Fakulta přírodovědně humanitní a pedagogická, Technická univerzita v Liberci

Matematika pro informatiky I

Doc. RNDr. Miroslav Koucký, CSc.

Liberec, 2016

Obsah

Předmluva

Skriptum Matematika pro informatiky I je určeno především pro studenty informatický zaměřených oborů. Cílem je podat zjednodušenou formou přehled základních matematických témat, která nachází uplatnění v oblasti informačních technologií, zejména v oblasti šifrování a kódování.

Na toto skriptum navazuje skriptum Matematiky pro informatiky II obsahující vybraná témata z teorie kódování, bezeztrátové komprese a kryptologie.

1. Matematické základy

Mezi základní pojmy, které budeme používat (ale nebudeme je zcela exaktně definovat), patří neuspořádaná, resp. uspořádaná n-tice. Neuspořádanou n-tici rozumíme libovolnou množinu obsahující právě n prvků (tj. nezáleží na pořadí, ve kterém jsou prvky uvedeny). Neuspořádanou n-tici budeme značit $\{a_{i1}, .., a_{in}\}$. V případě uspořádané n-tice záleží na pořadí prvků a budeme ji značit $(a_{i1}, .., a_{in})$.

1. 1. Kartézský součin, relace, zobrazení

Definice - kartézský součin

Nechť A, B jsou neprázdné množiny. Kartézský součin množin A, B budeme značit $A \times B$ a definujeme ho jako množinu všech uspořádaných dvojic (a, b), kde $a \in A, b \in B$, tj.

$$A \times B = \{(a, b) | a \in A, b \in B\}.$$

Poznámky

- Je-li $A \neq B$, potom $A \times B \neq B \times A$, tj. kartézský součin není komutativní.
- Jsou-li A, B konečné množiny, potom platí $|A \times B| = |A| \cdot |B|$.
- V případě, kdy $A = B$, používáme obvykle místo zápisu $A \times A$ zápis A^2 a mluvíme o druhé kartézské mocnině množiny A.

Definice – (binární) relace

Nechť je $A \neq \emptyset$ množina. Binární relací na množině A rozumíme libovolnou podmnožinu A^2.

Poznámky

- Binární relace budeme značit písmeny R, S, T apod. Dále je dobré si uvědomit, že binární relaci tvoří uspořádané dvojice prvků (které jsou v relaci). Skutečnost, že uspořádaná dvojice (a, b) patří do relace R budeme (v závislosti na kontextu) zapisovat $(a, b) \in R$, resp. aRb. Druhý způsob zápisu je běžně používán u některých známých relací. Píšeme např. $a = b, a \leq b, A \subseteq B$, místo méně obvyklého $(a, b) \in =, (a, b) \in \leq, (A, B) \in \subseteq$.
- Relaci na konečné množině lze zadat výčtem všech jejich prvků nebo pomocí matice sousednosti (resp. orientovaného grafu).
  Je-li R relace na konečné množině $A = \{a_1, \ldots, a_n\}$, tj. $R \subseteq A^2$, potom matice sousednosti $M_R = \left(m_{ij}\right)_{i,j=1}^{n}$ relace R je definována následovně: $m_{ij} = \begin{cases} 1, & \left(a_i, a_j\right) \in R \\ 0, & \left(a_i, a_j\right) \notin R \end{cases}$.
- Pro následující speciální relace se vžilo označení:
  $I_A = \Delta_A = \{(a, a) | a \in A\}$ … tvz. diagonální relace na A (diagonála A), resp. identita na A,
  A^2 … tzv. úplná relace na A.
- Jsou-li $R \subseteq A \times B, S \subseteq B \times C$ relace, potom symbolem $R \circ S$ označujeme relaci
  $$\{(a, c) | \exists b \in B \ (a, b) \in R \ \wedge \ (b, c) \in S\},$$
  kterou nazýváme složení relací R a S (v tomto pořadí). Zřejmě $R \circ S \subseteq A \times C$.
- Je-li $R \subseteq A \times B$, potom symbolem R^{-1} označujeme inverzní relaci k relaci R definovanou vztahem $R^{-1} = \{(b, a) | (a, b) \in R\}$. Zřejmě platí $R \circ R^{-1} \subseteq I_A, R^{-1} \circ R \subseteq I_B$.

Definice – vlastnosti relací

Nechť R je relace na množině A. Řekneme, že R je:

a) reflexivní relace na A, jestliže

$$\forall a \in A \ \ (a,a) \in R,$$

b) symetrická relace na A, jestliže

$$\forall a,b \in A \ \ (a,b) \in R \rightarrow (b,a) \in R,$$

c) antisymetrická relace na A, jestliže

$$\forall a,b \in A \ \ (a,b) \in R \wedge (b,a) \in R \rightarrow a = b,$$

d) tranzitivní relace na A, jestliže

$$\forall a,b,c \in A \ \ (a,b) \in R \wedge (b,c) \in R \rightarrow (a,c) \in R.$$

e) trichotomická relace na A, jestliže

$$\forall a,b \in A \ \ (a,b) \in R \vee (b,a) \in R \vee a = b.$$

Poznámky

Je-li R relace na množině A, potom snadno nahlédneme, že platí:

a) R je reflexivní na A právě když $I_A \subseteq R$; b) R je symetrická na A právě když $R^{-1} = R$; c) R je antisymetrická na A právě když $R \cap R^{-1} \subseteq I_A$; d) R je tranzitivní na A právě když $R \circ R \subseteq R$.

V následující tabulce je uveden přehled vlastností základních, obecně známých relací.

množina	relace	reflexivní	symetrická	antisym.	tranzitivní
$A \neq \emptyset$ (neprázdná množina)	$=$	ano	ano	ano	ano
$A \neq \emptyset$ (neprázdná množina)	$\neq$	ne	ano	ne	ne
R (reálná čísla)	$\leq$	ano	ne	ano	ano
R (reálná čísla)	$<$	ne	ne	ano	ano
Z (celá čísla)	$\equiv_m$ (kongruence mod m)	ano	ano	ne	ano
N^+ (kladná přirozená čísla)	$b \mid a$ (b dělí a beze zbytku)	ano	ne	ano	ano
libovolný systém množin	$\subseteq$	ano	ne	ano	ano
libovolný systém množin	$\subset$	ne	ne	ano	ano

V další části využijeme následující dva základní typy relací - relaci ekvivalence a relaci uspořádání.

Definice – relace ekvivalence

Nechť R je relace na A. Řekneme, že R je relace ekvivalence na A, jestliže je reflexivní, symetrická a tranzitivní.

Poznámky

- Je-li R ekvivalence na $A \neq \emptyset$, potom symbolem $[a]$ označujeme třídu ekvivalence určenou reprezentantem $a \in A$. Je definována vztahem $[a] = \{b \mid (a,b) \in R\}$ a tvoří ji tedy všechny prvky ekvivalentní s a.
- Systém množin $B_1, \ldots, B_k$ definuje rozklad množiny $A \neq \emptyset$, jestliže:

  a) $\forall i \neq j \ \left(B_i \cap B_j = \emptyset\right)$ (tzv. disjunktnost po dvou), b) $B_1 \cup \ldots \cup B_k = A$.

  Množiny $B_1, \ldots, B_k$ nazýváme třídy rozkladu.

- Každá ekvivalence na množině definuje její rozklad a obráceně. Třídy ekvivalence zřejmě splývají s třídami rozkladu.

Definice – relace uspořádání, poset

Nechť R je relace na A. Řekneme, že R je relace (částečného) uspořádání na A, jestliže je reflexivní, antisymetrická a tranzitivní. Uspořádanou dvojici (A, R) nazýváme (částečně) uspořádanou množinou, resp. posetem (partially ordered set).

Poznámka

- Je dobré si uvědomit, že v relaci uspořádání nemusí být každé dva prvky „porovnatelné“ (tj. relace uspořádání není obecně trichotomická). Např. níže uvedená relace býti dělitelem, resp. následující příklad.
- Důležitým příkladem uspořádané množiny je $(N^+, |\ )$, kde | označuje relaci „býti dělitelem“.

Definice - předchůdce, následník, minimální, nejmenší, maximální, největší prvek

Nechť $(A, \preccurlyeq)$ je poset. Řekneme, že:

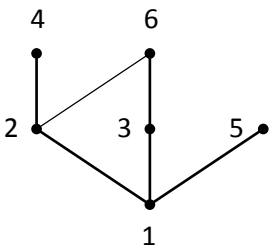
- Prvek $a \in A$ je předchůdce prvku $b \in A$ (resp. b je následník prvku a), jestliže
$$(a \preccurlyeq b) \wedge \big((a \preccurlyeq c \preccurlyeq b) \rightarrow (c = a) \vee (c = b)\big).$$
- Prvek $a \in A$ je minimální prvek A, jestliže
$$(\forall b \in A)\ (b \preccurlyeq a \rightarrow b = a).$$
- Prvek $a \in A$ je nejmenší prvek A, jestliže
$$(\forall b \in A)\ (a \preccurlyeq b).$$
- Prvek $a \in A$ je maximální prvek A, jestliže
$$(\forall b \in A)\ (a \preccurlyeq b \rightarrow b = a).$$
- Prvek $a \in A$ je největší prvek A, jestliže
$$(\forall b \in A)(b \preccurlyeq a).$$

Pokud existuje nejmenší/největší prvek dané množiny, je určen jednoznačně.

Ke grafickému znázornění uspořádaných množin lze užít Hasseův diagram. Jde o nákres grafu, jehož množinu uzlů tvoří prvky množiny A a hrany spojují pouze předchůdce a následníky. Při kreslení je třeba dodržet pravidlo - je-li a předchůdce b, potom a nakreslíme níže než b.

Příklad

Nakreslete Hasseův diagram následujících uspořádaných množin a rozhodněte o existenci minimálních, maximálních prvků, největšího a nejmenšího prvku.



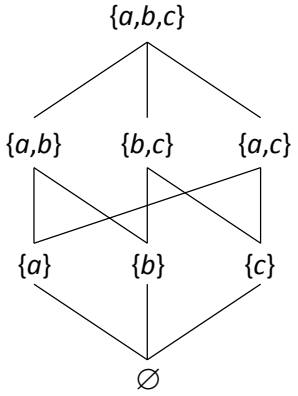
- Uspořádaná množina $(A, |\ )$, kde $A = \{1,2,3,4,5,6\}$ a | je relace „býti dělitelem“.

  Z Hasseova diagramu snadno zjistíme, že:

  1 je nejmenší prvek a tedy i jediný minimální prvek,

  4, 5, 6 jsou maximální prvky a tedy neexistuje největší prvek.

- Uspořádaná množina $(P(A), \subseteq)$, kde $P(A)$ je potenční množina množiny $A = \{a, b, c\}$ a $\subseteq$ je relace býti podmnožinou.
  Z Hasseova diagramu snadno zjistíme, že $\emptyset$ je nejmenší prvek a tedy i jediný minimální prvek, $\{a, b, c\}$ je největší a tedy i jediný maximální prvek.



Definice – lineárně uspořádaná množina

Nechť $\preccurlyeq$ je relace uspořádání na A taková, že $\forall a, b \in A \ \ (a \preccurlyeq b) \vee (b \preccurlyeq a)$, tj. libovolné dva prvky jsou porovnatelné. Potom řekneme, že $\preccurlyeq$ je lineární uspořádání na A a dvojici $(A, \preccurlyeq)$ nazýváme lineárně uspořádanou množinou.

Poznámky

- Alternativně se místo pojmu lineární používá také označení úplné (úplné uspořádání, úplně uspořádaná množina).
- Dále se zavádí pojem řetězec. Je definován jako taková podmnožina posetu, která je lineárně uspořádaná.
  Např. ve výše uvedeném příkladů se nejedná o lineárně uspořádané množiny. Ovšem množiny $\{1,2,6\}; \{3,6\}$ jsou vzhledem k relaci býti dělitelem řetězce, stejně jako množiny $\{\{b\}, \{b, c\}\}$; $\{\emptyset, \{a\}, \{a, c\}, \{a, b, c\}\}$ jsou řetězce vzhledem k inkluzi.
- Významným příkladem lineárního uspořádání je následující tzv. lexikografické uspořádání, které odpovídá uspořádání používanému např. ve slovnících.

Definice – lexikografické uspořádání

Označme $(A, \preccurlyeq)$ lineárně uspořádanou množinu (A je tzv. abeceda), A^* množinu všech konečných slov nad A (slovo = posloupnost znaků z A). Potom na A^* definujeme relaci lexikografického uspořádání $\preccurlyeq_{Le}$ následovně: $\boldsymbol{x} \preccurlyeq_{Le} \boldsymbol{y}$, kde $\boldsymbol{x} = x_1 \dots x_n, \boldsymbol{y} = y_1 \dots y_m$ jestliže buď

$[\exists k \ (x_k \prec y_k)] \ \wedge \ [\forall i \in \{1, .., k-1\} \ (x_i = y_i)]$, nebo $[n < m] \ \wedge \ [\forall i \in \{1, \dots, n\} \ (x_i = y_i)]$.

(zápis $x_k \prec y_k$ je zkratkou za $(x_k \preccurlyeq y_k) \ \wedge \ (x_k \neq y_k)$)

Na závěr části týkající se relací se ještě velmi stručně zmíníme o tzv. dobrém uspořádání, které má v matematice zcela zásadní roli.

Definice - dobré uspořádání

Nechť $(A, \preccurlyeq)$ je poset jehož každá neprázdná podmnožina má nejmenší prvek. Potom relaci $\preccurlyeq$ nazýváme dobré uspořádání a $(A, \preccurlyeq)$ nazýváme dobře uspořádanou množinou.

Poznámky

- Snadno nahlédneme, že každé dobré uspořádání je lineární uspořádání (řádně zdůvodněte). Obrácené tvrzení zřejmě obecně neplatí a jako protipříklad lze uvést poset $(Z, \leq)$, jehož podmnožina $2Z = \{n \in Z | \exists k \in Z \ \ n = 2k\}$ nemá nejmenší prvek. Na druhé straně je snadné nahlédnout, že poset $(N, \leq)$ dobře uspořádaný je.
- Každá konečná lineárně uspořádaná množina je dobře uspořádaná.

Definice – zobrazení

Nechť $\emptyset \neq f \subseteq A \times B$. Jestliže pro každé $a \in A$ existuje nejvýše jedno $b \in B$ tak, že $(a, b) \in f$, potom relaci f nazýváme zobrazení množiny A do množiny B.

Poznámky

- Skutečnost, že f je zobrazení A do B vyjadřujeme obvykle zápisem $f: A \to B$ a místo zápisu $(a, b) \in f$ používáme zápis $b = f(a)$. Prvek a nazýváme vzor, b nazýváme obraz vzoru a v zobrazení f. Dále definujeme:

  $D(f) = \{a \in A | \exists b \in B\ b = f(a)\} \subseteq A$ … definiční obor zobrazení f,

  $Im(f) = \{b \in B | \exists a \in A\ b = f(a)\} \subseteq B$ … obor hodnot zobrazení f, resp. obraz zobrazení f.

- Nechť $f: A \to B$ je zobrazení. Řekneme, že f je:

  a) Prosté (injektivní) zobrazení, jestliže
  $$(\forall a_1, a_2 \in A)\ \big(a_1 \neq a_2 \ \to\ f(a_1) \neq f(a_2)\big).$$
  b) Zobrazení na množinu B (surjektivní), jestliže
  $$(\forall b \in B\ \exists a \in A)\ \big(b = f(a)\big)$$
  c) Vzájemně jednoznačné (bijektivní) zobrazení, jestliže je prosté a na. Zapisujeme $f: A \xrightarrow{1-1} B$

- Nechť $f: A \to B$ je prosté zobrazení. Zobrazení $f^{-1}: B \to A$ definované vztahem
  $$(\forall a \in A, \forall b \in B)\big(a = f^{-1}(b)\big) \ \leftrightarrow\ \big(b = f(a)\big)$$
  nazveme inverzní zobrazení k zobrazení f.

- Nechť $f: A \to A$ je vzájemně jednoznačné zobrazení takové, že $(\forall a \in A)\ \Big(a = f\big(f(a)\big)\Big)$, potom f nazýváme involucí. Involuce je tedy vzájemně jednoznačné zobrazení, které je inverzí samo k sobě. Jako příklad lze uvést zobrazení $f: Z \to Z$ definované vztahem $f(x) = -x$.

Poznámky

- V případě zobrazení mezi číselnými množinami se častěji mluví o funkci, a v případě, kdy je oborem hodnot číselná množina mluvíme o funkcionálu.
- Funkci, jejíž definiční obor je množina přirozených čísel N nazýváme posloupnost. V případě, kdy oborem hodnot je podmnožina reálných čísel R, resp. komplexních čísel C, mluvíme o reálné, resp. komplexní posloupnosti. Posloupnost budeme zápisovat $\{a_n\}_{n=0}^{\infty}$, resp. $(a_n)_{n=0}^{\infty}$, kde a_n označuje n-tý člen posloupnosti, členy posloupnosti číslujeme od 0.

Nyní se krátce seznámíme s několika třídami funkcí, které hrají důležitou roli v kryptografii.

Definice – jednosměrná funkce

Řekneme, že funkce $f: A \to B$ je jednosměrná funkce, jestliže pro libovolné $x \in D(f)$ je výpočetně jednoduché určit $f(x)$ a současně pro skoro všechny obrazy $y \in Im(f)$ je výpočetně složité určit jakékoliv $x \in D(f)$ takové, že $y = f(x)$.

Poznámky

- Základní idea jednosměrných funkcí spočívá v tom, že je zásadní kvalitativní rozdíl ve výpočetní složitosti výpočtu funkční hodnoty $f(x)$ pro zadané x a určením hodnoty x ze zadané funkční hodnoty $f(x)$, tj. výpočtem inverzní funkce. V tomto duchu je třeba rozumět pojmům „výpočetně jednoduché“ a „výpočetně složité“ použitým v definici.

- Fráze „skoro všechny“ lze chápat tak, že pro náhodně zvolené $y \in Im(f)$ je výpočetně složité určit příslušný vzor x. Nicméně mohou existovat jisté funkční hodnoty $y \in Im(f)$, pro které to snadné je. (na rozdíl od reálných situací, budeme v příkladech používat malá čísla a z tohoto důvodu bude možné použít pro určení vzoru na základě funkční hodnoty metodu hrubé síly).

Příklad

Na množině $Z_{19}^* = \{1,2,\dots,18\}$ definujeme funkci $f(x)$ následovně: $x \in Z_{19}^* \rightarrow f(x) = r_x$, kde r_x je zbytek po vydělení čísla 3^x číslem 19. Tuto funkci lze označit jako jednosměrnou, neboť je výpočetně snadné pro libovolné x určit funkční hodnotu r_x. Naopak je obtížné z hodnoty r_x určit vzor x (v podstatě nezbývá nic jiného, než postupně počítat hodnoty r_x pro jednotlivá $x \in Z_{19}^*$ a pouze díky malému rozsahu to není problém).

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
r_x	3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1

Definice – jednosměrná funkce se zadními vrátky

Řekneme, že funkce $f: A \rightarrow B$ je jednosměrná funkce se zadními vrátky, jestliže má vlastnosti jednosměrné funkce s tím, že pokud disponujeme jistou dodatečnou informací (tzv. zadními vrátky), která není nutná pro výpočet $f(x)$, potom se stává výpočetně snadné určit k hodnotě $f(x)$ její vzor x.

Příklad

Uvažujme množinu $A = \{1,2,\dots,n-1\}$, kde $n = 2\,624\,653\,723$ a funkci definovanou na A vztahem $f(x) = r_x$, kde r_x je zbytek po dělení čísla x^3 číslem n. Jde o jednosměrnou funkci, neboť je poměrně snadné určit hodnotu r_x pro libovolné x. Např. spočteme, že $f(3\,489\,935) = 839\,913\,692$, neboť $3\,489\,935^3 = 16\,194\,964\,521 \cdot n + 839\,913\,692$. Nicméně, je velmi obtížné pro zadané r_x určit odpovídající vzor x. V tomto případě ale existují algoritmy, které umožňují výpočetně snadno vzor určit, pokud disponujeme kanonickým rozkladem čísla n. V reálných situacích je číslo n součinem dvou prvočísel majících řádově sto cifer a proto jejich nalezení je výpočetně velmi obtížný problém.

Poznámka

Otázka existence skutečně jednosměrné funkce (tj. odpovídající exaktně definovaným pojmům výpočetně snadné, resp. výpočetně složité) není dosud vyřešena. Existuje však celá řada funkcí, které na označení jednosměrná funkce aspirují (a se kterými se ještě podrobněji seznámíme).

Definice – hash funkce

Hash funkcí nazýváme zobrazení $h: \{0,1\}^* \rightarrow \{0,1\}^n$, které bitovému řetězci libovolné konečné délky přiřadí bitový řetězec pevné délky n nazývaný hash hodnota, resp. jenom hash. V případě kryptografických aplikací se obvykle dále požaduje:

i) Pro libovolné $x \in \{0,1\}^*$ je výpočetně snadné určit hash hodnotu $h(x)$.

ii) Pro libovolné $y \in \{0,1\}^n$ je výpočetně složité nalézt $x \in \{0,1\}^*$ tak, že $h(x) = y$.

iii) Pro libovolné dané $x \in \{0,1\}^*$ je výpočetně složité určit $\bar{x} \in \{0,1\}^*$ tak, že $(x \neq \bar{x}) \wedge \big(h(x) = h(\bar{x})\big)$. (tzv. slabá kolizní rezistence)

iii‘) Je výpočetně složité nalézt $x \neq \bar{x} \in \{0,1\}^*$ tak, že $h(x) = h(\bar{x})$. (tzv. silná kolizní rezistence)

1.2. Základy teorie dělitelnosti

Základním číselným oborem, se kterým budeme v této kapitole pracovat, jsou celá čísla Z, resp. přirozená čísla N nebo N^+. Celá čísla tvoří algebraickou strukturu, označovanou jako eukleidovský obor integrity, která je uzavřená vzhledem k operaci sčítání, odčítání a násobení (tj. součet, rozdíl i součin celých čísel je opět celé číslo). Vzhledem k operaci dělení však celá čísla uzavřená nejsou. Obsahem této kapitoly budou právě vlastnosti celých čísel vzhledem k operaci dělení a hlavní výsledky, které se dotýkají problematiky dělitelnosti, prvočísel a kongruencí, mají zásadní význam, např. v kryptologii, kódování, stochastického modelování apod.

Definice - dělitelnost

Řekneme, že nenulové celé číslo b dělí a, píšeme $b|a$, jestliže

$$(\exists q \in Z)\ (a = b \cdot q).$$

V opačném případě píšeme $b \nmid a$ a říkáme, že b nedělí a.

Poznámky

- Jestliže b dělí a, říkáme také, že a je dělitelné b. V tomto případě q nazýváme podílem, a násobkem b a b dělitelem a.
- Dělitele b nazveme vlastním dělitelem a, pokud $|a| \neq |b|$ a $|b| \neq 1$. Dělitele, který není vlastní, nazýváme nevlastním dělitelem. Například 3 je vlastním dělitelem 6, kdežto 1 a 6 jsou nevlastní dělitele 6.
- Snadno nahlédneme, že platí

  $$(b|a)\ \rightarrow\ (-b|a)\ \wedge (-b|-a) \wedge (b|-a)$$

  a proto se bez újmy na obecnosti omezíme v další části skript pouze na kladné dělitele!

Tvrzení

Výše definovaná relace dělitelnosti | má následující vlastnosti:

a) $\forall a \in Z\ \ 1|a$ b) $\forall a \in Z - \{0\}\ \ a|0$

c) $\forall a \in Z - \{0\}\ \ a|a$ d) $\forall a, b \in Z\ \ (b|a) \wedge (a|b)\ \rightarrow\ (a = b) \vee (a = -b)$

e) $\forall a, b, c \in Z\ \ (c|b) \wedge (b|a)\ \rightarrow\ c|a$ f) $\forall a, b, c \in Z\ \ (b|a)\ \rightarrow\ b|ac$

g) $\forall a, b, c \in Z\ \ (a + b = c) \wedge (d|a) \wedge (d|c)\ \rightarrow\ d|b$

Důkaz - cvičení pro čtenáře.

Poznámky

- Vlastnost c) se nazývá reflexivita a e) tranzitivita relace dělitelnosti. Pokud bychom ve předchozí větě nahradili číselný obor Z oborem přirozených čísel N^+, dostali bychom místo d) vlastnost d')

  $$\forall a, b \in N\ \ (b|a) \wedge (a|b)\ \rightarrow\ (a = b),$$

  která se nazývá antisymetrie. Je tedy zřejmé, že v oboru N^+ je relace dělitelnosti (částečným) uspořádáním, které však není lineární (libovolná dvojice přirozených čísel a, b nemusí být v relaci, tj. nemusí platit $a|b$ ani $b|a$).
- Vlastnost g) předcházející věty lze zobecnit následujícím způsobem:
  g') Je-li známo, že číslo d dělí všechny členy rovnosti $\sum_{i=1}^{n} a_i = \sum_{j=1}^{m} b_j$ kromě jediného, nutně dělí i zbývající člen.
- Jako zřejmý důsledek vlastnosti g') dostáváme:
  Jestliže $a|b_i, i = 1, \ldots, n$, potom pro libovolná $x_i \in Z,\ i = 1, \ldots, n$ platí $a|(\sum_{i=1}^{n} b_i x_i)$.

Pro další úvahy má zásadní význam následující tvrzení, označované jako věta o dělení se zbytkem.

Tvrzení - dělení se zbytkem

Nechť $a \in Z, b \in N^+$. Potom existuje jediné $q, r \in Z$ takové, že

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

Důkaz.

