Univerzita Karlova
Pedagogická fakulta
Katedra matematiky a didaktiky matematiky

BAKALÁŘSKÁ PRÁCE

Geometrické vlastnosti komplexních čísel
The geometric properties of complex number

František Kouba

Vedoucí bakalářské práce: doc. RNDr. Antonín Jančařík, Ph.D.
Studijní program: Specializace v pedagogice
Studijní obor: Informační technologie a matematika

Praha 2018

Odevzdáním této bakalářské práce na téma **Geometrické vlastnosti komplexních čísel** potvrzuji, že jsem ji vypracoval pod vedením vedoucího práce samostatně za použití v práci uvedených pramenů a literatury. Dále potvrzuji, že tato práce nebyla využita k získání jiného nebo stejného titulu.

V Praze dne 20. 4. 2018

František Kouba

Rád bych poděkoval doc. RNDr. Antonínu Jančaříkovi, Ph.D. za vstřícnost, trpělivost a cenné rady při zpracování bakalářské práce. Dále patří mé poděkování rodině, která při mně po celou dobu studia a psaní bakalářské práce stála a podporovala mě.

Název práce: Geometrické vlastnosti komplexních čísel

Autor: František Kouba

Katedra: Katedra matematiky a didaktiky matematiky

Vedoucí bakalářské práce: doc. RNDr. Antonín Jančařík, Ph.D.

Anotace: Bakalářská práce shrnuje poznatky o Gaussově celých číslech, které se dále využívají při geometrické interpretaci. Práce se skládá z celkem 7 kapitol. První tři obsahují teoretické znalosti v podobě potřebných definic, vět a důkazů. Další tři kapitoly se zabývají grafickým znázorněním Gaussovo celých čísel a jejich vlastností v Gaussově rovině, které jsou doplněny o řešené úlohy. V poslední kapitole jsou popsány applety, jež demonstrují vybrané vlastnosti daných čísel v komplexní rovině.

Klíčová slova: Gaussovo celé číslo, komplexní rovina, Gaussovo prvočíslo, applet

Title: The geometric properties of complex number

Author: František Kouba

Department: Department of Mathematics and Mathematical Education

Supervisor: doc. RNDr. Antonín Jančařík, Ph.D.

Annotation: The Bachelor's thesis summarizes knowledge of Gaussian intengers, which are used in geometrical interpretation. The work consists of 7 chapters. The first three of them contain theoretical knownledge in the form of the necessary definitions, theorems and proofs. The next three of chapters is engaged in the graphical representation of Gaussian integers and their properties in the Gaussian plane, which are supplemented by solved tasks. In the last chapter applets are described, that demonstrate chosen properties of these numbers in the complex plane.

Keywords: Gaussian integer, complex plane, Gaussian prime, applet

Obsah

Úvod **7**

1 Gaussova celá čísla **8**
1.1 Zavedení a základní vlastnosti 8
1.2 Komplexně sdružené číslo 12
1.3 Absolutní hodnota Gaussova celého čísla 13
1.4 Norma Gaussových celých čísel 16

2 Dělitelnost a dělení v $\mathbb{Z}[i]$ **18**
2.1 Dělitelnost v $\mathbb{Z}[i]$ 18
2.2 Jednotka v $\mathbb{Z}[i]$ 20
2.3 Dělení se zbytkem v $\mathbb{Z}[i]$ 21
2.4 Největší společný dělitel v $\mathbb{Z}[i]$ 22
2.5 Euklidův algoritmus v $\mathbb{Z}[i]$ 24
2.6 Asociovaná čísla (prvky) v $\mathbb{Z}[i]$ 26
2.7 Nesoudělná čísla v $\mathbb{Z}[i]$ 27

3 Prvočísla v $\mathbb{Z}[i]$ **29**
3.1 Zavedení a vlastnosti v $\mathbb{Z}[i]$ 29
3.2 Rozklad v $\mathbb{Z}[i]$ 34
3.3 Prvočíselný rozklad v $\mathbb{Z}[i]$ 34

4 Geometrické znázornění Gaussových celých čísel **36**
4.1 Geometrická interpretace Gaussových celých čísel 36
4.2 Gaussova rovina 37
4.3 Komplexně sdružené číslo 37
4.4 Opačné číslo 37
4.5 Sčítání a odčítání Gaussových celých čísel 38
4.6 Násobení Gaussových celých čísel 39
4.6.1 Vynásobení Gaussova celého čísla číslem celým ($\mathbb{Z}$) 39
4.6.2 Vynásobení Gaussova celého čísla číslem ryze imaginárním 40
4.6.3 Vynásobení Gaussova celého čísla Gaussovým celým číslem 40

5 Dělitelnost a dělení v komplexní rovině **42**
5.1 Dělitelnost Gaussových celých čísel 42
5.2 Dělení Gaussových celých čísel se zbytkem 45
5.3 Počet řešení pro dvojici (q,r) při dělení Gaussových celých čísel se zbytkem 47
5.4 Největší společný dělitel Gaussových celých čísel 50

6 Prvočísla a rozklad v Gaussově rovině **57**
6.1 Přirozená čísla . . . 57
6.2 Gaussova celá čísla . . . 65
6.3 Prvočísla v komplexní rovině . . . 70

7 Applety **72**
7.1 Obecně o appletech . . . 72
7.2 Výhody appletů . . . 72
7.3 Nevýhody appletů . . . 73
7.4 Využití . . . 73
7.5 Matematické applety . . . 73
7.5.1 Applet č. 1 . . . 74
7.5.2 Applet č. 2 . . . 74
7.5.3 Applet č. 3 . . . 75
7.5.4 Applet č. 4 . . . 76
7.5.5 Applet č. 5 . . . 77
7.5.6 Applet č. 6 . . . 78
7.5.7 Applet č. 7 . . . 79
7.5.8 Applet č. 8 . . . 79
7.5.9 Applet č. 9 . . . 80
7.5.10 Applet č. 10 . . . 81
7.5.11 Applet č. 11 . . . 82
7.5.12 Applet č. 12 . . . 82
7.5.13 Applet č. 13 . . . 83
7.5.14 Applet č. 14 . . . 84
7.5.15 Applet č. 15 . . . 84
7.5.16 Applet č. 16 . . . 85
7.5.17 Applet č. 17 . . . 85
7.5.18 Applet č. 18 . . . 86

Závěr **87**

Literatura **88**

Seznam obrázků **91**

Úvod

Bakalářská práce je věnována základním vlastnostem Gaussových celých čísel, které jsou podmnožinou komplexních čísel. Autora vedla k výběru tohoto tématu z velké části skutečnost, že daná oblast není příliš dostupná v českém znění, podrobně a souhrnně zpracovaná. O tom se lze přesvědčit pomocí zdrojů uvedených v seznamu literatury na konci této práce. Druhým a mnohem zajímavější důvodem byla geometrická interpretace Gaussovo celých čísel. Gaussova celé čísla můžeme graficky znázornit jako mřížové body a vektory v Gaussově rovině. Z toho vyplývá, že s nimi dokážeme pracovat snadněji a lépe z vizuálního hlediska než se samotnými komplexními čísly, jež nemusí mít celočíselnou reálnou nebo imaginární část.

A tedy cílem bakalářské práce je popsat vlastnosti Gaussových celých čísel a vytvoření appletů demonstrujících vybrané geometrické vlastnosti těchto čísel.

Samotná práce je rozdělena do 7 kapitol. V prvních třech kapitolách najdeme ucelené obecné poznatky z Gaussových celých čísel pomocí definic, vět a jejich důkazů. V kapitole 1 zavádíme Gaussova celá čísla, seznamuje se se základními vlastnostmi a pojmy, které můžeme převzít z komplexních čísel. V kapitole 2 a 3 zjišťujeme, zda poznatky z běžných celých čísel platí i v Gaussově celých číslech, případně jaké omezení a úskalí přináší. Hlavními kapitolami a přínosem této práce by měly být následující tři kapitoly, tj. 4, 5 a 6, ve kterých se řeší grafické znázornění Gaussových celých čísel a geometrické vlastnosti, jež jsme v předchozích kapitolách představili z algebraického (teoretického) hlediska. Navíc jsou doplněny o řešené úlohy a odkazy na applety demonstrující vždy vybraný předmět zkoumání. V poslední kapitole (7) je krátce napsáno o appletech. Dále zde nalezneme následující internetový odkaz https://ggbm.at/rusK9KPN na autorovy applety, které vznikly při tvorbě bakalářské práce a slouží jako podklad daného textu, a krátký popis jednotlivých appletů.

Definice a věty, které jsou převzaty z cizojazyčné literatury, nejsou uváděny v originálním znění, ale jsou přeloženy do češtiny. Značení je přizpůsobeno charakteru práce. Citované zdroje jsou uvedeny přímo v jednotlivých částech textu.

Obrázky, které doplňují text a úlohy, byly pořízeny z autorových appletů, jež byly vytvořeny v matematickém programu GeoGebra.

Kapitola 1

Gaussova celá čísla

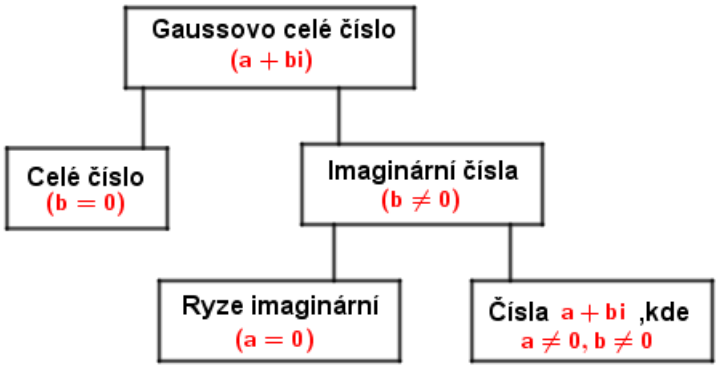
V této kapitole shrnujeme základní informace (algebraické vlastnosti) o Gaussových celých číslech. Tyto poznatky jsou využívány v dalších kapitolách s grafickou interpretací Gaussových celých čísel a pro vytvoření appletů demonstrujících vybrané geometrické vlastnosti.

