Počítání modulo n

1. přednáška z algebraického kódování

Obsah

Množiny s jednou binární operací

Definice

Na množině A je dána binární operace $*$, tj. $*: A \times A \to A$.

- $(A, *)$ se nazývá *pologrupa*, pokud je operace $*$ asociativní, tj. pro každé $x, y, z \in A$ platí $x * (y * z) = (x * y) * z$.
- $(A, *)$ se nazývá *monoid*, pokud je operace $*$ asociativní a má neutrální prvek, tj. existuje $e \in A$ tak, že pro každé $x \in A$ platí $e * x = x = x * e$.
- $(A, *)$ se nazývá *grupa*, pokud je operace $*$ asociativní, má neutrální prvek a má všechny inverzní prvky, tj. pro každé $x \in A$ existuje $y \in A$ tak, že $x * y = e = y * x$.
- Pologrupa, monoid či grupa jsou *komutativní*, pokud je operace $*$ komutativní, tj. pro každé $x, y \in A$ platí $x * y = y * x$.

Množiny se dvěma binárními operacemi

Definice

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

- $(A, +, \cdot)$ se nazývá *okruh*, jestliže
  1. $(A, +)$ je komutativní grupa (neutrální prvek značíme 0);
  2. $(A, \cdot)$ je pologrupa;
  3. 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 v okruhu $(A, +, \cdot)$ násobení komutativní a má-li neutrální prvek (značíme jej 1), mluvíme o *komutativním okruhu s jednotkou*.

Množiny se dvěma binárními operacemi

Definice - pokračování

- $(A, +, \cdot)$ se nazývá *těleso*, jestliže
  1. je to okruh s jednotkou;
  2. každý nenulový prvek má inverzní prvek, tedy $(A - \{0\}, \cdot)$ je grupa;
  3. $0 \neq 1$, tedy neutrální prvek pro sčítání není současně neutrálním prvkem pro násobení.
- Většinou budeme říkat stručně těleso, ale půjde o *komutativní těleso*, tj. násobení bude komutativní.

Pro kódování budeme potřebovat konečná komutativní tělesa.

Věta o dělení se zbytkem

Celá čísla $(\mathbb{Z}, +, \cdot)$ tvoří komutativní okruh s jednotkou, v němž pouze 1 a -1 mají inverzní prvek.

Věta o dělení se zbytkem

Pro každé $a, b \in \mathbb{Z}$, kde $b > 0$, existují jednoznačně určené $q, z \in \mathbb{Z}$ tak, že

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

Věta o dělení se zbytkem

Díky větě o dělení se zbytkem můžeme na celých číslech vystavět následující teorii.

Důsledky věty o dělení se zbytkem

1. relace dělitelnosti, prvočísla
2. největší společný dělitel, Eukleidův algoritmus
3. kongruence modulo n, okruh zbytkových tříd $\mathbb{Z}_n$

Relace dělitelnosti

Definice

Nechť $a, b \in \mathbb{Z}$, řekneme, že a *dělí* b (nebo a je dělitelem b), když existuje $k \in \mathbb{Z}$ tak, že $b = ka$. Značíme $a \mid b$.

Relace dělitelnosti je uspořádáním na $\mathbb{N}$ (tj. reflexivní, antisymetrickou a tranzitivní relací).

Relace dělitelnosti však není antisymetrická na $\mathbb{Z}$, tam má smysl mluvit o *relaci asociovanosti*: $a||b$, pokud $a|b$ a zároveň $b|a$
Platí, že $a||b$ právě, když $b = \pm a$.

Prvočísla

Definice

Přirozené číslo $p \geq 2$ je *prvočíslo*, pokud je dělitelné pouze čísly 1 a p, aneb pokud 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 $p \leq \sqrt{n}$.

Problém testování prvočíselnosti (resp. rozložení čísla n na součin dvou menších čísel) "hrubou silou" má exponenciální časovou složitost v závislosti na počtu cifer čísla n. Musíme vykonat $\sqrt{n} = 2^{\frac{1}{2}\log_2(n)}$ dělení.

Prvočísla

Věta (Eukleid)

Neexistuje největší prvočíslo, aneb prvočísel je nekonečně mnoho.

Tvrzení

Pokud prvočíslo dělí součin dvou čísel, pak dělí aspoň jedno z nich.

Základní věta aritmetiky

Každé přirozené číslo $n \geq 2$ lze jednoznačně (až na pořadí) napsat jako součin mocnin různých prvočísel.

