ZÁPADOČESKÁ UNIVERZITA V PLZNI
FAKULTA PEDAGOGICKÁ
KATEDRA MATEMATIKY, FYZIKY A TECHNICKÉ VÝCHOVY

DĚLITELNOST V RŮZNÝCH OBORECH INTEGRITY

BAKALÁŘSKÁ PRÁCE

Michaela Táborová
Přírodovědná studia, Obor Matematická studia

Vedoucí práce: PhDr. Lukáš Honzík, Ph.D.

Plzeň 2019

Prohlašuji, že jsem bakalářskou práci vypracovala samostatně s použitím uvedené literatury a zdrojů informací.

V Plzni, 15. dubna 2019

.....

vlastnoruční podpis

PODĚKOVÁNÍ

Ráda bych poděkovala panu PhDr. Lukášovi Honzíkovi Ph.D. za jeho cenné rady, připomínky, ochotu, čas věnovaný konzultacím a odborné vedení mé bakalářské práce. Dále děkuji všem, kteří mě podporovali při psaní práce.

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta pedagogická
Akademický rok: **2016/2017**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Michaela TÁBOROVÁ**
Osobní číslo:	**P15B0018P**
Studijní program:	**B1001 Přírodovědná studia**
Studijní obor:	**Matematická studia**
Název tématu:	**Dělitelnost v různých oborech integrity**
Zadávající katedra:	**Katedra matematiky, fyziky a technické výchovy**

Zásady pro vypracování:

1. Pojem dělitelnosti a soudělnosti ve vybraných oborech integrity, zavedení jednotkového prvku, asociovaného prvku a euklidovské normy.
2. Kritéria dělitelnosti v oborech integrity.
3. Pojem ireducibilního prvku a prvočinitele v oboru integrity, jejich vlastnosti. Zjištění prvočíselnosti prvku (Eratostenovo síto). Rozklad prvku v součin ireducibilních prvků.

Rozsah grafických prací:

Rozsah kvalifikační práce: **30 - 50**

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

DRÁBEK, Jaroslav. přednášky z KMT/Elementární algebra.
HEFLER, Stanislav. Příklady na dělitelnost v oborech integrity.
Plzeň, 2013. Bakalářská práce. Západočeská univerzita v Plzni.
Vedoucí práce doc. RNDr. Jaroslav Hora, CSc.
RAIS, Michal. Prvočíselný rozklad a jeho užití. Plzeň, 2011.
Diplomová práce. Západočeská univerzita v Plzni.
Vedoucí práce doc. PaedDr. Jana Coufalová, CSc.
ČERMÁKOVÁ, Petra. Dělitelnost: modely dělitelnosti v různých soustavách a v Gaussových oborech integrity. Plzeň, 2006. Bakalářská práce. Západočeská univerzita v Plzni. Vedoucí práce RNDr. Libuše Tesková, CSc.

Vedoucí bakalářské práce: **PhDr. Lukáš Honzík, Ph.D.**
Katedra matematiky, fyziky a technické výchovy

Datum zadání bakalářské práce: **13. června 2017**

Termín odevzdání bakalářské práce: **30. června 2018**

RNDr. Miroslav Randa, Ph.D.
děkan

L.S.

Doc. PaedDr. Jarmila Honzíková, Ph.D.
vedoucí katedry

V Plzni dne 19. června 2017

OBSAH

ÚVOD

Již na základní škole se vyučuje dělitelnost čísel. Vzniká zde mylná představa o tom, že se tato problematika týká pouze celých čísel. Tato bakalářská práce onu představu vyvrací, jelikož se zabývá dělitelností v různých oborech integrity. Byly pro ni zvoleny následující obory integrity: celá čísla, Gaussova celá čísla a polynomy.

Obor integrity spadá do algebraických struktur. Jednou z relací algebraických struktur je relace dělitelnosti, kterou se práce podrobněji zabývá. Stejně jako každé jiné odvětví matematiky mají i algebraické struktury své důležité prvky, bez kterých se nelze obejít. Mezi významné prvky jsou řazeny jednotkový prvek, asociovaný prvek a euklidovská norma. Všechny tyto prvky jsou aplikovatelné na konkrétní obory integrity.

Dělitelnost jako takovou lze uplatnit několika možnými způsoby. Mezi základní principy aplikace dělitelnosti patří kritéria dělitelnosti, jejímž příkladem jsou znaky dělitelnosti. Tyto znaky patří mezi základní znalosti, které by si měli žáci odnést právě ze základní školy. Jedná se o zjišťování, kdy je číslo dělitelné dvěma, třemi, čtyřmi atd.

Málokdo si spojí, že součástí relace dělitelnosti jsou také ireducibilní prvky či prvočísla. Čtenář si obvykle pod rozkladem složeného čísla v součin prvočísel představí operaci násobení, avšak princip je opačný. I tato problematika je důkladně rozebrána v jedné z kapitol práce.

Jedním z nejdůležitějších uplatnění relace dělitelnosti je výpočet největšího společného dělitele a nejmenšího společného násobku. Tyto dva pojmy jsou spolu velmi silně provázány, a proto by se neměly opomíjet. Největší společný dělitel prvků se dá zjišťovat několika způsoby. V práci je pro tento postup použit výpočet Euklidova algoritmu, který patří mezi nejefektivnějším způsobem řešení této problematiky.

Cílem práce je sjednotit a ucelit poznatky o dělitelnosti ve vybraných oborech integrity. Dílčím cílem je praktická ukázka relace dělitelnosti a její aplikace na ilustrační příklady.

MOTIVAČNÍ ÚKOL:

Mohou se objevit situace, kdy je třeba rozhodnout o tom, zda dané číslo je prvočíslem, například při určování společného jmenovatele zlomku.

Uvažujme například číslo 13567. Prvočíselnost lze určit pomocí více metod. Jmenujme například využití známých znaků dělitelnosti přirozených čísel, Eratosthenova síta nebo aplikování počítačového algoritmu, který bude postupně zkoušet, zda je toto číslo dělitelné prvočísly od 2 do odmocniny ze zkoumaného čísla. Zmíněné metody úzce souvisí s obsahem této práce. Řešení nastoleného problému těmito metodami pak objasníme v závěrečné kapitole.

1 ALGEBRAICKÉ STRUKTURY

Algebraickou strukturou se rozumí množina nějakých objektů, na kterých je definována alespoň 1 binární operace, s tím souvisí následující definice.

Definice: Nechť je M libovolná neprázdná množina. ***Binární operací*** v množině M nazýváme zobrazení kartézského součinu $M\ x\ M$ do množiny M tzn., že každé uspořádané dvojici $[x, y]$ z $M\ x\ M$ je přiřazen nejvýše jeden prvek z z množiny M**.**

Algebraické struktury se rozlišují podle toho, kolik mají definovaných binárních operací. Jestliže je určuje jedna binární operace, jedná se o algebraické struktury s jednou binární operací. Jestliže naopak mají dvě binární operace, pak se hovoří o algebraických strukturách se dvěma binárními operacemi.

Definice: Uspořádanou dvojici $(M, +)$, kde M je neprázdná množina, ve které je definována binární operace sčítání $(+)$, se nazývá ***algebraická struktura s jednou operací***.

Binární operace mají také své vlastnosti, mezi které se řadí neomezená definovanost v množině M, asociativnost, neutrální prvek, inverzní prvek ke všem prvkům dané množiny M a komutativnost.

Definice: Nechť jsou na množině M definovány dvě binární operace $(+)$ a $(\cdot)$. Říkáme, že ***operace násobení*** $(\cdot)$ ***je distributivní vzhledem k operaci*** $(+)$ v M právě tehdy, když platí

$$\forall a, b, c \in M: (a + b) \cdot c = (a \cdot c) + (b \cdot c) \ \wedge\ \mathrm{c} \cdot (\mathrm{a} + \mathrm{b}) = (\mathrm{c} \cdot \mathrm{a}) + (\mathrm{c} \cdot \mathrm{b}).$$

Na základě těchto uvedených vlastností pro binární operace lze snadno určit typy algebraických struktur. Algebraické struktury rozdělují na grupoid, pologrupu, grupu, polokruh, okruh, obor integrity a těleso.

Pro lepší přehlednost jsou zde uvedeny Tabulka 1 a Tabulka 2, ve kterých jsou znázorněné algebraické struktury s jednou binární operací a se dvěma binárními operacemi.

Tabulka 1: Typy algebraických struktur s jednou binární operací

STRUKTURA	**VLASTNOSTI BINÁRNÍCH OPERACÍ**
grupoid	neomezená definovanost v M
komutativní grupoid	neomezená definovanost v M, komutativnost
pologrupa	neomezená definovanost v M, asociativnost
komutativní pologrupa	neomezená definovanost v M, asociativnost, komutativnost
grupa	neomezená definovanost v M, asociativnost, neutrální prvek, inverzní prvky pro všechny prvky
komutativní grupa = Abelova grupa	neomezená definovanost v M, asociativnost, neutrální prvek, inverzní prvek, komutativnost

Tabulka 2: Typy algebraických struktur se dvěma binárními operacemi

STRUKTURA	**VLASTNOSTI BINÁRNÍCH OPERACÍ**	
	operace $(+)$	**operace** $(\cdot)$
polookruh	neomezená definovanost v M, asociativnost, komutativnost	neomezená definovanost v M, asociativnost, distributivní k operaci $+$
komutativní polookruh	neomezená definovanost v M, asociativnost, komutativnost	neomezená definovanost v M, asociativnost, distributivní k operaci $+$, komutativnost
okruh	neomezená definovanost v M, asociativnost, neutrální prvek, inverzní prvek, komutativnost	neomezená definovanost v M, asociativnost, distributivní k operaci $+$
komutativní okruh	neomezená definovanost v M, asociativnost, neutrální prvek, inverzní prvek, komutativnost	neomezená definovanost v M, asociativnost, distributivní k operaci $+$, komutativnost
obor integrity	neomezená definovanost v M, asociativnost, neutrální prvek, inverzní prvek, komutativnost	neomezená definovanost v M, asociativnost, distributivní k operaci $+$, komutativnost, neexistují netriviální dělitelné nuly
těleso	neomezená definovanost v M, asociativnost, neutrální prvek, inverzní prvek, komutativnost	neomezená definovanost v M, asociativnost, distributivní k operaci $+$, inverzní prvek
komutativní těleso	neomezená definovanost v M, asociativnost, neutrální prvek, inverzní prvek, komutativnost	neomezená definovanost v M, asociativnost, distributivní k operaci $+$, inverzní prvek, komutativnost

1.1 OBOR INTEGRITY

V předchozí kapitole je definováno, co to je algebraická struktura, jaké má vlastnosti a jak se rozděluje. Tato podkapitola je zaměřena na určitou algebraickou strukturu, kterou je obor integrity. V Tabulce 2 jsou uvedeny vlastnosti oboru integrity.

Obor integrity musí splňovat následující axiómy:

1. Operace sčítání:
    a. Komutativnost: $\forall a, b \in I: a + b = b + a$

       tzn., nezáleží na pořadí jednotlivých sčítanců.

    b. Asociativnost: $\forall a, b, c \in I: (a + b) + c = a + (b + c)$

       tzn., lze libovolně změnit pořadí závorky jednotlivých sčítanců.

    c. Neutrální prvek *e*: $\exists e \in I, \forall a \in I: a + e = e + a = a$

       tzn., sečte-li se libovolný prvek s neutrálním prvkem, výsledek je původní prvek.

    d. Inverzní prvek a^{-1}: $\forall a \in I, \exists a^{-1} \in I: a + a^{-1} = a^{-1} + a = e$

       tzn., ke každému prvku existuje prvek inverzní.

2. Operace násobení:
    a. Komutativnost: $\forall a, b \in I: a \cdot b = b \cdot a$

       tzn., nezáleží na pořadí jednotlivých činitelů.

    b. Asociativnost: $\forall a, b, c \in I: (a \cdot b) \cdot c = a \cdot (b \cdot c)$

       tzn., nezáleží na pořadí provedených operacích s činiteli.

    c. Neexistence netriviálních dělitelů nuly:

       $$\forall a, b, \in I: a \neq 0 \wedge b \neq 0 \Rightarrow a \cdot b \neq 0$$

       tzn., nulový součin se získá pouze nulovými činiteli.

3. Distributivnost: $\forall a, b, c \in I: (a + b) \cdot c = (a \cdot c) + (b \cdot c)$

   tzn., roznásobení sčítanců (Hefler, 2013).

2 POJEM DĚLITELNOSTI VE VYBRANÝCH OBORECH INTEGRITY

V této kapitole jsou vysvětleny základní pojmy, které se týkají dělitelnosti. Je zavedena definice dělitelnosti, jednotkový prvek, asociovaný prvek či Euklidovská norma. Dále pak jsou přiloženy ukázkové příklady na tyto vlastnosti v jednotlivých oborech integrity.

2.1 POJEM DĚLITELNOSTI

Tato část se zabývá dělitelností v libovolném (komutativním) oboru integrity, který je značen I. Nulový prvek je značen symbolem 0, naopak jednotkový prvek symbolem 1 (Blažek, 1985).

Definice: Nechť $a, b \in I$. Řekneme, že ***a dělí b*** (respektive a je dělitel b nebo b je násobek a, popřípadě b je dělitelné a) právě, když existuje $x \in I$ tak, že $a \cdot x = b$.

Symbolicky zapisujeme, že a dělí b takto: $a|b$. Naopak když a nedělí b, zapisujeme $a \nmid b$.

Lemma: Nechť I je libovolný obor integrity, pak platí

a) $\forall a \in I: a|a$ (neplatí pro nulový prvek)

b) $\forall a, b, c \in I: (a|b \wedge b|c) \Rightarrow a|c$

c) $\forall a, b \in I: (a \neq b \wedge a|b) \Longrightarrow (b \nmid a)$

d) $\forall a, b, c \in I: a|b \Rightarrow a|bc$

e) $\forall a, b, c \in I: ab|c \Rightarrow a|c \wedge b|c$

f) $\forall a, b, c \in I: (c|a \wedge c|b) \Rightarrow \big(c|(a+b) \wedge c|(a-b)\big)$

g) $\forall a_1, \dots, a_n, k_1, \dots, k_n \in I: (c|a_1 \wedge \dots \wedge c|a_n) \Rightarrow c|\sum_{i=1}^{n} k_i a_i$

h) $\forall a, b, c, \in I: (c \neq 0 \Rightarrow (a|b \Leftrightarrow ac|bc)$

2.1.1 CELÁ ČÍSLA

Jak je již výše uvedeno, množina celých čísel splňuje 8 základních axiomů týkajících se oboru integrity. Pro tuto podkapitolu se zvolí jako obor integrity množina celých čísel. Pro tento obor integrity se vychází ze základní definice dělitelnosti, kdy číslo ***a*** **dělí** číslo ***b*** právě tehdy, když existuje číslo $x \in I$ takové, že $a \cdot x = b$. Zapisujeme $a|b \Leftrightarrow a \cdot x = b$.