1.1 Zavedení a základní vlastnosti

Definice 1. *Gaussovo celé číslo je komplexní číslo* $a+bi$*, kde* $a, b \in \mathbb{Z}$. [1, s. 149]

Jinými slovy Gaussovo celé číslo je komplexní číslo skládající se z reálné části a a imaginární části b, kde navíc obě tyto části jsou celá čísla.[1]

Zápis Gaussova celého čísla $z = (a,b)$ nazveme **algebraickým tvarem čísla** z. Číslo, jehož reálná část je rovna nule a imaginární část se rovná jedné, se nazývá **imaginární jednotka** a značí se i. Tu můžeme tedy zapsat následovně $i := (0,1)$. Každé Gaussovo celé číslo, jehož imaginární část není rovna nule, se nazývá **číslo imaginární**. Je-li navíc jeho reálná část rovna nule ($a = 0$), tj. tvaru $(0,b) = bi$, kde b je celé číslo různé od nuly, pak jej označujeme jako **číslo ryze imaginární**. Grafické schéma můžeme vidět na obrázku 1.1.[2]



Obrázek 1.1: Grafické schéma Gaussových celých čísel

[1] Celé číslo Re $z := a$ označujeme jako reálnou část. Celé číslo Im $z := b$ nazýváme jako jeho imaginární část.[2]

Definice 2. *Množinu Gaussových celých čísel značíme* $\mathbb{Z}[i]$ *a definujeme*

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}, \qquad kde\ i = \sqrt{-1}.[3, \text{s. } 599]$$

Definice 3. *Nechť* $a + bi$ *a* $c + di$ *jsou Gaussova celá čísla. Potom jejich součet a součin je definován následovně* [3, s. 599]*:*

$$(a + bi) + (c + di) = (a + c) + (b + d)i \tag{1.1}$$

$$(a + bi) \cdot (c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i \tag{1.2}$$

Z definice 3 vidíme, že při součtu nebo součinu dvou Gaussových celých čísel dostáváme zase Gaussovo celé číslo, nebo-li množina Gaussových celých čísel $\mathbb{Z}[i]$ je uzavřená na sčítání a násobení a tvoří obor integrity (značení $\mathbb{Z}[i]$, viz Lemma 1).

Lemma 1. $\mathbb{Z}[i]$ *je oborem integrity.* [4, s. 408]

Důkaz.
Nejprve dokážeme, že Gaussova celá čísla s dvěma binárními operacemi + a · tvoří komutativní okruh[1] s jednotkovým prvkem.
Snažíme se ukázat, že Gaussova celá čísla splňují vlastnosti, které jsou uvedeny v definici okruhu.
Nechť $x, y, z \in \mathbb{Z}[i]$, kde $x = a + bi$, $y = c + di$ a $z = e + fi$ a samozřejmě $a, b, c, d, e, f \in \mathbb{Z}$.

1. Tuto vlastnost Gaussových celých čísel jsme definovali dříve v definici 3.

2. Asociativita sčítání: $(x + y) + z = x + (y + z)$.

$$\begin{aligned}(x + y) + z &= [(a + bi) + (c + di)] + (e + fi) \\ &= [(a + c) + (b + d)i] + (e + fi) \\ &= ((a + c) + e) + ((b + d) + f)i\end{aligned}$$

[1] **Definice okruhu:** Struktura R s nosičem $\mathbb{R}$ a dvěma binárními operacemi + (sčítání) a · (násobení) na $\mathbb{R}$ nazýváme okruh, platí-li pro všechny prvky x, y, z z $\mathbb{R}$ následující vlastnosti:

1. Uzavřenost obou operací: $x + y$ i $x \cdot y$ jsou prvky $\mathbb{R}$.
2. Asociativita sčítání i násobení: $(x + y) + z = x + (y + z)$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
3. Existence nulového prvku 0 vzhledem ke sčítání.
4. Existence opačného prvku vzhledem ke sčítání: Pro každé x z $\mathbb{R}$ existuje y z $\mathbb{R}$ tak, že $x + y = 0 = y + x$, značíme $y = -x$.
5. Komutativita obou operací: $x + y = y + x$ i $x \cdot y = y \cdot x$
6. (Oboustranná) distributivita násobení ke sčítání: $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$, $(y + z) \cdot x = (y \cdot x) + (z \cdot x)$.

Pokud navíc existuje jednotkový prvek (neutrální při násobení): existuje $1 \in \mathbb{R}$ takový, že pro všechna $x \in \mathbb{R}$ platí $x \cdot 1 = x$ a $1 \cdot x = x$, jedná se o unitární okruh (někdy též jako okruh s jednotkovým prvkem). [5]

$$\begin{aligned} x + (y + z) &= (a + bi) + [(c + di) + (e + fi)] \\ &= (a + bi) + [(c + e) + (d + f)i] \\ &= (a + (c + e)) + (b + (d + f))i \end{aligned}$$

Z toho vidíme, že se obě strany rovnají.

Asociativita násobení: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

$$\begin{aligned} (x \cdot y) \cdot z &= [(a + bi) \cdot (c + di)] \cdot (e + fi) \\ &= [(ac - bd) + (ad + bc)i] \cdot (e + fi) \\ &= (ace - bde - adf - bcf) + (acf - bdf + ade + bce)i \end{aligned}$$

$$\begin{aligned} x \cdot (y \cdot z) &= (a + bi) \cdot [(c + di) \cdot (e + fi)] \\ &= (a + bi) \cdot [(ce - df) + (cf + ed)i] \\ &= (ace - adf - bcf - bde) + (acf + aed + bce - bdf)i \end{aligned}$$

Z toho vidíme, že se obě strany rovnají.

3. Dokážeme existenci nulového prvku vzhledem ke sčítání.
   Předpokládejme, že nulový prvek je $0 = 0 + 0i \in \mathbb{Z}[i]$. Pak platí:

$$x + 0 = (a + bi) + (0 + 0i) = (a + 0) + (b + 0)i = a + bi = x$$

   a podobně:

$$0 + x = (0 + 0i) + (a + bi) = (0 + a) + (0 + b)i = a + bi = x$$

4. Předpokládáme, že opačným prvkem vzhledem ke sčítání je

$$y = -x = -(a + bi) = -a - bi.$$

   Z toho plyne:

$$\begin{aligned} x + y &= x + (-x) \\ &= (a + bi) + (-a - bi) \\ &= (a - a) + (b - b)i \\ &= 0 + 0i \\ &= 0 \end{aligned}$$

   A podobně:

$$\begin{aligned} y + x &= (-x) + x \\ &= (-a - bi) + (a + bi) \\ &= (-a + a) + (-b + b)i \\ &= 0 + 0i \\ &= 0 \end{aligned}$$

5. Komutativita sčítání: $x + y = y + x$.

$$\begin{aligned} x + y &= (a + bi) + (c + di) \\ &= (a + c) + (b + d)i \\ &= (c + a) + (d + b)i \\ &= (c + di) + (a + bi) \\ &= y + x \end{aligned}$$

Komutativita násobení: $x \cdot y = y \cdot x$.

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

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

Z toho vidíme, že se obě strany rovnají.

6. Dokážeme distributivitu násobení ke sčítání: $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

$$\begin{aligned} x \cdot (y + z) &= (a + bi) \cdot [(c + di) + (e + fi)] \\ &= (a + bi) \cdot [(c + e) + (d + f)i] \\ &= a \cdot (c + e) + a \cdot (d + f)i + bi \cdot (c + e) + bi \cdot (d + f)i \\ &= (ac + ae - bd - bf) + (ad + af + bc + be)i \end{aligned}$$

$$\begin{aligned} (x \cdot y) + (x \cdot z) &= [(a + bi) \cdot (c + di)] \cdot [(a + bi) \cdot (e + fi)] \\ &= [(ac - bd) + (ad + bc)i] + [(ae - bf) + (af + be)i] \\ &= (ac - bd + ae - bf) + (ad + bc + af + be)i \end{aligned}$$

Vidíme, že se obě strany rovnají.
Analogicky pro vztah $(y + z) \cdot x = (y \cdot x) + (z \cdot x)$.

Nyní jsme dokázali, že se jedná o okruh. My jsme ale tvrdili, že se jedná o unitární okruh, proto stačí ukázat, že navíc existuje jednotkový prvek $1 = 1 + 0i \in \mathbb{Z}[i]$ vzhledem k násobení:

$$\begin{aligned} x \cdot 1 &= (a + bi) \cdot (1 + 0i) \\ &= (a \cdot 1 - b \cdot 0) + (bi \cdot 1 + a \cdot 0i) \\ &= a + bi \\ &= x \end{aligned}$$

$$\begin{aligned} 1 \cdot x &= (1 + 0i) \cdot (a + bi) \\ &= (1 \cdot a - 0 \cdot b) + (1 \cdot bi + 0i \cdot a) \\ &= a + bi \\ &= x \end{aligned}$$

Na závěr ukážeme, že neexistují dělitelé 0: Nechť $r, s \in \mathbb{Z}[i]$. Využijeme lemma 2, pokud $rs = 0$ potom

$$N(r)N(s) = N(rs) = N(0) = 0$$

Z $rs = 0$ vyplývá, že $N(r) = 0$ nebo $N(s) = 0$. Z lemma 2 vyplývá, že $r = 0$ nebo $s = 0$. Tím pádem $\mathbb{Z}[i]$ nemá žádné dělitele 0, takže $\mathbb{Z}[i]$ je oborem integrity. [4, s. 408]

❑

Gaussova celá čísla nelze porovnávat, uspořádat jako např. celá čísla. Jediné co můžeme porovnávat, je jejich velikost (absolutní hodnota), kterou definujeme v podkapitole 1.3.

1.2 Komplexně sdružené číslo

Pojmem **komplexně sdružené číslo** ke Gaussovu celému číslu $z = a + bi$ nazýváme číslo $\overline{z} = a - bi$. Vznikne změnou znaménka u imaginární části.

Následující tvrzení byla čerpána z vlastností o komplexně sdružených číslech ke komplexním číslům ([6], [7]) a ověřována, zda platí pro všechna Gaussova celá čísla $z_1 = a + bi$ a $z_2 = c + di$, kdy $\overline{z_1} = a - bi$ a $\overline{z_2} = c - di$ jsou komplexně sdružená čísla ke Gaussovým celým číslům.

1. $\overline{(\overline{z_1})} = z_1$,
2. $z_1 = \overline{z_1} \iff z_1$ je elementem $\mathbb{Z}$,
3. $z_1 = -\overline{z_1} \iff z_1$ je elementem ryze imaginárních celých čísel,
4. $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$,
5. $\overline{z_1 - z_2} = \overline{z_1} - \overline{z_2}$,
6. $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$,
7. $z_1 + \overline{z_1} = 2\ Re(z_1)$,
8. $z_1 - \overline{z_1} = 2i\ Im(z_1)$,
9. $z_1 \cdot \overline{z_1} = a^2 + b^2$.

Důkaz.

