ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA PEDAGOGICKÁ

KATEDRA MATEMATIKY, FYZIKY A TECHNICKÉ VÝCHOVY

ROZŠÍŘENÁ STUDIE EUKLIDOVSKÝCH OBORŮ INTEGRITY

DIPLOMOVÁ PRÁCE

Martin Dudek

Učitelství pro 2. stupeň základní školy

Vedoucí práce: doc. RNDr. Jaroslav Hora, CSc.

Plzeň, 2023

Prohlašuji, že jsem diplomovou práci vypracoval samostatně s použitím uvedené literatury a zdrojů informací.

V Plzni dne……

……

Vlastnoruční podpis

Poděkování

Děkuji vedoucímu mé diplomové práce doc. RNDr. Jaroslavu Horovi, CSc. za odborné vedení při zpracovávání

Dále bych chtěl vyjádřit poděkování rodině, přátelům a mé snoubence Veronice Ibrahimové za jejich neustále trvající podporu.

Obsah

Úvod

Učení o algebraických strukturách přináší základní seznámení s pojmem, který bude v rámci této práce často zmiňován - pojmem "obor integrity". Při studiu tohoto pojmu se setkáváme s různými formulacemi, interpretacemi a souvisejícími pojmy, které mohou být s tématem spojené. Cílem této práce je poskytnout čtenáři komplexní přehled o tomto pojmu, představit další související pojmy, významné vlastnosti a důsledky vět. Zejména bude práce věnována dělitelnosti, která je neodmyslitelnou součástí pojmu "euklidovy obory integrity".

Definice, pojmy, věty, důkazy a příklady v této práci jsou založeny na společné znalosti algebraických struktur, které jsou představeny v první kapitole. Tato kapitola také popisuje jejich vlastnosti. Je důležité zdůraznit, že hlavním cílem práce je poskytnout čtenáři komplexní přehled všeho, co se týká především euklidových a dalších oborů integrity, s důrazem na dělitelnost v oborech integrity jak v rámci přirozených čísel, tak v rámci celých čísel, Gaussových čísel a polynomů. **Práce si klade za cíl seznámit čtenáře s úvodními znalostmi o tématu a poté tyto znalosti aplikovat na konkrétnějších principech teorie čísel.**

V dnešní době máme k dispozici informační technologie, které nám umožňují zkvalitnit studium a výzkum. V této práci budou tedy tyto technologie také využity.

1. Algebraické struktury

Algebraická struktura je poměrně obšírný pojem, k jehož definici je potřeba mít k dispozici libovolnou **množinu** a také libovolnou **binární operaci**. Algebraickou strukturou poté rozumíme každou libovolnou množinu, na níž je definována ona operace. Důležité je zmínit, že zvolená množina musí být na dané operaci uzavřená, tj. každý další nově vzniklý prvek se musí nacházet ve zvolené množině prvků. Většina definic pochází z osobních poznámek z přednášek či cvičení z vysokých škol.

Definice:

Prvky uspořádané do celku (nebo také souboru) nazýváme **množinou**. Zpravidla je označujeme velkým písmenem a popisujeme výčtem prvků nebo intervalem.

V daném oboru teorie množin se určitě budeme bavit o množinách, které mají číselné proměnné, je ovšem na místě minimálně zmínit existenci množin s prvky o různých datových typech, tj. i prvky nečíselné.

Definice:

Nechť je dána libovolná neprázdná množina **M**. **Binární operace f** je zobrazení $f: M \times M \rightarrow M$. Zapisujeme: $c = f(a, b) = a \square b$, kde prvky $a, b, c \in M$.

Rozumíme jakoukoli binární operaci, která má za následek vytvoření prvku z téže množiny. Mezi typické příklady binárních operací, na kterých se snadno představí pojem, patří sčítání nebo násobení na množině přirozených čísel.

Definice:

Uspořádanou n-tici (dvojici, trojici atd.), chápejme jako množinu **M** prvků, které jsou seřazeny na základě předem stanovené vlastnosti. Záleží tedy na pořadí jednotlivých prvků množiny **M**.

Definice:

Nechť je dána libovolná neprázdná množina **M** a k ní libovolný nenulový počet binárních operací (□, ○, …, ◊). **Algebraickou strukturou** rozumíme uspořádanou n-tici (M, (□, ○, …, ◊)). Množina M se také nazývá **nosičem**.

Algebraická struktura se vztahuje na širokou škálu n-tic různých operací a množin. Každé těleso, grupa nebo obor integrity je příkladem algebraické struktury. Například operace sčítání na množině přirozených čísel, odčítání na množině celých čísel jsou příklady elementárních algebraických struktur. Důležitou vlastností, která provází algebraické struktury, je uzavřenost binární operace na množině.

Nechť je dána libovolná algebraická struktura (M, □). Pro libovolnou trojici prvků z nosiče M platí, že: $z = x \square y$; $x, y, z \in M$.

1.1. Vlastnosti binárních operací

Výčet vlastností, se kterými se setkáváme napříč teorií množin a vlastně matematikou obecně. Je třeba je klasifikovat a rozlišit, neboť jednotlivé vlastnosti hledáme, určujeme a studujeme u jednotlivých algebraických struktur. Rychlý přehled ve vlastnostech nabízí portál Základní poznatky z matematiky (Katedra didaktiky matematiky, 2010-2023).

Komutativnost	Na operaci □ (sčítání)	$x \square y = y \square x$
	Na operaci ○ (násobení)	$x \circ y = y \circ x$
Asociativnost	Na operaci □ (sčítání)	$x \square (y \square z) = (x \square y) \square z$
	Na operaci ○ (násobení)	$x \circ (y \circ z) = (x \circ y) \circ z$
Neutrální prvek (oboustranný)	Vzhledem k □ (sčítání)	$n \square x = x \square n = x$
	Vzhledem k ○ (násobení)	$n \circ x = x \circ n = x$
Agresivní prvek (oboustranný)	Vzhledem k □ (sčítání)	$a \square x = x \square a = a$
	Vzhledem k ○ (násobení)	$a \circ x = x \circ a = a$
Distributivnost (zleva)	□ vzhledem k ○ (sčítání vzhledem k násobení)	$x \square (y \circ z) = (x \square y) \circ (x \square z)$
	○ vzhledem k □ (násobení vzhledem ke sčítání)	$x \circ (y \square z) = (x \circ y) \square (x \circ z)$

Tabulka 1. – Přehled vlastností binárních operací

*Poznámka: $x, y, z \in M$, kdy M je množina, na níž je binární operace definována. Prvky **n** a **a** značí prvek neutrální a agresivní.*

1.2. Klasifikace Algebraických struktur

Jak již bylo naznačeno v kapitole 1, algebraické struktury procházejí dalším dělením na základě specifických vlastností. Lze si to představit tak, že na algebraické struktury kladeveme další a komplexnější požadavky. Většina definic spojených s jednotlivými algebraickými strukturami je převzata ze skript Algebra (Procházka, a další, 1990) a Algebra a teoretická aritmetika 2. díl (Blažek, a další, 1984).

Vzhledem k tomu, že práce se zaměřuje specificky na jeden druh algebraických struktur (tj. obory integrity), bude v této kapitole poskytnut pouze základní přehled těchto specifických typů struktur. Problémem je, že existuje velké množství těchto struktur a liší se pouze v dílčích vlastnostech. Definujme tedy pouze grupoidy a pomocí nich představíme i definice ostatních algebraických struktur.

Definice:

Grupoid je neprázdná množina M, jenž je opatřena binární operací.

Množina M se poté nazývá nosič, nebo-li nosná množina grupoidu. Pokud je binární operace označena třeba jako □, je značení nejčastěji v podobě (M; □) nebo M(□), a tímto značením se odkazuje na grupoid (Procházka, a další, 1990).

Algebraická struktura	Vlastnosti příslušné binární operace				
	uza	aso	kom	neu	agr
Grupoid	Ano	Ne	Ne	Ne	Ne
Komutativní grupoid	Ano	Ne	Ano	Ne	Ne
Pologrupa	Ano	Ano	Ne	Ne	Ne
Komutativní pologrupa	Ano	Ano	Ano	Ne	Ne
Grupa	Ano	Ano	Ne	Ano	Ano
Abelova grupa	Ano	Ano	Ano	Ano	Ano
Kvazigrupa	Ano	Ne	Ne	Ne	Ano
Komutativní kvazigrupa	Ano	Ne	Ano	Ne	Ano
Lupa	Ano	Ne	Ne	Ano	Ano
Komutativní lupa	Ano	Ne	Ano	Ano	Ano
Monoid	Ano	Ano	Ne	Ano	Ne
Komutativní monoid	Ano	Ano	Ano	Ano	Ne

Tabulka 2 – Přehled vlastností různých algebraických struktur s jednou binární operací

Poznámka: kom – komutativita, aso – asociativita, neu – existence neutrálního prvku, agr – existence agresivního prvku (resp. inverzního), dis – distributivita vůči druhé operaci. Pro všechny algebraické struktury platí, že jsou uzavřené na množině, dle definice pojmu algebraické struktury.

Algebraická struktura	Binární operace □ (sčítání)	Binární operace ○ (násobení)	Distributivita	Obsahuje dělitele nuly
Polookruh	Komutativní pologrupa	Pologrupa	Ano	Ano
Komutativní polookruh	Komutativní pologrupa	Komutativní pologrupa	Ano	Ano
***Okruh**	Abelova grupa	Pologrupa	Ano	Ano
***Komutativní okruh**	Abelova grupa	Komutativní pologrupa	Ano	Ano
Obor integrity	Abelova grupa	Komutativní pologrupa	Ano	Ne
Těleso	Abelova grupa	Grupa	Ano	Ne
Komutativní těleso	Abelova grupa	Abelova grupa	Ano	Ne

Tabulka 3 – Přehled vlastností různých algebraických struktur se dvěma binárními operacemi

**Poznámka: Tabulka 1.3 je sestavena kombinací dvou publikací, což vytváří zajímavý konflikt. Například kniha Základy elementární algebry (Drábek a spol., 1985, strany 111, 115) uvádí definici okruhu, kde operace sčítání tvoří abelovu grupu, operace násobení tvoří pologrupu a platí distributivita. Na druhou stranu, kniha Algebra I (Hora, 1991, strana 45) uvádí téměř stejnou definici, s tím rozdílem, že operace násobení je nazývána monoidem místo pologrupy. Podobně lze pozorovat konflikt i v případě definice komutativní pologrupy, kde jediný rozdíl spočívá v existenci komutativity pro operaci násobení. Je vhodné upozornit, že existuje mnoho publikací, které se v definici okruhu mohou různit. Autoři obvykle upozorní na odlišné pojmenování a můžeme se tak setkat i s pojmy jako „Asociativní okruh s jednotkovým prvkem“ a podobně.*

1.3. Obor integrity

Pro přehlednost se přesuňme z obecného zápisu operací a uvažujme, že operace □ je sčítáním a operace ○ je násobením. Následující definice oboru integrity pochází ze skript Algebra I. (Hora, 1991). Definice vychází z pojmu dělitel nuly a mimo jiné je postupně definována pomocí jednotlivých dílčích pojmů ostatních algebraických struktur z tabulek 1.2. a 1.3.

Definice:

Nechť x je nenulový prvek okruhu R. Prvek x se označuje jako **levý dělitel nuly**, pokud k němu existuje nenulový prvek y takový, že:

$x \cdot y = 0$

Nechť je x nenulový prvek okruhu R. Prvek x se označuje jako **pravý dělitel nuly**, pokud k němu existuje nenulový prvek takový, že:

$y \cdot x = 0$

Je-li prvek levým i pravým dělitelem nuly, nazývá se **dělitelem nuly**.

Definice:

Obor integrity je komutativní okruh, který neobsahuje dělitele nuly.

Ze stejné publikace pochází i příklad, který uvádí jako obor integrity právě množinu celých čísel $\mathbb{Z}$ s volenými operacemi sčítání i násobení.

2. Dělitelnost v oborech integrity

Autoři ve skriptech Algebra a teoretická aritmetika (Blažek, a další, 1984) tvrdí, že je třeba definovat pojem dělitelnosti, neboť z původní definice oboru integrity I nevyplývá existence prvku $x \in I$ při volbě prvků $a, b \in I$ tak, že:

$a \cdot x = b,$

jinými slovy, že prvek b je násobkem prvku a, kdy x je koeficientem, při volbě oboru celých čísel $\mathbb{Z}$ jako příklad oboru integrity I. Zavádíme proto pojem dělitelnost v oborech integrity.

2.1. Základní pojmy

Většina definic základních pojmů pochází ze skript Algebra I. (Hora, 1991) a Algebra a teoretická aritmetika (Blažek, a další, 1984).

Definice:

Nechť je dán obor integrity (I, +, ·) a dva jeho prvky označené jako **a** a **b**. Říkáme, že **a** dělí **b** (nebo též **a** | **b**, **a** je dělitelem **b**, **b** je násobek **a**), jestliže existuje **q ∈ I** takové, že

b = q · a

V opačném případě tvrdíme, že **a** nedělí prvek **b** (nebo též **a** ∤ **b**, **a** není dělitelem **b**, **b** není násobek **a**).

K pojmu dělitelnost přikládají autoři Algebry a teoretické aritmetiky (Blažek, a další, 1984 str. 102) lemma v 9 bodech, které je důsledkem zavedení dělitelnosti na vlastnostmi definovaném oboru integrity s binárními operacemi.