Definujme q jako největší celé číslo pro které $b \cdot q \leq a$ a číslo r vztahem $r = a - b \cdot q$. Obě čísla zřejmě existují a zbývá proto ukázat jejich jednoznačnost. Označme q_1, r_1, q_2, r_2 libovolná celá čísla, taková, že $a = b \cdot q_1 + r_1, 0 \leq r_1 < b$ a $a = b \cdot q_2 + r_2, 0 \leq r_2 < b$. Bez újmy na obecnosti lze předpokládat, že $0 \leq r_2 \leq r_1$. Odečtením obou rovností zřejmě dostáváme $b \cdot (q_1 - q_2) + (r_1 - r_2) = 0$. Jelikož $b|0$ a $b|b \cdot (q_1 - q_2)$ musí $b|(r_1 - r_2)$, což vzhledem k vlastnosti $0 \leq r_1 - r_2 < b$ nutně vede k $r_1 = r_2$ a $q_1 = q_2$.

Poznamenejme, že pro čísla a, b, q, r z věty věty o dělení se zbytkem se běžně používá terminologie: a … dělenec, b … dělitel, q … neúplný podíl, r … zbytek.

Příklad

Zřejmě platí:

a = 128	b = 23	128 = 23·5 + 13, tj. q = 5, r = 13,
a = -128	b = 23	-128 = 23·(-6) + 10, tj. q = -6, r = 10,
a = 19	b = 54	19 = 54·0 + 19, tj. q = 0, r = 19,
a = -19	b = 54	-19 = 54·(-1) + 35, tj. q = 0, r = 35,
a = 108	b = 36	108 = 36·3 + 0, tj. q = 3, r = 0,
a = 0	b = 29	0 = 29·0 + 0, tj. q = 0, r = 0.

Poznámka

Věta o dělení se zbytkem nachází využití při převodech z desítkové soustavy do ostatních číselných soustav. Připomeňme, že v soustavě o základu $b \in N^+$ (obvykle alespoň 2), vyjadřujeme přirozená čísla ve tvaru

$$r_0 + r_1 b + r_2 b^2 + \cdots + r_k b^k,$$

kde $r_i \in \{0,1, \ldots, b-1\}, k \in N$ a používáme zkrácený zápis $(r_k \ldots r_1 r_0)_b$. V případě dvojkové (binární) soustavy $(b = 2)$, nazýváme jednotlivé cifry r_i bity (r_0 nejméně významný bit, r_k nejvýznamnější bit).

Příklad

Převeďte číslo 6 862 do číselné soustavy o základu a) 2, b) 13.

Řešení.

Hledané cifry $r_0, r_1, \ldots r_k$ získáme jako zbytky při opakovaném dělení daného čísla a následně i získaných podílů základem b. V jednotlivých případech tak dostáváme:

ad a) Základ $b = 2, r_i \in \{0,1\}$. Postupným dělením číslem 2 dostáváme:

6862 = 2·3431 + 0 (r_0),	3431 = 2·1 715 + 1 (r_1),	1715 = 2·857 + 1 (r_2),
857 = 2·428 + 1 (r_3),	428 = 2·214 + 0 (r_4),	214 = 2·107 + 0 (r_5),
107 = 2·53 + 1 (r_6),	53 = 2·26 + 1 (r_7),	26 = 2·13 + 0 (r_8),
13 = 2·6 + 1 (r_9),	6 = 2·3 + 0 (r_{10}),	3 = 2·1 + 1 (r_{11}),

ad b) Základ $b = 13, r_i \in \{0,1, \ldots, 9, A, B, C\}$. Postupným dělením číslem 16 dostáváme:

6862 = 13· 527 + 11 (r_0),	527= 13· 40 + 7 (r_1),	40= 13·3+ 1 (r_2),
3 = 13·0 + 3 (r_3),	tedy 6 862 = $(317B)_{13}$.	

Poznámka

K vyjádření čísel v oblasti výpočetní techniky se používají různé číselné formáty, jejichž velikost bývá násobkem bytů, tj. osmi bitů. Například pomocí osmi bitů lze ve dvojkové soustavě vyjádřit přirozená čísla 0,…, 255, pomocí 16 bitů čísla 0,…, 65 535 a 32 bitů 0,…, 4 294 967 295. Snadno zjistíme, že pomocí n bitů lze ve dvojkové soustavě vyjádřit 2^n přirozených čísel $0, \dots, 2^n - 1$, kde u čísel $0, \dots, 2^{n-1} - 1$ je nejvýznamnější bit nastaven na 0 a u zbývajících čísel, tj. $2^{n-1}, \dots, 2^n - 1$ je nejvýznamnější bit nastaven na 1. Této skutečnosti se využívá k vyjádření záporných čísel $-1, \dots, -2^{n-1}$ ve tvaru tzv. dvojkových doplňků čísel $0, \dots, 2^{n-1} - 1$ tak, že u záporných čísel je nejvýznamnější bit nastaven na 1. V tomto případě se pomocí n bitů vyjadřují celá čísla z množiny $\{-2^{n-1}, \dots, -1,0,1, \dots, 2^{n-1} - 1\}$. Například, využitím čtyř bitů lze zapsat čísla $-8, \dots, -1,0,1, \dots 7$. Jejich vyjádření je uvedeno v následující tabulce:

Nezáporné číslo	Vyjádření v dvojkové soustavě		Vyjádření ve tvaru dvojkového doplňku	Záporné číslo
7	0111	……	1000	-8
6	0110	……	1001	-7
5	0101	……	1010	-6
4	0100	……	1011	-5
3	0011	……	1100	-4
2	0010	……	1101	-3
1	0001	……	1110	-2
0	0000	……	1111	-1

Formát záporného celého čísla k, kde $-2^n \leq k \leq -1$ lze popsat následovně:

1) Vypočti přirozené číslo $\bar{k} = 2^n - |k|$.
2) Přirozené číslo $\bar{k}$ vyjádři pomocí n bitů ve dvojkové soustavě, tj. $\bar{k} = (0b_{n-1} \dots b_1 b)_2$. (Jelikož $0 \leq k \leq 2^n - 1$, je nejvýznamnější bit zřejmě nastaven na nulu, tj. $b_n = 0$).
3) Hledané vyjádření záporného celého čísla k pak dostáváme nastavením nejvýznamnějšího bitu na jedničku, tj. $k = (1b_{n-1} \dots b_1 b)_2$.

1.2.1. Společný dělitel, společný násobek

Definice - společný dělitel
Kladné přirozené číslo d nazveme společným dělitelem celých čísel a, b jestliže $d|a \wedge d|b$, tj. d dělí obě čísla.

Zdůrazněme skutečnost, že v souladu s výše uvedenou definicí (a bez újmy na obecnosti) vyšetřujeme pouze kladné společné dělitele.

Označme $d_{a,b} = \{d \in N^+ | (d|a) \wedge (d|b)\}$, kde $a, b \in Z - \{0\}$ množinu všech společných dělitelů. Snadno zjistíme, že $d_{a,b} \neq \emptyset$ a shora omezená $\left(\forall d \in d_{a,b} \ 1 \leq d \leq \min\{|a|, |b|\}\right)$, a tedy množina $d_{a,b}$ má vzhledem k přirozenému uspořádání největší prvek. Tato skutečnost nás opravňuje k zavedení pojmu největší společný dělitel.

Definice – největší společný dělitel, nesoudělnost
- Největším společným dělitelem čísel $a, b \in Z - \{0\}$ nazveme takového jejich společného dělitele, který je ze všech společných dělitelů největší. Označujeme ho $NSD(a, b)$.
- Řekneme, že čísla $a, b \in Z$ jsou nesoudělná, jestliže $NSD(a, b) = 1$.

Tvrzení
Pro libovolná čísla $a, b \in Z - \{0\}$ platí, že $NSD(a, b)$ existuje a je určen jednoznačně.
Důkaz – viz poznámka před definicí.

Nyní přirozeně vzniká otázka, jak nalézt $NSD(a, b)$. V zásadě máme následující tři možnosti:
- Metoda hrubé síly – „prohledání“ množiny $d_{a,b}$. (neefektivní metoda).
- Využití kanonických rozkladů čísel a, b. Detaily viz odstavec věnovaný prvočíslům. (neefektivní metoda).
- Využití následujícího Eukleidova algoritmu, jehož základem je věta o dělení se zbytkem. (efektivní metoda).

Eukleidův algoritmus
Nechť $a \in Z, b \in N^+$. Postupnou aplikací věty o dělení se zbytkem dostáváme:

$$\begin{aligned}
a &= b \cdot q_0 + r_1, & 0 < r_1 < b,\\
b &= r_1 \cdot q_1 + r_2, & 0 < r_2 < r_1,\\
r_1 &= r_2 \cdot q_2 + r_3, & 0 < r_3 < r_2,\\
&\vdots & \vdots\\
r_{n-2} &= r_{n-1} \cdot q_{n-1} + r_n, & 0 < r_n < r_{n-1},\\
r_{n-1} &= r_n \cdot q_n
\end{aligned}$$

Poznámka
Pro libovolná $a \in Z, b \in N^+$ je Eukleidův algoritmus konečný, neboť zbytky tvoří klesající shora omezenou posloupnost přirozených čísel, tj. $0 < r_n < r_{n-1} < \cdots < r_1 < b$. Dá se ukázat (G. Lamé, 1795-1870), že počet kroků (tj. počet aplikací věty o dělení se zbytkem) je roven nejvýše pětinásobku počtu cifer menšího z čísel a, b.

Tvrzení

Pro libovolná čísla $a \in Z, b \in N^+$ platí $NSD(a,b) = r_n$.

($NSD(a,b)$ je rovno poslednímu nenulovému zbytku v Eukleidově algoritmu aplikovanému na a, b)

Důkaz.

Vzhledem ke konečnosti Eukleidova algoritmu a zřejmé vlastnosti společných dělitelů

$$(d|a) \wedge (d|b) \leftrightarrow d|NSD(a,b)$$

dostáváme

$$NSD(a,b) = NSD(b,r_1) = NSD(r_1,r_2) = \cdots = NSD(r_{n-1},r_n) = r_n.$$

Tvrzení - základní vlastnosti *NSD*

Pro libovolná čísla $a, b \in Z - \{0\}$ platí:

a) $NSD(a,b) = NSD(b,a)$

b) $NSD(a,b) = NSD(-a,b) = NSD(a,-b) = NSD(-a,-b)$

c) $\forall k \in N^+ \; NSD(k \cdot a, k \cdot b) = k \cdot NSD(a,b)$

d) $\forall d \in N^+ \; (d|a) \wedge (d|b) \rightarrow NSD\left({}^{a}/_{d}, {}^{b}/_{d}\right) = {}^{NSD(a,b)}/_{d}$

e) $NSD(a,b) = 1 \rightarrow NSD(a \cdot c, b) = NSD(c,b)$

Důkaz.

Části a), b) - zřejmé.

ad c) Jednotlivé řádky Eukleidova algoritmu vynásobíme $k \in N^+$.

ad d) Vzhledem k předpokladu a již dokázané části c) dostáváme

$NSD(a,b) = NSD\left(a \cdot {}^{d}/_{d}, b \cdot {}^{d}/_{d}\right) = d \cdot NSD\left({}^{a}/_{d}, {}^{b}/_{d}\right)$, tj.

${}^{NSD(a,b)}/_{d} = NSD\left({}^{a}/_{d}, {}^{b}/_{d}\right)$

(Uvědomte si, kde využíváme předpoklad, že d je společným dělitelem čísel a, b.)

ad e) Stačí ukázat, že $\left(NSD(a \cdot c, b)|NSD(c,b)\right) \wedge \left(NSD(c,b)|NSD(a \cdot c, b)\right)$

Zřejmě $NSD(a \cdot c, b)|NSD(a \cdot c, b \cdot c)$, tj. $NSD(a \cdot c, b)|\left(c \cdot NSD(a,b)\right)$ a s ohledem na $NSD(a,b) = 1$ dostáváme $NSD(a \cdot c, b)|c$, tedy $NSD(a \cdot c, b)|NSD(c,b)$.

Naopak, $NSD(c,b)|c$, tedy $NSD(c,b)|a \cdot c$. Odtud $NSD(c,b)|NSD(a \cdot c, b)$.

Naopak, $NSD(c,b)|c$, tedy $NSD(c,b)|a \cdot c$. Odtud $NSD(c,b)|NSD(a \cdot c, b)$.

Poznámky

- Z části b) plyne, že se při hledání největšího společného dělitele čísel a, b můžeme (bez újmy na obecnosti) omezit na obor kladných přirozených čísel N^+.
- Jako užitečné důsledky předchozího tvrzení dostáváme:

  i) $NSD(a,b) = 1 \wedge (b|a \cdot c) \rightarrow b|c$

  ii) $NSD\left({}^{a}/_{NSD(a,b)}, {}^{b}/_{NSD(a,b)}\right) = 1$, tedy každá kladná přirozená čísla a, b lze psát ve tvaru

$$a = a_1 \cdot NSD(a,b), b = b_1 \cdot NSD(a,b), \text{kde } NSD(a_1,b_1) = 1.$$

Kromě výše uvedených způsobů výpočtů $NSD(a,b)$, lze použít následující tzv. dvojkový NSD algoritmus (efektivní metoda).

Dvojkový NSD algoritmus

Pro libovolná $a, b \in N^+$ lze $NSD(a,b)$ nalézt opakovanou aplikací následujících pravidel (dokažte!):

1) Jsou-li a, b sudá, potom $NSD(a,b) = 2 \cdot NSD\left({}^{a}/_{2}, {}^{b}/_{2}\right)$.
2) Je-li a sudé, b liché, potom $NSD(a,b) = NSD\left({}^{a}/_{2}, b\right)$.
3) Jsou-li a, b lichá, $a < b$, potom $NSD(a,b) = NSD\left(a, {}^{(b-a)}/_{2}\right)$.

Algoritmus končí v situaci, kdy $a = b$ (zdůvodněte, že skutečně nastane!) a využijeme $NSD(a,a) = a$.

Tvrzení – Bézoutova rovnost

Pro libovolná $a, b \in N^+$ platí $NSD(a,b) = \min_{x,y \in Z}\{ax + by > 0\}$.

Důkaz.

Označme $x_0, y_0 \in Z$, pro která $ax_0 + by_0 = \min_{x,y \in Z}\{ax + by > 0\}$ (zřejmě existují, zdůvodněte).

Jako důkaz nyní stačí ukázat, že $NSD(a,b)|(ax_0 + by_0) \wedge (ax_0 + by_0)|NSD(a,b)$. Jelikož $NSD(a,b)|a \wedge NSD(a,b)|b$, dostáváme $NSD(a,b)|(ax_0 + by_0)$. Z věty o dělení se zbytkem plyne $\forall x, y \in Z \ (ax_0 + by_0)|(ax + by)$, tedy speciálně pro $x = 1, y = 0$ dostáváme $(ax_0 + by_0)|a$ a pro $x = 0, y = 1$ $(ax_0 + by_0)|b$. Odtud $(ax_0 + by_0)|NSD(a,b)$.

Poznámka

Čísla $x_0, y_0 \in Z$ taková, že $NSD(a,b) = ax_0 + by_0$ lze nalézt pomocí Eukleidova algoritmu, resp. pomocí řetězových zlomků (viz dále).

Příklad

Pro $a = 583, b = 231$ vyjádřete $NSD(a,b)$ ve tvaru $ax_0 + by_0$.

Řešení.

Aplikací Eukleidova algoritmu dostáváme:

$583 = 231 \cdot 2 + 121$ (r_1) $\quad 231 = 121 \cdot 1 + 110$ (r_2)

$121 = 110 \cdot 1 + 11$ (r_3) $\quad 110 = 11 \cdot 10$

tedy $NSD(583{,}231) = 11$ (r_3). Postupným „zpětným“ vyjádřením zbytku r_3 dostáváme

$r_3 = 11 = 121 - 110 \cdot 1 = 121 - (231 - 121 \cdot 1) \cdot 1 = 121 \cdot 2 - 231 =$

$= (583 - 231 \cdot 2) \cdot 2 - 231 = 583 \cdot 2 + 231 \cdot (-5)$,

tedy $NSD(583{,}231) = 11 = 583 \cdot 2 + 231 \cdot (-5)$.

Pojem společný dělitel a největší společný dělitel dvou čísel lze rozšířit na více čísel následovně.

Definice - společný dělitel, největší společný dělitel čísel $a_1, \dots, a_n$

- Kladné přirozené číslo d nazveme společným dělitelem čísel $a_1, \dots, a_n \in Z - \{0\}, n \geq 2$, jestliže $d|a_1 \wedge \dots \wedge d|a_n$, tj. d dělí každé z čísel $a_1, \dots, a_n$.
- Největším společným dělitelem čísel $a_1, \dots, a_n \in Z - \{0\}$ nazveme takového jejich společného dělitele, který je ze všech jejich společných dělitelů největší (existuje vždy a jediný). Značíme ho $NSD(a_1, \dots, a_n)$.

Poznámka

- Výpočet $NSD(a_1, \dots, a_n)$ převádíme na opakovaný výpočet největšího společného dělitele dvou čísel dle vztahu $NSD(a_1, \dots, a_n) = NSD(\dots NSD(NSD(a_1, a_2), a_3) \dots, a_n)$.
- Platí Bézoutova rovnost, tj. $NSD(a_1, \dots, a_n) = \min_{x_i \in Z}\{\sum_{i=1}^{n} a_i x_i > 0\}$ (dokažte!) a tedy $\exists y_1, \dots, y_n \in Z$ taková, že $NSD(a_1, \dots, a_n) = \sum_{i=1}^{n} a_i y_i$.

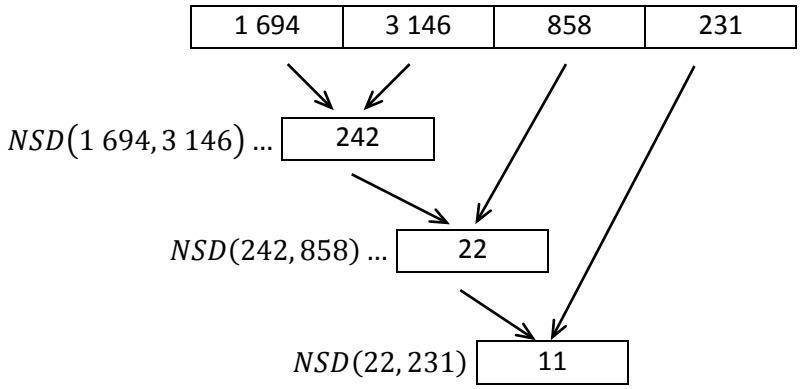
- V případě $n > 2$ se kromě pojmu nesoudělnost ($NSD(a_1, \dots, a_n) = 1$) zavádí pojem nesoudělnost po dvou:
  Řekneme, že čísla $a_1, \dots, a_n \in Z - \{0\}, n > 2$ jsou nesoudělná po dvou, jestliže
  $$\forall i \neq j \;\; NSD(a_i, a_j) = 1$$
  Je zřejmé, že z nesoudělnosti po dvou vyplývá nesoudělnost a jak dokládá následující ukázka, obrácené tvrzení neplatí. Např. trojice čísel 12, 15, 35 je nesoudělná, ale není nesoudělná po dvou.

Příklad

Nalezněte největšího společného dělitele čísel 1 694, 3 146, 858, 231.

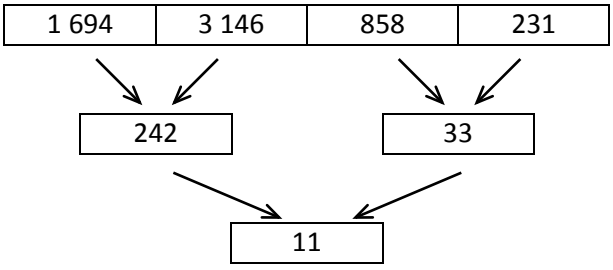
Řešení.

Strukturu výpočtu lze znázornit následujícím schématem, jehož jednotlivé kroky výpočtu jsou realizovány pomocí Eukleidova algoritmu:



Tedy $NSD(1\,694, 3\,146, 858, 231) = 11$.

Ke stejnému výsledku samozřejmě dospějeme i v případě následujícího postupu:



Bézoutova rovnost v tomto případě dává např.

$NSD(1\,694, 3\,146, 858, 231) = 1\,694 \cdot 2 + 3\,146 \cdot (-1) + 858 \cdot (-21) + 231 \cdot 77$

Nyní se zastavíme u pojmů společný násobek a nejmenší společný násobek.

Definice - společný násobek

Kladné přirozené číslo D nazveme společným násobkem čísel $a, b \in Z - \{0\}$, jestliže $a|D \;\wedge\; b|D$, tj. D je dělitelné oběma čísly.

Poznámka

Označme $D_{a,b} = \{D \in N^+ |\; (a|D) \wedge (b|D)\}$ množinu všech společných násobků čísel $a, b \in Z - \{0\}$.

$D_{a,b}$ je neprázdná, zdola omezená $\left(\forall D \in D_{a,b} \ \max\{|a|,|b|\} \leq D \leq a \cdot b\right)$, a má tedy vzhledem k přirozenému uspořádání nejmenší prvek. Tato skutečnost nás opravňuje k zavedení následujícího pojmu.

Definice – nejmenší společný násobek
Nejmenším společným násobkem čísel $a, b \in Z - \{0\}$ nazveme takový jejich společný násobek, který je ze všech společných násobků nejmenší. Označujeme ho $NSN(a, b)$.

Tvrzení
Pro libovolná čísla $a, b \in Z - \{0\}$ platí, že $NSN(a, b)$ existuje a je určen jednoznačně.
Důkaz – viz poznámka před definicí.

Poznámky
Nyní vyřešíme otázku, jak nalézt $NSN(a, b)$. V zásadě máme následující tři možnosti:

- Metoda hrubé síly – „prohledání" množiny $D_{a,b}$. (neefektivní metoda)
- Využití kanonických rozkladů čísel a, b. Detaily viz odstavec věnovaný prvočíslům. (neefektivní metoda)
- Využití následující možnosti převedení výpočtu $NSN(a, b)$ na výpočet $NSD(a, b)$, tj. využití Eukleidova algoritmu. (efektivní metoda)
  Označme D libovolný společný násobek čísel a, b. Vzhledem k tomu, že čísla a, b lze psát ve tvaru $a = a_1 \cdot NSD(a, b), b = b_1 \cdot NSD(a, b)$, kde $NSD(a_1, b_1) = 1$ a vzhledem k $(a|D) \wedge (b|D)$, dostáváme $D = a_1 \cdot b_1 \cdot NSD(a, b) \cdot n$, kde $n \in N^+$. Další úpravou pak pro D dostáváme vztah $D = \frac{a \cdot b}{NSD(a,b)} \cdot n$, kde $n \in N^+$. Odtud pak dostáváme následující vztah pro výpočet nejmenšího společného násobku
  $$NSN(a, b) = \frac{a \cdot b}{NSD(a, b)}$$
  V případě, kdy čísla a, b jsou nesoudělná, zřejmě platí $NSN(a, b) = a \cdot b$.

Analogicky, jako v případě společného dělitele a nejmenšího společného dělitele, lze rozšířit pojmy společný násobek a nejmenší společný násobek na případ více než dvou čísel.

Definice - společný násobek, nejmenší společný násobek čísel $a_1, \ldots, a_n$

- Kladné přirozené číslo D nazveme společným násobkem čísel $a_1, \ldots, a_n \in Z - \{0\}, n \geq 2$, jestliže $a_1|D \ \wedge \ldots \wedge \ a_n|D$, tj. D je dělitelné každým z čísel $a_1, \ldots, a_n$.
- Nejmenším společným násobkem čísel $a_1, \ldots, a_n \in Z - \{0\}$ nazveme takový jejich společný násobek, který je ze všech jejich společných násobků nejmenší (existuje vždy a jediný). Značíme ho $NSN(a_1, \ldots, a_n)$.

Poznámky

- Výpočet $NSN(a_1, \ldots, a_n)$ převádíme na opakovaný výpočet nejmenšího společného násobku dvou čísel dle vztahu $NSN(a_1, \ldots, a_n) = NSN(\ldots NSN(NSN(a_1, a_2), a_3) \ldots, a_n)$.
- Nechť $a_1, \ldots, a_n \in Z - \{0\}, n \geq 2$. Potom platí
  $$\forall i \neq j \ NSD(a_i, a_j) = 1 \ \rightarrow \ NSN(a_1, \ldots, a_n) = a_1 \cdot \ldots \cdot a_n.$$
  Předpoklad nesoudělnosti po dvou nelze pro $n > 2$ nahradit předpokladem nesoudělnosti.

- POZOR! Nejmenší společný násobek více než dvou čísel nelze obecně počítat jako v případě dvou čísel, tj. jejich součin dělený jejich největším společným dělitelem. V případě $n = 3$ platí vztah

$$NSN(a,b,c) = \frac{a \cdot b \cdot c \cdot NSD(a,b,c)}{NSD(a,b) \cdot NSD(a,c) \cdot NSD(b,c)}$$

1.2.2. Prvočísla a prvočíselné rozklady

Zkoumáme-li počet dělitelů kladných přirozených čísel, snadno zjistíme, že některá přirozená čísla větší než jedna mají pouze nevlastní dělitele (tj. číslo jedna a sebe sama), kdežto ostatní mají i vlastní dělitele. Odtud následující definice pojmu prvočíslo.

Definice - prvočíslo, složené číslo

Přirozené číslo $p > 1$ nazveme prvočíslem, jestliže platí

$$(\forall n \in N^+)\ (n|p\ \rightarrow n = 1 \vee n = p),$$

tj. číslo p má pouze nevlastní dělitele.

Ostatní kladná přirozená čísla větší než jedna nazýváme čísla složená.

Příklad

Čísla 2, 3, 5, 7 jsou prvočísla, neboť všechna mají pouze nevlastní dělitele. Naopak, čísla 4, 6, 189, 222 jsou čísla složená, neboť mají vlastní dělitele, např. $2|4, 3|6, 7|189, 37|222$. Ovšem mnohem obtížnější je zjistit, že číslo 162 259 276 829 213 363 391 578 010 288 127 je prvočíslo, kdežto 340 282 366 920 938 463 463 374 607 431 768 211 457 je číslo složené.

