Bi2011

Teoretické základy informatiky

Teorie čísel

Created by Miroslav Kubásek

Úvod

- Seznámíme se se základními termíny z teorie čísel, pojmy faktorizace, dělitelnost, nejmenší společný násobek.
- Dále pak s modulární aritmetikou, číselnými soustavami o různých základech a se způsobem uložení čísel ve tvaru dvojkového doplňku.

Motivace

- V informatice a algoritmizaci se hojně využívá množin „čísel“ a s čísly se také pomocí základních aritmetických operací manipuluje.
- Z teorie čísel vyplývá i notace hojně používaná v informatice.
- Důležité je také pochopit, jak jsou čísla v počítačích reprezentována a jaká z toho plynou omezení při výpočtech.

Celá čísla

termíny které známe

- **Přirozené číslo**
  - $1, 2, 3, 4, \ldots, \ldots, 101, 102, \ldots, n, \ldots$
- **Nula** 0
  - definujeme jako: $0 + n = n + 0 = n$
- **Záporné číslo** $-n$
  - definujeme jako: $n + (-n) = (-n) + n = 0$

Celá čísla

definice celých čísel

- Množinu přirozených čísel, záporných čísel a nuly souhrnně nazýváme celá čísla
- V matematice označujeme jako $\mathbb{Z}$ *(Zahlen - německy čísla)*
- V informatice používáme termín **`integer`**, případně **`positive integer`** a **`negative integer`**

Celá čísla

co to je uzavřenost množiny?

- To že je množina M uzavřená na nějakou operaci $\otimes$ se v teorii čísel vyskytuje velmi často a znamená to, že když tuto operaci aplikujeme na libovolné prvky z množiny $\mathbb{M}$, tak výsledek bude také náležet do množiny $\mathbb{M}$.
- Uzavřenost definujeme $\forall x, y \in \mathbb{M} : x \otimes y = z \in \mathbb{M}$

Celá čísla

uzavřenost

- Množina celých čísel je uzavřená na operaci **sčítání** a **násobení**
- Oproti přirozeným číslům je množina celých čísel uzavřená i pro odčítání
- Není uzavřena na dělení!!!

> *Přirozeným číslem (číslem z oboru přirozených čísel) se v matematice rozumí kladné celé číslo (1, 2, 3, …).*
>
> *V oborech jako matematická logika, teorie množin a informatika se mezi přirozená čísla počítá i nula, což však v teorii čísel může vést k potížím. Pokud by mohlo dojít k nejasnostem, budeme množinu celých kladných čísel včetně nuly značit $\mathbb{Z}^0$, a pro kladná celá čísla budeme používat označení $\mathbb{Z}^+$.*

Celá čísla

základní vlastnosti množiny celých čísel

1. $a + b = b + a$ - **komutativní zákon**
2. $a * b = b * a$ - **komutativní zákon**
3. $a + (b + c) = (a + b) + c$ - **asociativní zákon**
4. $a * (b * c) = (a * b) * c$ - **asociativní zákon**
5. $a + 0 = a$ - **existence neutrálního prvku**
6. $a * 1 = a$ - **existence neutrálního prvku**
7. $a + (-a) = 0$ - **existence inverzního prvku**
8. $a * (b + c) = (a * b) + (a * c)$ - **distributivní zákon**
9. Pro ušetření místa budeme psát a^k ako zkratku pro vynásobení čísla a samo sebou k-krát. Bude tedy platit, že $3^4 = 3 * 3 * 3 * 3$ a $2^1 0 = 1024$
10. $a^n * a^m = a^{n+m}$
11. $n^0 = 1$

Faktorizace a prvočísla

faktorizace

- faktorizace se v teorii čísel označuje problém rozložení čísla na součin menších čísel, v nejčastější podobě pak rozklad celého čísla na součin prvočísel

> *Například číslo $\boldsymbol{15}$ lze napsat jako součin $\boldsymbol{3 * 5}$*

- Obecněji lze rozkládat i jiné algebraické objekty, např. polynom druhého řádu $x^2 - 4$ lze vyjádřit jako součin dvou polynomů prvního řádu $(x-2)(x+2)$.