Lemma:

Nechť je I libovolný obor integrity, pak platí:

a) $(\forall a \in I) a|a$

b) $(\forall a,b,c \in I)[(a \mid b \wedge b \mid c) \Rightarrow a \mid c]$

c) $(\forall a \in I)[(a \mid 0 \wedge (0 \mid a \Rightarrow a = 0)]$

d) $(\exists a,b \in I)(a \mid b \wedge b \nmid a)$

e) $(\forall a,b \in I)(a \mid b \Rightarrow a \mid bc)$

f) $(\forall a,b,c \in I)(ab \mid c \Rightarrow (a \mid c \ \wedge \ b \mid c))$

g) $(\forall a,b,c \in I)\big[(c \mid a \ \wedge c \mid b) \ \Rightarrow \ \big(c|\ (a+b) \ \wedge c \mid (a-b)\big)\big]$

h) $(\forall a_1,\dots,a_n,k_1,\dots,k_n \in I)[(c \mid \ a_1 \ \wedge \ \dots \ \wedge \ c \mid a_n) \ \Rightarrow \ c \mid \sum_{i=1}^{n} k_i\, a_i]$

i) $(\forall a,b,c \in I)[(c \ \neq \ 0) \ \Rightarrow \ (a \mid b \ \Leftrightarrow \ ac \mid bc)]$

Důkazy výše zmíněného lemmatu vychází zejména ze základních vlastností, které obory integrity mají. V důkazu jsou použity zejména důkazy sporem s výjimkou několika bodů, kde byl použit důkaz přímý.

Důkaz:

a) $\mathbf{a} = \mathbf{a} \cdot 1 = 1 \cdot \mathbf{a}$, tj. každý prvek z oboru integrity lze chápat jako dělitele samo sebou a jedničkou.

b) Důkaz sporem. Prvek **a** dělí **b**, tudíž lze napsat $\mathbf{b} = \mathbf{k} \cdot \mathbf{a}$, $\mathbf{k} \in \mathbf{I}$, zároveň z tvrzení platí, že **b** dělí **c**, což lze zapsat jako $\mathbf{c} = \mathbf{l} \cdot \mathbf{b}$, zároveň by s tvrzením sporem tedy mělo platit, že **a** nedělí prvek **c**, tedy **c** nelze zapsat jako násobek čísla **a**. Nicméně z prvních dvou tvrzení vyplývá, že prvek **c** lze zapsat jako $\mathbf{c} = \mathbf{l} \cdot \mathbf{b} = \mathbf{l} \cdot (\mathbf{k} \cdot \mathbf{a}) = \mathbf{m} \cdot \mathbf{a}$, kdy $\mathbf{m} \in \mathbf{I}$. Což je spor, neboť jsme prvek **c** napsali jako násobek **a**.

c) Je-li a dělitel nuly, potom lze zapsat nulu jako násobek čísla **a** a koeficientu **k**, z čehož vyplývá, že buďto **a**, nebo **k** jsou nulová. Je-li nula dělitelem **a**, potom lze napsat že $\mathbf{0} \cdot \mathbf{m} = \mathbf{a}$, z čehož vyplývá, že **a** musí být nulové, neboť nula je agresivní (inverzní) prvek množiny vzhledem k operaci násobení.

d) Vyplývá ze skutečnosti, že **a** dělí **b**, tudíž lze zapsat prvek **b** jako násobek prvku **a**. Koeficient **k** násobku prvku **a** náleží oboru integrity. Zároveň platí, že **b** nedělí **a**, což musí být pravda, neboť po dosazení dostaneme, že $\mathbf{a} \cdot \mathbf{k}$ nedělí **a**, přičemž my víme, že to platí přesně naopak. Lze tedy vymyslet dosazením příklady, kdy **k** může být neutrální prvek oboru integrity, a tím pádem jsou prvky **a**, **b** asociovány, nebo **k** lze zvolit jako jakýkoli jiný prvek mimo neutrální a tvrzení tudíž bude pravdivé.

e) Důkaz sporem. Prvek **a** dělí **b**, tudíž $\mathbf{b} = \mathbf{a} \cdot \mathbf{k}$. Zároveň dle důkazu sporem má platit, že **a** nedělí $\mathbf{b} \cdot \mathbf{c}$, nicméně **b** lze zapsat jako násobek prvku **a** koeficientem **k**, tudíž dle tvrzení **a** nedělí $\mathbf{(a \cdot k \cdot c)}$, přičemž z tvrzení **a)** víme, že prvek oboru integrity vždy dělí sám sebe, tudíž dělí i svůj násobek.

f) Důkaz sporem. Prvek **ab** dělí **c**, tudíž lze **c** zapsat jako $\mathbf{a} \cdot \mathbf{b} \cdot \mathbf{k}$, kdy **k** je koeficient náležící oboru integrity **I**. Dále z tvrzení sporem vyplývá, že **a** nedělí **c**, nebo že **b** nedělí **c**. Po dosazení výrazu $\mathbf{a} \cdot \mathbf{b} \cdot \mathbf{k}$ za **c** získáváme tvrzení, že **a** nedělí $\mathbf{a} \cdot \mathbf{b} \cdot \mathbf{k}$, nebo že **b** nedělí $\mathbf{a} \cdot \mathbf{b} \cdot \mathbf{k}$, což vidíme, že je spor, neboť výraz vpravo je násobkem obou prvků **a** i **b**, tudíž je dělit musí.

g) Důkaz sporem. Prvek **c** dělí **a,** a zároveň **c** dělí **b**, z toho vyplývá, že prvky **a**, **b** lze zapsat jako násobky **c** nějakými koeficienty **k** a **l**, které náleží oboru integrity. Zároveň ale z tvrzení sporem platí, že **c** nedělí **(a + b)**, nebo že **c** nedělí **(a – b)**. Po dosazení za **a**, **b** dostáváme tvrzení, že: $\mathbf{c} \nmid (\mathbf{c} \cdot \mathbf{k} + \mathbf{c} \cdot \mathbf{l}) \wedge \mathbf{c} \nmid (\mathbf{c} \cdot \mathbf{k} - \mathbf{c} \cdot \mathbf{l})$. po vytknutí **c** ze závorek vidíme, že to je spor, neboť se jedná o násobek prvku **c** a tudíž jej prvek c musí dělit.

h) Důkaz sporem. Z tvrzení vidíme, že $(\boldsymbol{c} \mid \boldsymbol{a_1} \wedge \ldots \wedge \boldsymbol{c} \mid \boldsymbol{a_n})$. Jinými slovy platí tvrzení, že $(\boldsymbol{ck_1} = \boldsymbol{a_1} \wedge \ldots \wedge \boldsymbol{ck_n} = \boldsymbol{a_n})$. Z tvrzení sporem vyplývá, že **c** nedělí $\sum_{i=1}^{n} \boldsymbol{k_i}\, \boldsymbol{a_i}$, tedy **c** nelze zapsat jako sumu těchto výrazů. Po dosazení získáváme tvrzení, že **c** nedělí $\sum_{i=1}^{n} \boldsymbol{k_i}\, \boldsymbol{ck_i}$, z této sumy lze ovšem vytknout **c** a lze jasně vidět, že **c** dělí sumu výrazů, která je násobkem **c**, což je spor.

i) Prvek **a** dělí **b**, tedy lze zapsat $\boldsymbol{ak} = \boldsymbol{b}$. Je-li **c** nenulové, lze celou rovnici vynásobit prvkem **c**, takže získáváme rovnici $\boldsymbol{ack} = \boldsymbol{bc}$. Rovnici lze přepsat, že prvek $\boldsymbol{ac}$ dělí $\boldsymbol{bc}$. Tím je důkaz dokončen.

Nyní po základní definici dělitelnosti na oboru integrity, tvrzeních k dělitelnosti na této algebraické struktuře i důkazu, je určitě na místě definovat i asociaci prvků. Definice pochází z publikace Algebra 1. (Hora, 1991 str. 59). Asociace je ve vší podstatě rozšíření vlastnosti dělitelnosti na oboustrannou (vzájemnou) dělitelnost.

Definice:

Nechť je I obor integrity a prvky a, b jsou prvky oboru integrity. Říkáme, že prvek a je asociován s prvkem b, pokud platí, že $a \mid b \wedge b \mid a$. V takovém případě píšeme, že $a \,||\, b$. V opačném případě (jeden z výrazů, nebo oba výrazy konjunkce neplatí) hovoříme o tom, že prvky nejsou asociovány, tudíž lze zapsat $a \nparallel b$.

Dále je potřeba definovat existenci jednotky ve smyslu dělitelnosti v oboru integrity. Následující definice pochází od autorů Algebry a teoretické aritmetiky (Blažek, a další, 1984), nicméně i trochu jinou definici, která je ve vší podstatě stejná, pochází od autora Algebry 1. (Hora, 1991 str. 59).

Definice:

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

Nebo

Prvek **a**, jež náleží oboru integrity se nazývá **jednotkou ve smyslu dělitelnosti**, jestliže **a || 1**.

Autor (Hora, 1991 str. 59) dále zavádí pojmy:

Definice:

Nechť **I** je obor integrity a prvky **a**, **b** jsou prvky **I**.

Jestliže **a | b** a zároveň $a \nmid b$, potom je prvek **a** nazýván **vlastní dělitel** prvku **b**.

Jestliže je **a** jednotkou, nebo je **a || b**, potom je prvek **a** nazývá **nevlastní dělitel** prvku **b**.

Dále je vhodné připomenout vlastnosti, které autor dále zmiňuje:

Lemma:

Buďte **a**, **b**, **c**, **x**, **y** prvky oboru integrity **I**. Pak platí následující tvrzení:

a) Každý prvek oboru integrity dělí sám sebe.

b) Je zachována asociativnost, tj. pokud **a** dělí **b** a zároveň **b** dělí **c**, potom **a** dělí **c**.

c) Jestliže **a** dělí **b** a zároveň **a** dělí **c**, potom **a** dělí **(bx+cy)**.

d) Jestliže **a** dělí **b**, potom **ac** dělí **bc**.

Oba výše zmínění autoři uvádějí tentýž příklad, který demonstruje existenci jednotkového prvku ve smyslu dělitelnosti v daném oboru integrity (Z, +, ·). Bez dalšího vysvětlení tohoto příkladu lze interpretovat, že v takovém oboru integrity existují dvě jednotky ve smyslu dělitelnosti, a to 1 a -1. Tato skutečnost je zřejmá, stačí vydělit libovolné číslo samo sebou, nebo se řídit **definicí jednotky ve smyslu dělitelnosti**: Prvek a je asociován s 1, tj. a dělí 1, a zároveň 1 dělí a. Je zřejmé, že prvek a je roven 1.

Příklad:

Nejsou-li celá čísla a, b dělitelná třemi, je právě jedno z čísel a + b, a – b dělitelné třemi. Dokažte. (Drábek, a další, 1985 str. 185)

Řešení:

Celá čísla a, b lze přepsat dle definice dělitelnosti do tvarů:

a = 3x + 1 nebo a = 3x + 2, respektive b = 3y + 1 nebo b = 3y + 2. Kombinací nastává:

1. a = 3x + 1 a zároveň b = 3y + 1

a – b = 3x – 3y = 3(x - y), tj. je dělitelné třemi.

2. a = 3x + 1 a zároveň b = 3y + 2

a + b = 3x + 1 + 3y + 2 = 3(x + y + 1), tj. je dělitelné třemi.

3. a = 3x + 2 a zároveň b = 3 y + 1

a + b = 3x + 2 + 3y + 1 = 3(x + y + 1), tj. je dělitelné třemi.

4. a = 3x + 2 a zároveň b = 3y + 2

a – b = 3x + 2 – 3y – 2 = 3(x – y), tj. je dělitelné třemi.

Příklad:

Dokaž, že ne/jsou čísla 720, 384, 659, 3792 a 9464 dělitelná šesti.

Řešení:

Důkaz přímý. Rozklad a ověřování dělitelností dvojkou a trojkou (asociativita).

1. 6 | 720, tj. 6x = 720, 720 je dělitelné dvojkou (sudé) a je dělitelné trojkou (600 + 2 · 60)

2. 6 | 384, tj. 6x = 384, číslo je dělitelné dvojkou (sudé) a je dělitelné trojkou (300 + 60 + 24)

3. 6 | 659, tj. 6x = 659, číslo není dělitelné dvojkou (liché)

4. 6 | 3792, tj. 6x = 3792, číslo je dělitelné dvojkou (sudé) a je dělitelné trojkou (3000 + + 2 · 300 + 6 · 30 + 4 · 3)

5. 6 | 9464, tj. 6x = 9464, číslo je dělitelné dvojkou (sudé) a není dělitelné trojkou (3 · 3000 + + 300 + 5 · 30 + 4 · 3 + 2)

Závěr: Čísla dělitelná šesti jsou 720, 284 a 3792, Ostatní zadaná čísla nejsou dělitelná šesti.

Postup ve druhém příkladu používá definici tzv. společného dělitele, která se nachází v následující kapitole a je uvedena společně s definicí společného násobku čísla.