Tvrzení – Eukleides

Existuje nekonečně mnoho prvočísel.

Důkaz – sporem.

Předpokládejme, že existuje konečně prvočísel $p_1, \dots, p_n$ a položme $p = p_1 \cdot \dots \cdot p_n + 1$. Zřejmě $\forall i\ p \neq p_i$, tudíž p je číslo složené a musí být proto dělitelné některým z prvočísel $p_1, \dots, p_n$, např. p_j. Vzhledem k tomu, že platí $p_j|p\ \wedge\ p_j|p_1 \cdot \dots \cdot p_n$ dostáváme $p_j|1$. Spor, existuje tedy nekonečně mnoho prvočísel.

Poznamenejme, že existuje celá řada dalších různě rafinovaných důkazů existence nekonečně mnoha prvočísel, které odkrývají mnohdy překvapivé souvislosti.

Poznámky

- Nejmenší od jedničky různý dělitel složeného čísla n je prvočíslo, které je nejvýše rovno $\lfloor\sqrt{n}\rfloor$. (Dokažte!)
- Je-li p prvočíslo takové, že $p|a \cdot b$, potom $p|a$ nebo $p|b$. (Dokažte!)
- Všechna prvočísla vyskytující se v množině $\{2, \dots, n\}$ lze nalézt pomocí algoritmu (nazývaného Eratosthenovo síto), který lze formulovat následovně:
  1. V posloupnosti $2, \dots, n$ označ první nevyškrtnuté a ještě neoznačené číslo. Toto číslo p je prvočíslo. Je-li $p \leq \lfloor\sqrt{n}\rfloor$, jdi na krok 2., jinak ukonči algoritmus a nevyškrtnutá čísla jsou právě všechna hledaná prvočísla.
  2. Vyškrtni všechny násobky čísla p, počínaje p^2. Po jejich vyškrtnutí jdi na krok 1.

Výše popsaný algoritmus (Eratosthenes, 276 – 195 př. n. l.) je pravděpodobně historicky první metoda umožňující „generovat“ posloupnost prvočísel.

V dalších úvahách hraje klíčovou roli následující věta, označovaná často jako Základní věta aritmetiky.

Tvrzení – Základní věta aritmetiky
Každé přirozené číslo větší než jedna lze rozložit na součin prvočísel, a to jednoznačně, nepřihlížíme-li k pořadí prvočísel.
Důkaz.
Je třeba dokázat dvě skutečnosti - existenci prvočíselného rozkladu a jeho jednoznačnost.
Označme a libovolné složené číslo (v případě, kdy a je prvočíslo, tvrzení evidentně platí). Dle první části výše uvedené poznámky existuje prvočíslo p_1 takové, že $p_1|a$, tj. $a = p_1 \cdot a_1$, kde $1 < a_1 < a$. Pokud a_1 je prvočíslo, dostali jsme již hledaný rozklad. V opačném případě, kdy číslo a_1 je složené, existuje prvočíselný dělitel p_2 čísla a_1, tj. $a_1 = p_2 \cdot a_2$, kde $1 < a_2 < a_1$. Je-li a_2 složené číslo, postup opakujeme (jinak jsme nalezli požadovaný rozklad), dokud nenastane situace, kdy a_k bude prvočíslo. Vzhledem k tomu, že čísla a_i tvoří klesající posloupnost přirozených čísel, musí tato situace skutečně nastat. Odtud již existence prvočíselného rozkladu $a = p_1 \cdot \ldots \cdot p_k$.
Nyní předpokládejme, že $a = p_1 \cdot \ldots \cdot p_k = q_1 \cdot \ldots \cdot q_l$ jsou dva prvočíselné rozklady čísla a. Zřejmě $\forall i \in \{1, \ldots k\}\, p_i | q_1 \cdot \ldots \cdot q_l$ a tedy musí existovat j takové, že $p_i = q_j$. Odtud $k = l$ a po případném přečíslování dostáváme $\forall i \in \{1, \ldots k\}\, p_i = q_i$.

Poznámka
Jako zřejmý důsledek Základní věty aritmetiky dostáváme fakt, že každé přirozené číslo $a > 1$ lze jednoznačně vyjádřit ve tvaru tzv. kanonického rozkladu, tj.

$$a = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k},$$

kde $p_i, i = 1, \ldots, k$ jsou všechna různá prvočísla (seřazená vzestupně) vyskytující se v rozkladu a,
$\alpha_i \in N^+, i = 1, \ldots, k$ (tzv. násobnost prvočísla p_i v rozkladu a).
(Často budeme používat kratší označení rozklad místo kanonický rozklad.)

Tvrzení
Nechť $a = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}, b = q_1^{\beta_1} \cdot \ldots \cdot q_l^{\beta_l}$ jsou kanonické rozklady. Potom platí:

a) $d|a \rightarrow d = p_1^{\delta_1} \cdot \ldots \cdot p_k^{\delta_k}$,
kde $0 \leq \delta_i \leq \alpha_i, i = 1, \ldots, k$.

b) $NSD(a, b) = r_1^{\gamma_1} \cdot \ldots \cdot r_h^{\gamma_h}$,
kde $r_1, \ldots, r_h$ jsou prvočísla společná kanonickým rozkladům čísel a, b,
γ_i je minimum z exponentů, se kterým se prvočíslo r_i vyskytuje v kanonických rozkladech čísel a, b.

c) $NSN(a, b) = r_1^{\lambda_1} \cdot \ldots \cdot r_m^{\lambda_m}$,
kde $r_1, \ldots, r_m$ jsou prvočísla vyskytující se v alespoň jednom kanonickém rozkladu, λ_i je maximum z exponentů, se kterým se prvočíslo r_i vyskytuje v kanonických rozkladech čísel a, b.

Důkaz.
ad a) Jelikož $d|a$, mohou se v kanonickém rozkladu d vyskytovat pouze prvočísla z kanonického rozkladu a, navíc s exponentem, který je nejvýše roven jeho exponentu v rozkladu a.

ad b) Jelikož $NSD(a,b)|a \wedge NSD(a,b)|b$, musí kanonický rozklad $NSD(a,b)$ obsahovat pouze prvočísla, která jsou společná kanonickým rozkladům a i b, navíc s exponentem rovným právě menšímu z exponentů.
ad c) Jelikož $a|NSN(a,b) \wedge b|NSN(a,b)$, musí kanonický rozklad $NSN(a,b)$ obsahovat všechna prvočísla z kanonických rozkladů a i b. Exponenty jednotlivých prvočísel v rozkladu $NSN(a,b)$ jsou zřejmě rovny jejich maximálnímu exponentu, se kterým se dané prvočíslo vyskytuje v kanonických rozkladech čísel a, b.

Poznámka
Označíme-li $\tau(a)$ počet dělitelů kladného přirozeného čísla $a = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, dostáváme jako důsledek části a) předchozího tvrzení vztah

$$\tau(a) = (\alpha_1 + 1) \cdot \ldots \cdot (\alpha_k + 1).$$

Příklad
Pomocí kanonických rozkladů čísel $a = 7\,875, b = 3\,900, c = 82\,500$ určete všechny dělitele čísla a, dále $NSD(a,b,c), NSN(a,b,c)$.
Řešení.
Nejprve určíme kanonické rozklady čísel a, b, c (uvedená čísla zkoušíme dělit prvočísly, dělení prvočíslem opakujeme, dokud je zbytek nulový). Dostáváme tak

$$a = 3^2 \cdot 5^3 \cdot 7, b = 2^2 \cdot 3 \cdot 5^2 \cdot 13, c = 2^2 \cdot 3 \cdot 5^4 \cdot 11.$$

Všechny dělitele čísla a jsou tvaru $d = 3^{\alpha_1} \cdot 5^{\alpha_2} \cdot 7^{\alpha_3}$, kde $0 \leq \alpha_1 \leq 2, 0 \leq \alpha_2 \leq 3, 0 \leq \alpha_3 \leq 1$ a jde o následující dělitele: 1; 3; 5; 7; 9; 15; 21; 25; 35; 45; 63; 75; 105; 125; 175; 225; 315; 375; 525; 875; 1125; 1575; 2625; 7875.
Jako kanonický rozklad $NSD(a,b,c)$ dostáváme $NSD(a,b,c) = 3 \cdot 5^2 = 75$ a jako kanonický rozklad $NSN(a,b,c)$ dostáváme $NSN(a,b,c) = 2^2 \cdot 3^2 \cdot 5^4 \cdot 7 \cdot 11 \cdot 13 = 22\,522\,500$.

Poznámka
Jedním z fundamentálních problémů teorie čísel je otázka rozložení prvočísel v množině všech přirozených čísel. Některé základní výsledky lze formulovat následovně:

- Existuje nekonečně mnoho libovolně dlouhých posloupností po sobě jdoucích složených čísel, tj. neobsahující žádné prvočíslo (dokažte!).
- Pro libovolná nesoudělná přirozená čísla a, m existuje nekonečně mnoho prvočísel p, která při dělení číslem m dávají zbytek a, tedy jsou tvaru $p = m \cdot q + a$, kde $q \in N^+$. (C. F. Gauss).
- Označíme-li $\pi(n)$ počet prvočísel menších nebo rovných přirozenému číslu n, platí

  $$\pi(n) \cong {}^{n}/_{\ln n},$$

  kde symbol $\cong$ chápeme jako přibližnou rovnost (přesněji, limita podílu obou stran je pro $n \to \infty$ rovna 1). Hodnoty obou stran výše uvedeného vztahu jsou pro vybraná n obsaženy v následujících tabulkách.

n	10	50	100	500	1 000	100 000	500 000	1 000 000
$\pi(n)$	4	15	25	95	168	9 592	41 538	78 498

Příklad

Dokažte speciální variantu obecného Gaussova tvrzení (poznámka výše), že existuje nekonečně mnoho prvočísel tvaru $4q + 3$.

Řešení. – sporem.

Nejprve si uvědomme, že každé prvočíslo větší než 2 dává při dělení číslem 4 zbytek 1, nebo 3. Nyní předpokládejme, že existuje pouze konečně prvočísel $p_1, \dots, p_n$ uvažovaného tvaru $4q + 3$ (určitě taková existují, např. 3, 7, 11, 19, 23 apod.) a položme $p = 4p_1 \cdot \dots \cdot p_n - 1$. Je zřejmé, že číslo p dává při dělení 4 zbytek 3, navíc není dělitelné žádným z prvočísel $p_1, \dots, p_n$ (jinak by dané prvočíslo muselo dělit 1). Vzhledem k tomu, že součin čísel tvaru $4q + 1$ je opět číslo téhož tvaru (dokažte!), musí být číslo p dělitelné prvočíslem tvaru $4q + 3$ různým od $p_1, \dots, p_n$. Spor, existuje tedy nekonečně mnoho prvočísel tvaru $4q + 3$.

Velmi významnou roli v teorii čísel a v celé řadě aplikací, např. moderní teorie šifrování, testy superpočítačů apod. (podrobnosti přesahují rámec těchto skript), hraje problematika kanonických rozkladů velkých čísel, resp. testy jejich prvočíselnosti. V tomto kontextu se nejčastěji vyskytují čísla speciálních tvarů, např. Fermatova, Mersennova a Cunninghamova čísla.

Definice - Fermatova a Mersennova čísla

Fermatovými čísly nazýváme čísla $F_n = 2^{2^n} + 1$ a Mersennovými čísly nazýváme čísla $M_n = 2^n - 1$, kde $n \in N$.

Poznámka - Fermatova a Mersennova prvočísla

- Fermatova čísla $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65\,537$ jsou prvočísla (tzv. Fermatova prvočísla). Tato skutečnost vedla vynikajícího francouzského matematika Pierre de Fermat (1601-1695) k vyslovení hypotézy, že všechna Fermatova čísla jsou prvočísla. Teprve později byla tato hypotéza vyvrácena Leonardem Eulerem (1707-1783), který ukázal, že číslo $F_5 = 4\,294\,967\,297$ je složené. Nyní panuje hypotéza, že všechna Fermatova čísla $F_n, n \geq 5$ jsou čísla složená. Ovšem ani v dnešní době není snadné prokázat, že pro některou konkrétní hodnotu n je F_n číslo složené (proč?). Například doposud (2016) nebylo zjištěno, zda F_{24} je skutečně číslo složené a u F_{12} (o kterém je prokázáno, že je složené) nebyl nalezen jeho kanonický rozklad.
- Historicky neméně zajímavá a z hlediska aplikací významná jsou tzv. Mersennova prvočísla (Marin Mersenne, 1588-1648), tj. prvočísla tvaru M_p, kde p je prvočíslo (snadno lze ukázat, že nutnou, ale nikoliv postačující, podmínkou pro to, aby šlo o prvočíslo je, že n musí být prvočíslo). V současné době se předpokládá (není ovšem dokázáno), že mezi všemi čísly M_n, kde n je prvočíslo, existuje nekonečně mnoho Mersennových prvočísel, ale i čísel složených. Například čísla $M_2, M_3, M_5, M_7, M_{13}, M_{17}, M_{19}, M_{31}$ jsou Mersennova prvočísla, kdežto M_{11}, M_{67}, M_{257} jsou čísla složená. Největší v současné době (2016) známé Mersennovo prvočíslo je $M_{6\,972\,593}$ (to ovšem neznamená, že o všech číslech M_n, kde n je prvočíslo menší než 6 972 593 je známo zda jsou prvočíslem). Pro zajímavost uveďme, že prvočíselnost $M_{1\,257\,787}$ byla prokázána na superpočítači Cray T-94, ovšem prvočíselnost $M_{6\,972\,593}$ již na pouhém PC Pentium 350 MHz.

1.2.3. Základní aritmetické funkce

V teorii čísel a v jejich aplikacích hrají významnou roli funkce, jejichž definiční obory tvoří kladná přirozená čísla N^+. Pro takové funkce se vžilo označení aritmetické funkce.

Definice - multiplikativní funkce

Řekneme, že aritmetická funkce f je multiplikativní, jestliže:

- $\exists n_0 \in N^+ \; f(n_0) \neq 0$,
- $\forall m,n \in N^+ \; \big(NSD(m,n) = 1 \; \rightarrow f(mn) = f(m)f(n)\big)$.

Základní vlastnosti multiplikativních funkcí popisuje následující tvrzení.

Tvrzení

a) Je-li f multiplikativní funkce, potom $f(1) = 1$.

b) Součin multiplikativních funkcí je multiplikativní funkce.

c) Je-li f multiplikativní, $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ kanonický rozklad, potom

$$\sum_{d|n} f(d) = \left(1 + f(p_1) + f(p_1^2) + \cdots + f\left(p_1^{\alpha_1}\right)\right) \cdot \ldots \cdot \left(1 + f(p_k) + f\left(p_k^2\right) + \cdots + f\left(p_k^{\alpha_k}\right)\right)$$

(Součet na levé straně se provádí přes všechny dělitele d čísla n.)

Důkaz.

ad a) Z definice multiplikativnosti plyne $\exists n_0 \in N^+ \; f(n_0) \neq 0$, navíc zřejmě s ohledem na $NSD(n_0, 1) = 1$ lze psát $f(n_0) = f(n_0 \cdot 1) = f(n_0) \cdot f(1)$, tedy $f(1) = 1$.

ad b) Označme $f = f_1 \cdot f_2$, kde f_1, f_2 jsou multiplikativní funkce. Zřejmě $f(1) = f_1(1) \cdot f_2(1) = 1$. Dále předpokládejme $NSD(m,n) = 1$, proto
$f(mn) = f_1(mn)f_2(mn) = f_1(m)f_1(n)f_2(m)f_2(n) = f_1(m)f_2(m)f_1(n)f_2(n) = f(m)f(n)$.

ad c) Jelikož $NSD\left(p_i^{\delta_i}, p_j^{\delta_j}\right) = 1$, pro $i \neq j$, je po roznásobení pravá strana dokazovaného vztahu zřejmě rovna (využijeme multiplikativnost)

$$\sum_{\substack{(\delta_1,\ldots,\delta_k) \\ 0 \leq \delta_1 \leq \alpha_1,\ldots,0 \leq \delta_k \leq \alpha_k}} f\left(p_1^{\delta_1}\right) \cdot \ldots \cdot f\left(p_k^{\delta_k}\right) = \sum_{\substack{(\delta_1,\ldots,\delta_k) \\ 0 \leq \delta_1 \leq \alpha_1,\ldots,0 \leq \delta_k \leq \alpha_k}} f\left(p_1^{\delta_1} \cdot \ldots \cdot p_k^{\delta_k}\right).$$

Jelikož dělitele d čísla n jsou právě tvaru $d = p_1^{\delta_1} \cdot \ldots \cdot p_k^{\delta_k}$, kde $0 \leq \delta_i \leq \alpha_i, i = 1, \ldots, k$ je vztah dokázán.

Poznámka – počet dělitelů, součet dělitelů

Aritmetická funkce $f_r(n) = n^r, n \in N^+$ je multiplikativní (dokažte!) a dle výše uvedeného tvrzení platí

$$\sum_{d|n} d^r = \left(1 + p_1^r + p_1^{2r} + \cdots + p_1^{\alpha_1 r}\right) \cdot \ldots \cdot \left(1 + p_k^r + p_k^{2r} + \cdots + p_k^{\alpha_k r}\right).$$

Odtud volbou $r = 0$ dostáváme nám již známý vztah pro počet dělitelů čísla n

$$\tau(n) = \sum_{d|n} 1 = \underbrace{(1 + \cdots + 1)}_{\alpha_1 + 1} \cdot \ldots \cdot \underbrace{(1 + \cdots + 1)}_{\alpha_k + 1} = (\alpha_1 + 1) \cdot \ldots \cdot (\alpha_k + 1),$$

Volbou $r = 1$ dostáváme vztah pro součet dělitelů čísla n

$$S(n) = \sum_{d|n} d = \left(1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1}\right) \cdot \ldots \cdot \left(1 + p_k + p_k^2 + \cdots + p_k^{\alpha_k}\right),$$

tj.

$$S(n) = \left(\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}\right) \cdot \ldots \cdot \left(\frac{p_k^{\alpha_k+1} - 1}{p_k - 1}\right).$$

Definice - Möbiova funkce

Aritmetickou funkci $\mu(n)$ definovanou vztahy

- $\mu(n) = 1,$
- $\mu(n) = \begin{cases} 0 & \text{, pokud existuje } d > 1 \text{ takové, že } d^2 | n \\ (-1)^k & \text{v ostatních případech, kde } k \text{ je počet prvočísel v rozkladu } n \end{cases}$

nazýváme Möbiovou funkcí.

Z definice je patrné, že hodnoty $\mu(n)$ snadno určíme z kanonického rozkladu čísla $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$. Jsou-li totiž všechna $\alpha_i = 1$, potom $\mu(n) = (-1)^k$ a pokud alespoň jedno $\alpha_i \geq 2$ je $\mu(n) = 0$.

Tvrzení

Möbiova funkce je multiplikativní a pro $n > 1$ platí $\sum_{d|n} \mu(d) = 0$.

Důkaz.

Multiplikativnost - jsou-li m, n nesoudělná, potom je počet prvočísel v kanonickém rozkladu $m \cdot n$ roven součtu počtu prvočísel v rozkladu m plus počet prvočísel v rozkladu n, navíc jejich exponenty se nemění. S ohledem na již dokázanou multiplikativitu si stačí uvědomit následující

$$\sum_{d|n} \mu(d) = (1 + (-1) + 0 + \cdots + 0) \cdot \ldots \cdot (1 + (-1) + 0 + \cdots + 0) = 0.$$

Definice - Eulerova funkce

Aritmetickou funkci $\varphi(n)$ definovanou jako počet čísel v řadě $1, \ldots, n$, která jsou nesoudělná s n, nazýváme Eulerovou funkcí.

Z definice snadno zjistíme, že pro libovolné prvočíslo p platí $\varphi(p) = p - 1$ (zdůvodněte!). V případě složených čísel je výpočet hodnoty Eulerovy funkce výpočetně složitý, neboť vyžaduje znalost kanonického rozkladu.

Tvrzení

a) Je-li $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ kanonický rozklad, potom

$$\varphi(n) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdot \ldots \cdot \left(p_k^{\alpha_k} - p_1^{\alpha_k - 1}\right).$$

b) Eulerova funkce je multiplikativní.

c) Platí $\sum_{d|n} \varphi(d) = n$.

Důkaz.

ad a) Označme $P(A)$ pravděpodobnost, že náhodně zvolené číslo z množiny $\{1, \ldots, n\}$ je nesoudělné s n. S ohledem na definici Eulerovy funkce a klasickou definici pravděpodobnosti platí

$$P(A) = {}^{\varphi(n)}/_{n}$$

Nesoudělnost s n je zřejmě ekvivalentní s nedělitelností žádným z prvočísel $p_1, \ldots, p_k$ vyskytujících se v kanonickém rozkladu n a tedy

$$P(A) = {}^{\varphi(n)}/_{n} = \left(1 - \tfrac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \tfrac{1}{p_k}\right),$$

(každé p_i-té číslo v řadě $1, \ldots, n$ je dělitelné prvočíslem p_i) a odtud platnost tvrzení.

ad b) Jsou-li m, n nesoudělná, potom se prvočísla a jejich exponenty v kanonickém rozkladu součinu $m \cdot n$ shodují s prvočísly a jejich exponenty v kanonickém rozkladu čísla m, resp. n. Zbytek důkazu je zřejmý.

ad c) S ohledem na již dokázanou multiplikativitu dostáváme

$$\sum_{d|n}\varphi(d) = \left(1 + (p_1 - 1) + (p_1^2 - p_1) + \cdots + \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right)\right) \cdot \ldots$$
$$\ldots \cdot \left(1 + (p_k - 1) + \left(p_k^2 - p_k\right) + \cdots + \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right)\right)$$

a tedy $\sum_{d|n}\varphi(d) = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} = n$.

Kromě aritmetických funkcí se v diskrétní matematice setkáme také následujícími funkcemi.

Definice

- Funkce dolní celá část x, kde $x \in R$, je definována jako největší celé číslo menší nebo rovné x. Tuto funkci budeme označovat symbolem $\lfloor x \rfloor$ (někdy se používá i kratší název celá část x) a platí:
  - $\forall x \in R \ \lfloor x \rfloor \in Z$,
  - $\forall x \in R \ \lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$.
- Funkce horní celá část x, kde $x \in R$, je definována jako nejmenší celé číslo větší nebo rovné x. Tuto funkci budeme označovat symbolem $\lceil x \rceil$ a platí:
  - $\forall x \in R \ \lceil x \rceil \in Z$,
  - $\forall x \in R \ \lceil x \rceil - 1 \leq x < \lceil x \rceil$.
- Funkci lomená část x, kde $x \in R$, budeme označovat symbolem $\{x\}$. Tato funkce je definována vztahem $\{x\} = x - \lfloor x \rfloor$. Oborem hodnot této funkce je zřejmě interval $\langle 0, 1)$.

Poznámka

Některé často využívané vlastnosti funkcí dolní a horní celá část jsou (dokažte!):

- $x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$,
- $\lfloor -x \rfloor = -\lceil x \rceil$ $\quad\quad$ $\lceil -x \rceil = -\lfloor x \rfloor$,
- $\lfloor x + n \rfloor = \lfloor x \rfloor + n, n \in N$ $\quad\quad$ $\lceil x + n \rceil = \lceil x \rceil + n, n \in N$,
- $\lfloor \sum_{i=1}^{n} x_i \rfloor \geq \sum_{i=1}^{n} \lfloor x_i \rfloor$ $\quad\quad$ $\lceil \sum_{i=1}^{n} x_i \rceil \leq \sum_{i=1}^{n} \lceil x_i \rceil$.

1.2.4. Řetězové zlomky

Při numerických výpočtech vždy pracujeme s racionálními čísly, resp. s jejich jistou konečnou podmnožinou. V tomto kontextu hraje důležitou roli problematika tzv. diofantické aproximace, která zkoumá, jak přesně lze dané číslo aproximovat pomocí racionálních čísel určitých vlastností. K této problematice má úzký vztah i následující část týkající se řetězových zlomků. Snadno totiž zjistíme, že každé číslo $\alpha \in R - Z$ (v případě celých čísel je situace triviální), lze vyjádřit jediným způsobem ve tvaru

$$\alpha = q_0 + \frac{1}{\alpha_1},$$

kde $q_0 = \lfloor \alpha \rfloor \in Z$ (největší celé číslo menší nebo rovné α) a $1 < \alpha_1$. Pokud α_1 není přirozené číslo, lze postupovat analogicky, tj. psát

$$\alpha_1 = q_1 + \frac{1}{\alpha_2},$$

kde $q_1 = \lfloor \alpha_1 \rfloor, 1 < \alpha_2$. Odtud

$$\alpha = q_0 + \frac{1}{q_1 + \frac{1}{\alpha_2}}.$$

Naznačený postup lze samozřejmě opakovat, dokud v některém kroku (např. i v prvním) nedostaneme $\alpha_n \in N^+$ (jak uvidíme později, tato situace nemusí nastat). Tím se již dostáváme k pojmu rozvoj (reálného) čísla α v řetězový zlomek.

Definice

Řetězovým zlomkem nazveme (konečný nebo nekonečný) výraz tvaru

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_{2+} \ddots + \cfrac{1}{q_n + \cfrac{1}{\ddots}}}}$$

kde $q_0 \in Z, q_i \in N^+$.

Čísla q_i se nazývají členy rozvoje (v řetězový zlomek) a výrazy

$$\delta_0 = q_0, \delta_1 = q_0 + \frac{1}{q_1}, \dots, \delta_n = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_{2+} \ddots + \cfrac{1}{q_n}}}, \dots$$

se nazývají přibližnými zlomky.