1. Mějme $\overline{z_1} = a - bi$. Potom $\overline{(\overline{z_1})} = a - (-bi) = a + bi = z_1$
2. Pokud $z_1 = a + bi$, potom vztah $z_1 = \overline{z_1}$ je ekvivalentní s $a + bi = a - bi$. Proto $2bi = 0$, takže $b = 0$ a nakonec $z = a \in \mathbb{Z}[i]$.
3. Pokud $z_1 = a + bi$, potom vztah $z_1 = -\overline{z_1}$ je ekvivalentní s $a + bi = -a + bi$. Proto $2a = 0$, takže $a = 0$ a nakonec $z = bi \in i\mathbb{Z}[i]$.
4. $$\begin{aligned} \overline{z_1 + z_2} &= \overline{(a + bi) + (c + di)} \\ &= \overline{a + c + (b + d)i} \\ &= a - bi + c - di \\ &= \overline{z_1} + \overline{z_2} \end{aligned}$$

5.

$$\begin{aligned}\overline{z_1 - z_2} &= \overline{(a+bi) - (c+di)} \\ &= \overline{a - c + (b-d)i} \\ &= a - c - (b-d)i \\ &= a - c - bi + di \\ &= a - bi - c + di \\ &= \overline{z_1} - \overline{z_2}\end{aligned}$$

6.

$$\overline{z_1 \cdot z_2} = \overline{(ac - bd + (ad+bc)i} = ac - bd - (ad+bc)i$$

$$\overline{z_1} \cdot \overline{z_2} = (a-bi)(c-di) = ac - bd - adi - bci = ac - bd - (ad+bc)i$$

Vidíme, že obě strany se rovnají.

7. $z_1 + \overline{z_1} = (a+bi) + (a-bi) = 2a = 2\ Re(z_1)$
8. $z_1 + \overline{z_1} = (a+bi) - (a-bi) = 2bi = 2i\ Im(z_1)$
9. $z_1 \cdot \overline{z_1} = (a+bi)(a-bi) = a^2 + b^2$.[1]

❑

1.3 Absolutní hodnota Gaussova celého čísla

Definice 4. *Absolutní hodnotou Gaussova celého čísla $z = a + bi$ rozumíme číslo $\sqrt{z\overline{z}}$, tj. $|z| = \sqrt{z\overline{z}} = \sqrt{a^2 + b^2}$.*[2] [2, s. 15]

Následující tvrzení byla čerpána z vlastností o absolutní hodnotě komplexních čísel ([6], [8]) a ověřována, zda platí pro všechna Gaussova celá čísla $z_1 = a + bi$ a $z_2 = c + di$.

1. (a) $-|z_1| \leq Re(z_1) \leq |z_1|$,
   (b) $-|z_1| \leq Im(z_1) \leq |z_1|$.
2. $\forall z_1 \in \mathbb{Z}[i] : |z_1| \geq 0$. Mimo to $|z_1| = 0$ pouze pokud $z_1 = 0$.
3. $|z_1| = |-z_1| = |\overline{z_1}|$.
4. $z_1 \cdot \overline{z_1} = |z_1|^2$.
5. $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$.

[1] Jedná se tedy vždy o nezáporné reálné číslo. Rovnost $z_1 \cdot \overline{z_1} = 0$ nastává pouze pro $z_1 = 0$.

[2] Absolutní hodnota Gaussova celého čísla je definována jako vzdálenost od počátku v Gaussově rovině (viz kapitola 4).

6. $||z_1| - |z_2|| \leq |z_1 + z_2| \leq |z_1| + |z_2|$. Vztahu se říká **trojúhelníková nerovnost**.

Důkaz.

1. (a) $-\sqrt{a^2 + b^2} \leq a \leq \sqrt{a^2 + b^2}$
   (b) $-\sqrt{a^2 + b^2} \leq b \leq \sqrt{a^2 + b^2}$.

   Z toho vidíme, že nerovnosti platí.

2. $\sqrt{a^2 + b^2} \geq 0$. Plyne z definice 4, neboť druhá odmocnina z nezáporného čísla je vždy číslo nezáporné, a proto dané tvrzení platí.

3. Nechť $\overline{z_1} = a - bi$, $-z_1 = -a - bi = -a + (-b)i$, potom

$$|\overline{z_1}| = \sqrt{a^2 + (-b)^2} = \sqrt{a^2 + b^2}$$

   a

$$| - z_1| = \sqrt{(-a)^2 + (-b)^2} = \sqrt{a^2 + b^2}.$$

   Nyní porovnáme $\sqrt{a^2 + b^2} = \sqrt{a^2 + b^2} = \sqrt{a^2 + b^2}$. Z toho vidíme, že rovnost platí.

4. Nechť $\overline{z_1} = a - bi$, potom

$$z_1 \cdot \overline{z_1} = (a + bi)(a - bi) = a^2 + b^2$$

   a

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

   Nyní porovnáme obě strany. Oba výsledky se shodují, a proto platí rovnost.

5. $z_1 \cdot z_2 = (ac - bd) + (bc + ad)i$, a proto

$$\begin{aligned} |z_1 \cdot z_2| &= \sqrt{(ac - bd)^2 + (bc + ad)^2} \\ &= \sqrt{a^2c^2 + b^2d^2 + b^2c^2 + a^2d^2} \\ &= \sqrt{(a^2 + b^2)\,(c^2 + d^2)} \\ &= \sqrt{a^2 + b^2}\sqrt{c^2 + d^2} \\ &= |z_1| \cdot |z_2| \end{aligned}$$

6.

   - **Z algebraického hlediska** [7]**:**
     Budeme dokazovat po částech.
     Část 1:
     Nejprve dokážeme nerovnost na pravé straně.

$$|z_1 + z_2| \leq |z_1| + |z_2|$$

$$\begin{aligned}|z_1+z_2|^2 &= (z_1+z_2)\overline{(z_1+z_2)}\\ &= (z_1+z_2)(\overline{z_1}+\overline{z_2})\\ &= z_1\cdot\overline{z_1}+z_2\cdot\overline{z_2}+z_1\cdot\overline{z_2}+\overline{z_1}\end{aligned}$$

Platí, že $z_1\cdot\overline{z_1}=|z_1|^2$ a $z_2\cdot\overline{z_2}=|z_2|^2$ (viz tvrzení výše).
Protože $\overline{z_1\cdot\overline{z_2}}=\overline{z_1}\cdot\overline{\overline{z_2}}=\overline{z_1}\cdot z_2$, z toho vyplývá, že

$$z_1\cdot\overline{z_2}+\overline{z_1}\cdot z_2 = 2\ Re(z_1\cdot\overline{z_2}) \le 2|z_1\cdot\overline{z_2}| = 2|z_1|\cdot|z_2|,$$

proto

$$|z_1+z_2|^2 \le (|z_1|+|z_2|)^2,$$

a následně

$$|z_1+z_2| \le |z_1|+|z_2|.$$

Část 2:
Nyní budeme dokazovat nerovnost na levé straně.

$$||z_1|-|z_2|| \le |z_1+z_2|$$

$$|z_1| = |z_1+z_2+(-z_2)| \le |z_1+z_2|+|-z_2| = |z_1+z_2|+|z_2|,$$

a proto

$$|z_1|-|z_2| \le |z_1+z_2|.$$

Stejně se odvodí $|z_2|-|z_1| \le |z_1+z_2|$.

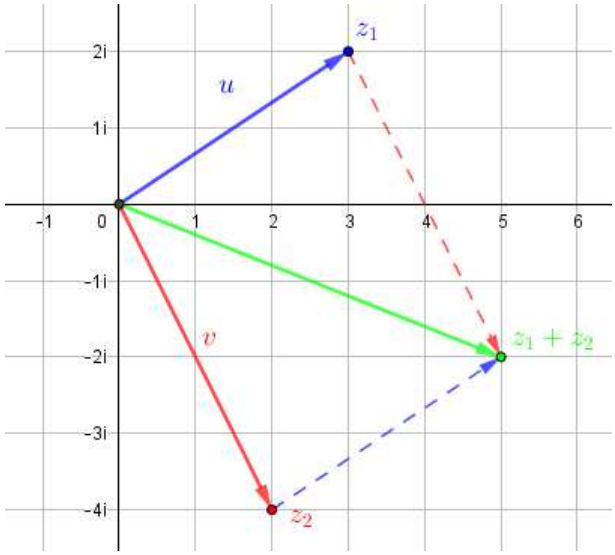
- **Z geometrického hlediska:**
Dokážeme nerovnost na pravé straně:

$$|z_1+z_2| \le |z_1|+|z_2|$$

Všimněte si na obrázku 1.2, že nejkratší vzdálenost mezi 0 a z_1+z_2 je absolutní hodnota ze z_1+z_2, neboli $|z_1+z_2|$. To je kratší délka než cesta, která vede z 0 do z_1 a ze z_1 do z_1+z_2. Celková vzdálenost této druhé cesty je $|z_1|+|z_2|$. Při dokazování využíváme vyjádření Gaussova celého čísla jako **vektor** (viz kapitola 4).
Analogicky bychom dokázali nerovnost na levé straně:

$$||z_1|-|z_2| \le |z_1+z_2|.$$

❑



Obrázek 1.2: Grafický důkaz trojúhelníkové nerovnosti

1.4 Norma Gaussových celých čísel

Definice 5. *Mějme Gaussovo celé číslo $z = a+bi$. Normu*[1] *čísla z, kterou značíme $N(z)$, definujeme vztahem $N(z) = a^2 + b^2$.*[2] [3, s. 601]

Lemma 2. *Na množině $\mathbb{Z}[i]$ platí následující vlastnosti normy N pro všechna $r, s \in \mathbb{Z}$* [4, s. 408]*:*

1. $N(r) \geq 0$,
2. $N(r) = 0$ *pouze, pokud* $r = 0$,
3. $N(rs) = N(r)N(s)$ *(multiplikativita normy).*

Důkaz.

1. Mějme $r = a + bi$. Potom $N(r) = a^2 + b^2$, z toho vidíme, že $a^2 + b^2 \geq 0$.
2. Předpokládejme $r = 0 + 0i$. Potom $N(r) = 0^2 + 0^2 = 0$. Pokud $N(r) = 0$. Potom součet druhých mocnin celých čísel musí být roven nule, proto reálná a imaginární část čísla r jsou čísla nulová.
3. Mějme $r = a + bi$ a $s = c + di$. Potom

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

Nyní porovnáme $N(r)N(s)$ a $N(rs)$:

$$N(r)N(s) = (a^2 + b^2)(c^2 + d^2) = (ac)^2 + (ad)^2 + (bc)^2 + (bd)^2$$

[1] Normou Gaussových celých čísel rozumíme metriku neboli vzdálenost těchto čísel na druhou.

[2] Ze vztahu vidíme, že norma Gaussova celého čísla se vypočte jako součin Gaussova celého čísla a komplexně sdruženého čísla: $N(z) = z\overline{z} = (a + bi)(a - bi) = a^2 + b^2$.

a

$$\begin{aligned} N(rs) &= (ac-bd)^2 + (ad+bc)^2 \\ &= (ac)^2 - 2abcd + (bd)^2 + (ad)^2 + 2abcd + (bc)^2 \\ &= (ac)^2 + (ad)^2 + (bc)^2 + (bd)^2. \end{aligned}$$

Tyto dva výsledky se shodují, a proto $N(rs) = N(r)N(s)$.