- Příklad: Mějme čísla $a = 28$ a $b = 1736$. Podle definice dělitelnosti nalezněte číslo x takové, že platí $a|b \Leftrightarrow a \cdot x = b$.

  $$a|b \Leftrightarrow a \cdot x = b$$
  $$28 \cdot x = 1736$$
  $$x = \frac{1736}{28}$$
  $$\underline{\underline{x = 62}}$$

  Hledané číslo x, pro které platí definice je $x = 62$.

- Příklad: Mějme čísla $a = 13$ a $b = 563$. Podle definice dělitelnost dokažte, jestli platí $a|b \Leftrightarrow a \cdot x = b$.

  $$a|b \Leftrightarrow a \cdot x = b$$
  $$13 \cdot x = 563$$
  $$x = \frac{563}{13}$$
  $$\underline{\underline{x = 43{,}3}}$$

  Vzhledem k tomu, že se nacházíme v oboru integrity celých čísel a číslo x není celým číslem, můžeme tvrdit, že $13 \nmid 563$.

2.1.2 GAUSSOVA CELÁ ČÍSLA

Uvažujme obor integrity množinu Gaussových celých čísel $(G, +, \cdot)$, kde G je množina všech komplexních čísel majících reálnou i imaginární složku z množiny celých čísel. Stejně jako u celých čísel u Gaussových celých čísel vycházíme z obecné definice dělitelnosti.

Definice: Mějme čísla $\alpha, \beta \in G$. Řekneme, že ***α dělí β*** právě tehdy, když existuje prvek $\gamma \in G$ takový, že platí $\beta = \alpha \cdot \gamma$. Číslo α nazýváme dělitel a číslo β dělenec. Zapisujeme $\alpha|\beta \Leftrightarrow \beta = \alpha \cdot \gamma$.

- Příklad: Máme čísla $\alpha = 1 + 2i$ a $\beta = 5 + 25i$. Dokažte dělitelnost v $(G, +, \cdot)$ pro $1 + 2i|5 + 25i$.

  Vyjdeme z definice dělitelnosti pro Gaussova celá čísla, tudíž musí existovat Gaussovo celé číslo $x_1 + x_2 i$, pro které platí:

$5 + 25\mathrm{i} = (1 + 2\mathrm{i}) \cdot (x_1 + x_2 i)$

$5 + 25\mathrm{i} = x_1 + x_2 i + 2x_1 i + 2x_2 i^2$

$5 + 25\mathrm{i} = x_1 + x_2 i + 2x_1 i - 2x_2$

Získáme soustavu dvou lineárních rovnic o dvou neznámých. V jedné rovnici porovnáme lineární složky a v druhé rovnici porovnáme imaginární složky.

$$\begin{aligned} 5 &= x_1 - 2x_2 \qquad | \cdot (-2) \\ \underline{25 &= 2x_1 + x_2} \\ -10 &= -2x_1 + 4x_2 \\ \underline{25 &= 2x_1 + x_2} \\ 15 &= 5x_2 \\ \underline{\underline{x_2 &= 3}} \end{aligned}$$

$$\begin{aligned} 2x_1 &= 25 - x_2 \\ 2x_1 &= 25 - 3 \\ \underline{\underline{x_1 &= 11}} \end{aligned}$$

Našli jsme řešení soustavy $x_1 = 11,\ x_2 = 3$. Hledané Gaussovo celé číslo je $11 + 3i$ a je dokázáno, že $1 + 2i | 5 + 25i$.

- Příklad: Mějme čísla $\alpha = 1 - i$ a $\beta = 3 + 2i$. Zjistěte zda $\alpha | \beta$.

  Použijeme postup jako v předchozím příkladu.

  $3 + 2i = (1 - i) \cdot (x_1 + x_2 i)$

  $3 + 2\mathrm{i} = x_1 + x_2 i - x_1 i - x_2 i^2$

  $\underline{3 + 2\mathrm{i} = x_1 + x_2 i - x_1 i + x_2}$

  $3 = x_1 + x_2$

  $\underline{2 = -x_1 + x_2}$

  $5 = 2x_2$

  $\underline{\underline{x_2 = \frac{5}{2}}}$

  Protože vyšlo $x_2 = \frac{5}{2}$ a nevyšlo celé číslo, můžeme tvrdit, že číslo $\alpha \nmid \beta$. Nicméně ještě ověříme dopočítáním x_2.

$$x_1 = 3 - x_2$$

$$x_1 = 3 - \frac{5}{2}$$

$$\underline{\underline{x_1 = \frac{1}{2}}}$$

Našli jsme sice řešení soustavy, ale ne z Gaussova celočíselné oboru, tudíž $1 - i \nmid 3 + 2i$.

2.1.3 POLYNOMY

Uvažujme obor integrity polynomů $(T[x],\ +,\ \cdot)$. Pro dělitelnost polynomů platí následující definice.

Definice: Říkáme, že polynom $\boldsymbol{g(x)}$ z oboru integrity $(T[x],\ +,\ \cdot)$ **dělí** polynom $\boldsymbol{f(x)}$ tohoto oboru integrity (značíme $g(x)|f(x)$) právě tehdy, když existuje polynom $h(x)$ takový, že $f(x) = g(x) \cdot h(x)$.

- Příklad: Pomocí definice dělitelnosti polynomů nalezněte polynom $h(x)$ takový, že platí $f(x) = g(x) \cdot h(x)$, pokud jsou dány polynomy takto:

  $f(x) = x^7 + 3x^6 + 5x^5 - 10x^4 - 36x^3 - 4x^2 - 26x - 3,$

  $g(x) = x^4 - 4x^2 + x - 3.$

  Nejprve je nutné zjistit, jaký stupeň polynomu $h(x)$ hledáme.

  $st[f(x)] = 7, st[g(x)] = 4$

  $7 - 4 = 3$

  Hledáme polynom $h(x) = ax^3 + bx^2 + cx + d.$

  Podle definice provedeme násobení polynomů $g(x)$ a $h(x)$ a získáme polynom $f'(x)$.

  $f'(x) = (x^4 - 4x^2 + x - 3) \cdot (ax^3 + bx^2 + cx + d) =$

  $= ax^7 + bx^6 - 4ax^5 + cx^5 + ax^4 - 4bx^4 + dx^4 - 3ax^3 + bx^3 - 4cx^3 -$

  $- 3bx^2 + cx^2 - 4dx^2 - 3cx + dx - 3d$

V dalším kroku porovnáme koeficienty mocnin polynomů $f(x)$ a $f'(x)$.

(1) $x^7 = ax^7$

(2) $3x^6 = bx^6$

(3) $5x^5 = -4ax^5 + cx^5$

(4) $-10x^4 = ax^4 - 4bx^4 + dx^4$

(5) $-36x^3 = -3ax^3 + bx^3 - 4cx^3$

(6) $-4x^2 = -3bx^2 + cx^2 - 4dx^2$

(7) $-26x = -3cx + dx$

(8) $-3 = -3d$

Získali jsme soustavu 8 rovnic o 4 neznámých.

Z rovnice (1) dostáváme koeficient $\underline{\underline{a = 1}}$.

Z rovnice (2) získáme koeficient $\underline{\underline{b = 3}}$.

Z rovnice (3) vyjádříme koeficient $c = 5 + 4 \cdot 1 = \underline{\underline{9}}$.

Z rovnice (8) obdržíme koeficient $\underline{\underline{d = 1}}$.

Nalezli jsme všechny 4 koeficienty a, b, c, d. Následně provedeme zkoušku, dosadíme do rovnic (4), (5), (6), (7) a ověříme, zda - li se rovná levá a pravá strana.

(4) $-10x^4 = ax^4 - 4bx^4 + dx^4$

$-10x^4 = 1 \cdot x^4 - 4 \cdot 3 \cdot x^4 + 1 \cdot x^4$

$\underline{\underline{-10x^4 = -10x^4}}$

(5) $-36x^3 = -3ax^3 + bx^3 - 4cx^3$

$-36x^3 = -3 \cdot 1 \cdot x^3 + 3 \cdot x^3 - 4 \cdot 9 \cdot x^3$

$\underline{\underline{-36x^3 = -36x^3}}$

(6) $-4x^2 = -3bx^2 + cx^2 - 4dx^2$

$-4x^2 = -3 \cdot 3 \cdot x^2 + 9 \cdot x^2 - 4 \cdot 1 \cdot x^2$

$\underline{\underline{-4x^2 = -4x^2}}$

(7) $-26x = -3cx + dx$

$26x = -3 \cdot 9 \cdot x + 1 \cdot x$

$\underline{26x = 26x}$

Po dosazení koeficientů a, b, c, d vyšla rovnost pravých a levých stran zbylých rovnic, tedy nalezli jsme koeficienty hledaného polynomu $h(x)$. Zbývá už jen dosadit koeficienty do hledaného polynomu $h(x)$.

Získali jsme polynom $h(x) = x^3 + 3x^2 + 9x + 1$.

2.2 JEDNOTKOVÝ PRVEK

Mezi významné prvky oboru integrity jsou řazeny jednotkové a asociované prvky. Tyto dva pojmy jsou důležité v relaci dělitelnosti.

Definice: Prvek $j \in I$ se nazývá ***jednotka ve smyslu dělitelnosti*** v J (též ***jednotka*** v I) právě tehdy, když existuje k prvku j inverzní prvek j^{-1} v I.

Zároveň lze tvrdit, že prvek j je jednotka v I právě tehdy, když $\exists x \in I: j \cdot x = 1$ tzn., že jednotka dělí 1, nebo-li $j|1$ (Blažek, 1985).

Věta: Součinem dvou jednotek je opět jednotka.

- Důkaz: Jako předpoklad zvolíme dvě jednotky z I j_1, j_2. Dle základní definice dělitelnosti existují prvky x, y, pro které platí: $1 = j_1 \cdot x$ a $1 = j_2 \cdot y$.

  Vynásobíme tyto rovnice.

  $1 = (j_1 \cdot x) \cdot (j_2 \cdot y) = (j_1 \cdot j_2) \cdot (x \cdot y)$

  Z rovnosti $1 = j_1 \cdot j_2$ plyne, že $(j_1 \cdot j_2)|1$, tedy prvek $j_1 \cdot j_2$ je též jednotka (Drábek).

Věta: Ke každé jednotce existuje v oboru integrity $(I, +, \cdot)$ převrácený prvek, který je opět jednotka.

- Důkaz: Prvek j opět předpokládáme, že je jednotkou v I. Opět dle definice dělitelnosti platí $1 = j \cdot x$, kde $x \in I$.

  Upravením rovnosti dostáváme $j = \frac{1}{x}$, jedná se o převrácenou hodnotu prvku j (Drábek).

Obecně jednotkový prvek je takový prvek, když k němu existuje v oboru integrity I inverzní prvek.

Počet jednotek v oboru integrity se odvíjí od toho, v jakém oboru integrity se nacházíme.

2.2.1 CELÁ ČÍSLA

Pro obor celých čísel Z existují právě dvě jednotky.

Jednotky snadno odvodíme. Víme, že hledáme taková čísla, která svým součinem dávají číslo 1.

$$1 \cdot 1 = 1$$
$$(-1) \cdot (-1) = 1$$

Jedinými dvěma jednotkami z oboru Z jsou čísla 1 a -1.

- Mějme libovolný prvek $a \in Z$, nechť a je jednotka. Jestliže a je jednotka, pak určitě musí existovat prvek $b \in Z$, pro který platí $a \cdot b = 1$.

  $$|a \cdot b| = |a| \cdot |b| = 1$$
  $$\Downarrow$$
  $$|a| = 1 \Rightarrow |b| = 1$$
  $$\Downarrow$$
  $$a = 1 \vee a = -1$$

  Tedy v tomto oboru integrity existují jediné dvě jednotky $J = \{1, -1\}$ (Blažek, 1985).

2.2.2 GAUSSOVA CELÁ ČÍSLA

V oboru integrity Gaussových celých číslech je hned několik jednotkových prvků. Jednotkami v oboru integrity $(G, +, \cdot)$ jsou čísla $1, -1, i, -i$. Množina J je označena jako množinu všech jednotek $J = \{1, -1, i, -i\}$.

Že existují pouze tyto jednotky v Gaussově celo číselném oboru lze opět jednoduše dokázat.

- Předpokládejme, že $\alpha = a + bi$ je $j \in G$, pak existuje $\beta = c + di$ tak, že $\alpha \cdot \beta = 1$. Postupujeme stejně jako u oboru celých čísel.

  $|\alpha \cdot \beta| = |\alpha| \cdot |\beta| = \sqrt{a^2 + b^2} \cdot \sqrt{c^2 \cdot d^2} = 1$, kde $a, b, c, d \in Z$, proto víme, že $a^2, b^2, c^2, d^2 \in N$. Z toho již můžeme určit čísla a a b (stejně c a d):

$(a = 1 \wedge b = 0) \Rightarrow \alpha = 1$

$(a = -1 \wedge b = 0) \Rightarrow \alpha = -1$

$(a = 0 \wedge b = 1) \Rightarrow \alpha = i$

$(a = 0 \wedge b = -1) \Rightarrow \alpha = -i$

Jednotkami v oboru integrity Gaussových celých čísel jsou právě čísla $1, -1, i, -i$ (Blažek, 1985).

2.2.3 POLYNOMY

Podobně jako v oboru integrity celých čísel a Gaussových celých číslech, tak i v oboru integrity polynomů nalezneme jednotkové prvky.

Věta: Jednotkami v oboru integrity $(T[x], +, \cdot)$ jsou dělitele jednotkového prvku 1. Jednotkami jsou všechny nenulové prvky tělesa $(T, +, \cdot)$.

2.3 ASOCIOVANÝ PRVEK

V předešlé kapitole byl zaveden jednotkový prvek, jenž je úzce spjat s prvek asociovaným.

Definice: Říkáme, že ***prvek a je asociován prvkem b*** oboru integrity $(I, +, \cdot)$ právě tehdy, když tyto prvky jsou vzájemně dělitelné. Zapisujeme $a \sim b \Leftrightarrow a|b \wedge b|a$.

Aby jeden prvek byl asociován druhým prvkem, platí nutná a postačující podmínka. Nutnou podmínku odvodíme důkazem z definice, kdy jeden prvek je asociován druhým prvkem.

- Důkaz:

  Vyjdeme z předpokladu $a \sim b$, pak existují prvky *x* a *y*.

  $a = b \cdot x$

  $b = a \cdot y$

  Dosadíme druhou rovnici do první rovnice.

  $a = (a \cdot y) \cdot x = a \cdot (x \cdot y)$

  $a \cdot 1 = a \cdot (x \cdot y)$

  $\underline{\underline{1 = x \cdot y}}$

Z toho víme, že čísla x a y jsou jednotkami daného oboru integrity I. Tedy prvek b získáme tak, že vynásobíme prvek a jednotkou j. Nutná podmínka je dána vztahem $a = j \cdot b$.

