Obsah

Kapitola 1
Úvod

Teoretická aritmetika je spojením elementární aritmetiky a algebry. Teoretická aritmetika zavádí a popisuje vlastnosti elementární aritmetiky a pomocí algebraických nástrojů je dokazuje.

Součástí teoretické aritmetiky je také teorie čísel. **Teorie čísel** se zabývá vlastnostmi čísel (především celých) v matematických operacích a rozšiřuje aritmetiku o další vlastnosti. Základními vlastnostmi celých čísel je jejich prvočíselnost, dělitelnost jinými čísly, uspořádání v množinách, ... Spojovacím článkem mezi aritmetikou a teorií čísel jsou číselné obory a číselné soustavy, které definují různé druhy hodnot a jejich znakovou reprezentaci, která následně také určují pravidla a postupy při aritmetických operacích s nimi.

Kapitola 2
Matematická operace

Nejdůležitějším pojmem aritmetiky a dá se říct i celé matematiky je operace. Matematická operace je postup, který na základě daných vstupů vyprodukuje (podle definice početní operace) jednu nebo více hodnot (nazývaných též výstupní hodnoty, výsledky nebo výstupy). Kolik vstupních a výstupních hodnot daná operace přijímá a předává na výstup plyne z její definice. Nejčastěji se vyskytující operace jsou unární operace a binární operace. Matematická operace se ale nemusí týkat jen čísel. Vstupem operace mohou být i různé matematické objekty jako například množiny, vektory, logické hodnoty, ...

Operace je zobrazení z kartézského součinu nějakých množin **A** (vstupní hodnoty) do kartézského součinu nějakých množin **B** (výstupní hodnoty). V mnoha případech platí: $A = B$. Formálně zapsáno je tedy operace ω zobrazení:

$$\omega : A_1 \times A_2 \times ... \times A_n \rightarrow A_1 \times A_2 \times ... \times A_n$$

kde A_i jsou množiny.

2.1 Operand a operátor

Operand je matematický název pro vstupní hodnoty matematické operace (nazývaných též argumenty operace). Operátor je matematický znakový identifikátor (symbol) definující určitou aritmetickou operaci. Dohromady pak vytvářejí početní výraz.

Operace nemusí být nutně definované pro všechny myslitelné hodnoty. Například operace dělení není pro reálná čísla definována, pokud je druhý argument 0. Argumenty (množinu hodnot), pro které je operace definována, tvoří definiční obor a hodnoty (množinu hodnot), které mohou být operací vyprodukovány, tvoří obor hodnot.

V matematice se rozlišují zejména dva druhy operací, jsou **aritmetické operece** a **algebraické operace**. Algebraické operace jsou zobecněním aritmetických operací, ve kterých vstupují jako operandy (argumenty operace) čísla z nějaké číselné množiny.

2.2 Arita operace

Arita udává počet vstupních operandů dané matematické operace. Podle počtu prvků operace se rozlišuje arita:

• Pro $n = 0$ se operace nazývají nulární. Formálně jde o předpis, který bez vstupu vrátí hodnotu. Příkladem nulární

operace mohou být konstanty (prvky množiny).

- Pro $n = 1$ se operace nazývají unární. Unární operace transformují jeden prvek množiny A na prvek množiny B (zobrazení). Mezi unární operace patří např. změna znaménka, absolutní hodnota čísla, nebo operace identity, která přiřazuje každému prvku a stejný prvek a.

- Pro $n = 2$ se operace nazývají binární. Binární operace přiřazují každé dvojici prvků prvek nějaké množiny. Sčítání, odčítání, násobení, dělení nebo mocnění patří mezi binární operace.

- Pro $n = 3$ se operace nazývají ternární. Taková operace přiřazuje každé trojici prvků prvek nějaké množiny. Většinou se tyto operace využívají v programovacích jazycích.

- Pro $n > 3$ se operace nazývají obecně n-ární. Operace vyšších arit se vyskytují především v programovacích jazycích, kde jsou nazývány funkce, metody, ...

2.2.1 Unární operace

Unární operace je taková operace, která má jen jediný operand. Unární operace *f* na množině **A** tedy je zobrazení:

$$A \to B$$

přičemž často platí $A = B$.

Příkladem unárních operací je například změna znaménka, faktoriál, goniometrické funkce, ...

2.2.2 Binární operace

V aritmetice a teorii čísel jsou nejdůležitější operace s aritou 2, tedy binární operace, která se vykonává mezi dvěma operandy. Binární operace je definována jako zobrazení, které každé uspořádané dvojici prvků dané množiny přiřadí právě jeden prvek z té samé množiny.

Nechť $\mathbf{M}$ je neprázdná množina, pak binární operace f na množině $\mathbf{M}$ je zobrazení uspořádané dvojice prvků kartézského součinu (kartézské mocniny) množiny $M \times M$ do množiny $\mathbf{M}$ (výsledkem je opět prvek z množiny $\mathbf{M}$). V binární operaci f je vzoru $[x, y] \in M \times M$ přiřazen obraz $z \in M$. To je obecně zapsáno jako:

$$f : [x, y] \in (M \times M) \rightarrow z \in M$$

Většinou jsou, ale tyto operace značeny nějakou schématickou značkou - operátor ve tvaru $x \circ y = z$

2.3 Operační tabulka

Definiční obor binární operace je možné zapsat pomocí

matematického nástroje, který se nazývá **operační tabulka**. Tento způsob se využívá zejména u konečných množin (algebraická tělesa). Pomocí operační tabulky lze zkoumat vlastnosti dané binární aritmetické (algebraické) operace.