❑

Věta 3. *Pokud $z_1 \cdot z_2 = z_3$, potom $N(z_1) \cdot N(z_2) = N(z_3)$.* [9, s. 634]

Důkaz.
Nechť $z_1 = a + bi$ a $z_2 = c + di \in \mathbb{Z}[i]$. Nejprve vynásobíme Gaussova celá čísla na levé straně:

$$\begin{aligned} z_1 \cdot z_2 &= (a+bi) + (c+di) \\ &= (ac-bd)(bc+ad)i \\ &= z_3. \end{aligned}$$

Nyní zjistíme normu čísel z_1 a z_2:

$$N(z_1) = a^2 + b^2, \qquad N(z_2) = c^2 + d^2.$$

Ze součinu čísel víme, čemu se rovná číslo z_3 a dokážeme vypočítat jeho normu:

$$\begin{aligned} N(z_3) &= (ac-bd)^2 + (bc+ad)^2 \\ &= a^2c^2 + b^2d^2 + b^2c^2 + a^2d^2. \\ &= z_3. \end{aligned}$$

A proto

$$N(z_1) \cdot N(z_2) = N(z_3).[9, s.\ 634]$$

❑

Kapitola 2

Dělitelnost a dělení v $\mathbb{Z}[i]$

V dané kapitole se věnujeme dělitelnosti a dělení v $\mathbb{Z}[i]$. Zjišťujeme, zda existují v Gaussových celých číslech definice a věty z celých čísel k dané problematice. Následně jsou tyto poznatky využívány v kapitole 5.

2.1 Dělitelnost v $\mathbb{Z}[i]$

Definice 6. *Řekneme, že Gaussovo celé číslo $z = a + bi$ dělí Gaussovo celé číslo $z_2 = c + di$[1], pouze pokud lze najít Gaussovo celé číslo $r = e + fi$ takové, pro které platí*

$$c + di = (a + bi)(e + fi).$$

Zapisujeme to jako $a + bi \mid c + di$ (neboli $z \mid z_2$). [10, s. 4]

Věta 4. *Na množině $\mathbb{Z}[i]$ platí pro Gaussova celá čísla p, q a r následující vlastnosti dělitelnosti* [11, s. 131]*:*

1. $p \mid q \Rightarrow rp \mid rq$,
2. $pr \mid qr, r \neq 0 \Rightarrow p \mid q$,
3. $p \mid q$, $q \mid r \Rightarrow p \mid r$.

Důkaz.

1. Pokud $p \mid q$, potom existuje Gaussovo celé číslo k takové,že $q = p \cdot k$. Potom $r \cdot q = r \cdot (p \cdot k)$, a tedy $rp \mid rq$.
2. Předpokládáme, že je splněno $pr \mid qr$. Z toho vyplývá, že existuje Gaussovo celé číslo k takové, pro které platí $qr = (pr)k$. Víme, že r je nenulové Gaussovo celé číslo, a proto $q = pk$.
3. Jestliže $p \mid q$ a $q \mid r$, potom existují Gaussova celá čísla k_1 a k_2 taková, že $q = p \cdot k_1$ a $r = q \cdot k_2$. Potom $r = q \cdot k_2 = p(k_1 k_2)$ a $k_1 k_2 \in \mathbb{Z}[i]$, a proto $p \mid r$.

❑

[1] Jinak řečeno, že $z = a + bi$ je dělitelem $z_2 = c + di$.

Věta 5. *Pokud z_1 je dělitelné číslem z_2, potom $N(z_1)$ je dělitelné $N(z_2)$.* [9, s. 634-635]

Důkaz.
Důkaz je převzatý ze stejného zdroje jako věta. Toto vychází z definice 6 a z věty 3. Z definice 6 můžeme zapsat z_1 ve tvaru:

$$z_1 = z_2 \cdot z.$$

Z věty 3 zapíšeme pomocí vztahu:

$$N(z_1) = N(z_2) \cdot N(z),$$

z něhož dostáváme celá čísla a víme, že $N(z_1)$ je dělitelné $N(z_2)$.

❑

Věta 6. *Pokud $\frac{z_1}{z_2} = z_3$, potom $\frac{N(z_1)}{N(z_2)} = N(z_3)$.* [9, s. 635]

Důkaz.
Důkaz je převzatý ze stejného zdroje jako věta. Nechť $z_1 = a + bi$ a $z_2 = c + di$ a $z_2 \neq 0$. Potom

$$\begin{aligned} \frac{z_1}{z_2} &= \frac{a+bi}{c+di} \\ &= \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i \\ &= z_3. \end{aligned}$$

Nyní zjistíme normy:

$$N(z_1) = a^2 + b^2, \qquad N(z_2) = c^2 + d^2.$$

Z toto

$$\frac{N(z_1)}{N(z_2)} = \frac{a^2+b^2}{c^2+d^2}.$$

Nyní vypočítáme $N(z_3)$:

$$\begin{aligned} N(z_3) &= (\frac{ac+bd}{c^2+d^2})^2 + (\frac{bc-ad}{c^2+d^2})^2 \\ &= \frac{a^2c^2 + b^2d^2 + b^2c^2 + a^2d^2}{(c^2+d^2)^2} \\ &= \frac{a^2+b^2}{c^2+d^2}. \end{aligned}$$

Proto

$$\frac{N(z_1)}{N(z_2)} = N(z_3).$$

❑

2.2 Jednotka v $\mathbb{Z}[i]$

Definice 7. *Nechť $u \in \mathbb{Z}[i]$. Řekneme, že u je jednotka, pokud existuje $z \in \mathbb{Z}[i]$ takové, pro které platí $u \cdot z = 1$.* [3, s. 609]

Věta 7. *Gaussova celá čísla mají přesně čtyři jednotky, kterými jsou 1, -1, i a $-i$.* [12, s. 140]

Důkaz.
Část 1:
Z definice 7 známe vztah $u \cdot z = 1$, který můžeme přepsat jako $z = \frac{1}{u}$ za podmínky, že $u \neq 0$. Nyní postupně zjistíme, že 1, -1, i a $-i$ jsou jednotky.

$$\begin{aligned}
u = 1, &\qquad \frac{1}{u} = \frac{1}{1} = 1 \\
u = -1, &\qquad \frac{1}{u} = \frac{1}{-1} = -1 \\
u = i, &\qquad \frac{1}{u} = \frac{1}{i} = \frac{1}{i} \cdot \frac{i}{i} = \frac{i}{-1} = -i \\
u = -i, &\qquad \frac{1}{u} = \frac{1}{-i} = \frac{1}{-i} \cdot \frac{-i}{-i} = \frac{i}{-1} = i
\end{aligned}$$

Část 2:
Když u je jednotka v $\mathbb{Z}[i]$, potom u musí být rovno 1, -1, i, nebo $-i$.
Nechť u je jednotkou $\mathbb{Z}[i]$. Potom existuje $z \in \mathbb{Z}[i]$ takové, že

$$u \cdot z = 1.$$

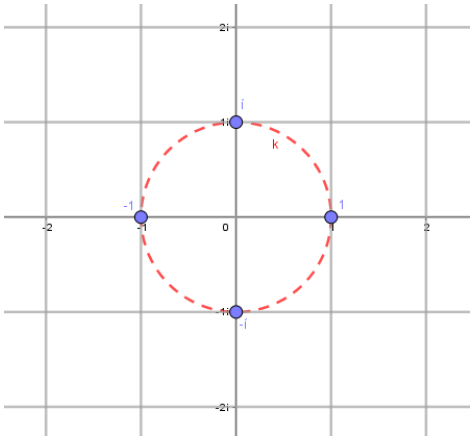
Z lemma 1

$$N(u)N(z) = N(1) = 1.$$

Tím pádem $N(u) \mid 1$. Protože norma Gaussova celého čísla je nezáporné celé číslo, to znamená, že $N(u) = 1$. Z toho vyplývá, že u musí být rovno 1, -1, i, nebo $-i$. Víme, že $N(z) = N(a+bi) = a^2+b^2 = 1$ pro celá čísla a a b. Potom $a^2 = 1-b^2 \leq 1$, podobně $b^2 \leq 1$, což znamená, že jedno z nich (a nebo b) musí být 1 a druhé z nich musí být 0. [3, s. 609]

❑

Gaussova celá čísla s normou 1 jsou pouze ± 1, $\pm i$. Tato čísla tvoří čtyři obrazy v Gaussově rovině na jednotkové kružnici s celočíselnými souřadnicemi. Grafické znázornění můžeme vidět na obrázku 2.1.



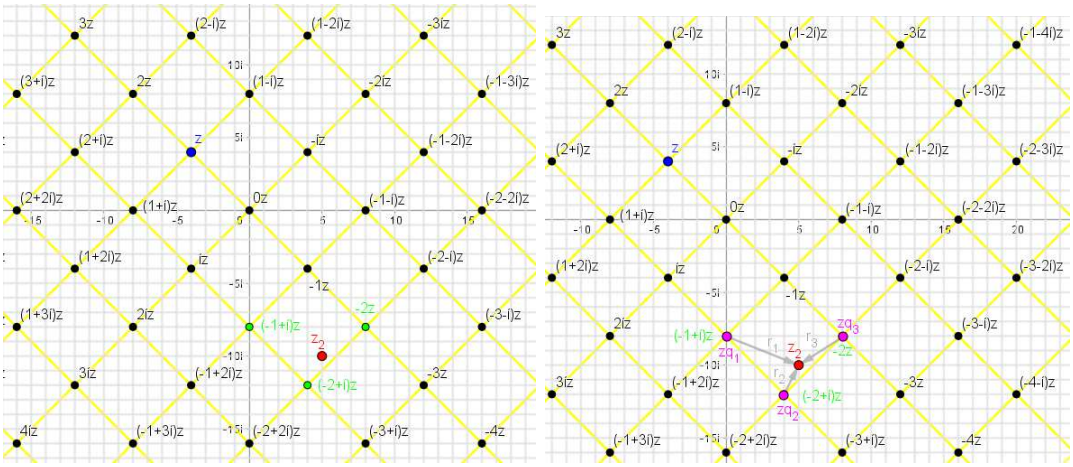
Obrázek 2.1: Jednotky $\mathbb{Z}[i]$ v komplexní rovině

2.3 Dělení se zbytkem v $\mathbb{Z}[i]$

Věta 8. *Nechť $z = a + bi$ a $z_2 = c + di$ $(z, z_2 \in \mathbb{Z}[i])$, $z \neq 0$. Potom existují Gaussova celá čísla q (říkáme kvocient) a r (zbytek) takový, že platí $z_2 = qz + r$ a $N(r) < N(z)$*[1] *.* [13, s. 140]

Důkaz.

- **Z geometrického hlediska** [3, s. 620-621]**:**
  Gaussovy celočíselné násobky z jsou vrcholy čtvercové mříže s délkou hrany $|z|$. Nechť qz je násobkem z, který je nejblíže k z_2 (pokud jsou dva nebo více násobků z, které jsou stejně blízké k z_2, vybereme jeden z nich, který bude qz). Následně ze vztahu ve větě 3 vyjádříme $r = z_2 - qz$. Grafické znázornění jednotlivých čísel můžete vidět na obrázku 2.2.