Poznámky

- Pro zjednodušení budeme přibližné zlomky častěji zápisovat ve tvaru
$$\delta_0 = [q_0], \delta_1 = [q_0, q_1], \dots, \delta_n = [q_0, q_1, \dots, q_n]$$
- Každý přibližný zlomek lze zapsat ve tvaru zlomku s jednou zlomkovou čarou, tj. $\delta_i = {}^{P_i}/_{Q_i}$.

Definice

Řekneme, že reálné číslo α má konečný (ukončený) rozvoj v řetězový zlomek, jestliže existuje $n \in N$ takové, že při postupu popsaném v úvodu je α_n celé číslo (tj. $\forall i \in N^+ \ \alpha_{n+i} = 0$). V tomto případě zřejmě platí

$$\alpha = [q_0, q_1, \dots, q_n], \text{tj. } \alpha = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_{2+} \ddots + \cfrac{1}{q_n}}}$$

Tvrzení

Reálné číslo α má konečný rozvoj v řetězový zlomek právě tehdy, je-li racionální.

Důkaz.

Z následující poznámky a z konečnosti Eukleidova algoritmu vyplývá, že každé racionální číslo má konečný rozvoj v řetězový zlomek. Zbývá tak dokázat platnost obráceného tvrzení, tj. z konečnosti rozvoje v řetězový zlomek plyne racionalita. Postupujme sporem a předpokládejme, že číslo s konečným rozvojem v řetězový zlomek není racionální. Spor, neboť bychom nalezli vyjádření iracionálního čísla ve tvaru zlomku.

Obecný postup jak sestrojovat řetězové zlomky je popsán v úvodu. Následující poznámka ukazuje na souvislost s již dobře známým Eukleidovým algoritmem.

Poznámka – řetězové zlomky a Eukleidův algoritmus

Je-li $^a/_b$ racionální číslo, potom užitím Eukleidova algoritmu dostáváme následující:

1. krok $a = bq_0 + r_1,\ 0 < r_1 < b,$ tj. $^a/_b = q_0 + \frac{1}{\alpha_1}$, kde $\alpha_1 = \frac{b}{r_1} > 1.$

2. krok $b = r_1q_1 + r_2,\ 0 < r_2 < r_1,$ tj. $^b/_{r_1} = q_1 + \frac{1}{\alpha_2}$, kde $\alpha_2 = \frac{r_1}{r_2} > 1,$

tedy $^a/_b = q_0 + \frac{1}{q_1 + \frac{1}{\alpha_2}}$.

3. krok $r_1 = r_2q_2 + r_3,\ 0 < r_3 < r_2,$ tj. $^{r_1}/_{r_2} = q_2 + \frac{1}{\alpha_3}$, kde $\alpha_3 = \frac{r_2}{r_3} > 1,$

tedy $^a/_b = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \frac{1}{\alpha_3}}}$.

Vzhledem k tomu, že zbytky tvoří klesající posloupnost přirozených čísel, je zaručena konečnost uvedeného postupu a musí nastat situace, kdy jisté r_n je poslední nenulový zbytek, tj.

n. krok $r_{n-2} = r_{n-1}q_{n-1} + r_n,\ 0 < r_n < r_{n-1},$ tj. $^{r_{n-2}}/_{r_{n-1}} = q_{n-1} + \frac{1}{\alpha_n}$, kde $\alpha_n = \frac{r_{n-1}}{r_n} > 1,$

tedy $^a/_b = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots + \cfrac{1}{q_{n-1} + \frac{1}{\alpha_n}}}}$.

$(n+1)$. krok $r_{n-1} = r_nq_n,$ tj. $^{r_{n-1}}/_{r_n} = q_n,$ tj. $^a/_b = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots + \frac{1}{q_n}}}$.

Vidíme tedy, že jednotlivé členy rozvoje racionálního čísla $^a/_b$ v řetězový zlomek tvoří právě neúplné podíly z Eukleidova algoritmu.

Tvrzení – základní vlastnosti přibližných zlomků

a) Mezi čitateli P_i a jmenovateli Q_i přibližných zlomků platí

$$P_i = q_iP_{i-1} + P_{i-2}, \text{ kde } P_{-1} = 1, P_0 = q_0,$$
$$Q_i = q_iQ_{i-1} + Q_{i-2}, \text{ kde } Q_{-1} = 0, Q_0 = 1.$$

b) Pro libovolné dva sousední přibližné zlomky δ_i, δ_{i-1} platí

$$\delta_i - \delta_{i-1} = \frac{(-1)^{i+1}}{Q_iQ_{i-1}}.$$

c) Přibližné zlomky jsou v základním tvaru, tj. $NSD(P_i, Q_i) = 1.$

Důkaz.

ad a) Použijeme indukci. Zřejmě platí $\delta_1 = q_0 + \frac{1}{q_1} = \frac{q_1q_0+1}{q_1\cdot 1+0} = \frac{q_1P_0+P_{-1}}{q_1Q_0+Q_{-1}} = \frac{P_1}{Q_1}.$

Nyní předpokládejme platnost dokazovaných vztahů pro $i-1$, tj. $\delta_{i-1} = \frac{P_{i-1}}{Q_{i-1}} = \frac{q_{i-1}P_{i-2}+P_{i-3}}{q_{i-1}Q_{i-2}+Q_{i-3}}.$

Z tvaru přibližných zlomků snadno zjistíme, že δ_i dostaneme z δ_{i-1} pouhou substitucí $q_{i-1} + \frac{1}{q_i}$ za q_{i-1}. Lze proto psát

$$\delta_i = \frac{\left(q_{i-1} + \frac{1}{q_i}\right)P_{i-2} + P_{i-3}}{\left(q_{i-1} + \frac{1}{q_i}\right)Q_{i-2} + Q_{i-3}} = \frac{q_i(q_{i-1}P_{i-2} + P_{i-3}) + P_{i-2}}{q_i(q_{i-1}Q_{i-2} + Q_{i-3}) + Q_{i-2}} = \frac{q_iP_{i-1} + P_{i-2}}{q_iQ_{i-1} + Q_{i-2}} = \frac{P_i}{Q_i}$$

a odtud již platnost dokazovaných vztahů.

ad b) Zřejmě platí

$$\delta_i - \delta_{i-1} = \frac{P_i}{Q_i} - \frac{P_{i-1}}{Q_{i-1}} = \frac{P_iQ_{i-1} - P_{i-1}Q_i}{Q_iQ_{i-1}}.$$

Nyní vyšetříme vztah mezi hodnotou čitatele a indexem i. Označme $f_i = P_iQ_{i-1} - P_{i-1}Q_i$. Z již dokázaných vztahů dostáváme

$f_i = (q_iP_{i-1} + P_{i-2})Q_{i-1} - P_{i-1}(q_iQ_{i-1} + Q_{i-2}) = (-1)(P_{i-1}Q_{i-2} - P_{i-2}Q_{i-1}) = (-1)f_{i-1}$,

tedy $f_i = (-1)^i f_0$ a vzhledem k $f_0 = P_0Q_{-1} - P_{-1}Q_0 = -1$ platí $P_iQ_{i-1} - P_{i-1}Q_i = (-1)^{i+1}$.

ad c) S ohledem na Bezoutovu rovnost a již dokázaný vztah $P_iQ_{i-1} - P_{i-1}Q_i = (-1)^{i+1}$ zřejmé.

Je zřejmé, že neúplné podíly $q_i, i = 0,1,\dots,n$ a rekurentní vztahy pro P_i, Q_i (s počátečními podmínkami) umožňují efektivní výpočet přibližných zlomků. Výpočet se často zapisuje do následující tabulky přibližných zlomků:

i	-1	0	1	2	…	n
q_i	- - -	q_0	q_1	q_2	…	q_n
P_i	1	q_0	P_1	P_2	…	P_n
Q_i	0	1	Q_1	Q_2	…	Q_n

Příklad

Číslo $^{781}/_{654}$ rozviňte v řetězový zlomek a sestavte tabulku přibližných zlomků.

Řešení.

Pomocí Eukleidova algoritmu získáme potřebné neúplné podíly:

$781 = 654 \cdot 1(q_0) + 127$, $654 = 127 \cdot 5(q_1) + 19$, $127 = 19 \cdot 6(q_2) + 13$,

$19 = 13 \cdot 1(q_3) + 6$, $13 = 6 \cdot 2(q_4) + 1$, $6 = 1 \cdot 6(q_5)$.

Tabulka přibližných zlomků má tedy tvar

i	-1	0	1	2	3	4	5
q_i	- - -	1	5	6	1	2	6
P_i	1	1	6	37	43	123	781
Q_i	0	1	5	31	36	103	654

Odtud hledaný rozvoj v řetězový zlomek

$$\frac{781}{654} = [1,5,6,1,2,6] = 1 + \cfrac{1}{5 + \cfrac{1}{6 + \cfrac{1}{1 + \cfrac{1}{2 + \frac{1}{6}}}}}$$

a zároveň z tabulky přibližných zlomků vidíme $NSD(781,654) = 781 \cdot 103 + 654 \cdot (-123) = 1$

Poznámka

- Lze ukázat (dokažte), že mezi všemi racionálními čísly, jejichž jmenovatel je nejvýše roven Q_i, je právě přibližný zlomek δ_i nejlepší aproximací rozvíjeného čísla. Přesněji:

  Je-li $\delta_i = \frac{P_i}{Q_i}$ přibližný zlomek rozvoje reálného čísla $^a/_b$ v řetězový zlomek, $\beta = {}^P/_Q$ libovolné racionální číslo takové, že $0 < Q \leq Q_i$, potom $\left|\delta_i - {}^a/_b\right| \leq \left|\beta - {}^a/_b\right|$.
- Pro zajímavost jsou v následující tabulce uvedeny (nekonečné) řetězové zlomky některých vybraných iracionálních čísel.

Číslo	Řetězový zlomek
e	[2,1,2,1,1,4,1,1,6,1,1,8,1,1,10, …]
π	[3,7,15,1,292,1,1,1,2,1,3,1,14, …]

$\sqrt{2}$	[1,2,2,2, …]
$\sqrt{5}$	[2,4,4,4, …]
$\sqrt{10}$	[3,6,6,6, …]
$\sqrt{17}$	[4,8,8,8, …]
$\sqrt{26}$	[5,10,10,10, …]

Jako důsledek tak dostáváme, že následující racionální čísla nejlépe aproximují (ve smyslu první odrážky této poznámky) číslo π.

P_i	3	22	333	355	103 993
Q_i	1	7	106	113	33 102
Δ_i	1,42E-01	1,26E-03	8,32E-05	2,67E-07	5,78E-10

Poslední řádek obsahuje horní hranici „chyby“ aproximace, tj. $\left|\pi - \frac{P_i}{Q_i}\right| \leq \Delta_i$.

1.2.5. Kongruence

Z věty o dělení se zbytkem víme, že celá čísla dávají při dělení přirozeným číslem $m \geq 1$ zbytky z množiny $\{0,1, \dots, m-1\}$. Z pohledu dělitelnosti, proto budeme čísla dávající stejný zbytek považovat za „totožná“. Odtud následující definice.

Definice

Řekneme, že celá čísla a, b jsou kongruentní modulo m , kde $m \in N^+$, jestliže obě čísla mají při dělení modulem m stejný zbytek.

Poznámky

- Skutečnost, že čísla a, b jsou kongruentní modulo m vyjadříme některým z následujících zápisů:
  $$a \equiv b\ (mod\ m), a \equiv b\ (m), \text{ resp. } a \equiv_m b.$$
  V opačném případě (a, b nemají při dělení modulem m stejný zbytek) píšeme $a \not\equiv b\ (m)$ a říkáme, že uvedená čísla nejsou kongruentní modulo m.
- Dále budeme používat zápis $a = (b\ mod\ m)$, kterým vyjádříme skutečnost, že číslo a je rovno zbytku při dělení čísla b modulem m. Například $386 \equiv 777\ (17)$, ale $12 = (386\ mod\ 17)$.

Poznámka

Přes svou jednoduchost nachází výše zavedený pojem kongruence velmi široké využití v celé řadě oblastí. Vzhledem k rozsahu skript se stručně zmíníme pouze o generování náhodných (přesněji řečeno pseudonáhodných) čísel a o některých způsobech šifrování.

- Efektivní metodou generování posloupnosti pseudonáhodných čísel $x_0, x_1, \dots$ jsou lineární kongruence. Jednotlivé členy posloupnosti jsou počítány rekurentně ze vztahu
  $$x_{n+1} = \big((ax_n + b)\ mod\ m\big),$$
  kde $m, a, c, x_0 \in N$ taková, že $2 \leq a < m, 0 \leq c < m, 0 \leq x_0 < m, NSD(a, m) = 1$.
  (m … modul, a … multiplikační koeficient, c … inkrement, x_0 … počáteční hodnota).
  Celá řada běžných počítačů využívá pro generování pseudonáhodných čísel $m = 2^{31} - 1$, $a = 7^5$, $c = 0$ (tzv. ryze multiplikativní generátor). V případě, kdy požadujeme pseudonáhodná čísla z intervalu $\langle 0,1)$, použijeme posloupnost x_n/m.
- Jedním z nejstarších způsobů šifrování je tzv. Caesarova šifra, které cyklicky posouvá abecedu o tři znaky vpřed ($A \to D, B \to E, \dots, Z \to C$). Z pohledu kongruencí lze toto šifrování popsat vztahem

$$Y = \big((x + 3)\ mod\ 26\big),$$

kde x je pořadové číslo kódovaného znaku (v rámci anglické abecedy, počet znaků 26), Y je pořadové číslo zašifrovaného znaku a 3 je posunutí. Dešifrování se pak provádí „zpětným“ posunutím, tj. dle vztahu

$$x = \big((Y + 23)\ mod\ 26\big).$$

Tvrzení

Následující tvrzení jsou ekvivalentní:

a) $a \equiv b\ (m)$,

b) $m|(a - b)$,

c) $\exists t \in Z\ \ a = b + mt$.

Důkaz - stačí dokázat a) → b) → c) → a).

ad a) → b)

Jelikož $a \equiv b\ (m)$, z věty o dělení se zbytkem dostáváme $a = a_1 m + r, b = b_1 m + r$, kde $0 \leq r < m$ a tedy $a - b = (a_1 - b_1)m$, tj. $m|(a - b)$.

ad b) → c)

Jelikož $m|(a - b)$ platí $a - b = mt, t \in Z$, tedy $a = b + mt$.

ad c) → a)

Z věty o dělení se zbytkem dostáváme $b = mq + r, 0 \leq r < m$ a následným dosazením do c) získáme $a = m(q + t) + r, 0 \leq r < m$, tj. obě čísla dávají při dělení m stejný zbytek.

Jak dokládá následující tvrzení, jsou početní pravidla pro kongruence s pevně daným modulem analogická početním pravidlům pro rovnice.

Tvrzení - stejný modul

Jestliže $a_1 \equiv b_1\ (m), a_2 \equiv b_2\ (m)$, potom platí:

a) $a_1 + a_2 \equiv b_1 + b_2\ (m)$,

b) $a_1 \cdot a_2 \equiv b_1 \cdot b_2\ (m)$,

c) $d|a_1, d|b_1, NSD(d, m) = 1\ \rightarrow\ {}^{a_1}\!/_{d} \equiv {}^{b_1}\!/_{d}\ (m)$.

Důkaz – cvičení.

Jako snadný důsledek pak dostáváme:

- K oběma stranám kongruence lze přičíst, resp. od nich odečíst libovolné celé číslo.
- Obě strany kongruence lze vynásobit libovolným číslem.
- Členy z jedné strany kongruence lze převést na druhou, pokud u nich změníme znaménko.
- Obě strany kongruence lze umocnit na $n \in N$.

Jak dokládá následující ukázka, je předpoklad $NSD(d, m) = 1$ v části c) předchozího tvrzení podstatný. Např. $144 \equiv 78\ (33)$, ovšem ${}^{144}\!/_{6} \not\equiv {}^{78}\!/_{6}\ (33)$.

Tvrzení - změna modulu

a) $a \equiv b\ (m)\ \rightarrow ka \equiv kb\ (km)$, kde $k \in N^+$,

b) $a \equiv b\ (m), m_1|m\ \rightarrow a \equiv b\ (m_1)$,

c) $a \equiv b\ (m), d|NSD(a, b, m)\ \rightarrow {}^{a}\!/_{d} \equiv {}^{b}\!/_{d}\ \left({}^{m}\!/_{d}\right)$,

d) $a \equiv b\ (m_1), a \equiv b\ (m_2)\ \rightarrow a \equiv b\ \big(NSN(m_1, m_2)\big)$.

Důkaz.
ad a) Zřejmě $a = b + mt$, tedy pro $k \in N^+$ $ka = kb + kmt$, tj. $ka \equiv kb\ (km)$.
ad b) Jelikož $m = m_1 q$ a $m|(a-b)$ nutně i $m_1|(a-b)$, tj. $a \equiv b\ (m_1)$.
ad c) $a = b + mt, d|NSD(a,b,m) \rightarrow {}^{a}/_{d} = {}^{b}/_{d} + {}^{m}/_{d} \cdot t$, tedy ${}^{a}/_{d} \equiv {}^{b}/_{d}\ \left({}^{m}/_{d}\right)$.
ad d) Jelikož $m_1|(a-b), m_2|(a-b)$ zřejmě i $NSN(m_1, m_2)|(a-b)$.

Pro další úvahy je důležité si uvědomit, že relace „býti kongruentní modulo m“ má vlastnosti:

- $\forall a \in Z \quad a \equiv a\ (m)$, (reflexivita)
- $\forall a, b \in Z \quad a \equiv b\ (m) \rightarrow b \equiv a\ (m)$, (symetrie)
- $\forall a, b \in Z \quad a \equiv b\ (m), b \equiv c\ (m) \rightarrow a \equiv c\ (m)$. (tranzitivita)

Relace „býti kongruentní modulo m“ je tedy ekvivalence na Z, která indukuje rozklad Z na m následujících tříd ekvivalence

$$[0] = \{\dots, -2m, -m, 0, m, 2m, \dots\} = \{tm | t \in Z\},$$
$$[1] = \{\dots, 1-2m, 1-m, 1, 1+m, 1+2m, \dots\} = \{1+tm | t \in Z\},$$
$$[2] = \{\dots, 2-2m, 2-m, 2, 2+m, 2+2m, \dots\} = \{2+tm | t \in Z\},$$
$$\vdots$$
$$[m-1] = \{\dots, -m-1, -1, m-1, 2m-1, \dots\} = \{(m-1)+tm | t \in Z\},$$

nazývané zbytkové třídy modulo m, resp. třídy zbytků modulo m. Každá třída zbytků obsahuje právě všechna navzájem modulo m kongruentní celá čísla. Pro množinu všech zbytkových tříd modulo m se vžilo označení Z_m, tj. $Z_m = \{[0], \dots, [m-1]\}$. Nyní na množině Z_m definujme operaci sčítání a násobení modulo m následovně

$$[a] + [b] = [a+b], \ [a] \cdot [b] = [a \cdot b].$$

Dokažte, že obě operace jsou definovány korektně, nezávisle na výběru reprezentanta, tj. platí
$\forall a_1, a_2, b_1, b_2 \in Z\ a_1 \equiv a_2(m), b_1 \equiv b_2(m) \ \rightarrow \ [a_1] + [b_1] = [a_2] + [b_2], [a_1] \cdot [b_1] = [a_2] \cdot [b_2]$.

Kromě obvyklých vlastností obou operací (asociativita, komutativita, distributivita, existence nulového, opačného a jednotkového prvku) platí:

- V Z_m lze dělit prvkem $[a]$ právě tehdy, je-li $NSD(a,m) = 1$. V tomto případě $\exists [b] \in Z_m$ takové, že $[a][b] = [1]$.
  (budeme používat označení $[a]^{-1}$ místo $[b]$ a mluvit o inverzním prvku k $[a]$)
  Zřejmým důsledkem je skutečnost: je-li p prvočíslo, potom $\forall [a] \in Z_p - \{[0]\} \ \ \exists [a]^{-1} \in Z_m$.
- V Z_m existují vlastní dělitelé nuly právě tehdy, je-li m číslo složené, tj.
  $\exists [a], [b] \in Z_m - \{[0]\}\ [a][b] = [0]$

Příklad
Algebraická struktura Z_5 obsahuje následujících pět zbytkových tříd:

$[0] = \{\dots, -10, -5, 0, 5, 10, \dots\} = \{5t | t \in Z\}$ … celá čísla dělitená 5,
$[1] = \{\dots, -9, -4, 1, 6, 11, \dots\} = \{5t+1 | t \in Z\}$ … celá čísla dávající při dělení 5 zbytek 1,
$[2] = \{\dots, -8, -3, 2, 7, 12, \dots\} = \{5t+2 | t \in Z\}$ … celá čísla dávající při dělení 5 zbytek 2,
$[3] = \{\dots, -7, -2, 3, 8, 13, \dots\} = \{5t+3 | t \in Z\}$ … celá čísla dávající při dělení 5 zbytek 3,
$[4] = \{\dots, -6, -1, 4, 9, 14, \dots\} = \{5t+4 | t \in Z\}$ … celá čísla dávající při dělení 5 zbytek 4,

kde operace sčítání a násobení jsou definovány následujícími tabulkami:

+	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

·	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

Nyní snadno ověříme, že v Z_5 je možné provádět „stejné“ výpočty jako v Q, resp. R, neboť lze „dělit“ pomocí násobení inverzním prvkem

$$[1]^{-1} = [1], [2]^{-1} = [3], [3]^{-1} = [2], [4]^{-1} = [4],$$

navíc platí

$$[a] \cdot [b] = [0] \ \rightarrow \ ([a] = [0]) \vee ([b] = [0]).$$

Například, pokud máme určit zbytkovou třídu $[x]$ tak, že $[3][x] + [4] = [1]$, lze postupovat následovně. Nejprve k oběma stranám přičteme prvek $[1]$ (tj. prvek opačný k $[4]$) a dostáváme $[3][x] = [2]$. Nyní obě strany vynásobíme prvkem $[2]$ (tj. prvkem inverzním k $[3]$) a dostáváme $[x] = [4]$.

Algebraická struktura Z_6 obsahuje následujících šest zbytkových tříd:

$[0] = \{6t | t \in Z\}$ … celá čísla dělitená 6,
$[1] = \{6t + 1 | t \in Z\}$ … celá čísla dávající při dělení 6 zbytek 1,
$[2] = \{6t + 2 | t \in Z\}$ … celá čísla dávající při dělení 6 zbytek 2,
$[3] = \{6t + 3 | t \in Z\}$ … celá čísla dávající při dělení 6 zbytek 3,
$[4] = \{6t + 4 | t \in Z\}$ … celá čísla dávající při dělení 6 zbytek 4,
$[5] = \{6t + 5 | t \in Z\}$ … celá čísla dávající při dělení 6 zbytek 5,

kde operace sčítání a násobení jsou definovány následujícími tabulkami:

+	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

·	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

V Z_6 již nelze provádět výpočty tak, jako v Q, resp. R, neboť neexistuje $[2]^{-1}, [3]^{-1}, [4]^{-1}$ (tj. nelze obecně dělit) a navíc může platit $[a] \cdot [b] = [0]$ přesto, že $[a] \neq 0$ i $[b] \neq 0$ (např. $[4] \cdot [3] = [0]$).

Odtud již motivace pro následující definici úplné a redukované soustavy zbytků.

Definice - úplná a redukované soustava zbytků

- Úplnou soustavou zbytků modulo m nazveme každou množinu obsahující m modulo m nekongruentních celých čísel. Značíme Z_m.
- Redukovanou soustavou zbytků modulo m nazveme takovou podmnožinu úplné soustavy zbytků modulo m, která obsahuje právě všechny zbytky nesoudělné s modulem m. Značíme Z_m^*.

Poznámky

- Z definice Eulerovy funkce plyne $|Z_m^*| = \varphi(m)$.

- V další části budeme používat zjednodušené značení zbytkových tříd, ve kterém vynecháme hranaté závorky, tj. budeme psát a místo $[a]$.
- Pro daný modul $m \geq 1$ existuje nekonečně mnoho úplných (i redukovaných) soustav zbytků modulo m, neboť každá zbytková třída je v úplné soustavě zastoupena libovolným svým prvkem (reprezentantem zbytkové třídy). Nejpoužívanější je však úplná soustava nejmenších nezáporných zbytků modulo m, tj.

  $$Z_m = \{0,1,\dots,m-1\},$$

  resp. úplná soustava absolutně nejmenších zbytků modulo m tj.

  $$Z_m = \left\{\frac{1-m}{2},\dots -1,0,1,\dots,\frac{m-1}{2}\right\} \text{ pro } m \text{ liché,}$$

  $$Z_m = \left\{-\frac{m}{2},\dots -1,0,1,\dots,\frac{m-2}{2}\right\}, \text{ resp. } Z_m = \left\{\frac{2-m}{2},\dots -1,0,1,\dots,\frac{m}{2}\right\} \text{ pro } m \text{ sudé.}$$

Příklad

Příklady úplných a redukovaných soustav zbytků modulo 5:

$Z_5 = \{0,1,2,3,4\}$ … úplná soustava nejmenších nezáporných zbytků modulo 5,

$Z_5 = \{-2,-1,0,1,2\}$ … úplná soustava absolutně nejmenších zbytků modulo 5,

$Z_5 = \{7,8,9,10,11\}$
$Z_5 = \{-21,-20,-19,-18,-17\}$
$Z_5 = \{4,10,16,22,28\}$
$Z_5 = \{-51,-23,-10,16,38\}$
… další příklady úplných soustav zbytků modulo 5.

Jelikož $\varphi(5) = 4$, má každá redukovaná soustava zbytků modulo 5 právě 4 modulo 5 nekongruentní prvky.

$Z_5^* = \{1,2,3,4\}$
$Z_5^* = \{-2,-1,1,2\}$
$Z_5^* = \{4,16,22,28\}$
$Z_5^* = \{-51,-23,16,38\}$
… příklady redukovaných soustav zbytků modulo 5.