2.2. Největší společný dělitel a nejmenší společný násobek

Definice:

Jsou-li $a_1, a_2, \ldots, a_n$ libovolné prvky z oboru integrity I, nazývá se prvek $u \in I$ jejich **společný dělitel**, právě tehdy, když $u \mid a_1, u \mid a_2, \ldots, u \mid a_n$. Obdobně prvek $v \in I$ se nazývá **společný násobek** prvků $a_1, a_2, \ldots, a_n$, platí-li současně $a_1 \mid v, a_2 \mid v, \ldots a_n \mid v$. (Blažek, a další, 1984 str. 107)

Taková definice nám ovšem zaručí existenci většího množství společných dělitelů. Jako příklad můžeme použít předchozí příklad, kde bylo ověřováno, zda je dané číslo dělitelné šesti. Tam jsme využili principu, že číslo dělitelné 6 musí být dělitelné třemi a dvěma, nehledě na to, že je určitě více čísel, které nám budou dělit číslo 720 a třeba číslo 384 (číslo 2, 3, 4, 6, 8 atd.).

Spíše než pojmy společný násobek nebo společný dělitel nás proto zajímá jejich poněkud užší definování, tzv. největší společný dělitel a nejmenší společný násobek.

Definice, kterou uvádím, vychází ze spojení dvou různých definic a mírné úpravy proměnných. První definice, která popisuje největší společný dělitel (NSD), je převzata z knihy Algebra I (Hora, 1991 str. 60). Druhá definice, která se týká nejmenšího společného násobku (NSN), pochází z knihy Algebra a teoretická aritmetika (Blažek, a další, 1984 stránky 107-108).

Definice:

Prvek d je nazýván **největším společným dělitelem** prvků a1, a2, ..., an a značí se d = D(a1, a2, ..., an), pokud je dělitelem všech těchto prvků a zároveň platí, že každý jiný společný dělitel t prvků a1, a2, ..., an dělí d.

Obdobně můžeme definovat nejmenší společný násobek, protože existuje více společných násobků čísel. Zmíněný příklad nám ukazuje, že společným násobkem čísel 2 a 3 je právě číslo 6, které je zároveň nejmenším společným násobkem. Nicméně existují i další společné násobky, jako například čísla 12, 18, 24 atd.

Definice:

Buďte $a_1, a_2, \ldots, a_n$ prvky oboru integrity I. Prvek $m \in I$ nazýváme **nejmenším společným násobkem** prvků $a_1, a_2, \ldots, a_n$, jestliže m je společným násobkem těchto prvků a zároveň pro libovolný společný násobek u prvků $a_1, a_2, \ldots, a_n$ platí, že $m \mid u$. Nejmenší společný násobek poté zapisujeme: $u = n(a_1, a_2, \ldots, a_n)$.

Definice:

Říkáme, že v oboru integrity I **existuje největší společný dělitel** (ENSD), jestliže ke každým dvěma prvkům z oboru integrity I existuje alespoň jeden největší společný dělitel z I. Říkáme, že v oboru integrity I **existuje nejmenší společný násobek** (ENSN), jestliže ke každým dvěma prvkům z oboru integrity I existuje v I alespoň jeden nejmenší společný násobek. (Hora, 1991 str. 62)

2.3. Největší společný dělitel a nejmenší společný násobek jako téma na ZŠ

Na základních školách se studenti obvykle seznamují s pojmy spojenými s hledáním společného jmenovatele při sčítání zlomků. Během prvního stupně se nejprve naučí, jak takový jmenovatel spočítat, avšak samotné pojmy, jako je největší společný dělitel (NSD) a nejmenší společný násobek (NSN), se jim představují až na druhém stupni. Je to zde, kde se studenti také seznámí se specifickými příklady zaměřenými na hledání NSD a NSN.

Jedním z triviálních způsobů hledání nejmenšího společného násobku (NSN) dvou čísel a a b je postupné násobení obou čísel prvky z množiny přirozených čísel a zaznamenávání těchto násobků do sloupců nebo řádků. Porovnáním těchto výpisů lze zjistit, které číslo je jejich společným násobkem. Tento společný násobek bude určitě stejný nebo menší než součin čísel a a b. Při hledání největšího společného dělitele (NSD) můžeme podobně postupovat a získat potřebný výsledek.

Existuje však problém s takovýmto postupem, který spočívá v tom, že není příliš obecný a závisí na konkrétním zadání příkladů. Při práci s čím dál většími čísly se tento postup stává stále více zdlouhavým. Proto je důležité dětem představit alternativní způsob hledání největšího společného dělitele (NSD) a nejmenšího společného násobku (NSN). Tento způsob využívá rozklad čísel na součin prvočísel, což se ukazuje jako efektivnější a univerzálnější metoda.

Při hledání největšího společného dělitele (NSD) dvou nebo více prvků je nejprve nutné přepsat tyto prvky jako součiny prvočísel. Poté je třeba identifikovat společné faktory, které se vyskytují ve všech těchto prvcích (i kdyby to byla pouze jednička). Toto společné číslo je pak označováno jako NSD.

Při hledání nejmenšího společného násobku (NSN) dvou nebo více prvků je nejprve nutné nalézt NSD všech dvojic těchto prvků. Poté se vytvoří nová množina prvků z původní množiny, kde každý prvek je vydělený NSD, které se vyskytují ve jeho součinném tvaru. Pro získání NSN je pak třeba vynásobit všechna NSD dvojic s každým prvkem nové množiny.

Poznámka: Nejmenší společný násobek (NSN) je součinem všech součinných tvarů prvků, přičemž opakující se části součinného tvaru jsou započítány pouze jednou. Toto je ilustrováno v následujícím příkladu a pomocí barevného zvýraznění. Oranžová barva označuje zbytky, modrá barva značí NSD (největší společný dělitel). Ostatní barvy značí další opakující se části součinného tvaru.

Příklad:

Nalezněte nejmenší společný násobek a největšího společného dělitele čísel:

a) 36 a 48

b) 96 a 128

c) 120 a 135

d) 12, 60 a 75

e) 125, 175 a 245

f) 24, 72 a 144

Řešení:

a) $36 = 2 \cdot 18 = 2 \cdot 2 \cdot 9 = 2 \cdot 2 \cdot 3 \cdot 3$

$48 = 2 \cdot 24 = 2 \cdot 2 \cdot 12 = 2 \cdot 2 \cdot 2 \cdot 6 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3$

$\boldsymbol{NSD = 2 \cdot 2 \cdot 3 = 12}$

$\boldsymbol{NSN = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 144}$

b) $96 = 2 \cdot 48 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3$ *(viz rozklad čísla 48 výše)*

$128 = 4 \cdot 32 = 4 \cdot 4 \cdot 8 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2$

$\mathbf{NSD = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 32}$

$\mathbf{NSN = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 384}$

b) $120 = 2 \cdot 60 = 2 \cdot 2 \cdot 30 = 2 \cdot 2 \cdot 2 \cdot 15 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5$

$135 = 3 \cdot 45 = 3 \cdot 3 \cdot 15 = 3 \cdot 3 \cdot 3 \cdot 5$

$\boldsymbol{NSD = 3 \cdot 5 = 15}$

$\boldsymbol{NSN = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5 = 1\,080}$

c) $12 = 2 \cdot 6 = 2 \cdot 2 \cdot 3$

$60 = 2 \cdot 30 = 2 \cdot 2 \cdot 15 = 2 \cdot 2 \cdot 3 \cdot 5$

$75 = 3 \cdot 25 = 3 \cdot 5 \cdot 5$

$\boldsymbol{NSD = 3}$

$\boldsymbol{NSN = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 = 1\,200}$

d) $125 = 5 \cdot 25 = 5 \cdot 5 \cdot 5$

$175 = 5 \cdot 35 = 5 \cdot 5 \cdot 7$

$245 = 5 \cdot 49 = 5 \cdot 7 \cdot 7$

$\boldsymbol{NSD = 5}$

$\boldsymbol{NSN = 5 \cdot 5 \cdot 5 \cdot 7 \cdot 7 = 6\,125}$

e) $24 = 2 \cdot 12 = 2 \cdot 2 \cdot 6 = 2 \cdot 2 \cdot 2 \cdot 3$

$72 = 2 \cdot 36 = 2 \cdot 2 \cdot 18 = 2 \cdot 2 \cdot 2 \cdot 9 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$

$144 = 2 \cdot 72 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$ *(viz rozklad čísla 72 výše)*

NSD $\boldsymbol{= 2 \cdot 2 \cdot 2 \cdot 3 = 24}$

NSN $\boldsymbol{= 2 \cdot 2 \cdot 2 \cdot 3 \cdot 2 \cdot 3 = 144}$

3. Euklidův algoritmus

Existuje několik postupů pro získání největšího společného dělitele (NSD) dvou přirozených čísel, které jsme se naučili v předchozí kapitole. Mezi nimi se nachází **Euklidův algoritmus**, další možnost pro nalezení NSD. Tento algoritmus využívá důležitou větu, která je popsána v knize "Základy elementární algebry" od RNDr. Drábka a spol. (Drábek, a další, 1985 str. 189).

Věta:

Jestliže přirozené číslo a dává při dělení nenulovým přirozeným číslem b nenulový zbytek z, potom platí, že dělitel D(a, b) = D(b, z).

Důkaz:

Především platí: $a = b \cdot q + z,\ 0 < z < b$,

Předpokládejme, že x ∈ D(a, b), tudíž x dělí a a zároveň dělí b. Když si z rovnice vyjádříme zbytek z, je patrné, že prvek x dělí i zbytek z. Tedy je tímto dokázána množinová inkluze D(a, b) ⊂ D(b, z).

Dále předpokládejme, že x ∈ D(b, z), tj. x dělí b a z. Z rovnice vyplývá, že x dělí i číslo a, tedy platí x ∈ D(a, b), z čehož vyplývá množinová inkluze D(b, z) ⊂ D(a, b).

(viz kapitola 4. věta 1)

Z věty je patrný nástin postupu hledání NSD dvou přirozených čísel. Mějme dvě čísla a a b, pro která platí, že b ∤ a. Potom platí:

$$a = b \cdot q + z_1, \qquad 0 < z_1 < b$$

Nicméně ke každým dvěma prvkům z množiny celých čísel a a b, kdy je b nenulové, existuje rozklad (respektive dvojice jiných celých čísel) takový, že a = b·q + r, 0 ≤ r < |b|. Tedy provádíme dělení se zbytkem, kde q je neúplný podíl a r je zbytek po dělení.

Lze tedy předpokládat, že existují čísla q_1 a z_2 taková, že $b = z_1 \cdot q_1 + z_2$, $0 \leq z_2 < |b|$. Pokud by se po takovém kroku prvek z_2 rovnal nule, potom jsme u konce a prvek z_1 by byl hledaným největším společným dělitelem. V opačném případě je potřeba postup zopakovat, tedy by existovala další čísla q_2 a z_3, pro která platí: $z_1 = z_2 \cdot q_2 + z_3$, $0 \leq z_3 \leq z_2$.

Příklad:

Nalezněte největšího společného dělitele s pomocí Euklidova algoritmu u následujících dvojic přirozených čísel:

a) 36 a 48

b) 120 a 135

c) 175 a 245

d) 1500 a 32

Řešení:

a) $48 = 36 \cdot 1 + 12$

$36 = 12 \cdot 3 + 0$

NSD = 12

b) $135 = 120 \cdot 1 + 15$

$120 = 15 \cdot 8 + 0$

NSD = 15

c) $245 = 175 \cdot 1 + 70$

$175 = 70 \cdot 2 + 35$

$70 = 35 \cdot 2 + 0$

NSD = 35

d) $1500 = 32 \cdot 46 + 28$

$32 = 28 \cdot 1 + 4$

$28 = 4 \cdot 7 + 0$

NSD = 4

3.1. Implementace Euklidova algoritmu do ICT s použitím VS2019

V rámci řešení příkladů s pomocí Euklidova algoritmu je často k užitku zkontrolovat si postup vlastního řešení, s čímž může správné užití ICT vhodně pomoci. Vytvořený program má tedy přesně tento úkol a dokáže zpracovat vstup dvou libovolných přirozených čísel, přičemž jeho výstupem je právě největší společný dělitel těchto zadaných čísel.

Program pracuje podle totožného postupu, jaký je představen v kapitole 3. Pro tento účel v programu existují vlastní metody VratZbytek a VratPodil, které u zadaných dvou čísel vrací právě neúplný podíl q a zbytek po dělení. Pro další fungování (respektive pro další krok) potom tyto metody volá program rekurzivně.

```
//Výpočet, ověření a výpis
int x = cislo1;
int y = cislo2;
while (y != 0)
{
    int podil = calculator.VratPodil(x, y);
    int zbytek = calculator.VratZbytek(x, y);
    calculator.VypisVysledek(x, y);
    x = y;
    y = zbytek;
    if (y == 0)
    {
        Console.WriteLine();
        Console.WriteLine("Závěr: Největším společným dělitelem zadaných čísel {0} a {1} je číslo {2}.", cislo1, cislo2, x);
    }
}
```

Obrázek 1 – Úsek kódu pro zjištění NSD dvou zadaných přirozených čísel

Pro názornost je níže přiložen výstřižek z průběhu programu pro zvolená čísla 1500 a 32 (tedy poslední ze zadaných počítaných příkladů).

```
Zadej mi 1. číslo
175
Zadej mi 2. číslo
245

245 = 175*1 + 70
175 = 70*2 + 35
70 = 35*2 + 0

Závěr: Největším společným dělitelem zadaných čísel 245 a 175 je číslo 35.
Přeješ si zadat nový příklad? a/n
```

Obrázek 2 – Ukázka běhu programu na zjištění NSD

Tento hledač největších společných dělitelů dvou přirozených čísel je ošetřen pro případ špatného vstupu, tedy pro případ, že uživatel vloží nežádoucí data. Lze tedy vložit pouze přirozená čísla. Dále se zastaví včas před dělením nulou a je ošetřen i pro špatné vstupy v případě cyklu pro běh programu (předpoklad opětovného použití uživatelem).