Obrázek 2.2: Grafické znázornění dělení Gaussovo celých čísel

Největší možná hodnota $|r|$ by nastala, kdyby se z_2 nacházelo v samém středu jednoho ze $|z| \times |z|$ čtverců. V tomto případě $|r|$ by měla být rovna

[1] V některých publikacích se místo normy porovnává absolutní hodnota: $|r| < |z|$.

$\frac{|z|}{\sqrt{2}}$. Bez ohledu na to, jaká je hodnota z_2 (nezáleží na tom, kde z_2 leží v Gaussově rovině), garantujeme, že

$$|r| \leq \frac{|z|}{\sqrt{2}}.$$

Umocněním obou stran této nerovnosti dostáváme

$$N(r) \leq \frac{N(z)}{2}.$$

Protože $N(r) > 0$, máme

$$N(r) < N(z).$$

❑

Jeden důležitý rozdíl mezi větami k dělení se zbytkem pro celá čísla a Gaussova celá čísla je ten, že u běžných celých čísel r a q jsou jedinečné (jednoznačné), ale u Gaussových celých čísel velmi často bývá více než jedna dvojice Gaussových celých čísel q a r, které vyhovují větě 3. Celkovým počtem řešením, které splňuje podmínku $N(r) < N(z)$ (z věty 3), může být jedna, dvě, tři nebo čtyři dvojice (q, r). Více se této otázce budeme věnovat v rámci geometrické interpretace dělení se zbytkem v komplexní rovině v podkapitole 5.3.

2.4 Největší společný dělitel v $\mathbb{Z}[i]$

Definice 8. *Nechť z a z_2 jsou Gaussova celá čísla a předpokládáme, že jeden z nich je nenulový. Řekneme, že d je největší společný dělitel Gaussových celých čísel z a z_2 pokud*

1. *$d \mid z$ a $d \mid z_2$, a*
2. *kdykoliv $d_2 \mid z$ a $d_2 \mid z_2$, potom $d_2 \mid d$.* [14, str. 436]

Poznámka. Budeme psát $d = NSD(z, z_2)$, i když v tomto kontextu je to zneužití zápisu, protože d není určeno jednoznačně. Jestliže d je $NSD(z, z_2)$, pak je zřejmé, že i $-d$, id a $-id$ jsou $NSD(z, z_2)$ viz 2. bod ve větě 9. [15, str. 144] Jinak řečeno, největší společný dělitel Gaussových celých čísel je určen jednoznačně až na násobek jednotky. [16, str. 96]

Věta 9. *Nechť z a z_2 jsou Gaussova celá čísla a předpokládáme, že jeden z nich je nenulový. Potom*

1. *Existuje $d = NSD(z, z_2)$.*
2. *Pokud d' je jiným největším společným dělitelem Gaussových celých čísel z a z_2, potom d' je asociované Gaussovo celé číslo s Gaussovým celým číslem d.*

3. *Existují x, $y \in \mathbb{Z}[i]$ taková, že $d = zx + z_2y$.*

4. *Pokud d_1 je společným dělitelem Gaussových celých čísel z a z_2, potom $N(d_1) \leq N(d)$.*

5. *Pokud d_1 je společným dělitelem Gaussových celých čísel z a z_2, a $N(d_1) = N(d)$, potom d_1 je také největším společným dělitelem Gaussových celých čísel z a z_2.* [14, str. 437]

Důkaz.

1. Nechť I je množina všech lineárních kombinací čísel z a z_2:

$$I = \{zx + z_2y \mid x, y \in \mathbb{Z}[i]\}.$$

Potom $z = 1 \cdot z + 0 \cdot z_2$ a $z_2 = 0 \cdot z + 1 \cdot z_2$ jsou v I, proto I zahrnuje přinejmenším jeden nenulový element (prvek). Nechť

$$d = zx_0 + z_2y_0$$

je nenulový prvek množiny I s nejmenší možnou normou: $0 < N(d) \leq N(s)$ pro všechna nenulová $s \in I$. Tvrdíme, že d je největším společným dělitelem čísel z a z_2. Z věty 8 o dělení se zbytkem víme, že můžeme z_2 dělit z a dostaneme

$$z = qd + r$$

s $N(r) < N(d)$. Poněvadž

$$r = z - qd = z - (zx_0 + z_2y_0)q = (1 - qx_0)z + (-qy_0)z_2,$$

máme $r \in I$. Ale $N(r) < N(d)$ a $N(d)$ je nejmenší hodnotou z norem nenulových elementů z I, proto musíme mít $r = 0$. To znamená, že $z = dq$, a proto $d \mid z$. Podobně bychom zjistili, že $d \mid z_2$. Tím jsme dokázali, že d je společným dělitelem. Předpokládejme, že d_1 je společný dělitel čísel z a z_2, a proto $z = q_1d_1$ a $z_2 = q_2d_1$, pro nějaké q_1, $q_2 \in \mathbb{Z}[i]$. Potom

$$d = zx_0 + z_2y_0 = q_1d_1x_0 + q_2d_1y_0 = (q_1x_0 + q_2y_0)d_1,$$

proto $d_1 \mid d$. To dokazuje, že d splňuje podmínky největšího společného dělitele, a proto existují největší společné dělitele.

2. Předpokládejme, že d' je jiný NSD. Potom d' je společný dělitel, tudíž $d' \mid d$. Tento zápis můžeme zapsat jako $d = d'k_1$ pro některé k_1 (vychází z definice 6 o dělitelnosti). V případ, že obrátíme d a d'. Zjistíme, že $d \mid d'$, což můžeme zapsat jako $d' = dk_2$. Z toho důvodu $dk_2k_1 = d$, a proto $k_1k_2 = 1$. Z toho vyplývá, že $N(k_1)N(k_2) = N(1) = 1$, tudíž $N(k_1) = N(k_2) = 1$. Z věty 7 víme, že $k_2 = \pm 1$ nebo $k_2 = \pm i$.

3. V rámci (1.) jsme již dokázali $d = zx_0 + z_2y_0$. Rovněž v rámci 2. bodu, že $d' = dk_2 = z(k_2x_0) + z_2(k_2x_0)$, a proto platí pro všechny největší společné dělitele.

4. Pokud d je společným dělitelem čísel z a z_2, potom definice 8 o NSD říká, že $d_1 \mid d$. Z toho vyplývá, že $d = d_1 k$ pro některé k, což znamená, že $N(d_1)N(k) = N(d)$. Tudíž $N(d_1) \leq N(d)$.

5. Pokud $N(d_1) = N(d)$, potom $N(k) = 1$. Z věty 7 víme, že k je jednotka, a proto $d = kd_1$ a d_1 je asociované číslo s číslem d v $\mathbb{Z}[i]$ a obě čísla jsou NSD. [14, str. 436-438]

❑

Poznámka. Vztah, který je uveden v 3. bodě věty 9, nazýváme **Bezoutovo rovností v** $\mathbb{Z}[i]$.

Poznámka. Pokud $N(NSD(z, z_2)) = 1$, pak říkáme, že z a z_2 jsou čísla nesoudělná viz podkapitola 2.7.[1]

2.5 Euklidův algoritmus v $\mathbb{Z}[i]$

Euklidův algoritmus pro Gaussova celá čísla je podobný tomu, který známe u běžných celých čísel nebo u polynomů.

Věta 10. *Nechť $z, z_2 \in \mathbb{Z}[i]$ jsou nenulová čísla. Opakovaně použijeme větu o dělení se zbytkem v $\mathbb{Z}[i]$ (viz výše 8). Nejprve vydělíme číslo z_2 číslem z, tím získáme Gaussova celá čísla q (kvocient) a r (zbytek). Následně číslo z vydělíme získaným zbytkem r za předpokladu, že zbytek r je nenulový. Daný postup opakujeme do té doby, než získáme zbytek r nulový* [2] *:*

$$\begin{aligned}
z_2 &= zq_1 + r_1, && N(r_1) < N(z) \\
z &= r_1 q_2 + r_2, && N(r_2) < N(r_1) \\
r_1 &= r_2 q_3 + r_3, && N(r_3) < N(r_2) \\
&\vdots \\
r_k &= r_{k+1} q_{k+2} + r_{k+2}, && N(r_{k+2}) < N(r_{k+1}) \\
r_{k+1} &= r_{k+2} q_{k+3} + 0.
\end{aligned}$$

Poslední nenulový zbytek je dělitelný všemi společnými děliteli čísel z_2 a z a sám je společným dělitelem těchto čísel, a proto tento zbytek je největším společným dělitelem čísel z_2 a z. [17, s. 7]

Důkaz.
Důkaz je totožný s důkazem pro Euklidův algoritmus běžných celých čísel, který si nyní stručně shrneme.

[1] Jinak řečeno, jestliže 1 je největším společným dělitelem čísel z a z_2, pak můžeme říci, že z a z_2 jsou čísla nesoudělná.

[2] Tento proces pokračuje do té doby, dokud norma zbytku není rovna nule. Jelikož hodnoty těchto norem jsou nenulová celá čísla a monotonicky klesají, proto po konečném počtu kroků získáme zbytek nula. [11, s. 133]

Pokud budeme procházet množinu rovnic od zdola (od poslední rovnice) nahoru, pak je snadno vidět, že

$$r_{k+2} \mid r_{k+1},\ r_{k+2} \mid r_k,\ \ldots\ ,\ r_{k+2} \mid r_1,\ r_{k+2} \mid z,\ r_{k+2} \mid z_2.$$

V zápisu výše je ukázáno, že poslední nenulový zbytek (tedy ten, který je v předposlední rovnici) je společným dělitelem čísel z_2 a z. Tento poslední nenulový zbytek je společným dělitelem, který je dělitelný všemi ostatními.
Při průchodu od první rovnice dolů (k poslední rovnici) snadno ukážeme, že

$$x \mid z_2,\ x \mid z\ \Rightarrow\ x \mid r_1,\ \ldots\ , x \mid r_k,\ x \mid r_{k+1},\ x \mid r_{k+2}.$$

Z toho vidíme, že každý společný dělitel čísel z_2 a z dělí poslední nenulový zbytek. [11, s. 133] [17, s. 7]

❑

Poznámka. Poslední nenulový zbytek má největší normu mezi společnými děliteli, a proto je to největší společný dělitel.