Postačující podmínka se dokazuje na shodném principu jako nutná podmínka, pouze jako předpoklad se určí rovnost $a = j \cdot b$.

Věta: Dva prvky a, b oboru integrity $(I, +, \cdot)$ jsou vzájemně asociované právě tehdy, když platí $a = j \cdot b$, kde j je jednotka daného oboru integrity.

Počet asociovaných prvků v jednotlivých oborech integrity závisí na tom, jaký je počet jednotkových prvků v daném oboru integrity (Drábek).

2.3.1 CELÁ ČÍSLA

Pro množinu Z vycházíme z definice asociovaného prvku. Platí tedy, že prvek a je asociován prvkem b právě tehdy, když číslo a dělí číslo b a zároveň i b dělí a. Jedná se tedy o celá čísla, která se vzájemně liší o znaménko, nebo-li čísla a a $-a$.

- Příklad: Mějme číslo $a = 73$ a číslo $b = -73$. Ověřte, že daná čísla jsou spolu asociovaná.

  $a \sim b \Leftrightarrow a|b \wedge b|a$

  Vydělíme číslo a číslem b a následně provedeme to samé v opačném případě, číslo b vydělíme číslem a.

  $73 \div (-73) = \underline{\underline{-1}}$

  $(-73) \div 73 = \underline{\underline{-1}}$

  Výsledek se shoduje. Tedy $a \div b = b \div a = -1$ a tím jsme ověřili, že číslo a je asociováno číslem b.

2.3.2 GAUSSOVA CELÁ ČÍSLA

V kapitole 2.2.2 jsou zavedeny jednotkové prvky pro Gaussův celočíselný obor integrity, mezi které patří množina $J = \{1, -1, i, -i\}$. Asociované prvky pro tento obor integrity jsou čísla přenásobena jednotkami, nebo-li čísla $\alpha, -\alpha, \alpha \cdot i, -\alpha \cdot i$.

- Příklad: Mějme Gaussovo celé číslo $\alpha = 9 - 4i$. Nalezněte všechny asociovaná čísla k číslu α.

1) $\alpha = 9 - 4i$

2) $-\alpha = -(9 - 4i) = -9 + 4i$

3) $\alpha \cdot i = (9 - 4i) \cdot i = 4 + 9i$

4) $-\alpha \cdot i = -(9 - 4i) \cdot i = (-9 + 4i) \cdot i = -4 - 9i$

2.3.3 POLYNOMY

Stejně jako u celých čísel a Gaussových celých číslech, tak i u polynomů vycházíme z definice pro asociovaný prvek.

Definice: Říkáme, že ***polynom $f(x)$ je asociován s polynomem $g(x)$*** právě tehdy, když $f(x)|g(x) \wedge g(x)|f(x)$. Značíme $f(x) \sim g(x)$.

Lze také konstatovat, že jeden polynom je asociován s druhým polynom právě tehdy, když v oboru integrity polynomů existuje nenulové číslo $c \in T$ takové, že platí $f(x) = c \cdot g(x)$. Jednoduše řečeno, polynom $f(x)$ vznikne z polynomu $g(x)$, který je násoben nenulovým prvkem z tělesa $(T, +, \cdot)$ a tyto polynomy jsou navzájem ekvivalentní. To znamená, že polynomy můžeme libovolně nahrazovat, to ovšem platí pouze pro relaci dělitelnosti (Drábek & Hora, 2001).

- Příklad:

$$\underbrace{4x^3 + 6x^2 + 22x + 2}_{f(x)} = \underbrace{2}_{c} \cdot (\underbrace{2x^3 + 3x^2 + 11x + 1}_{g(x)})$$

2.4 EUKLIDOVSKÁ NORMA

Další řešenou problematikou dělitelnosti je euklidovská norma. Než se budeme zabývat euklidovskou normou z hlediska různých oborů integrity, musíme ji nejprve definovat.

Definice: Obor integrity I se nazývá ***euklidovský obor integrity*** právě tehdy, když v něm existuje zobrazení v množiny I do množiny přirozených čísel N. Tohle zobrazení se nazývá ***euklidovská norma***. Pro libovolná $a, b \in I, b \neq 0$ platí:

1) $a|b \Rightarrow v(a) \leq v(b)$,

2) $\exists q, r \in I: (a = b \cdot q + r) \wedge [r = 0 \vee v(r) < v(b)]$.

Poznámka: Nechť I je euklidovský obor integrity. Pro libovolné prvky $a, b \in I, b \neq 0$ platí, $a|b \wedge v(a) = v(b) \Rightarrow b|a$.

2.4.1 CELÁ ČÍSLA – ABSOLUTNÍ HODNOTA

Euklidovskou normou v množině celých čísel je absolutní hodnota celého čísla. Absolutní hodnota celého čísla je nezáporné celé číslo, které se může přiřadit k libovolnému celému číslu a. Jednoduše je možné říct, že absolutní hodnota je zobrazení množiny Z na N. Absolutní hodnotu značíme $|a|$ (Blažek, 1982).

Definice: ***Absolutní hodnotu*** celého čísla a definujeme:

1. Je-li $a \geq 0$, pak $|a| = a$.
2. Je-li $a < 0$, pak $|a| = -a$.

V následující větě shrneme základní vlastnosti týkající se absolutní hodnoty.

Věta: Pro absolutní hodnotu v Z platí:

a. $\forall a \in Z: |a| \in N$,

b. $\forall a \in Z: |a| = 0 \Leftrightarrow a = 0$,

c. $\forall a \in Z: |a| = |-a|$,

d. $\forall a \in Z: -|a| \leq a \leq |a|$,

e. $\forall b \in N\ \forall a \in Z: -b \leq a \leq b \Rightarrow |a| \leq b$,

f. $\forall a, b \in Z: |a + b| \leq |a| + |b|$,

g. $\forall a, b \in Z: |a \cdot b| = |a| \cdot |b|$,

h. $\forall a, b \in Z: \left|\frac{a}{b}\right| = \frac{|a|}{|b|}$, pro $b \neq 0$.

2.4.2 GAUSSOVA CELÁ ČÍSLA - NORMA

Nyní se euklidovská normu aplikuje na obor integrity Gaussových celých čísel.

Definice: Mějme Gaussovo celé číslo $\alpha = a + bi$. ***Normou Gaussova celého čísla*** budeme rozumět přirozené číslo $N(\alpha)$, které je definováno následujícím předpisem: $N(\alpha) = \alpha \cdot \bar{\alpha}$, kde číslo $\bar{\alpha}$ je komplexně sdružené číslo k číslu α. Normu Gaussova celého čísla značíme $N(\alpha)$.

- Příklad: Mějme číslo $\alpha = 4 + 7i$. Nalezněte euklidovskou normu čísla α.

  Máme Gaussovo celé číslo $\alpha = 4 + 7i$.

Komplexně sdružené číslo je $\bar{\alpha} = 4 - 7i$.

Nyní vyjdeme z definice euklidovské normy.

$N(\alpha) = \alpha \cdot \bar{\alpha}$
$N(\alpha) = (4 + 7i) \cdot (4 - 7i)$
$N(\alpha) = 16 - 28i + 28i - 49i^2$
$N(\alpha) = 16 + 49$
$\underline{N(\alpha) = 65}$

Euklidovská norma čísla α je rovna $N(\alpha) = 65$.

Z předchozího příkladu jsme zjistili, že pro euklidovskou normu též platí následující poznámka.

Poznámka: Mějme normu $N(\alpha)$, která je rovna součtu čtverců $a^2 + b^2$ podle vzorce $N(\alpha) = \alpha \cdot \bar{\alpha}$, kde $\alpha = a + bi$. Normu můžeme chápat jako zobrazení $G \to N$, které splňuje rovnost $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$ (Conrad, 2019).

Provedeme jednoduchý důkaz poznámky, který vychází z věty o komplexně sdružených číslech.

- Důkaz: Mějme α a β.

  $N(\alpha \cdot \beta) = (\alpha \cdot \beta) \cdot \left(\overline{\alpha \cdot \beta}\right) = (\alpha \cdot \beta) \cdot \left(\bar{\alpha} \cdot \bar{\beta}\right) = (\alpha \cdot \bar{\alpha}) \cdot (\beta \cdot \bar{\beta})$

  Zde se už vychází z definice normy pro Gaussova celá čísla $N(\alpha) = \alpha \cdot \bar{\alpha}$, platí tedy: $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$ (Drábek).

Pomocí ilustračního příkladu je ověřena multiplikativní vlastnost euklidovské normy. Tedy podle znění výše uvedené poznámky, že euklidovská norma součinu dvou Gaussových celých čísel je totéž, jako součin jednotlivých norem Gaussových celých čísel.

- Příklad: Mějme čísla $\alpha = 4 + 7i$ a $\beta = 12 - 3i$. Ověřte, zda platí $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$.

  V minulém příkladu jsme vypočítali euklidovskou normu čísla α: $N(\alpha) = 65$.

  Vypočítáme normu čísla β. Použijeme vzorec $N(\beta) = a^2 + b^2$.

$N(\beta) = 12^2 + (-3)^2$

$N(\beta) = 144 + 9$

$\underline{\underline{N(\beta) = 153}}$

Dále spočítáme $\alpha \cdot \beta$.

$(4 + 7i) \cdot (12 - 3i) = 48 - 12i + 84i - 21i^2 = 48 + 72i + 21 = \underline{\underline{69 + 72i}}$

Zbývá ověřit zda $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$.

$L = N(\alpha \cdot \beta) = 69^2 + 72^2 = 4761 + 5184 = \underline{\underline{9945}}$

$P = N(\alpha) \cdot N(\beta) = 65 \cdot 153 = \underline{\underline{9945}}$

$\underline{\underline{L = P}}$

Ověřili jsme rovnost $N[(4 + 7i) \cdot (12 - 3i)] = N(4 + 7i) \cdot N(12 - 3i)$.

2.4.3 VYUŽITÍ NORMY GAUSSOVÝCH CELÝCH ČÍSEL

V minulé kapitole je zavedena norma pro Gaussova celá čísla. Další části je věnována normě z hlediska dělitelnosti a je ukázáno využití euklidovské normy. Dále platí následující věta.

Věta: Jestliže jsou Gaussova celá čísla dělitelná, pak i odpovídající normy Gaussových celých čísel jsou dělitelné. Platí vzorec: $\forall \alpha, \beta \in G: \alpha|\beta \Rightarrow N(\alpha)|N(\beta)$.

Jinak řečeno, jestliže normy nejsou dělitelné jako přirozená čísla, pak ani jejich příslušná Gaussova celá čísla nejsou dělitelná (Drábek).

- Důkaz: Při důkazu věty vycházíme ze vzorce, následně aplikujeme definici dělitelnosti.

$\alpha|\beta \;\Rightarrow\; \beta = \alpha \cdot x$

$\Downarrow$

$N(\beta) = N(\alpha \cdot x)$

$N(\beta) = N(\alpha) \cdot N(x)$

$\Downarrow$

$N(\alpha)|N(\beta)$

Ze vztahu $N(\beta) = N(\alpha) \cdot N(x)$ dostáváme dělitelnost norem Gaussových celých čísel, tedy pokud jedno Gaussovo celé číslo dělí to druhé, pak i jejich odpovídající normy jsou dělitelné.

Z věty plyne nutná podmínka dělitelnosti euklidovských norem tedy, pokud číslo α dělí číslo β, pak i $N(\alpha)$ dělí $N(\beta)$. Pak tedy platí, že normy Gaussových celých čísel sice mohou být dělitelné, ale ještě není jednoznačně dáno, že i daná čísla jsou dělitelná.

Dále je uvedeno několik ilustračních příkladů. V prvním příkladu se jedná o jasnou implikaci, kdy je brán jako předpoklad to, že číslo α dělí číslo β a z toho vyplývá, že i Euklidovské normy těch Gaussových celých čísel jsou dělitelné.

Ve druhém a třetím ukázkovém příkladu je použita postačující podmínka dělitelnosti norem. Ve druhém příkladu není splněna podmínka, že $N(\alpha)|N(\beta)$, a tedy ani číslo $\alpha \nmid \beta$. Naopak ve třetím příkladu je postačující podmínka splněna, ale Gaussova celá čísla dělitelná nejsou.

- Příklad: Mějme čísla $\alpha = 2 + 3i$ a $\beta = 7 + 4i$. Dokažte, že platí $\alpha|\beta$ a $N(\alpha)|N(\beta)$.

  Nejprve podle definice, dokážeme, že $\alpha|\beta$.

  $2 + 3i|7 + 4i$

  $7 + 4i = (2 + 3i) \cdot (x_1 + x_2 i)$
  $7 + 4i = 2x_1 + 3x_1 i + 2x_2 i + 3x_2 i^2$
  $7 + 4i = 2x_1 + 3x_1 i + 2x_2 i - 3x_2$
  $7 = 2x_1 - 3x_2 \quad | \cdot 3$
  $4 = 3x_1 + 2x_2 \quad | \cdot (-2)$
  $21 = 6x_1 - 9x_2$
  $-8 = -6x_1 - 4x_2$
  $13 = -13x_2$
  $x_2 = -1$

  $2x_1 = 7 + 3x_2$
  $2x_1 = 7 + 3(-1)$
  $2x_1 = 7 - 3$

$$2x_1 = 4$$
$$x_1 = \frac{4}{2}$$
$$\underline{\underline{x_1 = 2}}$$

Nyní dokážeme dělitelnost norem čísel α a β.

$N(\alpha)|N(\beta)$
$(2^2 + 3^2)|(7^2 + 4^2)$
$(4 + 9)|(49 + 16)$
$13|65$

Dokázali jsme, že $(2 + 3i)|(7 + 4i)$ a $N(2 + 3i)|N(7 + 4i)$.

- Příklad: Mějme čísla $\alpha = 3 + 3i$ a $\beta = 4 + 5i$. Zjistěte, zda platí $\alpha|\beta$.

  V tomto případě začneme nejdříve spočítáním norem čísel α a β, tedy zjistíme, zda platí nutná podmínka.

  $\alpha = 3 + 3i$

  $N(\alpha) = 3^2 + 3^2 = 9 + 9 = \underline{\underline{18}}$

  $\beta = 4 + 5i$

  $N(\beta) = 4^2 + 5^2 = 16 + 25 = \underline{\underline{41}}$

  $N(\alpha)$ dělí $N(\beta)$?

  ? $18|41$

  $18 \nmid 41$

  Není splněna nutná podmínka. Normy Gaussových celých čísel nejsou dělitelné, tedy ani Gaussova celá čísla nejsou spolu dělitelná.

- Příklad: Mějme čísla $\alpha = 1 + 2i$ a $\beta = 1 + 3i$. Zjistěte, zda platí $\alpha|\beta$.

  Nejprve opět zjistíme, zda je nebo není splněna postačující podmínka.

  $N(\alpha) = 1^2 + 2^2 = 1 + 4 = \underline{\underline{5}}$

  $N(\beta) = 1^2 + 3^2 = 1 + 9 = \underline{\underline{10}}$

  $N(\alpha)$ dělí $N(\beta)$?