4. Euklidovský obor integrity

V předchozích kapitolách byly zavedeny obory integrity a také pojem největší společný dělitel. Z principu Euklidova algoritmu vyplývá, že pro každé dva prvky oboru integrity lze nalézt největšího společného dělitele. Ve vší podstatě se jedná o obor integrity, na který implementujeme novou vlastnost vyplývající z existence Euklidova algoritmu.

Obor integrity R se nazývá **euklidovský obor integrity**, je-li ke každému nenulovému prvku a ∈ R přiřazeno celé nezáporné číslo n(a) tak, že:

1. Jestliže a | b, $b \neq 0$, potom $n(a) \leq n(b)$

2. Ke každým dvěma nenulovým prvkům a, b ∈ R existují prvky q, r takové, že $a = b \cdot q + r$, kde r je rovno nule, nebo n(r) < n(b)

Funkce n se potom nazývá **euklidovská norma** či také může být známé jako **euklidovská funkce**. (Hora, 1991 str. 71)

Poznámka: Původní publikace je v částečně jiném znění z důvodu záměny pojmů „euklidovský“ a „eukleidovský“. Tyto pojmy jsou ekvivalentní a v rámci této práce byl použit pouze jeden z nich.

4.1. Vlastnosti euklidových oborů integrity

Zavedení nového pojmu euklidovského oboru integrity vede k odhalení několika zajímavých vlastností, které platí pro tyto specifické obory. Následující zdroj "Algebra a teoretická aritmetika 2" (Blažek a další, 1984, stránky 115-116), obsahuje lemmata a důkazy, které dávají vzniknout důsledkům, tedy konkrétním vlastnostem, které pro tyto obory integrity plynou. Tyto důležité teoretické koncepty poskytují hlubší vhled do struktury euklidovských oborů integrity a mohou sloužit jako základ pro další studium a aplikace v různých oblastech matematiky. Nyní si představme některé z nich.

Lemma 1:

Nechť **R** je euklidovský obor integrity. Potom pro libovolné a, b ∈ R, kdy b je různé od nuly, platí: $a|b \Rightarrow (n(a) = n(b) \Rightarrow b|a)$

Důkaz:

Nechť a dělí b a současně v(a) = v(b). Podle druhého bodu definice euklidova oboru integrity platí, že existují čísla q a r z tohoto oboru, pro která platí, že $a = bq + r$, kde r je buď nulové, nebo je n(r) méně než n(b). První případ je zřejmý, pokud je zbytek nulový, potom je a roven nějakému násobku b a tudíž b dělí a. Druhý případ je, že n(r) < n(b), neboť je zbytek nenulový a n(r) < n(a). Z předpokladu, že a dělí b vyplývá existence prvku m takového, že $am = b$, potom ale platí $\begin{matrix} a = bq + r = amq + r \\ r = a \cdot (1 - mq) \end{matrix}$, tedy a dělí zbytek r, což by znamenalo, že $n(a) \leq n(r)$. Jinými slovy jsme dostali spor, neboť n(r) má být méně než n(a), možnost nenulového zbytku nemůže nikdy nastat, a tudíž je lemma dokázáno.

Lemma 2:

Nechť je **R** euklidovský obor integrity a jsou dány dva prvky a, b z R, kdy b je nenulové. Potom platí: $(a|b \wedge a \nmid b) \Rightarrow n(a) < n(b)$.

Důkaz:

Prvek a dělí b, tudíž lze psát, že $n(a) \leq n(b)$. Prvek a není asociován s prvkem b, což tedy znamená, že buď a nedělí b, nebo b nedělí a. První možnost nastat nemůže z předpokladu, že a dělí b, tudíž zbývá pouze prostudovat druhou možnost. Pokud b nedělí a, potom lze napsat, že $a = bq + r$, přičemž když b nedělí a, potom musí být zbytek r nenulový, čímž dostáváme, že n(r) < n(b) a tím je důkaz hotov, neboť n(a) < n(r) < n(b), tedy nalezli jsme prvek větší než n(a) a menší než n(b), takže se v zásadě nikdy nemohou n(a) a n(b) rovnat.

Věta:

Nechť je dán euklidovský obor integrity **R**. K libovolným dvěma prvkům z R existuje největší společný dělitel. (Blažek, a další, 1984 str. 116)

Důkaz:

Z Euklidova algoritmu plyne, že pokud máme dva prvky euklidovského oboru R a a b, můžeme je vyjádřit jako $a = bq_1 + r_1$, kdy b je menší než a a zároveň je nenulové (v případě hledání NSD libovolného prvku a nuly platí, že jejich společným dělitelem je právě onen libovolný prvek).

Z rovnice plyne, že pokud je zbytek r_1 roven nule, prvek b by byl hledaným NSD, což by byl triviální případ. Zajímá nás proto případ, že je zbytek nenulový, potom $n(r_1) < n(b)$. Dostáváme další rovnici v podobě $b = r_1q_2 + r_2$, kde jsou opět dva případy podle toho, zda je zbytek nenulový či nikoli. První případ, kdy je zbytek nulový, je opět triviální, druhý případ by se opět musel přepsat. Z principu Euklidova algoritmu (viz postup a kód) vyplývá, že po určitém konečném počtu kroků musíme naleznout NSD, což je zaručeno principem existence jednotky ve smyslu dělitelnosti v euklidovském oboru integrity.

$$
\begin{aligned}
a &= bq_1 + r_1 && n(r_1) < n(b)\\
b &= r_1q_2 + r_2 && n(r_2) < n(r_1)\\
r_1 &= r_2q_3 + r_3 && n(r_3) < n(r_2)\\
&\dots\\
r_{k-3} &= r_{k-2}q_{k-1} + r_{k-1} && n(r_{k-1}) < n(r_{k-2})\\
r_{k-2} &= r_{k-1}q_k + r_k && n(r_k) < n(r_{k-1})\\
r_{k-1} &= r_kq_{k+1} + r_{k+1} && r_{k+1} = 0
\end{aligned}
$$

Z poslední rovnosti plyne, že r_k dělí r_{k-1}, tím pádem lze napsat $r_{k-1} = r_kq_{k+1} + 0$, takže můžeme postupně dosazovat do rovnic postupně „vzhůru“. Při poslední iteraci lze tedy napsat závěr, že prvek r_k dělí prvek a a dělí i prvek b.

Zbývá dokázat, že je prvek r_k ze všech společných dělitelů ten největší, a to je zřejmé ze dvou důvodů:

1. Prvek r_k je v indukci prvním prvkem, který dělí předchozí prvek r_{k-1}, neboť je zbytek nulový. Kdyby se během postupu indukcí nacházel někde jiný takový prvek, narazili bychom na něj, neboť jsme velikost zbytku neustále ověřovali. Pokud by některý z nich byl nulový, porušili bychom původní předpoklad, že nás zajímají pouze případy, kdy není zbytek nula.

2. Během vypisování rovnic zapisujeme podmínky velikosti zbytku, tj. můžeme interpretovat v konečné rovnici, že $n(r_k) < n(r_{k-1}) < \cdots < n(r_1) < n(b)$, přičemž $n(r_{k+1})$ je dle nerovnice menší než $n(r_k)$ a navíc je roven nule.

Z obou bodů vyplývá, že prvek r_k je největším společným dělitelem prvků a a b, které jsou prvky euklidova oboru integrity, a tudíž je důkaz hotov.

Důkaz věty je zároveň důkazem principu fungování Euklidova algoritmu, který je zároveň použit pro počítání konkrétních příkladů v předchozí kapitole (3. Euklidův algoritmus) a také zároveň zdůvodňuje, proč program pro nalezení největšího společného dělitele dvou přirozených čísel nemůže selhat, neboť i kdyby neexistoval jiný společný dělitel než jednotka ve smyslu dělitelnosti, potom je největším společným dělitelem dvou prvků právě ona jednotka.

Lemma 3:

Nechť **R** je Euklidovský obor integrity, a, b náleží R. Jestliže a, b jsou nesoudělné prvky, existují prvky m, n z R takové, že $am + bn = 1$. (Blažek, a další, 1984 str. 117)

Důkaz lemmatu vyplývá z důkazu předchozí věty, že ke každým dvěma prvkům euklidovského oboru integrity lze nalézt největšího společného dělitele pomocí Euklidova algoritmu. Důkaz probíhá obdobně pomocí tvrzení, že libovolný prvek euklidovského oboru integrity lze získat pomocí součtu jiných dvou libovolných prvků oboru integrity, které jsou vynásobeny již konkrétními koeficienty z oboru integrity.

Výpisem jednotlivých rovnic v procesu Euklidova algoritmu a postupným dosazováním se získá poslední zbytek r_{k+1} jako nulový a r_k je rovno jedné. Je nutné si uvědomit, že v procesu dokazování lze opět získat více možností, jakého tvaru bude zbytek. Nulový zbytek by vedl na triviální řešení, kdežto nenulový by inicioval tvorbu další rovnice dle pravidel Euklidova algoritmu.

V této fázi je na místě se domnívat, že každý euklidovský obor integrity je oborem integrity hlavních ideálů. Pro připomenutí:

Definice:

Podgrupa **I** aditivní grupy okruhu (popř. oboru integrity) **R** se nazývá **levý *(resp. pravý)* ideál okruhu R**, jestliže I je levý *(resp. pravý)* ideál multiplikativního grupoidu R(.), tj. $ab \in I$ *(resp.* $ba \in I$*)* pro všechna $a \in R$, $b \in I$. Podgrupa I se nazývá ***(oboustranný)*** **ideál okruhu R**, je-li současně pravým i levým ideálem v R. (Procházka, a další, 1990 str. 185)

Tedy každý ideál je hlavním ideálem, pokud jej lze generovat s pomocí jednoho prvku. Například pro obor přirozených čísel můžeme vygenerovat hlavní ideál tvořený libovolným prvkem 2 tak, že postupně roznásobíme číslo 2 všem prvky množiny přirozených čísel.

Příklad:

Nalezněte hlavní ideál na přirozených číslech generovaný číslem 5 a hlavní ideál generovaný číslem 3 na množině celých čísel.

Řešení:

Nechť je R obor integrity, $R = \mathbb{N}$. Uvažujme hlavní ideál generovaný číslem 5, značený jako (5). Tento ideál je množina všech prvků R, které lze získat násobením prvku 5 s libovolným přirozeným číslem. V takovém případě bude hlavní ideál (5) obsahovat čísla {5, 10, 15, 20, …}. Pro případ, že uvažujeme přirozená čísla s nulou by obsahoval hlavní ideál čísla {0, 5, 10, 15, 20, …}. Tyto dva hlavní ideály generované číslem 5 jsou hlavními ideály, neboť díky vlastnosti komutativity na zvolené množině jsou prvky generovány stejně pro libovolná čísla množiny. Ideály jsou tedy levé i pravé zároveň.

Nechť je R obor integrity, $R = \mathbb{Z}$. Uvažujme hlavní ideál generovaný číslem 3, značený jako (3). Tento ideál je množina všech prvků R, které lze získat násobením prvku 3 s libovolným celým číslem. V takovém případě bude hlavní ideál (3) obsahovat násobky číslem 3, tedy {…, -9, -6, -3, 0, 3, 6, 9, …}. Zde je na místě poznamenat, že stejná čísla bychom získali i tím, že bychom hledali hlavní ideál (-3), jenom by čísla byla jinak uspořádaná a na pořadí zde nezáleží.

V principu navazující na příklady nalezení ideálů je patrné, že každý euklidovský obor integrity R je oborem hlavních ideálů. Důvodem je skutečnost, že všechny hlavní ideály jsou generovány právě prvky množiny největších společných dělitelů.

Příklad:

Nechť je R euklidovský obor integrity a a je libovolný prvek ∈ R. Uvažujte, že $R = \mathbb{Z}$. Pro a = 15 zjistěte, jaký hlavní ideál je generován prvkem a a ten vyjádřete jako množinu.

Řešení:

Pro generování hlavního ideálu (a) je potřeba najít prvek b tak, že $a = b \cdot c$, kde b i c jsou prvky z R. Čísla, která dělí číslo 15 jsou čísla $\pm 1, \pm 3, \pm 5, \pm 15$. Největším společným dělitelem čísla 15 je samotné číslo 15, tedy hlavní ideál (15) by odpovídal množině násobků čísla 15 všemi prvky z množiny celých čísel, tedy {…, -30, -15, 0, 15, 30, …}.

Poznámka: V případě, že se ptáme na hlavní ideál generovaný s pomocí dvou prvků euklidova oboru integrity, potom je principem nalezení největšího společného dělitele těchto dvou čísel a NSD by byl právě i prvkem k postupnému násobení všemi prvky zkoumaného oboru integrity.

Věta:

Každý euklidovský obor integrity je oborem hlavních ideálů. Každý euklidovský obor integrity je tedy oborem integrity s jednoznačným rozkladem. (Hora, 1991 str. 75)

Důkaz:

Buď **I** ideál euklidovského oboru integrity **R**. Je-li I = 0, potom I = {0} je hlavním ideálem v R. Předpokládejme tedy, že $I \neq 0$ a buď dán prvek a různý od nuly, který náleží I, pro který platí n(a) = min{n(x); x je různé od nuly a náleží I}. Protože a ∈ I, je {a} podmnožinou I. Je-li obráceně $0 \neq b \in I$ libovolný prvek, pak existují prvky q, r takové, že $b = aq + r$. Je-li r různé od nuly, potom n(r) < n(a), což je spor s volbou prvku a vzhledem k tomu, že r =0, b = aq, b ∈ {a} a tedy I={a} je hlavní ideál v R.