Poznámka. Euklidův algoritmus, který je popsán ve větě 10, zahrnuje možné volby v každém kroku tohoto algoritmu, proto kvocient (q) a zbytek (r) nejsou určeny jednoznačně ve vztahu $z_2 = qz + r$ z věty 8. *Při hledání největšího společného dělitele Gaussových celých čísel pomocí Euklidova algoritmu se budeme snažit, aby norma zbytku r byla co nejmenší. V případě že normy zbytků jsou stejné, budeme se snažit hledat zbytek r následovně:*

1. *reálná a imaginární část je kladné celé číslo,*
2. *reálná část je kladné celé číslo,*
3. *imaginární část je kladné celé číslo.*[1]

Poznámka. V každém případě Euklidův algoritmus poskytuje existenci největšího společného dělitele. [15, str. 144]

Důsledek (Euklidova algoritmu). Pro nenulová čísla z_2 a z v $\mathbb{Z}[i]$, nechť d je největším společným dělitelem získaný pomocí Euklidova algoritmu. Jakýkoliv největší společný dělitel čísel z_2 a z je jednotkovým násobkem d v $\mathbb{Z}[i]$. [17, str. 9]

Důkaz. Nechť d' je největším společným dělitelem čísel z_2 a z. Z důkazu Euklidova algoritmu víme, že $d'|d$, protože d' je společným dělitelem. Z definice 6 můžeme zapsat pomocí rovnosti $d = p \cdot d'$, takže

$$N(d) = N(d')N(p) \geq N(d').$$

Poněvadž d' je největší společný dělitel, jeho norma je největší mezi normami společných dělitelů, proto nerovnost $N(d) \geq N(d')$ musí být rovností. To znamená, že $N(p) = 1$, proto $p = \pm 1$ nebo $p = \pm i$. Tudíž d a d' jsou jednotkové násobky navzájem. [17, str. 9]

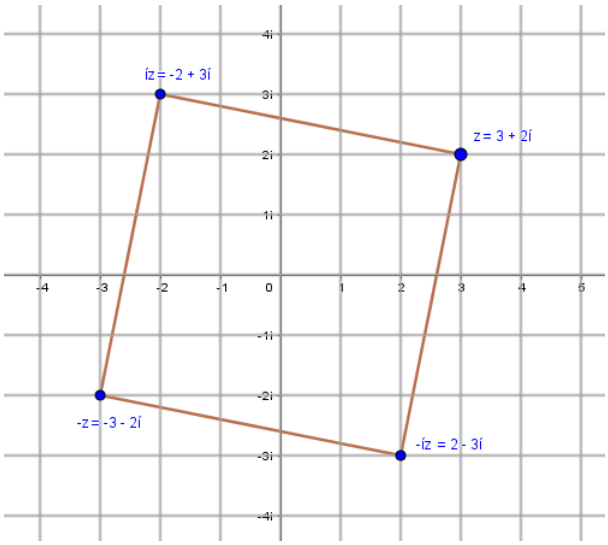
❑

[1] Podmínky uvedené kurzívou zvolil (stanovil) autor sám, protože v žádné dostupné literatuře, kterou procházel, nenašel v této otázce jednoznačně řečeno, jaká dvojice v rámci jednotlivých kroků je jedinečná.

2.6 Asociovaná čísla (prvky) v $\mathbb{Z}[i]$

Definice 9. *Gaussova celá čísla z_1 a z_2 jsou nazývána asociovaná* [1]*, jestliže $z_1 = z_2 \cdot u$ a u je jednotka.* [18, s. 154]

Například existuje asociovaný vztah mezi $a + bi$, $-b + ai$, $-a - bi$ a $b - ai$. Grafické znázornění asociovaných čísel ke konkrétnímu číslu $z = 3 + 2i$ v komplexní rovině můžeme vidět na obrázku 2.3. Tato čísla doplňují vrcholy čtverce. Navíc komplexně sdružené číslo $a - bi$ k číslu $a + bi$ není mezi asociovanými čísly.



Obrázek 2.3: Asociovaná čísla $\mathbb{Z}[i]$ v komplexní rovině

Asociovaná čísla a jejich zobrazení v Gaussově rovině si můžeme ověřit pomocí **Applet č. 10**. Bližší informace k danému appletu získáme v kapitole 7 s názvem Applety (přesněji 7.5.10).

Věta 11. *Pro dvojici Gaussových celých čísel z_1 a z_2 platí* [11, s. 131]*:*

$$z_1 \mid z_2, z_2 \mid z_1 \Rightarrow z_1 = \pm z_2 \text{ nebo } z_1 = \pm i z_2.$$

Důkaz.
Předpokládejme, že $z_1 \mid z_2 = q$. Potom q a $q^{-1} = z_2 \mid z_1$ jsou Gaussova celá čísla. Očividně,

$$1 = N(1) = N(q \cdot q^{-1}) = N(q) \cdot N(q^{-1}),$$

z čehož $N(q) = N(q^{-1}) = 1$ (víme, že $N(q)$ a $N(q^{-1})$ jsou běžná kladná celá čísla). Ale existují pouze 4 Gaussova celá čísla s normou 1, které jsme uvedli ve větě 7. [11, s. 131]

❑

[1] Asociované prvky se liší pouze vynásobením některou jednotkou. Asociované prvky jsou si navzájem svými děliteli.

2.7 Nesoudělná čísla v $\mathbb{Z}[i]$

Definice 10. *Pokud Gaussova celá čísla z_1 a z_2 mají pouze společné jednotkové dělitele $(1, -1, i$ a $-i)$, tato čísla nazýváme nesoudělná čísla.*[1] [17, s. 7]

Dříve jsme si uváděli znění Bezoutovy rovnosti v $\mathbb{Z}[i]$ (viz 3. bod ve větě 9). Nyní jsme si řekli, co jsou to nesoudělná čísla v $\mathbb{Z}[i]$, a proto můžeme vyslovit následující větu, která je důsledkem Bezoutovy rovnosti:

Věta 12. *Pokud z_1 a z_2 jsou nesoudělná Gaussova celá čísla, potom 1 může být vyjádřena jako kombinace čísel z_1 a z_2 ve tvaru* [2]

$$z_1x + z_2y = 1,$$

kde x a y jsou Gaussova celá čísla. [19, s. 141]

Důkaz.
Jestliže z_1 a z_2 jsou nesoudělná Gaussova celá čísla, potom 1 je největším společným dělitelem čísel z_1 a z_2, a proto $1 = z_1x + z_2y$ pro některé $x, y \in \mathbb{Z}[i]$ podle věty 9. Naopak pokud $1 = z_1x + z_2y$ platí pro některé $x, y \in \mathbb{Z}[i]$, potom nějakým společným dělitelem čísel z_1 a z_2 je 1 (neboli jednotka). To říká, že tato čísla z_1 a z_2 jsou čísla nesoudělná. [17, s. 9]

❑

Lemma 13. *Nechť $z_1 \mid z_2q \in \mathbb{Z}[i]$, kde z_1 a z_2 jsou čísla nesoudělná. Potom $z_1 \mid q$.* [17, s. 10]

Důkaz.
Důkaz je obdobný jako pro běžná celá čísla. Z definice 6 dostáváme vztah $z_2q = z_1k$ pro nějaké $k \in \mathbb{Z}[i]$. Poněvadž z_1 a z_2 jsou nesoudělná čísla, můžeme jej zapsat pomocí rovnice (viz věta 12)

$$1 = z_1x + z_2y,$$

kde $x, y \in \mathbb{Z}[i]$. Vynásobením obou stran rovnice q dostáváme

$$\begin{aligned} q &= qz_1x + qz_2y \\ &= z_1qx + z_1ky \\ &= z_1(qx + ky). \end{aligned}$$

Z toho vidíme, že $z_1 \mid q$. [17, s. 10]

❑

Lemma 14. *Pokud $z_1 \mid q$ a $z_2 \mid q \in \mathbb{Z}[i]$, kde z_1 a z_2 jsou čísla nesoudělná. Potom $z_1z_2 \mid q$.* [17, s. 11]

[1] Symbolicky: $u \mid z_1$ a $u \mid z_2$ a $u \in \mathbb{Z}[i]$ je jednotka.
[2] Někdy tento vztah nazýváme **lineární diofantická rovnice**.

Důkaz.
Z definice 6 dostáváme vztah $q = z_1 k$ a $q = z_2 l$ pro nějaké $k, l \in \mathbb{Z}[i]$. Poněvadž z_1 a z_2 jsou nesoudělná čísla, můžeme jej zapsat pomocí rovnice (viz věta 12)

$$1 = z_1 x + z_2 y,$$

kde $x, y \in \mathbb{Z}[i]$. Z toho důvodu

$$\begin{aligned} q &= q \cdot 1 \\ &= q z_1 x + q z_2 y \\ &= (z_2 l) z_1 x + (z_1 k) z_2 y \\ &= z_1 z_2 (lx + ky). \end{aligned}$$

Z toho $lx + ky \in \mathbb{Z}[i]$, a proto $z_1 z_2 \mid q$.

❑

Kapitola 3

Prvočísla v $\mathbb{Z}[i]$

V kapitole zkoumáme, zda platí stejné vlastnosti (věty a definice) o prvočíslech a prvočíselném rozkladu v $\mathbb{Z}[i]$ jako v oboru celých čísel. Tuto teorii následně využíváme v kapitole 6 pro geometrickou interpretaci.

3.1 Zavedení a vlastnosti v $\mathbb{Z}[i]$

Definice 11. *Nechť $p \in \mathbb{Z}[i]$ takové, že p není jednotkou. Řekneme, že p je prvočíslo*[1] *pro každé $a, b \in \mathbb{Z}[i]$, $p = ab$, to znamená, že a je jednotkou nebo b je jednotkou. [3]*

Definice 12. *Gaussovo celé číslo p je nazýváno prvočíslem, pouze pokud je toto číslo p dělitelné*[2]*:*

$$1, -1, i, -i, p, -p, pi \ a \ -pi.[10, \text{s. } 5]$$

Z definice 12 víme, že každé Gaussovo celé číslo z má alespoň čtyři dělitele 1, -1, i, $-i$. Navíc jakákoliv Gaussovo celé číslo z, které není zároveň jednotkou, má další čtyři dělitele, a to z, $-z$, iz, $-iz$. Vidíme, že každé takové číslo v $\mathbb{Z}[i]$ má alespoň osm různých dělitelů.

Definice 13. *Gaussovo celé číslo p je prvočíslo, pokud $N(p) > 1$ a jestliže toto číslo p nelze zapsat jako součin Gaussových celých čísel (činitelů) s normou větší než 1.* [20, s. 459]

Poznámka. Čísla, která lze zapsat jako netriviální rozklad (součin), nazýváme složená čísla. Tato čísla lze rozložit.

Věta 15. *Každé Gaussovo celé číslo z, jehož norma je větší než 1 ($N(z) > 1$), je možné zapsat jako součin Gaussových prvočísel.* [17, s. 13]

Důkaz.
Dokážeme pomocí indukce podle $N(z)$ (ne podle z).
Předpokládejme, že $N(z) = 2$. (Jinými slovy $z = 1 \pm i$ nebo $z = -1 \pm i$.) Potom z je prvočíslo podle lemma 17.

[1] Někdy se používá název komplexní prvočíslo nebo Gaussovo prvočíslo.
[2] Prvočíslo v $\mathbb{Z}[i]$ je dělitelné pouze jednotkou a asociovanými čísly.