Tabulka má n řádků a n sloupců, kde n je počet prvků dané množiny nad kterou je vykonávána daná binární operace. V prvním řádku se nacházejí všechny hodnoty, které se mohou nacházet na místě prvního operandu operace a v prvním sloupci tabulky se nacházejí všechny hodnoty, které se mohou nacházet na místě druhého operandů dané binární operace. V ostatních sloupcích se nacházejí hodnoty z definičního oboru aritmetické operace:

$$\begin{bmatrix} + & 0 & 1 & 2 \\ 0 & 1 & 2 & 0 \\ 1 & 2 & 0 & 1 \\ 2 & 0 & 1 & 2 \end{bmatrix}$$

2.4 Vlastnosti binárních operací

Aritmetické respektive algebraické operace se vyznačují určitými vlastnostmi, které buď mají nebo nemají. Z toho následně vyplývá jakým způsobem se s nimi zachází při jejich (interpretaci) výpočtech. Základní vlastnosti binárních algebraických respektive aritmetických operací jsou:

- **Úplnost**
- **Asociativnost**
- **Komutativnost**
- **Existence neutrálního prvku**
- **Existence inverzního prvku**
- **Distributivita**

Tyto vlastnosti jsou důležité především při úpravách a výpočtech složitějších algebraických výrazů.

2.4.1 Úplnost

Úplnost binární operace na $\circ$ množině **M** má vlastnost, že pro každé dvě čísla z této množiny je výsledkem opět číslo, které také patří do této číselné množiny. To je zapsáno jako:

$$\forall a, b, \in M \exists c \in M : (a \circ b = c)$$

2.4.2 Existence neutrálního prvku

Neutrální prvek je takový prvek, který při dosazení do dané binární algebraické, respektive aritmetické operace svou hodnotou nijak nezmění hodnotu druhého operandu:

$$a \circ b = a$$

kde operand b je neutrální prvek. Vzhledem k povaze algebraických (aritmetických) operací je neutrální prvek v každé operaci jiný.

2.4.3 Existence inverzního prvku

Inverzní prvek k prvku x v dané binární aritmetické operaci je takový prvek, který ve výsledku vrátí pro danou aritmetickou operaci neutrální prvek:

$$a \circ b = \oslash$$

kde b je inverzní prvek v dané operaci k prvku a. To znamená, že inverzní prvek je prvek s opačnou hodnotou k prvku původnímu. Stejně jako neutrální prvek je i inverzní prvek vzhledem k povaze algebraických operací v každé operaci jiný. Daný prvek se nazývá **invertibilní** pokud pro něj existuje prvek s inverzní hodnotou v dané aritmetické operaci. Tím vzniká základ pro inverzní operace.

Inverzní prvky jsou v algebře (a jiných matematických oborech) velmi důležité, protože umožňují definovat inverzní operace.

2.4.4 Komutativita

Komutativita je v matematice vlastnost binární operace která říká, že nezávisí na pořadí jejich operandů v operaci:

$$a \circ b = b \circ a$$

2.4.5 Asociativita

Asociativita je vlastnost binární operace která říká, že nezáleží na tom v jakém pořadí jsou operace prováděny, pokud se jich vedle sebe vyskytne více:

$$a \circ (b \circ c) = (a \circ b) \circ c$$

2.4.6 Distributivita

Distributivita je vlastnost binární operace vůči jiné binární operaci, která vychází z odvození složitějších operací z operací jednodušších, která říká, že lze danou operaci distribuovat (vyjádřit) přes jinou operaci:

$$a \circ (b \bullet c) = (a \bullet b) \circ (a \bullet c)$$

2.5 Inverzní operace

Kapitola 3
Dělitelnost

Dělitelnost je vlastnost celých čísel, která souvisí s operací celočíselného dělení. Celé číslo b je dělitelné bezezbytku celým číslem a, právě když existuje takové celé číslo k, že platí $b = a \cdot k$, to znamená, že číslo b je k-tým násobkem čísla a. Říká se pak, že **číslo a je dělitelem čísla b**, nebo že **číslo a dělí číslo b**. Tato vlastnost se zapisuje vertikální čárou mezi dělitelem a dělencem :

$$\forall a, b, k \in Z a|b :\Rightarrow b = a \cdot k$$

Jestliže naopak číslo a nedělí číslo b, zapisuje se to: $a \not| b$ a říká se, že **čísla a a b jsou nesoudělná**. Čísla a a b jsou nesoudělná právě tehdy, když je jich největší společný dělitel roven jedné.

3.1 Vlastnosti dělitelnosti

Dělitelnost v oboru celých čísel se vyznačuje určitými vlastnostmi:

- $\forall a \in Z : a|a$ - každé celé číslo a je dělitelné samo sebou:

$5 \div 5 = 1$

• $\forall a, b, c \in Z : a|b \wedge b|c \Rightarrow a|c$ - jestliže číslo b je násobek čísla a a zároveň číslo c je násobkem čísloa b, pak také číslo c je násobkem čísla a: $6 \div 3 \wedge 18 \div 6 \Rightarrow 18 \div 3$

• $\forall a, b \in Z : a|b \Rightarrow b \not| a$ - pro každé celé číslo a a b platí, že pokud je b násobkem a, tak a nemůže být násobkem b, to znamená, že operace dělení není komutativní a záleží na pořadí operandů.

• $\forall a, b \in Z : |a| = |b| \Rightarrow a|b \wedge b|a$ - jestliže jsou absolutní hodnoty celých čísel a a b stejné, pak je operace dělení komutativní:

• $\forall a, b, n \in Z : a|b \Rightarrow a|(b \cdot n)$ -jestliže je b násobek a, pak platí, že číslo $b \cdot n$ je stále násobek čísla a

• $\forall a, b \in Z : a|b \Rightarrow |a| \leq |b|$ - jestliže je celé b násobek celého čísla a, pak platí, že číslo a je menší než číslo b.