> *Rozklad celého čísla na prvočinitele je považován za velmi těžkou úlohu a na její nezvládnutelnosti pro velká čísla jsou založeny některé kryptografické metody, např. algoritmus RSA pro šifrování s veřejným klíčem.*

Faktorizace a prvočísla

prvočísla

- Ne všechna celá čísla lze rozdělit na prvočinitele.
- Ty, které nelze, jako např. $3, 5, 7, 11, 13, \ldots, 2216091 - 1$ jsou právě prvočísla.

> *Prvočísla jsou jak pro informatiky, tak i pro matematiky velmi fascinujícími objekty. Existují i vědní obory, které hledají nová prvočísla a snaží se najít nové či vylepšit stávající postupy pro rychlejší faktorizaci velkých čísel.*

Dělitelnost

- Celé číslo p je dělitelné nenulovým celým číslem q (číslo q dělí p), jestliže existuje takové celé číslo k, pro které platí, že $p = k * q$.

  *Např. číslo 27 je dělitelné třemi, neboť 27 = 9 * 3.*

- Číslo q se nazývá dělitel čísla p, zapisujeme $p|q$.

  Alternativně můžeme říci, že je p dělitelné q, jestliže zbytek po dělení p/q je nula.

Dělitelnost

známá fakta

1. Jako **triviální dělitele** $a \in \mathbb{Z}$ označujeme čísla 1 a číslo a samotné
2. Celé číslo c je **společným dělitelem** celých čísel a a b jestliže $c|a$ a zároveň $c|b$
3. **Prvočíslo** je číslo ≥ 2, které nemá jiné dělitele než triviální
4. Číslo, které není prvočíslem, nazýváme **číslem složeným**
5. Každé celé číslo ≥ 2 je buď prvočíslo, nebo se dá zapsat jako **součin prvočísel**

Dělitelnost

základní pojmy

- a(mod b)

Definice: *Jestliže* $a, b \in \mathbb{Z}$ *a* $b \geq 1$*, pak dělení čísla* a *číslem* b *dává čísla* q *(podíl) a* r *(zbytek) taková, že* $a = q * b + r$*, kde* $0 \leq r < b$*. Čísla* q *a* r *jsou jednoznačná. Zbytek po dělení budeme značit také* ***a(mod b)****.*

- Kanonický tvar

Definice: *Každé celé číslo* $n \geq 2$ *se dá zapsat jednoznačně (až na pořadí) v kanonickém tvaru* $n = p_1^{a_1} * p_2^{a_2} * \ldots * p_k^{a_k}$*, kde* $p_1, p_2, \ldots, p_k$ *jsou navzájem různá prvočísla a* $a_1, a_2, \ldots, a_k$ *jsou celá kladná čísla.*

Dělitelnost

příklad: Vyjádřete v kanonickém tvaru číslo 2394

1. $2394/2 = 1197$ - číslem 2 již nelze dělit, zkusíme dále dělení číslem 3
2. $1179/3 =$399$
3. $399/3 = 133$ - číslem 3 již nelze dělit, číslem 5 také ne , zkusíme dělení číslem 7
4. $133/7 = 19$ - číslo 19 je již prvočíslo, výsledek tedy bude $2394 = 2 * 3 * 3 * 7 * 19$

Příklady na procvičení:

Vyjádřete v kanonickém tvaru čísla $3600, 4864, 3458$

Dělitelnost

základní pojmy - pokračování

- NSD

Definice: *Kladné celé číslo d je největším společným dělitelem (dále jen NSD, anglicky GCD - greatest common divisor) celých čísel a a b, když platí:*

1. d *je společný dělitel celých čísel* a *a* b.
2. *Jestliže nějaké celé číslo* d_1 *dělí obě čísla* a *a* b, *pak* d_1 *dělí také* d.

- Nesoudělná čísla

Definice: *Dvě celá čísla jsou nesoudělná (relatively prime), když jejich NSD je* 1

Dělitelnost

Euklidův algoritmus

- Euklidův algoritmus slouží k nalezení NSD dvou čísel.

```
function nsd(a, b) {
    var c;
    while (b != 0) {
        c = b;
        b = a mod b;
        a = c;
    }
    return a;
}
```

příklad: Použijte Euklidův algoritmus pro čísla 72 a 246

1. $246 = 3 * 72 + 30$ *(246 mod 72 = 30)*
2. $72 = 2 * 30 + 12$ *(72 mod 30 = 12)*
3. $30 = 2 * 12 + 6$ *(30 mod 12 = 6)*
4. $12 = 2 * 6 + 0$ NSD*(72, 246) = 6*