Největší společný dělitel

Definice

Největší společný dělitel dvou čísel $a, b \in \mathbb{Z}$ je takové číslo $d \in \mathbb{Z}$, které splňuje:

1. d dělí obě čísla a i b
2. d je dělitelné všemi společnými děliteli obou čísel
3. $d \geq 0$

Značíme $d = \gcd(a, b)$.

Analogicky lze definovat *nejmenší společný násobek*, $\mathrm{lcm}(a, b)$.

Eukleidův algoritmus

Hledáme $\gcd(a, b)$. Předpokládejme, že $a \geq b > 0$.

1. Podělíme se zbytkem: $a = q\,b + z$ a $0 \leq z < b$
2. Pokud je zbytek $z = 0$, tak je $\gcd(a, b) = b$.
3. Pokud je zbytek $z > 0$, tak 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.

- rekurzivní algoritmus, který se opírá o dělení se zbytkem
- jelikož zbytky jsou celočíselné, nezáporné a stále menší, bude po konečném počtu kroků zbytek nulový (úloha se zastaví)
- časová složitost - počet dělení se zbytkem je lineární v závislosti na počtu cifer menšího čísla

Rozšířený Eukleidův algoritmus

Bezoutova věta

Největší společný dělitel čísel $a, b \in \mathbb{Z}$ je jejich celočíselnou kombinací, aneb

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

K nalezení celočíselných koeficientů $k, l \in \mathbb{Z}$ z Bezoutovy věty lze použít *rozšířený Eukleidův algoritmus*:

- V každém kroku Eukleidova algoritmu přepočítáme aktuální zbytek na kombinaci čísel a, b.
- $\gcd(a, b)$ je posledním nenulovým zbytkem, tudíž jednou nakombinujeme z čísel a, b i jejich největšího společného dělitele.

Diofantické rovnice

Věta

Rovnice $ax + by = c$, kde $a, b, c \in \mathbb{Z}$, má řešení v $\mathbb{Z}$ právě, když $\gcd(a, b) \mid c$.

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

Kongruence modulo n

Definice

Nechť $n \in \mathbb{N}$. Čísla $a, b \in \mathbb{Z}$ jsou *kongruentní modulo n*, pokud $n \mid (b - a)$. Značíme $a \equiv b \pmod{n}$.

Tvrzení

$a \equiv b \pmod{n}$ právě, když čísla a, b mají stejný zbytek po dělení číslem n,

$a \equiv b \pmod{n}$ právě, když $b = a + kn$ pro $k \in \mathbb{Z}$.

Kongruence modulo n

Věta

Relace kongruence modulo n je relace ekvivalence na množině celých čísel (tj. reflexivní, symetrická a tranzitivní relace).

Důsledek

Relace kongruence modulo n rozloží množinu celých čísel na třídy navzájem ekvivalentních prvků, tzv. *zbytkové třídy modulo n*, množinu všech zbytkových tříd modulo n značíme $\mathbb{Z}_n$.

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}, \text{kde } [a]_n = \{a + kn | k \in \mathbb{Z}\}$$

Kongruence modulo n

Věta

Relace kongruence modulo n je zachována při sčítání a násobení:
pokud $a \equiv b \pmod{n}$ i $c \equiv d \pmod{n}$,
pak také $a + c \equiv b + d \pmod{n}$ i $ac \equiv bd \pmod{n}$.

Důsledek

Na množině $\mathbb{Z}_n$ můžeme korektně definovat operace sčítání a násobení přes representanty:

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

Okruh zbytkových tříd $\mathbb{Z}_n$

Díky definici přes representanty zdědí operace $\oplus$ a $\odot$ vlastnosti, které měly operace sčítání a násobení na $\mathbb{Z}$.

Věta

Trojice $(\mathbb{Z}_n, \oplus, \odot)$ tvoří komutativní okruh s jednotkou, který se nazývá *faktorový okruh zbytkových tříd modulo n*.

V dalším textu zjednodušíme značení:

$$(\mathbb{Z}_n = \{0, 1, \ldots, n-1\}, +, \cdot)$$

Lineární rovnice v $\mathbb{Z}_n$

Lineární rovnice $ax = b$ v $\mathbb{Z}_n$ lze převést na diofantickou rovnici následujícími úpravami:

- $ax = b$ v $\mathbb{Z}_n$
- $ax \equiv b \pmod{n}$ v $\mathbb{Z}$
- $ax + ny = b$ v $\mathbb{Z}$

Věta

Lineární rovnice $ax = b$ má řešení v $\mathbb{Z}_n$ právě, když $\gcd(a, n) | b$.

