1 Počítání modulo n

Algebraické struktury - terminologie

1.1 Definice Na množině A je dána binární operace $*$, tj. zobrazení z $A \times A$ do A.

Dvojice $(A, *)$ se nazývá *pologrupa*, pokud je operace $*$ asociativní,
tj. jestliže pro každé $x, y, z \in A$ platí $x * (y * z) = (x * y) * z$.

Dvojice $(A, *)$ se nazývá *monoid*, pokud je operace $*$ asociativní a má neutrální prvek,
tj. jestliže existuje $e \in A$ tak, že pro každé $x \in A$ platí $e * x = x = x * e$.

Dvojice $(A, *)$ se nazývá *grupa*, pokud je operace $*$ asociativní, má neutrální prvek a má všechny inverzní prvky,
tj. jestliže pro každé $x \in A$ existuje $y \in A$ tak, že $x * y = e = y * x$.
Poznámka: Inverzní prvek k prvku x je určen jednoznačně, pokud vůbec existuje, a značíme jej x^{-1}.

Pologrupa, monoid či grupa jsou *komutativní*, pokud je operace $*$ komutativní,
tj. jestliže pro každé $x, y \in A$ platí $x * y = y * x$.

1.2 Definice Mějme množinu A se dvěma binárními operacemi, které označíme jako sčítání a násobení.

Trojice $(A, +, \cdot)$ se nazývá *okruh*, jestliže

- $(A, +)$ je komutativní grupa s neutrálním prvkem 0;
- $(A, \cdot)$ je pologrupa;
- platí oba distributivní zákony,
  tj. pro všechna $x, y, z \in A$ platí $x \cdot (y + z) = x \cdot y + x \cdot z$ a také $(y + z) \cdot x = y \cdot x + z \cdot x$.

Je-li navíc pologrupa $(A, \cdot)$ komutativní, říkáme, že se jedná o *komutativní okruh*; má-li pologrupa $(A, \cdot)$ jednotkový prvek, mluvíme o *okruhu s jednotkou*.

Trojice $(A, +, \cdot)$ se nazývá *těleso*, jestliže je to okruh s jednotkou 1, kde každý nenulový prvek má inverzní prvek, tedy $(A - \{0\}, \cdot)$ je grupa, a kde navíc $0 \neq 1$, tedy neutrální prvek 1 pro násobení není současně neutrálním prvkem 0 pro sčítání.

Většinou budeme říkat stručně těleso, ale půjde o *komutativní těleso*, tj. násobení bude komutativní.

Konstrukce faktorových okruhů modulo n

Vycházíme z množiny celých čísel s operacemi sčítání a násobení. $(\mathbb{Z}, +, \cdot)$ je komutativní okruh s jednotkou, invertibilními prvky jsou v něm pouze 1 a -1. V celých číslech umíme dělit se zbytkem a díky tomu můžeme vystavět celou následující teorii.

1.3 Věta o dělení se zbytkem *Pro každé $a, b \in \mathbb{Z}$, kde $b \neq 0$, existují jednoznačně určené $r, z \in \mathbb{Z}$ tak, že*

$$a = rb + z \quad \text{a} \quad 0 \leq z < b.$$

První sada důsledků:

1.4 Lze definovat *relaci dělitelnosti*: $a|b$ iff $b = ka$ pro nějaké $k \in \mathbb{Z}$. Tato relace je uspořádáním (reflexivní, antisymetrickou a tranzitivní relací) na $\mathbb{N}$. Není však antisymetrická na $\mathbb{Z}$, tam má smysl mluvit o *relaci asociovanosti*: $a||b$ iff $a|b$ a $b|a$; přitom platí, že $a||b$ jen, když $b = \pm a$.

1.5 Můžeme zavést pojem prvočíslo a rozkládat celá čísla na součin prvočísel. Celé číslo $p \geq 2$ je *prvočíslo*, jestliže je dělitelné pouze čísly 1 a p, aneb jestliže se nedá napsat jako součin dvou čísel menších než p. Test prvočíselnosti "hrubou silou": Číslo n je prvočíslo, pokud není dělitelné beze zbytku žádným prvočíslem do $\sqrt{n}$.