$?\ 5|10$

$5|10$

Nutná podmínka je splněna, ale nemůžeme jednoznačně říct, že číslo α dělí číslo β. Zbývá tedy zjistit, zda α dělí β.

$$1 + 3i = (1 + 2i) \cdot (x_1 \cdot x_2 i)$$
$$1 + 3i = x_1 + x_2 i + 2x_1 i + 2x_2 i^2$$
$$\underline{1 + 3i = x_1 + x_2 i + 2x_1 i - 2x_2}$$
$$1 = x_1 - 2x_2$$
$$\underline{3 = 2x_1 + x_2 \ | \cdot 2}$$
$$1 = x_1 - 2x_2$$
$$\underline{6 = 4x_1 + 2x_2}$$

Sečteme první a druhou rovnici.

$$7 = 5x_1$$
$$\underline{\underline{x_1 = \frac{7}{5}}}$$

Stejně tak jako v předešlém příkladu nám nevyšlo celé číslo, je možné prohlásit, že $1 + 2i \nmid 1 + 3i$.

2.4.4 POLYNOMY – STUPEŇ

I pro polynomy lze nalézt typ euklidovské normy, jedná se o stupeň polynomu.

Věta: Budiž dány polynomy $f(x) \neq 0, g(x)$ z oboru integrity $(T[x], +, \cdot)$, kde $st[g(x)] \geq 1$, potom existují polynomy $Q(x), R(x)$ takové, že platí:

$$\boldsymbol{f(x) = Q(x) \cdot g(x) + R(x)}, \text{ kde } R(x) = 0 \text{ nebo } st[R(x)] < st[g(x)].$$

Poznámka: Jestliže $R(x) = 0$ říkáme, že polynom $g(x)$ dělí polynom $f(x)$. Zapisujeme $\boldsymbol{g(x)|f(x)}$ (Drábek & Hora, 2001).

Z toho vyplývá, že stupeň polynomu, který dělí, nesmí být větší než stupeň polynomu, který je dělen.

- Příklad: Mějme komutativní těleso racionálních čísel $(Q, +, \cdot)$ a jsou dány polynomy $f(x) = 4x^4 + 4x^3 - 2x^2 + 6x + 5$ a $g(x) = x^2 - 2x - 1$. Nalezněte polynomy $Q(x)$ a $R(x)$ takové, že platí $f(x) = Q(x) \cdot g(x) + R(x)$.

$$(4x^4 + 4x^3 - 2x^2 + 6x + 5) \div (x^2 - 2x - 1) = \underbrace{4x^2 + 12x + 26}_{Q(x)}$$

$$\underline{-(4x^4 - 8x^3 - 4x^2)}$$

$$12x^3 + 2x^2 + 6x + 5$$

$$\underline{-(12x^3 - 24x^2 - 12x)}$$

$$26x^2 + 18x + 5$$

$$\underline{-(26x^2 - 52x - 26)}$$

$$\underbrace{70x + 31}_{R(x)}$$

Našli jsme polynomy $R(x)$ a $Q(x)$, pro které platí:

$$(4x^4 + 4x^3 - 2x^2 + 6x + 5) = (4x^2 + 12x + 26) \cdot (x^2 - 2x - 1) + (70x + 31).$$

2.4.5 VYUŽITÍ NORMY POLYNOMŮ

Obdobně jako je ukázáno využití euklidovské normy Gaussových celých čísel, tak je ukázáno využití euklidovské normy polynomů. Opět se vychází z postačující podmínky, jejíž znění je následující. Jestliže polynom $g(x)$ dělí polynom $f(x)$, pak stupeň polynomu $g(x)$ musí být menší nebo roven, než stupeň polynomu $f(x)$.

Euklidovská norma se užívá při dělení polynomů. Tento princip je ukázán klasickým způsobem, který se vyučuje na základní škole. V další části jsou uvedeny tři ukázkové příklady na dělení polynomů. V prvním a ve druhém příkladu je splněna nutná podmínka. Když je podmínka splněna, nastávají dvě možnosti. Buď je jeden polynom dělen druhým polynomem beze zbytku, nebo se zbytkem $R(x)$. Ve třetím ilustračním příkladu není splněna postačující podmínka, tím pádem ani polynom $g(x)$ nedělí polynom $f(x)$.

- Příklad: Mějme komutativní těleso racionálních čísel $(Q, +, \cdot)$ a jsou dány polynomy $f(x) = x^5 + 3x^4 - 11x^3 + 13x^2 + 18x - 8$ a $g(x) = x^2 + 5x - 2$. Určete, zda polynom $g(x)$ dělí polynom $f(x)$.

Určíme zda $st[g(x)] < st[f(x)]$.

$st[g(x)] = 2$

$st[f(x)] = 5$

$2 < 5$

Nutná podmínka je splněna, tudíž podle ní nelze rozhodnout o dělitelnosti polynomů a musíme ji ověřit dělením zadaných polynomů.

$(x^5 + 3x^4 - 11x^3 + 13x^2 + 18x - 8) \div (x^2 + 5x - 2) = \underline{\underline{x^3 - 2x^2 + x + 4}}$

$\underline{-(x^5 + 5x^4 - 2x^3)}$

$-2x^4 - 9x^3 + 13x^2 + 18x - 8$

$\underline{-(-2x^4 - 10x^3 + 4x^2)}$

$x^3 + 9x^2 + 18x - 8$

$\underline{-(x^3 + 5x^2 - 2x)}$

$4x^2 + 20x - 8$

$\underline{-(4x^2 + 20x - 8)}$

$\underline{\underline{0}}$

Zjistili jsme, že polynom $g(x) = x^2 + 5x - 2$ dělí beze zbytku polynom $f(x) = x^5 + 3x^4 - 11x^3 + 13x^2 + 18x - 8$.

- Příklad: Mějme komutativní těleso racionálních čísel $(Q, +, \cdot)$ a jsou dány polynomy $f(x) = 3x^3 - x^2 + 2x - 6$ a $g(x) = x^2 + x + 3$. Určete, zda polynom $g(x)$ dělí polynom $f(x)$.

  Určíme zda $st[g(x)] < st[f(x)]$.

  $st[g(x)] = 2$

  $st[f(x)] = 3$

  $2 < 3$

  Nutná podmínka je splněna.

$(3x^3 - x^2 + 2x - 6) \div (x^2 + x + 3) = \underline{\underline{3x - 4}}$

$\underline{-(-3x^3 - 3x^2 + 9x)}$

$-4x^2 - 7x - 6$

$\underline{-(-4x^2 - 4x - 12)}$

$\underbrace{-3x + 6}_{R(x)}$

Polynom $f(x)$ není dělitelný polynomem $g(x)$ beze zbytku $R(x)$, $f(x) = 3x^3 - x^2 + 2x - 6 = (x^2 + x + 3) \cdot (3x - 4) + (-3x + 6)$.

- Příklad: Mějme komutativní těleso racionálních čísel $(Q, +, \cdot)$ a jsou dány polynomy $f(x) = x^3 + 2x^2 - 10x + 5$ a $g(x) = x^5 + 4x^4 + 7x^3 - x^2 + x - 15$. Určete, zda polynom $g(x)$ dělí polynom $f(x)$.

  Nejprve opět určíme zda $st[g(x)] < st[f(x)]$.

  $st[g(x)] = 5$

  $st[f(x)] = 3$

  $5 \not< 3$

  Není splněna nutná podmínka, tudíž polynom $g(x) \nmid f(x)$.

3 KRITÉRIA DĚLITELNOSTI V OBORECH INTEGRITY

3.1 ZNAKY DĚLITELNOSTI NA MNOŽINĚ Z

V následující kapitole se je řešena dělitelnost na množině celých čísel. I pro množinu Z platí obecná definice dělitelnosti, tedy $b|a \Leftrightarrow a = x \cdot b$, pro $\forall a, b, x \in Z$.

Dělení se zbytkem: Ke každým dvěma celým číslům a, b $(b \neq 0)$ existuje právě jedna dvojice celých čísel q, r tak, že platí $a = b \cdot q + r$, pro $0 \leq r < |b|$. Číslo a se nazývá dělenec, číslo b dělitel, číslo q (neúplný) podíl a číslo r je zbytek. Důležité je, že číslo r musí být nezáporné číslo.

- Příklad:

  $368 \div 12 = 30$

  8

  zb. 8

  $\underline{368 = 12 \cdot 30 + 8}$

Dělení beze zbytku: Zvláštním případem pro dělení se zbytkem pro $r = 0$ na množině Z je dělení beze zbytku (Pěchoučková).

- Příklad:

  $272 \div 4 = 68$

  32

  zb. 0

  $\underline{272 = 4 \cdot 68 + 0}$

Mezi další znaky dělitelnosti řadíme vlastnosti relace, konkrétně vlastnosti relace dělitelnosti. Mějme množinu M z oboru celých čísel, pro kterou platí:

1) **Reflexivita**: $\forall a \in M: a \, \rho \, a$ tzn., prvek a je v relaci s prvkem a.

$$\forall a \in Z: a|a \qquad \exists x \in Z: a = a \cdot x$$

$$a = a \cdot 1$$

→ libovolné nenulové číslo a dělí samo sebe

- Příklad:

  $10|10, 45|45, -3|-3$

2) **Symetrie**: $\forall a, b \in M, a \neq b: a \rho b \Rightarrow b \rho a$

   $\forall a, b \in Z, a \neq b: a|b \Rightarrow b|a$

   → jestliže číslo a dělí číslo b, pak číslo b dělí číslo a.

- Příklad:

  $3|18$, ale $18 \nmid 3 \Rightarrow$ relace dělitelnosti není symetrická, je tedy antisymetrická.

3) **Tranzitivita**: $\forall a, b, c \in M: a \rho b \ \wedge b \rho c \Rightarrow a \rho c$

   $\forall a, b, c \in Z: a|b \ \wedge b|c \Rightarrow a|c$

- Příklad:

  $3|6 \ \wedge 6|18 \Rightarrow 3|18$

3.1.1 DĚLITELNOST DVĚMA

Libovolné číslo je dělitelné dvěma právě tehdy, když je poslední číslice daného čísla sudá tzn., pokud je číslo zakončené jednou z číslic $0, 2, 4, 6$ nebo 8.

- Příklad: $22, 100, 72\,836, \ldots$
- Důkaz:

  Mějme číslo a, které má a_0 jednotek, a_1 desítek, a_2 stovek, a_3 tisíců atd.

  $$a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + \cdots + \ a_n \cdot 10^n$$

  Vytkneme 10 z desítek, stovek, tisíců, …

  $$a = a_0 + 10 \cdot \underbrace{(a_1 + \ a_2 \cdot 10 + a_3 \cdot 10^2 + \cdots + a_n \cdot 10^{n-1})}_{x}$$

  Ze závorky $a_1 + \ a_2 \cdot 10 + a_3 \cdot 10^2 + \cdots + a_n \cdot 10^{n-1}$ dostaneme číslo x.

  $$a = a_0 + 10 \cdot x$$

  $$a = a_0 + 2 \cdot 5 \cdot x$$

  Z toho plyne, je – li číslo a_0 sudé, pak původní číslo a je dělitelné dvěma.

3.1.2 DĚLITELNOST TŘEMI

Libovolné číslo je dělitelné třemi právě tehdy, když je ciferný součet daného čísla dělitelný třemi.

- Příklad: $21, 351, 28\,431, \ldots$
- Důkaz:

  Mějme číslo a, které má a_0 jednotek, a_1 desítek, a_2 stovek, a_3 tisíců atd.

  $$a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + \cdots + a_n \cdot 10^n$$

  Protože víme, že žádná mocnina 10^n není dělitelná třemi, musíme si mocninu upravit.

konktrétně	obecně
$10 = 3 \cdot 3 + 1$	$= 3x_1 + 1$
$100 = 3 \cdot 33 + 1$	$= 3x_2 + 1$
$1000 = 3 \cdot 333 + 1$	$= 3x_3 + 1$

  Následně obecný zápis dosadíme do původního čísla a.

$$a = a_0 + a_1 \cdot (3x_1 + 1) + a_2 \cdot (3x_2 + 1) + a_3 \cdot (3x_3 + 1) + \cdots + a_n \cdot (3x_n + 1)$$
$$a = a_0 + 3a_1 \cdot x_1 + a_1 + 3a_2 \cdot x_2 + a_2 + 3a_3 \cdot x_3 + a_3 + \cdots + 3a_n \cdot x_n + a_n$$
$$a = \underbrace{(a_0 + a_1 + a_2 + a_3 + \cdots + a_n)}_{ciferný\ součet} + 3 \cdot \underbrace{(a_1 \cdot x_1 + a_2 \cdot x_2 + a_3 \cdot x_3 + \cdots + a_n \cdot x_n)}_{x}$$

  Z toho plyne, je – li ciferný součet čísla a dělitelný třemi, pak je číslo dělitelné třemi.

Věta: Číslo vyjádřené v desítkové soustavě dává přidělení třemi stejný zbytek, jako dává při dělení třemi jeho ciferný součet.

3.1.3 DĚLITELNOST ČTYŘMI

Libovolné číslo je dělitelné čtyřmi právě tehdy, když je jeho poslední dvojčíslí dělitelné čtyřmi.

- Příklad: $24, 864, 352\,836, \ldots$

- Důkaz:

  Mějme číslo a, které má a_0 jednotek, a_1 desítek, a_2 stovek, a_3 tisíců atd.

  $$a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + \cdots + a_n \cdot 10^n$$

  Vytkneme 10^2 ze stovek, tisíců, desetitisíců,…

  $$a = a_0 + a_1 \cdot 10 + 10^2 \cdot \underbrace{(a_2 + a_3 \cdot 10 + a_4 \cdot 10^2 + \cdots + a_n \cdot 10^{n-2})}_{x}$$

  Ze závorky $a_2 + a_3 \cdot 10 + a_4 \cdot 10^2 + \cdots + a_n \cdot 10^{n-2}$ dostaneme číslo *x*.

  $$a = a_0 + a_1 \cdot 10 + 100 \cdot x$$

  $$a = a_0 + a_1 \cdot 10 + 4 \cdot 25 \cdot x$$

  Z toho plyne, je – li číslo $a_0 + a_1 \cdot 10$ dělitelné čtyřmi, pak původní číslo a je také dělitelné čtyřmi.

3.1.4 DĚLITELNOST PĚTI

Libovolné číslo je dělitelné pěti právě tehdy, když jeho poslední číslice je 0 nebo 5.

- Příklad: $35, 940, 925\,675, \ldots$
- Důkaz:

  V důkazu dělitelnosti pěti postupujeme úplně stejně při důkazu dělitelnosti 2.