• $\forall m, n, a \in Z : a|m \wedge a|n \Rightarrow a|(m+n)$ - jestliže, číslo m a číslo n je násobkem čísla a, pak jejich součet je opět násobkem čísla a. Důkaz: $m = \underbrace{a + a + ... + a}_{k} \wedge n = \underbrace{a + a + ... + a}_{l} \Rightarrow m + n = \underbrace{a + a + ... + a}_{k+l}$

3.2 Kritéria dělitelnosti

Některé z dělitelů celočíselných čísel lze určit přímo ze zápisu přirozených čísel v desítkové číselné soustavě na základě vět, jimž se říká **kritéria dělitelnosti**:

- Dělení **nulou** není na množině celých čísel definováno.
- Každé celé číslo **je dělitelné číslem jedna a samo sebou**. Tomu se říká **samozřejmý** (triviální) dělitelé čísla n.
- Celé číslo je **dělitelné dvěma**, právě když jeho zápis končí na některou z číslic: 0, 2, 4, 6, 8. Dělitelné dvěma je tedy každé sudé číslo.
- Celé číslo je dělitelné **třemi**, právě když je jeho ciferný součet dělitelný třemi.
- Celé číslo je dělitené čtyřmi, přávě tehdy, když...
- Celé číslo je dělitelné pěti, právě když jeho zápis končí na číslici 0 nebo 5.
- Celé číslo je dělitelné šesti,...
- Metoda pro zjištění zda je celé číslo **dělitelné sedmi** je matematicky tak náročné, že je jednodušší dané číslo sedmi podělit a zjistit zda je dělitelné se zbytkem nebo bezezbytku (modulo sedm).
- Celé číslo je **dělitelné osmi**,...

• Celé číslo je dělitelné devíti,...

• Přirozené číslo je **dělitelné deseti**, právě když jeho zápis končí na číslici nula.

3.3 Zbytkový tvar celých čísel

Každé celé číslo a lze vyjádřit pomocí libovolného celého čísla $b > 1$ pomocí výrazu:

$$a = b \cdot k + z, a, b, z \in Z, 0 \leq z < b$$

Výraz $a = b \cdot k + z$ se nazývá **zbytkový tvar čísla** a a číslo z se nazývá zbytek po dělení čísla a číslem b. Je-li číslo $z = 0$, pak představuje podíl čísel a, b (v uvedeném pořadí $a \div b = k$) a operace dělení je v tomto případě inverzní k operaci násobení a říká se jí **dělení beze zbytku**. Je-li $z > 0$, pak se číslo k nazývá **neúplný podíl** a operaci dělení se v tomto případě říká **dělení se zbytkem**.

3.4 Sudost a lichost

V matematice je každé celé číslo buď **sudé**, nebo **liché**. Pokud je číslo násobkem dvou, je to **sudé číslo**, v opačném případě je **číslo liché**. Sudá čísla jsou tedy např. -4, 0, 12, 76; lichá čísla jsou např. -5, 1, 13, 37. Číslo nula je také sudé číslo. Protože sudé číslo je každé číslo dělitelné

dvěma bezezbytku, je sudé číslo každé druhé v číselné řadě. A proto platí že sudá čísla jdoucí po sobě jsou: 0, 2, 4, ... Číslo zapsané v desítkové soustavě je sudé právě tehdy, je-li sudá jeho poslední číslice. To samé platí i v ostatních číselných soustavách se sudou bází (se sudým počtem číslic používaných k zápisu číselných hodnot). V číselných soustavách s lichou bází má sudé číslo sudý ciferný součet.

Vlastnost (relace) čísla být sudým anebo lichým se někdy nazývá **parita čísla** (a může se chápat i jako číselná hodnota zbytku po dělení číslem dva, tzn. parita sudého čísla je nula, parita lichého čísla je jedna).

Množinu všech sudých čísel lze zapsat jako:

Sudá čísla $= 2k = \{..., -4, 0, 2, 4, ...\}$

Množinu všech lichých čísel lze zapsat jako:

Lichá čísla $= 2k + 1 = \{..., -5, 1, 3, 5, ...\}$

Libovolné sudé číslo je možno vyjádřit ve tvaru 2, kde $k \in Z$, zatímco libovolné liché číslo je možno vyjádřit jako $2k + 1$, opět $k \in Z$.

Množina sudých čísel je stejně jako množina lichých čísel spočetně nekonečná, což znamená, že každá z nich má stejnou mohutnost jako množina všech celých čísel.

3.4.1 Aritmetické vlastnosti sudých čísel

Při provádění některých základních aritmetických operací lze paritu výsledku poznat podle parity jednotlivých operandů:

Sudá a lichá čísla v operaci součet a rozdíl:

$$\textit{sudé} \pm \textit{sudé} = \textit{sudé}$$
$$\textit{sudé} \pm \textit{liché} = \textit{liché}$$
$$\textit{liché} \pm \textit{sudé} = \textit{liché}$$
$$\textit{liché} \pm \textit{liché} = \textit{sudé}$$

Sudá a lichá čísla v operaci součin:

$$\textit{sudé} \cdot \textit{sudé} = \textit{sudé}$$
$$\textit{sudé} \cdot \textit{liché} = \textit{sudé}$$
$$\textit{liché} \cdot \textit{sudé} = \textit{sudé}$$
$$\textit{liché} \cdot \textit{liché} = \textit{liché}$$

Sudá a lichá čísla v operaci podíl:

Dělení dvou celých čísel může mít jako výsledek číslo, které není celé, a proto u něj nelze mluvit o sudosti/lichosti. Někdy je však podíl dvou celých čísel také číslo celé, proto lze říci, že:

$$\textit{sudé} \div \textit{sudé} = \textit{nem}\text{ůže } \textit{být sudé}$$

$$\textit{sudé} \div \textit{liché} = \textit{nem}\text{ůže } \textit{být liché}$$

$$\textit{liché} \div \textit{sudé} = \textit{nikdy nem}\text{ůže } \textit{být celé} \text{ číslo}$$

$$\textit{liché} \div \textit{liché} = \text{záleží } \textit{na operandech}$$

Kapitola 4
Prvočísla a čísla složená

Každé přirozené číslo $P \in N \vee p \geq 2$, které je dělitelné pouze číslem 1 a sebou samým (samozřejmí dělitelé) se nazývá **prvočíslo**:

$$a|p \Leftrightarrow (a = 1 \wedge a = p)$$

Každé číslo $s \in N \vee s \geq 2$, které má vice než dva různé dělitele se nazývá **složené číslo**:

$$s = d_1 \cdot d_2$$

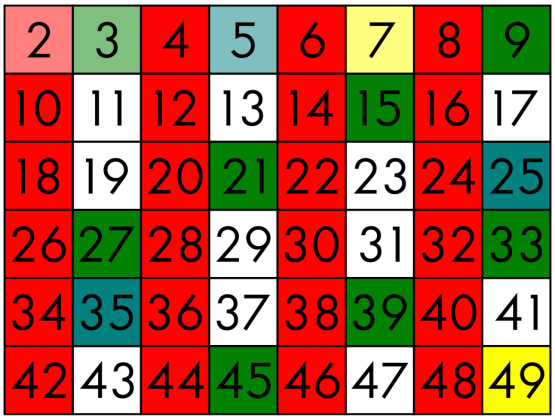
kde $d_1, d_2 \in N \vee d_1 > 1, d_2 > 1$

Jediná výjimka je číslo 1, které není ani prvočíslo ani složené číslo. Z toho plyne, že kromě jedničky je každé číslo buď prvočíslo a nebo číslo složené.

4.1 Eratosthenovo síto

Nejlepší způsob jak nalézt všechna prvočísla z dané množiny čísel je pomocí Eratosthenovo síta. Jedná o jednoduchý algoritmus, kdy jsou vypsána všechna čísla

z dané množiny uspořádaně podle velikosti, přičemž nejmenší může být číslo 2. Poté se ponechá první první prvočíslo v řadě (číslo 2). Následně jsou z dané řady vyškrtnuty všechny jeho násobky (v případě čísla 2 - 4, 6, 8, ...). Následně je nalezeno další prvočíslo ve zbývající číselné řadě (číslo 3). Opět jsou vyškrtnuty všechny jeho násobky. Následně se ve zbývající číselné řadě nalezne další prvočíslo a obdobně se postupuje pro další nevyškrtnutá čísla dokud je to možné. Zbylá nevyškrtnutá čísla jsou právě všechna prvočísla z dané množiny.



2	3	5	7	11	13	17	19
23	29	31	37	41	43	47	

4.2 Prvočíselný rozklad složeného čísla

Vyjádření složeného čísla ve tvaru součinu jeho dělitelů větších než 1 se nazývá **rozklad složeného čísla**:

$$32 = 4 \cdot 8 = 2 \cdot 16$$

Protože operace podíl je inverzní k operaci součin, je jasné že **jinými čísly, než jsou dělitelé daného čísla, nelze dané číslo rozložit**.

Speciálně rozklad složeného čísla v součinu prvočísel se nazývá **prvočíselný rozklad složeného čísla**. Prvočísla v tomto rozkladu se nazývají **prvočinitelé**.

Prvočíselný rozklad umožňuje vyjádření přirozeného čísla jako součinu mocnin prvočísel. Z toho vyplývá, že prvočísla fungují jako stavební bloky pro vyjádření libovolného složeného čísla. Definice prvočíselného rozkladu zní: Nechť je x přirozené číslo větší než 1. Za jeho prvočíselný rozklad se označuje každý zápis:

$$p_1^{m_3} \cdot p_2^{m_2} \cdot ... \cdot p_k^{m_n}$$

terý splňuje následující podmínky:

- výraz $p_1^{m_3} \cdot p_2^{m_2} \cdot ... \cdot p_k^{m_n}$ je roven číslu x.
- $k > 0, n > 0, m_1 > 0, m_2 > 0, ..., m_n > 0$ jsou kladná celá čísla (exponenty jsou větší než nula).

• $p_1 < p_2 < ... < p_n$ jsou vzájemně různá prvočísla seřazená podle velikosti.

Prvočísla z prvočíselného rozkladu čísla x, jsou zároveň dělitélé čísla x, proto platí, že rozklad složeného čísla x na součin jeho dělitelů je nadmnožina prvočíselného rozkladu.

Základní metoda určení prvočíselného rozkladu složeného čísla $x > 1$ je pomocí faktorizace, která je založena na postupném dělení prvočísly $p = 2, 3, 5, \ldots$ pro které platí, že jsou menšími než číslo x: a jsou jeho dělitelé $p|x$:

$$360 = \underbrace{6}_{2\cdot 3} \cdot \underbrace{60}_{10\cdot 6} = 2 \cdot 3 \cdot \underbrace{10}_{2\cdot 5} \cdot \underbrace{6}_{2\cdot 3} = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2^3 \cdot 3^2 \cdot 5$$

Protože prvočísla nelze dále dělit bezezbytku, je zákonitě dané, že postupným dělením se dojde k takovým dělitelům, které již nelze dále dělit - prvočísla.