Dělitelnost

základní pojmy - pokračování

- NSN

Definice: Kladné celé číslo d je nejmenším společným násobkem (dále jen NSN, anglicky LCM - least common multiple) celých čísel $\boldsymbol{a}$ *a* $\boldsymbol{b}$ *když platí:*

1. $\boldsymbol{a|d}$ *a zároveň* $\boldsymbol{b|d}$.
2. *Jestliže* $\boldsymbol{a|d_1}$ *a* $\boldsymbol{b|d_1}$, *pak* $\boldsymbol{d|d_1}$ *pro nějaké celé číslo* $\boldsymbol{d_1}$.

- Jestliže a a b jsou kladná celá čísla, pak $NSN(a,b) = a * b/NSD(a,b)$.

Např.:
$$NSN(12,18) = 12 * 18/NSD(12,18) = 36$$

Dělitelnost

NSD, NSN - příklad

Je snadné nalézt NSD a NSN dvou celých čísel ≥ 2, *pokud je vyjádříme v kanonockém tvaru:*

$$300 = 22 * 31 * 52$$

$$18 = 21 * 32$$

$$NSD(300, 18) = 21 * 31 * 50 = 6$$

$$NSN(300, 18) = 22 * 32 * 52 = 900$$

Modulární aritmetika

úvod

- Obecnější a zajímavější než zkoumat dělitelnost čísel, je zajímavé zkoumat zbytek při dělení.
- Na rozdíl od běžné aritmetiky je modulární aritmetika definována na konečné množině $\mathbb{Z}_n$.
- Ta vznikne ze $\mathbb{Z}$ tak, že jsou ztotožněna čísla se stejným zbytkem po dělení číslem n.
- Někdy se této aritmetice říká **aritmetika zbytkových tříd**.

Modulární aritmetika

základní pojmy

- a mod n ($b(mod\ n)$)

Definice: *Uvažujme celá čísla* a *a* b *a přirozené číslo* $n(a, b \in Z, n \in N)$ *a označme symbolem* ***"a mod n"*** *zbytek při dělení čísla* a *číslem* n.

Příklad: *V programovacích jazycích se pro výpočet zbytku po dělení používá právě operace mod. Například:*

$25 mod 4 = 1$ *- protože* $25/4 = 6$ *a zbytek je* 1

$19 mod 5 = 4$ *- protože* $19 = 3 * 5 + 4$

$24 mod 5 = 4$

Modulární aritmetika

základní pojmy - pokračování

- kongurence

Definice: *Řekneme, že* a *je kongruentní s* b **modulo** n*, pokud* $a \bmod n = b \bmod n$*. Jinými slovy, zbytek při dělení* a/n *a* b/n *je tentýž. Píšeme pak* $a \equiv b \bmod n$*.*

Dále pak platí že: $a \equiv b \bmod n \leftrightarrow n \text{ dělí } (a-b)$

Příklad:

$$53 \bmod 7 = 4$$

$$53 \equiv 4 \bmod 7$$

Modulární aritmetika

clock arithmetic

Všem známé užití modulární aritmetiky je například ve 12-hodinovém určování času. Den je rozdělen na dva 12-ti hodinové úseky. Jestliže je nyní čas 7:00, pak o 8 hodin později to bude 3:00.

Obvyklým sčítáním by nám ale vyšlo že by mělo být 7 + 8 = 15 hodin. Vzhledem ale k tomu že je k dispozici pouze 12 hodinových úseků, tak se čas vždy ve 12 hodin začne počítat od začátku.

Vzhledem k tomu, že se hodiny začnou počítat od začátku vždy ve 12 hodin, tak v tomto případě můžeme mluvit o aritmetice modulo 12.