Druhá část důkazu plyne z principu, že obor integrity hlavních ideálů splňuje podmínku existence největšího společného dělitele a kladné řízené vlastnosti dělitelnosti. (Hora, 1991 stránky 75-76)

5. Gaussův obor integrity

5.1. Definice ireducibility, prvočinitelů a Gaussova oboru integrity

V kapitole 2.3. jsme se zabývali hledáním největšího společného dělitele a také nejmenšího společného násobku čísel. V této kapitole využíváme principu rozkladu na prvočísla, nicméně pro kontext Gaussových oborů integrity by bylo vhodné prvočísla zobecnit. Každý čtenář by si mohl rozpomenout na princip definice prvočísel, například jako prvků přirozených čísel, které jsou dělitelné pouze jedničkou nebo jimi samými. Konkrétně u pojmu „ireducibilní prvek“ se můžeme setkat s různými dalšími definicemi, které užívají pojmu „triviální dělitel“ (tj. dělí jedničkou nebo sebou samým). Nicméně přejděme raději k formálnější definici.

Definice:

Nechť je **a** nenulovým prvkem oboru integrity **R** takovým, že a není asociován s jedničkou (tedy prvek a není jednotkou v oboru integrity R). Prvek a nazýváme **ireducibilním prvkem** v R, pokud má pouze nevlastní dělitele, tedy platí, že když vezmeme libovolný prvek b z oboru integrity, který dělí prvek a, tak potom je tento prvek b || a nebo b || 1.

Prvky, které nejsou ireducibilní nazýváme **reducibilní**. Tyto prvky můžeme znát pod pojmem, který je lépe „stravitelný“ pro žáky na základní škole, jako je „složený“ prvek. Tedy lze jej rozložit na součin prvočísel, pokud se bavíme o prvku (resp. čísle) z množiny přirozených čísel.

Další definice se může opět měnit v závislosti na použitých zdrojích, například se lze setkat s tím, že se definuje prvočinitel jako jedno z prvočísel, které tvoří rozklad reducibilního prvku. Raději ale přejděme opět k formálnější definici pomocí nám známým pojmům.

Definice:

Nechť je dán prvek **p** náležící oboru integrity **R**, který je nenulový a není asociován s jedničkou. Pokud pro libovolné dva prvky oboru integrity R **a** a **b** platí, že pokud prvek p dělí jejich součin, tak prvek p | a nebo p | b, potom je prvek p nazýván **prvočinitelem**.

Z těchto dvou definic vyplývá například skutečnost, že pokud jsou dva prvky oboru integrity asociované, potom mohou být buď oba ireducibilní, nebo reducibilní. Zároveň z definic plyne, že pokud vezmeme libovolný prvočinitel z oboru integrity, který dělí libovolně velký součin prvků oboru integrity, potom musí existovat nějaký prvek z tohoto součinu, který lze prvkem (resp. prvočinitelem) vydělit.

Věta:

Nechť je dán prvek **p** z oboru integrity **R**. Je-li tento prvek prvočinitelem, potom je též i ireducibilní. (Blažek, a další, 1984 str. 125)

Důkaz:

Předpokládejme důkaz sporem, tedy že prvek p není prvočinitelem a zároveň se jedná o prvek ireducibilní. Pokud prvek není prvočinitel, potom prvek není prvočíslem, tím pádem jej lze rozepsat na součin prvočinitelů, a tedy se jedná o reducibilní prvek, což je spor s předpokladem.

Nyní díky definovaným pojmům jsme schopni definovat pojem „Gaussův obor“, neboli také „Gaussův obor integrity“. Zvolená definice pochází z knihy Algebra (Procházka, a další, 1990 stránky 215-216) a je na místě k této definici zmínit jednu poznámku. Definice pojmu vychází z předpokladu, že se čtenář v rámci kontextu četby zabývá obory integrity, proto je pojem definovaný pouze jako „Gaussův obor“, ačkoli je z kontextu jasné, že se jedná o obor integrity. Je místě ovšem čtenáře této práce upozornit na skutečnost, že mimo kontext jsou pojmy „Gaussův obor“ a „Gaussův obor integrity“ odlišné.

Zatímco Gaussův obor je obecný pojem označující obor, ve kterém je možné provádět operace s komplexními čísly, tak v Gaussově oboru integrity se bavíme především o specifickém typu Gaussových oborů, které splňují podmínky, co se týče jednoznačnosti rozkladu na ireducibilní prvky (viz dál definice Gaussových oborů integrity).

Příklady Gaussových oborů zahrnují celá čísla, obory komplexních čísel nebo obory racionálních čísel. Příklady Gaussových oborů integrity obsahují Gaussovy obory nad $\mathbb{Z}$, Gaussovo obory nad obory komplexních čísel atd.

Definice:

Jestliže obor integrity **R** splňuje podmínky:

1. Jestliže je každý prvek z oboru integrity R součinem ireducibilních prvků z R.

2. Jsou-li dvě konečné posloupnosti ireducibilních prvků z R takové, že součin prvků první posloupnosti je asociovaný se součinem prvků posloupnosti druhé, potom je počet prvků v každé z posloupností stejný a existuje permutace π množiny $\{1, \ldots, n\}$ taková, že prvek první množiny $p_i \parallel q_{\pi(i)}$ $(i = 1, \ldots, n)$, tedy při vhodném přeuspořádání prvků dostáváme $p_i \parallel q_i$ $(i = 1, \ldots, n)$.

Potom tento obor integrity R se nazývá **Gaussův obor integrity** (též **faktoriální obor**). (Procházka, a další, 1990 stránky 215-216)

5.2. Gaussův obor integrity a euklidův obor integrity

Když vezmeme potaz definice Gaussova oboru integrity i euklidova oboru integrity, můžeme učinit závěr, že euklidův obor integrity je vlastně Gaussův, který má přísnější podmínky. Euklidův obor integrity na rozdíl od Gaussova oboru splňuje jednu další dodatečnou vlastnost a tou je existence tzv. euklidovské normy (nebo i zobrazení či funkce), která přidává další podmínky na rozklad na ireducibilní prvky (resp. součin ireducibilních prvků jednotlivých prvků oboru integrity).

Pokud chceme tuto skutečnost blíže interpretovat, znamená to, že euklidovská norma nám umožňuje porovnávat "velikosti" jednotlivých prvků a uspořádávat je. Například je snadné porovnat velikosti dvou přirozených (popř. reálných či celých) čísel, jako například čísel 2 a 3, ale porovnávání čísel v komplexním oboru je složitější. Můžeme si představit uspořádání čísel pomocí řadících algoritmů, jako je například Bubble sort nebo Insertion sort, které pracují pouze s reálnými čísly.

V Gaussově oboru integrity neexistuje dodatečná vlastnost normy a rozklad na ireducibilní faktory je jednoznačný (vyjma asociativity a pořadí faktorů). Gaussovo obory integrity mají proto širší (obecnější) rozsah a mohou obsahovat prvky s různou velikostí. Na základě této krátké úvahy můžeme interpretovat následující větu:

Věta:

Každý euklidovský obor integrity je rovněž Gaussovým oborem integrity. (Blažek, a další, 1984 stránky 130-131)

Jak uvádí autor (a vyplývá to i z úvahy), pořadí nelze obrátit a neplatí ani ekvivalence. Existují Gaussovy obory integrity, které nejsou euklidovské. Jako příklad takového Gaussova oboru integrity uvádí autor $\mathbb{Z}[x]$, což by poukazovalo na obor polynomů. Dále se však může jednat o obory $\mathbb{Z}[i]$ nebo $\mathbb{Z}[\sqrt{-5}]$, tedy obory celých čísel rozšířené (viz kapitola kvadratické obory integrity).

Důkaz:

Předpokládejme, že **R** je euklidovským oborem integrity. Mějme prvek a z R, který protože je z euklidova oboru integrity, lze jej buď označit jako ireducibilní prvek, nebo z definice euklidova oboru integrity vyplývá, že jej lze rozložit na $a = b \cdot q + r$, kde je buď r = 0, nebo je $n(r) < n(b)$. Zde jsme z věty o existenci největšího společného dělitele (kapitola 4.1.) dokázali, že lze největšího společného dělitele nalézt konečným množstvím kroků. Z toho vyplývá, že každý prvek z R je buď sám ireducibilním prvkem, nebo jej lze na součin ireducibilních prvků rozložit díky vlastnosti o existenci největšího společného dělitele.

Zbývá nám dokázat druhou vlastnost definice Gaussova oboru integrity, tj. že vezmeme-li dvě různé konečné posloupnosti prvků euklidova oboru integrity, potom pokud je součin prvků první posloupnosti asociován se součinem prvků druhé posloupnosti, potom libovolný prvek první posloupnosti dělí některý z prvků posloupnosti druhé. Uvažujme dvě posloupnosti prvků euklidova oboru integrity. Z definice lze každý z těchto prvků obou posloupností považovat za ireducibilní, nebo za prvek rozložitelný na součin ireducibilních prvků. Jsou-li posloupnosti asociovány, potom by se součiny těchto posloupností měly vzájemně rovnat. Tím pádem se zákonitě musí rovnat posloupnosti a součinné tvary obou čísel, a tudíž libovolný prvek libovolné posloupnosti je ireducibilní prvek, který musí být obsažen i v druhé posloupnosti.

5.3. Vlastnosti Gaussových oborů integrity

Pro následující vlastnosti je třeba trochu osvětlit pojem „kanonický rozklad“ a „obecný kanonický rozklad“. Zatímco kanonický rozklad čísla jsme již v rámci této práce představili jako **jednoznačný** rozklad čísla na ireducibilní prvky, tak zobecněný zatím definován nebyl.

Na rozdíl od kanonického rozkladu čísla je ten zobecněný jednoznačný, až na asociaci a pořadí prvků. Znamená to, že prvky mohou být vzájemně permutovány a mohou mít asociované násobky (tuto myšlenku jsme vyřkli již v definici Gaussových oborů integrity). Je důležité zmínit, že tyto asociované násobky nemění výsledek (z principu asociace). Zatímco příklad kanonického rozkladu čísla 12 je $2^2 3 = 2 \cdot 2 \cdot 3$, tak zobecněný kanonický rozklad může mít víc podob, mezi které patří třeba $2 \cdot 2 \cdot 3 = (-2) \cdot (-2) \cdot 3$ atd.

Lemma:

Nechť nenulový prvek **a** z Gaussova oboru integrity **R** má (zobecněný) kanonický rozklad $a = jp_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$. Potom je nenulový prvek b z R dělitelem prvku a, právě když má zobecněný kanonický rozklad tvaru $b = j' p_1^{s_1} p_2^{s_2} \ldots p_n^{s_n}$, kde platí $0 \leq s_i \leq r_i$ (i = 1, 2, …, n). (Blažek, a další, 1984 str. 132)

Tedy jinak řečeno, pokud b | a, tak je potom logické předpokládat, že určitá část součinného tvaru čísla a je zastoupena i v prvku b, který jej dělí.

Důkaz:

Předpokládejme, že máme prvek a Gaussova oboru integrity, který lze rozepsat jako $a = jp_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$ a je dán prvek b, který jej dělí. Pokud jej dělí, znamená to, že jeho rozklad na součin ireducibilních prvků je do jisté míry podobný a stejné ireducibilní prvky se nachází (maximálně s jinou mocninou) v jeho součinném tvaru také, tj. lze psát $b = j' p_1^{s_1} p_2^{s_2} \ldots p_n^{s_n}$.

Prvek b | a lze napsat jako $(j' p_1^{s_1} p_2^{s_2} \ldots p_n^{s_n}) \mid (jp_1^{r_1} p_2^{r_2} \cdots p_n^{r_n})$, kdy mohu mocnitel r_i přepsat jako $r_i = s_i + (r_i - s_i)$. Z takového rozložení je potom patrné, že kanonický rozklad prvku b je stejný jako kanonický rozklad prvku a. Jediný rozdíl spočívá v tom, že exponenty jednotlivých prvočinitelů v kanonickém rozkladu b se pohybují v uzavřeném intervalu od nuly do **k**, kdy k je exponent odpovídající stejnému prvočiniteli v prvku a.

Věta:

V libovolném Gaussově oboru integrity **R** existuje (pro libovolnou n-tici prvků R) největší společný dělitel a nejmenší společný násobek. (Blažek, a další, 1984 str. 132)

Důkaz výše zmíněné věty je zdlouhavý a je založen na principech popsaných v této práci. Pro jeho doslovnou interpretaci jej lze určitě dohledat v libovolné publikaci, která se zabývá Algebrou. V rámci práce poskytnu pouze shrnutí principu důkazu této věty.

Důkazy existence největšího společného dělitele a nejmenšího společného násobku jsou nejpravděpodobněji vždy založeny na principu Euklidova algoritmu. Ten zde byl představen aplikačně v rámci dvou zvolených prvků, nicméně je potřeba si uvědomit, že jej lze aplikovat i na celé řady prvků. Popřípadě jej lze zapojit cyklicky, tj. nalézt NSD (resp. NSN) dvou prvků, označit si NSD jako nový prvek a tím pádem se řada čísel snížila o jeden prvek a můžeme pokračovat v nové aplikaci Euklidova algoritmu.