Základní větou aritmetiky je, že každé číslo lze rozložit na jednoznačný součin prvočísel, tedy že pro jedno číslo neexistují dvě nebo více možností jak jej rozložit na prvočinitele.

Množinu všech dělitelů daného složeného čísla n se získá pomocí prvočíselného rozkladu. Číslo n se rozloží na součin

prvočísel a libovolní součin dvou nebo více prvočinitelů je dělitel daného čísla n:

$$208 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 13$$

$$208 \div 2 = 104$$

$$208 \div (2 \cdot 2) = 52$$

$$208 \div (2 \cdot 2 \cdot 2) = 26$$

$$208 \div (2 \cdot 2 \cdot 2 \cdot 2) = 13$$

$$208 \div (13) = 16$$

$$208 \div (13 \cdot 2) = 8$$

$$208 \div (13 \cdot 2 \cdot 2) = 4$$

$$208 \div (13 \cdot 2 \cdot 2 \cdot 2) = 2$$

4.3 Společný dělitel

Společným dělitelem čísel n_1, n_2, ..., n_k se nazývá každé číslo, které je dělitelem každého z nich. Společný dělitel, který je větší než všichni ostatní společní dělitelé, se nazývá **největší společný dělitel** čísel n_1, n_2, ..., n_k a označuje se $NSD(n_1, n_2, \ldots, n_k)$:

$$NSD(n_1, n_2, \ldots, n_k) = max(d \in N : d|n_1 \wedge d|n_2 \wedge ... \wedge d|n_k)$$

Obecněji je možné hovořit o největším společném děliteli celé množiny čísel $\{n1, n2, \ldots, nk\}$ - tím je největší číslo, které beze zbytku dělí všechna čísla v množině. Společní dělitelé čísel d_1, d_2, ..., d_k tvoří množinu společných dělitů daných čísel, ale existuje pouze jeden společný dělitel patřící do této množiny, který je větší než všichni ostatní.

Pro nalezení největšího společného dělitele dvou (nebo více) čísel se využívá vlastností prvočíselného rozkladu. Pomocí libovolné podmnožiny prvočísel prvočíselného rozkladu daného čísla lze vytvořit číslo, které je jeho dělitelem. Díky tomu lze říci, že číslo, které je dělitelem všech daných čísel, musí být složeno z prvočísel, které se vyskytují v prvočíselných rozkladech všech čísel. A díky základní větě aritmetiky, která říká, že pro dané složené číslo lze najít pouze jeden konkrétní prvočíselný rozklad a lze tak jednoznačně říct, že výsledné číslo je jediné číslo, které dělí obě složená čísla a je větší než všechny ostatní. Největší společný děliteldaných čísel musí obsahovat všechna prvočísla, která mají daná čísla společná, tedy skládá se z průniku množin prvočísel, které tvoří prvočíselný rozklad každého z čísel:

$$20 = 2 \cdot 2 \cdot 5$$

$$30 = 2 \cdot 3 \cdot 5$$

$$NDS(20, 30) = 2 \cdot 5 = 10$$

Prvočísla jsou vždy dělitelná pouze jedničkou a sebou samím, proto nemá smysl hledat NSD mezi prvočísly. Z toho plyne, že libovolná dvě prvočísla mezi sebou nejsou dělitelná bezezbytku.

U jednoho prvočísla a jednoho nebo více čísel složených má cenu hledat společného dělitele, pouze v případě, že čísla složená jsou x-tým násobkem daného prvočísla. V takovém případě je prvočíslo zároveň největší společný dělitel.

4.4 Společný násobek

Opakem společného dělitele je společný násobek. Společným násobkem přirozených čísel n_1, n_2, ..., n_k se nazývá takové přirozené číslo, které je nějakým násobkem každého z nich (každé číslo n_1, n_2, ..., n_k je dělitelné společným násobkem bezezbytku). Ten společný násobek, který je menší než kterýkoli jiný společný násobek, se nazývá **nejmenší společný násobek** čísel n_1, n_2, ..., n_k a označuje se $NSN(n_1, n_2, \ldots, n_k)$. Matematický zápis nejmenšího společného násobku je. Nejmenší společný

násobek se skládá ze sjednocení množin prvočísel, které tvoří prvočíselný rozklad každého z čísel:

$$NSN(n_1, n_2, \ldots, n_k) = min(m \in N : m = n_1 \cdot x \wedge m = n_2 \cdot y \wedge ... \wedge m = n$$

K výpočtu nejmenšího společného násobku daných čísel slouží prvočíselný rozklad. Jestliže NSN musí být bezezbytku dělitelné všemi čísly n_1, n_2, ..., n_k, pak se v jeho prvočíselném rozkladu musejí nacházet prvočísla z prvočíselného rozkladu všech jeho dělitelů. Protože se v daném společném násobku musí vyskytovat pouze nějaký násobek daného čísla, je možné využít prvočísel, které se již v prvočíselném rozkladu společného násobku vyskytují:

$$75 = 3 \cdot 5 \cdot 5$$

$$45 = 3 \cdot 3 \cdot 5$$

$$NSN(75, 45) = 3 \cdot 3 \cdot 5 \cdot 5 = 225$$

V prvočíselném rozkladu nejmenšího společného násobku se tedy vyskytuje jak prvočíselný rozklad čísla 45 - $(3 \cdot 3 \cdot 5) \cdot 5$ (číslo 45 se ve společném násobku vyskytuje právě 5-krát), tak prvočíselný rozklad čísla 75 - $3 \cdot (3 \cdot 5 \cdot 5)$

(číslo 75 se ve společném násobku vyskytuje právě 3-krát). A stejným způsobem lze postupovat i pro větší počet čísel. Ve společném násobku se musí nacházet prvočíselný rozklad každého z čísel.