Nyní předpokládáme, že $n \geq 3$ a každé Gaussovo celé číslo s normou větší než 1 a menší než n je součinem prvočísel. Chceme ukázat, že každé Gaussovo celé číslo s normou n je součinem prvočísel. Pokud neexistují žádná Gaussova celá čísla s normou n, potom není co dokazovat. Takže můžeme předpokládat, že existuje Gaussovo celé číslo s normou n, které je součinem prvočísel (v $\mathbb{Z}[i]$). Pokud máme Gaussovo celé číslo z s normou n, které je složené, můžeme zapsat netriviální rozklad z jako rs, kde $N(r)$, $N(s) < N(z) = n$. Podle indukční hypotézy r a s je součin prvočísel v $\mathbb{Z}[i]$. Proto rozklad čísla z je součin prvočísel v $\mathbb{Z}[i]$. Tímto jsme danou větu dokázali. [17, s. 13]

❑

Věta 16. *Pokud p je Gaussovo prvočíslo a a, b jsou Gaussova celá čísla taková, že $p \mid ab$, potom $p \mid a$ nebo $p \mid b$ v $\mathbb{Z}[i]$.*[21, s. 509]

Důkaz.
Předpokládáme, že $p \mid ab$, ale $p \nmid a$. Chceme ukázat, že $p \mid b$.
Protože $p \nmid a$ a p je prvočíslo v $\mathbb{Z}[i]$, největším společným dělitelem čísel p a a musí být jednotka, neboť p a a jsou čísla nesoudělná. Z věty 12 víme, že v tomto případě lze jednotku u vyjádřit jako lineární kombinaci čísel p a a

$$px + ay = u,$$

kde $x, y \in \mathbb{Z}[i]$. Vynásobíme obě strany rovnice b a dostáváme

$$pxb + ayb = ub,$$

Ale p dělí oba sčítance pravé strany rovnice, $p \mid ub$, proto $p \mid b$.

❑

Lemma 17. *Nechť z je Gaussovo celé číslo. Pokud $N(z) = p$ je prvočíslo*[1]*, potom z je Gaussovo prvočíslo (číslo nerozložitelné) v $\mathbb{Z}[i]$.* [14, s. 430]

Důkaz.
Předpokládáme, že $z = z_1 z_2$. Potom $p = N(z) = N(z_1)(z_2)$ (víme z věty 3). Z toho, že p je prvočíslo a $N(z_1)$ a $N(z_2)$ jsou celá čísla ($\mathbb{Z}$), musíme mít $N(z_1) = 1$ nebo $N(z_2) = 1$. Z věty 7 lze odvodit, že z_1 nebo z_2 je jednotka. Tudíž rozklady čísla z jsou jednoduché, a proto z je prvočíslo. [14, s. 430]

❑

[1]Prvočíslo je přizozené číslo větší než 1, které kromě sebe sama a jedničky není dělitelné žádným jiným přirozeným číslem. [22]

Věta 18. *Nechť p a q jsou Gaussova prvočísla. Pokud $p \mid q$, potom $q = u \cdot p$ pro některé jednotky $u \in \mathbb{Z}[i]$.*[3, s. 634]

Důkaz.
Z definice 6 vyjádříme dělitelnost následovně

$$g = p \cdot s.$$

Z definice prvočísel 11 víme, že $s = u$, protože q a p jsou prvočísla a dostáváme vztah

$$g = p \cdot u,$$

kde u jednotkou v $\mathbb{Z}[i]$. Tímto jsme danou větu dokázali.

❑

Věta 19. *Nechť $u \in \mathbb{Z}[i]$ je jednotkou. Potom jakýkoliv dělitel u v $\mathbb{Z}[i]$ je také jednotkou.* [3, s. 634]

Důkaz.
Nechť z je Gaussovo celé číslo, pro které platí $z \mid u$, kde $u \in \mathbb{Z}[i]$ je jednotkou. Z definice dělitelnosti 6 víme, že

$$u = z \cdot r.$$

Tento vztah můžeme přepsat jako $r = \dfrac{u}{z}$ za podmínky, že $z \neq 0$. Z toho vidíme, že abychom získali Gaussovo celé číslo, z musí být také jednotkou.

❑

Věta 20. *Nechť q je Gaussovo prvočíslo a předpokládejme, že q dělí součin $e \cdot f$ dvou Gaussových celých čísel e a f. Potom q dělí buď e nebo f.* [23, s. 212]

Důkaz.
Pokud q dělí f, potom není co dokazovat. Předpokládejme, že q nedělí f. Pak q je Gaussovo prvočíslo, q a f jsou nesoudělná čísla. Podle věty 12 dostáváme rovnici

$$qx + fy = 1,$$

kde x a y jsou Gaussova celá čísla. Vynásobením tohoto vztahu g získáváme

$$(q \cdot g)x + (f \cdot g)y = g.$$

Podle předpokladu obě podmínky na levé straně jsou dělitelné q. Proto je i pravá strana, tj. g je dělitelné q. [23, s. 212]

❑

Věta 21. *Nechť $p, p_1, p_2, ..., p_n$, kde $n \in \mathbb{N}$, jsou Gaussova prvočísla taková, že $p \mid p_1 \cdot ... \cdot p_n$. Potom p je asociované s jedním z Gaussových prvočísel $p_1, ..., p_n$.* [16, s. 97]

Důkaz.
Můžeme předpokládat, že p není asociováno s žádným z $p_1 \cdot ... \cdot p_{n-1}$. Potom předchozí věta (věta 21) říká, že $p \mid p_n$. Z toho p a p_n jsou Gaussova prvočísla, dostáváme vztah $p_n = up$, kde u je jednotkou. [16, s. 97]

❑

Věta 22. *Nechť $p, n \in \mathbb{Z}[i]$, p je prvočíslo a $p \mid n$. Potom $N(\frac{n}{p}) < N(n)$.* [3, s. 14]

Důkaz.
Předpokládáme, že $p \mid n$. Podle definice 6 vyjádříme dělitelnost pomocí následujícího zápisu

$$n = p \cdot q.$$

Z věty 3 lze zapsat pomocí vztahu

$$N(n) = N(p) \cdot N(q), \tag{3.1}$$

který můžeme přepsat jako

$$\frac{N(n)}{N(p)} = N(q). \tag{3.2}$$

Ze vztahů (3.1) a (3.2) vidíme, že platí tato nerovnost $N(\frac{n}{p}) < N(n)$[1].

❑

Věta 23. *Gaussovo prvočísel existuje nekonečně mnoho.* [24, s. 98]

Důkaz.
Budeme dokazovat sporem.
Předpokládejme, že Gaussových prvočísel existuje konečně mnoho. Označme jej $p_1, p_2, ..., p_n$, kde $n \in \mathbb{N}$. Uvažujme číslo $q = p_1 \cdot p_2 \cdot ... \cdot p_n + 1$, které není dělitelné žádným prvočíslem. Pokud by tomu bylo jinak, potom existuje $i \in 1, 2, ..., n$, pro které platí $p_i \mid q$, z to vyplývá, že $p_i \mid q - p_1 \cdot p_2 \cdot ... \cdot p_n$. Proto dostáváme $p_i \mid 1$, což je spor. Ale podle věty 15 lze číslo q rozložit na prvočinitele, tím získáváme spor. [25, s. 15]

❑

[1] Víme, že norma je kladné běžné celé číslo, které můžeme porovnávat.

Věta 24. *Pokud p je prvočíslo v $\mathbb{Z}[i]$, potom jeho komplexně sdružené číslo $\overline{p}$ je také prvočíslo v $\mathbb{Z}[i]$.* [26, s. 29]

Důkaz.
Nechť $p = a_1 + a_2 i$, potom $\overline{p} = a_1 - a_2 i$. Pokud $\overline{p} = (b_1 + b_2 i)(c_1 + c_2 i)$ je číslo rozložitelné (složené), pak můžeme předpokládat, že $N(b_1 + b_2 i) > 1$, $N(c_1 + c_2 i) > 1$. Jednoduše vidíme, že $p = \overline{\overline{p}}$ je také rozložitelné. [26, s. 29]

❑

Věta 25. *Pokud p je celé prvočíslo, potom p je buď Gaussovo prvočíslo nebo je součinem dvou komplexně sdružených Gaussových prvočísel.* [27, s. 72]

Důkaz.
Pokud p je celým prvočíslem, není jednotkou v $\mathbb{Z}[i]$, a proto p je dělitelné Gaussovým prvočíslem $z = a + bi$. Potom $\overline{z} = a - bi$ dělí $\overline{p}$ a $\overline{p} = p$. Z toho vyplývá, že $\overline{z}z = a^2 + b^2$ dělí p^2 v $\mathbb{Z}[i]$ a také v $\mathbb{Z}$. A tedy $\overline{z}z$ je rovno p^2 nebo p. Jestliže $\overline{z}z = p^2$, z a p jsou asociované, a proto p je Gaussovo prvočíslo.

❑

Věta 26. *Pokud p je Gaussovo prvočíslo, potom $p\overline{p}$ je prvočíslo nebo kvadrát*[1] *prvočísla v $\mathbb{Z}[i]$.* [27, s. 72]

Důkaz.
Nechť p je Gaussovo prvočíslo, $p\overline{p} = n \in \mathbb{Z}$ (a proto v $\mathbb{Z}[i]$). Gaussovo prvočíslo p dělí jeden z celých prvočíselných činitelů, např. q čísla n. Tedy $p\overline{p}$ je celočíselným dělitelem čísla p^2, tím jsme dokázali tuto větu. [27, s. 72]

❑

Věta 27. *(Reálná Gaussova prvočísla) Běžné prvočíslo $p \in \mathbb{N}$ je Gaussovo prvočíslo $\Leftrightarrow$ p není součtem dvou čtverců. (A samozřejmě $p < 0$ je Gaussovo prvočíslo $\Leftrightarrow -p \in \mathbb{N}$ je Gaussovo prvočíslo.)* [28, s. 105]

Důkaz.
($\Leftarrow$) Předpokládáme, že máme běžné prvočíslo p, které není Gaussovým prvočíslem, a proto jej můžeme rozložit v $\mathbb{Z}[i]$:

$$p = (a + bi)q, \tag{3.3}$$

kde $a + bi$ a q jsou Gaussova celá čísla s normou menší než norma p^2 čísla p (a tedy i norma větší než 1). Vezmeme-li komplexně sdružená čísla obou stran, dostaneme

$$p = (a - bi)\overline{q}, \tag{3.4}$$

poněvadž p je reálné, proto $p = \overline{p}$. Vynásobením výrazů (3.3) a (3.4) jako p získáme

$$\begin{aligned} p^2 &= (a - bi)(a + bi)q\overline{q} \\ &= (a^2 + b^2)|q|^2, \end{aligned}$$

