DMA

1. Vlastnosti celých čísel, euklidův algoritmus, binární relace, matematická indukce, rekurzivní vztahy

Vlastnosti celých čísel

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

Dělitelnost

Definice: Nechť $a, b \in Z$. Řekneme, že a dělí b, značeno $a|b$, jestliže existuje $k \in Z$ takové, že $b = a \cdot k$. 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 $a \nmid b$. Transitivita, pokud $a|b$ a $b|c$, tak $a|c$.

- Číslo $d \in N$ je **společný dělitel** (common divisor) čísel a, b, jestliže $d \mid a$ a $d \mid b$.
- **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 $d \in N$ je **společný násobek** (common multiple) čísel a, b, jestliže a|d a b|d.
- **nejmenší společný násobek** (least common multiple), značeno lcm(a, b) je nejmenší prvek množiny jejich společných násobků, pokud jsou obě a,b nenulové.
- $lcm(a, 0) = lcm(0, b) = 0$
- $gcd(0, 0) = 0$
- $lcm(a, b) \cdot gcd(a, b) = |a| \cdot |b|$
- čísla $a, b \in Z$ jsou **nesoudělná**, jestliže $gcd(a, b) = 1$

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**.

Počítání modulo

- **Definice** Nechť $n \in N$. Řekneme, že čísla $a, b \in Z$ jsou **kongruentní modulo** n, značeno a ≡ b (mod n), jestliže n|(a−b).

Nechť n ∈ N. Pro čísla a, b ∈ Z jsou následující podmínky ekvivalentní:

- $a \equiv b(\mod n)$
- existuje $k \in Z$ takové, že $a = b + k \cdot n$
- $a \mod n = b \mod n$, tj. jsou si rovny zbytky po dělení číslem n.

Vlastnosti

Nechť $n \in N$, uvažujme $a, b, u, v \in Z$ takové, že $a \equiv u \mod n$ a $b \equiv v \mod n$:

- $a + b \equiv u + v \mod n$
- $a - b \equiv u - v \mod n$
- $ab \equiv uv \mod n$

Inverzní číslo

- Řekneme, že $b \in Z$ je inverzní číslo k a mod n, $a \in Z$, jestliže $a * b \equiv 1$ (mod n).
- Převede libovolné číslo na 1 ve světě Z_n.
- Existuje když $gcd(a, n) = 1$.
- Výpočet pomocí Euklidova algoritmu.

Eukleidův algoritmus

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

- **vychází z lemmatu**: Nechť $a, b \in N$, nechť $q, r \in N_0$ splňují $a = q \cdot b + r$ a $0 \leq r < b$. Pak platí následující: $d \in N$ 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
- rozšířená verze počítá i s indexy jak se dostat k gcd (bezout)

Bezoutova identita

- $gcd(a, b)$ lze zapsat jako $gcd(a, b) = a * k + b * j$, kde $k, j \in Z$
- Lze použít pro řešení diofantických rovnic ($ax + by = c$, kde $a, b, c \in Z$) nebo hledání inverzního čísla

Malá fermatova věta

pro každé prvočíslo *p* a každé celé číslo *a* platí
$a^p \equiv a \pmod{p}$
$a^{p-1} \equiv 1 \pmod{p}$

Binární relace

Definice: Nechť 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 ∈ A platí aRa. např. “je stejný”
- R je **symetrická**, jestliže pro všechna a, b ∈ A platí ($aRb \Rightarrow bRa$). Důkaz -> prohodit a a b.
- R je **antisymetrická**, jestliže pro všechna a, b ∈ A platí ($[aRb \wedge bRa] \Rightarrow$ a = b). Důkaz -> do aRb dosadíme bRa, dostaneme podmínku a tu vložíme do bRa, kde zjistíme, co musí být a. Tím dokážeme určit jestli $a = b$.
- R je **tranzitivní**, jestliže pro všechna a, b, c ∈ A platí ($[aRb \wedge bRc] \Rightarrow aRc$). Důkaz -> do bRc dosadíme aRb, a to dosadíme do aRc.

