Počítání modulo n

1. a 2. přednáška z kryptografie

Obsah

Množiny s jednou binární operací

Definice

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

- $(A, *)$ 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 $x * y = e = y * x$.
- Grupa $(A, *)$ se nazývá *Abelova grupa*, 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 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 *obor*, jestliže
  1. je to okruh s jednotkou;
  2. je netriviální, tj. $0 \neq 1$ (neutrální prvek pro sčítání není současně neutrálním prvkem pro násobení);
  3. každým nenulovým prvkem $0 \neq a \in A$ lze krátit, tj. pro každé $x, y \in A$ z rovnosti $a \cdot x = a \cdot y$ plyne $x = y$ a také z rovnosti $x \cdot a = y \cdot a$ plyne $x = y$.
- Je-li v oboru násobení komutativní, mluvíme o *oboru integrity*.

Poznámka

Obor lze také definovat jako netriviální okruh s jednotkou, který nemá dělitele nuly, tj. pro každé $a, b \in A$ platí: je-li $a \neq 0$, $b \neq 0$, pak také $a \cdot b \neq 0$.

Množiny se dvěma binárními operacemi

Definice - pokračování

- $(A, +, \cdot)$ se nazývá *těleso*, jestliže
  1. je to okruh s jednotkou;
  2. je netriviální, tj. $0 \neq 1$ (neutrální prvek pro sčítání není současně neutrálním prvkem pro násobení);
  3. každý nenulový prvek má inverzní prvek, tedy $(A - \{0\}, \cdot)$ je grupa.
- Je-li v tělese násobení komutativní, mluvíme o *komutativním tělese*.

Poznámka

Těleso je zřejmě oborem, neboť každým invertibilním prvkem lze krátit.

Množiny se dvěma binárními operacemi

Příklad

Dále nás bude zajímat množina všech celých čísel $\mathbb{Z}$ s operacemi sčítání a násobení.

1. $(\mathbb{Z}, +)$ je Abelova grupa, $(\mathbb{Z}, \cdot)$ je komutativní monoid.
2. $(\mathbb{Z}, +, \cdot)$ tvoří netriviální komutativní okruh s jednotkou,
   - nemá dělitele nuly (lze krátit nenulovými čísly), tedy je to obor integrity,
   - inverzní prvek mají pouze čísla 1 a -1, tedy není to těleso.

Počítání s celými čísly

Věta o dělení se zbytkem

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

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

Důsledky věty o dělení se zbytkem

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

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 $a \mid b$ a zároveň $b \mid a$. Platí, že $a \,||\, b$ právě, když $b = \pm a$.

Prvočísla

Definice

Přirozené číslo $p \geq 2$ je *prvočíslo*, pokud je dělitelné pouze 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. problém faktorizace 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

Základní věta aritmetiky

Každé přirozené číslo $n \geq 2$ lze jednoznačně (až na pořadí) napsat jako součin mocnin různých prvočísel, $n = p_1^{e_1} \cdot \ldots \cdot p_k^{e_k}$.

Existence rozkladu lze dokázat silnou indukcí podle n. K důkazu jednoznačnosti je však potřeba Bezoutova věta. Probereme tedy nejdříve ještě jednu kapitolu.

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*, $\mathrm{lcm}(a, b)$.

Největší společný dělitel

Definice

Pokud je $\gcd(a, b) = 1$, pak říkáme, že a, b jsou *nesoudělná čísla*.

Hledání $\gcd(a, b)$

Známe-li prvočíselný rozklad pro čísla a, b, pak $\gcd(a, b)$ obsahuje právě všechna společná prvočísla ve společných mocninách.
Ovšem najít faktorizaci čísel a, b je exponenciální problém.

Eukleidův algoritmus

Eukleidův algoritmus

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

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

Jde o 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)
- Pokud je zbytek $r > 0$, tak dvojice a, b má stejné společné dělitele jako dvojice b, r. Tedy i $\gcd(a, b) = \gcd(b, r)$.
- Časová složitost - počet dělení se zbytkem je lineární v závislosti na počtu cifer menšího čísla

Eukleidův algoritmus

Eukleidův algoritmus

Vstup: přirozená čísla $a \geq b \geq 0$
Výstup: $d = \gcd(a, b)$
Algoritmus:

- $r \leftarrow a$, $r' \leftarrow b$
- while $r' \neq 0$ do
  - find $q, r'' \in \mathbb{N}$ such that $r = qr' + r''$ and $0 \leq r'' < r'$
  - $r \leftarrow r'$, $r' \leftarrow r''$
  - enddo
- $d \leftarrow r$
- output d

Rozšířený Eukleidův algoritmus

Bezoutova věta

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

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

K nalezení celočíselných koeficientů $s, t \in \mathbb{Z}$ 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.