U důkazu existence NSD lze pro libovolnou n-tici prvků v R nalézt a definovat NSD jako prvek, který je dělitelem všech prvků n-tice a je největším takovým. Tento prvek je jednoznačný a lze jej nalézt díky asociativitě, existenci ireducibilního součinného rozkladu a vlastnostem Euklidova algoritmu.

Důkaz pro existenci nejmenšího společného násobku (NSN) zahrnuje opět libovolně zvolenou n-tici prvků R. V tomto případě můžeme definovat NSN jako prvek, který je násobkem všech prvků n-tice a zároveň je nejmenším takovým prvkem. Jinými slovy, NSN je nejmenší společný násobek všech prvků v n-tici, což znamená, že je to prvek, který je dělitelný všemi prvky n-tice a zároveň je nejmenším prvkem s touto vlastností. Tímto způsobem lze najít NSN pro libovolnou n-tici prvků R.

Na závěr si dokažme poslední větu spojenou s existencí Gaussova oboru integrity R za podmínek existence největšího společného dělitele a konečnosti řetězce. Věta i důkaz pochází z Algebry a teoretické aritmetiky 2 (Blažek, a další, 1984 stránky 134-135).

Věta:

Obor integrity **R** je Gaussovým oborem integrity, právě když v R k libovolným dvěma prvkům existuje největší společný dělitel a když R splňuje podmínku konečnosti řetězce vlastních dělitelů.

Důkaz:

Je-li R Gaussův obor integrity, potom podle předchozí věty platí podmínka NSD. Nechť je tedy dána libovolná posloupnost v R $a_1, a_2, \ldots, a_n$ kde $a_{i+1} \mid a_i$ $(i = 1, 2, \ldots, n)$, z předchozích důkazů lze předpokládat, že člen a_1 je nenulový (jinak je řešení opět triviální kvůli nulovému zbytku po dělení) a stejně tak i ostatní prvky posloupnosti. Potom existuje zobecněný kanonický rozklad prvku $a_1 = jp_1^{r_1}p_2^{r_2}\cdots p_n^{r_n}$.

Všechny prvky dané libovolné posloupnosti ale mají v principu nějaký zobecněný kanonický rozklad téhož tvaru, ale protože dle posloupnosti platí dělitelnost (tj. každý další prvek dělí ten předchozí), pak se budou lišit ve velikosti exponentů nějakého ze svých ireducibilních prvků. Pokud platí, že prvek a_{i+1} není asociován s předchozím prvkem a_i, potom se v jejich kanonických rozkladech musí najít ireducibilní prvek, který mají rozdílný, a to konkrétně tak, že v prvku a_{i+1} musí být exponent takového ireducibilního prvku menší než v prvku a_i.

Tj. podle téhle úvahy může být v posloupnosti prvků maximálně $k_1 + k_2 + \ldots + k_n$ prvků, které nejsou vzájemně asociované, tj. dokázali jsme existenci indexu prvků (nalezli jsme určitou závoru), u které platí, že každý další prvek za závorou je asociován s libovolným prvkem dané libovolné posloupnosti.

5.4. Využití ICT pro rozklad celého čísla na ireducibilní prvky

Využití informačních technologií v tomto specifickém případě (tj. u rozkladu celého čísla na součin ireducibilních prvků) je relativně krátký, ale zato zacyklený program. Jeho krátkost nám dovoluje vyhnout se potřebě psaní programu objektově. Jeho hlavními části jsou opět vstupní data, zpracování dat a vypisování a na závěr ošetření cyklů a ukončení programu.

```
//Vnitřní cyklus vypisování ireducibilních prvků
for (int i = 2; i <= cislo; i++)
{
    if (cislo % i == 0)
    {
        soucin_prvocisel = soucin_prvocisel + " " + i;
        soucin_prvocisel = soucin_prvocisel.Trim();
        cislo = cislo / i;
        i = 1;
        if (cislo != zaklad)
            Console.WriteLine(cislo.ToString() + " * " + soucin_prvocisel.Replace(" ", " * "));
        else
            Console.WriteLine(soucin_prvocisel.Replace(" ", " * "));
    }
}
```

Obrázek 3 – Cyklus rozkládání čísla na ireducibilní prvky

```
Zadej mi libovolné celé číslo.
128
64 * 2
32 * 2 * 2
16 * 2 * 2 * 2
8 * 2 * 2 * 2 * 2
4 * 2 * 2 * 2 * 2 * 2
2 * 2 * 2 * 2 * 2 * 2 * 2
1 * 2 * 2 * 2 * 2 * 2 * 2 * 2
Přeješ si zadat nový příklad? a/n
a
Zadej mi libovolné celé číslo.
255
85 * 3
17 * 3 * 5
1 * 3 * 5 * 17
Přeješ si zadat nový příklad? a/n
a
Zadej mi libovolné celé číslo.
68
34 * 2
17 * 2 * 2
1 * 2 * 2 * 17
Přeješ si zadat nový příklad? a/n
n
Díky za použití programu, pro ukončení stiskni libovolnou klávesu.
```

Obrázek 4 – Ukázka rozkladu čísla na součin ireducibilních prvků

Obrázek výše ukazuje výstřižek z programu. Tato část kódu má na starost hlavní náplň celého programu, tj. cyklus se stará o postupné prohledávání prvků z přirozených čísel a hledá dělitele zadaného čísla, které jsou beze zbytku. Současně se program stará o výpis, který by v závěru u několika příkladů mohl vypadat stejně, jako vidíme na obrázku vlevo.

6. Kvadratické obory integrity

Uvažujme obor integrity **R**, jedná se obecně o množinu čísel, ve které jsou definovány základní početní operace, jako je sčítání, odčítání, násobení a dělení, a zachovává některé vlastnosti (jaké vlastnosti to jsou si lze připomenout v tabulce 1.2.). Kvadratické obory integrity nám umožňují rozšířit původní obory integrity o nové prvky, které nám neporušují již existující vlastnosti a operace.

Nové prvky často přidáváme v našem vlastním zájmu a to proto, abychom byli schopni provádět širší matematickou analýzu nebo pro možnost řešení rovnic, jako je třeba rovnice s kořeny v komplexní rovině čísel: $x^2 = -1$ (tj. kde je kořenem kvadratické rovnice imaginární jednotka i).

Kvadratický obor integrity je takový obor integrity **R**, který je rozšířen o prvky, které jsou kořeny kvadratické rovnice. Častěji se můžeme ovšem setkat s odlišným pojmem, který je v různých publikacích používán v podobném kontextu, ale přesto se jedná o konkrétněji zavedený pojem. Zde je potřeba upozornit na možnou záměnu pojmu s již definovaným pojmem **Gaussův obor integrity**, jehož definici si lze přečíst v kapitole 5.1.

Definice:

Uvažujme množinu $\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$ a za operace v $\mathbb{Z}[i]$ uvažujme zúžení operací sčítání a násobení na $\mathbb{Z}[i]$. Potom $(\mathbb{Z}[i], +, \cdot)$ je obor integrity – **obor integrity celých Gaussových čísel**. Jednotkami jsou prvky -1, 1, i a -i. (Blažek, a další, 1984 stránky 103-104)

Z definice uvedené výše je patrné, že Kvadratický obor integrity je obecnější pojem, který umožňuje rozšířit obor integrity o nové prvky, které jsou kořeny konkrétní kvadratické rovnice, kdežto obor integrity celých Gaussových čísel se již konkrétní aplikace, která rozšiřuje celá čísla o prvek „i“, který je kořenem kvadratické rovnice $x^2 = -1$.

Jednotky v oboru integrity Gaussových celých čísel $\mathbb{Z}[i]$ jsou prvky, které mají multiplikativní inverzi v tomto oboru. Pokud se bavíme o $\mathbb{Z}[i]$, potom jsou z definice jednotkami prvky 1, -1, i a -i.

Pro obě čísla 1, -1 platí, že mají v oboru $\mathbb{Z}[i]$ multiplikativní inverzi, tj. $1 \cdot 1 = 1$ a zároveň $(-1) \cdot (-1) = 1$. Pro oba prvky i, -i platí v principu totéž, tj. pokud vynásobíme prvky i a -i, získáme prvek 1 (z principu $i^2 = -1$). Po výměně pozic prvků i a -i získáváme i poslední jednotku v podobě -i.

Uvažujme, že prvek a + bi je prvkem oboru integrity Gaussových celých čísel $\mathbb{Z}[i]$. Jsou-li dány tyto konkrétní jednotky v oboru $\mathbb{Z}[i]$, potom rozklad na třídy asociovaných prvků obsahuje množinu $\{0\}$ a pro další nenulové prvky obsahuje množiny v následujících tvarech:

1. $a + bi$, tj. prvek je vynásoben jednotkou 1.
2. $-a - bi$, tj. prvek je vynásoben jednotkou -1.
3. $-b + ai$, tj. prvek je vynásoben jednotkou i.
4. $b - ai$, tj. prvek je vynásoben jednotkou -i.

Příklad:

Buď dán obor integrity celých Gaussových čísel $(\mathbb{Z}[i], +, \cdot)$. Ukažme, že je to euklidovský obor integrity. (Hora, 1991 stránky 71-72)

Poznámka: Přestože se bavíme o formulaci zadání příkladu, jedná se ve skutečnosti o větu, jejímž řešením je důkaz. V tomto konkrétním případě lze tedy ekvivalentně nahradit termíny „příklad" a „věta", stejně tak je možné zaměňovat pojmy „řešení" a „důkaz".

Řešení:

Abychom dokázali, že je obor integrity Gaussových celých čísel euklidovský, musíme dokázat, že ke každému prvku a jsme schopni přiřadit takové celé nezáporné číslo n(a), že:

1. Jestliže a | b a b je nenulové, potom $n(a) \leq n(b)$.

2. Ke každým dvěma nenulovým prvkům a, b z oboru integrity existují prvky q, r takové, že a = bq + r, kde r = 0 nebo n(r) < n(b).

Na prvek a je třeba se nyní dívat jako na prvek a + bi, kde a, b jsou celá čísla a i je imaginární jednotka. Euklidovskou normu prvku n(a + bi) položme rovnu $a^2 + b^2$, čímž nepochybně přiřadíme prvku nezáporné celé číslo. Řekněme, že a+bi | x+yi, tedy existuje nějaký prvek c+di, pro který platí, že (a+bi)(c+di)=x+yi.

Euklidovská norma je nicméně nezáporné celé číslo a u prvků jsme předem vyloučili, že by se norma rovnala nule, je proto z rovnice patrné, že $n(a + bi) \leq n(x + yi)$, čímž jsme dokázali bod č. 1 v definici euklidova oboru integrity.

Zaměřme se na druhý bod definice. Předpokládejme existenci dvou nenulových prvků z oboru integrity, ke kterým chceme nalézt prvky q, r takové, že a = bq + r, přičemž r je buď nulové nebo n(r) < n(b).

Vyjádřeme si tedy dva prvky $\mathbb{Z}[i]$ jako $a = a_1 + a_2 i$ a $b = b_1 + b_2 i$, kde a_1, a_2, b_1 a b_2 jsou celá čísla.

Platí, že a = bq + r, tedy po přepisu zároveň platí: $a_1 + a_2 i = (b_1 + b_2 i)q + r$.

Předpokládejme, že prvky q a r lze opět rozepsat podobným způsobem jako $q_1 + q_2 i$ a obdobně zbytek jako $r_1 + r_{2^i}$. Po dosazení do rovnice lze získat vyjádření a_1 a a_2 v tomto znění:

$$a_1 = b_1 q_1 - b_2 q_2 + r_1$$

$$a_2 = b_1 q_2 + b_2 q_1 + r_2$$

Zvolíme q_1 takové, aby $b_1 q_1$ bylo nejbližší menší nebo rovné a_1, dále zvolíme q_2 takové, aby $b_2 q_2$ bylo nejbližší menší nebo rovné a_2. Tedy můžeme zapsat, že $q_1 = a_1 / b_1$ a druhý prvek $q_2 = a_2 / b_2$. Po dosazení do rovnic výše a vyjádření zbytků r_1 a r_2 zjišťujeme, že jsou oba prvky celá čísla. Nalezli jsme tedy hodnoty prvků q a r takové, že a = bq + r.

Připomeňme Euklidův algoritmus a také program na nalezení největšího společného dělitele z kapitoly 3.1. Chceme-li nalézt největšího společného dělitele dvou prvků například v celých nebo přirozených číslech, potom je program plně funkční a dle postupu Euklidova algoritmu jej nalezne. V případě nalezení největšího společného dělitele dvou prvků v oboru integrity celých Gaussových číslech nám program selže, neboť je prvkem komplexní číslo. Je tedy na místě si položit otázku, jakým způsobem lze nalézt NSD dvou prvků v takovém oboru integrity, jakým jsou právě celá Gaussova čísla.

Zadejme si proto příklad právě z výše zmíněného oboru integrity a osvětleme tento specifický případ řešení. Postup řešení takového příkladu uvádí například autor v Algebra I. (Hora, 1991 str. 74).

Příklad:

Nalezněte největšího společného dělitele dvou prvků a, b v oboru integrity celých Gaussových čísel, platí-li že $a = 12 - 16i$ a prvek $b = 10 + 2i$.

Dle principu autora je nejprve potřeba nalézt podíl obou prvků a a b v oboru integrity celých Gaussových čísel. Tento podíl lze vyjádřit jako součet reálné a imaginární části. Důležité je, že existují celá čísla q_1 a q_2 taková, že absolutní hodnota součtu reálné části (resp. imaginární části) a q_1 (resp. q_2) je menší nebo rovna jedné polovině.