Příklady úplných a redukovaných soustav zbytků modulo 6:

$Z_6 = \{0,1,2,3,4,5\}$ … úplná soustava nejmenších nezáporných zbytků modulo 6,

$Z_6 = \{-3,-2,-1,0,1,2\}$
$Z_6 = \{-2,-1,0,1,2,3\}$
… úplné soustava absolutně nejmenších zbytků modulo 6,

Jelikož $\varphi(6) = 2$, má každá redukovaná soustava zbytků modulo 6 právě 2 prvky.

$Z_6^* = \{1,5\}$
$Z_6^* = \{-1,1\}$
… redukované soustavy (nejmenších nezáporných, resp. absolutně nejmenších) zbytků modulo 6.

Tvrzení

Nechť $a, b, m \in Z$, kde $m \geq 2, NSD(a,m) = 1$. Potom platí:

a) Je-li $\{x_1,\dots,x_m\}$ úplná soustava zbytků modulo m, potom $\{ax_1 + b,\dots,ax_m + b\}$ tvoří také úplnou soustavu zbytků modulo m.

b) Je-li $\{x_1,\dots,x_{\varphi(m)}\}$ redukovaná soustava zbytků modulo m, potom $\{ax_1,\dots,ax_{\varphi(m)}\}$ tvoří také redukovanou soustavu zbytků modulo m.

Důkaz.

ad a) Stačí dokázat, že čísla $ax_i + b, i = 1,\dots,m$ jsou nekongruentní modulo m. Pokračujme sporem a předpokládejme, že existují $i \neq j$ taková, že $ax_i + b \equiv ax_j + b\ (m)$, tj. $m | a(x_i - x_j)$. Vzhledem

k $NSD(a,m)=1$ platí $m|(x_i-x_j)$, tj. $x_i \equiv x_j\ (m)$. Spor, neboť $\{x_1,\dots,x_m\}$ tvoří úplnou soustavu zbytků modulo m.
ad b) Vzhledem k již dokázané části a) stačí ukázat, že čísla $\{ax_1,\dots,ax_{\varphi(m)}\}$ jsou nesoudělná s m. Jelikož $NSD(a,m)=1$ a $NSD(x_i,m)=1, i=1,\dots,\varphi(m)$, platí $NSD(ax_i,m)=1, i=1,\dots,\varphi(m)$.

Tvrzení - Eulerova věta
Pro libovolná $a,m \in Z, m \geq 2$ taková, že $NSD(a,m)=1$ platí

$$a^{\varphi(m)} \equiv 1\ (m).$$

Důkaz.
Označme $\{x_1,\dots,x_{\varphi(m)}\}$ redukovanou soustavu zbytků modulo m. Z předchozího tvrzení vyplývá, že $\{ax_1,\dots,ax_{\varphi(m)}\}$ tvoří také redukovanou soustavu zbytků modulo m (obecně v jiném pořadí) a tudíž

$$x_1 \equiv ax_{i_1}\ (m),\dots,x_{\varphi(m)} \equiv ax_{i_{\varphi(m)}}\ (m).$$

Vynásobení všech výše uvedených kongruencí dostáváme

$$a^{\varphi(m)} \cdot x_1 \cdot \dots \cdot x_{\varphi(m)} \equiv x_1 \cdot \dots \cdot x_{\varphi(m)}\ (m)$$

a vydělením obou stran čísly $x_i, i=1,\dots,\varphi(m)$ (jsou nesoudělná s m), dostáváme dokazované tvrzení.

Jako snadný důsledek Eulerovy věty dostáváme následující tzv. malou Fermatovu větu.

Tvrzení - malá Fermatova věta
Je-li p prvočíslo, a přirozené číslo takové, že $p \nmid a$, potom platí

$$a^{p-1} \equiv 1\ (p).$$

Jako cvičení zdůvodněte, že pro libovolné prvočíslo p a libovolné přirozené číslo a platí

$$a^{p} \equiv a\ (p).$$

Příklad
Určete zbytek při dělení čísla 3^{2882} číslem 97.
Řešení.
Pro hledaný zbytek (označíme ho r_0), platí $r_0 \equiv 3^{2882}\ (97)$. Jelikož $NSD(7,97)=1$, tak z Eulerovy věty plyne $3^{96} \equiv 1\ (97)$. Aplikace věty o dělení se zbytkem dává $2882 = 30 \cdot 96 + 2$, tedy 3^{2882} má při dělení 97 stejný zbytek jako 3^2, tj. $r_0 = 9$.

Poznámka
Staří čínští matematici se chybně domnívali, že číslo p je prvočíslo právě tehdy, jestliže platí

$$2^{p-1} \equiv 1\ (p).$$

Z malé Fermatovy věty vyplývá, že pro všechna prvočísla větší než dvě uvedený vztah skutečně platí a jelikož jim nebylo známé žádné složené číslo, které by mělo stejnou vlastnost, učinili již zmíněný chybný závěr (obdobného omylu se dopustil i Fermat v případě tzv. Fermatových čísel). V dnešní době lze poměrně snadno zjistit, že nejmenší složené číslo pro které uvedený vztah platí je $341 = 11 \cdot 31$, tj. $2^{340} \equiv 1\ (341)$. Lze dokonce ukázat, že takových složených čísel (nazývaných pseudoprvočísla) existuje nekonečně mnoho. Na druhé straně lze ukázat, že jejich výskyt je v porovnání s prvočísly řídký, tzn. je relativně velká pravděpodobnost, že číslo s uvedenou vlastností bude opravdu prvočíslo. Této skutečnosti využívají tzv. pravděpodobnostní testy prvočíselnosti (číslo, které tímto testem úspěšně projde je s vysokou pravděpodobností, tj. nikoliv nutně, prvočíslo).

1.2.6. Řešení kongruencí 1. stupně a jejich soustav

V tomto odstavci se budeme zabývat úlohou, která má v oblasti diskrétní matematiky široké využití, totiž řešením kongruencí. Pro tyto účely budeme pod pojmem kongruence rozumět výraz

$$f(x) \equiv 0\ (m),$$

kde $m \in N - \{0,1\}$ je modul,

$f(x) = a_n x^n + \ldots + a_1 x + a_0$ je nenulový polynom, $\forall i\ a_i \in Z_m$ a $m \nmid a_n$

(číslo n nazýváme stupněm kongruence).

Hlavním cílem bude nalézt všechna $x \in Z$, pro která uvedená kongruence platí. V tomto kontextu je podstatné si uvědomit (dokažte!), že platí

$$f(x_0) \equiv 0\ (m) \ \rightarrow\ \forall t \in Z\ \ f(x_0 + mt) \equiv 0\ (m)$$

a tedy pokud zkoumané kongruenci vyhovuje jisté celé číslo x_0, vyhovují jí také všechna celá čísla, která jsou s x_0 kongruentní modulo m, tj. $x \equiv x_0\ (m)$. Z těchto důvodů je rozumné, a dále tak budeme činit, považovat za jedno řešení celou zbytkovou třídu $[x_0] = \{x_0 + mt | t \in Z\}$. Zřejmým důsledkem pak je skutečnost, že uvedená kongruence má nejvýše m řešení (řádně zdůvodněte!), která lze nalézt metodou „hrubé síly“, tj. postupným dosazováním čísel $0,1,\ldots,m-1$. Na druhé straně je celá řada relevantních důvodů, pro které je vhodné nalézt efektivnější způsoby řešení. Vzhledem k rozsahu skript se dále omezíme na metody řešení kongruencí 1. stupně, tj. kongruencí tvaru

$$ax \equiv b\ (m)$$

a později i jejich soustav.

Tvrzení

Nechť $NSD(m,a) = 1$. Potom kongruence $ax \equiv b\ (m)$ má pro libovolné $b \in Z$ právě jedno řešení. Toto řešení je tvaru

$$x_0 \equiv (-1)^n P_{n-1} b\ (m),$$

kde P_{n-1} je čitatel předposledního přibližného zlomku rozvoje m/a v řetězový zlomek.

Důkaz.

Z předchozích tvrzení vyplývá (vzhledem k $NSD(m,a) = 1$), že uvedená kongruence má právě jedno řešení pro libovolné b a tedy stačí nalézt jediné $x_0 \in Z$, které jí vyhovuje (řešením je pak celá zbytková třída). Označme $\delta_{n-1} = P_{n-1}/Q_{n-1}$, $\delta_n = P_n/Q_n = m/a$ poslední dva přibližné zlomky rozvoje m/a v řetězový zlomek. Mezi jejich čitateli a jmenovateli platí již dříve dokázaný vztah

$$P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n+1}, \text{ tj. } mQ_{n-1} - aP_{n-1} = (-1)^{n+1},$$

tedy

$$-aP_{n-1} \equiv (-1)^{n+1}\ (m),\ \text{tj. } a\underbrace{[(-1)^n P_{n-1} b]}_{x_0} \equiv b\ (m).$$

Jak plyne z následující poznámky, má předchozí tvrzení základní význam pro řešení obecných kongruencí 1. stupně, tj. s libovolným modulem.

Poznámka – řešení obecných kongruencí 1. stupně

- Uvažujme nyní obecnou kongruenci 1. stupně a označme $d = NSD(m,a)$. V situaci, kdy $d = 1$ postupujeme dle předchozího tvrzení, proto předpokládejme, že $d \geq 2$. V tomto případě platí:
  a) Jestliže $d \nmid b$, potom kongruence $ax \equiv b\ (m)$ nemá řešení (řádně zdůvodněte!).

b) Jestliže $d|b$, potom kongruence $ax \equiv b\ (m)$ má právě d následujících modulo m nekongruentních řešení

$$x \equiv x_0; x_0 + m_1; \dots; x_0 + (d-1)m_1\ (m),$$

kde x_0 je jediné řešení kongruence $a_1 x \equiv b_1\ (m_1), a_1 = {}^{a}/_{d}, b_1 = {}^{b}/_{d}, m_1 = {}^{m}/_{d}$.

Zdůvodněte! Využijte pravidlo, že obě strany kongruence i modul lze vydělit jejich společným dělitelem, čímž dostaneme kongruenci $a_1 x \equiv b_1\ (m_1)$, kde $NSD(m_1, a_1) = 1$. Dle předchozího tvrzení má tato kongruence jediné modulo m_1 nekongruentní řešení $x \equiv x_0\ (m_1)$, které následně vyjádříme pomocí zbytků modulo m.

- Další možnost jak vyřešit základní typ kongruence 1. stupně nám poskytuje Eulerova věta. Dokažte, že v případě, kdy $NSD(a, m) = 1$ má kongruence $ax \equiv b\ (m)$ právě jedno řešení tvaru $x \equiv a^{\varphi(m)-1} \cdot b\ (m)$.
- Pro některé speciální tvary kongruencí lze nalézt jednodušší a efektivnější způsoby jejich řešení, než je využití výše uvedených tvrzení. Např. nalezněte co nejjednodušší způsob řešení kongruencí typu $2^k x \equiv b\ (m)$.

Příklad

Nalezněte všechna řešení kongruence: a) $210x \equiv 57\ (385)$, b) $116x \equiv 60\ (148)$.

Řešení.

ad a) Pomocí Eukleidova algoritmu vypočteme $NSD(385{,}210) = 35$. Jelikož $35 \nmid 57$, nemá daná kongruence řešení.

ad b) Aplikací Eukleidova algoritmu zjistíme, že $NSD(148{,}116) = 4|60$ a tedy uvedená kongruence má právě 4 řešení nekongruentní modulo 148. Nejprve převedeme původní kongruenci na kongruence s ní ekvivalentní (oběma vyhovují stejné množiny celých čísel), kterou dostaneme vydělením obou stran i modulu 4. Dostáváme tak

$$29x \equiv 15\ (37),$$

kde $NSD(37{,}29) = 1$ a kterou řešíme dle úvodního tvrzení.

i	-1	0	1	2	3	4	5
q_i	- - -	1	3	1	1	1	2
P_i	1	1	4	5	9	14	37

Jako řešení tak dostáváme $x_0 \equiv 12\ (37)$ a jako řešení původní kongruence pak dostáváme následující 4 řešeni nekongruentní modulo 148

$$x \equiv 12; 49; 86; 123\ (148).$$

Na závěr tohoto odstavce se budeme zabývat řešením soustav kongruencí 1. stupně.

Tvrzení - Čínská věta o zbytku

Uvažujme soustavu kongruencí tvaru

$$x \equiv b_1\ (m_1), \dots, x \equiv b_k\ (m_k),$$

kde $\forall i \neq j\ NSD(m_i, m_j) = 1$. Potom daná soustava má pro libovolné pravé strany $b_1, \dots, b_k$ právě jedno řešení modulo $M = m_1 \cdot \dots \cdot m_k$. Toto řešení je tvaru

$$x \equiv x_0\ (M),$$

kde $x_0 = M_1 \cdot \bar{M}_1 \cdot b_1 + \dots + M_k \cdot \bar{M}_k \cdot b_k$, $M_i = {}^{M}/_{m_i}$ a $M_i \cdot \bar{M}_i \equiv 1\ (m_i)$.

Důkaz.

Vzhledem k definicím čísel $M, M_i, \overline{M}_i$ snadno ověříme (pouhým dosazením), že číslo x_0 vyhovuje dané soustavě. Zbývá proto ukázat, že je to jediné řešení. Označme y_0 libovolné celé číslo, které dané soustavě vyhovuje, tj. platí $\forall i\ y_0 \equiv b_i\ (m_i)$. Víme, že každá z kongruencí $x \equiv b_i\ (m_i), i = 1, \dots, k$ má právě jedno řešení modulo m_i, tedy $\forall i\ y_0 \equiv x_0\ (m_i)$. Dále si uvědomíme, že pokud platí kongruence podle několika modulů, platí i podle modulu rovnému nejmenšímu společnému násobku modulů, tedy $y_0 \equiv x_0\ (M)$, což bylo třeba dokázati.

Poznámky

- Řešení soustavy k kongruencí 1. stupně převádíme na řešení k „nezávislých" kongruencí 1. stupně, totiž $M_i \cdot \overline{M}_i \equiv 1\ (m_i)$, kde $i \in \{1, \dots, k\}$.
- Soustavu kongruencí $a_1 x \equiv b_1\ (m_1), \dots, a_k x \equiv b_k\ (m_k)$, kde $\forall i \neq j\ NSD(m_i, m_j) = 1$ a $\forall i\ NSD(a_i, m_i) = 1$ nejprve převedeme na ekvivalentní tvar $x \equiv c_1\ (m_1), \dots, x \equiv c_k\ (m_k)$. Vzhledem k tomu, že $\forall i \neq j\ NSD(m_i, m_j) = 1$, postupujeme při jejím řešení dle Čínské věty o zbytku.

Příklad

Vyřešte následující soustavu kongruencí

$$3x \equiv 4\ (5), 6x \equiv 5\ (7), 7x \equiv 5\ (9), 11x \equiv 6\ (13).$$

Výsledek zapište v soustavě nejmenších nezáporných zbytků příslušného modulu.

Řešení

Nejprve soustavu převedeme na ekvivalentní soustavu mající tvar uvedený v Čínské větě o zbytku, tj.

$$x \equiv 3\ (5), x \equiv 2\ (7), x \equiv\ 2\ (9), x \equiv 10\ (13).$$

Odtud $M = 4\,095, M_1 = 819, \overline{M}_1 = 4, M_2 = 585, \overline{M}_2 = 2, M_3 = 455, \overline{M}_3 = 2, M_4 = 315, \overline{M}_4 = 9$ a tedy $x \equiv 42\,338(4\,095)$, což v soustavě nejmenších nezáporných zbytků dává $x \equiv 1\,388\ (4\,095)$.

<u>Poznámka</u> - aritmetika velkých čísel

Procesory jsou schopny provádět „efektivní" výpočty s přirozenými čísly, které lze uložit do paměti určité velikosti (např. 64, 128 bitů). Výpočty s velkými přirozenými čísly se efektivně realizovat pomocí tzv. modulární aritmetiky, která je založena na Čínské větě o zbytku. Z této věty vyplývá, že pokud máme po dvou nesoudělné moduly $m_1, \dots, m_k$ (obvykle tvaru $2^{k_i} - 1$), lze každé $a \in \{0,1, \dots, M-1\}$, kde $M = m_1 \cdot \dots \cdot m_k$, jednoznačně reprezentovat vektorem $(a_1, \dots, a_k)$, kde $a_i = (a\ mod\ m_i)$, tj. $a_i \in \{0,1, \dots, m_i - 1\}$. Tuto k-tici nazýváme modulární reprezentací čísla a. Výpočty se v modulární reprezentaci provádí po složkách (vzhledem k jejich velikosti velmi „efektivně") následovně:

Označme $(a_1, \dots, a_k)$ modulární reprezentaci čísla a, $(b_1, \dots, b_k)$ modulární reprezentaci čísla b, potom $a + b$ má modulární reprezentaci

$$\big(a_1 + b_1\ (m_1), \dots, a_k + b_k\ (m_k)\big)$$

ab má modulární reprezentaci

$$\big(a_1 b_1\ (m_1), \dots, a_k b_k\ (m_k)\big).$$

Na závěr poznamenejme, že převody mezi „standardní" a modulární reprezentací se provádí pouze na začátku a konci výpočtu.

Příklad

Vypočtěte $(3b - 2d)(c - a)$, kde $a = 454\,545, b = 313\,131, c = 888\,888, d = 171\,717$.

Řešení.

Využijeme následující po dvou nesoudělné moduly

$$m_1 = 2^{11} - 1 = 2\,047, m_2 = 2^{13} - 1 = 8\,191, m_3 = 2^{15} - 1 = 32\,767.$$

Modulární reprezentace čísel, se kterými budeme provádět výpočty, jsou následující

$a = (a \bmod m_1, a \bmod m_2, a \bmod m_3) = (111{,}4\,040{,}28\,574)$,

$b = (b \bmod m_1, b \bmod m_2, b \bmod m_3) = (1\,987{,}1\,873{,}18\,228)$,

$c = (c \bmod m_1, c \bmod m_2, c \bmod m_3) = (624{,}2\,350{,}26\,845)$,

$d = (d \bmod m_1, d \bmod m_2, d \bmod m_3) = (1\,816{,}7\,897{,}7\,882)$.

Vlastní výpočet (prováděný po složkách) dává následující výsledky

První složka výsledku: $(3 \cdot 1\,987 - 2 \cdot 1\,816)(624 - 111) \equiv 1\,376\ (2\,047)$.

Druhá složka výsledku: $(3 \cdot 1\,873 - 2 \cdot 7\,897)(2\,350 - 4\,040) \equiv 2\,841\ (8\,191)$.

Třetí složka výsledku: $(3 \cdot 18\,228 - 2 \cdot 7\,882)(26\,845 - 28\,574) \equiv 10\,738\ (32\,767)$.

Jako modulární reprezentaci výsledku tak dostáváme $(1\,376{,}2\,841{,}10\,738)$.

Posledním krokem je převedení výsledku z jeho modulární reprezentace do „standardní“, kterou získáme jako řešení soustavy $x \equiv 1\,376\ (2\,047), x \equiv 2\,841\ (8\,191), x \equiv 10\,738\ (32\,767)$.

Aplikací Čínské věty o zbytku dostáváme

$$(3b - 2d)(c - a) = 258\,850\,619\,937.$$

Tvrzení - zobecněná Čínská věta o zbytku

Uvažujme soustavu kongruencí tvaru

$$x \equiv b_1\ (m_1), \dots, x \equiv b_k\ (m_k).$$

Potom uvedená soustava má řešení právě tehdy, jestliže

$$\forall i \neq j\ NSD(m_i, m_j) \big| (b_i - b_j).$$

Označíme-li navíc $M = NSN(m_1, \dots, m_k)$ a $c_i, d_i, i = 1, \dots, k$ taková čísla, že

$[M = d_1 \cdot \dots \cdot d_k] \wedge [\forall i\ d_i | m_i] \wedge [\forall i \neq j\ NSD(d_i, d_j)]$,

$\forall i\ \left[c_i \equiv 0\left(M/d_i\right)\right] \wedge [\, c_i \equiv 1\ (d_i)]$,

potom jediné řešení soustavy je tvaru

$$x \equiv c_1 \cdot b_1 + \dots + c_k \cdot b_k\ (M).$$

Příklad

Vyřešte soustavu kongruencí $7x \equiv 84\ (15), 7x \equiv 42\ (9), 7x \equiv 49\ (10), 7x \equiv 21\ (8)$.

Výsledek zapište v soustavě nejmenších nezáporných zbytků odpovídajícího modulu.

Řešení.

Nejprve původní soustavu převedeme na „standardizovaný“ tvar uvedený v zobecněné Čínské větě o zbytku. Dostáváme tak soustavu $x \equiv 12\ (15), x \equiv 6\ (9), x \equiv 7\ (10), x \equiv 3\ (8)$.

Nyní snadno ověříme, že $\forall i \neq j\ NSD(m_i, m_j) \big| (b_i - b_j)$, tedy daná soustava má právě jedno řešení modulo $M = NSN(15,\ 9,\ 10,\ 8) = 360$. Jelikož $360 = 2^3 \cdot 3^2 \cdot 5$, lze volit $d_1 = 1, d_2 = 9, d_3 = 5$ a $d_4 = 8$. Nyní dopočteme čísla c_1, c_2, c_3, c_4 ze vztahů

$c_1 \equiv 0(360) \wedge c_1 \equiv 1(1) \rightarrow c_1 = 0$ $\qquad$ $c_2 \equiv 0(40) \wedge c_2 \equiv 1(9) \rightarrow c_2 = 280$

$c_3 \equiv 0(72) \wedge c_3 \equiv 1(5) \rightarrow c_3 = 216$ $\qquad$ $c_4 \equiv 0(45) \wedge c_4 \equiv 1(8) \rightarrow c_4 = 225$

Odtud $x \equiv 0 \cdot 12 + 280 \cdot 6 + 216 \cdot 7 + 225 \cdot 3 \equiv 3\,867\ (360)$ a v soustavě nejmenších nezáporných zbytků $x \equiv 267\ (360)$.

1.3. Vybrané algebraické struktury

V této kapitole budou předmětem našeho zájmu algebraické struktury, které hrají důležitou roli v informačních technologiích, zejména pak v oblasti šifrování a kódování. Algebraickou strukturou budeme rozumět neprázdnou množinu (tzv. nosič algebry), na které je definovaná alespoň jedna operace. Algebraickou strukturu tak tvoří např. množina celých čísel Z s operací sčítání $+$ a násobení $\cdot$ (tvoří eukleidovský obor integrity) nebo množina Z_p (p prvočíslo) s operacemi sčítání a násobení modulo p (tvoří těleso). Smyslem pak je, zjednodušeně řečeno, zkoumat obecné vlastnosti společné jednotlivým typům algebraických struktur. Nejprve však podáme přesnější vymezení (definice) základních pojmů.

Definice – binární operace na množině

Nechť $A \neq \emptyset$ je množina. Zobrazení $*: A^2 \rightarrow A$ nazveme binární operací na množině A.

Poznámky

- Budeme také používat zápis $*: (a, b) \rightarrow a * b$, kde prvky a, b nazýváme operandy a prvek $a * b$ výsledek operace.
- Binární operaci budeme obvykle značit některým z následujících symbolů $+$ nebo $\cdot$. V případě symbolu $+$ mluvíme o sčítání, resp. o aditivním zápisu operace a píšeme $a + b$.
  V případě symbolu $\cdot$ mluvíme o násobení, resp. o multiplikativním zápisu operace a píšeme $a \cdot b$, resp. ab (tj. vynecháme symbol $\cdot$).

Definice – uzavřenost množiny vzhledem k operaci

Nechť $*$ je binární operace na $\emptyset \neq A$ a $\emptyset \neq B \subseteq A$. Řekneme, že množina B je uzavřená vzhledem k operaci $*$, jestliže $\forall a, b \in B$ platí $a * b \in B$.

Poznámka

Množina přirozených čísel je uzavřena vzhledem k operaci sčítání, ale její podmnožina všech lichých přirozených čísel není uzavřena vzhledem ke sčítání. Dále např. množina celých čísel je uzavřená vzhledem k odčítání, ale její podmnožina přirozených čísel není uzavřená vzhledem k odčítání.

Definice - základní vlastnosti binárních operací

Nechť $*$ je binární operace na množině A.

a) Řekneme, že operace $*$ je asociativní, jestliže
$$\forall a, b, c \in A \quad (a * b) * c = a * (b * c)$$
b) Řekneme, že operace $*$ je komutativní, jestliže
$$\forall a, b \in A \quad a * b = b * a$$
c) Řekneme, že operace $*$ má neutrální prvek, jestliže
$$\exists e \in A \; \forall a \in A \quad a * e = e * a.$$
Prvek e nazýváme neutrální prvek operace $*$.
d) Řekneme, že prvek $a \in A$ je symetrizovatelný, jestliže operace $*$ má neutrální prvek e a platí
$$\exists \bar{a} \in A \quad a * \bar{a} = \bar{a} * a = e$$
Prvek $\bar{a}$ nazýváme prvkem symetrickým k prvku a (vzhledem k operaci $*$).

Tvrzení

Nechť $*$ je binární operace na množině A. Potom platí:

a) Operace $*$ má nejvýše jeden neutrální prvek.

b) Je-li $*$ asociativní operace s neutrálním prvkem e, potom ke každému prvku existuje nejvýše jeden prvek symetrický. Navíc, pokud k prvkům a, b existují symetrické prvky $\bar{a}, \bar{b}$, existuje i symetrický prvek k $a * b$ a platí $\overline{a * b} = \bar{b} * \bar{a}$

Důkaz.

a) Nechť $e_1, e_2 \in A$ jsou neutrální prvky a uvažujme $e_1 * e_2$. Využijeme-li neutrality e_1, dostáváme $e_1 * e_2 = e_2$, využijeme-li neutrality e_2, dostáváme $e_1 * e_2 = e_1$, tedy $e_1 = e_2$.

b) Označme $\bar{a}, \bar{\bar{a}} \in A$ prvky symetrické k $a \in A$. Zřejmě platí

$$\bar{a} = \bar{a} * e = \bar{a} * (a * \bar{\bar{a}}) = (\bar{a} * a) * \bar{\bar{a}} = e * \bar{\bar{a}} = \bar{\bar{a}}.$$

Navíc $(a * b) * \overline{(a * b)} = (a * b) * \left(\bar{b} * \bar{a}\right) = a * \left(b * \bar{b}\right) * \bar{a} = (a * e) * \bar{a} = a * \bar{a} = e$.