  Mějme číslo a, které má a_0 jednotek, a_1 desítek, a_2 stovek, a_3 tisíců atd.

  $$a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + \cdots + a_n \cdot 10^n$$

  Vytkneme 10 z desítek, stovek, tisíců, …

  $$a = a_0 + 10 \cdot \underbrace{(a_1 + a_2 \cdot 10 + a_3 \cdot 10^2 + \cdots + a_n \cdot 10^{n-1})}_{x}$$

  Dostáváme číslo x ze závorky $a_1 + a_2 \cdot 10 + a_3 \cdot 10^2 + \cdots + a_n \cdot 10^{n-1}$.

  $$a = a_0 + 10 \cdot x$$

  $$a = a_0 + 2 \cdot 5 \cdot x$$

  Z toho plyne, je – li číslo a_0 dělitelné pěti, pak původní číslo a je také dělitelné pěti.

3.1.5 DĚLITELNOST ŠESTI

Libovolné číslo je dělitelné šesti právě tehdy, když je dělitelné dvěma a zároveň je dělitelné třemi.

- Příklad: $36, 144, 2\,148,$ …

3.1.6 DĚLITELNOST SEDMI

Existuje více kritérií pro zjištění dělitelnosti čísla sedmi. Nicméně na základní škole se ani neučí, protože jsou složitá. V řadě případů je lepší dělitelnost ověřit dělením čísla sedmi.

- Příklad: $49, 455, 5\,964,$ …

Složitost kritérií bude představeno na jedním z nich a následně předvedeno i na ukázkovém příkladu.

„Od zkoumaného čísla oddělíme poslední cifru a dvojnásobek čísla vyjádřeného touto cifrou odečteme od čísla zapsaného zbylou částí zápisu. Je-li vzniklé číslo dělitelné sedmi, je i zkoumané číslo dělitelné sedmi.“

(Davidová, 2019, s. 2)

- Příklad: Ověřte, že je číslo 66584 dělitelné sedmi.

  Podle kritéria nejprve oddělíme poslední cifru (4), vynásobíme ji dvěma a odečteme od zbylé části zápisu.

  $$6658 - 4 \cdot 2 = 6658 - 8 = \underline{\underline{6650}}$$

  Číslo 6650 je stále moc velké, pro jednoduché zjištění dělitelnosti sedmi, pokračujeme opět oddělením poslední cifry.

  $$665 - 0 \cdot 2 = \underline{\underline{665}}$$

  $$66 - 5 \cdot 2 = \underline{\underline{56}}$$

  O číslu 56 víme, že je dělitelné sedmi: $56 \div 7 = 8$, tedy i původní číslo 66584 je dělitelné sedmi.

3.1.7 DĚLITELNOST OSMI

Libovolné číslo je dělitelné osmi právě tehdy, když je poslední trojčíslí daného čísla dělitelné osmi.

- Příklad: $64, 496, 6\,080,$ …
- Důkaz:

  Mějme číslo a, které má a_0 jednotek, a_1 desítek, a_2 stovek, a_3 tisíců atd.

  $$a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + a_4 \cdot 10^4 + \cdots + a_n \cdot 10^n$$

  Vytkneme 10^3 z tisíců, desetitisíců,…

$$a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + 10^3 \cdot \underbrace{(a_3 + a_4 \cdot 10 + a_5 \cdot 10^2 + \cdots + a_n \cdot 10^{n-3})}_{x}$$

  Ze závorky $a_3 + a_4 \cdot 10 + a_5 \cdot 10^2 + \cdots + a_n \cdot 10^{n-3}$ dostaneme číslo x.

  $$a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + 10^3 \cdot x$$

  $$a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + 8 \cdot 125 \cdot x$$

  Z toho plyne, je – li číslo $a_0 + a_1 \cdot 10 + a_2 \cdot 100$ dělitelné osmi, pak původní číslo a je také dělitelné osmi.

3.1.8 DĚLITELNOST DEVÍTI

Libovolné číslo je dělitelné devíti právě tehdy, když je ciferný součet daného čísla dělitelný devíti.

- Příklad: $54, 4\,104, 67\,788,$ …
- Důkaz:

  Mějme číslo a, které má a_0 jednotek, a_1 desítek, a_2 stovek, a_3 tisíců atd.

  $$a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + \cdots + a_n \cdot 10^n$$

  Protože víme, že žádná mocnina 10^n není dělitelná devíti, musíme si mocninu upravit.

konktrétně	obecně
$10 = 9 \cdot 1 + 1$	$= 9x_1 + 1$
$100 = 9 \cdot 11 + 1$	$= 9x_2 + 1$
$1000 = 9 \cdot 111 + 1$	$= 9x_3 + 1$

  Následně obecný zápis dosadíme do původního čísla a.

$$a = a_0 + a_1 \cdot (9x_1 + 1) + a_2 \cdot (9x_2 + 1) + a_3 \cdot (9x_3 + 1) + \cdots + a_n \cdot (9x_n + 1)$$
$$a = a_0 + 9a_1 \cdot x_1 + a_1 + 9a_2 \cdot x_2 + a_2 + 9a_3 \cdot x_3 + a_3 + \cdots + 9a_n \cdot x_n + a_n$$
$$a = \underbrace{(a_0 + a_1 + a_2 + a_3 + \cdots + a_n)}_{ciferný\ součet} + 9 \cdot \underbrace{(a_1 \cdot x_1 + a_2 \cdot x_2 + a_3 \cdot x_3 + \cdots + a_n \cdot x_n)}_{x}$$

Z toho plyne, je – li ciferný součet čísla a dělitelný devíti, pak je číslo dělitelné devíti.

Věta: Číslo vyjádřené v desítkové soustavě dává přidělení devíti stejný zbytek, jako dává při dělení devíti jeho ciferný součet.

3.1.9 DĚLITELNOST DESÍTI

Libovolné číslo je dělitelné desíti právě tehdy, když je poslední číslice 0.

Dělitelnost čísla deseti také souvisí s dělitelností dvěma a pěti. Libovolné číslo je dělitelné desíti právě tehdy, když je dané číslo dělitelné zároveň dvěma a pěti.

- Příklad: $30, 3\,520, 790\,620, \ldots$

3.1.10 DĚLITELNOST JEDENÁCTI

Libovolné číslo je dělitelné jedenácti právě tehdy, když je rozdíl součtu cifer sudých řádů a cifer lichých řádů dělitelný jedenácti.

- Příklad: $88, 7\,183, 105\,985, \ldots$
- Důkaz:

  Mějme číslo a, které má a_0 jednotek, a_1 desítek, a_2 stovek, a_3 tisíců atd.

  $$a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + a_3 \cdot 10^3 + \cdots + a_n \cdot 10^n$$

  Protože víme, že žádná mocnina 10^n není dělitelná jedenácti, musíme si mocninu upravit.

konktrétně	obecně
$10 = 11 \cdot 1 - 1$	$= 11x_1 - 1$
$100 = 11 \cdot 9 + 1$	$= 11x_2 + 1$
$1000 = 11 \cdot 91 - 1$	$= 11x_3 - 1$
$10000 = 11 \cdot 909 + 1$	$= 11x_4 + 1$

$\Rightarrow 11x_k + 1$ pro sudé mocniny 10

$\Rightarrow 11x_k - 1$ pro liché mocniny 10

Následně obecný zápis dosadíme do původního čísla a.

$$a = a_0 + a_1(11x_1 - 1) + a_2(11x_2 + 1) + a_3(11x_3 - 1) + \cdots + a_n[11x_n + (-1)^n]$$
$$a = a_0 + 11a_1x_1 - a_1 + 11a_2x_2 + a_2 + 11a_3x_3 - a_3 + \cdots + 11a_nx_n + (-1)^n a_n$$
$$a = [a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n] + 11 \cdot \underbrace{(a_1x_1 + a_2x_2 + a_3x_3 + \cdots + a_nx_n)}_{x}$$
$$a = \underbrace{(a_0 + a_2 + a_4 + \cdots) - (a_1 + a_3 + a_5 + \cdots)}_{\substack{Rozdíl\ součtu\ cifer\ sudých\ \text{řádů} \\ a\ cifer\ lichých\ \text{řádů}.}} + 11 \cdot x$$

Z toho plyne, je-li rozdíl součtu cifer sudých řádů a cifer lichých řádů dělitelný jedenácti, pak je číslo *a* dělitelné jedenácti.

Věta: Číslo vyjádřené v desítkové soustavě dává přidělení jedenácti stejný zbytek, jako dává při dělení jedenácti rozdíl součtu cifer sudých řádů a cifer lichých řádů.

- Praktické využití dělitelnosti jedenácti: Dělitelnost jedenácti se používá pro ověření pravosti rodného čísla.
    - Příklad: Rodné číslo je $\mathbf{935209/2310}$.

      cifry sudých řádů → $9 + 5 + 0 + 2 + 1 = 17$

      cifry lichých řádů → $3 + 2 + 9 + 3 + 0 = 17$

      sudé – liché → $17 - 17 = 0$

      Z toho vyplývá, odečteme – li cifry lichých řádů od těch sudých, dostáváme zbytek 0. Tudíž číslo $\mathbf{9352092310}$ je dělitelné 11 beze zbytku a dokázali jsme, že toto rodné číslo je pravé (Davidová, 2019).

4 POJEM IREDUCIBILNÍHO PRVKU A PRVOČINITELE V OBORU INTEGRITY

Nedílnou součástí oboru dělitelnosti jsou také ireducibilní prvky či prvočísla. Nejprve je potřeba definovat pojem samozřejmého dělitele.

Pod pojmem ***samozřejmí dělitele*** (též nevlastní dělitele) přirozeného čísla a jsou chápána čísla a a 1.

Pro každé číslo a platí rovnost $a = 1 \cdot a$. Z této rovnosti již víme, že pro číslo 1 existuje jediný dělitel, tím je právě číslo 1 (Polák, 2005).

Definice: Prvek a oboru integrity I takový, že $a \neq 0, a \nsim 1$, (tzn. prvek *a* není jednotkovým prvkem v I), se nazývá ***ireducibilní prvek*** v I, právě když má pouze nevlastního dělitele. ***Reducibilní prvek*** je nenulový prvek z I, který není jednotkou a není ireducibilní.

Definice: Mějme přirozené číslo $p \in I$, $p > 1$. Toto číslo nazýváme ***prvočíslem*** (též prvočinitel) právě tehdy, když má pouze samozřejmé dělitele.

Zapisujeme: p je prvočíslo $\Leftrightarrow D(p) = \{1, p\}$.

Definice: Libovolné přirozené číslo a se nazývá ***složené číslo***, jestliže není prvočíslo, to znamená, že je dělitelné více jak dvěma děliteli.

Věta: Pro prvek $p \in I, p \neq 0$, který je prvočíslo, platí ***prvočíselná vlastnost***:

$\forall p \in N: p|ab \Rightarrow p|a \vee p|b$.

Tento zápis říká, jestliže je p prvočíslo a dělí součin prvků a a b, pak dělí alespoň jeden z daných prvků a a b.

Pro prvočísla a ireducibilní prvky platí také následující věta.

Věta: Jestliže je přirozené číslo p prvočinitelem v I, pak číslo p je ireducibilní prvek v I.

4.1 ZJIŠTĚNÍ PRVOČÍSELNOSTI

Rozhodnout zda je číslo x prvočíslem či složeným číslem patří mezi důležité vlastnosti v oboru teorie čísel. Je několik způsobů, kterými lze prvočíselnost stanovit.

V předchozí kapitole jsou uvedeny znaky dělitelnosti, které jsou právě jedním způsobem, jak prvočíselnost zjistit. Tímto principem se dané číslo dělí postupně od 2 přes $3, 4, 5$ atd.

Výsledkem mohou být dvě situace. Buď se aplikují znaky dělitelnosti a zadané číslo je složené číslo, pak lze toto číslo rozložit v součin prvočísel, nebo znaky dělitelnosti použít nelze a dané číslo je prvočíslem.

Dalším způsobem zjištění prvočíselnosti je Eratosthenovo síto. Tato metoda je vhodná, pokud zadané číslo nemá velký počet řádů. Jak funguje Eratosthenovo síto, je podrobně vysvětleno v následující kapitole.

- Příklad: Rozhodněte, zda je číslo $x = 4851$ složené číslo či prvočíslo.

  V prvním kroku zkusíme aplikovat znaky dělitelnosti na číslo 4851. Položíme otázku: Je číslo 4851 dělitelné dvěma, třemi, …, jedenácti?

  Poslední číslice zadaného čísla není sudá, tudíž číslo 4851 není dělitelné dvěma zároveň ani čtyřmi, šesti či osmi.

  Dále otestujeme, zda je číslo dělitelné třemi. Ciferný součet je dělitelný třemi, tedy i zadané číslo je dělitelné třemi. Stejně tak je číselný součet dělitelný devíti, tudíž i číslo 4851 je dělitelné devíti.

  Poslední číslice není 0 ani 5, tím pádem ani zadané číslo není dělitelné pěti.

  Zbývá vyšetřit dělitelnost čísla sedmi a jedenácti. Podle kritéria dělitelnosti sedmi, které je uvedeno v kapitole 3.1.6, je číslo 4851 dělitelné sedmi. Obdobně lze podle kritéria dělitelnosti jedenácti také určitě, že zadané číslo je dělitelné jedenácti.

  V závěru lze konstatovat, že $x = 4851$ je složené číslo dle znaků dělitelnosti, které byly použity pro tento příklad.

4.2 ERATOSTHENOVO SÍTO

Základní algoritmus pro zjištění všech prvočísel do námi zvolené horní meze se nazývá Eratosthenovo síto. Tato metoda se jmenuje po známém matematikovi Eratosthenovi, který žil v Kyréně na přelomu 3. a 2. století před naším letopočtem. Tento algoritmus spočívá v tom, že jsou čísla tzv. prosévána, a tím nalezena všechna prvočísla v zadaném intervalu. Postup začíná tak, že se napíšou všechna přirozená čísla od prvočísla 2 do dané zvolené horní meze. Najde se první neškrtnuté číslo, kterým je číslo 2 a vzápětí se škrtnou všechny jeho násobky (tedy čísla 4, 6, …). Obdobně se pokračuje dalšími neškrtnutými čísly

(např. 3, 5, 7, …) a jejich násobky. Postupuje se dál, dokud se nedojde k poslednímu číslu horní meze zvoleného intervalu (Vojáček, 2019).

Metoda Eratosthenova síta bude ukázána na vzorovém příkladu.

- Příklad: Najděte všechna prvočísla do $n = 100$ pomocí Eratosthenova síta.

  Žlutou barvou označíme první nejmenší číslo v tabulce, kterým je číslo 2, a všechny jeho násobky přeškrtneme. Poté označíme další nejmenší nepřeškrtnuté číslo 3 a ze zbylých čísel opět přeškrtneme jeho násobky. Stejně tak postupujeme i s číslem 5, číslem 7. Po vyškrtání těchto čísel a jejich násobků zůstávají v tabulce pouze čísla, jejichž násobky jsou přeškrtnuté. Zbylá čísla opět označíme žlutou barvou.