Ekvivalence

Definice: Nechť R je relace na nějaké množině A. Řekneme, že R je ekvivalence, jestliže je **reflexivní, symetrická a tranzitivní**.
0.2.1.1 Třída ekvivalence
Každá ekvivalence rozdělí množinu A na systém disjunktních množin, které pak nazýváme třídy ekvivalence.
Definice: Nechť R je relace ekvivalence na nějaké množině A. Pro a ∈ A definujeme třídu ekvivalence prvku a (equivalence class of a) vzhledem k R jako [a] R = $b \in A; aRb$.

Částečné uspořádání

Definice: Nechť 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.

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.
- největší prvek - prvek do, kterého se dá dostat ze všech prvků a nemá prvek nad sebou (nemusí existovat)
- maximum - prvek, který nemá prvek nad sebou
- nejmenší prvek - prvek ze, kterého všechno vychází a nemá prvek pod sebou (nemusí existovat)
- minimum - prvek, který nemá prvek pod sebou
- linearizace částeč. uspoř. - Hessův diagram od minima, po úrovních zapsat na řádek, za sebe. Rozdělovací symbol $<_L$.

Matematická indukce

Matematická indukce je metoda dokazování matematických vět a tvrzení, která se používá, pokud chceme ukázat, že dané tvrzení platí pro všechna celá čísla $n \in Z$ počínající nějakým n_0.
Typický důkaz indukcí se skládá ze dvou kroků:

1. **Základní krok**: V tomto kroku se dokáže, že tvrzení platí pro nejmenší číslo n_0, nikoliv pro n=1, pro které nemusí vždy obecně platit.
2. ***Indukční krok***: Ukážeme, že *pokud* tvrzení platí pro $n = m$ **(***indukční předpoklad***),** pak* platí i pro $n = m + 1$.

Princip matematické indukce pak již říká, že tvrzení platí pro každé $n \geq n_0$.
Často se v prvním kroku dokazuje, že tvrzení platí pro $n = 0$.
Rozlišuje se slabý a silný princip matematické indukce: slabý princip v indukčním kroku předpokládá, že tvrzení platí pro $n = m$, zatímco silný předpokládá, že tvrzení platí pro všechna $n = n_0, n_0 + 1, \ldots, m$. Slabý a silný princip matematické indukce jsou ekvivalentní (tj. oběma lze dokázat stejnou množinu tvrzení).

Rekurzivní vztahy

Definice: Rekurentní vztah či rekurzivní vztah pro posloupnost $\{a_k\}$ je libovolná rovnice typu $F(a_n, a_{n-1}, a_{n-2}, \ldots, a_0) = 0$, kde F je nějaká funkce.
Např. podstata problému Hanojských věží se dá vyjádřit vztahem $H_n - 2 \cdot H_{n-1} - 1 = 0$

Lineární rekurentní rovnice

Lineární rekurentní rovnice, popřípadě **lineární rekursivní rovnice řádu** $k \in \mathbb{N}_0$ je libovolná rovnice ve tvaru

$$a_{n+k} + c_{k-1}(n)a_{n+k-1} + \cdots + c_2(n)a_{n+2} + c_1(n)a_{n+1} + c_0(n)a_n = b_n \quad \text{pro všechna } n \geq n_0,$$

kde $n_0 \in \mathbb{Z}$, $c_i(n)$ pro $i = \{0, \ldots, k-1\}$ (tzv. **koeficienty** rovnice) jsou nějaké funkce $\mathbb{Z} \mapsto \mathbb{R}$, přičemž $c_0(n)$ není identicky nulová funkce, a $\{b_n\}_{n=n_0}^{\infty}$ (tzv. **pravá strana rovnice**) je pevně zvolená posloupnost reálných čísel.

Jestliže $b_n = 0$ pro všechna $n \geq n_0$, pak se příslušná rovnice nazývá **homogenní**.

