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

PŘÍKLADY NA DĚLITELNOST V OBORECH INTEGRITY

BAKALÁŘSKÁ PRÁCE

Stanislav Hefler

Přírodovědná studia, obor Matematická studia

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

Plzeň, 2013

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

V Plzni, 10. dubna 2013

.....

vlastnoruční podpis

Děkuji mému vedoucímu bakalářské práce Doc. RNDr. Jaroslavu Horovi, CSc., za jeho cenné rady, připomínky a metodické vedení práce.

OBSAH

ÚVOD

Tato bakalářská práce se zabývá tématem dělitelnosti v oborech integrity. Obory integrity spadají do matematické disciplíny algebra, kterou se zabývají matematické osobnosti od nepaměti. Mezi nejvýznamnější matematiky řešící problematiku oborů integrity patřili v neposlední řadě Johann Carl Friedrich Gauss a Euklidés z Alexandrie, po kterých jsou pojmenovány nejvýznamnější skupiny oborů integrity.

V této práci najdeme vymezení pojmů oborů integrity, zpracované příklady dělitelnosti v oborech integrity a ukázky speciálních oborů integrity. Pro svoji práci jsem vybral Gaussovy a Euklidovy obory integrity.

Hlavním tématem této práce je dělitelnost a ta souvisí s pojmy největší společný dělitel a nejmenší společný násobek. Proto je těmto pojmům věnována největší část mé práce. Pro zajímavost jsem do své práce umístil ukázku výpočtu největšího společného dělitele a nejmenšího společného násobku v nejrozšířenějších matematických softwarech.

Práce je rozdělena na sedm kapitol, které obsahují praktickou a teoretickou část.

První kapitola se zabývá vymezením pojmu obor integrity.

V druhé kapitole najdeme definice základných pojmů souvisejících s obory integrity a dělitelností v nich.

Třetí kapitola je věnována Johannu Carlu Friedrichu Gaussovi a jeho oborům integrity.

Čtvrtá kapitola pojednává o Euklidovi z Alexandrie, Euklidovu algoritmu a Euklidových oborech integrity.

V páté kapitole najdeme příklady výpočtu největších společných dělitelů a nejmenších společných násobků pomocí Euklidova algoritmu v různých oborech integrity včetně prostoru polynomů.

Šestá kapitola je věnována oboru integrity nesplňujícímu podmínku konečnosti řetězce vlastních dělitelů, který tudíž není Gaussovým oborem integrity.

Poslední sedmá kapitola pojednává o oboru integrity, který nesplňuje podmínku existence největšího společného násobku a není Euklidovým oborem integrity. Navíc není ani Gaussovým oborem integrity.

1 OBOR INTEGRITY

Algebraickou strukturu $(\mathcal{I}; +, \cdot)$ nazýváme **oborem integrity** právě tehdy, když je komutativním okruhem, ve kterém neexistují netriviální dělitelé nuly. [Procházka, 1990]

Obor integrity je jedna z řady algebraických struktur, ve které jsou definovány dvě binární operace a to sčítání $(+)$ a násobení $(\cdot)$. Aby algebraická struktura byla oborem integrity, musí splňovat následující axiomy:

1) Komutativnost operace sčítání: $(\forall a, b \in \mathcal{I})$: $[a + b = b + a]$.
   Nezáleží na pořadí sčítanců.
2) Asociativnost operace sčítání: $(\forall a, b, c \in \mathcal{I})$: $[(a + b) + c = a + (b + c)]$.
   Nezáleží na pořadí provedených operací se sčítanci.
3) Existence neutrálního prvku e operace sčítání:
   $$(\forall a \in \mathcal{I}, \exists e \in \mathcal{I}): [a + e = e + a = a].$$
   Součtem libovolného prvku s neutrálním prvkem dostáváme původní prvek.
4) Existence inverzního prvku a^{-1} operace sčítání:
   $$(\forall a \in \mathcal{I}, \exists a^{-1} \in \mathcal{I}): [a + a^{-1} = a^{-1} + a = e].$$
   Součtem libovolnému prvku a prvku inverzního dostáváme prvek neutrální.
5) Komutativnost operace násobení: $(\forall a, b \in \mathcal{I})$: $[a \cdot b = b \cdot a]$.
   Nezáleží na pořadí činitelů.
6) Asociativnost operace násobení: $(\forall a, b, c \in \mathcal{I})$: $[(a \cdot b) \cdot c = a \cdot (b \cdot c)]$.
   Nezáleží na pořadí provedených operací s činiteli.
7) Distributivnost: $(\forall a, b, c \in \mathcal{I})$: $[(a + b) \cdot c = a \cdot c + b \cdot c]$.
   Možnost roznásobení sčítanců.
8) Neexistence netriviálních dělitelů nuly:
   $$(\forall a, b \in \mathcal{I}): [a \neq 0 \wedge b \neq 0 \Rightarrow a \cdot b \neq 0].$$
   Nulový součin můžeme získat pouze nulovými činiteli.

Příkladem oboru integrity je množina celých čísel $\mathbb{Z}$ vybavená operacemi sčítání a násobení.

Důkaz, že množina $\mathbb{Z}$ tvoří obor integrity, obecně neprovádíme. Ukážeme na náhodných numerických hodnotách, že splňuje 8 axiomů oboru integrity.

1) Komutativnost operace sčítání:

$$(\forall\, a, b \in \mathbb{Z}): (a + b = b + a\,)$$

$$\text{např. } 5 + 7 = 7 + 5 = 12.$$

2) Asociativnost operace sčítání:

$$(\forall\, a, b, c \in \mathbb{Z}):[(a + b) + c = a + (b + c)\,]$$

$$\text{např. } (3 + 4) + 6 = 3 + (4 + 6) = 13.$$

3) Existence neutrálního prvku e k operaci sčítání:

$$a + e = e + a = a$$

$$a + e = a \qquad /-a$$

$$\underline{\underline{e = 0}} \;\Rightarrow [\forall a \in \mathbb{Z}, \exists e \in \mathbb{Z}].$$

4) Existence inverzního prvku a^{-1} k operaci sčítání:

$$a + a^{-1} = a^{-1} + a = e$$

$$a^{-1} + a = 0 \qquad /-a$$

$$\underline{\underline{a^{-1} = -a}} \;\Rightarrow [\forall a \in \mathbb{Z}, \exists a^{-1} \in \mathbb{Z}].$$

Odtud vidíme, že inverzní prvek je prvek opačný.

5) Komutativnost operace násobení:

$$(\forall a, b \in \mathbb{Z}):(a \cdot b = b \cdot a)$$

$$\text{např. } 5 \cdot 7 = 7 \cdot 5 = 35.$$

6) Asociativnost operace násobení:

$$(\forall a, b, c \in \mathbb{Z}): [(a \cdot b) \cdot c = a \cdot (b \cdot c)]$$

$$\text{např. } (3 \cdot 4) \cdot 6 = 3 \cdot (4 \cdot 6) = 72.$$

7) Distributivnost:

$$(\forall a, b, c \in \mathbb{Z}): [(a + b) \cdot c = a \cdot c + b \cdot c]$$

$$\text{např. } (7 + 6) \cdot 5 = 7 \cdot 5 + 6 \cdot 5 = 65.$$

8) Neexistence netriviálních dělitelů nuly:

$$(\forall a, b \in \mathbb{Z}): (a \neq 0 \wedge b \neq 0) \Rightarrow a \cdot b \neq 0$$

$$\text{např. } 5 \cdot 7 \neq 0.$$

Dalším příkladem oboru integrity je fundamentální úplná soustava zbytků (FÚSZ) podle prvočíselného modulu $m = 5$ vzhledem ke sčítání a násobení.

2 DĚLITELNOST V OBORECH INTEGRITY

V této kapitole se budeme zabývat dělitelností v komutativních oborech integrity. **Komutativním oborem integrity** rozumíme netriviální komutativní a asociativní okruh $(\mathcal{O}; +, \cdot)$ bez dělitelů nuly a s jednotkovým prvkem. Je to tedy algebraická struktura, která splňuje následující axiomy:

1. Komutativnost operace sčítání: $(\forall a, b \in \mathcal{O})$: $[a + b = b + a]$.
2. Asociativnost operace sčítání: $(\forall a, b, c \in \mathcal{O})$: $[(a + b) + c = a + (b + c)]$.
3. Existence neutrálního prvku e operace sčítání:
$$(\forall a \in \mathcal{O}, \exists e \in \mathcal{O})\text{: } [a + e = e + a = a].$$
4. Existence inverzního prvku a^{-1}operace sčítání:
$$(\forall a \in \mathcal{O}, \exists a^{-1} \in \mathcal{O})\text{: } [a + a^{-1} = a^{-1} + a = e\ ].$$
5. Asociativnost operace násobení: $(\forall a, b, c \in \mathcal{O})$: $[\ (a \cdot b) \cdot c = a \cdot (b \cdot c)]$.
6. Distributivnost operace násobení:
$$(\forall a, b, c \in \mathcal{O})\text{: } [\ (a + b) \cdot c = a \cdot c + b \cdot c].$$
7. Komutativnost operace násobení: $(\forall a, b \in \mathcal{O})$: $[a \cdot b = b \cdot a]$.
8. Jednotkový prvek: $(\forall a \in \mathcal{O}, \exists j \in \mathcal{O})$: $[a \cdot j = a]$.

Oborem integrity rozumíme množinu prvků splňující výše uvedené axiomy a značíme jej I. Symbolem I^* pak rozumíme množinu **invertibilních prvků** oboru integrity I, kde invertibilním prvkem rozumíme prvek splňující vlastnost existence inverzního prvku vzhledem k operaci násobení, tedy

$$(\forall a \in I, \exists a^{-1} \in I)\text{: } [a \cdot a^{-1} = a^{-1} \cdot a = e].$$

Všechny invertibilní prvky okruhu I tvoří **multiplikativní grupu**, protože splují následující vlastnosti:

- Existence neutrálního prvku

  Z axiomů oboru integrity vyplývá, že v každém oboru integrity existuje neutrální prvek.
- Asociativita

  Z axiomů oboru integrity vyplývá, že v každém oboru integrity platí zákon asociativity.
- Existence inverzního prvku

  Z axiomů oboru integrity vyplývá, že v každém oboru integrity existuje inverzní prvek.

- Součin dvou invertibilních prvků je opět prvek invertibilní.
  Invertibilní prvek je takový prvek, ke kterému existuje prvek inverzní (operace násobení) a zároveň součinem takových prvků je prvek jednotkový (neutrální). Z axiomů oboru integrity plyne, že ke každému prvku v oboru integrity existuje prvek inverzní a proto i k součinu dvou invertibilních prvků musí existovat prvek inverzní.

O prvcích $a, b \in I$ říkáme, že **prvek $\boldsymbol{a}$ dělí prvek $\boldsymbol{b}$** nebo že je prvek b násobkem prvku a, existuje-li $c \in I$ takové, že $b = a \cdot c$. [Blažek, 1985]

Tuto skutečnost zapisujeme symbolem $\boldsymbol{a|b}$, čímž získáváme na množině I binární relaci dělitelnosti.

Relace dělitelnosti je reflexivní, antisymetrická a tranzitivní. Tvoří tedy neostré lineární uspořádání.

Důkaz, že relace dělitelnosti v $\mathbb{Z}$ tvoří neostré lineární uspořádání:

1) **Reflexivita**: $(\forall x \in \mathcal{M})$: (xRx) tj. x je v relaci s x.
   $$(\forall x \in \mathbb{Z}): (x|x)$$
   platí $\forall x \in \mathbb{Z} \Rightarrow$ je reflexivní.

2) **Symetričnost:** $(\forall x, y \in \mathcal{M}, x \neq y)$: $(xRy \Rightarrow yRx)$
   $$(\forall x, y \in \mathbb{Z}, x \neq y): (x|y \Rightarrow y|x).$$
   Neplatí, protože $2 \mid 6$ ale $6 \nmid 2 \Rightarrow$ není symetrická.
   Antisymetričnost: $(\forall x, y \in \mathcal{M}, x = y)$: $(xRy \Rightarrow yRx)$
   $$(\forall x, y \in \mathbb{Z}, x = y): (x|y \Rightarrow y|x).$$
   Platí $\forall x, y \in \mathbb{Z} \Rightarrow$ je antisymetrická.

3) **Tranzitivita**: $(\forall x, y, z \in \mathcal{M})$: $(xRy \wedge yRz \Rightarrow xRz)$
   $$(\forall x, y, z \in \mathbb{Z}): (x|y \wedge y|z \Rightarrow x|z)$$
   tj. $(x|y \wedge y|z) \Rightarrow y = ax \wedge z = by$, kde $(a, b \in \mathbb{Z}) \Rightarrow z = bax \Rightarrow x|z$.
   Platí $\forall x, y, z \in \mathbb{Z} \Rightarrow$ je tranzitivní.

Symbolem $\boldsymbol{a \nmid b}$ vyznačujeme, že prvek $\boldsymbol{a}$ **nedělí prvek $\boldsymbol{b}$**.

Prvky $a, b \in I$ jsou spolu **asociovány** $(\boldsymbol{a \parallel b})$, pokud platí $a|b$ a zároveň $b|a$.

Prvky asociované s jednotkovým prvkem 1 se nazývají **dělitelé jednotky**. Množinu všech dělitelů jednotky značíme $U(I)$.

Pokud je algebraická struktura I oborem integrity, potom platí:

1. Pro všechny prvky oboru integrity I platí, že $a|a$.
$$(\forall a \in I): (a|a)$$
2. Pro všechny prvky oboru integrity I platí, že $1|a$.
$$(\forall a \in I): (1|a)$$
3. Pro všechny prvky oboru integrity I platí $a|c$, pokud $a|b$ a $b|c$.
$$(\forall a, b, c \in I): [(a|b \wedge b|c) \Rightarrow a|c]$$
4. Existují prvky a a b oboru integrity I, že $a|b$, ale $b \nmid a$.
$$(\exists a, b \in I): (a|b \wedge b \nmid a)$$
5. Pro všechny prvky oboru integrity I platí $a|bc$, pokud $a|b$.
$$(\forall a, b, c \in I): (a|b \Rightarrow a|bc)$$
6. Pro všechny prvky oboru integrity I platí $a|bc$, pokud $a|b$ a $b|c$.
$$(\forall a, b, c \in I): [(a|b \wedge b|c) \Rightarrow a|bc]$$
7. Pro všechny prvky oboru integrity I platí, že $ac|bc$, pokud $a|b$ a $c \neq 0$.
$$(\forall a, b, c \in I): [(a|b \wedge c \neq 0) \Rightarrow ac|bc]$$

2.1 VLASTNÍ DĚLITEL, IREDUCIBILNÍ PRVEK A PRVOČINITEL

Prvek $a \in I$ se nazývá **vlastní dělitel** (triviální dělitel) prvku b, pokud $a|b, a \notin I^*$ a prvek a není asociován s prvkem b.

Ireducibilním prvkem nazýváme prvek $a \in I$, jestliže $a \neq 0$, $a \notin I^*$ a prvek a nemá žádné vlastní dělitele.

Prvek $a \in I$ se nazývá **prvočinitel**, pokud $a \neq 0$, $a \notin I^*$ a navíc pokud prvek a dělí součin, tak dělí alespoň jeden z činitelů.

2.2 SPOLEČNÝ DĚLITEL

Jsou-li $a_1, a_2, \dots, a_n$ libovolné prvky z I, nazývá se prvek $u \in I$ jejich **společným dělitelem**, právě když $u|a_1,\ u|a_2, \dots, u|a_n$.[Blažek, 1985]

Pod pojmem **největší společný dělitel** rozumíme prvek $x \in I$, který je společným dělitelem množiny $\mathcal{M}$ a navíc je dělen každým dalším společným dělitelem u množiny $\mathcal{M}$. Největšího společného dělitele množiny $\mathcal{M}$ značíme $x \in nsd(\mathcal{M})$, někdy též $x \in D(\mathcal{M})$.

$$[x = nsd(a_1, a_2, \dots, a_n)] \Rightarrow$$
$$\Big[(x|a_1, x|a_2, \dots, x|a_n) \wedge \big((\forall u \in \mathcal{M}): \big((u|a_1, u|a_2, \dots, u|a_n) \Rightarrow (u|x)\big)\big)\Big]$$

Množina $\mathcal{M}$ je jistá podmnožina nosné množiny oboru I.

2.2.1 PŘÍKLAD NEJVĚTŠÍHO SPOLEČNÉHO DĚLITELE

Najděte největšího společného dělitele čísel 1152 a 648.

$$nsd(1152, 648) = ?$$

$$1152 = \underline{2 \cdot 2 \cdot 2} \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot \underline{3 \cdot 3}$$

$$648 = \underline{2 \cdot 2 \cdot 2 \cdot 3 \cdot 3} \cdot 3 \cdot 3$$

$$nsd(1152, 648) = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = \underline{\underline{72}}$$

Největším společným dělitelem čísel 1152 a 648 je 72.

Tento postup nalezení největšího společného dělitele se používá na základních školách. Není ale příliš vhodný. Nejprve je totiž třeba nalézt prvočíselný rozklad obou čísel a to může být obecně velmi obtížné. Naštěstí existuje v daném případě mnohem efektivnější metoda výpočtu největšího společného dělitele (Euklidův algoritmus), kterou se budeme zabývat později.

2.3 NESOUDĚLNÉ PRVKY

Prvky $a, b \in I$ se nazývají **prvky nesoudělné**, právě když $nsd(a, b) = 1$. Prvky $a_1, a_2, \dots, a_n \in I$ nazveme nesoudělné, právě když $nsd(a_1, a_2, \dots, a_n) = 1$, a nazveme je prvky po dvou nesoudělné, právě když

$$(\forall i, j \in \{1, 2, \dots, n\}, i \neq j): [nsd(a_i, a_j) = 1].$$ [Blažek, 1985]

Nesoudělnými prvky jsou například prvočísla.

2.3.1 PŘÍKLAD NA NESOUDĚLNÁ ČÍSLA

Dokažte, že čísla 648 a 175 jsou nesoudělná, neboli že je jejich největší společný dělitel roven číslu 1. K výpočtu použijeme stejně jako výše prvočíselný rozklad.

$$nsd(648, 175) = ?$$

$$648 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 3$$

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

$$nsd(648, 175) = \underline{\underline{1}}$$

Největším společným dělitelem čísel 648 a 175 je 1. To dokazuje, že jsou nesoudělná.

2.4 SPOLEČNÝ NÁSOBEK

Jsou-li $a_1, a_2, \dots, a_n$ libovolné prvky z I, nazývá se prvek $v \in I$ jejich **společným násobkem**, právě když $a_1 | v, a_2 | v, \dots, a_n | v$. [Blažek, 1985]

To znamená, že společným násobkem prvků množiny $\mathcal{M}$ je takový prvek a, který je dělen všemi prvky množiny $\mathcal{M}$, ale nemusí být součinem všech prvků množiny $\mathcal{M}$.

Nejmenším společným násobkem rozumíme prvek $x \in I$, který je společným násobkem množiny $\mathcal{M}$ a navíc tento prvek x dělí každý další společný násobek v množiny $\mathcal{M}$. Nejmenší společný násobek množiny $\mathcal{M}$ značíme $x \in nsn(\mathcal{M})$, někdy též $x \in n(\mathcal{M})$.

$$[x = nsn(a_1, a_2, \dots, a_n)] \Rightarrow$$

$$\left[(a_1|x, a_2|x, \dots, a_n|x) \wedge \left((\forall v \in \mathcal{M}): \left((a_1|v, a_2|v, \dots, a_n|v) \Rightarrow (x|v)\right)\right)\right]$$

Množina $\mathcal{M}$ je jistá podmnožina nosné množiny oboru I.

2.4.1 PŘÍKLAD NA NEJMENŠÍ SPOLEČNÝ NÁSOBEK

Najděte nejmenší společný násobek čísel 25, 15 a 9.