4.5 Vlastnosti NSD a NSN

Pro nejmenší společný násobek a největšího společného dělitele platí vzájemný vztah, že součin nejmenšího společného násobku a největšího společného dělitele čísel n_1, n_2, ..., n_k je roven součinu těchto čísel:

$$n_1 \cdot n_2 \cdot \ldots \cdot n_k = NSD(n_1, n_2 \ldots, n_k) \cdot NSN(n_1, n_2 \ldots, n_k)$$

Z toho vyplývá, že pokud je znám největší společný dělitel, nebo nejmenší společný násobek, lze z této rovnice dopočítat hodnotu chybějící neznámé:

$$NSD(n_1, n_2, \ldots, n_k) = \frac{n_1, n_2, \ldots, n_k}{NSN(n_1, n_2, \ldots, n_k)}$$

nebo

$$NSN(n_1, n_2, \ldots, n_k) = \frac{n_1, n_2, \ldots, n_k}{NSD(n_1, n_2, \ldots, n_k)}$$

4.6 Testování prvočíselnosti

Prvočísla jsou čísla, která jsou dělitelná pouze jedničkou a sebou samým. Ale pro jejich identifikaci (rozlišení od čísel složených) není nutné testovat dělitelnost na všechny čísla v intervalu mezi číslem 1 a číslem n. Při procesu identifikace prvočísel je možné dedukcí mnoho čísel vyřadit a tím výrazně zkrátit a zjednodušit celý postup.

Nejhlavnější vlastností prvočísel je, že jsou všechny (kromě čísla 2) lichá, z toho důvodu je možné z procesu vyřadit všechna sudá čísla a říct, že pokud je dané testované číslo sudé, je automaticky považováno za číslo složené, protože je určitě dělitelné číslem 2 (a možná i jinými čísly). Testovat na prvočíselnost se tedy vyplatí pouze čísla lichá.

Dále je možné říci, že pokud prvočísla nejsou sudá, pak nemohou být bezezbytku dělitelná žádnými sudými čísly1, protože výsledek by nikdy nemohl být celé číslo, tedy lichá a sudá čísla nikdy nejsou dělitelná bezezbytku. Z toho vyplývá, že pokud dané číslo není sudé, nemá cenu ho testovat na dělitelnost sudými čísly. Díky tomu lze z intervalu (množiny) mezi čísly 3 (číslo 1 je samozřejmí dělitel a protože číslo n není sudé, pak nemůže být dělitelné 2) a číslem n vyškrtnout všechna sudá čísla a testovat na dělitelnost pouze lichými čísly.

Dále je možné bezpečně říct, že pokud je dané číslo n

číslo složené, pak má cenu hledat jeho nejmenšího dělitele maximálně do hodnoty $\sqrt{n}$. To plyne z toho, že pokud je dané číslo n číslo složené, lze ho rozepsat do tvaru, $n = a \cdot b$ kde $a, b \in N$. Odmocninou čísla n je získána hodnota, která je-li vynásobena sama sebou, je opět získána hodnota čísla n a proto platí $\sqrt{n} = x \Rightarrow n = a \cdot b$ kde $a = x \wedge b = a$. Jestliže je operand a nebo operand b (nebo oba) prvočíslo, pak nelze nalézt menší celé číslo, kterým by bylo číslo n bezezbytku dělitelné, a proto, jestliže nějaké takové prvočíslo existuje, pak je menší nebo rovno odmocnině z čísla n:

$$d|n \Rightarrow d \leq \sqrt{n}$$

Číslo x je střední hodnota čísel a a b $n = a \cdot b \Rightarrow a \leq \sqrt{n} \leq b$. Prvočíselnost čísla n má tedy cenu testovat maximálně do hodnoty $\sqrt{n}$.

Kapitola 5
Konstrukce číselných množin

5.1 Množina reálných čísel

Kapitola 6
Číselná soustava

Číselná soustava je způsob reprezentace čísel, které uchovávají určitou hodnotu. Zápis čísla dané číselné soustavy je posloupností symbolů, které se nazývají číslice. Jedná se v podstatě o množinu symbolů, používaných k reprezentaci číselných hodnot a pravidla pro aritmetické operace s nimi. Díky tomu mohou dva různé zápisy čísel reprezentovat stejnou číselnou hodnotu. Podle způsobu určení hodnoty čísla z dané reprezentace se rozlišují dva druhy číselných soustav:

- **poziční číselné soustavy**
- **nepoziční číselné soustavy**

Dnes nejpoužívanější číselné soustavy jsou poziční číselné soustavy.

6.1 Poziční číselná soustava

U poziční číselné soustavy je v zápisu čísel hodnota každé číslice dána její pozicí v sekvenci symbolů. Každá

číslice má touto pozicí dánu svou váhu pro výpočet celkové hodnoty čísla.

Klíčovou charakteristikou pozičních číselných soustav je jejich **základ**. To je obvykle reálné číslo větší než jedna, které určuje počet symbolů pro číslice používaných v dané číselné soustavě. Základ je obvykle značen písmenem R z anglického slova radix. **Váhy jednotlivých číslic** jsou mocninami tohoto základu. Název číselné soustavy je odvozen od čísla, které tvoří základ soustavy. Například pokud má soustava základ 10 jedná se o desítkovou soustavu.