Je-li x_p jedno řešení, pak každé řešení má tvar
$x = x_p + k\ x_0$, kde $x_0 = \frac{n}{\gcd(a,n)}$, $0 \leq k < \gcd(a, n)$.
V okruhu $\mathbb{Z}_n$ tak vznikne celkem $\gcd(a, n)$ různých řešení.

Těleso $\mathbb{Z}_p$

Speciálně rovnice $ax = 1$ bude mít řešení v $\mathbb{Z}_n$ právě, když $\gcd(a, n) = 1$ (řešením bude inverzní prvek a^{-1} v $\mathbb{Z}_n$).

Důsledek

Prvek $a \in \mathbb{Z}_n$ je invertibilní v $\mathbb{Z}_n$ právě, když je a nesoudělné s n.

Věta

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

Umocňování v $\mathbb{Z}_n$

Při sčítání a násobení můžeme čísla nahradit jejich zbytky modulo n.
Můžeme nějak zmenšit exponent při umocňování modulo n?
Čísel v $\mathbb{Z}_n$ je konečně mnoho, výsledky mocnin se musí opakovat:

$$\text{Existují} \quad k > l \in \mathbb{N} \quad \text{tak, že} \quad a^k = a^l.$$

Pokud je a invertibilní v $\mathbb{Z}_n$, získáme odtud $a^{k-l} = 1$. Mocniny čísla a se cyklí s periodou $k - l$.
Jaká je společná perioda pro všechna invertibilní $a \in \mathbb{Z}_n$?

Euler-Fermatova věta

Malá Fermatova věta

Nechť p je prvočíslo.
Pro každé $a \neq 0$ je $a^{p-1} = 1$ v $\mathbb{Z}_p$.

Euler-Fermatova věta

Pro každé $a \in \mathbb{Z}_n$, a nesoudělné s n, je $a^{\varphi(n)} = 1$ v $\mathbb{Z}_n$.

Aneb: Je-li základ nesoudělný s n, můžeme exponent zmenšit modulo $\varphi(n)$.

Euler-Fermatova věta

Eulerova funkce

$\varphi : \mathbb{N} \to \mathbb{N} : \varphi(n) =$ počet čísel mezi 0 až (n-1) nesoudělných s n

Pro výpočet Eulerovy funkce platí následující vzorce:

- $\varphi(p) = p - 1$ pro p prvočíslo
- $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$ pro p prvočíslo a $k \in \mathbb{N}$
- $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$ pro $n, m \in \mathbb{N}$ navzájem nesoudělná

Známe-li prvočíselný rozklad čísla n, umíme spočítat $\varphi(n)$, jinak ne.

Euler-Fermatova věta

Eulerova věta

Nechť $(G, \circ)$ je konečná grupa o n prvcích s neutrálním prvkem 1. Pro každé $a \in G$ platí: $a^n = \underbrace{a \circ a \circ \ldots \circ a}_{n\text{-krát}} = 1$ v G.

Euler-Fermatova věta je speciálním případem Eulerovy věty aplikované na grupu $(\mathbb{Z}_n^*, \cdot)$ invertibilních prvků v monoidu $(\mathbb{Z}_n, \cdot)$.

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n; a \text{ je nesoudělné s } n\}$$

Počet prvků této grupy $|\mathbb{Z}_n^*| = \varphi(n)$, neutrální prvek je 1.

Řád prvku v grupě

Pro každé $a \in G$ platí $a^n = 1$ v n-prvkové grupě G.
Pro dané a ale nemusí být n tím nejmenším exponentem, na který musíme umocnit, aby vyšlo 1.

Definice

Nechť $(G, \circ)$ je konečná grupa s neutrálním prvkem 1, $a \in G$.
Nejmenší přirozené číslo $r > 0$ takové, že $a^r = \underbrace{a \circ a \circ \ldots \circ a}_{r\text{-krát}} = 1$

se nazývá *řád prvku* a v grupě G. Značíme $\mathrm{r}(a)$.