Výpočet provedeme s využitím prvočíselného rozkladu známého ze základní školy. Stejně jako pro největšího společného dělitele, tak i pro nejmenší společný násobek existuje efektivnější metoda.

$$nsn(25, 15, 9) = ?$$

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

$$15 = 3 \cdot 5$$

$$9 = \underline{3} \cdot \underline{3}$$

$$nsn(25, 15, 9) = 5 \cdot 5 \cdot 3 \cdot 3 = \underline{\underline{225}}$$

2.5 ASOCIOVANÉ ROZKLADY

Nechť I je obor integrity. Dále ať $a = p_1 \cdot p_2 \cdot \dots \cdot p_n$ a $a = q_1 \cdot q_2 \cdot \dots \cdot q_m$ **jsou rozklady prvku $a \in I$ v součin ireducibilních prvků**. Řekneme, že tyto **rozklady jsou spolu asociovány**, právě když $m = n$ a při vhodném očíslování činitelů platí:

$p_i \parallel q_i$ pro $i = 1, 2, \dots, n$. [Blažek, 1985]

2.6 PODMÍNKY OBORU INTEGRITY

Podmínkami oboru integrity jsou podmínky ENSD, P, J, I a KŘVD.

- ESND - Pro každé dva prvky oboru integrity existuje největší společný dělitel.
- P - Každý ireducibilní prvek oboru integrity je prvočinitel.
- J - Každý ireducibilní rozklad je jednoznačný.
- I - Každý nenulový prvek z $I - I^*$ je součinem prvků ireducibilních.
- KŘVD - Neexistence nekonečné posloupnosti $a_1, a_2, \dots$ prvků oboru I tak, že a_{i+1} je vlastní dělitel $a_i, \forall\, i \in \mathbb{N}$.

3 GAUSSOVY OBORY INTEGRITY

Obor integrity I se nazývá **Gaussův obor integrity** (faktoriální obor integrity nebo obor integrity s jednoznačným rozkladem), právě když pro každé $a \in I, a \neq 0, a \nmid 1$ existuje rozklad v součin ireducibilních prvků a když libovolné dva rozklady prvku a jsou spolu asociovány. [Blažek, 1985]

Když obor integrity I splňuje podmínku konečnosti řetězce vlastních dělitelů (KŘVD) a existuje k libovolným dvěma prvkům v I největší společný dělitel (podmínka ENSD), tak se jedná o Gaussův obor integrity.

Gaussův obor integrity je pojmenován po německém matematikovi a fyzikovi Johannu Carlu Friedrichu Gaussovi.

3.1 JOHANN CARL FRIEDRICH GAUSS

Johann Carl Friedrich Gauss se narodil 30. dubna 1777 v německém Brunšviku (Braunschweig). Už od raného mládí ho bavila matematika a i přes přání svého otce, aby se stal kameníkem, vystudoval Univerzitu v Göttingenu. Během studií na této univerzitě dokázal několik vět, které byly už dávno objeveny, ale stále se čekalo na dokázání jejich pravdivosti. Byly to základní matematické operace a binomická věta.

Obrázek 1 - Johann Carl Friedrich Gauss

$$(x+a)^n = \sum_{k=0}^{n} \binom{n}{k} x^k a^{n-k} = \binom{n}{0} x^n a^0 + \binom{n}{1} x^{n-1} a^1 + \ \ldots + \binom{n}{n} x^0 a^n$$

Jeho přínos matematice se začal ukazovat hned po dokončení studií na univerzitě. Jako první se věnoval eukleidovské geometrii (geometrie bez vzdálenosti), kde dokázal, že je každý pravidelný n-úhelník, kde n je rovno Fermatovu prvočíslu, sestrojitelný pouze pravítkem a kružítkem.

Také se věnoval teorii čísel. Objevil aritmetiku zbytkových tříd a statistické zákonitosti, které popsal známou křivkou, která je po něm pojmenována (Gaussova křivka). Díky jeho práci se teorie čísel stala samostatnou matematickou disciplínou.

Nevěnoval se pouze matematice. Mezi jeho zájmy patřila i astronomie. Dlouhá léta byl ředitelem hvězdárny v Göttingenu a přednášel astronomii na tamější univerzitě. Ve svých 23 letech dokázal spočítat dráhu planetky Ceres, kterou astronomové ztratili z dohledu a určit, kdy jí bude možno zase sledovat.

Dále se věnoval i fyzice, ve které se společně s profesorem Wilhelmem Weberem snažil o nový pohled na magnetismus a Kirchhoffovy zákony.

4 EUKLIDOVY OBORY INTEGRITY

Obor integrity I se nazývá Euklidův obor integrity právě tehdy, když existuje zobrazení N (někdy též v) množiny I-{0} do množiny přirozených čísel $\mathbb{N}$ (nazýváme ho Euklidova norma) takové, že pro libovolné prvky $a, b \in I, b \neq 0$ platí současně:

1. $a|b \Rightarrow N(a) \leq N(b)$
2. $(\exists \eta, v \in I)$: $[a = b\eta + v \wedge (v = 0 \vee N(v) < N(b))]$. [Blažek, 1985]

To znamená, že pokud prvek a dělí prvek b a zároveň prvek b dělí prvek a, tak se Euklidova norma prvku a rovná Euklidově normě prvku b.

$$a|b \wedge b|a \Leftrightarrow N(a) = N(b)$$

4.1 EUKLIDŮV ALGORITMUS

Euklidův algoritmus je postup, který se používá pro zjištění největšího společného dělitele dvou prvků. Tyto prvky mohou být celá čísla $(\mathbb{Z})$, přirozená čísla $(\mathbb{N})$, Gaussova celá čísla ve tvaru $z = a + bi$, kde $a, b \in \mathbb{Z}$, značíme $(\mathbb{Z}[i])$, komplexní čísla ve tvaru $k = a + b\sqrt{n}$ pro některá $n \in \mathbb{N}$, kde $a, b \in \mathbb{Z}$, či komplexní čísla ve tvaru $z = a + bi\sqrt{n}$ pro některá $n \in \mathbb{N}$, kde $a, b \in \mathbb{Z}$, a v neposlední řadě i polynomy ve tvaru

$$Q_{(x)} = a_1 \cdot x^n + a_2 \cdot x^{n-1} + \cdots + a_{n-1} \cdot x^0, \text{ kde } a_i \in \mathbb{Q},\ n, i \in \mathbb{N}.$$

Tento algoritmus je pojmenován podle řeckého matematika a geometra Euklida.

Euklidův algoritmus: Nechť jsou a a b dva nenulové prvky Euklidova oboru integrity I. Pak v I existují prvky $\eta_0, \eta_1, \ldots, \eta_n,\ v_1, v_2, \ldots, v_n$ tak, že $v_n = nsd(a, b)$ a platí:

$$\begin{aligned}
a &= b \cdot \eta_0 + v_1 && N(v_1) < N(b) \\
b &= v_1 \cdot \eta_1 + v_2 && N(v_2) < N(v_1) \\
v_1 &= v_2 \cdot \eta_2 + v_3 && N(v_3) < N(v_2) \\
&\vdots && \vdots \\
v_{i-1} &= v_i \cdot \eta_i + v_{i+1} && N(v_{i+1}) < N(v_i) \\
&\vdots && \vdots \\
v_{n-2} &= v_{n-1} \cdot \eta_{n-1} + v_n && N(v_n) < N(v_{n-1}) \\
v_{n-1} &= v_n \cdot \eta_n + 0. \text{ [Blažek, 1985]}
\end{aligned}$$

Důkaz:

V případě, že $b|a$ máme samozřejmě $v_0 = b = nsd(a,b)$. V ostatních případech vyplývá existence čísel $v_i, \eta_i \in I$ z druhé podmínky Euklidova oboru integrity, tedy

$$(\exists \eta, v \in I): [a = b\eta + v \wedge (v = 0 \vee N(v) < N(b))].$$

Stačí tedy dokázat, že $v_n = nsd(a,b)$.

Z poslední rovnosti uvedené výše v Euklidovu algoritmu $v_{n-1} = v_n \cdot \eta_n$ plyne, že $v_n|v_{n-1}$. Dále z předposlední rovnosti $v_{n-2} = v_{n-1} \cdot \eta_{n-1} + v_n$ plyne, že $v_n|v_{n-2}$. Tímto způsobem postupujeme dále. Nakonec dostáváme z druhé rovnosti $v_n|b$ a z první $v_n|a$. Vidíme, že prvek v_n je společným dělitelem prvků a a b. Nechť t je libovolný společný dělitel prvků a a b. Pak z první rovnosti Euklidova algoritmu plyne $t|v_1$, z druhé rovnosti $t|v_2$, až nakonec z poslední rovnosti $t|v_n$. Prvek v_n je proto největším společným dělitelem prvků a a b.

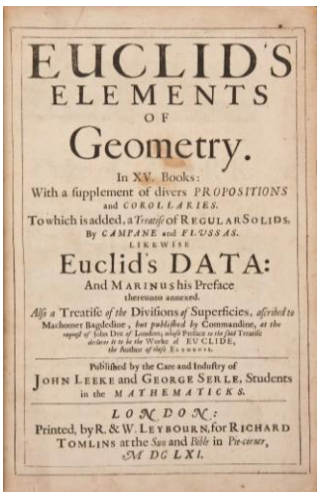
4.2 EUKLIDÉS Z ALEXANDRIE

Obrázek 2 - Euklidés z Alexandrie

Euklidés z Alexandrie (někdy též Eukleides či Euklid) byl řecký matematik žijící ve 3. století př. n. l. Euklidés je autorem díla Stoicheia (česky Základy, anglicky The Euclid´s Elements), ve kterém popisuje základy matematiky a geometrie. Dílo Stoicheia je rozděleno do třinácti knih a je považováno za základ euklidovské geometrie.

V první knize toho díla stanovil základní definice, postuláty a axiomy geometrie, které jsou dané a nemusí se dokazovat. V dalších knihách tohoto díla dokazuje pomocí těchto základních pojmů složitější věty geometrie. V následujících knihách se věnuje planimetrii (geometrie v rovině), podobnosti a shodnosti trojúhelníků, stereometrii (geometrie v prostoru), povrchům a objemům těles…

V tomto díle najdeme i Euklidův algoritmus. Je zařazen v osmé knize, která se zabývá teorií čísel.


EUCLID'S
ELEMENTS
OF
Geometry.
In XV. Books:
With a supplement of divers PROPOSITIONS and COROLLARIES.
To which is added, a Treatise of REGULAR SOLIDS,
By CAMPANE and FLUSSAS.
LIKEWISE
Euclid's DATA:
And MARINUS his Preface
thereunto annexed.
Also a Treatise of the Divisions of Superficies, ascribed to Machomet Bagdedine, but published by Commandine, at the request of John Dee of London, who'd Preface to the said Treatise declares it to be the Worke of EUCLIDE, the Author of these Elements.
Published by the Care and Industry of
JOHN LEEKE and GEORGE SERLE, Students in the MATHEMATICKS.
LONDON:
Printed, by R. & W. LEYBOURN, for RICHARD TOMLINS at the Sun and Bible in Pie-corner,
M DC LXI.

Obrázek 3 –
Anglický překlad díla Stoicheia

5 PŘÍKLADY NA NSD A NSN V RŮZNÝCH OBORECH INTEGRITY

V této kapitole se budeme zabývat největším společným dělitelem a nejmenším společným násobkem prvků různých množin, které tvoří obor integrity. K výpočtu budeme používat Euklidův algoritmus.

5.1 MNOŽINA CELÝCH ČÍSEL $\mathbb{Z}$

V následující části se budeme věnovat největším společným dělitelům a nejmenším společným násobkům v oboru integrity celých čísel.

5.1.1 NEJVĚTŠÍ SPOLEČNÝ DĚLITEL V $\mathbb{Z}$

Spočtěte největšího společného dělitele čísel 440895 a 332640.

$$nsd(440895, 332640) = ?$$

V prvním kroku Euklidova algoritmu dělíme číslo 440895 číslem 332640.

$$440895 = 1 \cdot 332640 + 108255$$

V následujícím kroku budeme dělit číslo 332640 pomocí zbytku z předchozího kroku.

$$332640 = 3 \cdot 108255 + 7875$$

Euklidův algoritmus opakujeme, dokud nedostaneme nulový zbytek. Největším společným dělitelem je pak poslední nenulový zbytek.

$$108255 = 13 \cdot 7875 + 5880$$

$$7875 = 1 \cdot 5880 + 1995$$

$$5880 = 2 \cdot 1995 + 1890$$

$$1995 = 1 \cdot 1890 + \boxed{105}$$

$$1890 = 18 \cdot 105 + 0$$

$$nsd(440895, 332640) = \underline{\underline{105}}$$

Největším společným dělitelem čísel 440895 a 332640 je číslo 105.

5.1.2 NEJMENŠÍ SPOLEČNÝ NÁSOBEK V $\mathbb{Z}$

Spočtěte nejmenší společný násobek čísel 326 a -896.

$$nsn(326, -896) = ?$$

Nejmenší společný násobek spočteme pomocí vzorce:

$$nsn(a, b) = \frac{a \cdot b}{nsd(a, b)}.$$

Nejdříve musíme určit největšího společného dělitele. Postup bude stejný jako v předchozím příkladu.

$$nsd(326, -896) = ?$$
$$-896 = (-2) \cdot 326 - 244$$
$$326 = (-1) \cdot (-244) + 82$$
$$-244 = (-2) \cdot 82 - 80$$
$$82 = (-1) \cdot (-80) + \boxed{2}$$
$$-80 = (-40) \cdot 2 + 0$$
$$nsd(326, -896) = \underline{2}$$

Nyní už můžeme dosadit do vzorce pro výpočet nejmenšího společného násobku:

$$nsn(326, -896) = \frac{326 \cdot (-896)}{nsd(326, -896)} = \frac{-292096}{2} = \underline{\underline{-146048}}.$$

Nejmenším společným násobkem čísel 326 a -896 je číslo -146048. Správným výsledkem je i číslo opačné k číslu -146048 tedy číslo 146048.

5.2 $\mathbb{Z}[i]$ JAKO OBOR INTEGRITY

V této části se budu zabývat oborem integrity Gaussových celých čísel $\mathbb{Z}[i]$. Gaussova celá čísla mají tvar $\mathbb{Z}[i] = \{z = a + bi,$ kde $a, b \in \mathbb{Z}\}$. Nejprve zjistíme, zda množina Gaussových celých čísel tvoří obor integrity.

Množina $\mathbb{Z}[i]$ je podmnožinou tělesa všech komplexních čísel $(\mathbb{C}, +, \cdot)$. To nám zajišťuje zachování jednotlivých vlastností operací sčítání a násobení v množině $\mathbb{Z}[i]$. Musíme ukázat, že množina $\mathbb{Z}[i]$ je uzavřená na operace sčítání a násobení.

Zaměříme se na operaci sčítání:

$$(a + bi) + (c + di) = (a + c) + (b + d)i.$$

Na první pohled je patrné, že je operace sčítání uzavřená v množině $\mathbb{Z}[i]$.

Nyní ověříme uzavřenost pro operaci násobení v množině $\mathbb{Z}[i]$:

$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i.$$

Vidíme, že i operace násobení je uzavřená na množině $\mathbb{Z}[i]$.

Je tedy patrné, že množina $\mathbb{Z}[i]$ je oborem integrity Gaussových celých čísel.

Nyní ještě ověříme, jestli se jedná o Euklidův obor integrity. Aby množina $\mathbb{Z}[i]$ byla Euklidovým oborem integrity, musí v něm existovat Euklidova norma N a pro libovolné prvky $a, b \in I, b \neq 0$ musí splňovat dvě podmínky:

1. $a|b \Rightarrow N(a) \leq N(b)$
2. $(\exists \eta, v \in I)$: $[a = b\eta + v \wedge (v = 0 \vee N(v) < N(b))]$.

Euklidova norma u Gaussových celých čísel $x = a + bi$ je definována takto:

$$N(a + bi) = a^2 + b^2 .$$

Ověříme první podmínku.

Pro prvky množiny $\mathbb{Z}[i]$, kde $a+bi \neq 0$ a $c+di \neq 0$ je Euklidova norma prvku $a+bi = a^2+b^2$ a Euklidova norma prvku $c+di = c^2+d^2$, takže $N(a+bi)$, $N(c+di) \in \mathbb{N}$.

Dále vezmeme prvek $(a+bi)\cdot(c+di)$ a určíme jeho Euklidovu normu:

$$N\big((a+bi)\cdot(c+di)\big) = N\big((ac-bd)+(ad+bc)i\big) =$$

$$= (ac-bd)^2+(ad+bc)^2 =$$

$$= a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2 =$$

$$= a^2(c^2+d^2) + b^2(c^2+d^2) = (a^2+b^2)\cdot(c^2+d^2) =$$

$$= N(a+bi)\cdot N(c+di).$$

Označíme prvek $z = e+fi = (a+bi)\cdot(c+di)$.

Je patrné, že $(a+bi)|(e+fi)$ a $N(a+bi) \leq N\big((a+bi)\cdot(c+di)\big) = N(e+fi)$.

Množina $\mathbb{Z}[i]$ splňuje první podmínku Euklidova oboru integrity.

Nyní ověříme platnost druhé podmínky Euklidova oboru integrity v množině $\mathbb{Z}[i]$.

Nechť $x = a+bi$ a $y = c+di$ jsou dva nenulové prvky množiny $\mathbb{Z}[i]$.

Zřejmě existují celá čísla q_1, q_2 taková, že:

$$\left|\frac{ac+bd}{c^2+d^2} - q_1\right| \leq \frac{1}{2}$$

$$\left|\frac{bc-ad}{c^2+d^2} - q_2\right| \leq \frac{1}{2}.$$

Pak $q = q_1 + q_2\, i \in \mathbb{Z}[i]$ a $r = r_1 + r_2 i = x - yq \ \in \mathbb{Z}[i]$.

Jelikož $N(r) < N(y)$ právě když $\frac{N(r)}{N(y)} < 1$, stačí počítat $\frac{N(r)}{N(y)}$.

Označíme $\overline{x} = a-bi$ a $\overline{y} = c-di$ (prvky $\overline{x}$ a $\overline{y}$ jsou prvky asociované s prvky x a y).

Dále platí $N(x) = x\cdot\overline{x} = N(\overline{x})$.

Důkaz:

$$x = a+bi \ \Rightarrow N(x) = a^2+b^2 = a^2+(-b)^2 = N(\overline{x}) \Rightarrow a-bi = \overline{x}$$

$$x\cdot\overline{x} = (a+bi)\cdot(a-bi) = a^2 - abi + abi + b^2 = a^2+b^2 \Rightarrow N(x)$$

$$N(x) = x\cdot\overline{x} = N(\overline{x}).$$

Nyní zjistíme čemu se rovná zlomek $\frac{N(r)}{N(y)}$.

$$\frac{N(r)}{N(y)} = \frac{N(x-yq)}{N(y)} = \frac{N\left((x-yq)\cdot\frac{\overline{y}}{\overline{y}}\right)}{N(y)} = \frac{N(x\overline{y}\ -y\overline{y}\,q)}{\left(N(y)\right)^2} = N\left(\frac{x\overline{y}}{N(y)} - q\right)$$

Podle volby čísel q_1, q_2 dostáváme pro $q = q_1 + q_2$:

$$N\left(\frac{x\overline{y}}{N(y)} - q\right) = N\left(\frac{ac+bd}{c^2+d^2} - q_1 + \left(\frac{bc-ad}{c^2+d^2} - q_2\right)i\right) =$$

$$= \left(\frac{ac+bd}{c^2+d^2} - q_1\right)^2 + \left(\frac{bc-ad}{c^2+d^2} - q_2\right)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1.$$

Tím je splněna druhá podmínka Euklidova oboru integrity pro prvky množiny $\mathbb{Z}[i]$.

Protože platí obě podmínky Euklidova oboru integrity, můžeme říci, že obor integrity Gaussových celých čísel je Euklidovým oborem integrity.

5.2.1 NEJVĚTŠÍ SPOLEČNÝ DĚLITEL V $\mathbb{Z}[i]$

Spočtěte největšího společného dělitele čísel $126 + 64i$ a $48 - 72i$.

$$nsd(126+64i, 48-72i) = ?$$

Nejprve musíme určit Euklidovu normu obou čísel:

$$N(126+64i) = 126^2 + 64^2 = \underline{\underline{19972}}$$

$$N(48-72i) = 48^2 + (-72)^2 = \underline{\underline{7488}}.$$

Největšího společného dělitele nalezneme pomocí Euklidova algoritmu. Z Euklidových norem vidíme, že má číslo $48 - 72$i menší Euklidovu normu než číslo $126 + 64$i. Budeme dělit číslo $126 + 64$i číslem $48 - 72$i.