6.1.1 Číselný řád

V pozičních číselných soustavách má také smysl mluvit o **číselných řádech**. Rozlišuje se **řád číslice** a **řád čísla**. Řád číslice určuje její váha v čísle a řád čísla určuje nenulová číslice v čísle s nejvyšší hodnotou (nejvíce vlevo). Řád desetinného čísla (části vpravo za desetinnou čárkou) určuje nenulová číslice s nejnižší váhou (nejvíce vpravo). Jednotlivé číselné řády v desítkové (dvojkové) soustavě jsou pojmenovány a tvoří důležitou součást technických dokumentů, kde slovně popisují velikost daného čísla a umožňují zkrácení jeho zápisu:

10^n	*Předpona*	*Značka*	*Název*	*Násobek*
10^12	*tera*	T	*bilion*	1000000000000
10^9	*giga*	G	*miliarda*	1000000000
10^6	*mega*	M	*milion*	1000000
10^3	*kilo*	K	*tisíc*	1000
10^2	*hekto*	h	*sto*	100
10^1	*dela*	da	*deset*	10
10^0	–	–	*jedna*	1
10^{-1}	*deci*	d	*desetina*	$0,1$
10^{-2}	*centy*	c	*setina*	$0,01$
10^{-3}	*mili*	m	*tisícina*	$0,001$
10^{-6}	*mikro*	μ	*miliontina*	$0,000001$
10^{-9}	*nano*	n	*miliardtina*	$0,000000001$
10^{-12}	*piko*	p	*biliontina*	$0,000000000001$

6.1.2 Řádové přetečení

Číselná soustava o základu R používá právě R symbolů k reprezentaci libovolného čísla. Těmito základními R symboly lze reprezentovat pouze čísla nultého řádu (jednociferné). Pro zápis větších čísel se využívá **řádového přetečení**, které nastane v případě, kdy je k hodnotě reprezentované číslicí s nejvyšší hodnotou v soustavě přičtena hodnota jedna (nebo vyšší). V nultém řádu čísla dojde k přetočení číslicových symbolů a ty začínají opět od číslice s nejnižší

hodnotou. Hodnota číslice na i-té řádové pozici tedy udává kolikrát došlo k řádovému přetečení na pozici $i-1$. Z tohoto důvodu je jejich hodnota určena jako násobek mocniny o základu R a exponentem i. Na pozici $i-1$ je pak hodnota, která definuje o kolik dané číslo přeteklo číselný řád:

$$9 \rightarrow 10$$

6.1.3 Způsob zápisu čísel

V běžně používaných pozičních číselných soustavách se jednotlivé číslice zapisují za sebe a nijak se neoddělují. Desetinná čárka pouze odděluje celou a desetinnou část čísla. Někdy se také oddělují významnější číselné řády: tisíce, miliony, ... Hodnota čísla N v soustavě o základu R se tak zapisuje:

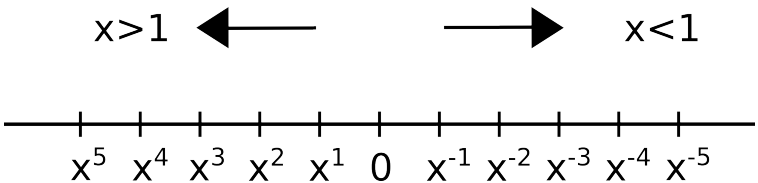
$$N = (n_{k-1}n_k{-}2...n_0, n{-}1n_{-2}...n_L)_R$$

kde n_{k-1} je **nejvyšší významová číslice** (její změna nejvíce ovlivní hodnotu daného čísla), n_L je **nejméně významná číslice** (její změna nejméně ovlivní hodnotu daného čísla) a R je základ číselné soustavy.

V případě desítkové soustavy se čísla dle konvence nezapisuje do kulatých závorek, ani není nutné k němu přip-

isovat jeho základ (pokud nejde o převod do jiné číselné soustavy pro účely přehlednějšího zápisu).

Dolní index u jednotlivých číslic určuje jejich řád. Řád je tedy poziční index na řádové stupnici jehož počátkem je hodnota nula (jednotky).



Takovému zápisu se říká **poziční zápis** - pozice každé číslice v daném čísle představuje její **relativní váhu významnosti**.

Číselné soustavy v nichž lze čísla pomocí rovnice se nazývají **polyadické** - číselnou hodnotu v nich zapsanou lze vyjádřit součtem mocnin o základu dané soustavy vynásobených příslušnými platnými číslicemi.

6.1.4 Určení hodnoty čísla

Hodnota čísla N zapsaného v dané soustavě o základě R je získána jako součet hodnot jednotlivých číslic vynásobených jejich váhou. Takovému způsobu zápisu se říká

polynomální zápis. Obecně lze zapsat libovolné reálné číslo v poziční číselné soustavě o základu R polynomem:

$$N = \sum_{i=-L+1}^{k-1} n_i \cdot R^i = \underbrace{n_{k-1} \cdot R^{k-1} + ... + n_0 \cdot R^0}_{Celá\ část} + \overbrace{n_{-1} \cdot R^{-1} + ... + n_-}^{Desetinná}$$

Každá číslice n_i je vynásobena váhou, která je dána její pozicí (řádem) i a která je vyjádřena mocninou o základu R, k vyjadřuje počet číslic v celé části daného čísla a L vyjadřuje počet číslic desetinné části daného čísla. Řádová čárka je umístěna za členem $n_0 \cdot R^0$ a odděluje celou část čísla od zlomkové (desetinné).

6.2 Nepoziční číselné soustavy

Nepoziční číselná soustava je způsob reprezentace čísel, ve kterém hodnota každé číslice není dána jejím umístěním v dané sekvenci číslic. Tyto způsoby zápisu čísel se v matematických a jiných technických oborech již nepoužívají a jsou považovány za zastaralé.