- Základní vlastnosti - jejich množina řešení tvoří vektorový prostor dimenze rovné řádu rovnice, takže řešení lze generovat pomocí vhodné báze
- jak najít vhodnou bázi - pomocí kořenů charakteristického polynomu

Řešení

Nechť je dána lineární rekurentní rovnice

$$a_{n+k} + c_{k-1}(n)a_{n+k-1} + \ldots + c_1(n)a_{n+1} + c_0(n)a_n = b_n \quad \text{pro všechna } n \geq n_0.$$

Jako její **řešení** označíme libovolnou posloupnost $\{a_n\}_{n=n_0}^{\infty}$ takovou, že po dosazení odpovídajících členů do dané rovnice dostáváme pro všechna n pravdivý výrok.

viz příklad 5

Charakteristická rovnice

Definice
Nechť je dána lineární rekurentní rovnice s konstantními koeficienty

$$a_{n+k} + c_{k-1}a_{n+k-1} + \ldots + c_1a_{n+1} + c_0a_n = b_n \text{ pro všechna } n \geq n_0.$$

Její **charakteristický polynom** (**characteristic polynomial**) je definován jako polynom

$$p(\lambda) = \lambda^k + c_{k-1}\lambda^{k-1} + \ldots + c_1\lambda + c_0.$$

Kořeny charakteristického polynomu se nazývají **charakteristická čísla**, popřípadě **vlastní čísla** dané rovnice (**characteristic numbers/roots** or **eigenvalues**).

K získání charakteristických čísel potřebujeme vyřešit rovnici $p(\lambda) = \lambda^k + c_{k-1}\lambda^{k-1} + \ldots + c_1\lambda + c_0 = 0$, které se také říká charakteristická rovnice.

Příklady

1. Chceme najít $gcd(408, 108)$
   408 = 3 · 108 + 84 (408 mod 108 = 84), proto gcd(408, 108) = gcd(108, 84).
   108 = 1 · 84 + 24, proto gcd(408, 108) = gcd(108, 84) = gcd(84, 24).
   84 = 3 · 24 + 12, proto gcd(408, 108) = gcd(108, 84) = gcd(84, 24) = gcd(24, 12).
   24 = 2 · 12, proto gcd(408, 108) = gcd(108, 84) = gcd(84, 24) = gcd(24, 12) = gcd(12, 0) = 12

Příklad 5b.b: Nechť $A = \mathbb{N}$. Uvažujme relaci R na A danou následující podmínkou: $(a, b) \in R$ právě tehdy, když existuje $k \in \mathbb{N}$ splňující $b = a^k$. Jaké má vlastnosti?

Nejprve se ujistíme, že definici dobře rozumíme. Jak jsme již diskutovali v příkladě 5a.h, to k je individuální pro každý testovací pár (a, b). Takže třeba víme, že $(3, 9) \in R$, protože existuje $k = 2 \in \mathbb{N}$ splňující $8 = 3^2$, a také $(2, 16) \in R$, to má zase své $k = 4 \in \mathbb{N}$ splňující $16 = 2^4$. Naopak $(4, 2) \notin R$, protože nenajdeme $k \in \mathbb{N}$ tak, aby platilo $2 = 4^k$ (sice najdeme $k = \frac{1}{2}$, ale to není z $\mathbb{N}$). Relaci už rozumíme, podívejme se na vlastnosti.

R: Uvažujme nějaké $a \in \mathbb{N}$. Aby byla relace reflexivní, muselo by platit $(a, a) \in R$, tedy $a = a^k$ pro nějaké $k \in \mathbb{N}$. To umíme zařídit.

Odpověď: R je reflexivní, protože pro <u>každé $a \in \mathbb{N}$</u> existuje $k = 1 \in \mathbb{N}$ splňující $a = a^1$, tedy <u>$(a, a) \in R$</u>.

S: Uvažujme nějaká čísla $a, b \in \mathbb{N}$. Symetrie vyžaduje, aby v případě, že splňují $(a, b) \in R$, platilo nutně i $(b, a) \in R$.