  Z toho vyplývá, že všechna prvočísla do $n = 100$ jsou v Tabulce 3 zvýrazněna výplní celé buňky.

  Tabulka 3: Zjištění prvočísel pomocí Eratosthenova síta

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

4.3 ROZKLAD PRVKU V SOUČIN IREDUCIBILNÍCH PRVKŮ

Prvočísla se uplatňují při rozkladu složeného čísla v součin prvočinitelů. Jedná se o základní větu a říká se, že složené číslo rozkládáme v součin ireducibilních prvků nebo také hovoří se o prvočíselném rozkladu.

Věta: Každé složené číslo lze zapsat ve tvaru $a = p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_n^{r_n}$, kde $p_1, p_2, \ldots, p_n$ jsou prvočísla a $r_1, r_2, \ldots, r_n$ jsou přirozená čísla. Řekneme, že jsme provedli ***rozklad složeného čísla v součin ireducibilních prvků***.

Metoda prvočíselného rozkladu funguje na základě postupného dělení prvočísel tedy, že každé číslo je děleno vždy nejmenším možným prvočíslem (Polák, 2005).

Mezi ***základní vlastností prvočísel*** je řazena skutečnost, že číslo p není možné rozložit v součin dvou prvků. Pokud dané číslo nelze už dále rozložit, je zřejmé, že se jedná o prvočíslo. Nastávají dvě možnosti, jak to zjistit. Mějme číslo $x = p \cdot a$. Vezmeme-li prvek a z rozkladu $x = p \cdot a$ pak,

1. číslo a je jednotkou,
    - Příklad:

      $7 = 7 \cdot 1$
2. nebo číslo a je asociované s číslem x.
    - Příklad:

      $-225 = 15 \cdot (-15)$

Pro prvočíselný rozklad se též používá věta, která se nazývá ***věta o existenci rozkladu čísel v součin prvočísel***, která je formulována následující způsobem.

Věta: Každé přirozené číslo $a > 1$ lze formulovat, jako součin konečného počtu prvočísel tzn., lze zapsat ve tvaru $a = p_1 \cdot p_2 \cdot \ldots \cdot p_n$.

Prvočíselný rozklad je možné počítat a zapisovat několika způsoby. Jedná se o metodu, kdy se hledají nejmenší možná prvočísla, která dělí složené číslo. Pomocí ilustračních příkladů budou uvedeny 3 způsoby zápisu, které se učí na základní škole.

4.3.1 GRAFICKÁ METODA

Grafická metoda je jednou z nejpřehlednějších, ale zároveň jednou z nejpracnějších metod prvočíselného rozkladu. Nejprve se zapíše složené číslo (x) a hledá se nejmenší možný prvočíselný dělitel (a) čísla x. Když se nalezne číslo a, pak se číslem a vydělí číslo x a získá se číslo (b). Tento rozklad se zapíše tak, že pod číslo x se dají dvě čáry, každá z nich vede k jednomu z čísel a a b. Čáry značí daný součin čísel a a b. V dalším kroku se stejným

způsobem rozkládá číslo b. Takto se pokračuje, dokud nezbydou pouze prvočísla. Tato prvočísla se vynásobí a získá se prvočíselný rozklad složeného čísla (Rais, 2011).

- Příklad: Určete prvočíselný rozklad čísla 36 pomocí grafické metody.

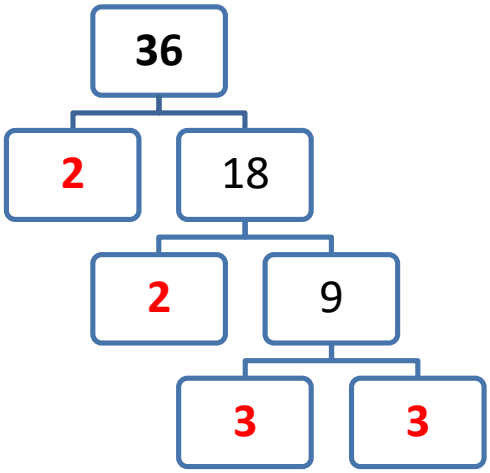

Schéma 1: Grafická metoda prvočíselného rozkladu

Schéma 1 představuje prvočíselný rozklad. Červenou barvou jsou vyznačena prvočísla, která tvoří prvočíselný rozklad. Prvočíselný rozklad čísla 36 je $2 \cdot 2 \cdot 3 \cdot 3$.

4.3.2 TABULKOVÁ METODA

Při použití tabulkové metody se vytvoří tabulka se dvěma sloupci a $n + 1$ řádky, kde n je počet všech možných prvočísel, na které lze složené číslo x rozložit. Do prvního sloupce na první řádek se zapíše číslo (x) a nalezne se nejmenší možné prvočíslo (a), kterým lze dělit číslo x beze zbytku. Vydělením čísla x číslem a se nalezne číslo (b). Číslo a se zapíše do druhého sloupce na první řádek a číslo b na druhý řádek do prvního sloupce. Stejným postupem se pokračuje tak dlouho, dokud se neobjeví v prvním sloupci na posledním řádku číslo 1 a v pravém sloupci prázdné pole. V pravém sloupci se nalezne prvočíselný rozklad složeného čísla x (Rais, 2011).

Tabulková metoda bude ukázána v dalším příkladu pomocí Tabulky 4.

- Příklad: Určete prvočíselný rozklad čísla 276 pomocí tabulkové metody.

Tabulka 4: Tabulková metoda prvočíselného rozkladu

276	**2**
138	**2**
69	**3**
23	**23**
1	

Prvočíselný rozklad čísla 276 představuje součin $2 \cdot 2 \cdot 3 \cdot 23$.

4.3.3 ŘÁDKOVÁ METODA

Metoda spočívá v tom, že se do řádku zapíše složené číslo, které se rozkládá. Složené číslo (x) se vydělí nejmenším možným prvočíslem (a) tak, aby výsledek byl beze zbytku. Vydělením složeného čísla se získá druhý činitel rozkladu (b). První rozklad za rovnítkem je tedy tvořen součinem čísel a a b. Tímto postupem se pokračuje do té doby, dokud se nedojde k rozkladu v součin prvočísel (Rais, 2011).

- Příklad: Určete prvočíselný rozklad čísla 64 pomocí řádkové metody.

  $64 = 2 \cdot 32 = 2 \cdot 2 \cdot 16 = 2 \cdot 2 \cdot 2 \cdot 8 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 4 = \underline{\mathbf{2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2}}$

  Rozklad čísla 64 je tvořen součinem $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2$.

4.4 CELÁ ČÍSLA

V případě oboru integrity celých čísel se vychází ze základní definice prvočísla. Z toho plyne, že prvočíslo z oboru Z je číslo dělitelné samo sebou, jedničkou a v neposlední řadě je také ireducibilním prvkem.

Jak je známo, prvočísel je nekonečně mnoho. Pro zajímavost nejdelší známé prvočíslo má 44 cifer, má hodnotu $20988936657440586486151264256610222593863921$. Bylo objeveno roku 1951 Francouzem Aimém Ferrierem (Šplíchal, 2018).

Pomocí Tabulky 5 jsou uvedena první prvočísla do čísla 100.

Tabulka 5: Příklady prvočísel do 100

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

4.5 GAUSSOVA CELÁ ČÍSLA

Co se týče oboru integrity Gaussových celých čísel $(G,\ +,\ \cdot)$, víme, že pro ireducibilní prvek platí $r = a \cdot b$, tudíž vychází pouze možnosti $r \sim a$ nebo $a = j$, kde j je jednotka oboru integrity. V případě, že $a = j$, potom nastává $r \sim b$.

Definice: Prvek r oboru integrity $(I,\ +,\ \cdot)$ nazýváme ***ireducibilním prvkem*** tohoto oboru integrity právě tehdy, když platí $r = a \cdot b \Rightarrow r \sim a\ \vee r \sim b$.

V Gaussově celočíselné oboru je každý ireducibilní prvek prvočinitelem. Tyto prvočinitele představují Gaussova prvočísla.

Definice: Nechť α je ***Gaussovo prvočíslo***, které neleží v Z. Pak i $\overline{\alpha}$ je Gaussovo prvočíslo a $\alpha \cdot \overline{\alpha}$ je prvočíselný rozklad $N(\alpha)$ v $Z[i]$, kde $N(\alpha)$ je norma Gaussova čísla. Gaussova prvočísla, která neleží v Z, jsou ve tvaru $a + bi$, kde $a, b \in Z$ a $a^2 + b^2$ je prvočíslo. Je – li nějaké prvočíslo v Z ve tvaru $a^2 + b^2$, pak $\alpha = a + bi$ a $\overline{\alpha} = a - bi$ jsou prvočísla.

Věta: Gaussovo prvočíslo v oboru integrity $(G,\ +,\ \cdot)$ je nenulové Gaussovo celé číslo, které je různé ode všech jednotek tohoto oboru integrity, tj. $(1, -1, i, -i)$.

Věta: Celočíselné prvočíslo p je Gaussovo prvočíslo, právě tehdy když $p \equiv 3\ mod\ 4$ (Gaussova prvočísla, 2019).

4.6 POLYNOMY

Pro ireducibilními prvky z hlediska polynomů je v první řadě nutné zformulovat pojem primitivní polynom. Následně je možné vysvětlit ireducibilní prvky v oboru integrity polynomů.

Definice: Polynom $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0, a_n \neq 0$ nazýváme ***primitivním polynomem*** nad oborem integrity $(T[x], +, \cdot)$ právě tehdy, když jeho koeficienty představují nesoudělná čísla.

Gaussova věta platí pro libovolné primitivní polynomy.

Věta: Jestliže vynásobíme dva primitivní polynomy, pak dostáváme opět primitivní polynom.

Dále je známo, že každý neprimitivní polynom, který má nejméně první stupeň, je polynom reducibilní. Tento fakt lze jednoduše dokázat.

- Důkaz: Mějme polynom $f(x) = a \cdot g(x)$, kde $|a| = 1$ a $g(x)$ představuje primitivní polynom. Prvky a a $g(x)$ prezentují vlastní dělitele polynomu $f(x)$.

Z důkazu plyne, že ireducibilní prvky se nachází v oboru I a v množině primitivních polynomů. Nyní je možné zavést pojem ireducibilního prvku v oboru integrity polynomů.

Věta: Ireducibilní prvky v oboru integrity $(T[x], +, \cdot)$ jsou:

a) všechna prvočísla z oboru integrity celých čísel,

b) všechny primitivní polynomy stupně alespoň prvního z oboru integrity $(T[x], +, \cdot)$, které jsou ireducibilními polynomy nad oborem integrity $(Q(x), +, \cdot)$.

Typickým příkladem ireducibilního polynomu je polynom $f(x) = x^2 + 1$. Polynom $f(x)$ je ireducibilní, protože v množině racionálních čísel ho už nelze dále rozložit v součin ireducibilních prvků. Koeficienty by se nacházely v množině komplexních čísel.

5 SPOLEČNÝ DĚLITEL

Tato kapitola je věnována společnému děliteli prvků, který je nedílnou součástí teorie dělitelnosti. Společný dělitel dvou prvků je vyučován již na druhém stupni základních škol, a proto je nutné se u tohoto tématu na chvíli pozastavit.

Definice: Mějme libovolné prvky $a_1, a_2, \dots, a_n$ z I. ***Společným dělitelem*** prvků nazýváme číslo $d \in I$ právě tehdy, když $d|a_1, d|a_2, \dots, d|a_n$.

Definice: Nechť $a_1, \dots, a_n \in I$. Prvek $D \in I$ se nazývá ***největší společný dělitel*** prvků $a_1, \dots, a_n$ právě tehdy, když platí:

1. $D|a_1 \wedge D|a_2 \wedge \dots \wedge D|a_n$,
2. $\forall d \in I: (d|a_1 \wedge d|a_2 \wedge \dots \wedge d|a_n) \Rightarrow d|D$.

Značíme: $D(a_1, \dots, a_n)$ nebo jen D. Číslo D je největším společným dělitelem prvků $a_1, \dots, a_n$ právě tehdy, když číslo d je společný dělitel prvků a zároveň když každý společný dělitel d je také dělitelem čísla D.

Poznámka: Největším společným dělitelem přirozených čísel a, b rozumíme číslo $Max\ d(a, b)$. Dále platí $d(a, b) = d(a) \cap d(b)$ (Drábek, 1985).

Největší společný dělitel dvou a více prvků se klasicky nejjednodušeji určuje pomocí Euklidova algoritmu, který je uveden v podkapitole věnované tomuto algoritmu.

5.1 VĚTY O SPOLEČNÝCH DĚLITELÍCH

V následující podkapitole jsou zformulovány základní věty, které platí pro společného dělitele čísel a aplikace vět na jednoduchých příkladech.

Věta 1: Jestliže je číslo d společným dělitelem čísel $a, b \in I$, pak je také dělitelem čísla $k_1a + k_2b$, kde k_1, k_2 jsou libovolná čísla a pro $k_1a > k_2b$je dělitelem $k_1a - k_2b$.

Jinak řečeno, jestliže je číslo d dělitelem čísel $a, b \in I$, pak je číslo d dělitelem i součtu a rozdílu násobku čísel a a b vzhledem k číslům k_1 a k_2, pro $a > b$.

- Příklad: Mějme čísla $a = 15$, $b = 6$, $k_1 = 4$ a $k_2 = 7$. Určete $d(a, b)$, dále ověřte, že součet $k_1a + k_2b$ a rozdíl $k_1a - k_2b$ je též dělitelný číslem $d(a, b)$.

  Provedeme rozklad na prvočinitele čísel a a b.

$a = 15 = \boxed{3} \cdot 5$

$b = 6 = 2 \cdot \boxed{3}$

Společný dělitel čísel a a b je číslo $d = 3$.

Ověříme, že číslo $d = 3$ dělí i součet $k_1 a + k_2 b$ a rozdíl $k_1 a - k_2 b$.

SOUČET: $\boldsymbol{k_1 a + k_2 b}$

$4 \cdot 15 + 7 \cdot 6 = 102$

$102 \div 3 = \underline{\underline{34}}$

ROZDÍL: $\boldsymbol{k_1 a - k_2 b}$

$4 \cdot 15 - 7 \cdot 6 = 18$

$18 \div 3 = \underline{\underline{6}}$

Ověřili jsme, že $d = 3$ je společným dělitelem a a b a dělí i součet $k_1 a + b$ a rozdíl $k_1 a - k_2 b$.

Věta 2: Jestliže jsou $a, b \in I$ a *d* je společným dělitelem čísel $a, a + b, a - b$, pro $a > b$, pak je také dělitelem čísla b.

- Příklad: Mějme čísla $a = 30,\ b = 5$. Určete $d(a, b)$, součet a rozdíl prvků a a b.

  $a = 30 = 2 \cdot 3 \cdot \boxed{5}$

  $b = \boxed{5}$

  Společným dělitelem je číslo $d = 5$.