V systému nepoziční číselné soustavy má každý znak svoji hodnotu a pro reprezentaci libovolné hodnoty je zvolena taková kombinace číselných symbolů, jejichž výsledný součet definuje danou hodnotu. Příkladem nepoziční

číselné soustavy jsou římské číslice. Pokud mají symboly hodnoty: $A = 1$, $B = 10$, $C = 100$, $D = 1000$, pak vyjádření čísla 3542 může vypadat:

$$DDDCCCCCBBBBAA$$

Nevýhodou je jejich dlouhý a nepřehledný zápis a často tyto soustavy neobsahují symbol pro nulu a záporná čísla. Výhodou ale je jejich jednoduché sčítání a odčítání.

6.3 Běžné číselné soustavy

Dnes nejvíce používané číselné soustavy jsou dvojková, osmičková, desítková, šestnáctková a šedesátková. Dvojková, osmičková a šestnáctková soustava se používají převážně ve výpočetní technice a ke kódování dat, desítková soustava se používá k běžným výpočtům blízký běžným lidem a šedesátková soustava se používá k práci s časem (hodiny, minuty a vteřiny).

6.3.1 Dvojková soustava

Dvojková nebo také **binární číselná soustava** je poziční číselná soustava mocnin čísla 2. K reprezentaci libovolných čísel používá pouze dva symboly - 1 a 0. Používá se ve všech moderních číslicových obvodech, protože její dva symboly odpovídají jednoduše rozdělitelných stavům elek-

trického obvodu - zapnuto = 1 a vypnuto = 0, popřípadě pravdivosti či nepravdivosti výroků. Číslo zapsané ve dvojkové soustavě se nazývá binární nebo dvojkové číslo.

6.3.2 Osmičková soustava

Osmičková nebo také **oktalová číselná soustava** je poziční číselná soustava o základu 8, která v tradičním zápisu může obsahovat číslice 0-7. Používá se pro zkrácení zápisu binárních čísel z důvodu jednoduchého převodu mezi binární a osmičkovou soustavou, protože $8 = 2^3$.

6.3.3 Šestnáctková soustava

Šestnáctková nebo také **hexadecimální číselná soustava** je poziční číselná soustava o základu čísla 16. Protože čísla v šestnáctkové soustavě používají pro zápis 16 různých znaků, používá tato soustava ne jenom čísla desítkové soustavy, ale i písmena abecedy. Pro zápis šestnáctkových čísel se používají znaky $1-9$ a znaky $A-F$ pro čísla s hodnotou $10-15$. Čísla v hexadecimálním tvaru obvykle označují písmenem H nebo číslem *16* v dolním indexu: $A1_H$. Opět se používají pro zkrácení zápisu binárních čísel díky snadnému převodu mezi binární a šestnáctkovou soustavou. Příkladem použití je zápis adresy v operační paměti počítače.

6.4 Kódování hodnot

Zápis čísla v dané číselné soustavě může mít pro danou hodnotu více tvarů. To závisí na použitém způsobu zakodování hodnoty do čísla. Běžně používané zápisy číselných hodnot jsou předem domluvené způsoby kódování. Díky tomu každý ví jakou hodnotu daný zápis čísla vyjadřuje a jak s ním dále pracovat. Zakódování hodnoty do číselného zápisu určuje **kódovací algoritmus**.

Typickým příkladem může být způsob reprezentování binárních čísel v přímém dvojkovém kódu, nebo kódu dvojkového doplňku, BCD kód, ...

6.5 Převody mezi soustavami

Pro převod zápisů číselných hodnot mezi číselnými soustavami o různých základech existuje univerzálí způsob, který je založen na polynomální reprezentaci čísel:

$$n_{k-1} \cdot R^{k-1} + ... + n_0 \cdot R^0 + n_{-1} \cdot R^{-1} + ... + n_{-L+1} \cdot R^{-L+1}$$

6.6 Rotace

Číslicová rotace je stav při přesunu číslic uvnitř čísla. Jedná se o speciální operaci s důležitou vlastností, která se využívá při aritmetických výpočetech (především v binární soustavě). Rozlišují se dva druhy číslicové rotace:

- Rotace vpravo
- Rotace vlevo.

V případě číslicové rotace vpravo dochází v čísle v číselné soustavě o základu R k **podílu hodnoty čísla** hodnotou základu R. V případě, že podíl čísla základem číselné soustavy není celočíselný (se zbytkem) dojde k oříznutí desetinné části, a nebo k přenosu do desetinné části čísla.

$$244 >> 1 = 24 \leftrightarrow 244 \div 10 = 24 \rightarrow 4$$

V případě číslicové rotace vlevo dochází v čísle v číselné soustavě o záklkadu R k **součinu hodnoty čísla** hodnotou základu R.

$$24 << 1 = 240 \leftrightarrow 24 \cdot 10 = 240$$

Při rotaci dojde ke změně n počtu číslic daného čísla a tím pádem také k posunutí hodnot exponentů základu R v polynomálním vyjádření hodnoty čásla:

$$a_{n-1} \cdot R^{n-1} + ... + a_0 \cdot R^0 \Rightarrow a_{m-2} \cdot R^{m-2} + ... + a_0 \cdot R^0$$

kde n je počet platných číslic daného čísla před číslicovou rotací a m je počet platných číslic daného čísla po číslicové rotaci. Platí, že při číslicové rotaci vpravo je $n > m$ a při číslicové rotaci vlevo je $n < m$. Hodnota výsledného čísla se změní (změnší nebo zvětší) R-krát.