1. $126 + 64i = \eta_1 \cdot (48 - 72i) + v_1$

$$\eta_1 = \frac{126+64i}{48-72i} = \frac{126+64i}{48-72i}\cdot\frac{48+72i}{48+72i} =$$

$$= \frac{6048+9072i+3072i+4608i^2}{2304+3456i-3456i-5184i^2} = \frac{1440+12144i}{7488} =$$

$$= \frac{1440}{7488} + \frac{12144}{7488} \doteq \underline{\underline{2i}}$$

$$v_1 = 126 + 64i - \eta_1 \cdot (48 - 72i)$$

$$v_1 = 126 + 64i - 2i \cdot (48 - 72i) = 126 + 64i - 96i + 144i^2 =$$

$$= 126 - 32i - 144 = \underline{\underline{-18 - 32i}}$$

$$126 + 64i = (2i) \cdot (48 - 72i) + (-18 - 32i)$$

Vidíme, že zbytek $-18-32i$ je nenulový. V této fázi Euklidova algoritmu ještě nemůžeme určit největšího společného dělitele čísel $126+64i$ a $48-72i$. Zbytek má Euklidovu normu 1348, která je menší než Euklidova norma čísla $48-72i$ (7488), počítáme tedy správně. Pokračujeme dále v Euklidovu algoritmu.

Nyní budeme dělit číslo $48-72i$ zbytkem $-18-32i$.

2. $48-72i=\eta_2\cdot(-18-32i)+\upsilon_2$

$$\eta_2=\frac{48-72i}{-18-32i}=\frac{48-72i}{-18-32i}\cdot\frac{-18+32i}{-18+32i}=$$

$$=\frac{-864+1536i+1296i-2304i^2}{324-576i+576i-1024i^2}=\frac{1440+2832i}{1348}=$$

$$=\frac{1440}{1348}+\frac{2831i}{1348}\doteq\underline{\underline{1+2i}}$$

$$\upsilon_2=48-72i-\eta_2\cdot(-18-32i)$$

$$\upsilon_2=48-72i-(1+2i)\cdot(-18-32i)=$$

$$=48-72i-(-18-32i-36i-64i^2)=$$

$$=66-4i-64=\underline{\underline{2-4i}}$$

$$48-72i=(1+2i)\cdot(-18-32i)+(2-4i)$$

Jako v předchozím kroku tak i nyní je zbytek $2-4i$ nenulový a tudíž stále nemůžeme určit největšího společného dělitele. Zkontrolujeme tedy Euklidovu normu zbytku $2-4i$ (20). Je tedy menší než Euklidova norma čísla $-18-32i$, počítáme správně a můžeme pokračovat v Euklidovu algoritmu. Budeme dělit číslo $-18-32i$ zbytkem $2-4i$.

3. $-18-32i=\eta_3\cdot(2-4i)+\upsilon_3$

$$\eta_3=\frac{-18-32i}{2-4i}=\frac{-18-32i}{2-4i}\cdot\frac{2+4i}{2+4i}=$$

$$=\frac{-36-72i-64i-128i^2}{4+8i-8i-16i^2}=\frac{92-136i}{20}=$$

$$=\frac{92}{20}-\frac{136i}{20}\doteq\underline{\underline{5-7i}}$$

$$\upsilon_3=(-18-32i)-(2-4i)\cdot\eta_3$$

$$\upsilon_3=(-18-32i)-(2-4i)\cdot(5-7i)=$$

$$=-18-32i-(10-14i-20i+28i^2)=\underline{\underline{2i}}$$

$$-18-32i=(5-7i)\cdot(2-4i)+(2i)$$

Stále je zbytek nenulový. Euklidova norma zbytku $\upsilon_3=2i$ (4) je opět menší než Euklidova norma čísla $2-4$i, pomocí kterého jsme dělili číslo $-18-32$i. Počítáme tedy správně. Dále budeme pokračovat v Euklidovu algoritmu. Dělíme číslo $2-4$i zbytkem $2i$.

4. $2-4i=\eta_4\cdot(2i)+v_4$

$$\eta_4=\frac{2-4i}{2i}=\frac{2-4i}{2i}\cdot\frac{-2i}{-2i}=\frac{-4i-8}{4}=\underline{\underline{-2-i}}$$

$$v_4=(2-4i)-(2i)\cdot\eta_4$$

$$v_4=(2-4i)-(2i)\cdot(-2-i)=2-4i+4i-2=\underline{\underline{0}}$$

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

Nyní jsme získali nulový zbytek a můžeme určit největšího společného dělitele čísel $126+64i$ a $48-72i$.

Z dílčích výsledků si pro přehlednost sestavíme Euklidův algoritmus.

$$126+64i=(2i)\cdot(48-72i)+(-18-32i)$$

$$48-72i=(1+2i)\cdot(-18-32i)+(2-4i)$$

$$-18-32i=(5-7i)\cdot(2-4i)+\boxed{(2i)}$$

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

$$nsd(26+52i,34-114i)=\underline{\underline{2i}}$$

Z Euklidova algoritmu je patrné, že největším společným dělitelem čísel $126+64i$ a $48-72i$ je číslo $2i$. Dále je správným výsledkem i číslo komplexně sdružené k číslu $2i$, tedy $-2i$.

Pro kontrolu si provedeme zkoušku.

1. $2i$ musí dělit $126+64i$

$$\frac{126+64i}{2i}=\frac{126+64i}{2i}\cdot\frac{-2i}{-2i}=\frac{-252i+128}{4}=32-63i$$

2. $2i$ musí dělit $48-72i$

$$\frac{48-72i}{2i}=\frac{48-72i}{2i}\cdot\frac{-2i}{-2i}=\frac{-96i-144}{4}=-36-24i$$

Číslo $2i$ dělí obě čísla, je tedy jejich společným dělitelem.

5.2.2 NEJVĚTŠÍ SPOLEČNÝ DĚLITEL V $\mathbb{Z}[i]$ (2)

Spočtěte největšího společného dělitele čísel $26+52i$ a $34-114i$.

$$nsd(26+52i,34-114i)=?$$

$$N(26+52i)=\underline{\underline{3380}}$$

$$N(34-114i)=\underline{\underline{14152}}$$

1. $34 - 114i = \eta_1 \cdot (26 + 52i) + v_1$

$$\eta_1 = \frac{34 - 114i}{26 + 52i} = \frac{34 - 114i}{26 + 52i} \cdot \frac{26 - 52i}{26 - 52i} =$$

$$= \frac{-5044 - 4732i}{3380} \doteq \underline{\underline{-1 - i}}$$

$$v_1 = (34 - 114i) - (26 + 52i) \cdot \eta_1$$

$$v_1 = (34 - 114i) - (26 + 52i) \cdot (-1 - i) = \underline{\underline{8 - 36i}}$$

$$34 - 114i = (-1 - i) \cdot (26 + 52i) + (8 - 36i)$$

2. $26 + 52i = \eta_2 \cdot (8 - 36i) + v_2$

$$\eta_2 = \frac{26 + 52i}{8 - 36i} = \frac{26 + 52i}{8 - 36i} \cdot \frac{8 + 36i}{8 + 36i} =$$

$$= \frac{-1664 - 1352i}{1360} \doteq \underline{\underline{-1 + i}}$$

$$v_2 = (26 + 52i) - (-1 + i) \cdot \eta_2$$

$$v_2 = (26 + 52i) - (8 - 36i) \cdot (-1 + i) = \underline{\underline{-2 + 8i}}$$

$$26 + 52i = (-1 + i) \cdot (8 - 36i) + (-2 + 8i)$$

3. $8 - 36i = \eta_3 \cdot (-2 + 8i) + v_3$

$$\eta_3 = \frac{8 - 36i}{-2 + 8i} = \frac{8 - 36i}{-2 + 8i} \cdot \frac{-2 - 8i}{-2 - 8i} =$$

$$= \frac{-304 + 8i}{68} \doteq \underline{\underline{-4}}$$

$$v_3 = (836 - i) - (-2 + 8i) \cdot \eta_3$$

$$v_3 = (8 - 36i) - (-2 + 8i) \cdot (-4) = \underline{\underline{-4i}}$$

$$8 - 36i = (-4) \cdot (-2 + 8i) + (-4i)$$

4. $-2 + 8i = \eta_4 \cdot (-4i) + v_4$

$$\eta_4 = \frac{-2 + 8i}{-4i} = \frac{-2 + 8i}{-4i} \cdot \frac{4i}{4i} = \frac{-32 - 8i}{16} \doteq \underline{\underline{-2 - i}}$$

Zde máme dvě možnosti zaokrouhlení. Zlomek $\frac{-32-8i}{16}$ lze zaokrouhlit na $-2 - i$ nebo na -2. Na výsledek nemá ani jedno zaokrouhlení vliv (může nám vyjít číslo opačné nebo komplexně sdružené, ale stále máme správný výsledek). Dále budeme počítat se zaokrouhlením na $-2 - i$.

$$v_4 = (-2 + 8i) - (-4i) \cdot \eta_4$$

$$v_4 = (-2 + 8i) - (-4i) \cdot (-2 - i) = \underline{\underline{2}}$$

$$-2 + 8i = (-2 - i) \cdot (-4i) + 2$$

5. $-4i = \eta_5 \cdot 2 + \upsilon_5$

$$\eta_5 = \frac{-4i}{2} = \underline{\underline{-2i}}$$

$$\upsilon_5 = -4i - 2 \cdot \eta_5$$

$$\upsilon_5 = (-4i) - 2 \cdot (-2i) = \underline{\underline{0}}$$

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

Z dílčích výsledků sestavíme pro přehlednost samotný Euklidův algoritmus bez dílčích výsledků.

$$34 - 114i = (-1 - i) \cdot (26 + 52i) + (8 - 36i)$$

$$26 + 52i = (-1 + i) \cdot (8 - 36i) + (-2 + 8i)$$

$$8 - 36i = (-4) \cdot (-2 + 8i) + (-4i)$$

$$-2 + 8i = (-2 - i) \cdot (-4i) + \boxed{2}$$

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

Odtud vidíme, že $nsd(26 + 52i, 34 - 114i) = \underline{\underline{2}}$.

Pro kontrolu si provedeme zkoušku.

1. 2 musí dělit $26 + 52i$

$$\frac{26 + 52i}{2} = 13 + 26i$$

2. 2 musí dělit $34 - 114i$

$$\frac{34 - 114i}{2} = 17 - 57i$$

Číslo 2 dělí obě čísla, je tedy jejich společným dělitelem.

Nyní ještě ukážeme, jak se změní výpočet, když ve čtvrtém kroku zaokrouhlíme na -2 místo na $-2 - i$. Výpočet budeme provádět od čtvrtého kroku.

4. $-2 + 8i = \eta_4 \cdot (-4i) + \upsilon_4$

$$\eta_4 = \frac{-2 + 8i}{-4i} = \frac{-2 + 8i}{-4i} \cdot \frac{4i}{4i} =$$

$$= \frac{-32 - 8i}{16} \doteq \underline{\underline{-2}}$$

$$\upsilon_4 = (-2 + 8i) - (-4i) \cdot \eta_4$$

$$\upsilon_4 = (-2 + 8i) - (-4i) \cdot (-2) = \underline{\underline{-2}}$$

$$-2 + 8i = (-2) \cdot (-4i) - 2$$

5. $-4i = \eta_5 \cdot (-2) + \upsilon_5$

$$\eta_5 = \frac{-4i}{-2} = \underline{\underline{2i}}$$

$$\upsilon_5 = -4i - (-2) \cdot \eta_5$$

$$\upsilon_5 = (-4i) - (-2) \cdot (2i) = \underline{\underline{0}}$$

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

Posledním nenulovým zbytkem je číslo -2. Dospěli jsme k číslu opačnému než v předchozím případě. Výsledek -2 je také největším společným dělitelem čísel $26 + 52i$ a $34 - 114i$.

5.2.3 NEJMENŠÍ SPOLEČNÝ NÁSOBEK V $\mathbb{Z}[i]$

Spočtěte nejmenší společný násobek čísel $1 + 3i$ a $3 - 3i$.

$$nsn(1 + 3i, 3 - 3i) = ?$$

Největší společný násobek určíme pomocí vzorce:

$$nsn(a, b) = \frac{a \cdot b}{nsd(a, b)}.$$

Nejdříve musíme určit největšího společného dělitele. Budeme tedy postupovat jako v předchozích příkladech, dokud nedostaneme nulový zbytek.

$$nsd(1 + 3i, 3 - 3i) = ?$$

$$N(1 + 3i) = \underline{\underline{10}}$$

$$N(3 - 3i) = \underline{\underline{18}}$$

1. $3 - 3i = \eta_1 \cdot (1 + 3i) + \upsilon_1$

$$\eta_1 = \frac{3 - 3i}{1 + 3i} = \frac{3 - 3i}{1 + 3i} \cdot \frac{1 - 3i}{1 - 3i} =$$

$$= \frac{-6 - 12i}{10} \doteq \underline{\underline{-1 - i}}$$

$$\upsilon_1 = (3 - 3i) - (1 + 3i) \cdot \eta_1$$

$$\upsilon_1 = (3 - 3i) - (1 + 3i) \cdot (-1 - i) = \underline{\underline{1 + i}}$$

$$3 - 3i = (-1 - i) \cdot (1 + 3i) + (1 + i)$$

2. $1 + 3i = \eta_2 \cdot (1 + i) + v_2$

$$\eta_2 = \frac{1+3i}{1+i} = \frac{1+3i}{1+i} \cdot \frac{1-i}{1-i} = \frac{4+2i}{2} = \underline{\underline{2+i}}$$

$$v_2 = (1+3i) - (-1+i) \cdot \eta_2$$

$$v_2 = (1+3i) - (2+i) \cdot (1+i) = \underline{\underline{0}}$$

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

Pro přehlednost si opět sepíšeme Euklidův algoritmus.

$$3 - 3i = (-1-i) \cdot (1+3i) + \boxed{(1+i)}$$

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

$$nsd(1+3i, 3-3i) = \underline{\underline{1+i}}$$

Nyní můžeme spočítat nejmenší společný násobek dosazením do vzorce.

$$nsn(1+3i, 3-3i) = \frac{(1+3\mathrm{i}) \cdot (3-3\mathrm{i})}{\mathrm{nsd}(1+3\mathrm{i},\ 3-3\mathrm{i})} = \frac{12+6\mathrm{i}}{1+\mathrm{i}} =$$

$$= \frac{12+6\mathrm{i}}{1+\mathrm{i}} \cdot \frac{1-\mathrm{i}}{1-\mathrm{i}} = \frac{18-6\mathrm{i}}{2} = \underline{\underline{9-3i}}$$

$$nsn(1+3i, 3-3i) = \underline{\underline{9-3i}}$$

Nejmenším společným násobkem je i číslo $9 + 3i$, které je komplexně sdružené s číslem $9 - 3i$.

5.2.4 NEJMENŠÍ SPOLEČNÝ NÁSOBEK V $\mathbb{Z}[i]$ (2)

Spočtěte nejmenší společný násobek čísel 125 a $67 - i$.

$$nsn(125, 67-i) = ?$$

$$N(125) = \underline{\underline{15625}}$$

$$N(67-i) = \underline{\underline{4490}}$$

Nejdříve spočteme $nsd(125, 67-i)$.

1. $125 = \eta_1 \cdot (67-i) + v_1$

$$\eta_1 = \frac{125}{67-i} = \frac{125}{67-i} \cdot \frac{67+i}{67+i} = \frac{8375+125i}{4490} \doteq \underline{\underline{2}}$$

$$v_1 = (125) - (67-i) \cdot \eta_1$$

$$v_1 = (125) - (67-i) \cdot (2) = \underline{\underline{-9+2i}}$$

$$125 = 2 \cdot (67-i) + (-9+2i)$$

2. $67 - i = \eta_2 \cdot (-9 + 2i) + v_2$

$$\eta_2 = \frac{67 - i}{-9 + 2i} = \frac{67 - i}{-9 + 2i} \cdot \frac{-9 - 2i}{-9 - 2i} =$$

$$= \frac{-605 - 125i}{85} \doteq \underline{\underline{-7 - i}}$$

$$v_2 = (67 - i) - (-9 + 2i) \cdot \eta_2$$

$$v_2 = (67 - i) - (-9 + 2i) \cdot (-7 - i) =$$

$$= 67 - i - (63 - 14i + 9i + 2) = \underline{\underline{2 + 4i}}$$

$$67 - i = (-7 - i) \cdot (-9 + 2i) + (2 + 4i)$$

3. $-9 + 2i = \eta_3 \cdot (2 + 4i) + v_3$

$$\eta_3 = \frac{-9 + 2i}{2 + 4i} = \frac{-9 + 2i}{2 + 4i} \cdot \frac{2 - 4i}{2 - 4i} =$$

$$= \frac{-10 + 40i}{20} \doteq \underline{\underline{-1 + 2i}}$$

Zde lze zaokrouhlit na $-1 + 2i$ nebo na $2i$. Na výsledek nemá ani jedno zaokrouhlení vliv.

$$v_3 = (-9 + 2i) - (2 + 4i) \cdot \eta_3$$

$$v_3 = (-9 + 2i) - (2 + 4i) \cdot (-1 + 2i) =$$

$$= -9 + 2i - (-2 + 4i + 4i - 8) = \underline{\underline{1 + 2i}}$$

$$-9 + 2i = (-1 + 2i) \cdot (2 + 4i) + (1 + 2i)$$

4. $2 + 4i = \eta_4 \cdot (1 + 2i) + v_4$

$$\eta_4 = \frac{2 + 4i}{1 + 2i} = \frac{2 + 4i}{1 + 2i} \cdot \frac{1 - 2i}{1 - 2i} = \frac{10}{5} = \underline{\underline{2}}$$

$$v_4 = (2 + 4i) - (1 + 2i) \cdot \eta_4$$

$$v_4 = (2 + 4i) - (1 + 2i) \cdot (2) = \underline{\underline{0}}$$

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

Z dílčích výsledků si pro přehlednost sepíšeme samotný Euklidův algoritmus.

$$125 = 2 \cdot (67 - i) + (-9 + 2i)$$

$$67 - i = (-7 - i) \cdot (-9 + 2i) + (2 + 4i)$$

$$-9 + 2i = (-1 + 2i) \cdot (2 + 4i) + \boxed{(1 + 2i)}$$

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

$$nsd(125, 67 - i) = \underline{\underline{1 + 2i}}$$

Nyní můžeme dosadit do vzorce pro výpočet nejmenšího společného násobku.

$$nsn(125, 67-i) = \frac{125 \cdot (67-i)}{1+2i} = \frac{8375-125i}{1+2i} \cdot \frac{1-2i}{1-2i} =$$

$$= \frac{8125}{5} - \frac{16875i}{5} = \underline{\underline{1625-3375i}}$$

Nejmenším společným násobkem čísel 125 a $67-i$ je číslo $1625-3375i$.

5.3 $\mathbb{Z}[\sqrt{2}]$ JAKO OBOR INTEGRITY

V této části se budu zabývat množinou $\mathbb{Z}[\sqrt{2}]$. Čísla této množiny mají tvar

$$\mathbb{Z}[\sqrt{2}] = \{z = a + b\sqrt{2}, \text{ kde } a, b \in \mathbb{Z}\}.$$

Na první pohled je patrné, že při obvyklých operacích sčítání a násobení těchto čísel dostáváme obor integrity $(\mathbb{Z}[\sqrt{2}], +, \cdot)$. Operace v tomto oboru integrity jsou uzavřené.

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$$

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = ac + ad\sqrt{2} + bc\sqrt{2} + 2bd = (ac + 2bd) + (ad + bc)\sqrt{2}$$

Nyní ověříme, že je obor integrity $(\mathbb{Z}[\sqrt{2}], +, \cdot)$ Euklidův obor integrity. Musí tedy existovat Euklidova norma N a platit obě podmínky Euklidova oboru integrity.