1.6 Základní věta aritmetiky Každé celé číslo $n \geq 2$ lze jednoznačně (až na pořadí) napsat jako součin mocnin různých prvočísel.

Druhá sada důsledků:

1.7 Definice *Největší společný dělitel* dvou čísel $a, b \in \mathbb{Z}$ je takové číslo $d \in \mathbb{Z}$, že d dělí obě čísla a i b, d je dělitelné všemi společnými děliteli obou čísel a konečně $d > 0$. Značíme $d = \gcd(a, b)$.

1.8 Největšího společného dělitele lze najít pomocí **Eukleidova algoritmu**. Jedná se o rekurzivní algoritmus, který se opírá o dělení se zbytkem. Předpokládejme, že $a > b$. Podělíme se zbytkem: $a = rb + z$ a $0 \leq z < b$. Pokud je zbytek $z = 0$, tak je $\gcd(a, b) = b$. Pokud je zbytek $z > 0$, tak se snadno dokáže, že dvojice a, b má stejné společné dělitele jako dvojice b, z, tedy i $\gcd(a, b) = \gcd(b, z)$. Budeme dále hledat $\gcd(b, z)$ stejným postupem. Jelikož zbytky jsou celočíselné, nezáporné a stále menší, bude po konečném počtu kroků zbytek nulový a úlohu pro nalezení gcd vyřešíme přímo.

1.9 Věta (Bezoutova) *Největší společný dělitel čísel $a, b \in \mathbb{Z}$ je jejich celočíselnou kombinací, aneb*

$$\gcd(a, b) \;=\; ka \;+\; lb \quad \text{pro} \quad k, l \in \mathbb{Z}.$$

K nalezení celočíselných koeficientů k, l lze použít rozšířený Eukleidův algoritmus. V každém kroku Eukleidova algoritmu přepočítáme aktuální zbytek na kombinaci čísel a a b. Jelikož $\gcd(a, b)$ je posledním nenulovým zbytkem, tak jednou nakombinujeme z čísel a a b i jejich největšího společného dělitele.

1.10 Diofantické rovnice Rovnice $ax + by = c$, kde $a, b, c \in \mathbb{Z}$, má řešení v $\mathbb{Z}$ právě, když $\gcd(a, b)|c$.
Pokud nějaké celočíselné řešení Diofantické rovnice existuje, pak je jich nekonečně mnoho a jsou tvaru

$$(x, y) = (x_p, y_p) + k(x_0, y_0) \quad \text{pro} \quad k \in \mathbb{Z},$$

kde (x_p, y_p) je partikulární řešení a najdeme ho pomocí rozšířeného Eukleidova algoritmu a kde (x_0, y_0) je nesoudělné řešení homogenní rovnice, tedy $(x_0, y_0) = (\frac{b}{d}, -\frac{a}{d})$, kde $d = \gcd(a, b)$.

Třetí sada důsledků:

1.11 Definice Čísla $a, b \in \mathbb{Z}$ jsou *kongruentní modulo* n pro $n \in \mathbb{N}$, jestliže $n|(b - a)$. To nastává právě, když mají čísla a a b stejný zbytek po dělení číslem n. Značíme $a \equiv b \pmod{n}$.

1.12 Tvrzení *Relace kongruence modulo n je relace ekvivalence (reflexivní, symetrická a tranzitivní relace) na množině celých čísel, která je zachována při sčítání a násobení, tj. pokud $a \equiv b \pmod{n}$ a $c \equiv d \pmod{n}$, pak $a + c \equiv b + d \pmod{n}$ i $ac \equiv bd \pmod{n}$.*