Rozšířený Eukleidův algoritmus

Rozšířený Eukleidův algoritmus

Vstup: přirozená čísla $a \geq b \geq 0$
Výstup: přirozená čísla d, s, t, kde $d = \gcd(a, b) = sa + tb$

- $r \leftarrow a$, $r' \leftarrow b$
- $s \leftarrow 1$, $t \leftarrow 0$
- $s' \leftarrow 0$, $t' \leftarrow 1$
- while $r' \neq 0$ do
  - find $q, r'' \in \mathbb{N}$ such that $r = qr' + r''$ and $0 \leq r'' < r'$
  - $s'' \leftarrow s - qs'$, $t'' \leftarrow t - qt'$
  - $r \leftarrow r'$, $r' \leftarrow r''$, $s \leftarrow s'$, $s' \leftarrow s''$, $t \leftarrow t'$, $t' \leftarrow t''$
  - enddo
- $d \leftarrow r$
- output d, s, t

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 $d = \gcd(a, b)$.

Diofantické rovnice

Příklad

Řešte v $\mathbb{Z}$ rovnici $105x + 39y = 6$.

Rozšířený Eukleidův algoritmus pro $a = 105$, $b = 39$:

$$\begin{array}{rcl@{\qquad}rcl} 105 &=& 2 \cdot 39 + 27 & 27 &=& a - 2b \\ 39 &=& 1 \cdot 27 + 12 & 12 &=& -a + 3b \\ 27 &=& 2 \cdot 12 + 3 & 3 &=& 3a - 8b \\ 12 &=& 4 \cdot 3 + 0 & 0 &=& -13a + 35b \end{array}$$

$\gcd(105, 39) = 3 \mid 6$, řešení v $\mathbb{Z}$ tedy existuje.
Partikulární řešení $(x_p, y_p) = 2 \cdot (3, -8) = (6, -16)$,
nesoudělné řešení homogenní rovnice $(x_0, y_0) = (-13, 35)$.
Všechna řešení v $\mathbb{Z}$ jsou $(x, y) = (6, -16) + k(-13, 35)$ pro $k \in \mathbb{Z}$.

Prvočíslelný rozklad - faktorizace

Tvrzení

- Pokud $a \mid bc$ a $\gcd(a, c) = 1$, pak $a \mid b$.
- Pokud prvočíslo $p \mid ab$, pak $p \mid a$ nebo $p \mid b$.

Základní věta aritmetiky

Každé přirozené číslo $n \geq 2$ lze jednoznačně napsat jako součin mocnin různých prvočísel:

$$n = p_1^{e_1} \cdot \ldots \cdot p_k^{e_k} = \prod_{i=1}^{k} p_i^{e_i},$$

kde $p_1 < \ldots < p_k$ jsou prvočísla, $e_i \geq 1$ pro $1 \leq i \leq k$, $k \geq 1$.
Mluvíme o jednoznačné *faktorizaci čísla n na prvočísla*.

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

Následující tvrzení jsou ekvivalentní:

- $a \equiv b \pmod{n}$
- a, b mají stejný zbytek po dělení číslem n
- $b = a + kn$ 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 $\odot$ většinu vlastností, 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 $\gcd(a, n) \mid b$.

Je-li x_p jedno řešení, pak každé řešení má tvar $x = x_p + kx_0$, kde $x_0 = \frac{n}{\gcd(a,n)}$.
V okruhu $\mathbb{Z}_n$ tak vznikne celkem $\gcd(a, n)$ různých řešení.

Hledání inverzních prvků v $\mathbb{Z}_n$

Důsledek

Rovnice $ax = 1$ bude mít řešení v $\mathbb{Z}_n$, právě když $\gcd(a, n) = 1$.
Řešením rovnice bude inverzní prvek k prvku a v $\mathbb{Z}_n$.
K nalezení a^{-1} budeme používat rozšířený Eukleidův algoritmus.

Tvrzení

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

V okruhu $\mathbb{Z}$ měli inverzní prvek pouze čísla ± 1.
V okruhu $\mathbb{Z}_n$ mají inverzní prvek všechna čísla nesoudělná s n, speciálně pro $n = p$ prvočíslo jsou to úplně všechny nenulové prvky.

Těleso zbytkových tříd $\mathbb{Z}_p$

Věta

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

Příklad

V $\mathbb{Z}_5$ je $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$.

Poznámka

Je-li n složené číslo, pak okruh $(\mathbb{Z}_n, +, \cdot)$ není ani obor integrity, protože každé číslo soudělné s n je dělitelem nuly.

Například rovnice $2x = 4$ má v $\mathbb{Z}_6$ dvě řešení $x_1 = 2$, $x_2 = 5$, aneb prvkem $a = 2$ nelze v $\mathbb{Z}_6$ krátit.

Počítání modulo n

Literatura

- Velebil: Diskrétní matematika. Kapitoly 2.1-3, 3.1 a 3.4. ftp://math.feld.cvut.cz/pub/velebil/y01dma/dma-notes.pdf
- Shoup: A Computational Introduction to Number Theory and Algebra. Kapitoly 1.1-3, 2.1-3, 2.5. http://shoup.net/ntb/