Euklidova norma v $\mathbb{Z}[\sqrt{2}] = \{z = a + b\sqrt{2}, \text{ kde } a, b \in \mathbb{Z}\}$ je definována takto:

$$N(a + b\sqrt{2}) = |a^2 - 2b^2|.$$

Ověříme první podmínku $a|b \Rightarrow N(a) \leq N(b)$, kde $a, b \in \mathbb{Z}[\sqrt{2}]$.

Pro prvky množiny $\mathbb{Z}[\sqrt{2}]$, kde $a + b\sqrt{2} \neq 0$ a $c + d\sqrt{2} \neq 0$ je Euklidova norma prvku $a + b\sqrt{2} = |a^2 - 2b^2|$ a Euklidova norma prvku $c + d\sqrt{2} = |c^2 - 2d^2|$, takže $N(a + b\sqrt{2})$, $N(c + d\sqrt{2}) \in \mathbb{N}$.

Dále vezmeme prvek $(a + b\sqrt{2}) \cdot (c + d\sqrt{2})$ a určíme jeho Euklidovu normu.

$$N\left((a + b\sqrt{2}) \cdot (c + d\sqrt{2})\right) = N\left((ac + 2bd) + (ad + bc)\sqrt{2}\right) =$$

$$= (ac + 2bd)^2 - 2(ad + bc)^2 =$$

$$= a^2c^2 + 4abcd + 4b^2d^2 - 2a^2d^2 - 4abcd - 2b^2c^2 =$$

$$= a^2(c^2 - 2d^2) - 2b^2(c^2 - 2d^2) = (a^2 - 2b^2) \cdot (c^2 - 2d^2) =$$

$$= N(a + b\sqrt{2}) \cdot N(c + d\sqrt{2})$$

Označíme prvek $z = e + f\sqrt{2} = (a + b\sqrt{2}) \cdot (c + d\sqrt{2})$.

Je patrné, že $(a+b\sqrt{2})|(e+f\sqrt{2})$, proto platí:

$$N(a+b\sqrt{2}) \leq N\left((a+b\sqrt{2})\cdot(c+d\sqrt{2})\right) = N(e+f\sqrt{2}).$$

Množina $\mathbb{Z}[\sqrt{2}]$ splňuje první podmínku Euklidova oboru integrity.

Nyní ještě ověříme druhou podmínku Euklidova oboru integrity

$$(\exists \eta, v \in I)\colon [a = b\eta + v \wedge (v = 0 \vee N(v) < N(b))].$$

Nechť $x = a + b\sqrt{2}$ a $y = c + d\sqrt{2}$ jsou dva nenulové prvky množiny $\mathbb{Z}[\sqrt{2}]$.

Zřejmě existují celá čísla q_1, q_2 taková, že:

$$\left|\frac{ac-2bd}{c^2-2d^2} - q_1\right| \leq \frac{1}{2}$$

$$\left|\frac{bc-ad}{c^2-2d^2} - q_2\right| \leq \frac{1}{2}.$$

Pak $q = q_1 + q_2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ a $r = r_1 + r_2\sqrt{2} = x - yq \in \mathbb{Z}[\sqrt{2}]$.

Protože $N(r) < N(y)$ právě když $\frac{N(r)}{N(y)} < 1$, stačí spočítat $\frac{N(r)}{N(y)}$.

Označíme $\overline{x} = a - b\sqrt{2}$ a $\overline{y} = c - d\sqrt{2}$ (prvky $\overline{x}$ a $\overline{y}$ jsou prvky asociované s prvky x a y).

Dále platí $N(x) = x \cdot \overline{x} = N(\overline{x})$.

Nyní zjistíme čemu se rovná zlomek $\frac{N(r)}{N(y)}$.

$$\frac{N(r)}{N(y)} = \frac{N(x-yq)}{N(y)} = \frac{N\left((x-yq)\cdot\frac{\overline{y}}{\overline{y}}\right)}{N(y)} = \frac{N(x\overline{y} - y\overline{y}\,q)}{\left(N(y)\right)^2} = N\left(\frac{x\overline{y}}{N(y)} - q\right)$$

Podle volby čísel q_1, q_2 dostáváme pro $q = q_1 + q_2$:

$$N\left(\frac{x\overline{y}}{N(y)} - q\right) = N\left(\frac{ac-2bd}{c^2-2d^2} - q_1 + \left(\frac{bc-ad}{c^2-2d^2} - q_2\right)\sqrt{2}\right) =$$

$$= \left|\left(\frac{ac+bd}{c^2+d^2} - q_1\right)^2 - 2\left(\frac{bc-ad}{c^2+d^2} - q_2\right)^2\right| \leq \left|\frac{1}{4} - 2\frac{1}{4}\right| = \frac{1}{4} < 1.$$

$$\frac{N(r)}{N(y)} < 1 \Rightarrow N(r) < N(y)$$

Tím je splněna druhá podmínka Euklidova oboru integrity pro prvky množiny $\mathbb{Z}[\sqrt{2}]$.

Protože platí obě podmínky Euklidova oboru integrity, můžeme říci, že obor integrity na množině $\mathbb{Z}[\sqrt{2}]$ je Euklidovým oborem integrity.

Obdobně bychom postupovali i pro množinu $\mathbb{Z}[\sqrt{3}]$, která také tvoří Euklidův obor integrity. Norma v $\mathbb{Z}[\sqrt{3}] = \{z = a + b\sqrt{3}$, kde $a, b \in \mathbb{Z}\}$ je definována takto:

$$N(a + b\sqrt{3}) = |a^2 - 3b^2|.$$

5.3.1 NEJVĚTŠÍ SPOLEČNÝ DĚLITEL V $\mathbb{Z}[\sqrt{2}]$

Spočtěte největšího společného dělitele čísel $-50 + 3\sqrt{2}$ a $22 + 15\sqrt{2}$.

$$nsd(-50 + 3\sqrt{2}, 22 + 15\sqrt{2}) = ?$$

$$N(-50 + 3\sqrt{2}) = \underline{\underline{2482}}$$

$$N(22 + 15\sqrt{2}) = \underline{\underline{34}}$$

1. $-50 + 3\sqrt{2} = \eta_1 \cdot (22 + 15\sqrt{2}) + \upsilon_1$

$$\eta_1 = \frac{-50 + 3\sqrt{2}}{22 + 15\sqrt{2}} = \frac{-50 + 3\sqrt{2}}{22 + 15\sqrt{2}} \cdot \frac{22 - 15\sqrt{2}}{22 - 15\sqrt{2}} =$$

$$= \frac{-1100 + 750\sqrt{2} + 66\sqrt{2} - 90}{484 + 330\sqrt{2} - 330\sqrt{2} - 450} = \frac{-1190 + 816\sqrt{2}}{34} =$$

$$= -\frac{1190}{34} + \frac{816}{34}\sqrt{2} = \underline{\underline{-35 + 24\sqrt{2}}}$$

$$\upsilon_1 = (-50 + 3\sqrt{2}) - (22 + 15\sqrt{2}) \cdot \eta_1$$

$$\upsilon_1 = (-50 + 3\sqrt{2}) - (22 + 15\sqrt{2}) \cdot (-35 + 24\sqrt{2}) =$$

$$= -50 + 3\sqrt{2} - (770 + 582\sqrt{2} - 525\sqrt{2} + 720) = \underline{\underline{0}}$$

Euklidův algoritmus tedy vypadá takto:

$$-50 + 3\sqrt{2} = (3 + 4\sqrt{2}) \cdot \boxed{(22 + 15\sqrt{2})} + 0$$

$$nsd(-50 + 3\sqrt{2}, 22 + 15\sqrt{2}) = \underline{\underline{22 + 15\sqrt{2}}}.$$

Největším společným dělitelem čísel $-50 + 3\sqrt{2}$ a $22 + 15\sqrt{2}$ je číslo $22 + 15\sqrt{2}$.

5.3.2 NEJMENŠÍ SPOLEČNÝ NÁSOBEK V $\mathbb{Z}[\sqrt{2}]$

Spočtěte nejmenší společný násobek čísel $-50+3\sqrt{2}$ a $22+15\sqrt{2}$.

$$nsn\left(-50+3\sqrt{2}, 22+15\sqrt{2}\right) = ?$$

Nejmenší společný násobek určíme pomocí vzorce:

$$nsn(a,b) = \frac{a \cdot b}{nsd(a,b)}.$$

Největšího společného dělitele známe z předchozího příkladu, tak rovnou dosadíme.

$$nsn\left(-50+3\sqrt{2}, 22+15\sqrt{2}\right) = \frac{\left(-50+3\sqrt{2}\right)\cdot\left(22+15\sqrt{2}\right)}{22+15\sqrt{2}} = \underline{\underline{-50+3\sqrt{2}}}$$

Nejmenší společný násobek čísel $-50+3\sqrt{2}$ a $22+15\sqrt{2}$ je číslo $-50+3\sqrt{2}$.

5.3.3 NEJVĚTŠÍ SPOLEČNÝ DĚLITEL V $\mathbb{Z}\left[\sqrt{3}\right]$

Spočtěte největšího společného dělitele čísel $10+2\sqrt{3}$ a $54+44\sqrt{3}$.

$$nsd\left(10+2\sqrt{3}, 54+44\sqrt{3}\right) = ?$$

$$N\left(10+2\sqrt{3}\right) = \underline{\underline{88}}$$

$$N\left(54+44\sqrt{3}\right) = \underline{\underline{2892}}$$

1. $54+44\sqrt{3} = \eta_1 \cdot \left(10+2\sqrt{3}\right) + v_1$

$$\eta_1 = \frac{54+44\sqrt{3}}{10+2\sqrt{3}} = \frac{54+44\sqrt{3}}{10+2\sqrt{3}} \cdot \frac{10-2\sqrt{3}}{10-2\sqrt{3}} =$$

$$= \frac{540-108\sqrt{3}+440\sqrt{3}-264}{100-20\sqrt{3}+20\sqrt{3}-12} =$$

$$= \frac{276+332\sqrt{3}}{88} = \frac{276}{88} + \frac{332}{88}\sqrt{3} \doteq \underline{\underline{3+4\sqrt{3}}}$$

$$v_1 = \left(54+44\sqrt{3}\right) - \left(10+2\sqrt{3}\right)\cdot\eta_1$$

$$v_1 = \left(54+44\sqrt{3}\right) - \left(10+2\sqrt{3}\right)\cdot\left(3+4\sqrt{3}\right) =$$

$$= 54+44\sqrt{3} - \left(30+6\sqrt{3}+40\sqrt{3}+24\right) = \underline{\underline{-2\sqrt{3}}}$$

$$54+44\sqrt{3} = (3+4\sqrt{3})\cdot\left(10+2\sqrt{3}\right) + (-2\sqrt{3})$$

2. $10+2\sqrt{3}=\eta_2\cdot\left(-2\sqrt{3}\right)+\upsilon_2$

$$\eta_2=\frac{10+2\sqrt{3}}{-2\sqrt{3}}=\frac{10+2\sqrt{3}}{-2\sqrt{3}}\cdot\frac{2\sqrt{3}}{2\sqrt{3}}=\frac{12+20\sqrt{3}}{-12}\doteq\underline{\underline{-1-2\sqrt{3}}}$$

$$\upsilon_2=\left(10+2\sqrt{3}\right)-\left(-2\sqrt{3}\right)\cdot\eta_2$$

$$\upsilon_2=\left(10+2\sqrt{3}\right)-\left(-2\sqrt{3}\right)\cdot\left(-1-2\sqrt{3}\right)=$$

$$=10+2\sqrt{3}-2\sqrt{3}-12=\underline{\underline{-2}}$$

$$10+2\sqrt{3}=\left(-1-2\sqrt{3}\right)\cdot\left(-2\sqrt{3}\right)+(-2)$$

3. $-2\sqrt{3}=\eta_3\cdot(-2)+\upsilon_3$

$$\eta_3=\frac{-2\sqrt{3}}{-2}=\underline{\underline{\sqrt{3}}}$$

$$\upsilon_3=\left(-2\sqrt{3}\right)-(-2)\cdot\eta_3$$

$$\upsilon_3=\left(-2\sqrt{3}\right)-(-2)\cdot\left(\sqrt{3}\right)=\underline{\underline{0}}$$

$$-2\sqrt{3}=\left(\sqrt{3}\right)\cdot(-2)+0$$

Pro přehlednost sepíšeme Euklidův algoritmus.

$$54+44\sqrt{3}=(3+4\sqrt{3})\cdot\left(10+2\sqrt{3}\right)+(-2\sqrt{3})$$

$$10+2\sqrt{3}=\left(-1-2\sqrt{3}\right)\cdot\left(-2\sqrt{3}\right)+\boxed{(-2)}$$

$$-2\sqrt{3}=\left(\sqrt{3}\right)\cdot(-2)+0$$

$$nsd\left(10+2\sqrt{3},54+44\sqrt{3}\right)=\underline{\underline{-2}}$$

Největší společný dělitel čísel $10+2\sqrt{3}$ a $54+44\sqrt{3}$ je číslo -2.

5.4 $\mathbb{Z}\left[i\sqrt{2}\right]$ JAKO OBOR INTEGRITY

V této části se budu zabývat množinou $\mathbb{Z}\left[i\sqrt{2}\right]$. Čísla této množiny mají tvar

$$\mathbb{Z}\left[i\sqrt{2}\right]=\{z=a+bi\sqrt{2},\text{ kde } a,b\in\mathbb{Z}\}.$$

Množina $\mathbb{Z}\left[i\sqrt{2}\right]$ bývá někdy psána jako množina $\mathbb{Z}\left[\sqrt{-2}\right]$. Tyto množiny jsou totožné a jsou podmnožinou tělesa všech komplexních čísel $(\mathbb{C},+,\cdot)$. Fakt, že tato množina tvoří obor integrity a splňuje podmínky Euklidova oboru integrity, bychom dokázali stejně jako v předešlých podkapitolách pro $\mathbb{Z}\left[\sqrt{2}\right]$ a $\mathbb{Z}[i]$.

Nadefinujeme si tedy jen Euklidovu normu N.

Euklidova norma v $\mathbb{Z}[i\sqrt{2}] = \{z = a + bi\sqrt{2}$, kde $a, b \in \mathbb{Z}\}$ je definována takto:

$$N(a + bi\sqrt{2}) = a^2 + 2b^2.$$

Stejně tak pro množinu $\mathbb{Z}[i\sqrt{3}] = \{z = a + bi\sqrt{3}$, kde $a, b \in \mathbb{Z}\}$, kde je norma definována takto:

$$N(a + bi\sqrt{3}) = a^2 + 3b^2.$$

5.4.1 NEJVĚTŠÍ SPOLEČNÝ DĚLITEL V $\mathbb{Z}[i\sqrt{2}]$

Spočtěte největšího společného dělitele čísel $24 - 17i\sqrt{2}$ a $4 + 32i\sqrt{2}$.

$$nsd(24 - 17i\sqrt{2}, 4 + 32i\sqrt{2}) = ?$$

Nejprve musíme určit Euklidovu normu obou čísel.

$$N(24 - 17i\sqrt{2}) = 24^2 + 2 \cdot 17^2 = \underline{\underline{1154}}$$

$$N(4 + 32i\sqrt{2}) = 4^2 + 2 \cdot 32^2 = \underline{\underline{2064}}$$

Z Euklidových norem vidíme, že číslo $24 - 17i\sqrt{2}$ má menší Euklidovu normu a proto s ním budeme dělit číslo $4 + 32i\sqrt{2}$. Euklidův algoritmus budeme opakovat, dokud nezískáme nulový zbytek.

1. $4 + 32i\sqrt{2} = \eta_1 \cdot (24 - 17i\sqrt{2}) + v_1$

$$\eta_1 = \frac{4 + 32i\sqrt{2}}{24 - 17i\sqrt{2}} = \frac{4 + 32i\sqrt{2}}{24 - 17i\sqrt{2}} \cdot \frac{24 + 17i\sqrt{2}}{24 + 17i\sqrt{2}} =$$

$$= \frac{96 + 68i\sqrt{2} + 768i\sqrt{2} + 544i^2 \cdot \sqrt{2}^2}{576 + 408i\sqrt{2} - 408i\sqrt{2} - 289i^2\sqrt{2}^2} = \frac{-992 + 836i\sqrt{2}}{576 + 578} =$$

$$= -\frac{992}{1154} + \frac{836i\sqrt{2}}{1154} \doteq \underline{\underline{-1 + i\sqrt{2}}}$$

$$v_1 = 4 + 32i\sqrt{2} - \eta_1 \cdot (24 - 17i\sqrt{2})$$

$$v_1 = 4 + 32i\sqrt{2} - (-1 + i\sqrt{2}) \cdot (24 - 17i\sqrt{2}) =$$

$$= 4 + 32i\sqrt{2} + 24 - 17i\sqrt{2} - 24i\sqrt{2} + 34i^2 =$$

$$= 28 - 9i\sqrt{2} - 34 = \underline{\underline{-6 - 9i\sqrt{2}}}$$

$$4 + 32i\sqrt{2} = (-1 + i\sqrt{2}) \cdot (24 - 17i\sqrt{2}) + (-6 - 9i\sqrt{2})$$

Vidíme, že zbytek $-6 - 9i\sqrt{2}$ je nenulový. V této fázi Euklidova algoritmu ještě nemůžeme určit největšího společného dělitele. Zbytek má Euklidovu normu 198, která je menší než Euklidova norma čísla $24 - 17i\sqrt{2}$ (1154), počítáme tedy správně. Budeme pokračovat v algoritmu. Nyní budeme dělit číslo $24 - 17i\sqrt{2}$ zbytkem $-6 - 9i\sqrt{2}$.

2. $24-17i\sqrt{2}=\eta_2\cdot\left(-6-9i\sqrt{2}\right)+v_2$

$$\eta_2=\frac{24-17i\sqrt{2}}{-6-9i\sqrt{2}}=\frac{24-17i\sqrt{2}}{-6-9i\sqrt{2}}\cdot\frac{-6+9i\sqrt{2}}{-6+9i\sqrt{2}}=$$

$$=\frac{-144+216i\sqrt{2}+102i\sqrt{2}-306i^2}{36-54i\sqrt{2}+54i\sqrt{2}-162i^2}=\frac{162+318i\sqrt{2}}{198}=$$

$$=\frac{162}{198}+\frac{318i\sqrt{2}}{198}\doteq\underline{\underline{1+2i\sqrt{2}}}$$

$$v_2=24-17i\sqrt{2}-\eta_2\cdot\left(-6-9i\sqrt{2}\right)$$

$$v_2=24-17i\sqrt{2}-\left(1+2i\sqrt{2}\right)\cdot\left(-6-9i\sqrt{2}\right)=$$

$$=24-17i\sqrt{2}-\left(-6-9i\sqrt{2}-12i\sqrt{2}-36i^2\right)=$$

$$=30+4i\sqrt{2}-36=\underline{\underline{-6+4i\sqrt{2}}}$$

$$24-17i\sqrt{2}=\left(1+2i\sqrt{2}\right)\cdot\left(-6-9i\sqrt{2}\right)+\left(-6+4i\sqrt{2}\right).$$

Jako v předchozím kroku, tak i nyní je zbytek $-6+4i\sqrt{2}$ nenulový. Zkontrolujeme Euklidovu normu zbytku $N(-6+4i\sqrt{2})=68$. Je tedy menší než Euklidova norma čísla $-6-9i\sqrt{2}$, počítáme správně a můžeme pokračovat v Euklidovu algoritmu. Dělíme číslo $-6-9i\sqrt{2}$ zbytkem $-6+4i\sqrt{2}$.

