R .

Druhy relací:

- R je reflexivní, jestliže pro všechna $a \in A$ platí aRa . např. "je stejný"
- R je symetrická, jestliže pro všechna $a, b \in A$ platí $(aRb \Rightarrow bRa)$. "je sourozencem"
- R je antisymetrická, jestliže pro všechna $a, b \in A$ platí $([aRb \wedge bRa] \Rightarrow a = b)$.
- R je tranzitivní, jestliže pro všechna $a, b, c \in A$ platí $([aRb \wedge bRc] \Rightarrow aRc)$. "je vyšší; A je vyšší než B , B je vyšší než $C \Rightarrow A$ je vyšší než C "

3.2.1 Ekvivalence

Definice: Necht' R je relace na nějaké množině A . Řekneme, že R je ekvivalence, jestliže je **reflexivní, symetrická a tranzitivní**.

3.2.1.1 Třída ekvivalence

Každá ekvivalence rozdělí množinu A na systém disjunktních množin, které pak nazýváme třídy ekvivalence.

Definice: Necht' R je relace ekvivalence na nějaké množině A . Pro $a \in A$ definujeme třídu ekvivalence prvku a (equivalence class of a) vzhledem k R jako $[a]_R = \{b \in A; aRb\}$.

Příklad: Mějme ekvivalenci R na množině celých číslech \mathbb{Z} definovanou takto: $[a, b] \in R$ právě tehdy, když $|a| = |b|$. Pak:

$\mathbb{Z}[0] = \{0\}$. Nula je v relaci pouze s nulou.

$\mathbb{Z}[1] = \{-1, 1\}$. Jednička je v relaci s jedničkou a s minus jedničkou, protože $|1| = |-1|$.

$\mathbb{Z}[2] = \{-2, 2\}$. Dvojka je v relaci s dvojkou a s minus dvojkou.

$\mathbb{Z}[3] = \{-3, 3\}$

3.2.2 Částečné uspořádání

Definice: Necht' R je relace na nějaké množině A . Řekneme, že R je částečné uspořádání, jestliže je **reflexivní, antisymetrická a tranzitivní**. V tom případě řekneme, že dvojice (A, R) je částečně uspořádaná množina.

Příklad: Relace \leq je uspořádání na přirozených, celých, racionálních i reálných číslech.

Relace \subseteq je uspořádání na třídě všech množin (na univerzální třídě).

Relace dělitelnosti $|$ (a dělí b) je uspořádáním na přirozených číslech

Relace "Být potomkem" je uspořádáním na množině osob.

3.2.2.1 Hasseův diagram

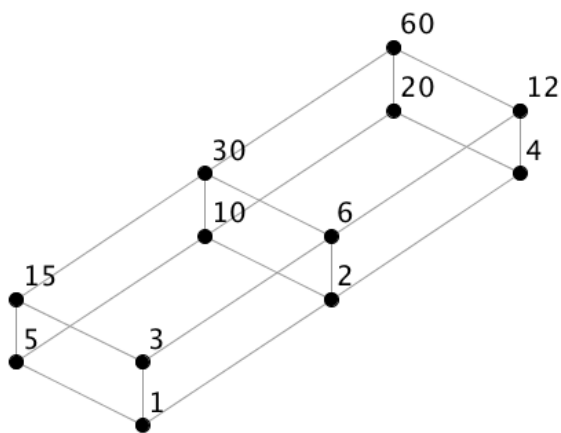
- Uspořádané množiny můžeme zakreslit pomocí Hasseova diagramu.
- vrcholy představují prvky množiny
- hrana mezi vrcholy (a, b) nám říká, že $a < b$ a zároveň neexistuje c takové, že $a < c < b$. Tedy mezi prvky a a b už žádný jiný prvek není. Přitom musí platit, že v grafu je vrchol a níže než vrchol b .

Příklad: Dělitelé čísla 60: $A = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$. Uspořádání podle dělitelnosti:

3.3 Počítání modulo

Definice Necht' $n \in \mathbb{N}$. Řekneme, že čísla $a, b \in \mathbb{Z}$ jsou **kongruentní modulo n** , značeno $a \equiv b \pmod{n}$, jestliže $n|(a-b)$.

Necht' $n \in \mathbb{N}$. Pro čísla $a, b \in \mathbb{Z}$ jsou následující podmínky ekvivalentní:



- $a \equiv b \pmod{n}$
- existuje $k \in \mathbb{Z}$ takové, že $a = b + kn$
- $a \bmod n = b \bmod n$, tj. jsou si rovny zbytky po dělení číslem n .

3.3.1 vlastnosti

Nechť $n \in \mathbb{N}$, uvažujme $a, b, u, v \in \mathbb{Z}$ takové, že $a \equiv u \pmod{n}$ a $b \equiv v \pmod{n}$:

- $a + b \equiv u + v \pmod{n}$
- $a - b \equiv u - v \pmod{n}$
- $ab \equiv uv \pmod{n}$