  SOUČET: $\boldsymbol{a + b}$

  $a + b = 30 + 5 = 35$

  $35 \div 5 = \underline{\underline{7}}$

  ROZDÍL: $\boldsymbol{a - b}$

  $a - b = 30 - 5 = 25$

  $25 \div 5 = \underline{\underline{5}}$

  $b = 5$

  $5 \div 5 = \underline{\underline{1}}$

Číslo $d = 5$ je společným dělitelem a jestliže dělí $a, a + b\ a - b$, pak dělí i číslo b.

Věta 3: Jestliže je číslo *d* dělitelem alespoň jednoho z čísel $a, b \in I$, tzn. $d|a \vee d|b$, potom je také dělitelem jejich součinu $a \cdot b$.

- Příklad: Máme čísla $a = 78$ a $b = 325$. Určete $d(a, b)$, součin prvků a a b.

  $a = 78 = 2 \cdot 3 \cdot \boxed{13}$

$b = 325 = 5 \cdot 5 \cdot \boxed{13}$

Společným dělitelem je číslo $d = 13$.

$a \cdot b = 78 \cdot 325 = 25350$

$25350 \div 13 = \underline{\underline{1950}}$

Číslo $d = 13$ je dělitelem alespoň jednoho z prvků a a b, pak tedy platí, že je dělitel i součinu prvků a a b.

Věta 4: Jestliže je číslo d společným dělitelem čísel $a, b \in I$, pak je součin těchto čísel dělitelný číslem d^2.

- Příklad: Uvažujme čísla $a = 14$ a $b = 63$. Určete $d(a, b)$, součin prvků a a b, dále ověřte, že součin je dělitelný společným dělitelem umocněným na druhou.

  $a = 14 = 2 \cdot \boxed{7}$

  $b = 63 = 3 \cdot 3 \cdot \boxed{7}$

  Společný dělitel je $d = 7$.

  Společný dělitel umocněný na druhou: $d^2 = 7^2 = 49$

  $a \cdot b = 14 \cdot 63 = 882$

  $882 \div 49 = \underline{\underline{18}}$

  Společný dělitel čísel a a b umocněný na druhou je též dělitelem jejich součinu.

Věta 5: Největší společný dělitel $D(a, b)$ má ve svém prvočíselném rozkladu všechny společné prvočinitele rozkladů čísel a a b s nejmenším mocnitelem, který se v těchto rozkladech vyskytuje (Polák, 2005).

- Příklad: Určete největšího společného dělitele čísel $a = 36$ a $b = 276$.

  V první řadě provedeme prvočíselný rozklad čísel a a b a vybereme shodnou část z obou rozkladů.

  $a = 36 = \boxed{2 \cdot 2 \cdot 3} \cdot 3$

  $b = 276 = \boxed{2 \cdot 2 \cdot 3} \cdot 23$

  $D = 2 \cdot 2 \cdot 3 = \underline{\underline{12}}$

  Největší společný dělitel čísel 36 a 276 je číslo 12.

Se společným dělitelem čísel je úzce spjat pojem soudělnosti prvku. Platí pro n následující definice.

Definice: Čísla $a_1, a_2, \dots, a_n$, která mají alespoň jednoho společného dělitele $d > 1$, se nazývají ***soudělná čísla***. Jestliže nemají čísla $a_1, a_2, \dots, a_n$ žádného společného dělitele $d > 1$ tzn., že $D(a_1, a_2, \dots, a_n) = 1$, se nazývají ***nesoudělná čísla***.

- Příklad: Mějme čísla $a = 13$ a $b = 21$. Rozhodněte, zda jsou čísla soudělná či nesoudělná.

  Nejprve určíme největší společný dělitel čísel a, b.

  $13 = 13 \cdot 1$

  $21 = 21 \cdot 1$

  $D(13{,}21) = 1$

  Čísla 13 a 21 jsou čísla nesoudělná, protože $D(13{,}21) = 1$.

- Příklad: Mějme čísla $a = 54$ a $b = 92$. Rozhodněte, zda jsou čísla soudělná či nesoudělná.

  $54 = 2 \cdot 3 \cdot 3 \cdot 3$
  $92 = 2 \cdot 2 \cdot 23$

  $D(54{,}92) = 2$

  Čísla 54 a 92 jsou čísla soudělná, jelikož $D(54{,}92) = 2$.

Jak je výše uvedeno, k určení největšího společného dělitele se používá spíše Euklidův algoritmus, který je důkladněji popsán v následující kapitole.

5.2 NEJVĚTŠÍ SPOLEČNÝ DĚLITEL - EUKLIDŮV ALGORITMUS

Jedná se o postup, kterým se zjišťuje největšího společného dělitele dvou a více čísel. Euklidův algoritmus lze využít v různých oborech integrity. V našem případě se podíváme, jak tento princip funguje z hlediska celých čísel, Gaussových celých čísel a polynomů.

Euklidův algoritmus: Mějme dva nenulové prvky a a b z Euklidova oboru integrity ***I***, $a > b$. Dále víme, že v ***I*** existují prvky $\eta_0, \eta_1, \dots, \eta_n, r_1, r_2, \dots, r_n$ takové, že $r_n = D(a, b)$ a platí pro ně:

$$
\begin{aligned}
a &= b \cdot \eta_0 + r_1 & N(r_1) &< N(b) \\
b &= r \cdot \eta_1 + r_2 & N(r_2) &< N(r_1) \\
r_1 &= d_2 \cdot \eta_2 + r_3 & N(r_3) &< N(r_2) \\
&\vdots & &\vdots \\
r_{i-1} &= r_i \cdot \eta_i + r_{i+1} & N(r_{i+1}) &< N(r_i) \\
&\vdots & &\vdots \\
r_{n-2} &= r_{n-1} \cdot \eta_{n-1} + \boxed{r_n} & N(r_n) &< N(r_{n-1}) \\
r_{n-1} &= r_n \cdot \eta_n + 0
\end{aligned}
$$

(Hefler, 2013).

Algoritmus začínáme tak, že nejprve dělíme větší číslo a menším číslem b, dále pokračujeme dělením menšího čísla b zbytkem prvního dělení r_1, stejným postupem pokračujeme do té doby, než dostaneme zbytek po dělení nula. Největším společným dělitelem čísel a a b je pak poslední nenulový zbytek po dělení, tedy číslo r_n.

5.2.1 CELÁ ČÍSLA

V další části je ukázáno několik názorných příkladů na počítání největšího společného dělitele pomocí Euklidova algoritmu. Jak je vidět ve výše uvedeném názvu podkapitoly jako obor integrity je zvolen obor celých čísel. Tento postup je používán zejména při zjišťování největšího společného dělitele čísel s větším počtem řádů.

- Příklad: Zjistěte největšího společného dělitele čísel $a = 638$ a $b = 451$ pomocí Euklidova algoritmu, $D = (638, 451)$?

  $638 = 1 \cdot 451 + 187$
  $451 = 2 \cdot 187 + 77$
  $187 = 2 \cdot 77 + 33$
  $77 = 2 \cdot 33 + \boxed{11}$
  $33 = 3 \cdot 11 + 0$

  $\underline{D(638{,}451) = 11}$

  Posledním nenulový zbytkem je číslo 11, které je tedy největším společným dělitelem čísel 638 a 451.

- Příklad: Vypočítejte největšího společného dělitele čísel $a = 5376$ a $b = 621$.

$$5376 = 8 \cdot 621 + 408$$
$$621 = 1 \cdot 408 + 213$$
$$408 = 1 \cdot 213 + 195$$
$$213 = 1 \cdot 195 + 18$$
$$195 = 10 \cdot 18 + 15$$
$$18 = 1 \cdot 15 + \boxed{3}$$
$$15 = 5 \cdot 3 + 0$$

$$\underline{D(5376,621) = 3}$$

Největším společným dělitelem čísel *a* a *b* je číslo 3.

- Příklad: Pomocí Euklidova algoritmu vypočítejte $D(572169, 349852)$.

$$572169 = 1 \cdot 349852 + 222317$$
$$349852 = 1 \cdot 222317 + 127535$$
$$222317 = 1 \cdot 127535 + 94782$$
$$127535 = 1 \cdot 94782 + 32753$$
$$94782 = 2 \cdot 32753 + 29276$$
$$32753 = 1 \cdot 29276 + 3477$$
$$29276 = 8 \cdot 3477 + 1460$$
$$3477 = 2 \cdot 1460 + 557$$
$$1460 = 2 \cdot 557 + 346$$
$$346 = 1 \cdot 211 + 135$$
$$211 = 1 \cdot 135 + 75$$
$$135 = 1 \cdot 75 + 60$$
$$75 = 1 \cdot 60 + \boxed{15}$$
$$60 = 4 \cdot 15 + 0$$

$$\underline{D(572169, 349852) = 15}$$

Číslo 15 je největší společný dělitel.

5.2.2 GAUSSOVA CELÁ ČÍSLA

Stejně jako v oboru celých čísel, tak i v oboru Gaussových celých číslech bude uplatněn Euklidův algoritmus k výpočtu největšího společného dělitele dvou čísel.

- Příklad: Pomocí Euklidova algoritmu nalezněte $D(\alpha,\beta)$, jestliže jsou čísla zadaná takto: $\alpha = 5+5i$, $\beta = 3-4i$.

  Nejprve zjistíme, jaký je podíl α a β.

  $$\frac{\alpha}{\beta} = \frac{5+5i}{3-4i} = \frac{(5+5i)\cdot(3+4i)}{(3-4i)\cdot(3+4i)} = \frac{-5+35i}{25} = \underbrace{-\frac{1}{5}}_{A} + \underbrace{\frac{7}{5}}_{B}i$$

  Zvolíme $A = -\frac{1}{5}$, $B = \frac{7}{5}i$.

  Nyní učíme číslo $\eta = a + bi$. Čísla a a b zvolíme jako nejbližší nejmenší možná celá čísla k číslům *A* a *B*, tudíž $a = 0$, $b = 1$. Odtud dostáváme $\eta = i$.

  Dále stavíme číslo $\upsilon = \alpha - \beta\cdot\eta$.

  $$\upsilon = (5+5i) - i\cdot(3-4i) = 5+5i-3i+4i^2 = \underline{\underline{1+2i}}$$

  Dostáváme první řádek Euklidova algoritmu: $5+5i = (3-4i)\cdot i + (1+2i)$.

  Provedeme zkoušku:

  $$L = 5+5i$$
  $$P = i\cdot(3-4i) + (1+2i) = 3i - 4i^2 + 1 + 2i = 5+5i$$
  $$\underline{\underline{L = P}}$$

  Zkouška vyšla a pokračujeme druhým řádkem Euklidova algoritmu.

  $$\alpha = 3-4i,\ \beta = 1+2i$$

  $$\frac{\alpha}{\beta} = \frac{3-4i}{1+2i} = \frac{(3-4i)\cdot(1-2i)}{(1+2i)\cdot(1-2i)} = \frac{-5-10i}{5} = \underline{\underline{-1-2i}}$$

  $$3-4i = (1+2i)\cdot(-1-2i) = 3-4i+0$$

  Odtud rovnou vidíme, že $L = P$ a nemusíme provádět zkoušku.

  V posledním kroku sestavíme ještě jednou celý Euklidův algoritmus a určíme největšího společného dělitele.

(1) $5 + 5i = (3 - 4i) \cdot i + \underline{(1 + 2i)}$

(2) $3 - 4i = (1 + 2i) \cdot (-1 - 2i) + 0$

Největším společným dělitelem čísel α a β je číslo $D(5 + 5i, 3 - 4i) = 1 + 2i$.

5.2.3 POLYNOMY

Na závěr této kapitoly zbývají příklady z oboru integrity polynomů a aplikujeme na něj opět Euklidův algoritmus. Zadání příkladů jsem převzala ze skript *Algebra: Polynomy a rovnice*.

- Příklad: Vypočítejte největšího společného dělitele polynomů $f(x)$ a $g(x)$, jestliže jsou polynomy zadány takto: $f(x) = x^4 - 2x^2 + 1,\ g(x) = x^3 + 3x^2 - x - 3$ (Drábek, 2001).

  V prvním kroku budeme dělit polynom $f(x)$ polynomem $g(x)$.

  $x^4 - 2x^2 + 1 = \eta_1 \cdot (x^3 + 3x^2 - x - 3) + r_1$

  $(x^4 - 2x^2 + 1) \div (x^3 + 3x^2 - x - 3) = \underline{\underline{x - 3}}$

  $\underline{-(x^4 + 3x^3 - x^2 - 3x)}$

  $-3x^3 - x^2 + 3x + 1$

  $\underline{-(-3x^3 - 9x^2 + 3x + 9)}$

  $\underline{\underline{8x^2 - 8}}$

  Z prvního dělení dostáváme $\eta_1 = x - 3$ a zbytek $r_1 = 8x^2 - 8$.

  Provedeme zkoušku, zda se rovná pravá a levá strana rovnice.

  $L = x^4 - 2x^2 + 1$

  $P = (x - 3) \cdot (x^3 + 3x^2 - x - 3) + (\ 8x^2 - 8) =$

  $= x^4 + 3x^3 - x^2 - 3x - 3x^3 - 9x^2 + 3x + 9 + 8x^2 - 8 = x^4 - 2x^2 + 1$

  $\underline{\underline{L = P}}$

  Vzhledem k tomu, že nám zkouška vyšla, tak jsme získali první řádek Euklidova algoritmu. Nyní pokračujeme dále v počítání. Pro lepší počítání si upravíme zbytek $r_1 = 8x^2 - 8$ na asociovaný polynom $r_1' = x^2 - 1$.

  $x^3 + 3x^2 - x - 3 = \eta_2 \cdot (x^2 - 1) + r_2$

$(x^3 + 3x^2 - x - 3) \div (x^2 - 1) = \underline{\underline{x + 3}}$

$\underline{-(x^3 - x)}$

$3x^2 - 3$

$\underline{-(3x^2 - 3)}$

$\underline{\underline{0}}$

Z druhého dělení dostáváme $\eta_2 = x + 3$ a zbytek $r_2 = 0$.

Opět spočítáme pro kontrolu zkoušku.

$L = x^3 + 3x^2 - x - 3$
$P = (x + 3) \cdot (x^2 - 1) + 0 = x^3 + 3x^2 - x - 3$
$\underline{\underline{L = P}}$

Zkouška vyšla a teď už můžeme zapsat znovu celý Euklidův algoritmus pro lepší přehled.

(1) $x^4 - 2x^2 + 1 = (x - 3) \cdot (x^3 + 3x^2 - x - 3) + \underline{\underline{(x^2 - 1)}}$

(2) $x^3 + 3x^2 - x - 3 = (x + 3) \cdot (x^2 - 1) + 0$

Teď už lze jednoznačně určit největší společný dělitel polynomů $f(x)$ a $g(x)$, kterým je polynom $D(x^4 - 2x^2 + 1,\ x^3 + 3x^2 - x - 3) = \underline{\underline{x^2 - 1}}$.