Díky tomu se můžete u modulární aritmetiky setkat s označením ***Clock arithmetic****.*

Modulární aritmetika

základní vlastnosti kongurence

Pro všechna a, b, a1, b1, c ∈ Z platí:

1. $a \equiv b (mod\ n)$ právě tehny, když zbytek po dělení čísel a i b číslem n je stejný
2. $a \equiv a (mod\ n)$ pro $\forall a \in \mathbb{Z}$ - **reflexivita**
3. Jestliže $a \equiv b (mod\ n) \rightarrow b \equiv a (mod\ n)$ - **symetrie**
4. Jestliže $a \equiv b (mod\ n)$ a $b \equiv c (mod\ n)$, potom $a \equiv c (mod\ n)$ - **tranzitivita**
5. Jestliže $a \equiv a_1 (mod\ n)$ a $b \equiv b_1 (mod\ n)$, potom $a + b \equiv a_1 + b_1 (mod\ n)$

Modulární aritmetika

zbytkové třídy

- Z předchozího vidíme, že relace **kongruence** je **ekvivalencí**, protože je **reflexivní**, **symetrická** a **tranzitivní**.
- Třída ekvivalence celých čísel a je množina všech celých čísel kongruentních s a $modulo$ n.
- Vidíme, že pro dané n relace kongruence a $modulo$ n dělí množinu $\mathbb{Z}$ na třídy ekvivalence, na tzv. **zbytkové třídy modulo n**.

Definice: *Nechť je dáno* $n > 0$. *Pro každé celé číslo* a *definujeme* $[a]_n = x | x \equiv a (mod\ n)$ *jako množinu celých čísel kongruentních* a $modulo$ n *a nazveme ji množinou zbytkových tříd* $modulo$ n *- značíme* $\mathbb{Z}_n$.

Modulární aritmetika

zbytkové třídy - pokračování

Definice: *Nechť* $a \in Z_n$. ***Multiplikativní inverzní prvek*** *k prvku* $a \bmod n$ *je číslo* $x \in Z_n$ *takové, že* $a * x \equiv 1 (\bmod n)$. *Pokud takové* x *existuje, pak je jednoznačné. Inverzní prvek k* $a \bmod n$ *označujeme* a^{-1}.

Definice: *Nechť* $a \in Z_n$. *Dělení čísla* a *číslem* b *modulo* n *je definováno jako součin* $a * b^{-1}$ *modulo* n *je definováno jen tehdy, je-li* b *invertovatelné* $\bmod n$.

Definice: *Nechť* $a \in Z_n$. ***Aditivní opačný prvek*** *k prvku* a *modulo* n *je číslo* $x \in \mathbb{Z}_n$ *takové, že* $a + x \equiv 0 (\bmod n)$. *Pokud takové* x *existuje, je jednoznačné. Opačný prvek k* a *modulo* n *budeme označovat* $-x$.

Modulární aritmetika

zbytkové třídy - příklady

- Každé číslo ze $\mathbb{Z}_n$ reprezentuje zbytkovou třídu. Nechť $n = 7$, zbytkové třídy $modulo$ 7 označme jako $[0]_7, [1]_7, \ldots, [6]_7$, pak $[2]_7 = \ldots, -12, -5, 2, 9, 16, \ldots$.
- **Příklad:** Nechť $n = 9$, $\mathbb{Z}_n = 0, 1, 2, 3, 4, 5, 6, 7, 8$. Určete invertovatelné prvky.

> ***Řešení:*** *Invertovatelné jsou prvky $1, 2, 4, 5, 7, 8$, např. $5 - 1 = 2$, protože $5 * 2 \equiv 1 (mod\ 9)$*

- **Příklad**: Kolik je $3^8 (mod\ 7)$?

> *Řešení:*
>
> - $3^8 \equiv 3^4 * 3^4 \equiv (81 (mod\ 7)) * (81 (mod\ 7)) \equiv 4 * 4 = 16 \equiv 2 (mod\ 7)$

Racionální a reálná čísla

Racionální číslo

- Racionální číslo je číslo, které lze vyjádřit jako zlomek, tj. podíl dvou celých čísel, většinou zapsaný ve tvaru a/b, kde b není nula.
- Číslo a označujeme jako čitatel a číslo b jako jmenovatel.
- Každé racionální číslo lze vyjádřit nekonečně mnoha zlomky (např. $1/2 = 2/4 = 3/6$...).
- Nejjednodušší je tvar, kde jsou čísla a a b nesoudělná a b je kladné.
- Každé racionální číslo má tento základní tvar dán jednoznačně.
- Množinu všech racionálních čísel značíme $\mathbb{Q}$.