Nyní, když známe tato dvě čísla q_1 a q_2, můžeme ze vzorce dopočítat lehce zbytek r. Připomeňme tedy vztah $a = bq + r$. V tomto vztahu je potřeba chápat prvek q jako součet q_1 a q_2, a protože prvky dávají v součinu s reálnou a imaginární částí opět reálné a komplexní číslo, tak je prvek q komplexním číslem. Z Euklidova algoritmu vyplývá, je-li zbytek r nulový, potom je b největším společným dělitelem. Může ovšem nastat případ (také je v praxi častější), že je zbytek r nenulový a tím pádem pokračujeme v Euklidově algoritmu s novým podílem b/r, a tudíž i hledání nových prvků q_3 a q_4, popř. hledání nových zbytků.

Řešení:

$$\frac{a}{b} = \frac{12 - 16i}{10 + 2i} = \frac{(12 - 16i) \cdot (10 - 2i)}{104} = \frac{-88 - 184i}{104} = \frac{-88}{104} - \frac{184}{104}i$$

q = 1 - 2i

$$r = 12 - 16i - (10 + 2i)(1 - 2i) = -2 + 2i$$

$$\frac{b}{r} = \frac{10 + 2i}{-2 + 2i} = \frac{-16 - 24i}{8} = -2 - 3i$$

Největším společným dělitelem je tedy -2-3i.

Poznámka: Tento postup, jakkoli se zdá poměrně přímočarý, může být velice zdlouhavý. Musíme počítat s tím, že se jedná o aproximaci a neustále se tak přibližujeme k nějaké hodnotě prvků q, které mohou určit NSD beze zbytku, ale také nemusí. Pro názornou ukázku stačí prohodit libovolné číslo u výše zmíněného příkladu a můžeme se dostat i na desítky iterací, než dojdeme k dělení beze zbytku.

7. Obory integrity polynomů

Kvalitní úvod do problematiky oborů integrity polynomů poskytuje kniha Algebra – polynomy a rovnice (Drábek, a další, 2001 stránky 4-5). Tři počáteční definice byly převzaty z tohoto výtisku. První z nich se vztahuje k definování pojmu „polynom“ v oborech integrity. Druhá definice stanovuje pravidla pro rovnost dvou polynomů a třetí definice určuje součet a součin dvou polynomů.

Definice:

Budiž (I; +, .) obor integrity a n přirozené číslo. Funkci **f(x)** definovanou předpisem

$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, kde $a_n \neq 0$, nazýváme **polynomem n-tého stupně o jedné proměnné nad oborem integrity (I; +, .)**. Prvky a_n, a_{n-1}, …, a_1, a_0 z oboru integrity (I; +, .) nazýváme koeficienty polynomu. Pod polynomem 0-tého stupně rozumíme polynom f(x) = 0, který budeme značit o(x), nemá stupeň.

Definice:

Dva polynomy f(x) a g(x) se sobě rovnají nad oborem integrity (I; +, .), zapisujeme f(x) = g(x), právě tehdy, když pro všechny prvky a z oboru integrity I je f(a) = g(a).

Z praxe je pro čtenáře pravděpodobně intuitivní, že součtem (resp. součinem) polynomů vzniká nový polynom. Tato skutečnost je prakticky demonstrována během základního a středního školního vzdělávání. Nicméně, pro účely této práce si definujme proces vzniku těchto polynomů a jejich obecnou podobu. V případě definice součtu dvou polynomů využíváme principu vytýkání proměnných o stejné mocnině, proto je zde logický předpoklad rovnosti stupně polynomů.

Definice:

Nad oborem integrity (I; +, .) budiž dány polynomy

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, kde $a_n \neq 0$, a

$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$, kde $b_m \neq 0$

Součinem těchto polynomů, zapisujeme $f(x) \cdot g(x)$, rozumíme polynom $c_{n+m} x^{n+m} + + \cdots + c_k x^k + \cdots + c_1 x + c_0$, kde $c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_{k-1} b_1 + a_k b_0 = \sum_{1=0}^{k} a_i b_{k-i}$

Součtem těchto polynomů (poznámka: m=n, viz odstavec výše), zapisujeme f(x) + $+g(x)$, budeme rozumět polynom $(a_n + b_n)x^n + (a_{n-1}b_{n-1})x^{n-1} + \cdots + (a_1 + b_1)x +$ $+(a_0 + b_0)$

Autoři knihy (Drábek, a další, 2001 stránky 4-5) dále poskytují čtenáři cvičení spojené s definicemi. Tato cvičení navazují na to, že polynom je definovaný nad oborem integrity, tj. vlastnosti oborů integrity se do něj plně promítají. Nějaká tato cvičení jsou řešena v rámci práce.

Příklad:

Dokažte, že sčítání polynomů definované výše je komutativní, asociativní a že nulový polynom o(x) je neutrálním prvkem vůči sčítání polynomů.

Řešení:

1. Komutativita

Chceme-li dokázat existenci vlastnosti komutativity, je potřeba nalézt součty polynomů f(x)+g(x) a g(x)+f(x) a následně dokázat, že výsledky jsou si rovny. Vzhledem k tomu, že reálná čísla (resp. koeficienty polynomů) jsou komutativní na sčítání, tak lze přeuspořádat i výsledné součty dvou polynomů a získat tak stejný výsledek. Závěr tedy zní, že součet polynomů je komutativní.

2. Asociativita

Mějme polynomy f(x), g(x) a h(x) o stupních polynomů n, m a k. Chceme dokázat platnost vztahu $\big(f(x) + g(x)\big) + h(x) = f(x) + \big(g(x) + h(x)\big)$. Můžeme postupovat obdobně jako u prvního bodu při důkazu komutativity, tedy zjistíme výsledky obou stran rovnice a vzájemně porovnáme.

3. Neutrální prvek o(x)

Mějme polynom f(x) o stupni k a nulový polynom o(x). Chceme dokázat, že o(x) je neutrálním prvkem vzhledem k sčítání polynomů. Spočítáme součet f(x) + o(x). Nulový polynom neobsahuje žádné nenulové členy, takže se při sčítání s f(x) žádný člen výrazu nezmění. Výsledkem je tedy opět f(x). Stejný výsledek dostaneme i při součtu o(x) + f(x). Z toho vyplývá, že polynom o(x) je neutrálním prvkem vzhledem k sčítání polynomů.

Věta:

Jestliže (R, +, .) je oborem integrity, pak též (R[x], +, .) je oborem integrity. (Hora, 1991 str. 77)

Důkaz:

K důkazu je potřeba dokázat základní vlastnosti operace sčítání v R[x]. Konkrétně je potřeba dokázat uzavřenost, tedy že součet dvou polynomů R[x] je opět polynomem R[x]:

Abychom dokázali uzavřenost na sčítání, postupujeme následujícím způsobem: sčítáme příslušné mocninné členy a jejich koeficienty. Každý získaný koeficient je součtem dvou prvků z oboru integrity R, což zajišťuje, že je opět prvkem oboru integrity R. Takto získané koeficienty sestavíme do nového polynomu, který je tedy polynomem s koeficienty z R. Tedy operace sčítání je uzavřená v oboru polynomů R[x].

Dále je potřeba dokázat komutativitu, asociativitu a existenci neutrálního prvku na sčítání, což bylo dokázáno realizováním cvičení z Algebry – polynomy a rovnice (Drábek, a další, 2001 stránky 4-5). Zároveň jsme završili důkazy spojené s operací sčítání na oboru integrity R.

Zbývá dokázat, že součin dvou polynomů R[x] je opět polynomem R[x], komutativitu vzhledem k součinu polynomů, asociativitu k součinu polynomů a distributivitu.

Předpokládáme dva polynomy f(x) a g(x) z R[x]. Chceme dokázat, že jejich součin $f(x) \cdot g(x)$ je opět polynom z R[x]. Postupujeme tak, že násobíme jednotlivé členy polynomů f(x) a g(x) a poté sčítáme členy se stejnými mocninami x. Získáme tak koeficienty nového polynomu, který je polynomem s koeficienty z R. Každý koeficient je součinem dvou prvků z R, což zajišťuje, že je opět prvkem R. Sestavíme takto získané koeficienty do nového polynomu, který je polynomem s koeficienty z R. Tím jsme dokázali, že součin polynomů f(x) * g(x) je opět polynom z R[x]. Tudíž je operace součinu uzavřená v oboru polynomů R[x].

Pro důkaz komutativity násobení polynomů $f(x) \cdot g(x)$ je třeba vzít v úvahu, že pro každý člen polynomu $f(x) \cdot g(x)$ lze pozměnit pořadí násobení. Poté můžeme využít důkazu komutativity na sčítání polynomů (viz příklad výše) a aplikovat ho na jednotlivé členy výrazu $f(x) \cdot g(x)$. Tímto způsobem dokážeme, že výsledky obou výrazů $f(x) \cdot g(x)$ a $g(x) \cdot f(x)$ jsou si rovny.

U důkazu asociativity násobení polynomů $f(x) \cdot \big(g(x) \cdot h(x)\big) = (f(x) \cdot g(x)) \cdot h(x)$ postupujeme obdobně jako u důkazu asociativity na sčítání polynomů. Nejprve aplikujeme asociativitu sčítání na součin $g(x) \cdot h(x)$. Poté využijeme asociativity ze sčítání a aplikujeme ji na výrazy obě strany rovnice (zbavíme se závorek), abychom dokázali jejich rovnost.

Na závěr nám chybí důkaz distributivity násobení vzhledem ke sčítání. Předpokládáme, že máme tři polynomy f(x), g(x) a h(x) z oboru integrity R[x]. Na levé straně rovnice máme f(x) vynásobené výrazem $g(x) + h(x)$. Na pravé straně rovnice máme součet dvou výrazů $f(x) \cdot g(x)$ a $f(x) \cdot h(x)$. Porovnáním rozepsaných výrazů na obou stranách rovnice vidíme, že se shodují.

Vzhledem k tomu, že obor integrity polynomů R[x] je vlastnostmi definovaný oborem integrity R, vychází z této relace mezi nimi řada vlastností, tj. že obor integrity polynomů nad R spoustu vlastností zdědí. Jednou takovou vlastností je právě i existence jednotkových prvků. Následující informace pochází z knihy Algebra I. (Hora, 1991 stránky 77-79).

Věta:

Buď R obor integrity. Pak jednotky v oboru integrity R[x] jsou právě všechny jednotky v oboru integrity R.

Věta:

Jestliže R je komutativní těleso, potom R[x] je euklidovský obor integrity. Euklidovskou funkcí je přitom stupeň polynomu.

Obzvláště zajímavým důsledkem této věty je fakt, že obor integrity R[x] je oborem integrity polynomů, které mají jednoznačný rozklad na ireducibilní prvky. To znamená, že každý polynom z R[x] může být vyjádřen jako součin ireducibilních polynomů, přičemž tento rozklad je jednoznačný. Tento důsledek nám umožňuje provádět další závěry, jak uvádí autor ve své následné větě, která navazuje na tuto skutečnost.

Věta:

Je-li R oborem integrity s jednoznačným rozkladem, pak i R[x] je Gaussův obor integrity.

Závěr

V první kapitole této práce je věnován prostor představení algebraických struktur. Při studiu jednotlivých definic se můžeme setkat s určitými nepřesnostmi, které je důležité vzít v úvahu při dalším studiu. Tato kapitola zavádí algebraické struktury a představuje jejich základní vlastnosti, které jsou zde také definovány a objasněny. Na konci kapitoly je nám představen pojem "obor integrity" spolu s jeho definicí, vlastnostmi a významnými větami a důkazy. Tento pojem je zde zkoumán s větší pozorností z důvodu jeho širšího výzkumu.

Druhá kapitola se zaměřuje na dělitelnost v oborech integrity a přináší základní pojmy, které vycházejí z předchozích studií. Na základě těchto předchozích znalostí jsou následně představeny přesné definice jednotlivých pojmů. Kapitola dále představuje společné násobky, společné dělitele a zejména se zaměřuje na největší společné dělitele a nejmenší společné násobky. Pro lepší pochopení těchto konceptů jsou představeny jednoduché příklady, které nás postupně přivádějí k metodám hledání největšího společného dělitele. Tato problematika je pak podrobněji rozebrána v následující kapitole.

Třetí kapitola se zaměřuje na postup hledání největšího společného dělitele. Je zde uveden pojem Euklidův algoritmus a popsán jeho princip fungování na konkrétních příkladech. V této kapitole byly využity informační a komunikační technologie (ICT), a algoritmus byl adekvátně přepracován do podoby textového programu, který slouží k hledání největšího společného dělitele dvou prvků.

Další kapitola se zaměřuje na hlavní předmět této práce, kterým je euklidovský obor integrity. Stejně jako v předchozích kapitolách, i zde jsou nejprve představeny základní definice, na kterých je postaveno. Následně jsou představeny věty, jejichž důsledky jsou důkladněji vysvětleny. Kapitola je obohacena o případné důkazy těchto vět a také o několik dalších příkladů, které slouží k lepšímu pochopení tématu.

Následující kapitola se zabývá Gaussovým oborem integrity, který je představen jako další pojem. Vedle definic, vět a důkazů je v této kapitole kladen důraz na zkoumání vztahu mezi Gaussovým oborem integrity a euklidovým oborem integrity.