3. $-6-9i\sqrt{2}=\eta_3\cdot\left(-6+4i\sqrt{2}\right)+v_3$

$$\eta_3=\frac{-6-9i\sqrt{2}}{-6+4i\sqrt{2}}=\frac{-6-9i\sqrt{2}}{-6+4i\sqrt{2}}\cdot\frac{-6-4i\sqrt{2}}{-6-4i\sqrt{2}}=$$

$$=\frac{36+24i\sqrt{2}+56i\sqrt{2}+72i^2}{36+24i\sqrt{2}-24i\sqrt{2}-32i^2}=\frac{-36+80i\sqrt{2}}{68}=$$

$$=-\frac{36}{68}+\frac{80i\sqrt{2}}{68}\doteq\underline{\underline{-1+i\sqrt{2}}}$$

$$v_3=\left(-6-9i\sqrt{2}\right)-\left(-6+4i\sqrt{2}\right)\cdot\left(-1+i\sqrt{2}\right)=$$

$$=-6-9i\sqrt{2}-\left(6-6i\sqrt{2}-4i\sqrt{2}+8i^2\right)=-12+i\sqrt{2}-8i^2=$$

$$=\underline{\underline{-4+i\sqrt{2}}}$$

$$-6-9i\sqrt{2}=\left(-1+i\sqrt{2}\right)\cdot\left(-6+4i\sqrt{2}\right)+(-4+i\sqrt{2})$$

Stále je zbytek nenulový. Euklidova norma zbytku $-4+i\sqrt{2}$ (18) je opět menší než Euklidova norma čísla $-6+4i\sqrt{2}$, pomocí kterého jsme dělili číslo $-6-9i\sqrt{2}$, počítáme tedy správně. Dále budeme pokračovat v Euklidovu algoritmu. Budeme dělit číslo $-6+4i\sqrt{2}$ pomocí zbytku $-4+i\sqrt{2}$.

4. $-6+4i\sqrt{2}=\eta_4\cdot\left(-4+i\sqrt{2}\right)+\upsilon_4$

$$\eta_4=\frac{-6+4i\sqrt{2}}{-4+i\sqrt{2}}=\frac{-6+4i\sqrt{2}}{-4+i\sqrt{2}}\cdot\frac{-4-i\sqrt{2}}{-4-i\sqrt{2}}=$$

$$=\frac{24+6i\sqrt{2}-16i\sqrt{2}+8}{16+4i\sqrt{2}-4i\sqrt{2}+2}=\frac{32-10i\sqrt{2}}{18}=\frac{32}{18}-\frac{10}{18}i\sqrt{2}\doteq\underline{\underline{2-i\sqrt{2}}}$$

$$\upsilon_4=\left(-6+4i\sqrt{2}\right)-\left(-4+i\sqrt{2}\right)\cdot\eta_4$$

$$\upsilon_4=\left(-6+4i\sqrt{2}\right)-\left(-4+i\sqrt{2}\right)\cdot\left(2-i\sqrt{2}\right)=$$

$$=-6+4i\sqrt{2}-(-8+4i\sqrt{2}+2i\sqrt{2}+2)=\underline{\underline{-2i\sqrt{2}}}$$

$$-6+4i\sqrt{2}=\left(2-i\sqrt{2}\right)\cdot\left(-4+i\sqrt{2}\right)-2i\sqrt{2}$$

Zbytek je stále nenulový a Euklidova norma zbytku je oproti předchozímu menší, počítáme tedy správně a pokračujeme v Euklidovu algoritmu.

5. $-4+i\sqrt{2}=\eta_5\cdot\left(-2i\sqrt{2}\right)+\upsilon_5$

$$\eta_5=\frac{-4+i\sqrt{2}}{-2i\sqrt{2}}=\frac{-4+i\sqrt{2}}{-2i\sqrt{2}}\cdot\frac{2i\sqrt{2}}{2i\sqrt{2}}=$$

$$=\frac{-8i\sqrt{2}-4}{8}=-\frac{4}{8}-\frac{8}{8}i\sqrt{2}\doteq\underline{\underline{-1-i\sqrt{2}}}$$

Zde můžeme zaokrouhlit také na $-i\sqrt{2}$. Ani jedno zaokrouhlení nemá vliv na výsledek.

$$\upsilon_5=\left(-4+i\sqrt{2}\right)-\left(-2i\sqrt{2}\right)\cdot\eta_4$$

$$\upsilon_5=\left(-4+i\sqrt{2}\right)-\left(-2i\sqrt{2}\right)\cdot\left(-1-i\sqrt{2}\right)=$$

$$=-4+i\sqrt{2}-(2i\sqrt{2}-4)=\underline{\underline{-i\sqrt{2}}}$$

$$-4+i\sqrt{2}=\left(-1-i\sqrt{2}\right)\cdot\left(-2i\sqrt{2}\right)-i\sqrt{2}$$

Ani nyní nemáme nulový zbytek. Dále pokračujeme v Euklidovu algoritmu.

6. $-2i\sqrt{2}=\eta_6\cdot\left(-i\sqrt{2}\right)+\upsilon_6$

$$\eta_6=\frac{-2i\sqrt{2}}{-i\sqrt{2}}=\underline{\underline{2}}$$

$$\upsilon_6=\left(-2i\sqrt{2}\right)-\left(-i\sqrt{2}\right)\cdot(2)=-2i\sqrt{2}-(-2i\sqrt{2})=\underline{\underline{0}}$$

$$-2i\sqrt{2}=(2)\cdot\left(-i\sqrt{2}\right)+0$$

Nyní jsme získali nulový zbytek a můžeme určit největšího společného dělitele čísel $4+32i\sqrt{2}$ a $24-17i\sqrt{2}$.

Z dílčích výsledků si pro přehlednost sestavíme Euklidův algoritmus.

$$4 + 32i\sqrt{2} = \left(-1 + i\sqrt{2}\right) \cdot \left(24 - 17i\sqrt{2}\right) + (-6 - 9i\sqrt{2})$$
$$24 - 17i\sqrt{2} = \left(1 + 2i\sqrt{2}\right) \cdot \left(-6 - 9i\sqrt{2}\right) + (-6 + 4i\sqrt{2})$$
$$-6 - 9i\sqrt{2} = \left(-1 + i\sqrt{2}\right) \cdot \left(-6 + 4i\sqrt{2}\right) + (-4 + i\sqrt{2})$$
$$-6 + 4i\sqrt{2} = \left(2 - i\sqrt{2}\right) \cdot \left(-4 + i\sqrt{2}\right) - 2i\sqrt{2}$$
$$-4 + i\sqrt{2} = \left(-1 - i\sqrt{2}\right) \cdot \left(-2i\sqrt{2}\right)\boxed{-i\sqrt{2}}$$
$$-2i\sqrt{2} = (2) \cdot \left(-i\sqrt{2}\right) + 0$$
$$nsd\left(4 + 32i\sqrt{2}, 24 - 17i\sqrt{2}\right) = \underline{\underline{-i\sqrt{2}}}$$

Z Euklidova algoritmu je patrné, že největším společným dělitelem čísel $4 + 32i\sqrt{2}$ a $24 - 17i\sqrt{2}$ je číslo $-i\sqrt{2}$. Dále je správným výsledkem číslo komplexně sdružené k číslu $-i\sqrt{2}$, tedy $i\sqrt{2}$.

Pro kontrolu si provedeme zkoušku.

1. $-i\sqrt{2}$ musí dělit $4 + 32i\sqrt{2}$

$$\frac{4 + 32i\sqrt{2}}{-i\sqrt{2}} = \frac{4 + 32i\sqrt{2}}{-i\sqrt{2}} \cdot \frac{i\sqrt{2}}{i\sqrt{2}} = \frac{4i\sqrt{2} - 64}{2} = -32 + 2i\sqrt{2}$$

2. $-i\sqrt{2}$ musí dělit $24 - 17i\sqrt{2}$

$$\frac{24 - 17i\sqrt{2}}{-i\sqrt{2}} = \frac{24 - 17i\sqrt{2}}{-i\sqrt{2}} \cdot \frac{i\sqrt{2}}{i\sqrt{2}} = \frac{24i\sqrt{2} + 34}{2} = 17 + 12i\sqrt{2}$$

Číslo $-i\sqrt{2}$ dělí obě čísla, je tedy jejich společným dělitelem.

5.4.2 NEJVĚTŠÍ SPOLEČNÝ DĚLITEL V $\mathbb{Z}\left[i\sqrt{3}\right]$

Spočtěte největšího společného dělitele čísel $-16 - 22i\sqrt{3}$ a $82i\sqrt{3}$.

$$nsd\left(-16 - 22i\sqrt{3}, 82i\sqrt{3}\right) = ?$$
$$N\left(-16 - 22i\sqrt{3}\right) = \underline{\underline{1708}}$$
$$N\left(82i\sqrt{3}\right) = \underline{\underline{20172}}$$

1. $82i\sqrt{3} = \eta_1 \cdot \left(-16 - 22i\sqrt{3}\right) + v_1$

$$\eta_1 = \frac{82i\sqrt{3}}{-16 - 22i\sqrt{3}} = \frac{82i\sqrt{3}}{-16 - 22i\sqrt{3}i} \cdot \frac{-16 + 22i\sqrt{3}}{-16 + 22i\sqrt{3}} =$$

$$= \frac{-1312i\sqrt{3} - 5412}{256 + 352i\sqrt{3} - 352i\sqrt{3} + 1452} = -\frac{5412}{1708} - \frac{1312i\sqrt{3}}{1708} \doteq \underline{\underline{-3 - i\sqrt{3}}}$$

$$v_1 = \left(82i\sqrt{3}\right) - \left(-16 - 22i\sqrt{3}\right) \cdot \eta_1$$

$$v_1 = \left(82i\sqrt{3}\right) - \left(-16 - 22i\sqrt{3}\right) \cdot \left(-3 - i\sqrt{3}\right) =$$

$$= 82i\sqrt{3} - 48 - 66i\sqrt{3} - 16i\sqrt{3} + 66 = \underline{\underline{18}}$$

$$82i\sqrt{3} = \left(-3 - i\sqrt{3}\right) \cdot \left(-16 - 22i\sqrt{3}\right) + 18$$

2. $-16 - 22i\sqrt{3} = \eta_2 \cdot 18 + v_2$

$$\eta_2 = \frac{-16 - 22i\sqrt{3}}{18} = -\frac{16}{18} - \frac{22}{18}i\sqrt{3} \doteq \underline{\underline{-1 - i\sqrt{3}}}$$

$$v_2 = \left(-16 - 22i\sqrt{3}\right) - 18 \cdot \eta_2$$

$$v_2 = \left(-16 - 22i\sqrt{3}\right) - 18 \cdot \left(-1 - i\sqrt{3}\right) =$$

$$= -16 - 22i\sqrt{3} + 18i\sqrt{3} + 18 = \underline{\underline{2 - 4i\sqrt{3}}}$$

$$-16 - 22i\sqrt{3} = 18 \cdot \left(-1 - i\sqrt{3}\right) + (2 - 4i\sqrt{3})$$

3. $18 = \eta_3 \cdot \left(2 - 4i\sqrt{3}\right) + v_3$

$$\eta_3 = \frac{18}{2 - 4i\sqrt{3}} = \frac{18}{2 - 4i\sqrt{3}} \cdot \frac{2 + 4i\sqrt{3}}{2 + 4i\sqrt{3}} = \frac{36 + 72i\sqrt{3}}{4 + 48} \doteq \underline{\underline{1 + i\sqrt{3}}}$$

$$v_3 = 18 - \left(2 - 4i\sqrt{3}\right) \cdot \left(1 + i\sqrt{3}\right) =$$

$$= 18 - 2 - 2i\sqrt{3} + 4i\sqrt{3} - 12 = \underline{\underline{4 + 2i\sqrt{3}}}$$

$$18 = \left(1 + i\sqrt{3}\right) \cdot \left(2 - 4i\sqrt{3}\right) + (4 + 2i\sqrt{3})$$

4. $2 - 4i\sqrt{3} = \eta_4 \cdot \left(4 + 2i\sqrt{3}\right) + v_4$

$$\eta_4 = \frac{2 - 4i\sqrt{3}}{4 + 2i\sqrt{3}} = \frac{2 - 4i\sqrt{3}}{4 + 2i\sqrt{3}} \cdot \frac{4 - 2i\sqrt{3}}{4 - 2i\sqrt{3}} =$$

$$= \frac{8 - 4i\sqrt{3} - 16i\sqrt{3} - 24}{28} = -\frac{16}{28} - \frac{20i\sqrt{3}}{28} \doteq \underline{\underline{-1 - i\sqrt{3}}}$$

$$v_4 = \left(2 - 4i\sqrt{3}\right) - \left(4 + 2i\sqrt{3}\right) \cdot \eta_4$$

$$v_4 = \left(2 - 4i\sqrt{3}\right) - \left(4 + 2i\sqrt{3}\right) \cdot \left(-1 - i\sqrt{3}\right) =$$

$$= 2 - 4i\sqrt{3} + 4 + 4i\sqrt{3} + 2i\sqrt{3} - 6 = \underline{\underline{2i\sqrt{3}}}$$

$$2 - 4i\sqrt{3} = \left(-1 - i\sqrt{3}\right) \cdot \left(4 + 2i\sqrt{3}\right) + 2i\sqrt{3}$$

5. $4 + 2i\sqrt{3} = \eta_5 \cdot 2i\sqrt{3} + v_5$

$$\eta_5 = \frac{4 + 2i\sqrt{3}}{2i\sqrt{3}} = \frac{4 + 2i\sqrt{3}}{2i\sqrt{3}} \cdot \frac{-2i\sqrt{3}}{-2i\sqrt{3}} = \frac{12 - 8i\sqrt{3}}{12} \doteq \underline{\underline{1 - i\sqrt{3}}}$$

$$v_5 = \left(4 + 2i\sqrt{3}\right) - 2i\sqrt{3} \cdot \eta_5$$

$$v_5 = \left(4 + 2i\sqrt{3}\right) - 2i\sqrt{3} \cdot \left(1 - i\sqrt{3}\right) = 4 + 2i\sqrt{3} - 2i\sqrt{3} - 6 = \underline{\underline{-2}}$$

$$4 + 2i\sqrt{3} = \left(1 - i\sqrt{3}\right) \cdot 2i\sqrt{3} - 2$$

6. $2i\sqrt{3} = \eta_6 \cdot (-2) + v_6$

$$\eta_6 = \frac{2i\sqrt{3}}{-2} = \underline{\underline{-i\sqrt{3}}}$$

$$v_6 = \left(2i\sqrt{3}\right) - (-2) \cdot \eta_5$$

$$v_6 = \left(2i\sqrt{3}\right) - (-2) \cdot \left(-i\sqrt{3}\right) = \underline{\underline{0}}$$

$$2i\sqrt{3} = \left(-i\sqrt{3}\right) \cdot (-2) + 0$$

Z dílčích výsledků si pro přehlednost sestavíme Euklidův algoritmus.

$$82i\sqrt{3} = \left(-3 - i\sqrt{3}\right) \cdot \left(-16 - 22i\sqrt{3}\right) + 18$$

$$-16 - 22i\sqrt{3} = 18 \cdot \left(-1 - i\sqrt{3}\right) + (2 - 4i\sqrt{3})$$

$$18 = \left(1 + i\sqrt{3}\right) \cdot \left(2 - 4i\sqrt{3}\right) + (4 + 2i\sqrt{3})$$

$$2 - 4i\sqrt{3} = \left(-1 - i\sqrt{3}\right) \cdot \left(4 + 2i\sqrt{3}\right) + 2i\sqrt{3}$$

$$4 + 2i\sqrt{3} = \left(1 - i\sqrt{3}\right) \cdot 2i\sqrt{3}\,\boxed{-2}$$

$$2i\sqrt{3} = \left(-i\sqrt{3}\right) \cdot (-2) + 0$$

Odtud vidíme, že výsledkem je číslo -2.

$$nsd\left(-16 - 22i\sqrt{3}, 82i\sqrt{3}\right) = \underline{\underline{-2}}$$

Pro kontrolu si provedeme zkoušku.

1. -2 musí dělit $-16 - 22i\sqrt{3}$

$$\frac{-16 - 22i\sqrt{3}}{-2} = 8 - 11i\sqrt{3}$$

2. -2 musí dělit $82i\sqrt{3}$

$$\frac{82i\sqrt{3}}{-2} = 41i\sqrt{3}$$

Číslo -2 dělí obě čísla, je tedy jejich společným dělitelem.

5.4.3 NEJMENŠÍ SPOLEČNÝ NÁSOBEK V $\mathbb{Z}[i\sqrt{3}]$

Spočtěte nejmenší společný násobek čísel $-16-22i\sqrt{3}$ a $82i\sqrt{3}$.

$$nsn\left(-16-22i\sqrt{3}, 82i\sqrt{3}\right) = ?$$

Největšího společného dělitele jsme spočítali v předchozím příkladě, můžeme tedy rovnou dosadit.

$$nsd\left(-16-22i\sqrt{3}, 82i\sqrt{3}\right) = \underline{\underline{-2}}$$

$$nsn\left(-16-22i\sqrt{3}, 82i\sqrt{3}\right) = \frac{\left(-16-22i\sqrt{3}\right)\cdot\left(82i\sqrt{3}\right)}{-2} =$$

$$= \frac{5412-1312i\sqrt{3}}{-2} = \underline{\underline{-2706+656\sqrt{3}}}$$

Nejmenším společným násobkem čísel $-16-22i\sqrt{3}$ a $82i\sqrt{3}$ je číslo $-2706+656\sqrt{3}$.

5.5 OBOR INTEGRITY POLYNOMŮ

Nechť $(T,+,\cdot)$ je komutativní těleso a n přirozené číslo. Funkci $f_{(x)}$ definovanou předpisem

$$f_{(x)} = a_n x^n + a_{n-1}x^{n-1} + \ \ldots + a_2x^2 + a_1x + a_0, \text{ kde } a_n \neq 0,$$

nazýváme **polynomem n-tého stupně o jedné proměnné x nad tělesem** $(T,+,\cdot)$. Prvky $a_n,\ a_{n-1},\ \ldots,\ a_2,\ a_1, a_0 \in (T,+,\cdot)$ nazýváme **koeficienty polynomu.** Stupeň polynomu $f_{(x)}$ značíme $st\left[f_{(x)}\right]$.

Věta 1: Algebraická struktura $(T[x],+,\cdot)$ je oborem integrity.[Drábek, 2001]

Tuhle větu nebudeme dokazovat. Snadno bychom ukázali, že je splněno všech osm axiomů oboru integrity.

Ukážeme, že algebraická struktura $(T[x],+,\cdot)$ je Euklidovým oborem integrity.
Euklidovou normou ve struktuře $(T[x],+,\cdot)$ je stupeň polynomu.

První podmínka říká, že $f_{(x)}|g_{(x)} \Rightarrow st\left[f_{(x)}\right] \leq st\left[g_{(x)}\right]$.
Protože Euklidovou normou u polynomů je stupeň polynomu, což je nejvyšší mocnina u proměnné (v našem případě x), budou nás zajímat pouze členy s nejvyšší mocninou.
Nechť $f_{(x)} = a_n x^n$ a $g_{(x)} = b_m x^m$, kde $m,n \in \mathbb{N}$. Aby platilo $f_{(x)}|g_{(x)}$, musí nutně platit $n \leq m$. Takže

$$n \leq m \Rightarrow f_{(x)}|g_{(x)} \Rightarrow st\left[f_{(x)}\right] \leq st\left[g_{(x)}\right].$$

Platí tedy první podmínka Euklidova oboru integrity.

Věta 2: Budiž dány polynomy $f_{(x)} \neq 0$ a $g_{(x)}$ z oboru integrity $(T[x], +, \cdot)$**,** kde je Euklidova norma $(g_{(x)}) \geq 1$, potom existují polynomy $R_{(x)}$ a $Q_{(x)}$ takové, že platí

$$f_{(x)} = Q_{(x)} \cdot g_{(x)} + R_{(x)}, \text{ kde } R_{(x)} = 0 \vee st[R_{(x)}] < st[g_{(x)}],$$

tyto polynomy jsou jednoznačně určené. [Drábek, 2001]

Z věty 2 je patrné, že je splněna druhá podmínka Euklidova oboru integrity.

Platí obě podmínky Euklidova oboru integrity a obor integrity polynomů je Euklidův.

Dva **polynomy $f_{(x)}$ a $g_{(x)}$ jsou spolu asociovány** právě tehdy, když existuje nenulový prvek $c \in T$ takový, že platí $f_{(x)} = c \cdot g_{(x)}$. V jakékoliv úvaze o dělitelnosti polynomů můžeme libovolný polynom nahradit polynomem asociovaným. Asociované polynomy jsou ve smyslu dělitelnosti ekvivalentní (rovnocenné).[Procházka, 1990]

V následujících příkladech uvažujeme polynomy s racionálními koeficienty.