Racionální a reálná čísla

Reálné číslo

- Reálná čísla jsou taková čísla, kterým můžeme jednoznačně přiřadit body nekonečné přímky (číselné osy) tak, aby tato čísla popisovala „vzdálenost“ od nějakého vybraného bodu (nuly) na takové přímce.
- Tato nula pak přirozeně dělí reálná čísla na kladná a záporná.
- Množinu všech reálných čísel označujeme $\mathbb{R}$.
- Reálné číslo, které není racionální, se nazývá iracionální číslo.
- Iracionální čísla jsou např. $\sqrt{2}$ nebo π.

Číselné soustavy

úvod

- Pravidla pro zápis čísla pomocí číslic nazýváme číselnou soustavou.
- Z běžného života známe například soustavu desítkovou, šedesátinnou (čas) či římskou.
- Obecně můžeme vyjádřit pravidlo zápisu čísla v soustavě mnohočlenem (polynomem):

$xm * g^m + . . . + x_1 * g^1 + x_0 * g^0 + x{-1} * g^{-1} + . . . + x_{-n} * g^{-n}$

Např.:

$$3542,395(10) = 3 * 10^3 + 5 * 10^2 + 4 * 10^1$$
$$+2 * 10^0 + 3 * 10^{-1} + 9 * 10^{-2} + 5 * 10^{-3}$$

Číselné soustavy

úvod pokračování

- Každá číselná soustava, která zobrazuje čísla pomocí mnohočlenu (polynomu), se nazývá polyadická (polynomická) číselná soustava o základu g (desítková soustava má základ 10).
- Počítače mají však logické obvody, které pracují se dvěma logickými stavy (zapnuto $= 1$, vypnutu $= 0$), a proto je základem dnešních počítačů technologie založená na soustavě dvojkové.

Číselné soustavy

dvojková (binární) soustava

- je polyadická číselná soustava o základu g = 2.
- Dvojková soustava používá pouze dvě číslice, nulu a jedničku, ale i tak lze zobrazit ve dvojkové soustavě jakékoliv číslo (i když někdy nepřesně).
- Těmito prostými číslicemi zvanými bity (z anglického výrazu pro dvojkovou číslici – BInary digiT) lze vyjádřit jakékoli číslo tím, že ho rozložíme na součet postupných mocnin se základem 2, tj. na čísla: 20 = 1, 21 = 2, 22 = 4, 23 = 8, 24 = 16, atd.
- Pokud se při tomto rozkladu příslušná mocnina v daném řádu vyskytuje, zapisujeme ji jako 1, chybí-li píšeme 0.

Číselné soustavy

další číselné soustavy

- Osmičková (oktalová) soustava je polyadická číselná soustava o základu $g = 8$. Používá osm číslic: $0, 1, 2, 3, 4, 5, 6, 7$.
- Desítková (dekadická) soustava je polyadická číselná soustava o základu $g = 10$. Používá číslice $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$.
- Šestnáctková (hexadecimální) soustava je polyadická číselná soustava o základu $g = 16$. Používá šestnáct číslic (znaků): $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$ (místo $10, 11, 12, 13, 14, 15$). Šestnáctková soustava se používá například pro zápis barvy v HTML kódu. Je to v podstatě zkrácená forma zápisu dvojkové soustavy.

Číselné soustavy

příklady

- Převod z desítkové do dvojkové soustavy
- Převod z dvojkové do desítkové soustavy
- Převod desetinných čísel
- Převod do jiných soustav
- Aritmetické operace s binárními čísly
  - Sčítání binárních čísel
  - Odčítání binárních čísel
  - Násobení binárních čísel

Dvojkový doplněk

- Dvojkový doplněk je způsob kódování celého záporného čísla v binární soustavě. Dvojkový doplněk umožňuje zjednodušit konstrukci aritmeticko-logické jednotky uvnitř procesoru, protože není nutné implementovat speciální strojovou instrukci pro odečítání. Odečítání lze pomocí dvojkového doplňku realizovat pomocí operace sčítání.

Příklad: Vytvořte dvojkový doplněk čísla 10110_2*, pracujeme-li s osmibitovým vyjádřením čísla.*

Řešení:

Zarovnáme počet bitů čísla na osm: ***00010110***

Provedeme negaci: ***11101001***

Přičteme jedničku: ***11101010***

Výsledkem je tedy číslo: 11101010_2

Konec