Příklad

$\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8, \}$, $|\mathbb{Z}_9^*| = \varphi(9) = 6$
$\mathrm{r}(8) = 2$, $\mathrm{r}(4) = 3$, $\mathrm{r}(2) = 6$

Řád prvku v grupě

Poznámky

- Definice pojmu řád prvku a v konečné grupě G je smysluplná, podle Eulerovy věty takové číslo existuje a je $\mathrm{r}(a) \leq |G|$.
- V monoidu je situace jiná - pokud prvek a není invertibilní, pak $a^k \neq 1$ pro každé $k \geq 1$ (jinak by pro dané k byl prvek a^{k-1} inverzním prvkem k prvku a).
- Známe-li $\mathrm{r}(a)$ v grupě G, usnadní nám to umocňování: při výpočtu a^k můžeme v exponentu počítat modulo $\mathrm{r}(a)$.
- Je-li grupa aditivní $(G, +)$ s neutrálním prvkem 0, pak řád je nejmenší $r > 0$ takové, že $ra = \underbrace{a + \ldots + a}_{r\text{-krát}} = 0$.

Řád prvku v grupě

-

Tvrzení

Nechť $(G, \circ)$ je konečná grupa, $a \in G$.
Pak $a^k = 1$ v grupě G právě, když $r(a) \mid k$.

Důsledek

Řád prvku $\mathrm{r}(a)$ v konečné grupě G je dělitelem počtu prvků grupy.

Poznámka

Jedná se o důsledek Eulerovy věty (kterou jsme pro komutativní grupy dokázali přímo), a předchozího tvrzení.
V nekomutativním případě se postupuje obráceně: z Lagrangeovy věty se odvodí tvrzení, že řád prvku dělí počet prvků grupy, odtud potom Eulerova věta.

Řád prvku v grupě

Tvrzení

Je-li $\mathrm{r}(a) = r$, pak množina $P = \{a, a^2, a^3, \ldots, a^r = 1\}$ tvoří r-prvkovou podgrupu grupy G. Nazýváme ji *cyklická podgrupa* generovaná prvkem a, značíme ji $P = \langle a \rangle$.

Lagrangeova věta

Počet prvků libovolné podgrupy P (v konečné grupě G) je dělitelem počtu prvků grupy G.

Důsledek

Řád prvku $\mathrm{r}(a)$ v konečné grupě G je dělitelem počtu prvků grupy.

Řád prvku v grupě

Tvrzení

Nechť G je konečná grupa, $a \in G$.

- pokud $d \mid \mathrm{r}(a)$, pak $r(a^d) = \frac{\mathrm{r}(a)}{d}$
- $\mathrm{r}(a^k) = \frac{\mathrm{r}(a)}{\gcd(k,\mathrm{r}(a))}$
- $\mathrm{r}(a^k) = \mathrm{r}(a)$ právě, když $\gcd(k, \mathrm{r}(a)) = 1$
- podgrupa $P = \langle a \rangle$ má celkem $\varphi(\mathrm{r}(a))$ prvků řádu $\mathrm{r}(a)$

Příklad

$\mathbb{Z}_9^* = \langle 2 \rangle$, protože $\mathrm{r}(2) = 6 = |\mathbb{Z}_9^*|$.
Všechny prvky řádu 6 v $\mathbb{Z}_9^*$ jsou tvaru 2^k, kde $\gcd(k, 6) = 1$.
Odtud $k \in \{1, 5\}$ a prvky řádu 6 jsou $2^1 = 2$ a $2^5 = 5$.

Cyklické grupy

Definice

Grupa $(G, \circ)$ se nazývá *cyklická grupa*, pokud pro nějaký prvek $a \in G$ je $G = \langle a \rangle$. Prvek a je *generátor* grupy G.

Tvrzení

- Konečná grupa G o n prvcích je cyklická právě, když obsahuje prvek a řádu $\mathrm{r}(a) = n$.
- Cyklická grupa o n prvcích má celkem $\varphi(n)$ generátorů. Pravděpodobnost, že při náhodné volbě prvku $a \in G$ najdeme generátor, je $\frac{\varphi(n)}{n}$.

Cyklické grupy

Tvrzení - hledání generátoru

Prvek a je generátor konečné grupy G o n prvcích právě, když je splněna některá z podmínek:

- $a^r \neq 1$ pro každé $r < n$, kde $r \mid n$
- $a^r \neq 1$ pro každé $r = \frac{n}{p}$, kde p je prvočíslo a $p \mid n$

Tvrzení

Nechť G je konečná komutativní grupa, $a, b \in G$.
(Resp. nechť $ab = ba$.)