Podmínka $(a, b) \in R$ znamená, že $b = a^k$ pro nějaké $k \in \mathbb{N}$. Potřebujeme z toho nějakým způsobem odvodit, že pak $a = b^l$ pro nějaké $l \in \mathbb{N}$ (musíme zvolit jiné písmeno, protože dvojice (b, a) má právo na svůj vlastní exponent). Z dané rovnice $b = a^k$ hravě odvodíme $a = b^{1/k}$, takže bychom museli mít $l = \frac{1}{k}$, ale pak nevypadá nadějně, že by platilo $l \in \mathbb{N}$. To nás inspiruje k nalezení protipříkladu.

Odpověď: S není symetrická, protože dvojice $a = 2$, $b = 4$ splňuje $4 = 2^2$ neboli $(2, 4) \in R$, ale nesplňuje $(4, 2) \in R$.

A: Antisymetrie vyžaduje, aby pro $a, b \in \mathbb{N}$ platilo, že když $b = a^k$ a $a = b^l$ pro nějaká $k, j \in \mathbb{N}$, pak nutně $a = b$. Všimněte si, že jsme při překládání definice do naší situace každé z dvojic $(a, b) \in R$, $(b, a) \in R$ dali možnost mít svůj vlastní exponent. Pokud bychom v obou případech použili k, tak by byl důkaz špatně, protože by nevyčerpal všechny možné případy. Zpět k otázce, je splněna? Poslechneme radu a rovnou začneme psát důkaz, třeba to vyjde.

Vezměme <u>libovolné $a, b \in \mathbb{N}$</u> takové, že <u>$(a, b) \in R$ a $(b, a) \in R$</u>. Pak pro nějaká $k, l \in \mathbb{N}$ platí $b = a^k$ a $a = b^l$. Dosazením první rovnice do druhé dostaneme $a = a^{kl}$. Toto je pro $a \in \mathbb{N}$ možné jedině tehdy, když $kl = 1$. Toto je zase pro $k, l \in \mathbb{N}$ možné jedině tehdy, když $k = l = 1$. Dostáváme proto <u>$b = a^1 = a$</u>. Ukázali jsme, že R je antisymetrická.

Poznámka: Pokud nám důkaz vznikne za pochodu, obvykle zahrnuje i rozličné pomocné úvahy. Bývá dobré pak pro čtenáře zvýraznit, která místa tvoří důkaz samotný.

Poznámka: Šel by i jiný důkaz. Můžeme si všimnout, že pro $a, k \in \mathbb{N}$ platí $a^k \geq a$. Pro dvojici $(a, b) \in R$ proto platí $b \geq a$. Z předpokladů $[(a, b) \in R \wedge (b, a) \in R]$ tak dostáváme $[b \geq a \wedge a \geq b]$, odkud hned máme $a = b$.

T: Mějme $a, b, c \in \mathbb{N}$. Tranzitivita vyžaduje, aby v případě, že $b = a^k$ a $c = b^l$ pro nějaká $k, l \in \mathbb{N}$, také platilo, že $c = a^m$ pro nějaké $m \in \mathbb{N}$.

Tradiční přístup je eliminovat z daných rovnic b, což se snadno povede dosazením první rovnice do druhé. Dostáváme $c = (a^k)^l$, což vypadá téměř jako to, co chceme dokázat.

Odpověď: R je tranzitivní: Vezměme <u>libovolné $a, b, c \in \mathbb{N}$</u> a předpokládejme, že <u>$(a, b) \in R$ a $(b, a) \in R$</u>. To znamená, že existují $k, l \in \mathbb{N}$ splňující $b = a^k$ a $c = b^l$. Dosazením získáme $c = a^{kl}$ a také platí $kl \in \mathbb{N}$, proto dle definice <u>$(a, c) \in R$</u>.

△

2.

3. Relace ≤ je uspořádání na přirozených, celých, racionálních i reálných číslech.
   Relace ⊆ 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.