- Příklad: Vypočítejte největšího společného dělitele polynomů $f(x)$ a $g(x)$, které jsou dány takto: $f(x) = x^4 + x^3 + x^2 - x - 2,\ \ g(x) = x^3 + 6x^2 + 7x + 10$ (Drábek, 2001).

$x^4 + x^3 + x^2 - x - 2 = \eta_1 \cdot (x^3 + 6x^2 + 7x + 10) + r_1$

$(x^4 + x^3 + x^2 - x - 2) \div (x^3 + 6x^2 + 7x + 10) = \underline{\underline{x - 5}}$

$\underline{-(x^4 + 6x^3 + 7x^2 + 10x)}$

$-5x^3 - 6x^2 - 11x - 2$

$\underline{-(-5x^3 - 30x^2 - 35x - 50}$

$\underline{\underline{24x^2 + 24x + 48}}$

Po prvním dělení dostáváme $\eta_1 = x - 5$ a $r_{1=}\ 24x^2 + 24x + 48$.

Zkouška:

$$L = x^4 + x^3 + x^2 - x - 2$$
$$P = (x-5)\cdot(x^3 + 6x^2 + 7x + 10) + 24x^2 + 24x + 48 =$$
$$= x^4 + 6x^3 + 7x^2 + 10x - 5x^3 - 30x^2 - 35x - 50 + 24x^2 + 24x + 48 =$$
$$= x^4 + x^3 + x^2 - x - 2$$

$\underline{\underline{L = P}}$

Polynom $r_{1=}\ 24x^2 + 24x + 48$ vydělíme 24 a dostaneme polynom $r_1' = x^2 + x + 2$.

$$x^3 + 6x^2 + 7x + 10 = \eta_2 \cdot (x^2 + x + 2) + r_2$$

$$(x^3 + 6x^2 + 7x + 10) \div (x^2 + x + 2) = \underline{\underline{x + 5}}$$

$$\underline{-(x^3 + x^2 + 2x)}$$

$$5x^2 + 5x + 10$$

$$\underline{-(5x^2 + 5x + 10)}$$

$$\underline{\underline{0}}$$

Získali jsme $\eta_2 = x + 5$ a $r_2 = 0$.

Zkouška:

$$L = x^3 + 6x^2 + 7x + 10$$
$$P = (x+5)\cdot(x^2 + x + 2) = x^3 + x^2 + 2x + 5x^2 + 5x + 10 =$$
$$= x^3 + 6x^2 + 7x + 10$$

$\underline{\underline{L = P}}$

Euklidův algoritmus:

(1) $x^4 + x^3 + x^2 - x - 2 = (x-5)\cdot(x^3 + 6x^2 + 7x + 10) + (\underline{24x^2 + 24x + 48})$

(2) $x^3 + 6x^2 + 7x + 10 = (x+5)\cdot(x^2 + x + 2) + 0$

Největším společným dělitelem polynomů $f(x)$ a $g(x)$ je polynom

$D(x^4 + x^3 + x^2 - x - 2,\ x^3 + 6x^2 + 7x + 10) = \underline{\underline{x^2 + x + 2}}$.

6 SPOLEČNÝ NÁSOBEK

Nejmenší společný násobek se vyučuje spolu s největším společným dělitelem

Jak je uvedeno v předchozí kapitole, největší společný dělitel prvků je obecně brán jako $Max\ D(a,b)$. Naopak nejmenší společný násobek je obecně brán jako $Min\ N(a,b)$.

Definice: Jsou-li prvky $a_1, a_2, \dots, a_n$ libovolné prvky z I, prvek $n \in I$ se nazývá ***společný násobek prvků*** $a_1, a_2, \dots, a_n$, jestliže platí: $a_1|n \wedge a_2|n \wedge \dots \wedge a_n|n$. Značíme $N(a_1, a_2, \dots, a_n)$.

Definice: Nechť $a_1, a_2, \dots, a_n \in I$. Prvek $N \in I$ se nazývá ***nejmenší společný násobek prvků*** $a_1, a_2, \dots, a_n$ právě tehdy, když platí:

1. $a_1|N \wedge a_2|N \wedge \dots \wedge a_n|N$,
2. $\forall n \in I: (a_1|n \wedge a_2|n \wedge \dots \wedge a_n|n) \Rightarrow N|n$.

To znamená, že číslo N je nejmenší společný násobek prvků $a_1, a_2, \dots, a_n$ právě tehdy, když číslo x je společný násobek všech prvků $a_1, a_2, \dots, a_n$ a zároveň každý společný násobek n těchto prvků je násobkem prvku N. Značíme $x = n(a_1, a_2, \dots, a_n)$.

Věta: Nechť v oboru integrity I k libovolným dvěma prvkům existuje největší společný dělitel. Pak existuje v I i nejmenší společný násobek k libovolné konečné množině prvků z I. Platí $n = (a \cdot b) \div D = (a \div D) \cdot b = a \cdot (b \div D)$.

Výpočet nejmenšího společného násobku je jednoduchý. Při výpočtu se používá prvočíselný rozklad. Každé z čísel se rozloží v součin prvočísel, vybere se každý prvek s největší mocninou ze součinu. Nejmenší společný násobek je roven součinu všech vybraných prvočísel ze všech rozkladů v součin prvočísel. Zjištění nejmenšího společného násobku se názorně ukáže ilustračním příkladem.

- Příklad: Mějme čísla $a = 64$ a $b = 235$. Nalezněte nejmenší společný násobek čísel a a b.

  Nejprve provedeme prvočíselný rozklad.

  $64 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = \boxed{2^6}$

  $235 = \boxed{5 \cdot 47}$

V závěru provedeme součin prvočísel.

$n(64{,}235) = 2^6 \cdot 5 \cdot 47 = \underline{15040}$

Nejmenší společný násobek čísel 64 a 235 je 15040.

ZÁVĚR

V úvodu práce byl zvolen motivační úkol, který je zde vyřešen. K rozhodnutí o tom, zda je zadané číslo 13567 prvočíslem slouží několik způsobů. Jaký způsob je vhodný použít závisí na počtu řádů zadaného čísla.

Pokud se někomu zadá příklad na rozklad prvočísel, pravděpodobně jako první metodu použije znaky dělitelnosti. Kritéria pro použití této metody jsou podrobně rozebrána v kapitole 3.1 Znaky dělitelnosti na množině Z. Jedná se o základní kritéria znaků dělitelnosti pro čísla od 2 do 11. Aplikují-li se na číslo 13567, dojde se k závěru, že tímto způsobem prvočíselnost tohoto čísla nelze stanovit. Dalo by se pokračovat dalšími kritérii pro čísla větší než 11, avšak tato kritéria se běžně nepoužívají, protože jsou početně náročná.

Druhým způsobem zjištění prvočíselnosti daného čísla je Eratosthenovo síto. Tento způsob se dá efektivně využít v případě, že zadané číslo nebude mít velký počet řádů. V opačném případě by tabulka Eratosthenova síta byla velmi obsáhlá, tudíž by metoda zjištění prvočíselnosti byla početně náročná a velmi zdlouhavá. Tento způsob se dá snadno použít pro čísla do 3 řádů, např. pro číslo 396. V tomto případě by výsledek byl $2 \cdot 2 \cdot 3 \cdot 3 \cdot 11$. V případě čísla 13567 je metoda Eratosthenova síta tedy také neefektivní.

Dvě výše zmíněné metody se vyučují na základní škole a jsou součástí obsahu této práce. Dalším možným způsobem řešení, který je však nad rámec této práce, je počítačový algoritmus. Tato metoda se využívá, pokud pomocí přechozích dvou metod nelze stanovit prvočíselnost. Jedná se o počítačové programy k tomu určené.

Metody pro zjištění prvočíselnosti byly aplikovány na číslo 13567. Pomocí první a druhé metody nebylo dosaženo kladného výsledku. Naopak pomocí počítačového algoritmu lze zjistit, že zadané číslo 13567 je prvočíslo. Existují tabulky prvočísel, podle kterých je možné ověřit prvočíselnost zvoleného čísla.

Bakalářská práce na téma „Dělitelnost v různých oborech integrity“ se zabývala relací dělitelnosti v oboru integrity celých čísel, Gaussových celých čísel a polynomů. Byly vysvětleny základní prvky oboru integrity a zavedeny znaky dělitelnosti.

Další část práce byla věnována ireducibilním prvkům a prvočíslům. Součástí této problematiky je rozklad složeného čísla v součin prvočinitelů, který se vysvětluje třemi možnými způsoby zápisu.

V závěru práce byla věnována kapitola největšímu společnému děliteli a nejmenšímu společnému násobku. Tyto dva pojmy jsou jedním z nejdůležitějších uplatnění relace dělitelnosti. Největší společný dělitel se užívá k převodu zlomku na základní tvar nebo při krácení zlomků. Oproti tomu nejmenší společný násobek je nezbytný ke zjištění společného jmenovatele více zlomků.

Cílem práce byla praktická aplikace teoretických poznatků na ukázkových příkladech. Pomocí vlastních příkladů byla zároveň dokázána platnost daných definic a vět, které byly zmíněny.

SHRNUTÍ

Dělitelnost je jedna z důležitých odvětví matematiky. Tato bakalářská práce se věnuje dělitelnosti z pohledu celých čísel, Gaussových celých čísel a polynomů. Práce je členěna do 6 kapitol.

První kapitola popisuje algebraické struktury, vymezuje jednu ze základních algebraických struktur, kterou je obor integrity. Druhá kapitola obsahuje obecnou definice dělitelnosti, dále významné prvky algebraických struktur a následnou aplikaci na vybrané obory integrity z hlediska dělitelnosti. Ve třetí kapitole jsou vymezeny kritéria dělitelnosti, zejména pak znaky dělitelnosti na množině celých čísel. Čtvrtá kapitola pojednává o pojmu ireducibilního prvku a prvočísla. Je zde popsáno, jak se zjistí prvočíselnost daného prvku pomocí znaků dělitelnosti či Eratosthenova síta. Součástí této kapitoly je rozklad prvku v součin ireducibilních prvků. V páté kapitole je popsán společný dělitel prvků a největší společný dělitel prvků. Je zde uveden Euklidův algoritmus, který je vhodným způsobem pro zjišťování největšího společného dělitele. V neposlední řadě šestá kapitola pojednává o společném násobku a nejmenším společným násobku.

RESUMÉ

Divisibility is one of the most important parts of mathematics. This bachelor thesis focuses on divisibility of integers, Gaussian integers and polynomials. The thesis is divided into 6 chapters.

First chapter describes the algebraic structures, defines one of the basic algebraic structures which is the integral domain. Second chapter contains a general definition of divisibility, important elements of algebraic structures and subsequent application to selected integral domains in terms of divisibility. Third chapter defines the divisibility criteria, especially the divisibility characters of integers. Fourth chapter deals with the concept of irreducible element and prime number. It describes, how the primality od specific elements is determined using the divisibility characters of the sieve of Eratosthenes. Part of this chapter is also the decomposition of the element into the product of irreducible elements. Fifth chapter describes the common divisor of elements and the greatest common divisor. In this chapter is presented Euclidean algorithm which is a suitable way to find the greatest common divisor. Finally, the sixth chapter deals with a common multiple and the least common multiple.

SEZNAM LITERATURY

BLAŽEK, Jaroslav, CALDA, Emil a kol. *Algebra a teoretická aritmetika I. díl*. 1. vyd. Praha: Státní pedagogické nakladatelství, 1982.

BLAŽEK, Jaroslav, KOMAN, Milan a VOJTÁSKOVÁ, Blanka. *Algebra a teoretická aritmetika II. díl*. 1. vyd. Praha: Státní pedagogické nakladatelství, 1985.

COUFALOVÁ, Jana. *Základy elementární aritmetiky v 1. ročníku učitelství pro 1. stupeň ZŠ*. 1. vyd. Plzeň: Pedagogická fakulta v Plzni, 1990.

ČERMÁKOVÁ, Petra*. Dělitelnost: modely dělitelnosti v různých soustavách a v Gaussových oborech integrity.* Plzeň, 2006. Bakalářská práce. Západočeská univerzita v Plzni. Vedoucí práce RNDr. Libuše Tesková, CSc.

DRÁBEK, Jaroslav. *Přednášky z KMT/Elementární algebra*. Plzeň. Západočeská univerzita. Fakulta pedagogická.

DRÁBEK, Jaroslav, Križalkovič, Karol a kol. *Základy elementární aritmetiky: pro učitelství 1. stupně ZŠ*. 1. vyd. Praha: státní pedagogické nakladatelství, 1985.

DRÁBEK, Jaroslav & HORA, Jaroslav. *Algebra: Polynomy a rovnice*. 1. vyd. Plzeň: Západočeská univerzita v Plzni, 2001. ISBN 80-7082-787-4.

HEFLER, S. *Příklady na dělitelnost v oborech integrity*. Plzeň, 2013. Bakalářská práce. Západočeská univerzita v Plzni. Vedoucí práce doc. RNDr. Jaroslav Hora, CSc.

PĚCHOUČKOVÁ, Š. *Poznámky k přípravě na výuku předmětu Matematika s didaktikou 2*. Plzeň. Západočeská univerzita. Fakulta pedagogická.

POLÁK, Josef. *Přehled středoškolské matematiky*. 8. vyd. Praha: Prometheus, spol. s. r. o., 2005. ISBN 80-7196-267-8.

PROCHÁZKA, Ladislav a kol. *Algebra*. 1. vyd. Praha: Academia, 1990. ISBN 80-200-301-0.

RAIS, M. *Prvočíselný rozklad a jeho užití.* Plzeň, 2011. Diplomová práce. Západočeská univerzita v Plzni. Vedoucí práce doc. PaedDr. Jana Coufalová, CSc.

ŠPLÍCHAL, Tomáš. *Prvočísla - hledání a využití*. Brno, 2018. Bakalářská práce. Masarykova univerzita. Vedoucí práce RNDr. Karel Lepka Dr.

INTERNETOVÉ ZDROJE

CONRAD, Keith. *Gaussian Integers* [online]. Storrs (Connecticut): University of Connecticut, 34 s. [cit. 2019-03-10]. Dostupné z: https://kconrad.math.uconn.edu/blurbs/ugradnumthy/Zinotes.pdf

DAVIDOVÁ, Eva. *Dělitelnost* [online]. Ostrava: Wichterlovo gymnázium, 10 s. [cit. 2019-04-14]. Dostupné z: http://kdm.karlin.mff.cuni.cz//konference2012/p1.pdf

Gaussova prvočísla [online]. Praha: Karlova univerzita, 2 s. [cit. 2019-03-27]. Dostupné z: http://www.karlin.mff.cuni.cz/~holub/soubory/GaussInteger.pdf

VOJÁČEK, Jakub. *Pročíslo* [online]. Matematika pro každého, publikováno 2008-09-17. [cit. 2019-04-04]. Dostupné z: https://www.maths.cz/clanky/138-prvocislo

SEZNAM SCHÉMAT

SEZNAM TABULEK