- Pokud jsou $\mathrm{r}(a)$ a $\mathrm{r}(b)$ nesoudělné, pak $\mathrm{r}(ab) = \mathrm{r}(a)\,\mathrm{r}(b)$.

Cyklické grupy

Příklad

Je dána grupa $\mathbb{Z}_{19}^* = \mathbb{Z}_{19} \setminus \{0\}$.

- $|\mathbb{Z}_{19}^*| = \varphi(19) = 18 = 2 \cdot 3^2$. Možné řády jsou $1, 2, 3, 6, 9, 18$.
- Určete $\mathrm{r}(8)$ a použijte ho při výpočtu 8^{195} v $\mathbb{Z}_{19}$:
  $8^2 = 7$, $8^3 = (-1)$, $8^6 = 1$ poprvé, tedy $\mathrm{r}(8) = 6$,
  $8^{195} = 8^3 = 18$ v $\mathbb{Z}_{19}$.
- Najděte generátor v $\mathbb{Z}_{19}^*$:
  Zkusíme $a = 2$: $2^6 = 7 \neq 1$ (odtud také $2^2 \neq 1$, $2^3 \neq 1$),
  $2^9 = -1 \neq 1$, tudíž $\mathrm{r}(2) = 18$ a 2 je generátor v $\mathbb{Z}_{19}^*$.
- Pravděpodobnost trefy do generátoru je $P = \frac{\varphi(18)}{18} = \frac{1}{3}$.

Cyklické grupy

Příklady

- Grupa $(\mathbb{Z}_n, +)$ je cyklická s generátorem 1 pro každé $n \geq 1$.
- Grupa $(\mathbb{Z}_p^*, \cdot)$ je cyklická pro každé p prvočíslo.
- Grupa $(\mathbb{Z}_9^*, \cdot)$ je cyklická s generátorem 2.
- Grupa $(\mathbb{Z}_8^* = \{\pm 1, \pm 3\}, \cdot)$ není cyklická grupa, neboť $a^2 = 1$ pro každé $a \in \mathbb{Z}_8^*$.

Cyklické grupy

Vnitřní struktura cyklických grup

Nechť $G = \langle a \rangle$ je cyklická grupa o n prvcích s neutrálním prvkem 1. Nechť $r \mid n$, tehdy a jen tehdy platí:

1. V grupě G lze nalézt prvek řádu r, například prvek $b = a^k$, kde $k = \frac{n}{r} \in \mathbb{N}$
2. V grupě G je právě jedna podgrupa o r prvcích a to podgrupa $P_r = \langle b \rangle$, kde $\mathrm{r}(b) = r$.
3. Rovnice $x^r = 1$ má v grupě G právě r řešení a jsou to všechny prvky z r-prvkové podgrupy P_r, jsou tedy tvaru $x = b^i$, kde $\mathrm{r}(b) = r$ a $0 \leq i \leq r - 1$.
4. Pro libovolné $k \in \mathbb{N}$ má rovnice $x^k = 1$ v grupě G právě $d = \gcd(k, n)$ řešení a redukuje se na rovnici $x^d = 1$.

Cyklické grupy

Příklad

Řešte rovnici $x^{21} = 1$ v grupě.$\mathbb{Z}_{19}^*$.

- Už víme, že $|\mathbb{Z}_{19}^*| = \varphi(19) = 18$ a 2 je generátor v $\mathbb{Z}_{19}^*$.
- Prvek a řeší rovnici $x^{21} = 1$ právě, když $\mathrm{r}(a) \mid 21$.
  Navíc $a \in \mathbb{Z}_{19}^*$, tudíž $\mathrm{r}(a) \mid 18$. Odtud $\mathrm{r}(a) \mid \gcd(21, 18) = 3$
  a rovnice se redukuje na rovnici $x^3 = 1$.
- Najdeme prvek b řádu 3: $b = 2^{\frac{18}{3}} = 2^6 = 7$.
  Rovnice má tři řešení $x_1 = 7$, $x_2 = 7^2 = 11$, $x_3 = 7^3 = 1$.
- Tyto tři prvky jsou kořeny polynomu $x^3 - 1$ v $\mathbb{Z}_{19}$.
  Protože $(\mathbb{Z}_{19}, +, \cdot)$ je těleso, tak polynom nemůže mít více
  kořenů než je jeho stupeň.