5.5.1 NEJVĚTŠÍ SPOLEČNÝ DĚLITEL POLYNOMŮ

Spočtěte největšího společného dělitele polynomů $P_{(x)}$ a $Q_{(x)}$.

$$P_{(x)} = x^5 + x^4 - 6x^3 - 7x^2 - 7x$$

$$Q_{(x)} = 2x^4 + 2x^3 + x^2 - x - 1$$

$$nsd(P_{(x)}, Q_{(x)}) = ?$$

Výpočet provedeme opět Euklidovým algoritmem. Aby nám nevycházely ve výsledcích zlomky, můžeme polynomy $P_{(x)}$ a $Q_{(x)}$ nahradit polynomy asociovanými. Tato náhrada nám nezmění největšího společného dělitele.

Polynom $P_{(x)} = x^5 + x^4 - 6x^3 - 7x^2 - 7x$ vynásobíme číslem 2 a získáme polynom $P'_{(x)} = 2x^5 + 2x^4 - 12x^3 - 14x^2 - 14x$, který je asociovaný s polynomem $P_{(x)}$ a při dělení polynomem $Q_{(x)} = 2x^4 + 2x^3 + x^2 - x - 1$ nám budou vycházet celočíselné koeficienty.

1. $2x^5 + 2x^4 - 12x^3 - 14x^2 - 14x = \eta_1 \cdot (2x^4 + 2x^3 + x^2 - x - 1) + \upsilon_1$

$$(2x^5 + 2x^4 - 12x^3 - 14x^2 - 14x) : (2x^4 + 2x^3 + x^2 - x - 1) = \underline{x}$$

$$-\underline{(2x^5 + 2x^4 + 1x^3 - 1x^2 - 1x)}$$

$$\underline{\underline{-13x^3 - 13x^2 - 13x}}$$

Z dělení se zbytkem plyne, že $\eta_1 = x$ a $\upsilon_1 = -13x^3 - 13x^2 - 13x$.

Zkouška:

$$L = 2x^5 + 2x^4 - 12x^3 - 14x^2 - 14x$$

$$P = x \cdot (2x^4 + 2x^3 + x^2 - x - 1) - 13x^3 - 13x^2 - 13\text{x} =$$

$$= 2x^5 + 2x^4 + x^3 - x^2 - x - 13x^3 - 13x^2 - 13x =$$

$$= 2x^5 + 2x^4 - 12x^3 - 14x^2 - 14x$$

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

Tím máme první řádek Euklidova algoritmu. Na první pohled je patrné, že máme nenulový zbytek $\upsilon_1 = -13x^3 - 13x^2 - 13x$. Pokračujeme v Euklidovu algoritmu.

Nyní budeme dělit polynom $Q_{(x)} = 2x^4 + 2x^3 + x^2 - x - 1$ polynomem asociovaným s polynomem $\upsilon_1 = -13x^3 - 13x^2 - 13x$, tedy $\upsilon'_1 = x^3 + x^2 + x$.

2. $2x^4 + 2x^3 + x^2 - x - 1 = \eta_2 \cdot (x^3 + x^2 + x) + \upsilon_2$

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

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

$$\underline{\underline{-x^2 - x - 1}}$$

Vidíme, že $\eta_2 = 2x$ a $\upsilon_2 = -x^2 - x - 1$.

I po druhém kroku máme stále nenulový zbytek $\upsilon_2 = -x^2 - x - 1$.

Zkouška:

$$L = 2x^4 + 2x^3 + x^2 - x - 1$$

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

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

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

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

Pokračujeme v Euklidovu algoritmu. Dělíme polynom $\upsilon'_1 = x^3 + x^2 + x$ polynomem $\upsilon'_2 = x^2 + x + 1$, který je asociován s polynomem $\upsilon_2 = -x^2 - x - 1$.

3. $x^3 + x^2 + x = \eta_3 \cdot (x^2 + x + 1) + \upsilon_3$

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

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

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

Vidíme, že $\eta_3 = x$ a $\upsilon_3 = 0$.

Na první pohled je patrné, že máme nulový zbytek a můžeme určit největšího společného dělitele polynomů $P_{(x)}$ a $Q_{(x)}$.

Zkouška:

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

Pro přehlednost ještě sestavíme Euklidův algoritmus.

$$P_{(x)} = x \cdot (2x^4 + 2x^3 + x^2 - x - 1) - 13x^3 - 13x^2 - 13\text{x}$$
$$2x^4 + 2x^3 + x^2 - x - 1 = 2x \cdot (x^3 + x^2 + x) - \boxed{(x^2 + x + 1)}$$
$$x^3 + x^2 + x = x \cdot (3\,x^2 + x + 1) + 0$$
$$nsd\big(P_{(x)}, Q_{(x)}\big) = \underline{\underline{x^2 + x + 1}}$$

Největším společným dělitelem polynomů $P_{(x)}$ a $Q_{(x)}$ je polynom $R_{(x)} = x^2 + x + 1$.

5.5.2 NEJVĚTŠÍ SPOLEČNÝ DĚLITEL POLYNOMŮ (2)

Spočtěte největšího společného dělitele polynomů $P_{(x)}$ a $Q_{(x)}$.

$$P_{(x)} = x^3 + 4x^2 + 4x + 3$$
$$Q_{(x)} = x^3 + 3x^2 + x + 3$$
$$nsd\big(P_{(x)}, Q_{(x)}\big) = ?$$

1. $x^3 + 4x^2 + 4x + 3 = \eta_1 \cdot (x^3 + 3x^2 + x + 3) + \upsilon_1$

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

Zkouška:

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

2. $x^3 + 3x^2 + x + 3 = \eta_2 \cdot (x^2 + 3x) + v_2$

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

Zkouška:

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

3. $x^2 + 3x = \eta_3 \cdot (x + 3) + v_3$

$$(x^2 + 3x) : (x + 3\ ) = \underline{\underline{x}}$$
$$-\underline{(x^2 + 3x)}$$
$$\underline{\underline{0}}$$

Sestavíme Euklidův algoritmus.

$$x^3 + 4x^2 + 4x + 3 = 1 \cdot (x^3 + 3x^2 + x + 3) + x^2 + 3x$$
$$x^3 + 3x^2 + x + 3 = x \cdot (x^2 + 3x) + \boxed{x + 3}$$
$$x^2 + 3x = x \cdot (x + 3) + 0$$
$$nsd(x^3 + 4x^2 + 4x + 3, x^3 + 3x^2 + x + 3) = \underline{\underline{x + 3}}$$

Největším společným dělitelem polynomů $P_{(x)}$ a $Q_{(x)}$ je polynom $R_{(x)} = x + 3$.

5.5.3 NEJMENŠÍ SPOLEČNÝ NÁSOBEK POLYNOMŮ

Spočtěte nejmenší společný násobek polynomů $P_{(x)}$ a $Q_{(x)}$.

$$P_{(x)} = x^4 - 2x^3 - 2x^2 + 7x - 6$$
$$Q_{(x)} = 2x^3 - 4x^2 - x + 2$$
$$nsn\left(P_{(x)}, Q_{(x)}\right) = ?$$

Nejdříve spočteme největšího společného dělitele. S jeho pomocí poté spočteme nejmenší společný násobek.

$$nsd\left(P_{(x)}, Q_{(x)}\right) = ?$$

1. $2x^4 - 4x^3 - 4x^2 + 14x - 12 = \eta_1 \cdot (2x^3 - 4x^2 - x + 2) + \upsilon_1$

$$(2x^4 - 4x^3 - 4x^2 + 14x - 12) : (2x^3 - 4x^2 - x + 2) = \underline{\underline{x}}$$
$$-\underline{(2x^4 - 4x^3 - x^2 + 2x)}$$
$$\underline{\underline{-3x^2 + 12x - 12}}$$

Zkouška:

$$L = 2x^4 - 4x^3 - 4x^2 + 14x - 12$$
$$P = x \cdot (2x^3 - 4x^2 - x + 2) - 3x^2 + 12x - 12 =$$
$$= 2x^4 - 4x^3 - x^2 + 2x - 3x^2 + 12x - 12 =$$
$$= 2x^4 - 4x^3 - 4x^2 + 14x - 12$$
$$\underline{\underline{L = P}}.$$

2. $2x^3 - 4x^2 - x + 2 = \eta_2 \cdot (x^2 - 4x + 4) + \upsilon_2$

$$(2x^3 - 4x^2 - x + 2) : (x^2 - 4x + 4x\ ) = \underline{\underline{2x + 4}}$$
$$-\underline{(2x^3 - 8x^2 + 8x)}$$
$$4x^2 - 9x + 2$$
$$\underline{-(4x^2 - 16x + 16)}$$
$$\underline{\underline{7x - 14}}$$

Zkouška:

$$L = 2x^3 - 4x^2 - x + 2$$
$$P = (2x + 4) \cdot (x^2 - 4x + 4) + 7x - 14 =$$
$$= 2x^3 - 8x^2 + 8x + 4x^2 - 16x + 16 + 7x - 14 = 2x^3 - 4x^2 - x + 2$$
$$\underline{\underline{L = P}}.$$

3. $7x^2 - 28x + 28\ = \eta_3 \cdot (x - 2) + \upsilon_3$

$$(7x^2 - 28x + 28) : (x - 2\ ) = \underline{\underline{7x - 14}}$$
$$-\underline{(7x^2 - 14x)}$$
$$-14x + 28$$
$$\underline{-(-14x + 28)}$$
$$\underline{\underline{0}}$$

Zkouška:

$$L = 7x^2 - 28x + 28$$
$$P = (7x - 14) \cdot (\mathrm{x} - 2) = 7x^2 - 14x - 14x + 28 =$$
$$= 7x^2 - 28x + 28$$
$$\underline{\underline{L = P}}.$$

Z Euklidova algoritmu vidíme, že největším společným dělitelem polynomů $P_{(x)}$ a $Q_{(x)}$ je polynom $R_{(x)} = x - 2$, který je asociován s polynomem $\eta_3 = 7x - 14$. Mohlo by se zdát, že je polynom $\eta_3 = 7x - 14$ „větší", ale u polynomů je Euklidovou normou stupeň polynomu. Oba polynomy mají tedy stejnou Euklidovu normu a jsou stejně „velké". Obecně zapisujeme polynomy s co nejmenším koeficientem u členu s nejvyšší mocninou.

Nyní ještě dopočteme nejmenší společný násobek polynomů $P_{(x)}$ a $Q_{(x)}$ pomocí vzorce.

$$nsn\left(P_{(x)}, Q_{(x)}\right) = \frac{P_{(x)} \cdot Q_{(x)}}{nsd(P_{(x)}, Q_{(x)})}$$

$$nsn\left(P_{(x)}, Q_{(x)}\right) = \frac{2x^7 - 8x^6 + 3x^5 + 26x^4 - 42x^3 + 13x^2 + 20x - 12}{x - 2} =$$

$$= \frac{(x-2)(2x^6 - 4x^5 - 5x^4 + 16x^3 - 10x^2 - 7x + 6)}{x - 2} =$$

$$= \underline{2x^6 - 4x^5 - 5x^4 + 16x^3 - 10x^2 - 7x + 6}$$

Nejmenším společným násobkem polynomů $P_{(x)}$ a $Q_{(x)}$ je polynom:

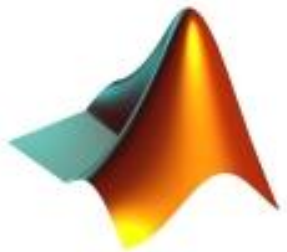
$$S_{(x)} = 2x^6 - 4x^5 - 5x^4 + 16x^3 - 10x^2 - 7x + 6.$$

5.6 VÝPOČET NSN A NSD POMOCÍ POČÍTAČOVÝCH PROGRAMŮ

V této podkapitole si ukážeme výpočet největšího společného dělitele a nejmenšího společného násobku v programech MATLAB, Wolfram Mathematica a Wolfram|Alpha.

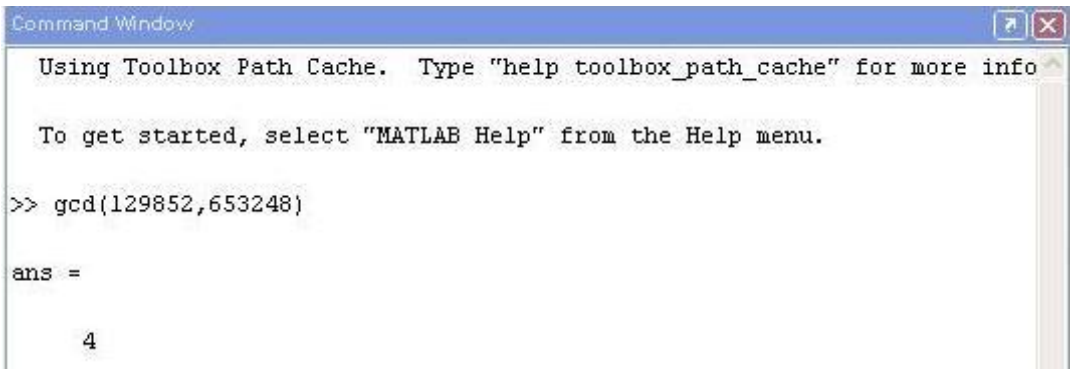
5.6.1 MATLAB

Program MATLAB je v dnešní době nejrozšířenějším matematickým softwarem. Zvládá základní matematické operace a vykreslování grafů pomocí přednastavených funkcí. Dále je možnost si další operace naprogramovat, což ulehčí práci při počítání velkého počtu stejných příkladů.



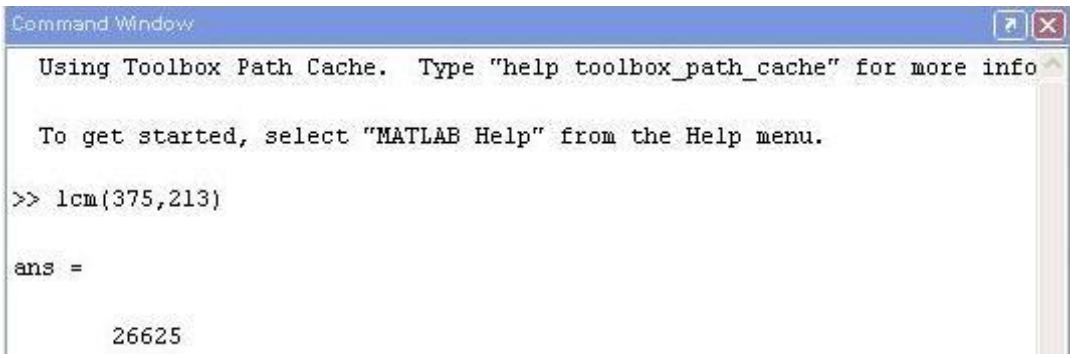
Obrázek 4 - Logo programu MATLAB

Pomocí příkazu $gcd(a,b)$ nám program spočte největší společný násobek čísel a a b. Výsledek je značen ans (answer – odpověď). Gcd je zkratka anglického greatest common divisor, což je v překladu největší společný dělitel.



Obrázek 5 - Ukázka výpočtu nsd v programu MATLAB

Pro nejmenší společný násobek funguje příkaz $lcm(a,b)$, který je zkratkou anglického least common multiple (v překladu nejmenší společný násobek).



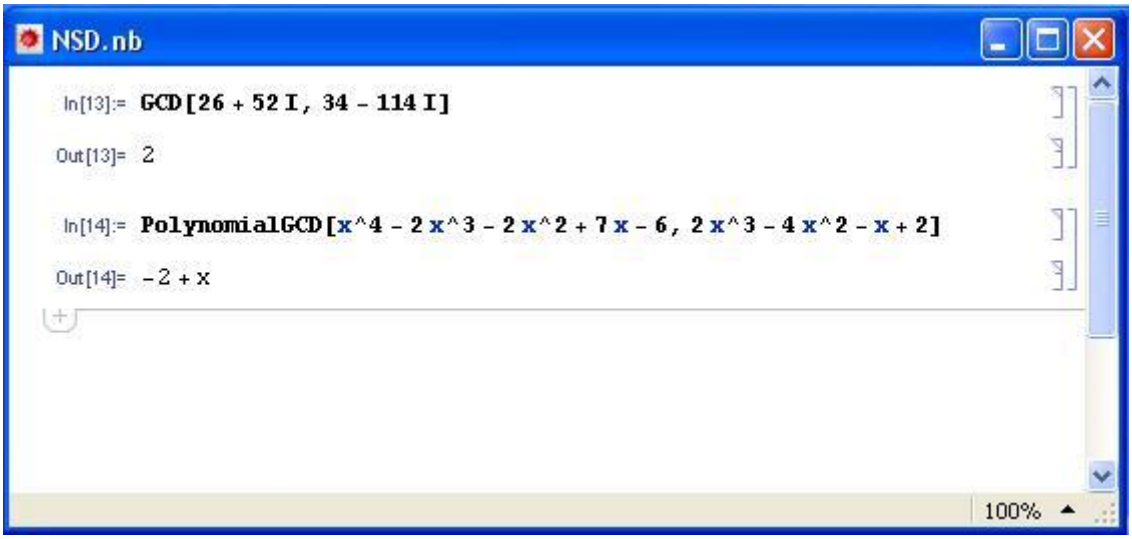
Obrázek 6 - Ukázka výpočtu nsn v programu MATLAB

Nevýhodou tohoto programu je vysoká pořizovací cena, bohužel nemá žádnou bezplatnou verzi.

5.6.2 WOLFRAM MATHEMATICA

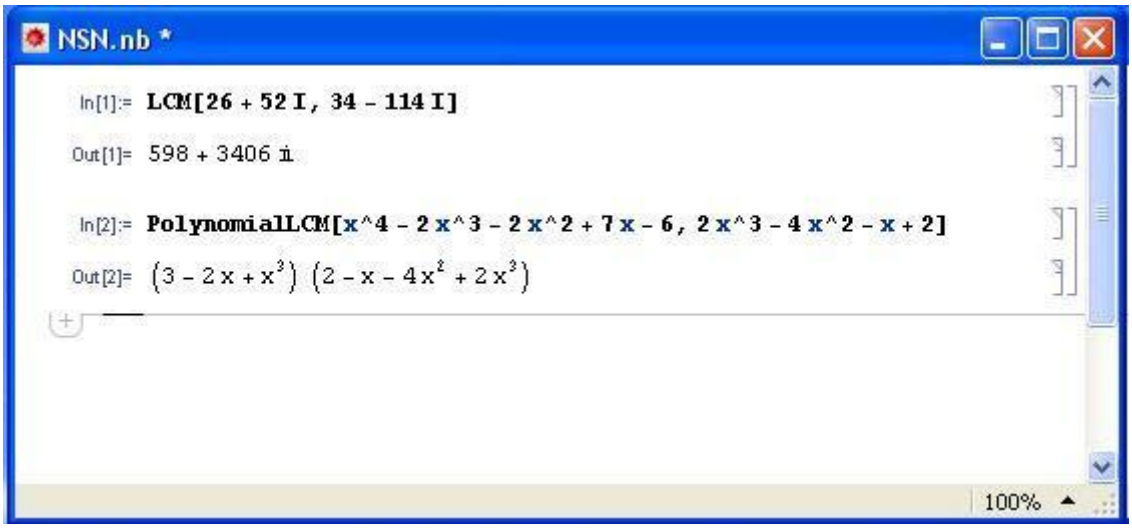
Obrázek 7 - Logo programu Wolfram Mathematica 8

Program Wolfram Mathematica nám, stejně jako program MATLAB, umožňuje používat přednastavené operace a další si můžeme naprogramovat. Pro největšího společného dělitele celých a komplexních čísel slouží příkaz $GCD[a, b]$. Pro největšího společného dělitele polynomů příkaz $PolynomialGCD[a, b]$. Výsledek je značen Out, což je v překladu výstup. Vstup je značen In.



Obrázek 8 - Ukázka výpočtu nsd v programu Wolfram Mathematica

Pro nejmenší společný násobek použijeme příkazy $LCM[a, b]$ a $PolynomialLCM[a, b]$.