4. Vyřešte homogenní lineární rekurentní rovnici $F_n = F_{n-1} + F_{n-2}$, $n \geq 2$.
   Nejdříve si přepíšeme indexy, aby byl nejnižší n. To si také můžeme představit jako substituci $n = m + 2$. Dostáváme $F_{m+2} = F_{m+1} + F_m$.
   Nezapomeneme na podmínku, do které také substituujeme za n: $m + 2 \geq 2$, neboli $m \geq 0$.
   Nyní přepíšeme rovnici tak, aby na pravé straně byla 0, tedy na $F_{m+2} - F_{m+1} - F_m = 0$.
   Dosadíme λ^i za každé F_{m+i} a vyřešíme kvadratickou rovnici.
   $\lambda^2 - \lambda - 1 = 0$
   $\lambda_1 = \frac{1+\sqrt{5}}{2}$, $\lambda_2 = \frac{1-\sqrt{5}}{2}$
   Dostáváme řešení $F_n = u\frac{1+\sqrt{5}}{2} + v\frac{1-\sqrt{5}}{2}$, $n \geq 0$. (kořeny na n ?)

5. Vyřešte homogenní lineární rekurentní rovnici $a_{n+3} - 3a_{n+2} + 3a_{n+1} - a_n = 0$, $n \geq 1$.
   Znovu sestrojíme charakteristický polynom: $\lambda^3 - 3\lambda^2 + 3\lambda - 1 = 0$.
   Charakteristickými čísly jsou $\lambda_1 = \lambda_2 = \lambda_3 = 1$.
   Protože je násobnost kořene rovna 3, nebude řešením $a_n = u \cdot 1^n$, ale
   $a_n = u \cdot (1^n) + v \cdot (n \cdot 1^n) + w \cdot (n^2 \cdot 1^n) = u + v \cdot n + w \cdot n^2$, $n \geq 1$.

6. Vyřešte homogenní lineární rekurentní rovnici $a_{n+2} - 2a_{n+1} - 3a_n = -9n \cdot 2^n$, $n \geq 0$.
   Zjistíme charakteristická čísla pro homogenní rovnici (položíme rovno nule):
   $\lambda^2 - 2\lambda - 3 = 0 \rightarrow \lambda_1 = -1, \lambda_2 = 3$.
   Tím pádem je homogenním řešením $a_{h,n} = u \cdot (-1)^n + v \cdot 3^n$, $n \geq 0$.
   Partikulární řešení zjistíme tak, že odhadneme pravou stranu přes polynom.
   Protože je na pravé straně $-9n \cdot 2^n$, odhadneme lineární polynom $a_n = (An + B) \cdot 2^n$.
   Kdyby ovšem na pravé straně bylo $-9n \cdot 3^n$, tak musíme odhadovat $a_n = n \cdot (An + B) \cdot 3^n$. Obecně - pokud má pravá straně $P(x) \cdot \lambda_i^n$, tak násobíme odhad n^m, kde m je násobnost λi.
   Ten dosadíme do levé strany za a_n:
   $(A(n + 2) + B) \cdot 2^{n+2} - 2(A(n + 1) + B) \cdot 2^{n+1} - 3(An + B) \cdot 2^n =$
   $4(An + 2A + B) \cdot 2^n - 4(An + A + B) \cdot 2^n - 3(An + B) \cdot 2^n =$
   $[(-3A)n + (4A - 3B)] \cdot 2^n$.
   Když výsledný výraz položíme roven $-9n \cdot 2^n$, dostáváme soustavu lineárních rovnic
   $-3A = -9$
   $4A - 3B = 0$, jejímž řešením je $A = 3, B = 4$. Partikulární řešení je tedy $a_{p,n} = (3n + 4) \cdot 2^n, n \geq 0$.

Zkombinováním $a_n = a_{p,n} + a_{h,n}$ získáme obecné řešení
$a_n = (3n + 4) \cdot 2^n + u \cdot (-1)^n + v \cdot 3^n, n \geq 0.$
https://www.youtube.com/watch?v=6hkBATZVOjg