Poslední dvě kapitoly jsou věnovány kvadratickým oborům integrity a oborům integrity polynomů. Tyto kapitoly mají za cíl sjednotit poznatky z předchozích kapitol. Jsou zde prezentovány důkazy vět a příklady, které podtrhávají význam těchto kapitol a zároveň i hlavní cíl celé práce.

Resumé

Tato diplomová práce se zabývá obory integrity a jejich dělitelností. Jedním z cílů je představení Euklidova algoritmu jako klíčovou metodu pro hledání největšího společného dělitele. V první kapitole jsou představeny základní pojmy algebraických struktur, binárních operací a oborů integrity. Následující kapitoly pak rozvíjejí tyto definice a zaměřují se na specifické obory integrity, jako jsou euklidovské obory integrity, gaussovy obory integrity, kvadratické obory integrity a obory integrity polynomů. Důraz je kladen na dělitelnost, která je podrobněji prozkoumána v úvodních kapitolách o Euklidově algoritmu a dělitelnosti v oborech integrity. Zvláštní důraz je věnován praktické aplikaci poznatků prostřednictvím představení algoritmu pro hledání největšího společného dělitele. Celkově tedy tato práce poskytuje komplexní přehled o oborech integrity a jejich dělitelnosti s důrazem na praktické využití.

Summary

This master's thesis focuses on domains of integrity and their divisibility. One of the objectives is to introduce Euclid's algorithm as a key method for finding the greatest common divisor. The first chapter presents the basic concepts of algebraic structures, binary operations, and domains of integrity. Subsequent chapters develop these definitions and focus on specific domains of integrity, such as Euclidean domains of integrity, Gaussian domains of integrity, quadratic domains of integrity, and domains of integrity of polynomials. Emphasis is placed on divisibility, which is examined in more detail in the introductory chapters on Euclid's algorithm and divisibility in domains of integrity. Special attention is given to the practical application of knowledge through the introduction of an algorithm for finding the greatest common divisor. Overall, this work provides a comprehensive overview of domains of integrity and their divisibility with an emphasis on practical applications

Citovaná literatura

Blažek, Jaroslav, Koman, Milan a Vojtášková, Blanka. 1984. *Algebra a teoretická aritmetika.* Praha : Státní pedagogické nakladatelství Praha, 1984. 56-02-11/II/1..

Drábek, CSc. RNDr. Jaroslav a Hora, CSc. RNDr. Jaroslav. 2001. *Algebra. Polynomy a rovnice.* Plzeň : Západočeská univerzita v Plzni, 2001. ISBN 80-7082-787-4.

Drábek, RNDr. Jaroslav, a další. 1985. *Základy elementární aritmetiky pro učitelství 1. stupně ZŠ.* Praha : Státní pedagogické nakladatelství Praha, 1985.

Hora, CSc. RNDr. Jaroslav. 1991. *Algebra I.* Plzeň : Pedagogická fakulta v Plzni, 1991.

Katedra didaktiky matematiky. 2010-2023. Základní poznatky z matematiky. *www.karlin.mff.cuni.cz.* [Online] Matematicko-fyzikální fakulta, Univerzita Karlova v Praze, 2010-2023. [Citace: 8. 3 2023.] https://www2.karlin.mff.cuni.cz/~portal/mocniny/?page=Ciselne_obory.

Procházka, Ladislav, a další. 1990. *Algebra.* Praha : Academia Praha, 1990. ISBN 80-200-0301-0.

Seznam tabulek a obrázků

Poznámka: Všechny tabulky i obrázky jsou znovu k nahlédnutí v přílohách níže.

Přílohy

Komutativnost	Na operaci □ (sčítání)	x □ y = y □ x
	Na operaci ○ (násobení)	x ○ y = y ○ x
Asociativnost	Na operaci □ (sčítání)	x □ (y □ z) = (x □ y) □ z
	Na operaci ○ (násobení)	x ○ (y ○ z) = (x ○ y) ○ z
Neutrální prvek (oboustranný)	Vzhledem k □ (sčítání)	n □ x = x □ n = x
	Vzhledem k ○ (násobení)	n ○ x = x ○ n = x
Agresivní prvek (oboustranný)	Vzhledem k □ (sčítání)	a □ x = x □ a = a
	Vzhledem k ○ (násobení)	a ○ x = x ○ a = a
Distributivnost (zleva)	□ vzhledem k ○ (sčítání vzhledem k násobení)	x □ (y ○ z) = (x □ y) ○ (x □ z)
	○ vzhledem k □ (násobení vzhledem ke sčítání)	x ○ (y □ z) = (x ○ y) □ (x ○ z)

Tabulka 1. – Přehled vlastností binárních operací

Algebraická struktura	**Vlastnosti příslušné binární operace**				
	uza	**aso**	**kom**	**neu**	**agr**
Grupoid	Ano	Ne	Ne	Ne	Ne
Komutativní grupoid	Ano	Ne	Ano	Ne	Ne
Pologrupa	Ano	Ano	Ne	Ne	Ne
Komutativní pologrupa	Ano	Ano	Ano	Ne	Ne
Grupa	Ano	Ano	Ne	Ano	Ano
Abelova grupa	Ano	Ano	Ano	Ano	Ano
Kvazigrupa	Ano	Ne	Ne	Ne	Ano
Komutativní kvazigrupa	Ano	Ne	Ano	Ne	Ano
Lupa	Ano	Ne	Ne	Ano	Ano
Komutativní lupa	Ano	Ne	Ano	Ano	Ano
Monoid	Ano	Ano	Ne	Ano	Ne
Komutativní monoid	Ano	Ano	Ano	Ano	Ne

Tabulka 2 – Přehled vlastností různých algebraických struktur s jednou binární operací

Algebraická struktura	Binární operace □ (sčítání)	Binární operace ○ (násobení)	Distributivita	Obsahuje dělitele nuly
Polookruh	Komutativní pologrupa	Pologrupa	Ano	Ano
Komutativní polookruh	Komutativní pologrupa	Komutativní pologrupa	Ano	Ano
***Okruh**	Abelova grupa	Pologrupa	Ano	Ano
***Komutativní okruh**	Abelova grupa	Komutativní pologrupa	Ano	Ano
Obor integrity	Abelova grupa	Komutativní pologrupa	Ano	Ne
Těleso	Abelova grupa	Grupa	Ano	Ne
Komutativní těleso	Abelova grupa	Abelova grupa	Ano	Ne

Tabulka 3 – Přehled vlastností různých algebraických struktur se dvěma binárními operacemi

```
//Výpočet, ověření a výpis
int x = cislo1;
int y = cislo2;
while (y != 0)
{
    int podil = calculator.VratPodil(x, y);
    int zbytek = calculator.VratZbytek(x, y);
    calculator.VypisVysledek(x, y);
    x = y;
    y = zbytek;
    if (y == 0)
    {
        Console.WriteLine();
        Console.WriteLine("Závěr: Největším společným dělitelem zadaných čísel {0} a {1} je číslo {2}.", cislo1, cislo2, x);
    }
}
```

Obrázek 1 – Úsek kódu pro zjištění NSD dvou zadaných přirozených čísel

```
Zadej mi 1. číslo
175
Zadej mi 2. číslo
245

245 = 175*1 + 70
175 = 70*2 + 35
70 = 35*2 + 0

Závěr: Největším společným dělitelem zadaných čísel 245 a 175 je číslo 35.
Přeješ si zadat nový příklad? a/n
```

Obrázek 2 – Ukázka běhu programu na zjištění NSD

```
//Vnitřní cyklus vypisování ireducibilních prvků
for (int i = 2; i <= cislo; i++)
{
    if (cislo % i == 0)
    {
        soucin_prvocisel = soucin_prvocisel + " " + i;
        soucin_prvocisel = soucin_prvocisel.Trim();
        cislo = cislo / i;
        i = 1;
        if (cislo != zaklad)
            Console.WriteLine(cislo.ToString() + " * " + soucin_prvocisel.Replace(" ", " * "));
        else
            Console.WriteLine(soucin_prvocisel.Replace(" ", " * "));
    }
}
```

Obrázek 3 – Cyklus rozkládání čísla na ireducibilní prvky

```
Zadej mi libovolné celé číslo.
128
64 * 2
32 * 2 * 2
16 * 2 * 2 * 2
8 * 2 * 2 * 2 * 2
4 * 2 * 2 * 2 * 2 * 2
2 * 2 * 2 * 2 * 2 * 2 * 2
1 * 2 * 2 * 2 * 2 * 2 * 2 * 2
Přeješ si zadat nový příklad? a/n
a
Zadej mi libovolné celé číslo.
255
85 * 3
17 * 3 * 5
1 * 3 * 5 * 17
Přeješ si zadat nový příklad? a/n
a
Zadej mi libovolné celé číslo.
68
34 * 2
17 * 2 * 2
1 * 2 * 2 * 17
Přeješ si zadat nový příklad? a/n
n
Díky za použití programu, pro ukončení stiskni libovolnou klávesu.
```

Obrázek 4 – Ukázka rozkladu čísla na součin ireducibilních prvků

Kompletní kód programu na nalezení NSD dvou prvků

Třída program

```
//Založení instancí a proměnných
Calculator calculator = new Calculator();
int cislo1;
int cislo2;
bool chce_pokracovat = true;

//Začátek hlavního cyklu
while (chce_pokracovat)
{
  //Zadávání vstupních proměnných
  Console.WriteLine("Zadej mi 1. číslo");
  while (!int.TryParse(Console.ReadLine(), out cislo1))
    Console.WriteLine("Zadej prosím přirozené číslo.");
  Console.WriteLine("Zadej mi 2. číslo");
  while (!int.TryParse(Console.ReadLine(), out cislo2))
    Console.WriteLine("Zadej prosím přirozené číslo.");
  Console.WriteLine();

  //Prohazovač
  if (cislo1 < cislo2)
  {
    int prohazovac = cislo2;
    cislo2 = cislo1;
    cislo1 = prohazovac;
  }

  //Výpočet, ověření a výpis
  int x = cislo1;
  int y = cislo2;
  while (y != 0)
  {
    int podil = calculator.VratPodil(x, y);
    int zbytek = calculator.VratZbytek(x, y);
    calculator.VypisVysledek(x, y);
    x = y;
    y = zbytek;
    if (y == 0)
    {
    Console.WriteLine();
    Console.WriteLine("Závěr: Největším společným dělitelem zadaných čísel {0} a {1} je
číslo {2}.", cislo1, cislo2, x);
    }
  }

  //Ošetření hlavního cyklu
  bool zadal_spatne = true;
  while (zadal_spatne)
  {
    Console.WriteLine("Přeješ si zadat nový příklad? a/n");
    string vstup = Console.ReadLine().Trim().ToLower();
    switch (vstup)
```

```
            {
              case "a":
                Console.Clear();
                zadal_spatne = false;
                chce_pokracovat = true;
                break;
              case "n":
                Console.Clear();
                zadal_spatne = false;
                chce_pokracovat = false;
                break;
              default:
                zadal_spatne = true;
                chce_pokracovat = true;
                break;
            }
          }
        }

        //Ukončování
        Console.WriteLine("Díky za použití programu. Pro ukončení stiskněte libovolnou klávesu.");
        Console.ReadKey();
```

Třída Calculator

```
        class Calculator
        {
          public void VypisVysledek(int cislo1, int cislo2)
          {
          Console.WriteLine("{0} = {1}*{2} + {3}", cislo1, cislo2, VratPodil(cislo1, cislo2),
VratZbytek(cislo1, cislo2));
          }
          public int VratPodil(int cislo1, int cislo2)
          {
            int podil = cislo1 / cislo2;
            int zbytek = cislo2 - cislo2 * podil;
            return podil;
          }
          public int VratZbytek(int cislo1, int cislo2)
          {
            int podil = VratPodil(cislo1, cislo2);
            int zbytek = cislo1 - cislo2 * podil;
            return zbytek;
          }
        }
```

Kompletní kód programu na rozklad na součin ireducibilních prvků

```
//Cyklus nad programem
bool pokracovat = true;
while (pokracovat)
{
  //Vstupní data
  Console.WriteLine("Zadej mi libovolné celé číslo.");
  int cislo;
  while (!int.TryParse(Console.ReadLine().Trim(), out cislo))
    Console.WriteLine("Nesprávné zadání.");
  string soucin_prvocisel = "";
  string soucin_zbytku = "";
  int zaklad = cislo;

  //Vnitřní cyklus vypisování ireducibilních prvků
  for (int i = 2; i <= cislo; i++)
  {
    if (cislo % i == 0)
    {
      soucin_prvocisel = soucin_prvocisel + " " + i;
      soucin_prvocisel = soucin_prvocisel.Trim();
      cislo = cislo / i;
      i = 1;
      if (cislo != zaklad)
        Console.WriteLine(cislo.ToString() + " * " + soucin_prvocisel.Replace(" ", " * "));
      else
        Console.WriteLine(soucin_prvocisel.Replace(" ", " * "));
    }
  }

  //Cyklus ověřující správnost zadání
  bool spatne = true;
  while (spatne)
  {
    Console.WriteLine("Přeješ si zadat nový příklad? a/n");
    switch (Console.ReadLine().Trim().ToLower())
    {
      case "a":
        spatne = false;
        pokracovat = true;
        break;
      case "n":
        spatne = false;
        pokracovat = false;
        break;
      default:
        spatne = true;
        pokracovat = true;
        break;
    }
  }
}
Console.WriteLine("Díky za použití programu, pro ukončení stiskni libovolnou klávesu.");
Console.ReadKey();
```