Obrázek 9 - Ukázka výpočtu nsn v programu Wolfram Mathematica

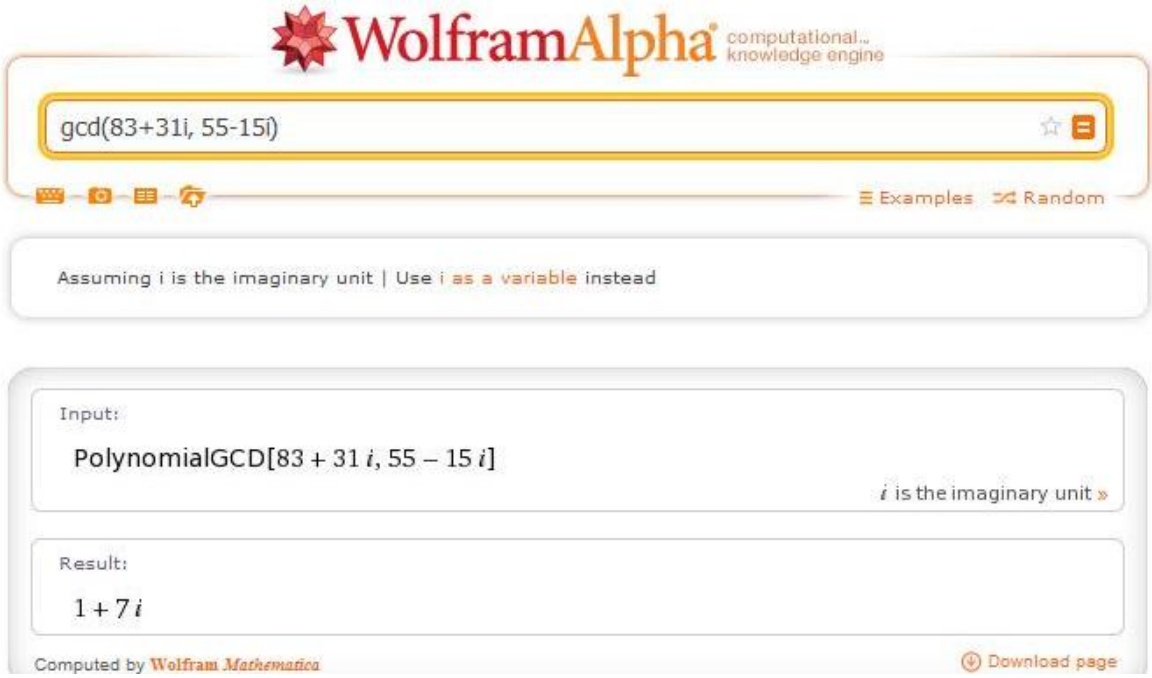
Program Wolfram Mathematica nám bohužel neposkytuje bezplatnou verzi.

5.6.3 WOLFRAM|ALPHA

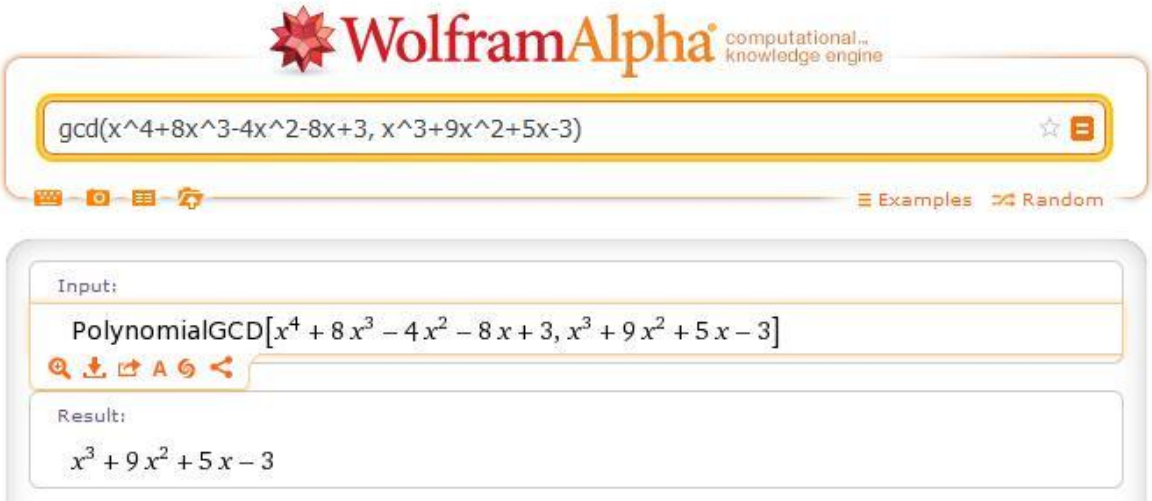
Wolfram|Alpha je internetový server, který umožňuje řadu matematických operací. Jedná se o obdobu programu Wolfram Mathematica, který je volně dostupný na Internetu. Ve své bezplatné verzi umožňuje přístup k předdefinovaným funkcím, které nám zobrazí výsledek zvolené operace. Placená verze dále zobrazuje postup výpočtu a umožňuje další užitečné funkce.

Obrázek 10 - Logo Wolfram|Alpha

Pomocí příkazu $gcd(a, b)$ nám vypočte největšího společného dělitele čísel a a b v mnoha číselných množinách, včetně prostoru polynomů. Výsledek je zobrazen jako $Result$.

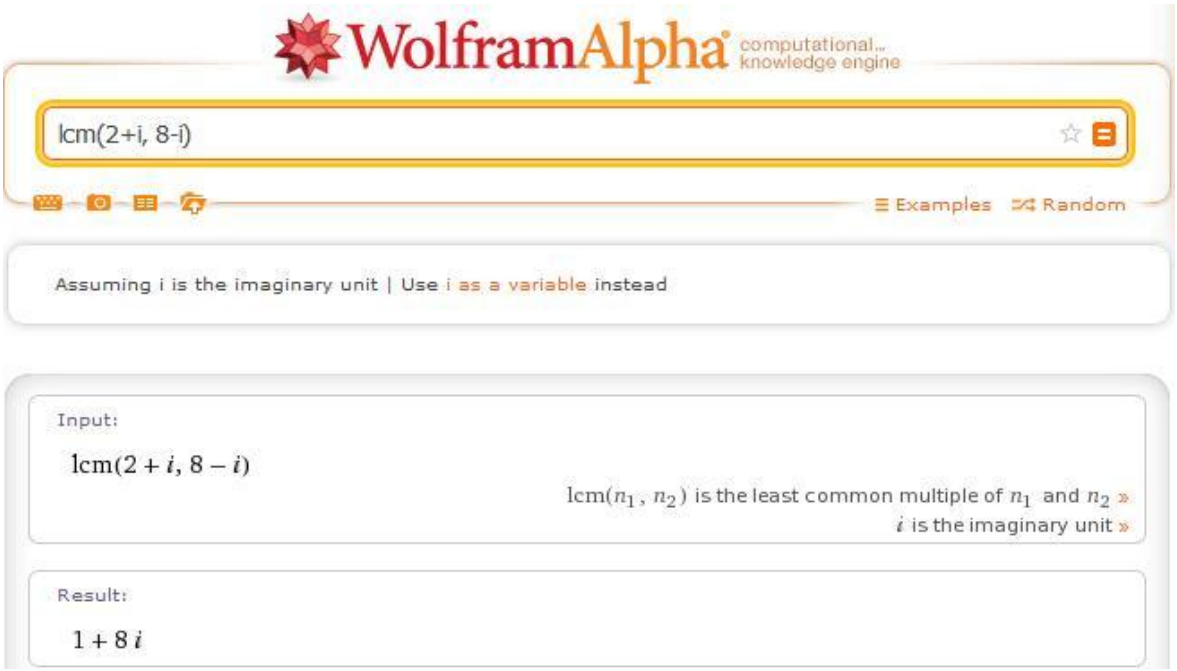


Obrázek 11 - Ukázka výpočtu nsd Gaussových čísel na serveru Wolfram|Alpha



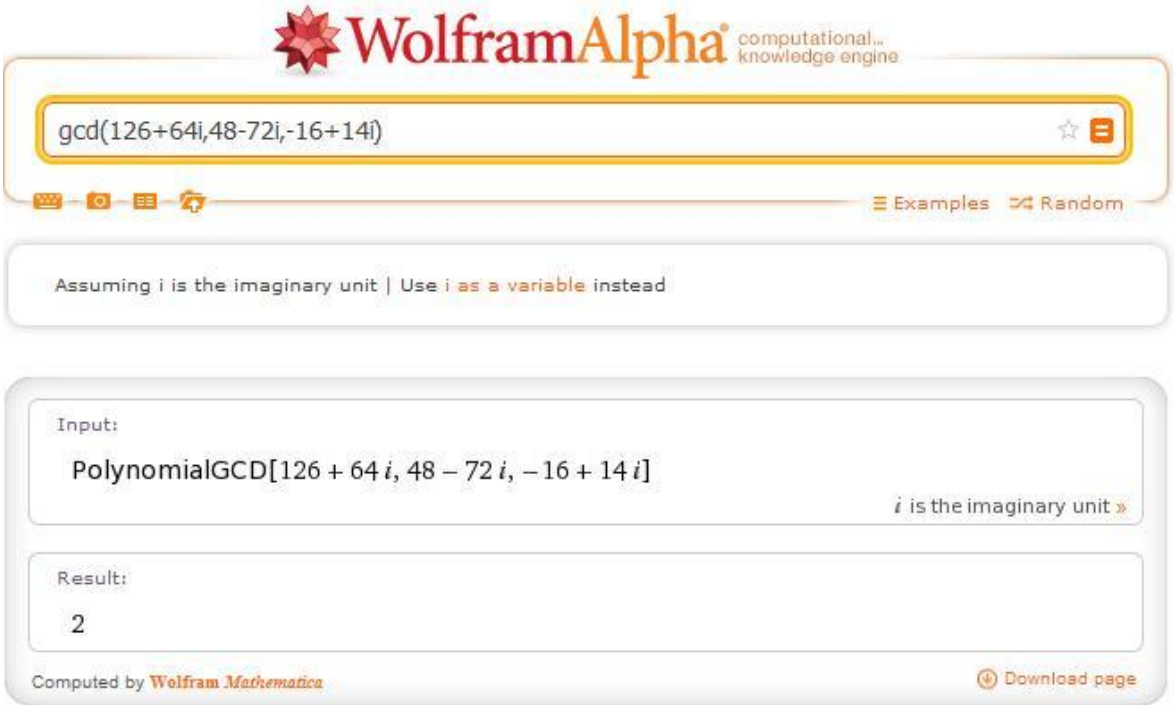
Obrázek 12 - Ukázka výpočtu nsd polynomů na serveru Wolfram|Alpha

Stejně funguje i příkaz pro nejmenší společný násobek $lcm(a, b)$.



Obrázek 13 - Ukázka výpočtu nsn na serveru Wolfram|Alpha

Všechny tři programy nám umožňují počítat násobky a dělitele více než dvou čísel současně, stačí do závorky za příkaz zadat více prvků.



Obrázek 14 - Ukázka výpočtu nsd tří prvků na serveru Wolfram|Alpha

Dále musíme počítat s tím, že všechny tři ukázané programy nejsou bezchybné, proto je důležité si výsledek zkontrolovat v dalším programu nebo si udělat zkoušku.

6 OBOR INTEGRITY NESPLŇUJÍCÍ PODMÍNKU KŘVD

Najít množinu prvků, která tvoří obor integrity a splňuje podmínku konečnosti řetězce vlastních dělitelů (KŘVD), není problém. Takových množin existuje celá řada $(\mathbb{Z}, \mathbb{Z}[i], \dots)$. Zaměříme se tedy na množinu prvků, která tvoří obor integrity, ale nesplňuje podmínku KŘVD, tudíž není Gaussovým oborem integrity.

Nechť R je libovolný obor integrity. Symbolem S označíme množinu prvků, jejíž prvky jsou formální součty ve tvaru

$$r_1 \cdot a_1 + r_2 \cdot a_2 + \dots + r_n \cdot a_n,$$

kde $n \in \mathbb{N}$, $r_1, r_2, \dots, r_n$ jsou nenulové prvky oboru integrity R a $a_1, a_2, \dots, a_n$ jsou nezáporná racionální čísla $\mathbb{Q}$, přičemž $a_1 < a_2 < \dots < a_n$.

Neutrálním (nulovým) prvkem v množině S bude prázdný součet pro $n = 0$ a budeme ho značit σ. Značení σ použijeme kvůli odlišení neutrálního prvku množiny S od neutrálního prvku O v množině všech racionálních číslech.

Nyní musíme dokázat, že námi zvolená množina S tvoří obor integrity, to znamená ověřit platnost základních axiomů oboru integrity.

6.1 OPERACE SČÍTÁNÍ

Nejdříve si musíme nadefinovat operaci sčítání $(+)$ na množině S a ověřit platnost axiomů pro operaci sčítání, což jsou komutativnost, asociativita, existence neutrálního a inverzního prvku.

Součet dvou prvků množiny S provedeme sepsáním prvků za sebe a upravením na vhodný tvar přehazováním jednotlivých členů podle tohoto pravidla:

$$r \cdot a + s \cdot a = (r + s) \cdot a, \text{ kde } r, s \in R, r \neq 0, s \neq 0, r + s \neq 0, a \in \mathbb{Q}, a \geq 0.$$

Pokud $r + s = 0$, pak je součet $r \cdot a + s \cdot a$ roven neutrálnímu prvku σ.

Součet formální řady pro $x, y \in S$, kde $x = r_1 \cdot a_1 + r_2 \cdot a_2 + \dots + r_n \cdot a_n$ a $y = s_1 \cdot a_1 + s_2 \cdot a_2 + \dots + s_m \cdot a_m$, kde $m > n$, vypadá takto:

$$x + y = r_1 \cdot a_1 + r_2 \cdot a_2 + \dots + r_n \cdot a_n + s_1 \cdot a_1 + s_2 \cdot a_2 + \dots + s_m \cdot a_m =$$

$$= r_1 \cdot a_1 + s_1 \cdot a_1 + r_2 \cdot a_2 + s_2 \cdot a_2 + \dots + r_n \cdot a_n + s_n \cdot a_n + \dots + s_m \cdot a_m =$$

$$= (r_1 + s_1) \cdot a_1 + (r_2 + s_2) \cdot a_2 + \dots + (r_n + s_n) \cdot a_n + \dots + s_m \cdot a_m.$$

Nyní máme definovanou operaci sčítání a ověříme platnost axiomů.

1. Komutativnost operace sčítání.

   Pro každé dva prvky množiny S musí platit $x + y = y + x$.

$$x = r_1 \cdot a_1 + \ \dots + r_n \cdot a_n$$

$$y = s_1 \cdot a_1 + \ \dots + s_m \cdot a_m, \text{ kde } m > n$$

$$L = x + y = r_1 \cdot a_1 + \ \dots + r_n \cdot a_n + s_1 \cdot a_1 + \ \dots + s_m \cdot a_m =$$

$$= r_1 \cdot a_1 + s_1 \cdot a_1 + \ \dots + r_n \cdot a_n + s_n \cdot a_n + \ \dots + s_m \cdot a_m =$$

$$= (r_1 + s_1) \cdot a_1 + \ \dots + (r_n + s_n) \cdot a_n + \ \dots + s_m \cdot a_m$$

$$P = y + x = s_1 \cdot a_1 + \ \dots + s_m \cdot a_m + r_1 \cdot a_1 + \ \dots + r_n \cdot a_n =$$

$$= s_1 \cdot a_1 + r_1 \cdot a_1 + \ \dots + s_n \cdot a_n + r_n \cdot a_n + \ \dots + s_m \cdot a_m =$$

$$= (s_1 + r_1) \cdot a_1 + \ \dots + (s_n + r_n) \cdot a_n + \ \dots + s_m \cdot a_m$$

Pro $i = 0, 1, 2, \dots$ jsou prvky r_i a s_i prvky oboru integrity R, proto $r_1 + s_1 = s_1 + r_1$ (vyplývá z komutativnosti operace sčítání oboru integrity R) a proto platí, že $\underline{\underline{L = P}}$.

Pro každé dva prvky $x, y \in S$ platí $x + y = y + x$. Tím je dokázáno, že operace sčítání je na množině S komutativní.

2. Asociativita operace sčítání.

   Pro každé tři prvky množiny S musí platit $(x + y) + z = x + (y + z)$.

$$x = r \cdot a$$

$$y = s \cdot a$$

$$z = t \cdot a$$

$$L = (x + y) + z = (r \cdot a + s \cdot a) + t \cdot a =$$

$$= (r + s) \cdot a + t \cdot a = (r + s + t) \cdot a$$

$$P = x + (y + z) = r \cdot a + (s \cdot a + t \cdot a) =$$

$$= r \cdot a + (s + t) \cdot a = (r + s + t) \cdot a$$

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

   Pro každé tři prvky množiny S je operace sčítání asociativní.

3. Existence neutrálního prvku pro operaci sčítání.

   Pro každý prvek množiny S musí platit součet $x + e = x$, kde $x \in S$ a e je neutrální prvek.

$$x + e = x \ /-x$$
$$e = 0$$

   Pro každý prvek množiny S existuje neutrální prvek vůči operaci sčítání. Již dříve jsme označili $e = \sigma$.

4. Existence inverzního prvku pro operaci sčítání.

   Pro každý prvek množiny S musí platit $x + x^{-1} = e$.

$$x + x^{-1} = \sigma \ /-x$$
$$x^{-1} = -x$$

   Pro každý prvek množiny S existuje prvek inverzní, v tomto případě se jedná o prvek opačný.

6.2 OPERACE NÁSOBENÍ

Nyní musíme nadefinovat operaci násobení $(\cdot)$ a ověřit platnost axiomů pro tuto operaci. Operaci násobení budeme provádět podle pravidla:

$$r \cdot a + s \cdot b = rs \cdot (a + b), \text{ kde } r, s \in R, r \neq 0, s \neq 0, a, b \in \mathbb{Q}, a, b \geq 0.$$

5. Komutativnost operace násobení.

   Pro každé dva prvky množiny S musí platit $x \cdot y = y \cdot x$.

$$x = r \cdot a$$
$$y = s \cdot b$$
$$L = x \cdot y = (r \cdot a) \cdot (s \cdot b) = rs \cdot (a + b)$$
$$P = y \cdot x = (s \cdot b) \cdot (r \cdot a) = sr \cdot (b + a)$$

   $\underline{\underline{L = P}}$, protože r, s jsou prvky oboru integrity R a platí pro ně $rs = sr$ (vychází z komutativnosti operace násobení v oboru integrity R). Prvky a a b jsou prvky množiny $\mathbb{Q}$, ve které platí $a + b = b + a$.

   Operace násobení je na množině S komutativní.

6. Asociativnost operace násobení.

   Pro každé tři prvky množiny S musí platit $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

$$x = r \cdot a$$
$$y = s \cdot b$$
$$z = t \cdot c$$
$$L = (x \cdot y) \cdot z = [(r \cdot a) \cdot (s \cdot b)] \cdot (t \cdot c) = [rs \cdot (a + b)] \cdot (t \cdot c) =$$
$$= rst \cdot (a + b + c)$$
$$P = x \cdot (y \cdot z) = (r \cdot a) \cdot [(s \cdot b) \cdot (t \cdot c)] = (r \cdot a) \cdot [st \cdot (b + c)] =$$
$$= rst \cdot (a + b + c)$$
$$\underline{\underline{L = P}}$$

   Operace násobení je na množině S asociativní.

7. Distributivnost operace násobení.

   Pro každé tři prvky množiny S musí platit $(x + y) \cdot z = x \cdot z + y \cdot z$.

$$x = r \cdot a$$
$$y = s \cdot a$$
$$z = t \cdot b$$
$$L = (x + y) \cdot z = [(r \cdot a) + (s \cdot a)] \cdot (t \cdot b) = [(r + s) \cdot a] \cdot (t \cdot b) =$$
$$= t \cdot (r + s) \cdot (a + b)$$
$$P = x \cdot z + y \cdot z = (r \cdot a) \cdot (t \cdot b) + (s \cdot a) \cdot (t \cdot b) =$$
$$= rt \cdot (a + b) + st \cdot (a + b) = t \cdot (r + s) \cdot (a + b)$$
$$\underline{\underline{L = P}}$$

   Operace násobení je na množině S distributivní.