1.13 Relace kongruence modulo n tudíž rozbije množinu celých čísel na třídy navzájem ekvivalentních prvků, tzv. zbytkové třídy modulo n. Množinu zbytkových tříd modulo n značíme $\mathbb{Z}_n$,

$$\mathbb{Z}_n = \mathbb{Z}/\equiv (\text{mod } n) = \{[0]_n, [1]_n, \ldots, [n-1]_n\},$$

kde $[a]_n = \{a + kn | k \in \mathbb{Z}\}$.
Na množině $\mathbb{Z}_n$ můžeme korektně definovat operace sčítání a násobení přes representanty:

$$[a]_n \oplus [b]_n = [a + b]_n, \quad [a]_n \odot [b]_n = [a \cdot b]_n$$

Díky definici přes representanty zdědí operace $\oplus$ a $\odot$ vlastnosti, které měly operace sčítání a násobení na $\mathbb{Z}$. Trojice $(\mathbb{Z}_n, \oplus, \odot)$ tvoří komutativní okruh s jednotkou, nazývá se *faktorový okruh modulo n*. V dalším textu zjednodušíme jeho značení na $(\mathbb{Z}_n = \{0, 1, \ldots, n-1\}, +, \cdot)$.

1.14 V okruhu $\mathbb{Z}_n$ umíme řešit lineární rovnice $ax = b$ převedením na Diofantickou rovnici $ax + ny = b$. Víme tedy, že řešení existuje právě, když $\gcd(a, n)|b$, pak $x = x_p + kx_0$, kde $x_0 = \frac{n}{\gcd(a,n)}$. V okruhu $\mathbb{Z}_n$ tak vznikne celkem $\gcd(a, n)$ různých řešení.
Speciálně, pokud řešíme rovnici $ax = 1$ v $\mathbb{Z}_n$, bude řešení existovat jen, když $\gcd(a, n) = 1$, a pak bude toto řešení jediné. Prvek a je invertibilní v $\mathbb{Z}_n$ právě, když a je nesoudělné s n.

1.15 Věta *Okruh $(\mathbb{Z}_n, +, \cdot)$ je těleso právě, když $n = p$ je prvočíslo.*

2 Lineární algebra nad $\mathbb{Z}_p$

2.1 Soustavy lineárních rovnic budeme řešit pouze nad $\mathbb{Z}_p$, kde p je prvočíslo. Zde funguje Gaussova eliminační metoda s tím rozdílem, že místo dělení budeme násobit inverzními prvky (ty existují v $\mathbb{Z}_p$ pro všechny nenulové prvky). Nad $\mathbb{Z}_n$, kde n není prvočíslo, Gaussova eliminační metoda nefunguje.

Všechna řešení homogenní soustavy tvoří podprostor v $\mathbb{Z}_p^n$. Každé řešení nehomogenní soustavy je součtem partikulárního řešení této soustavy a nějakého řešení přidružené homogenní soustavy.
Soustava m lineárních rovnic o n neznámých může mít nad $\mathbb{Z}_p$ žádné řešení, jedno řešení (jedinou n-tici), nebo p^k řešení, kde k je počet proměnných, které smíme volit libovolně v $\mathbb{Z}_p$.

2.2 Maticový počet lze dělat i nad $\mathbb{Z}_n$, ale záležitosti související s Gaussovou eliminací se tam budou chovat jinak, než jak to známe u reálných matic (např hodnost matice $\mathbb{A}^T$ se nemusí rovnat hodnosti matice $\mathbb{A}$).
Matice $\mathbb{A}$ je *regulární matice* nad $\mathbb{Z}_n$, když $\det \mathbb{A}$ je invertibilní v $\mathbb{Z}_n$. Tehdy a jen tehdy existuje inverzní matice k matici $\mathbb{A}$ a lze spočítat jako $\mathbb{A}^{-1} = (\det \mathbb{A})^{-1}\mathbb{D}^T$, kde $\mathbb{D}$ je matice algebraických doplňků k matici $\mathbb{A}$, $\mathbb{D} = (d_{ij}) = ((-1)^{i+j} \det \mathbb{A}_{ij})$, a kde podmatice $\mathbb{A}_{ij}$ vznikla z $\mathbb{A}$ vyškrtnutím i-tého řádku a j-tého sloupce.