Poznámky

- V případě aditivního zápisu operace mluvíme místo o neutrálním prvku o nulovém prvku (značíme 0), tj. platí $\exists 0 \in A\ \forall a \in A \quad a + 0 = 0 + a = a$. Místo o symetrickém prvku mluvíme o opačném prvku (značíme $-a$), tj. platí $a + (-a) = (-a) + a = 0$. Dále používáme zkrácené zápisy:
  - $a - b$ místo obšírnějšího zápisu $a + (-b)$,
  - $n \times a$, kde $n \in N$ místo $a + \cdots + a$ (tj. součet n prvků a), speciálně $0 \times a = 0$,
  - $(-n) \times a$, kde $n \in N$ místo $(-a) + \cdots + (-a)$ (tj. součet n opačných prvků $-a$).
- V případě multiplikativního zápisu operace mluvíme místo o neutrálním prvku o jednotkovém prvku (značíme 1), tj. platí $\exists 1 \in A\ \forall a \in A \quad a \cdot 1 = 1 \cdot a = a$. Místo o symetrickém prvku pak mluvíme o inverzním prvku (značíme a^{-1}), tj. platí $a \cdot a^{-1} = a^{-1} \cdot a = 1$. Dále používáme zkrácené zápisy:
  - a^n, kde $n \in N$ místo $a \cdot \ldots \cdot a$ (tj. součin n prvků a), speciálně $a^0 = 1$,
  - a^{-n}, kde $n \in N$ místo $a^{-1} \cdot \ldots \cdot a^{-1}$ (tj. součin n inverzních prvků a^{-1}).

  V případě, že operace násobení je komutativní, lze použít zápis $\frac{a}{b}$, resp. a/b, neboť $ab^{-1} = b^{-1}a$.

  Opět připomeňme, že znak $\cdot$ budeme v zápisu, kde nehrozí nedorozumění, běžně vynechávat.

1.3.1. Grupy

Grupa (zavedl Evariste Galois, 1811-1832) je nejdůležitější algebraická struktura s jednou binární operací. V následující části se seznámíme pouze s nejelementárnějšími pojmy a výsledky.

Definice - grupa

Nechť $*$ je binární operace na množině $G \neq \emptyset$ (tzv. nosič) s vlastnostmi:

- $\forall a,b,c \in G \quad (a*b)*c = a*(b*c)$ … asociativita
- $\exists e \in G \ \forall a \in G \quad a*e = e*a = a$ … existence neutrálního prvku
- $\forall a \in G \ \exists \bar{a} \in G \quad a*\bar{a} = \bar{a}*a = e$ … symetrizovatelnost

Potom uspořádanou dvojici $(G, *)$ nazýváme grupou a počet prvků nosiče G nazýváme řádem grupy, značíme $|G|$, resp. $ord(G)$.

Je-li navíc operace $*$ komutativní, tj. $\forall a,b \in G \quad a*b = b*a$, potom mluvíme o komutativní, resp. o abelově grupě (abelova grupa = komutativní grupa; pojmenováno Camille Jordanem na počest norského matematika Niels Henrik Abela, 1802-1829).

V navazující části budeme grupovou operaci obvykle značit buď symbolem $\cdot$ a mluvit o multiplikativní grupě $(G,\cdot)$, nebo $+$ a mluvit o aditivní grupě $(G,+)$.

Příklady aditivních grup:

$(Z,+)$ … aditivní grupa celých čísel,

$(Z_m,+)$ … aditivní grupa (nejmenších nezáporných) zbytků modulo m, $+$ je sčítání modulo m,

$(Q,+)$ … aditivní grupa racionálních čísel,

$(R,+)$ … aditivní grupa reálných čísel,

$(C,+)$ … aditivní grupa komplexních čísel.

Příklady multiplikativních grup:

$(Z_m^*, \cdot)$ … multiplikativní grupa redukovaných zbytků modulo m, $\cdot$ je násobení modulo m,

$(Q-\{0\}, \cdot)$ … multiplikativní grupa nenulových racionálních čísel,

$(R-\{0\}, \cdot)$ … multiplikativní grupa nenulových reálných čísel,

$(C-\{0\}, \cdot)$ … multiplikativní grupa nenulových komplexních čísel.

Definice – podgrupa

Nechť $(G,\cdot)$ je grupa a $\emptyset \neq H \subseteq G$. Řekneme, že $(H,\cdot)$ je podgrupa grupy $(G,\cdot)$, píšeme $(H,\cdot) \trianglelefteq (G,\cdot)$, resp. jen $H \trianglelefteq G$, jestliže podmnožina H je uzavřená vzhledem k operacím grupy G, tj. platí $\forall a,b \in H \quad ab^{-1} \in H$.

Poznámky

- Ověřte, že důsledkem vlastnosti $\forall a,b \in H \quad ab^{-1} \in H$ uvedené v definici podgrupy je platnost: $(1 \in H) \wedge (a \in H \rightarrow a^{-1} \in H) \wedge (a,b \in H \rightarrow ab \in H)$.
- Je-li $(G,\cdot)$ grupa, potom její nejmenší podgrupou je $(\{1\},\cdot)$ a největší je $(G,\cdot)$. Tyto podgrupy se nazývají nevlastní podgrupy, všechny ostatní se označují jako vlastní podgrupy.
- Počet prvků grupy, resp. podgrupy, nazýváme řádem grupy, resp. řádem podgrupy a používáme značení $|G|$ nebo $ord(G)$.
- Je třeba zdůraznit, že operace podgrupy je totožná s operací grupy a proto např. $(Z_m,+)$ není podgrupa $(Z,+)$ a to přesto, že $Z_m \subset Z$. Ze stejných důvodů není $(Z_5,+)$ podgrupou $(Z_{10},+)$.

Tvrzení

Nechť $(H,\cdot) \trianglelefteq (G,\cdot)$ a $\sim$ relace na G definovaná vztahem:

$$\forall g_1, g_2 \in G \text{ platí } g_1 \sim g_2 \leftrightarrow g_1^{-1} g_2 \in H.$$

Potom platí: a) $\sim$ je ekvivalence na G, b) $[g] = gH = \{gh | h \in H\}$, c) $\forall g_1, g_2 \in G \ |g_1| = |g_2|$.

Důkaz.

a) Reflexivita: $\forall g \in G \ g^{-1} g = 1 \in H$, tedy $g \sim g$; symetrie: pokud $g_1 \sim g_2$, je $g_1^{-1} g_2 \in H$ a tedy i $(g_1^{-1} g_2)^{-1} = g_2^{-1} g_1 \in H \rightarrow g_2 \sim g_1$; tranzitivita: $g_1 \sim g_2 \wedge g_2 \sim g_3$, tedy $g_1^{-1} g_2 \in H \wedge g_2^{-1} g_3 \in H$, proto i $(g_1^{-1} g_2)(g_2^{-1} g_3) = g_1^{-1}(g_2 g_2^{-1}) g_3 = g_1^{-1} g_3 \in H$, tj. $g_1 \sim g_3$.

b) $g_1 \in [g]$, právě když $g^{-1} g_1 \in H$, tj. $\exists h \in H \ g^{-1} g_1 = h$, tj. $g_1 = gh \in gH$.

c) Uvažujme zobrazení φ: $[g_1] = g_1 H \rightarrow [g_2] = g_2 H$ definované vztahem $\forall h \in H \ \varphi(g_1 h) = g_2 h$. Nyní stačí využít skutečnosti, že $H \trianglelefteq G$a nahlédnout, že φ je vzájemně jednoznačné zobrazení $g_1 H$ na $g_2 H$ (cvičení).

Poznámky

- Připomeňme, že ekvivalence na množině definuje její rozklad. V případě výše definované ekvivalence $\sim$ mluvíme o rozkladu grupy G podle podgrupy H a značíme ho ${}^{G}/_{H}$.
- Snadno ověříme, že jediné vlastní podgrupy aditivní grupy $(Z,+)$ jsou právě všechny celočíselné násobky pevně daného čísla $m \in N^+$, tj. $(mZ,+) \trianglelefteq (Z,+)$, kde $mZ = \{mt | t \in Z\}$. Aplikujeme-li nyní výše uvedené tvrzení, vidíme, že relace $\sim$ je definována vztahem $k \sim l \leftrightarrow k - l \in mZ$. V tomto případě jde o nám již dobře známou relaci $\equiv_m$ býti kongruentní modulo m. Místo zápisu ${}^{Z}/_{mZ}$ používáme dříve zavedené značení Z_m a mluvíme o zbytkových třídách modulo m.

Definice – index podgrupy

Nechť $H \trianglelefteq G$, potom počet tříd rozkladu ${}^{G}/_{H}$ nazýváme index podgrupy H v grupě G a značíme ho $[G:H]$.

Tvrzení (Joseph Luis Lagrange, 1736-1813)

Nechť G je konečná grupa a $H \trianglelefteq G$. Potom platí $|G| = [G:H] \cdot |H|$.

Důkaz.

Vzhledem k definici indexu podgrupy a již dokázané skutečnosti, že všechny třídy rozkladu ${}^{G}/_{H}$ mají stejnou mohutnost, je tvrzení zřejmé.

V další části se velmi stručně seznámíme s důležitou třídou grup, totiž s cyklickými grupami. Jde o grupy s jednoduchou strukturou, které se často vyskytují např. v oblasti šifrování a kódování.

Tvrzení

Nechť $(G, \cdot)$ je grupa, $g \in G$. Potom $(\langle g \rangle, \cdot) \trianglelefteq (G, \cdot)$, kde $\langle g \rangle = \{g^n | n \in Z\}$, tj. množina $\langle g \rangle$ je uzavřená na součin, inverzi a obsahuje jednotkový prvek.

Důkaz.

Stačí si uvědomit následující: $g^n g^m = g^{n+m}, g^0 = 1, (g^n)^{-1} = g^{-n}$.

Definice – cyklická grupa/podgrupa

Nechť $(G, \cdot)$ je grupa, $g \in G$.

a) Podgrupu $(\langle g \rangle, \cdot)$ definovanou v předchozím tvrzení nazýváme cyklickou podgrupou grupy $(G, \cdot)$.

b) Grupu $(G,\ \cdot)$ nazýváme cyklickou, jestliže $\exists g \in G$ takový, že $G = \langle g \rangle$.
Prvek $g \in G$ nazýváme generátorem grupy, resp. podgrupy.

Poznámky

- Každá cyklická grupa (zřejmě i její podgrupa) je komutativní.
- $(Z, +)$ je cyklická grupa mající právě dva generátory -1 a 1, tj. $(Z, +) = (\langle 1 \rangle, +) = (\langle -1 \rangle, +)$.
- $(Z_m, +)$ je cyklická grupa a platí $(Z_m, +) = (\langle k \rangle, +)$ právě když $NSD(k, m) = 1$, tj. generátorem je libovolný prvek $k \in Z_m$, který je nesoudělný s modulem m.
- Multiplikativní grupa $(Z_m^*,\ \cdot)$ je cyklická právě tehdy, když $m = 2, 4, p^k, 2p^k$, kde $k \in N^+$ a p je liché prvočíslo.

Tvrzení

Nechť $(G,\ \cdot)$ je cyklická grupa s generátorem g. Potom platí:
a) Každá podgrupa cyklické je opět cyklická.
b) Je-li $|G| = m$, potom $G = \{g^0 = 1, g, \dots, g^{m-1}\}$. Navíc $g^k = g^l \leftrightarrow k \equiv l\ (m)$ a
$G = \langle g^k \rangle \leftrightarrow NSD(k, m) = 1$.
c) Je-li $|G| = m$, potom pro libovolné k takové, že $k|m$ existuje jediná podgrupa řádu k. Žádné jiné podgrupy grupa G neobsahuje.

Definice - izomorfismus

Řekneme, že grupy $(G_1,\ \cdot_1), (G_2,\ \cdot_2)$ jsou izomorfní (píšeme $G_1 \cong G_2$), jestliže existuje zobrazení $\varphi: G_1 \rightarrow G_2$ takové, že:

a) φ je vzájemně jednoznačné zobrazení G_1 na G_2,
b) $\forall g_1, h_1 \in G_1\ \ \varphi(g_1 \cdot_1 h_1) = \varphi(g_1) \cdot_2 \varphi(h_1)$.

Zobrazení φ nazýváme izomorfismus grup G_1, G_2.

Poznámky

- Izomorfismus grup lze chápat jako jejich rovnost, kdy se obě grupy liší pouze formálně (např. mají jinak značené prvku, grupovou operaci apod.).
  Grupa $(G_1,\ \cdot_1)$ s nosičem $G_1 = \{1, -1, i, -i, j, -j, k, -k\}$ a operací násobení danou tabulkou

$\cdot_1$	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-i	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	-1	1	k	-k	-j	j
-i	-i	i	1	-1	-k	k	j	-j
j	j	-j	-k	k	-1	1	i	-i
-j	-j	j	k	-k	1	-1	-i	i
k	k	-k	j	-j	-i	i	-1	1
-k	-k	k	-j	j	i	-i	1	-1

  je izomorfní s grupou $(G_2,\ \cdot_2)$ s nosičem

  $G_2 = \left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}-1&0\\0&-1\end{pmatrix}, \begin{pmatrix}-i&0\\0&i\end{pmatrix}, \begin{pmatrix}i&0\\0&-i\end{pmatrix}, \begin{pmatrix}0&1\\-1&0\end{pmatrix}, \begin{pmatrix}0&-1\\1&0\end{pmatrix}, \begin{pmatrix}0&i\\i&0\end{pmatrix}, \begin{pmatrix}0&-i\\-i&0\end{pmatrix}\right\}$, kde $i^2 = -1$ a

  operace $\cdot_2$ je „obyčejné“ násobení matic.
- Výše uvedená grupa je nekomutativní (např. $ij = -ji = k, jk = -kj = i, ki = -ik = j$) a nazývá se grupa kvaternionů.

Tvrzení

a) Každá konečná cyklická grupa řádu m je izomorfní s grupou $(Z_m, +)$.

b) Každá nekonečná cyklická grupa je izomorfní s grupou $(Z, +)$.

c) Každá grupa prvočíselné ho řádu je cyklická. (zřejmý důsledek Lagrangeova tvrzení)

Dalším důležitým příkladem grup jsou tzv. symetrické, resp. permutační grupy. Pro jejich definici však potřebujeme mít zaveden pojem permutace.

Definice - permutace

Nechť A je n-prvková množina, tj. $|A| = n$. Potom permutací na množině A rozumíme libovolné vzájemně jednoznačné zobrazení A na A.

Poznámky

- Permutací na množině A lze interpretovat jako uspořádání prvků množiny A, přesněji jako libovolnou uspořádanou n-tici tvořenou právě všemi prvky množiny A.
- Permutace budeme značit symboly $\pi, \rho, \sigma, \ldots$ a pro jejich zápis budeme využívat tzv. dvouřádkový zápis (později také zápis ve tvaru součinu (obvykle disjunktních) cyklů).
  Dvouřádkový zápis permutace na množině $A = \{1,2, \ldots, n\}$ má tvar

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix},$$

  kde horní řádek obsahuje vzory a dolní řádek obsahuje jim odpovídající obrazy. Je zřejmě, že při zápisu permutace není podstatné pořadí sloupců, podstatné je pouze přiřazení obrazů vzorům. Z tohoto pohledu např. zápisy $\begin{pmatrix} 1&2&3&4&5 \\ 3&4&2&5&1 \end{pmatrix}, \begin{pmatrix} 3&1&5&2&4 \\ 2&3&1&4&5 \end{pmatrix}$ definují stejnou permutaci.

Označíme-li S_n množinu všech permutací na n-prvkové množině, lze na S_n definovat operaci násobení permutací $\pi, \rho \in S_n$ následovně:

$$\pi\rho = \begin{pmatrix} 1 & 2 & \cdots & n \\ \rho(\pi(1)) & \rho(\pi(2)) & \cdots & \rho(\pi(n)) \end{pmatrix}.$$

Je-li např. $\pi = \begin{pmatrix} 1&2&3&4&5 \\ 5&3&1&2&4 \end{pmatrix}, \rho = \begin{pmatrix} 1&2&3&4&5 \\ 2&1&5&4&3 \end{pmatrix}$, dostáváme $\pi\rho = \begin{pmatrix} 1&2&3&4&5 \\ 3&5&2&1&4 \end{pmatrix}, \rho\pi = \begin{pmatrix} 1&2&3&4&5 \\ 3&5&4&2&1 \end{pmatrix}$.

Nyní snadno ověříme (permutace je vzájemně jednoznačné zobrazení), že $(S_n, \cdot)$ je grupa, tj. platí:

i) $\forall \pi, \rho, \tau \in S_n \quad (\pi \cdot \rho) \cdot \tau = \pi \cdot (\rho \cdot \tau)$,

ii) $\exists id \in S_n \; \forall \pi \in S_n \quad id \cdot \pi = \pi \cdot id = \pi$,

iii) $\forall \pi \in S_n \; \exists \pi^{-1} \in S_n \quad \pi \cdot \pi^{-1} = \pi^{-1} \cdot \pi = id$.

Konkrétně $id = \begin{pmatrix} 1&2&\cdots&n \\ 1&2&\cdots&n \end{pmatrix}$ a je-li $\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix}$, potom $\pi^{-1} = \begin{pmatrix} \pi(1) & \pi(2) & \cdots & \pi(n) \\ 1 & 2 & \cdots & n \end{pmatrix}$

Např. pro $\pi = \begin{pmatrix} 1&2&3&4&5 \\ 4&3&2&5&1 \end{pmatrix}$ dostáváme $\pi^{-1} = \begin{pmatrix} 4&3&2&5&1 \\ 1&2&3&4&5 \end{pmatrix} = \begin{pmatrix} 1&2&3&4&5 \\ 5&3&2&1&4 \end{pmatrix}$.

Definice – symetrická/permutační grupa

Grupu $(S_n, \cdot)$ nazýváme symetrickou grupou na n-prvkové množině. Každou podgrupu grupy $(S_n, \cdot)$ nazýváme permutační grupou.

Poznámka
Symetrická grupa $(S_n,\cdot)$ je řádu $n!$ a pro $n \geq 3$ není komutativní.

Tvrzení – Cayleyova věta (Arthur Cayley, 1821-1895)
Každá konečná grupa $(G,\ \cdot)$ řádu n je izomorfní s nějakou podgrupou grupy $(S_n,\cdot)$.
Důkaz.
$\forall a \in G$ definujme zobrazení $\pi_a: G \to G$ vztahem $\forall g \in G\ \ \pi_a(g) = ga$. Zobrazení π_a jsou vzájemně jednoznačně a tedy definují permutace na G (řádu n), která zřejmě tvoří podgrupu $(S_n,\cdot)$.

Nyní se krátce vrátíme k vyjádření permutací pomocí tzv. cyklů. Jde o přehledný a efektivní způsob zápisu permutací, který se používá v celé řadě aplikací (transpoziční šifry, Pólyaova enumerační metoda atd.).

Definice - cyklus
Řekneme, že permutace $\pi \in (S_n,\cdot)$ je cyklus délky k, jestliže:

i) $\exists\{i_1,\dots,i_k\} \subseteq \{1,\dots,n\}$ taková, že $\forall j \in \{1,\dots,k-1\}\ \left(\pi(i_j) = i_{j+1}\right) \wedge (\pi(i_k) = i_1)$,
ii) $\forall i \notin \{i_1,\dots,i_k\}\ \ \pi(i) = i$.

V tomto případě píšeme $\pi = (i_1,\dots,i_k)$. Speciálně, cyklus délky 2 se nazývá transpozice.

Např. permutace $\pi = \begin{pmatrix}1&2&3&4&5&6&7&8\\5&7&3&2&4&6&8&1\end{pmatrix}$ je cyklus délky 6 a píšeme $\pi = (1,5,4,2,7,8)$, resp. obšírněji $\pi = (1,5,4,2,7,8)(3)(6)$.

Poznámky
- Je dobré si uvědomit, že z definice cyklu vyplývá, že jeho zápis není jednoznačný. Lze ho totiž interpretovat jako umístění prvků uspořádané k-tice $(i_1,\dots,i_k)$ na kružnici. Zjednodušeně řečeno, nezáleží na tom, kde cyklus začíná, ale na tom, jaký prvek následuje za daným prvkem při pohybu (např. ve směru hodinových ručiček) po kružnici. Z tohoto pohledu např. platí
  $(1,5,4,2,7,8) = (8,1,5,4,2,7) = (7,8,1,5,4,2) = (2,7,8,1,5,4) = (4,2,7,8,1,5) = (5,4,2,7,8,1)$.
- Cyklus je speciální permutace a proto lze cykly násobit.
  Např. $(1,5,3,2)(4,3) = (1,5,4,3,2)$, kdežto $(4,3)(1,5,3,2) = (1,5,3,4,2)$.
- Řekneme, že cykly $\pi,\rho \in S_n$, kde $\pi = (i_1,\dots,i_k), \rho = (j_1,\dots,j_l)$ jsou disjunktní, jestliže $\{i_1,\dots,i_k\} \cap \{j_1,\dots,j_l\} = \emptyset$.
  S výhodou se využívá zřejmá skutečnost, že součin disjunktních cyklů je komutativní!

Tvrzení
i) Každou permutaci lze zapsat, až na pořadí jednoznačně, ve tvaru součinu disjunktních cyklů.
ii) Každý cyklus lze zapsat ve tvaru součinu transpozic s tím, že toto vyjádření není jednoznačné. Platí však, že každý cyklus, resp. permutaci lze zapsat vždy pouze jako součin sudého počtu transpozic, nebo lichého počtu transpozic.

Poznámky
- Identická permutace $id \in S_n$ má jako součin disjunktních cyklů zápis $id = (1)(2)\dots(n)$.

- Je-li $\pi = (i_1, i_2, \dots, i_{k-1}, i_k)$ cyklus, potom π^{-1} je také cyklus a má tvar $\pi^{-1} = (i_k, i_{k-1}, \dots, i_2, i_1)$. Např. $(1,5,4,3,2)^{-1} = (2,3,4,5,1)$. Navíc, každá transpozice je zřejmě inverzní sama k sobě, tedy $(i_1, i_2)^{-1} = (i_1, i_2)$.
- Cyklus $(i_1, i_2, i_3, \dots, i_k)$ lze zapsat ve tvaru součinu transpozic následovně
$$(i_1, i_2, i_3, \dots, i_k) = (i_1, i_2)(i_1, i_3) \cdot \dots \cdot (i_1, i_k).$$
- Je-li π permutace zapsaná ve tvaru disjunktních cyklů, potom inverzní permutace π^{-1} má tvar součinu inverzních cyklů tvořících permutaci π (vzhledem k jejich disjunktnosti nezáleží na jejich pořadí).
Např. pro $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 5 & 2 & 6 & 7 & 4 & 3 & 1 & 8 \end{pmatrix} = (198)(2573)(46)$ dostáváme $\pi^{-1} = (891)(3752)(46)$.

Definice – sudá, lichá permutace

Permutaci nazveme sudou, jestliže ji lze zapsat ve tvaru součinu sudého počtu transpozic. Ostatní permutace nazýváme liché.

Poznámky

- Snadno se přesvědčíme, že součin sudých permutací je opět sudá permutace, inverzní permutace k sudé je také sudá a identita je sudá. Označíme-li tedy A_n množinu všech sudých permutací na n-prvkové množině, je zřejmé, že tato množina je uzavřená vzhledem k násobení permutací a tedy $(A_n, \cdot) \trianglelefteq (S_n, \cdot)$. Grupa $(A_n, \cdot)$ se nazývá alternující grupa, je řádu $n!/2$ (polovina permutací je sudých a polovina lichých) a pro $n \geq 4$ je nekomutativní.
- Důležité příklady permutačních grup jsou tzv. dihedrální grupy $D_n, n \geq 2$, Které popisují prostorové symetrie pravidelných n-úhelníků (jejich vrcholy pro tyto účely očíslujeme $1, \dots, n$). Dihedrální grupa D_n je řádu $2n$ (obsahuje n otočení a n osových symetrií).
- Symetrie obdélníka (vrcholy číslujeme 1, 2, 3, 4) tvoří tzv. Kleinovu čtyřgrupu (Felix Klein, 1849-1925). Obsahuje následující permutace:
  $(13)(24)$ … otočení o 180°,
  $(1)(2)(3)(4)$ … otočení o 360°,
  $(12)(34)$ … překlopení kolem osy procházející středy stran 12 a 34,
  $(14)(23)$ … překlopení kolem osy procházející středy stran 14 a 23.

Příklad

Dihedrální grupa D_4 popisuje prostorové symetrie čtverce (vrcholy očíslovány 1, 2, 3, 4), tj. obsahuje permutace popisující otáčení a osovou symetrii.

Permutace popisující otáčení čtverce:

(1234) … otočení o 90°, $(13)(24)$ … otočení o 180°,
(1432) … otočení o 270°, $(1)(2)(3)(4)$ … otočení o 360° (identita).

Permutace popisující osové symetrie čtverce (překlopení kolem 4 os symetrie):

$(14)(23)$ … překlopení kolem osy procházející středy stran 14 a 24,
$(12)(34)$ … překlopení kolem osy procházející středy stran 12 a 34,
$(1)(3)(24)$ … překlopení kolem osy vedoucí vrcholy 1 a 3,
$(13)(2)(4)$ … překlopení kolem osy vedoucí vrcholy 2 a 4.