Dva formální součty, což jsou prvky množiny S, mezi sebou plně roznásobíme pomocí distributivity a výše uvedených pravidel.

Jako poslední nám zbývá ověřit neexistenci netriviálních dělitelů nuly.

8. Neexistence netriviálních dělitelů nuly.

   Pro všechny prvky množiny S musí platit $x \neq \sigma \wedge y \neq \sigma \Rightarrow x \cdot y \neq \sigma$.

$$x = r_1 \cdot a_1 + \ \ldots + r_n \cdot a_n$$
$$y = s_1 \cdot b_1 + \ \ldots + s_m \cdot b_m$$

   Jsou-li x a y nenulové prvky množiny S, pak $m, n \geq 1$ a v součinu $x \cdot y$ nám mimo jiné zůstane nenulový člen $(r_n s_m) \cdot (a_n + b_m)$.

Platí všech osm axiomů a je jasné, že množina S tvoří obor integrity.

6.3 PODMÍNKA KŘVD

Ukázali jsme, že množina S tvoří obor integrity. Nyní se zaměříme na podmínku KŘVD.

Z množiny S si vybereme podmnožinu $S´$, jejíž členy jsou ve tvaru

$$x_i = 1 \cdot \frac{1}{2^i}, \text{ kde } i = \{0, 1, 2, \dots\}.$$

Aby nebyla splněna podmínka KŘVD, musí platit, že $x_{i+1} | x_i \ \wedge \ x_i \nmid x_{i+1}$, to znamená, že prvek $x_{i+1} = a \cdot x_i$.

Vezmeme si prvek $(x_{i+1})^2$ a budeme ho upravovat.

$$(x_{i+1})^2 = (x_{i+1}) \cdot (x_{i+1}) = \left(1 \cdot \frac{1}{2^{i+1}}\right) \cdot \left(1 \cdot \frac{1}{2^{i+1}}\right)$$

Tyto dva prvky roznásobíme podle pravidla pro násobení prvků oboru integrity $S´$ uvedeného výše.

$$\left(1 \cdot \frac{1}{2^{i+1}}\right) \cdot \left(1 \cdot \frac{1}{2^{i+1}}\right) = (1 \cdot 1) \cdot \left(\frac{1}{2^{i+1}} + \frac{1}{2^{i+1}}\right) = 1 \cdot \left(\frac{2}{2^{i+1}}\right)$$

Na první pohled je patrné, že dvojka v čitateli lze krátit s jedničkou v exponentu dvojky ve jmenovateli. Dostáváme tedy:

$$(x_{i+1})^2 = 1 \cdot \left(\frac{1}{2^i}\right),$$

což je prvek x_i.

To znamená, že v oboru integrity $S´$ dělí prvek x_{i+1} prvek x_i.

Pokud volíme $i = 1$, dostáváme $x_2 | x_1$. Pro $i = 2$ platí $x_3 | x_2$. Je patrné, že i $x_4 | x_3$, $x_5 | x_4$, $x_6 | x_5$,…

Dostáváme tedy nekonečnou řadu dělitelů $x_2 | x_1$, $x_3 | x_2$, $x_4 | x_3$, $x_5 | x_4$, $x_6 | x_5$,…, což je spor s podmínkou KŘVD.

Nalezli jsme obor integrity, který nesplňuje podmínku KŘVD.

Jednoduše prohlédneme, že když označíme

$$x_i = a \cdot \frac{b}{(2b)^i}, \text{ kde } x_i \in S_i, a \in R, b \in \mathbb{Z},$$

tak dostáváme nekonečně mnoho oborů integrity S_i, které nesplňují podmínku KŘVD.

7 OBOR INTEGRITY NESPLŇUJÍCÍ PODMÍNKY P A ENSD

Existuje řada oborů integrity, které splňují podmínky P (každý ireducibilní prvek je prvočinitelem) a ENSD (existence největšího společného dělitele pro každé dva prvky). Proto se zaměříme na to, jestli existuje obor integrity, který tyto podmínky nesplňuje.

Nechť je r kladné liché číslo, které navíc splňuje dvě podmínky:

1. $4|(r-1)$
2. r není druhá mocnina žádného celého čísla.

Těmto podmínkám vyhovují čísla $5, 13, 17, 21, 29, 33, 37, \ldots$

Dále řekněme, že číslo s je definováno jako $s = \sqrt{r}$. Číslo s je tedy kladné iracionální číslo.

Uvažujme obor integrity $R = \mathbb{Z}[s]$, kde $s = \sqrt{r}$ a prvky tohoto oboru integrity mají tvar $x = a + bs$, kde $a, b \in \mathbb{Z}$. Fakt, že množina $\mathbb{Z}[s]$ tvoří obor integrity, bychom dokázali stejně jako v kapitole 5.3 pro $\mathbb{Z}[\sqrt{2}]$.

7.1 PRVKY $\mathbb{Z}[s]$ JSOU JEDNOZNAČNĚ URČENÉ

Nejdříve ověříme, zda je zápis $x = a + bs$ jednoznačný. Toto tvrzení dokážeme sporem.

Řekneme, že $x = a + bs$ a $y = c + ds$, kde $c, d \in \mathbb{Z}$.

Pokud je zápis jednoznačný musí platit:

$$a + bs = c + ds$$

$$a - c = (d - b)s.$$

Pokud $d \neq b$, dostáváme spor s tvrzením, že číslo s je iracionální (součinem jakéhokoliv čísla s číslem iracionálním je opět číslo iracionální, zatímco rozdílem dvou celých čísel je číslo celé).

Z toho vyplývá, že $a = c \wedge d = b$ a zápis $x = a + bs$ je jednoznačný.

7.2 ČÍSLO 2 NEDĚLÍ KAŽDÝ PRVEK $\mathbb{Z}[s]$

Řekněme, že $x = a + bs$ je prvek oboru integrity R, pro který platí $2|x$. Musí tedy existovat takový prvek $y = c + ds$, kde $c, d \in \mathbb{Z}$, že $x = 2y$.

$$x = 2y$$

$$a + bs = 2 \cdot (c + ds) = 2c + 2ds$$

Z toho plyne, že $a = 2c$ a $b = 2d$. Odtud je vidět, že $2|x$, kde $x = a + bs$, právě tehdy, když jsou a a b sudá čísla.

V dalším textu si v daném oboru integrity R budeme definovat normu t (zde se nejedná o Euklidovu normu, protože se nepohybujeme v Euklidovu oboru integrity), o níž dokážeme, že je multiplikativní. Tato norma nám pak v mnoha věcech poslouží: určíme například invertibilní prvky v $\mathbb{Z}[s]$, ukážeme, že neexistují prvky s normou $t_{(x)} \neq \pm 2$ a dospějeme k důkazu ireducibility prvku $x = 2$.

7.3 NORMA (ZOBRAZENÍ) V $\mathbb{Z}[s]$

Řekněme, že $x = a + bs \in R$ a $t_{(x)} = a^2 - rb^2$. Aby zobrazení t bylo normou, tak musí být multiplikativní tedy $t_{(x \cdot y)} = t_{(x)} \cdot t_{(y)}$ pro všechny prvky oboru integrity R.

$$x = a + bs$$

$$y = c + ds$$

$$x \cdot y = (a + bs) \cdot (c + ds) = ac + ads + bcs + bds^2$$

Číslo s je definováno jako $s = \sqrt{r} \Rightarrow s^2 = r$.

Dostáváme tedy, že $x \cdot y = (ac + bdr) + (ad + bc) \cdot s$.

Nyní můžeme ověřit multiplikativnost zobrazení t.

$$t_{(x \cdot y)} = t_{(x)} \cdot t_{(y)}$$

$$L = t_{(x \cdot y)} = t_{((ac+bdr)+(ad+bc) \cdot s)} = (ac + bdr)^2 - r \cdot (ad + bc)^2 =$$

$$= a^2c^2 + 2abcdr + b^2d^2r^2 - ra^2d^2 - 2abcdr - rb^2c^2 =$$

$$= \underline{a^2c^2 + b^2d^2r^2 - ra^2d^2 - rb^2c^2}$$

$$P = t_{(x)} \cdot t_{(y)} = t_{(a+bs)} \cdot t_{(c+ds)} = (a^2 - rb^2) \cdot (c^2 - rd^2) =$$

$$= \underline{a^2c^2 - ra^2d^2 - rb^2c^2 + r^2b^2d^2}$$

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

Zobrazení t: $R \mapsto \mathbb{Z}$ je multiplikativní.

7.4 INVERTIBILNÍ PRVEK V R

S použitím multiplikativního zobrazení t dokážeme, že prvek $x \in R$ je invertibilním prvkem (existuje k němu inverzní prvek pro operaci násobení), když $t_{(x)} = 1$ nebo $t_{(x)} = -1$.

Řekněme, že $x \cdot y = 1$ pro nějaké $y \in R$. Dále musí platit že $t_{(x)} \cdot t_{(y)} = t_{(xy)} = t_{(1)} = 1$ a tedy $t_{(x)} = \pm 1$.

To znamená, že $t_{(x)} = \pm 1$, kde $x = a + bs$.

$$t_{(x)} = t_{(a+bs)} = a^2 - rb^2$$

Protože $\sqrt{r} = s \Rightarrow r = s^2$ tak dostáváme:

$$t_{(x)} = (a + bs) \cdot (a - bs) = x \cdot (a - bs).$$

Pro $t_{(x)} = 1$ je tedy $x^{-1} = a - bs$ a pro $t_{(x)} = -1$ je $x^{-1} = -a + bs$.

Odtud je patrné, že pokud $t_{(x)} = \pm 1$, kde prvek $x \in R$, tak k němu existuje inverzní prvek pro operaci násobení, tedy invertibilní prvek.

7.5 NEEXISTENCE PRVKU, KDE $t_{(x)} = \pm 2$

Nyní ukážeme, že $t_{(x)} \neq \pm 2$ pro každý prvek oboru integrity R. Důkaz provedeme sporem.

Řekněme, že $t_{(x)} = a^2 - rb^2 = \pm 2$ pro libovolný prvek z R, kde $x = a + bs$. Protože číslo r je kladné liché celé číslo, tak čísla a a b musí být současně lichá nebo sudá.

1. Řekněme, že jsou čísla a a b sudá čísla, tedy $a = 2m$ a $b = 2n$, kde $m, n \in \mathbb{Z}$.

$$x = 2m + 2ns$$

$$t_{(x)} = t_{(2m+2ns)} = 4m^2 - 4rn^2 = 4p, \text{ kde } p = m^2 - rn^2$$

$$4p = \pm 2$$

$$p = \pm\frac{1}{2}$$

Zde dostáváme spor, protože podle předpokladu se pohybujeme v množině celých čísel (t je zobrazení do $\mathbb{Z}$).

2. Řekněme, že jsou čísla a a b lichá čísla, tedy $a = 2m + 1$ a $b = 2n + 1$, kde $m, n \in \mathbb{Z}$.

$$x = (2m + 1) + (2n + 1)s$$

$$t_{(x)} = t_{((2m+1)+(2n+1)s)} = (2m + 1)^2 - r(2n + 1)^2 =$$

$$= 4m^2 + 4m + 1 - 4rn^2 - 4rn - r$$

Protože $4|r - 1$, můžeme člen $r - 1$ psát jako $4q$.

$t_{(x)} = 4m^2 + 4m - 4rn^2 - 4rn - 4q = 4p$, kde $p = m^2 + m - rn^2 - rn - q$

$$4p = \pm 2$$

$$p = \pm\frac{1}{2}$$

Zde dostáváme spor, protože podle předpokladu se pohybujeme v množině celých čísel.

Dostáváme, že neexistuje prvek $x \in R$, pro který by platilo $t_{(x)} = \pm 2$.

7.6 PRVEK $x = 2$ JE IREDUCIBILNÍ V R

Nyní ukážeme, že prvek $x = 2$ je ireducibilní prvek oboru integrity R.

$$x = 2$$

$$t_{(x)} = t_{(2)} = 4$$

Dříve jsme ukázali, že invertibilním prvkem v oboru integrity R je prvek ± 1. Dále jsme ukázali, že neexistuje prvek, pro který by platilo $t_{(x)} = \pm 2$.

Platí tedy, že $4 = t_{(2)} = t_{(xy)} = t_{(x)} \cdot t_{(y)}$.

Protože $t_{(x)} \neq \pm 2$, tak mohou nastat dvě možnosti:

1. $t_{(x)} = \pm 1$ a $t_{(y)} = \pm 4$, kde $x \in R^*$ a $t_{(y)} \notin R^*$ nebo
2. $t_{(x)} = \pm 4$ a $t_{(y)} = \pm 1$, kde $x \notin R^*$ a $t_{(y)} \in R^*$.

V obou případech je patrné, že jeden prvek je invertibilní a druhý nikoli, protože k prvku $x = 2$ neexistuje inverzní prvek vůči operaci násobení.

To znamená, že prvek $x = 2 \notin R^* \wedge 2 \neq 0$. Jedná se tedy o prvek ireducibilní.

7.7 PODMÍNKA P

Nyní máme vše připraveno, abychom ukázali, že obor integrity $R = \mathbb{Z}[s]$ nesplňuje podmínku P.

Podmínka P říká, že každý ireducibilní prvek v R musí být prvočinitel a prvočinitel je prvek, který dělí jednoho z činitelů, pokud dělí jejich součin. To znamená, že ireducibilní prvek $x = 2$ musí dělit y nebo z pokud dělí yz.

Zvolíme $y, z \in R$:

$$y = 1 + s$$

$$z = -1 + s$$

$$y \cdot z = (1 + s) \cdot (-1 + s) = -1 + s - s + s^2 = r - 1.$$

Podle předpokladu $4|r - 1$ je rozdíl $r - 1$ sudé číslo a $2|yz$.

Prvek $x = 2$ musí tedy dělit jeden z prvků y a z.

Podle kapitoly 7.2 je však patrné, že $2 \nmid y$ ani $2 \nmid z$.

Dostáváme ireducibilní prvek oboru integrity R, který ale není prvočinitelem. Tím není splněna podmínka P.

7.8 PODMÍNKA ENSD

Nyní ověříme, jestli obor integrity R splňuje podmínku KŘVD (podmínka KŘVD nám pomůže ukázat, že neplatí podmínka ENSD).

Označme $x = a + bs$ a $y = c + ds$ prvky množiny $\mathbb{Z}[s]$. Jestliže $x|y$, tak musí $t_{(x)}|t_{(y)}$. Přitom x je vlastním dělitelem y, právě když $t_{(x)}$ je vlastním dělitelem $t_{(y)}$.

Buď $y = x \cdot z$, kde $z \in \mathbb{Z}[s]$. Pak $t_{(y)} = y\overline{y} = xz \cdot \overline{xz} = x\overline{x} \cdot z\overline{z} = t_{(x)} \cdot t_{(z)}$. Protože t je zobrazení na množinu celých čísel, je patrné, že $t_{(x)} \leq t_{(y)}$. Odtud je patrné, že obor integrity R na množině $\mathbb{Z}[s]$ splňuje podmínku KŘVD.

S využitím následující věty ukážeme, že není splněna podmínka ENSD.

Věta 3: Nechť R je obor integrity. Pak jsou následující podmínky ekvivalentní:

i. R je obor integrity s jednoznačným rozkladem
ii. R splňuje podmínku KŘVD a ENSD
iii. R splňuje podmínku KŘVD a P.[Bican, 1979]

Z věty 3 vyplývá, že pokud jsou splněny podmínky KŘVD a P, tak musí být splněna i podmínka ENSD nebo naopak.

Tedy obor integrity R nesplňuje podmínku ENSD, protože nesplňuje podmínku P.

Nalezli jsme nekonečně mnoho oborů integrity, které nesplňují podmínku P ani podmínku ENSD. Prvky těchto oborů integrity mají tvar $x = a + bs$, kde $a, b \in \mathbb{Z}$ a $s = \sqrt{r}$, kde r je kladné liché celé číslo, které není druhou mocninou žádného celého čísla a zároveň platí $4|r - 1$.

ZÁVĚR

Ve své práci jsem se snažil ukázat zajímavou část odvětví matematické algebry, které bývá občas nazýváno teorie komutativních okruhů.

Příklady v mé práci jsou pouze úvodem do nespočtu oborů integrity a jejich dělitelnosti.

Cílem této práce bylo seznámení se s problematikou Gaussových a Euklidových oborů integrity a jejich dělitelnosti.

Také jsem se snažil ukázat využití Euklidova algoritmu v různých oborech integrity, jako je obor integrity celých čísel, obor integrity Gaussových celých čísel, obor integrity komplexních čísel s odmocninou a obor integrity prostoru polynomů.

Své poznatky získané studiem dělitelnosti v oborech integrity mohu použít ve své budoucí profesi a seznámit mladé nadšené matematiky s jiným způsobem hledání největšího společného dělitele a nejmenšího společného násobku, než je prvočíselný rozklad.

Závěrem bych chtěl ještě jednou poděkovat mému vedoucímu bakalářské práce Doc. RNDr. Jaroslavu Horovi, CSc., za jeho cenné rady, připomínky a metodické vedení práce.

RESUMÉ

This thesis (Examples of the divisibility of integral domains) deals with the area of mathematics, which is called algebra. More precisely, it is a part of algebra, which is called commutative rings.

The main idea of this thesis is divisibility of integral domains. It mainly deals with Gaussian domain (Gaussian ring) and Euclidean domain (Euclidean ring).

It also contains a number of examples of finding a greatest common divisor and a least common multiple in various fields of integral domain. These integral domains are e.g. the integer domain, the Gaussian integer domain, the ring of polynomials and others.

One part of my thesis is devoted to the calculation of a greatest common divisor and a least common multiple in mathematical software like the Wolfram Mathematica, the MATLAB and the Wolfram|Alpha.

The final part of this thesis is devoted to integral domains, which do not meet the condition of finality series of proper divisor or the condition of existence of the greatest common divisors.

SEZNAM LITERATURY

Procházka, L. a kol. Algebra: Celost. vysokoškolská učebnice pro stud. matematicko-fyzikálních a přírodovědeckých fakult, stud. oborů matematické vědy. 1. vyd. Praha: Academia, 1990. 560 s. ISBN 80-200-0301-0.

Bican, L. Algebra I. Praha: SPN, 1979. Skriptum MFF UK Praha.

Bicanová, A., Kepka, T., Nováková, E. Sbírka úloh, příkladů a cvičení z algebry. Praha: SPN, 1984. Skriptum MFF UK Praha.

Blažek, J. a kol. Algebra a teoretická aritmetika: Celost. a vysokošk. učebnice pro stud. matematicko-fyzikálních, přírodověd. a pedagog. fakult. Díl 1. 1. vyd. Praha: SPN, 1985. 278 s.

Blažek, J. a kol. Algebra a teoretická aritmetika: Celost. a vysokošk. učebnice pro stud. matematicko-fyzikálních, přírodověd. a pedagog. fakult. Díl 2. 1. vyd. Praha: SPN, 1985. 258 s.

Drábek, J. Algebra. Polynomy a rovnice. 1. vyd. Plzeň: Západočeská univerzita, 2001. 125 s. ISBN 80-7082-787-4.

Wikipedia: The free encyclopedia. Areas of mathematics. [Online]. c2013 [cit. 2013-02-01]. Dostupný z WWW: http://en.wikipedia.org/wiki/Areas_of_mathematics.

Magcraft. Johann Carl Friedrich Gauss. Magnet university. [Online] [cit. 2013-02-15]. Dostupný z http://www.rare-earth-magnets.com/t-johann-carl-friedrich-gauss.aspx.

Wikipedie: Otevřená encyklopedie: Eukleidés [Online]. c2013 [citováno 2013-02-12]. Dostupný z WWW: http://cs.wikipedia.org/wiki/Euklides.

Wikipedia: The free encyclopedia. Integral domain. [Online]. c2013 [cit. 2013-01-20]. Dostupný z WWW: http://en.wikipedia.org/wiki/Integral_domain.

SEZNAM OBRÁZKŮ

PŘÍLOHY

Všechny materiály k bakalářské práci jsou vypáleny na přiloženém CD, které obsahuje:

- Obrázky a loga použité v textu
- BP ve formátu pdf
- BP ve formátu docx