2.3 Definice *Lineární prostor* nad tělesem $(T, +, \cdot)$ je množina L spolu s operací sčítání $\oplus : L \times L \to L$ a číselného násobku $\boxdot : T \times L \to L$ (číselný násobek ovšem není binární operace na množině L!), pro které platí:

- $(L, \oplus)$ je komutativní grupa s neutrálním prvkem $\bar{o}$;
- Pro všechny $\alpha, \beta \in T$ a všechny $\bar{u}, \bar{v} \in L$:
  - $\alpha \boxdot (\bar{u} \oplus \bar{v}) = (\alpha \boxdot \bar{u}) \oplus (\alpha \boxdot \bar{v})$
  - $(\alpha + \beta) \boxdot \bar{u} = (\alpha \boxdot \bar{u}) \oplus (\beta \boxdot \bar{u})$
  - $(\alpha \cdot \beta) \boxdot \bar{u} = \alpha \boxdot (\beta \boxdot \bar{u})$
  - $1 \boxdot \bar{u} = \bar{u}$

Prvky lineárního prostory se nazývají vektory, prvky tělesa jsou skaláry. Operace budeme opět značit jen $\cdot$ a $+$.

Množina všech uspořádaných n-tic ze $\mathbb{Z}_p$, tj. $\mathbb{Z}_p^n = \{\bar{u} = (u_1, \ldots, u_n),\ u_i \in \mathbb{Z}_p\}$, spolu se sčítáním a číselným násobkem definovanými po složkách, $\bar{u} + \bar{v} = (u_1 + v_1, \ldots, u_n + v_n)$, $\alpha \cdot \bar{u} = (\alpha u_1, \ldots, \alpha u_n)$, tvoří lineární prostor nad tělesem $\mathbb{Z}_p$. Budeme mu říkat *lineární prostor všech slov délky n nad $\mathbb{Z}_p$*.
Na tomto prostoru lze definovat *skalární součin* předpisem $\bar{u} \odot \bar{v} = u_1 v_1 + \ldots u_n v_n$ a tudíž zde můžeme mluvit o kolmosti vektorů: $\bar{u} \perp \bar{v}$ právě, když $\bar{u} \odot \bar{v} = 0$.

2.4 *Podprostor* lineárního prostoru je neprázdná podmnožina, která je uzavřená na sčítání a číselné násobky. Podprostor musí vždy obsahovat nulový vektor daného prostoru. Nás budou zajímat především podprostory v lineárním prostoru všech slov délky n nad $\mathbb{Z}_p$.

Jsou dvě možnosti, jak jednoznačně popsat podprostor P v lineárním prostoru $\mathbb{Z}_p^n$. První možnost je zvolit v něm nějakou bázi (tj. generující lineárně nezávislou množinu vektorů v P). Pak v podprostoru P jsou jen ty vektory, které se dají nakombinovat z bázických vektorů:

$$\vec{u} \in P \quad \text{iff} \quad \bar{u} = \sum_{i=1}^{k} \alpha_i \bar{b}_i,$$

kde $B = \{\bar{b}_1, \ldots, \bar{b}_k\}$ je báze podprostoru P a $\dim P = k$.

Druhá možnost je najít takovou homogenní soustavu lineárních rovnic, aby množinou všech jejích řešení byl právě podprostor P. Přitom vektor $\bar{u}$ řeší homogenní soustavu $\mathbb{A}\bar{x}^T = \bar{o}^T$ právě, když $R_i \odot \bar{u} = 0$ pro každý řádek R_i matice $\mathbb{A}$, aneb když jsou všechny řádky matice $\mathbb{A}$ kolmé na vektor $\bar{u}$. Hledaná soustava musí mít v řádcích bázi ortogonálního doplňku k podprostoru P:

$$\vec{u} \in P \quad \text{iff} \quad \vec{u} \text{ řeší soustavu } \mathbb{A}\bar{x}^T = \bar{o}^T \text{ s maticí } \mathbb{A} = \begin{pmatrix} \bar{c}_1 \\ \vdots \\ \bar{c}_{n-k} \end{pmatrix},$$

kde $\bar{c}_1, \ldots, \bar{c}_{n-k}$ tvoří bázi podprostoru $P^\perp$.
Díky tomu, že $(P^\perp)^\perp = P$, můžeme naopak určit vektory $\bar{c}_1, \ldots, \bar{c}_{n-k}$ jako bázi podprostoru všech řešení soustavy $\mathbb{B}\bar{x}^T = \bar{o}^T$, kde v řádcích matice $\mathbb{B}$ jsou bázické vektory $\bar{b}_1, \ldots, \bar{b}_k$ podprostoru P.