Nyní se krátce seznámíme s algebraickými strukturami majícími dvě binární operace, které budeme standardně označovat $+$ a $\cdot$.

1.3.2. Okruhy, obory integrity

Definice – okruh

Nechť $+, \cdot$ jsou dvě binární operace definované na množině $A \neq \emptyset$ (nosič okruhu) takové, že:

- $\forall a, b, c \in A \quad (a + b) + c = a + (b + c)$,
- $\exists 0 \in A \ \forall a \in A \quad a + 0 = 0 + a = a$,
- $\forall a \in A \ \exists -a \in A \quad (-a) + a = a + (-a) = 0$,
- $\forall a, b \in A \quad a + b = b + a$,

tj. $(A, +)$ tvoří abelovu grupu, dále

- $\forall a, b, c \in A \quad (ab)c = a(bc)$,
- $\exists 1 \in A \ \forall a \in A \quad 1a = a1 = a$,
- $\forall a \in A \ \exists -a \in A \quad (-a) + a = a + (-a) = 0$,
- $\forall a, b, c \in A \quad (a + b)c = ac + bc \ \wedge \ a(b + c) = ab + ac$,

potom uspořádanou trojici $(A, +, \cdot)$ nazýváme okruhem.

Poznámky

- Příklady důležitých okruhu: $(Z, +, \cdot), (Z_m, +, \cdot), (Q, +, \cdot), (R, +, \cdot), (C, +, \cdot), (M_n, +, \cdot)$, kde M_n je množina všech reálných/komplexních čtvercových matic řádu n.
- Z vlastností okruhových operací $+, \cdot$ lze odvodit často využívanou vlastnost nulového prvku
$$\forall a \in A \quad 0a = 0.$$
Jelikož $0 = 0 + 0$ dostáváme $0a = (0 + 0)a$, tedy z distribučního zákona $(0 + 0)a = 0a + 0a$ a tudíž $0a = 0a + 0a$. Přičtením opačného prvku $-(0a)$ dostáváme $0 = 0a$.
- Je třeba upozornit, že v okruhu obecně neplatí $ab = 0 \ \rightarrow \ (a = 0) \vee (b = 0)$ (využíváme např. při řešení rovnic), tj. mohou existovat $(a \neq 0) \wedge (b \neq 0)$ taková, že $ab = 0$. Např. v okruhu $(Z_{12}, +, \cdot)$ dostáváme $3 \cdot 4 = 0, 6 \cdot 6 = 0$ apod.

Definice – dělitel nuly

Nechť $(A, +, \cdot)$ je okruh. Řekneme, že prvek $a \in A$ je dělitelem nuly, jestliže $\exists b \in A - \{0\} \ a \cdot b = 0$. Je-li navíc $a \neq 0$, mluvíme o vlastním děliteli nuly, jinak o nevlastním děliteli nuly.

Snadno se přesvědčíme, že v $(Z_{18}, +, \cdot)$ jsou 2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16 vlastní dělitele nuly (0 je nevlastní dělitel nuly).

Definice – obor integrity

Nechť $(A, +, \cdot)$ je okruh, který nemá vlastní dělitele nuly, tj. $\forall a, b \in A \ (ab = 0) \rightarrow (a = 0) \vee (b = 0)$, potom řekneme, že $(A, +, \cdot)$ je obor integrity.

Definice - charakteristika

Nechť $(A, +, \cdot)$ je obor integrity. Nejmenší $p \in N^+$ takové, že $p \times 1 = 0$ nazveme charakteristikou oboru integrity $(A, +, \cdot)$. Jestliže takové p neexistuje, mluvíme o oboru integrity charakteristiky 0.

Poznámky

- Připomeňme, že $p \times 1$ je zkrácený zápis za součet p prvků 1.
- Snadno se přesvědčíme, že:
$(Z_p, +, \cdot)$, kde p je prvočíslo, je obor integrity charakteristiky p,

$(Z, +, \cdot), (Q, +, \cdot), (R, +, \cdot), (C, +, \cdot)$ jsou obory integrity charakteristiky 0.

Je-li m číslo složené, potom $(Z_m, +, \cdot)$ není obor integrity (vlastními děliteli nuly jsou čísla soudělná s m).

Tvrzení

Každý obor integrity má prvočíselnou charakteristiku, nebo charakteristiku nula.

Důkaz.

Uvažujme obor integrity a označme p nejmenší kladné přirozené číslo takové, že $p \times 1 = 0$ (pokud neexistuje, jde o charakteristiku 0, jinak zřejmě $p \geq 2$). Pokud p není prvočíslo, lze psát $p = nm$, kde $2 \leq n, m < p$, a platí $p \times 1 = nm \times 1 = (n \times 1)(m \times 1)$. Vzhledem k tomu, že obor integrity nemá vlastní dělitele nuly, dostáváme $(n \times 1 = 0) \vee (m \times 1 = 0)$. Spor s volbou p jako nejmenší takové, že $p \times 1 = 0$.

Definice - Eukleidovská norma oboru integrity

Nechť $(A, +, \cdot)$ je obor integrity a $\delta: A - \{0\} \rightarrow N$ je funkce taková, že:

a) $\forall a, b \in A - \{0\}\ \ \delta(a) \leq \delta(ab)$,

b) $\forall a, b \in A, b \neq 0\ \ \exists q, r \in A$ tak, že $a = bq + r$, kde buď $r = 0$, nebo $\delta(r) < \delta(b)$.

Definice – Eukleidovský obor integrity

Obor integrity $(A, +, \cdot)$ nazveme Eukleidovský, jestliže na $(A, +, \cdot)$ existuje Eukleidovská norma.

Poznámky

- $(Z, +, \cdot)$ je Eukleidovský obor integrity, kde absolutní hodnota je Eukleidovská norma.
- V každém Eukleidovském oboru integrity lze pro nalezení největšího společného dělitele využít Eukleidův algoritmus.

1.3.3. Tělesa, polynomy nad tělesy

Definice – těleso

Nechť $+,\ \cdot$ jsou dvě binární operace definované na množině $T \neq \emptyset$ (nosič tělesa) takové, že $(T, +)$ tvoří abelovu grupu, dále $(T - \{0\},\ \cdot)$ tvoří abelovu grupu a platí distributivní zákony. Potom uspořádanou trojici $(T, +,\ \cdot)$ nazýváme tělesem.

Poznámky

- Snadno se přesvědčíme, že každý konečný obor integrity je tělesem (tedy ke každému nenulovému prvku existuje prvek inverzní).
- Jelikož každé těleso je oborem integrity, je pojem charakteristika používán také u těles a proto každé těleso má prvočíselnou charakteristiku, nebo charakteristiku 0.
- Podle počtu prvků nosiče rozdělujeme tělesa na konečná a nekonečná.
  Např. $(Q, +,\ \cdot)$ … nekonečné těleso racionálních čísel charakteristiky 0,
  $(R, +,\ \cdot)$ … nekonečné těleso reálných čísel charakteristiky 0,
  $(C, +,\ \cdot)$ … nekonečné těleso komplexních čísel charakteristiky 0,
  $\left(Z_p, +,\ \cdot\right)$ … konečné těleso (p je prvočíslo) charakteristiky p.
  Pozor - $(Z, +,\ \cdot)$ není těleso, ale pouze eukleidovský obor integrity (charakteristiky 0).
- Zjednodušeně řečeno, tělesa lze považovat za algebraické struktury, ve kterých lze počítat tak, jak je „obvyklé“, tj. obě operace mají vlastnosti, na které jsme zvyklí (asociativita, komutativita, distributivita, lze odčítat i dělit nenulovými prvky).

Definice - izomorfismus těles

Řekneme, že tělesa $(T_1, +_1,\ \cdot_1), (T_2, +_2,\ \cdot_2)$ jsou izomorfní (píšeme $T_1 \cong T_2$), jestliže existuje zobrazení $\varphi\colon T_1 \rightarrow T_2$ takové, že:

a) φ je vzájemně jednoznačné zobrazení T_1 na T_2,

b) $\forall a, b \in T_1$ platí $\varphi(a +_1 b) = \varphi(a) +_2 \varphi(b)$,
$\varphi(a \cdot_1 b) = \varphi(a) \cdot_2 \varphi(b)$.

Zobrazení φ nazýváme izomorfismus těles T_1, T_2.

Definice - podtěleso, rozšíření tělesa

Nechť $(T, +,\ \cdot)$ je těleso a $\emptyset \neq K \subseteq T$. Řekneme, že $(K, +,\ \cdot)$ je podtěleso tělesa $(T, +,\ \cdot)$, píšeme $(K, +,\ \cdot) \trianglelefteq (T, +,\ \cdot)$, resp. jen $K \trianglelefteq T$, jestliže K je uzavřená vzhledem k operacím tělesa T, tj. platí:

- $\forall a, b \in K \quad a - b \in K$,
- $\forall a, b \in K - \{0\} \quad ab^{-1} \in K$.

V tomto případě také říkáme, že těleso T je rozšířením tělesa K a píšeme T/K.

Poznámky

- Např. $(Q, +,\ \cdot) \trianglelefteq (R, +,\ \cdot) \trianglelefteq (C, +,\ \cdot)$, tedy těleso reálných čísel je rozšířením tělesa racionálních čísel, těleso komplexních čísel je rozšířením tělesa reálných čísel.
- Snadno ověříme, že pokud $(K_1, +,\ \cdot)$ a $(K_2, +,\ \cdot)$ jsou podtělesa tělesa $(T, +,\ \cdot)$, potom $(K_1 \cap K_2, +,\ \cdot)$ je podtěleso $(T, +,\ \cdot)$.

Definice – prvotěleso

Nechť $(T, +,\ \cdot)$ je těleso. Průnik všech jeho podtěles nazýváme prvotěleso tělesa $(T, +,\ \cdot)$.

Poznámky

- Prvotěleso tělesa charakteristiky 0 je izomorfní s tělesem racionálních čísel. Speciálně - těleso racionálních čísel je prvotěleso tělesa reálných i komplexních čísel.

Hlavním cílem následující části je najít všechna konečná tělesa. Z tohoto důvodu je nutné nejprve zformulovat některé elementární výsledky o polynomech.

Definice - polynom

Nechť $(T, +, \cdot)$ je těleso, $a_0, a_1, \dots, a_n \in T, a_n \neq 0, x \notin T$. Potom výraz $a_0 + a_1 x + \cdots + a_n x^n$ nazýváme polynomem stupně n (v neurčité x) nad tělesem T. Polynom, jehož vedoucí koeficient (tj. koeficient u nejvyšší mocniny x) je roven 1 se nazývá monický polynom.

Poznámky

- Polynomy budeme značit $f(x), g(x), r(x), q(x)$ apod. Symbolem $T[x]$ pak označíme množinu všech polynomů (v neurčité x) nad tělesem T.
- Rovnost polynomů $f(x) = \sum_{i=0}^{n} a_i x^i, g(x) = \sum_{i=0}^{m} b_i x^i$ definujeme následovně
$$f(x) = g(x) \leftrightarrow (n = m) \wedge (\forall i \in \{0, \dots, n\}\ a_i = b_i).$$
V tomto kontextu je třeba upozornit na rozdíl mezi polynomem a funkcí, kterou tento polynom definuje. Různé polynomy totiž mohou definovat stejné funkce. Např. pro $f(x), g(x) \in Z_3[x]$, kde $f(x) = 2x^3 + 2x + 1, g(x) = 2x^4 + x^2 + x + 1$platí $\forall n \in Z_3\ f(n) = g(n)$, tj. definují stejnou funkci, ale různé polynomy.
- Stupeň polynomu $f(x)$ budeme značit $st(f)$, resp. $st\big(f(x)\big)$ (je roven nejvyšší mocnině u které se vyskytuje nenulový koeficient). Polynomy stupně 0 jsou právě všechny nenulové prvky tělesa T, tj. polynomy $a_0 \neq 0$ (nenulové „konstanty“). Nulový polynom je roven nulovému prvku $0 \in T$, přičemž jeho stupeň buď nedefinujeme, nebo definujeme roven -1.

Definice - hodnota, kořen polynomu

Nechť $f(x) = \sum_{i=0}^{n} a_i x^i$ je polynom nad tělesem T. Potom hodnotu polynomu $f(x)$ v bodě $b \in T$ značíme $f(b)$ a definujeme vztahem $f(b) = \sum_{i=0}^{n} a_i b^i$.
Kořen (nulový bod) nenulového polynomu $f(x) \in T[x]$ je definován jako libovolné $b \in T$ takové, že $f(b) = 0$.

Poznámky

- Je-li $b \in T, f(x) \in T[x]$, potom zřejmě i $f(b) \in T$.
- Pro výpočet hodnoty $f(b)$ polynomu $f(x) = \sum_{i=0}^{n} a_i x^i$ využíváme obvykle Hornerovo schéma, které je založeno na vztahu
$$f(b) = \sum_{i=0}^{n} a_i b^i = \big(\dots\big((a_n b + a_{n-1})b + a_{n-2}\big)b + \cdots + a_1\big)b + a_0.$$
Výpočet pak zapisujeme do následující tabulky

b	a_n	a_{n-1}	…	a_1	a_0
	0	$P_n b$	…	$P_2 b$	$P_1 b$
$\sum$	$P_n = a_n$	$P_{n-1} = P_n b + a_{n-1}$	…	$P_1 = P_2 b + a_1$	$P_0 = P_1 b + a_0 = f(b)$

Příklad

Pro $f(x) \in R[x]$, kde $f(x) = 5 + 4x - x^3 + 3x^4 - 2x^5$, určete $f(0{,}5)$.

0,5	-2	3	-1	0	4	5
	0	-1	1	0	0	2
$\sum$	-2	2	0	0	4	$7 = f(0{,}5)$

Pro $f(x) \in Z_5[x]$,kde $f(x) = 3 + 2x^2 + x^3 + 2x^5, b = 3$ dostáváme následující

3	2	0	1	2	0	3
	0	1	3	2	2	1
$\sum$	2	1	4	4	2	$4 = f(3)$

Nyní na množině $T[x]$ nadefinujeme (všeobecně známé) operace sčítání a násobení polynomů.
Nechť $f(x), g(x) \in T[x]$, kde $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$. Potom:

$$f(x) + g(x) = \sum_{i=0}^{max\{st(f),st(g)\}} (a_i + b_i)x^i,$$
$$f(x) \cdot g(x) = \sum_{k=0}^{st(f)+st(g)} c_k x^k, \text{ kde } c_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

Zřejmě platí (zdůvodněte): $st(f + g) \leq \max\{st(f), st(g)\}$, $st(f \cdot g) = st(f) + st(g)$.

Tvrzení

Nechť $(T, +, \cdot)$ je těleso. Potom $(T[x], +, \cdot)$ je Eukleidovský obor integrity.

Důkaz.

Jelikož T je těleso, snadno ověříme, že $(T[x], +, \cdot)$ je obor integrity, kde Eukleidovskou normu definujeme jako stupeň polynomu. Z následující věty o dělení polynomů se zbytkem vyplývá, že jde skutečně o Eukleidovskou normu.

(poznamenejme, že $(T[x], +, \cdot)$ nemůže být těleso, neboť k polynomu $f(x) = x$ neexistuje inverzní prvek)

Tvrzení – věta o dělení polynomů se zbytkem

Nechť $(T, +, \cdot)$ je těleso, $f(x), g(x) \in T[x]$, $g(x)$ nenulový polynom. Potom existují jediné polynomy $q(x), r(x) \in T[x]$ takové, že

$$f(x) = g(x)q(x) + r(x), \text{ kde } st(r) < st(g), \text{ nebo } r(x) = 0 \text{ (nulový polynom).}$$

Důkaz.

Označme $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{i=0}^{m} b_i x^i$, kde $n = st(f), m = st(g)$.

Je-li $n < m$ položíme $q(x) = 0$ (nulový polynom) a $r(x) = f(x)$.

Je-li $n \geq m$, postupujeme indukcí dle rozdílu $n - m$.

Pro $n - m = 0$ položíme $q(x) = a_n b_n^{-1}$ a $r(x) = f(x) - g(x)q(x)$. Zřejmě $st(r) < st(g)$, nebo $r(x) = 0$ (nulový polynom).

Předpokládejme nyní (tzv. indukční předpoklad), že uvedené tvrzení platí pro libovolné dva polynomy, jejichž rozdíl stupňů je ostře menší než $n - m$ a dokážeme, že v tom případě platí i polynomy $f(x), g(x)$, pro které je rozdíl stupňů roven $n - m$.

Položme $q_1(x) = a_n b_m^{-1} x^{n-m}$ a $f_1(x) = f(x) - g(x)q_1(x)$ (vztah označíme $(*)$). Polynom $f_1(x)$ je zřejmě buď nulový polynom (v tom případě je důkaz hotový), nebo $st(f_1) \leq n - 1$. Z indukčního předpokladu aplikovaného na polynomy $f_1(x)$ a $g(x)$ dostáváme existenci polynomů $q_2(x), r(x)$ takových, že $f_1(x) = g(x)q_2(x) + r(x)$ (vztah označíme $(**)$), kde $st(r) < st(g)$ nebo $r(x) = 0$.

Dosazením vztahu $(**)$ do $(*)$ dostáváme $f(x) = g(x)\big(q_1(x) + q_2(x)\big) + r(x)$, kde $st(r) < st(g)$, nebo $r(x) = 0$.

Příklad

Nechť $f(x), g(x) \in Z_5[x]$, kde

$$f(x) = 3x^7 + 4x^6 + x^5 + 3x^3 + 2x + 1, g(x) = 4x^5 + 3x^4 + 2x^3 + x^2.$$

Nalezněte podíl $q(x)$ a zbytek $r(x)$ při dělení polynomu $f(x)$ polynomem $g(x)$.

Řešení.

$3x^7 + 4x^6 + x^5 + 3x^3 + 2x + 1 = (4x^5 + 3x^4 + 2x^3 + x^2)(2x^2 + 2x + 4) + (2x^4 + 3x^3 + x^2 + 2x + 1)$,

tedy $q(x) = 2x^2 + 2x + 4$ a $r(x) = 2x^4 + 3x^3 + x^2 + 2x + 1$.

Poznámky

- Polynom $q(x)$ z předchozího tvrzení nazýváme podíl (po dělení polynomu $f(x)$ polynomem $g(x)$). V případě polynomu $r(x)$ mluvíme o zbytku. (zcela analogicky jako v případě věty o dělení se zbytkem pro celá čísla).
- Jestliže ve větě o dělení polynomů se zbytkem nastane situace, kdy zbytek $r(x)$ je nulový polynom, říkáme, že $g(x)$ dělí (beze zbytku) $f(x)$ a píšeme $g(x)|f(x)$. O polynomu $g(x)$ mluvíme jako o děliteli $f(x)$ a o polynomu $f(x)$ mluvíme jako o násobku $g(x)$. (zcela analogicky jako v Z)
- Jednoduchým (a často využívaným) důsledkem věty o dělení se zbytkem je skutečnost, že $a \in T$ je kořen polynomu $f(x) \in T[x]$, tj. $f(a) = 0$, právě když $(x - a)|f(x)$, tj. $f(x) = (x - a)q(x)$.
  V této souvislosti poznamenejme, že koeficienty polynomu $q(x)$ lze získat z Hornerova schématu. Např. pro $f(x) \in Z_7[x]$, kde $f(x) = 3x^6 + 6x^5 + 2x^4 + x^3 + x^2 + 5x + 3$ dostáváme

2	3	6	2	1	1	5	3
	0	6	3	3	1	4	4
$\sum$	3	5	5	4	2	2	$0 = f(2)$

  tedy $f(x) = (x + 5)(3x^5 + 5x^4 + 5x^3 + 4x^2 + 2x + 2)$, tj. $(x + 5)|f(x)$.
- Řekneme, že $a \in T$ je $k(\in N^+)$ násobný kořen polynomu $f(x) \in T[x]$, jestliže $(x - a)^k \big| f(x)$ a $(x - a)^{k+1} \nmid f(x)$. Např. pro polynom z předchozí odrážky dostáváme další aplikací Hornerova schématu na polynom $3x^5 + 5x^4 + 5x^3 + 4x^2 + 2x + 2 \in Z_7[x]$

2	3	5	5	4	2	2
	0	6	1	5	4	5
$\sum$	3	4	6	2	6	0

  tedy $f(x) = (x + 5)(3x^5 + 5x^4 + 5x^3 + 4x^2 + 2x + 2) =$

  $= (x + 5)^2(3x^4 + 4x^3 + 6x^2 + 2x + 6)$, tj. $(x + 5)^2|f(x)$.

  Další aplikací Hornerova schématu dostáváme

2	3	4	6	2	6
	0	6	6	3	3
$\sum$	3	3	5	5	2

  Odtud $f(x) = (x + 5)^3(3x^3 + 3x^2 + 5x + 5) + 2$ a tedy $(x + 5)^3 \nmid f(x)$. Zjistili jsme tedy, že číslo 2 je dvojnásobný kořen polynomu $f(x)$.

Důsledek

Zřejmým důsledkem výše uvedené poznámky, resp. věty o dělení polynomů se zbytkem, je skutečnost, že každý nenulový polynom $f(x) \in T[x]$ stupně n má v tělese T nejvýše n kořenů.

Definice - ireducibilní polynom

Nechť $f(x) \in T[x]$, kde $st(f) \geq 1$. Řekneme, že $f(x)$ je ireducibilní polynom nad tělesem T, jestliže

$$f(x) = f_1(x)f_2(x) \;\rightarrow\; \big(st(f_1) = st(f)\big) \vee \big(st(f_2) = st(f)\big).$$

(tj. ireducibilní polynom nelze zapsat jako součin dvou polynomů stupně ostře menšího než $st(f)$)

Ireducibilní polynomy hrají důležitou roli (analogickou prvočíslům v oboru N^+) a proto se nyní seznámíme se základními poznatky vztahujícími se k ireducibilním polynomům nad různými tělesy.

Poznámky

- Je důležité si uvědomit, že ireducibilita souvisí s tělesem, nad kterým uvažujeme polynom. Např. polynom $f(x) = 2x^3 + 3x^2 + x + 4$ je ireducibilní nad tělesem Z_7 a není ireducibilní nad Z_5, neboť $f(x) = (x + 4)(2x^2 + 1)$. Polynom $f(x) = x^2 + 1$ je ireducibilní nad R, ale není ireducibilní nad C, neboť $f(x) = (x + i)(x - i)$, ani nad Z_2, neboť $f(x) = (x + 1)^2$.

Tvrzení

Nechť $(T, +, \cdot)$ je těleso. Potom platí:

i) Každý polynom stupně 1 je ireducibilní nad T.

ii) Má-li polynom stupně alespoň 2 kořen, potom není ireducibilní nad T.

iii) Každý polynom stupně 2 nebo 3 je ireducibilní nad T právě tehdy, jestliže nemá kořen.

iv) Každý polynom $f(x) \in T[x]$ stupně alespoň 1, lze zapsat ve tvaru $f(x) = af_1(x) \cdot \ldots \cdot f_k(x)$, kde $a \in T$ a $f_1(x), \ldots, f_k(x) \in T[x]$ jsou monické ireducibilní polynomy. Tento rozklad je jednoznačný, pokud nepřihlížíme k pořadí polynomů v součinu. (analogie prvočíselných rozkladů)

Důkaz.

i) Jelikož $st(fg) = st(f) + st(g)$ je tvrzení zřejmé (součin fg je polynom stupně 1).

ii) Je-li $f(a) = 0 \;\wedge\; st(f) \geq 2$, dostáváme z výše uvedených poznámek $f(x) = (x - a)q(x)$, kde $st(q) = st(f) - 1 \geq 1$.

iii) Stačí si uvědomit, že $2 = 1 + 1$ a $3 = 2 + 1$, navíc jde o jediné možnosti, jak daná čísla (stupně polynomů) zapsat ve tvaru součtu dvou nenulových přirozených čísel (stupňů jednotlivých činitelů součinu). Sčítanec 1 reprezentuje polynom stupně 1, který má zřejmě vždy kořen.

Poznámky

- Jelikož $(Z, +, \cdot)$ i $(T[x], +, \cdot)$, kde T je těleso, jsou eukleidovské obory integrity, lze pojmy typické pro $(Z, +, \cdot)$ jako eukleidovský obor integrity analogicky zavést i pro $(T[x], +, \cdot)$.
  Jde o následující pojmy:
  - ireducibilní polynomy nad T (analogie prvočísel), rozklad polynomu na součin ireducibilních polynomů (analogie kanonických rozkladů),
  - dělitel polynomu (polynom, který dělí daný polynom beze zbytku), společný dělitel polynomů (polynom dělící beze zbytku každý z uvažovaných polynomů), NSD … největší společný dělitel polynomů (= společný dělitel uvažovaných polynomů, který je největšího stupně a navíc monický), nesoudělnost polynomů (největší společný dělitel má stupeň 0),

- společný násobek polynomů (= nenulový polynom, který je dělitelný beze zbytku každým z uvažovaných polynomů), NSN … nejmenší společný násobek polynomů (= společný násobek uvažovaných polynomů, který je nejmenšího stupně a navíc monický).

Analogicky se využívá věta o dělení se zbytkem i Eukleidův algoritmus (aplikované na polynomy) pro nalezení největšího společného dělitele, resp. nejmenšího společného násobku.

- V souvislosti s pojmy NSD, NSN poznamenejme, že vzhledem k tomu, že T je těleso, platí $g(x)|f(x) \rightarrow k \cdot g(x)|f(x)$, kde $k \in T - \{0\}$. Z tohoto důvodu by $NSD(f,g)$, resp. $NSN(f,g)$ nebyly určeny jednoznačně a jsou proto definovány jako monické polynomy.

Příklad

Uvažujme polynomy $f(x), g(x) \in Z_5[x]$, kde

$$f(x) = 2x^4 + 2x^3 + 4x^2 + 3x + 4,\ g(x) = 3x^4 + x^3 + 4x^2 + x + 1\ .$$

Spočtěte $NSD\big(f(x), g(x)\big)$ a) pomocí Eukleidova algoritmu, b) pomocí rozkladu na ireducibilní polynomy.

ad a) Aplikací Euklieidova algoritmu (v tělese Z_5) dostáváme:

$$f(x) = 4 \cdot g(x) + (3x^3 + 3x^2 + 4x),$$
$$g(x) = (x+1)(3x^3 + 3x^2 + 4x) + (2x^2 + 2x + 1),$$
$$(3x^3 + 3x^2 + 4x) = (4x)(2x^2 + 2x + 1).$$

Tedy $NSD(f,g) = x^2 + x + 3$ (tj. až na případnou multiplikativní konstantu jde o poslední od nuly různý zbytek v Eukleidově algoritmu).

ad b) Rozložit polynomy na ireducibilní polynomy je obecně složité, nicméně v tomto případě vystačíme se znalostí kořenů (postupně a opakovaně dosazujeme prvky tělesa Z_5, pro výpočet hodnoty polynomu využijeme Hornerovo schéma). Postupujeme následně:

1	2	2	4	3	4
	0	2	4	3	1
$\sum$	2	4	3	1	$0 = f(1)$

Odtud $f(x) = (x+4)(2x^3 + 4x^2 + 3x + 1)$

1	2	4	3	1
	0	2	1	4
$\sum$	2	1	4	0

Odtud $f(x) = (x+4)^2(2x^2 + x + 4)$

3	2	1	4
	0	1	1
$\sum$	2	2	0

Odtud $f(x) = (x+4)^2(x+2)(2x+2) = 2(x+4)^2(x+2)(x+1)$.

Analogicky postupujeme i v případě polynomu $g(x)$. Dostáváme:

1	3	1	4	1	1
	0	3	4	3	4
$\sum$	3	4	3	4	$0 = g(1)$

Odtud $g(x) = (x+4)(3x^3 + 4x^2 + 3x + 4)$

2	3	4	3	4
	0	1	0	1
$\sum$	3	0	3	0

Odtud $g(x) = (x+4)(x+3)(3x^2+3)$

2	3	0	3
	0	1	2
$\sum$	3	1	0

Odtud $g(x) = (x+4)(x+3)^2(3x+1) = 3(x+4)(x+3)^2(x+2)$.
Rozklady na ireducibilní polynomy jsou

$$f(x) = 2(x+1)(x+2)(x+4)^2, g(x) = 3(x+2)(x+3)^2(x+4)$$

a proto $NSD\big(f(x), g(x)\big) = (x+2)(x+4) = x^2+x+3$.

Tvrzení – Základní věta algebry

Nechť $f(x) \in C[x], st(f) = n \geq 1$. Potom $f(x)$ má v tělese C alespoň jeden kořen.

Důsledky

- Bezprostředním důsledkem Základní věty algebry je skutečnost, že $f(x) \in C[x], st(f) = n \geq 1$ má v oboru komplexních čísel právě n kořenů počítáno včetně jejich násobnosti.
- Nechť $f(x) \in R[x]$, potom platí:
  - Je-li $f(x)$ lichého stupně, potom má alespoň jeden reálný kořen.
  - Je-li $c \in C$ kořen polynomu $f(x)$, potom i $\bar{c}$ je kořenem.
    ($\bar{c}$ označuje číslo komplexně sdružené k c)
- Nechť $f(x) \in R[x]$. Ukažte, že platí $f(\bar{c}) = \overline{f(c)}$.

Poznámky

- V souvislosti se Základní větou algebry vyvstává otázka, jak určit kořeny polynomu pouze na základě znalosti jeho koeficientů a s využitím základních algebraických operací, tj. sčítání, odčítání, násobení, dělení a n-té odmocniny (tzv. řešitelnost polynomů v radikálech). Dlouho byly známé vztahy pro nalezení kořenů polynomů stupně 2, 3 a 4. Matematici proto vyvíjeli značné úsilí, aby nalezli obdobné vztahy i pro polynomy stupně 5 a vyšší, nicméně neúspěšně. Teprve norský matematik N. H. Abel ukázal (přesahuje rámec těchto skript), že takové vzorce neexistují, tj. polynomy stupně 5 a vyšší nejsou řešitelné v radikálech.
- Dnes se prakticky využívá pouze obecně známý vzorec pro řešení kvadratických rovnic, ostatní případy se řeší numericky.

Tvrzení - ireducibilita nad R, C

a) Jediné ireducibilní polynomy nad C jsou právě všechny polynomy 1. stupně. Každý polynom $f(x) \in C[x]$ lze proto rozložit jediným způsobem na součin

$$f(x) = a(x-r_1)^{n_1} \cdot \ldots \cdot (x-r_k)^{n_k},$$

kde $a, r_1, \ldots, r_k \in C,\ \forall i \neq j\ r_i \neq r_j$ a $\sum_{i=1}^{k} n_i = n$.

b) Jediné ireducibilní polynomy nad R jsou právě všechny polynomy 1. stupně a všechny polynomy 2. stupně (tj. ax^2+bx+c) se záporným diskriminantem (tj. $b^2-4ac<0$). Každý polynom $f(x) \in R[x]$ lze proto rozložit jediným způsobem na součin

$$f(x) = a(x - r_1)^{n_1} \cdot \ldots \cdot (x - r_k)^{n_k} \cdot (x^2 + p_1 x + q_1)^{m_1} \cdot \ldots \cdot (x^2 + p_l x + q_l)^{m_l},$$

kde $a, r_1, \ldots, r_k, p_1, \ldots, p_l, q_1, \ldots, q_l \in R$, $\forall i \neq j \left(r_i \neq r_j\right) \wedge \left((p_i, q_i) \neq (p_j, q_j)\right)$,

$\forall i\ p_i^2 - 4q_i < 0$, $\sum_{i=1}^{k} n_i + 2\sum_{i=1}^{l} m_i = n$.

Důkaz.

a) Bezprostřední důsledek Základní věty algebry, dále tvrzení, že r_i je kořenem $f(x)$ právě když $(x - r_i) | f(x)$ a skutečnosti, že polynomy 1. stupně jsou vždy ireducibilní.

b) Jelikož $R[x] \subset C[x]$, lze každé $f(x) \in R[x]$ rozložit v C na součin uvedený v části a), tj. monických polynomů 1. stupně. Vzhledem k tomu, že $f(\bar{c}) = \overline{f(c)}$, musí platit – je-li r_i kořen, potom i $\overline{r_i}$ je kořen. Komplexní kořeny mající nenulovou imaginární část, se tudíž vyskytují v páru jako komplexně sdružená čísla a proto platí $(x - r_i)(x - \overline{r_i}) = x^2 + p_i x + q_i$, kde $p_i, q_i \in R \wedge p_i^2 - 4q_i < 0$.

Tvrzení – existenční věta pro ireducibilní polynomy nad Z_p

Nechť p je prvočíslo, $n \in N^+$. Potom existuje polynom stupně n ireducibilní nad Z_p.

Zcela analogicky, jako jsme v eukleidovském oboru integrity Z nadefinovali relaci „býti kongruentní modulo m“, nám umožňuje věta o dělení polynomů se zbytkem nadefinovat na eukleidovském oboru integrity $T[x]$ relaci „býti kongruentní modulo $q(x)$“.

Definice – býti kongruentní modulo $q(x)$

Řekneme, že polynomy $f(x), g(x) \in T[x]$, kde $(T, +, \cdot)$ je těleso, jsou kongruentní modulo $q(x) \in T[x]$, jestliže oba polynomy dávají při dělení polynomem $q(x)$ stejný zbytek.

Poznámky

- Skutečnost, že polynomy $f(x), g(x)$ jsou kongruentní modulo $q(x)$, vyjadřujeme některým z následujících zápisů:

  $$f(x) \equiv g(x)\ \left(mod\ q(x)\right), f(x) \equiv g(x)\ \left(q(x)\right), \text{ resp. } f(x) \equiv_{q(x)} g(x).$$

  V opačném případě ($f(x), g(x)$ nemají při dělení $q(x)$ stejný zbytek) píšeme $f(x) \not\equiv g(x)\ \left(q(x)\right)$ a říkáme, že uvedené polynomy nejsou kongruentní modulo $q(x)$.
- Dále budeme používat zápis $f(x) = \left(g(x)\ mod\ q(x)\right)$, kterým vyjádříme skutečnost, že polynom $f(x)$ je roven zbytku při dělení polynomu $g(x)$ modulem $q(x)$.

  Snadno ověříme, že např. pro polynomy $f(x), g(x), q(x) \in Z_5[x]$, kde

  $$f(x) = 4x^5 + 2x^3 + x^2 + 3x + 1, g(x) = 4x^6 + 4x^5 + 2x^4 + 1, q(x) = 2x^3 + 3x + 4,$$

  platí $f(x) \equiv g(x)\ \left(mod\ q(x)\right)$, resp. $(3x^2 + 4x + 4) = g(x)\ \left(mod\ q(x)\right)$

Tvrzení

Nechť $q(x) \in T[x]$. Potom relace býti kongruentní modulo $q(x)$ je ekvivalence na eukleidovském oboru integrity $(T[x], +, \cdot)$.

Důkaz – cvičení pro čtenáře.

Poznámka

Ekvivalence býti kongruentní modulo $q(x)$ definuje rozklad množiny $T[x]$, který značíme $T[x]/q(x)$.

Jako reprezentanty jednotlivých tříd ekvivalence bereme právě všechny zbytky po dělení polynomem $q(x)$ a tedy $T[x]/q(x) = \{f(x) \in T[x] \mid st(f) < st(q)\}$.

Nyní, analogicky jako případě relace býti kongruentní modulo m, nedefinujeme na množině $T[x]/q(x)$ binární operace sčítání a násobení modulo $q(x)$ následovně.

Je-li $f(x), g(x) \in T[x]/q(x)$, potom:

- $f(x) + g(x) = \big(f(x) + g(x)\ mod\ q(x)\big)$,
  kde $+$ na levé straně rovnosti je sčítání v $T[x]/q(x)$ a $+$ na pravé straně je sčítání v $T[x]$. Vzhledem k tomu, že $st(f+g) \leq \max\{st(f), st(g)\} < st(q)$ jsou obě operace totožné.
- $f(x) \cdot g(x) = \big(f(x) \cdot g(x)\ mod\ q(x)\big)$,
  kde $\cdot$ na levé straně rovnosti je násobení v $T[x]/q(x)$, kdežto $\cdot$ na pravé straně je „obyčejné“ násobení polynomů v $T[x]$.
  (tj. provedeme součin $f(x) \cdot g(x)$ v $T[x]$ a jako součin v $T[x]/q(x)$ uvedeme zbytek po dělení součinu $f(x) \cdot g(x)$ polynomem $q(x)$)

Příklad

Nechť $f(x), g(x) \in Z_7[x]/(5x^4 + 2x^3 + 4x + 2)$, kde $f(x) = 3x^3 + 6x^2 + 5x + 2, g(x) = 4x^2 + 5$ potom dostáváme:

$f(x) + g(x) = 3x^3 + 3x^2 + 5x, \qquad f(x)g(x) = x^3 + 6x^2 + 4x + 4$

Tvrzení - podílové těleso eukleidovského oboru integrity

Nechť $(T, +, \cdot)$ je těleso, $q(x) \in T[x]$ je polynom ireducibilní nad T. Potom $\left(T[x]/q(x), +, \cdot\right)$ je těleso.

Poznámky

- Těleso $\left(T[x]/q(x), +, \cdot\right)$ z výše uvedeného tvrzení nazýváme podílové těleso eukleidovského oboru integrity $(T[x], +, \cdot)$.
- Těleso komplexních čísel lze zavést jako podílové těleso $R[x]/(x^2 + 1)$ jehož prvky tvoří polynomy stupně nejvýše 1 (tj. polynomy $ax + b$, kde $a, b \in R$).
  Operace sčítání: $(a_1x + b_1) + (a_2x + b_2) = (a_1 + a_2)x + (b_1 + b_2)$
  Operace násobení: $(a_1x + b_1) \cdot (a_2x + b_2) = (a_1b_2 + a_2b_1)x + (b_1b_2 - a_1a_2)$
  Speciálně tedy $x^2 = -1$ (= zbytek po dělení polynomu x^2 polynomem $x^2 + 1$).
  Vidíme tedy, že pokud nahradíme symbol x symbolem i, dostáváme všeobecně známý algebraický zápis komplexních čísel a standardní operace sčítání a násobení komplexních čísel.

Důsledek

Z výše uvedeného tvrzení a existenční věty pro ireducibilní polynomy nad Z_p plyne, že pro libovolné $n \in N^+$ a libovolné prvočíslo p existuje ireducibilní polynom $q(x) \in Z_p[x]$ stupně n a tedy $\left(Z_p[x]/q(x), +, \cdot\right)$ je těleso. Toto těleso má charakteristiku p a celkem p^n prvků (polynomů ze $Z_p[x]$ stupně ostře menšího než n).

Definice - Galoisovo těleso

Těleso $\left(\left.Z_p[x]\right/_{q(x)}, +, \cdot\right)$, kde $st(q) = n$ nazýváme Galoisovo těleso a značíme $GF(p^n)$.

Poznámka

Zdůrazněme, že Galoisovo těleso je nezávislé na volbě ireducibilního polynomu, ale pouze na jeho stupni, tj. každý polynom $q(x)$ stupně n ireducibilní nad Z_p vede ke stejnému (izomorfnímu) $GF(p^n)$.

Tvrzení

Každé konečné těleso je izomorfní s Galoisovým tělesem $GF(p^n)$ pro vhodné prvočíslo p a kladné přirozené číslo n.

Důsledek

Těleso $(Z_p[x], +, \cdot)$ je prvotěleso tělesa $GF(p^n)$ pro libovolné $n \in N^+$, tj. $(Z_p[x], +, \cdot)$ je prvotěleso libovolného tělesa charakteristiky p.

Poznámka

Následující obsahuje ukázky Galoisových těles $GF(p^n)$ pro vybrané hodnoty p a n.

$GF(2^2) = \left.Z_2[x]\right/_{(x^2+x+1)}$, $GF(2^3) = \left.Z_2[x]\right/_{(x^3+x+1)}$,

$GF(2^4) = \left.Z_2[x]\right/_{(x^4+x+1)}$, $GF(2^5) = \left.Z_2[x]\right/_{(x^5+x^2+1)}$,

$GF(3^2) = \left.Z_3[x]\right/_{(x^2+x+2)}$, $GF(3^3) = \left.Z_3[x]\right/_{(x^3+2x+1)}$,

$GF(5^2) = \left.Z_5[x]\right/_{(x^2+x+1)}$, $GF(5^3) = \left.Z_5[x]\right/_{(x^3+2x+1)}$.

Poznámka

Připomeňme, že množina všech nenulových prvků každého tělesa tvoří multiplikativní grupu. V případě konečných těles $GF(p^n)$ je příslušná multiplikativní grupa cyklická (tedy existuje její generátor) a budeme ji značit $GF(p^n)^*$. (Je multiplikativní grupa těles Q, R, C cyklická? Proč?)

Definice – primitivní kořen/prvek

Primitivním kořenem tělesa $GF(p^n)$ nazýváme generátor jeho cyklické multiplikativní grupy $GF(p^n)^*$.

Definice – diskrétní exponenciála

Nechť α je primitivní kořen tělesa $GF(p^n)$. Potom funkci $exp_\alpha: \{0,1,\dots,p^n-2\} \to GF(p^n)^*$ definovanou vztahem $exp_\alpha(k) = \alpha^k$ nazýváme diskrétní exponenciální funkcí se základem α.

Poznámky

- Vzhledem k cykličnosti multiplikativní grupy $GF(p^n)^*$, která má $p^n - 1$ prvků, skutečně postačuje množina $\{0,1,\dots,p^n-2\}$ jako definiční obor funkce exp_α.
- Funkce exp_α je zřejmě vzájemné jednoznačné zobrazení množiny $\{0,1,\dots,p^n-2\}$ na množinu $GF(p^n)^*$ a tedy existuje k němu inverzní zobrazení (viz následující definice).

Definice – diskrétní logaritmus/index funkce

Nechť α je primitivní kořen tělesa $GF(p^n)$. Potom inverzní funkci k diskrétní exponenciále se základem α označujeme ind_α a nazýváme diskrétním logaritmem, resp. index funkcí o základu α.

Poznámky

Diskrétní logaritmus/index funkci lze využít pro snadné násobení a dělení v $GF(p^n)$. Platí totiž:

$ind_\alpha(xy) \equiv ind_\alpha(x) + ind_\alpha(y)\ \big(mod\ (p^n - 1)\big)$,

$ind_\alpha(xy^{-1}) \equiv ind_\alpha(x) - ind_\alpha(y)\ \big(mod\ (p^n - 1)\big)$,

$ind_\alpha\big(x^k\big) \equiv k \cdot ind_\alpha(x)\ \big(mod\ (p^n - 1)\big)$.

Definice – Zech/Jacobi logaritmus

Nechť α je primitivní kořen tělesa $GF(p^n)$. Potom Zech, resp. Jacobiho logaritmem o základu α nazýváme funkci Z_α: $\{1, \dots, p^n - 1\} \rightarrow \{0, \dots, p^n - 2\}$ takovou, že $\alpha^{Z_\alpha(k)} = 1 + \alpha^k$ a jestliže $1 + \alpha^k = 0$, potom definujeme $Z_\alpha(k) = 0$.

Poznámka

Zech logaritmus lze využít při sčítání v $GF(p^n)$, neboť platí (α označuje primitivní kořen):
Je-li $i > j$, potom $\alpha^i + \alpha^j = \alpha^j\big(\alpha^{i-j} + 1\big) = \alpha^j \cdot \alpha^{Z_\alpha(i-j)} = \alpha^{j+Z_\alpha(i-j)}$.

Příklad - těleso $GF(2^3)$

Polynom $f(x) = x^3 + x + 1$ je zřejmě ireducibilní nad Z_2. Označíme-li symbolem α kořen polynomu $f(x)$, tj. $\alpha^3 + \alpha + 1 = 0$ (zřejmě $\alpha \notin Z_2$), potom $GF(2^3) = \{c_2\alpha^2 + c_1\alpha + c_0 | c_0, c_1, c_2 \in Z_2\}$.
Prvek α je primitivní kořen $GF(2^3)$ a tedy je generátorem cyklické grupy $GF(2^3)^*$ mající řád 7 a tudíž všechny nenulové prvky tělesa $GF(2^3)$ lze vyjádřit jako mocniny α. Vzhledem k tomu, že

$$\alpha^3 = \alpha + 1, \alpha^4 = \alpha^2 + \alpha, \alpha^5 = \alpha^2 + \alpha + 1, \alpha^6 = \alpha^2 + 1, \alpha^7 = 1,$$

dostáváme $GF(2^3) = \{0, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, 1(= \alpha^7)\}$.
Nyní je evidentně snadné provádět v tělese $GF(2^3) = \{0, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, 1(= \alpha^7)\}$ násobení i dělení prvků (využíváme vlastnosti diskrétní exponenciály a $\alpha^7 = 1$).
S využitím Zech logaritmu je snadné provádět sčítání. Platí

$$Z_\alpha(1) = 3, Z_\alpha(2) = 6, Z_\alpha(3) = 1, Z_\alpha(4) = 5, Z_\alpha(5) = 4, Z_\alpha(6) = 2, Z_\alpha(7) = 0$$

a tedy např.

$$\alpha^2 + \alpha^6 = \alpha^2 \cdot \alpha^{Z_\alpha(6-2)} = \alpha^2 \cdot \alpha^5 = \alpha^7 = 1,\ \alpha^3 + \alpha^5 = \alpha^3 \cdot \alpha^{Z_\alpha(5-3)} = \alpha^3 \cdot \alpha^6 = \alpha^9 = \alpha^2.$$

Poznámka

Těleso $GF(2^3)$ lze zkonstruovat i pomocí polynomu $g(x) = x^3 + x^2 + 1$, který je ireducibilní nad Z_2. Označíme-li symbolem β kořen polynomu $g(x)$, tj. $\beta^3 + \beta^2 + 1 = 0$, dostáváme

$$\beta^3 = \beta^2 + 1, \beta^4 = \beta^2 + \beta + 1, \beta^5 = \beta + 1, \beta^6 = \beta^2 + \beta, \beta^7 = 1.$$

V tomto případě dostáváme následující hodnoty Zech logaritmu

$$Z_\beta(1) = 5, Z_\beta(2) = 3, Z_\beta(3) = 2, Z_\beta(4) = 6, Z_\beta(5) = 1, Z_\beta(6) = 4, Z_\beta(7) = 0$$

a tedy např.

$\beta^2 + \beta^6 = \beta^2 \cdot \beta^{Z_\beta(6-2)} = \beta^2 \cdot \beta^6 = \beta^8 = \beta,\ \beta^3 + \beta^5 = \beta^3 \cdot \beta^{Z_\beta(5-3)} = \beta^3 \cdot \beta^3 = \beta^6.$

Poznamenejme však, že obě takto zkonstruovaná tělesa $GF(2^3)$ jsou izomorfní.

Přehled značení

$\wedge$	… logická spojka „a“ (konjunkce, and)
$\vee$	… logická spojka „nebo“ (disjunkce, or)
$\oplus$	… logická spojka „vylučující nebo“ (or exclusive, xor)
$\rightarrow$	… implikace (jestliže)
$\leftrightarrow$	… ekvivalence (právě když)
$\bar{}$, resp. $\neg$	… negace
::	… zkratka za slovní spojení takov(ý/á/é), že …
N	… množina přirozených čísel $0,1,2,\ldots$
N^+	… množina kladných přirozených čísel
Z	… množina celých čísel
Z_m	… úplná soustava zbytků modulo $m \in N^+$
Q	… množina racionálních čísel
R	… množina reálných čísel
C	… množina komplexních čísel
$\{a_1, \ldots, a_n\}$	… neuspořádaná n-tice, tj. množina skládající se z prvků $a_1, \ldots, a_n$
$(a_1, \ldots, a_n)$	… uspořádaná n-tice
$\{a \mid V(a)\}$	… množina prvků s vlastností V
$A \cap B$	… průnik množin A, B
$A \cup B$	… sjednocení množin A, B
$A - B$	… rozdíl množin A, B
$\bar{A}$	… doplněk množiny A
$A \times B$	… kartézský součin množin A, B
$P(A)$	… potenční množina (systém všech podmnožin množiny A)
$\lvert A \rvert$	… počet prvků (mohutnost, kardinalita) množiny A
S_n	… množina všech permutací řádu n (symetrická grupa)
$GF(p^n)$	… Galoisovo těleso ($n \in N^+, p$ prvočíslo)
$\equiv$	… relace býti kongruentní (modulo m)
$\mid$	… relace býti dělitelem
$\preccurlyeq_{Le}$	… relace lexikografického uspořádání
$f(a)$	… hodnota funkce f v bodě a
$\{a_n\}_{n=0}^{\infty}$, resp. $(a_n)_{n=0}^{\infty}$	… číselná posloupnost
$\lceil x \rceil$	… horní celá část čísla x
$\lfloor x \rfloor$	… dolní celá část čísla x
$\{x\}$	… lomená část x
$\ln x$	… přirozený logaritmus čísla x
$NSD(\ \ )$	… největší společný dělitel čísel, polynomů
$NSN(\ \ )$	… nejmenší společný násobek čísel, polynomů

Tabulka prvočísel (menších než 3 650)

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541
547	557	563	569	571	577	587	593	599	601
607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733
739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863
877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997	1009	1013
1019	1021	1031	1033	1039	1049	1051	1061	1063	1069
1087	1091	1093	1097	1103	1109	1117	1123	1129	1151
1153	1163	1171	1181	1187	1193	1201	1213	1217	1223
1229	1231	1237	1249	1259	1277	1279	1283	1289	1291
1297	1301	1303	1307	1319	1321	1327	1361	1367	1373
1381	1399	1409	1423	1427	1429	1433	1439	1447	1451
1453	1459	1471	1481	1483	1487	1489	1493	1499	1511
1523	1531	1543	1549	1553	1559	1567	1571	1579	1583
1597	1601	1607	1609	1613	1619	1621	1627	1637	1657
1663	1667	1669	1693	1697	1699	1709	1721	1723	1733
1741	1747	1753	1759	1777	1783	1787	1789	1801	1811
1823	1831	1847	1861	1867	1871	1873	1877	1879	1889
1901	1907	1913	1931	1933	1949	1951	1973	1979	1987
1993	1997	1999	2003	2011	2017	2027	2029	2039	2053
2063	2069	2081	2083	2087	2089	2099	2111	2113	2129
2131	2137	2141	2143	2153	2161	2179	2203	2207	2213
2221	2237	2239	2243	2251	2267	2269	2273	2281	2287
2293	2297	2309	2311	2333	2339	2341	2347	2351	2357
2371	2377	2381	2383	2389	2393	2399	2411	2417	2423
2437	2441	2447	2459	2467	2473	2477	2503	2521	2531
2539	2543	2549	2551	2557	2579	2591	2593	2609	2617
2621	2633	2647	2657	2659	2663	2671	2677	2683	2687
2689	2693	2699	2707	2711	2713	2719	2729	2731	2741
2749	2753	2767	2777	2789	2791	2797	2801	2803	2819
2833	2837	2843	2851	2857	2861	2879	2887	2897	2903
2909	2917	2927	2939	2953	2957	2963	2969	2971	2999
3001	3011	3019	3023	3037	3041	3049	3061	3067	3079
3083	3089	3109	3119	3121	3137	3163	3167	3169	3181
3187	3191	3203	3209	3217	3221	3229	3251	3253	3257
3259	3271	3299	3301	3307	3313	3319	3323	3329	3331
3343	3347	3359	3361	3371	3373	3389	3391	3407	3413
3433	3449	3457	3461	3463	3467	3469	3491	3499	3511
3517	3527	3529	3533	3539	3541	3547	3557	3559	3571
3581	3583	3593	3607	3613	3617	3623	3631	3637	3643