[1] Kvadrát = druhá mocnina

kde obojí $a^2 + b^2$, $|q|^2 > 1$. Ale jediný takový rozklad p^2 je pp, proto $p = a^2 + b^2$. ($\Rightarrow$) Naopak, pokud běžné prvočíslo p je rovno $a^2 + b^2$, kde $a, b \in \mathbb{Z}$, pak p není Gaussovo prvočíslo, protože lze prvočíselně rozložit v $\mathbb{Z}[i]$ jako

$$p = (a - bi)(a + bi)$$

na činitele o normě $a^2 + b^2 = p$, která je menší než norma $N(p) = p^2$. [28, s. 105] ❑

Věta 28. *(Imaginární Gaussova prvočísla) Gaussova prvočísla $a + bi$, kde a a b jsou nenulové, jsou součinem běžných prvočísel p ve tvaru $a^2 + b^2$.* [28, s. 108]

Důkaz.
Z věty 24 víme, že pokud $a+bi$ je Gaussovo prvočíslo, potom i $a-bi$ je Gaussovo prvočíslo. Dále podle věty 25 $(a - bi)(a + bi)$ je (nutně jedinečný) prvočíselný rozklad v $\mathbb{Z}[i]$ jako

$$p = (a - bi)(a + bi)$$

Ale p potom musí být běžné (celé) prvočíslo. Pokud ano

$$p = r \cdot s$$

s $1 < r, s < p$ a $r, s \in \mathbb{Z}$, pak Gaussovi prvočíselní činitelé r a s vyjadřují Gaussův prvočíselný rozklad čísla p různý od $(a - bi)(a + bi)$ (buď dva reálné činitele r a s, nebo $\geq$ čtyři komplexní činitele). [28, s. 108] ❑

3.2 Rozklad v $\mathbb{Z}[i]$

Definice 14. *Pokud Gaussovo celé číslo g je součinem dvou Gaussových celých čísel f a h, takže*

$$g = fh,$$

řekneme, že f a h dělí g. Tato rovnost je pak nazývána rozklad čísla g, kde f a h jsou jeho činitelé (dělitelé). [19, s. 140]

3.3 Prvočíselný rozklad v $\mathbb{Z}[i]$

Věta 29. *Každé Gaussovo celé číslo z, které je nenulové a není jednotkou, můžeme zapsat jako součin Gaussových prvočísel. Navíc je takový prvočíselný rozklad jedinečný až na pořadí a násobek jednotky.* [29, s. 173]

Důkaz.
Existenci prvočíselného rozkladu v $\mathbb{Z}[i]$ jsme dokázali ve větě 15.

Nyní dokážeme jedinečnost věty (29). Musíme ukázat, že každé nenulové Gaussovo celé číslo z, které není jednotkou, má nejvýše jeden prvočíselný rozklad až na pořadí a násobek jednotky. K dokazování použijeme silnou matematickou indukci. Poněvadž z je Gaussovo celé číslo, nikoliv přirozené číslo, proto nemůžeme provést indukci podle z přímo. Místo toho provedeme naší indukci podle normy čísla z.

Podmínka, že nenulové Gaussovo celé číslo z není jednotkou, je ekvivalentní s $N(z) > 1$.

Nechť $z \in \mathbb{Z}[i]$, $N(z) > 1$, a předpokládejme indukční hypotézu, že každé číslo k, které vyhovuje $1 < N(k) < N(z)$, má nejvýše jeden prvočíselný rozklad až na pořadí a násobek jednotky.

Nyní ukážeme, že z má nejvýše jeden prvočíselný rozklad až na pořadí a násobek jednotky. Předpokládáme, že z může být zapsáno jako součin Gaussových prvočísel dvěma různými způsoby. To znamená, že připouštíme

$$z = p_1 \cdot p_2 \cdot \cdots \cdot p_e = q_1 \cdot q_2 \cdot \cdots \cdot q_f, \tag{3.5}$$

kde $p_1, p_2, \cdots, p_e$ a $q_1, q_2, \cdots, q_f$ jsou Gaussova prvočísla.

Musíme ukázat, že tyto dva prvočíselné rozklady čísla z jsou stejné až na pořadí a násobek jednotky.

Rovnice (5.2) naznačuje (podle definice dělitelnosti 6), že

$$p_1 \mid q_1 \cdot q_2 \cdot \cdots \cdot q_f.$$

Z vět 16 a 21 vyplývá, že p_1 dělí jedno z prvočísel $q_1, q_2, \cdots, q_f$. Bez újmy na obecnosti můžeme předpokládat, že $p_1 \mid q_1$. Poněvadž p_1 a q_1 jsou obě prvočísla, tak z toho vyplývá, že $q_1 = p_1 \cdot u$ pro nějakou jednotku u (vychází z věty 18. Substitucí do této rovnice (5.2) získáme

$$\frac{z}{p_1} = p_2 \cdot \cdots \cdot p_e = u \cdot q_2 \cdot \cdots \cdot q_f. \tag{3.6}$$

Nejprve uvažujeme o tom, že $N(\frac{z}{p_1}) = 1$. V tomto případě $\frac{z}{p_1}$ je jednotkou. Poněvadž jednotky nemohou být dělitelné prvočíslem (vychází z věty 19), nesmí existovat vůbec žádná prvočísla v rozkladu. Jinými slovy, $e = f = 1$, a proto p_1 a q_1 jsou rovny jednotkám. V rozkladech čísla z v (5.2) jsou stejné až na jednotky.

Případ $N(\frac{z}{p_1}) = 1$ jsme pokryli. Po zbytek důkazu budeme předpokládat, že $N(\frac{z}{p_1}) > 1$, navíc $N(\frac{z}{p_1}) < N(z)$ (což jsme dokázali ve větě 22). Proto můžeme používat naší indukční hypotézu k závěru, že dva rozklady v rovnici (3.6) jsou stejné až na pořadí a násobek jednotky. Ale rozklad v rovnici (5.2) jsou právě rozklady v rovnici (3.6) s dalším činitelem p_1. Uzavřeme to tím, že oba rozklady v rovnici 5.2 jsou stejné až na pořadí a násobek jednotky. Tudíž jsme ukázali, že z má nejvýše jeden prvočíselný rozklad, který se liší až na pořadí a násobek jednotky.

Z principu silné matematické indukce vyplývá, že každé Gaussovo celé číslo z s normou větší než 1 má nejvýše jeden prvočíselný rozklad až na pořadí a násobek jednotky. [3, s. 632-633]

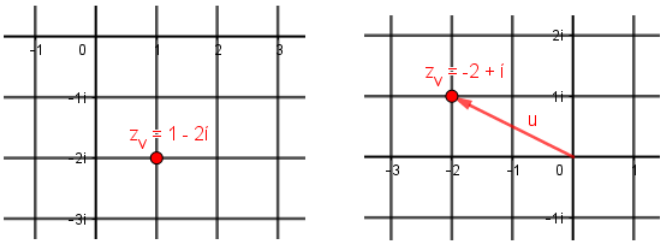
❑

Kapitola 4

Geometrické znázornění Gaussových celých čísel

V této kapitole se budeme věnovat geometrické interpretaci Gaussových celých čísel, vybraným vlastnostem těchto čísel a zároveň základním operacím, které můžeme u daných čísel provádět. Tyto vlastnosti a operace jsou doplněny obrázky z autorových appletů. U některých témat se můžeme setkat s úlohy k procvičení dané problematiky.

4.1 Geometrická interpretace Gaussových celých čísel



Obrázek 4.1: Gaussovo celá čísla jako bod (vlevo) a vektor (vpravo)

Gaussova celá čísla můžeme geometricky interpretovat jako **body** (nebo **vektory**) karteziánské souřadnicové roviny. Tyto body (vektory) označujeme jako **mřížové** [1]. Ke Gaussovu celému číslu $z = (a,b) = a + bi$ můžeme přiradit obraz (bod) M v rovině xy, který má karteziánské souřadnice $[a,b]$, nebo vektor $\overrightarrow{u} = \overrightarrow{OM}$, kde M$[a, b]$ je obraz Gaussova celého čísla z. Tento vektor má délku $|z|$ a směr polopřímky $\overrightarrow{OM}$. Grafické znázornění Gaussových celých čísel v komplexní rovině můžeme vidět na obrázku 4.1. [31] [6]

[1] **Mřížové body** jsou takové body, jejichž obě souřadnice jsou celá čísla. **Mřížovým vektorem** nazveme vektor, jehož obě souřadnice jsou celá čísla. Někdy se slovo mřížový zkracuje předponou „m“, např. **m-přímka** je přímka, která obsahuje alespoň dva (a tedy nekonečně mnoho) mřížových bodů. [30]

Rovinu komplexních čísel (komplexní rovina) někdy nazýváme jako **Argandova rovina** nebo **Gaussova rovina**. [32]

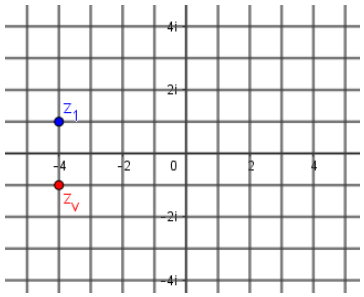
Úloha 1. K určování algebraického tvaru (souřadnic) Gaussova celého čísla, které je zobrazeno v komplexní rovině, lze využít **Applet č. 1**. Bližší popis daného appletu nalezneme v kapitole 7 s názvem Applety (přesněji 7.5.1).

Úloha 2. K procvičení geometrické interpretace Gaussových celých čísel v komplexní rovině můžeme využít **Applet č. 2**. Bližší popis daného appletu nalezneme v kapitole 7 s názvem Applety (přesněji 7.5.2).

4.2 Gaussova rovina

Gaussova rovina je rovina s pravoúhlým souřadnicovým systémem, jehož osy označíme x a y, a jejíž body pokládáme za obrazy Gaussových celých čísel. Osu x budeme nazývat **reálnou osou** a osu y **imaginární osou**.[7]

4.3 Komplexně sdružené číslo



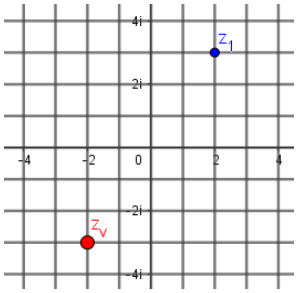
Obrázek 4.2: Grafické znázornění komplexně sdruženého čísla

Geometricky je **komplexně sdružené číslo** $\overline{z}$ obrazem daného Gaussova celého čísla $z = a + bi$ v osové souměrnosti podle reálné osy (osy x) v Gaussově rovině. Z toho vyplývá, že pokud je Gaussovo celé číslo reprezentováno bodem M$[a, b]$, tak komplexně sdružené číslo je reprezentováno zápisem M'$[a, -b]$. Grafickou interpretaci můžeme vidět na obrázku 4.2, kde vzor Gaussova celého čísla z_1 má modrou barvu a k němu komplexně sdružené číslo z_v má červenou barvu.

4.4 Opačné číslo

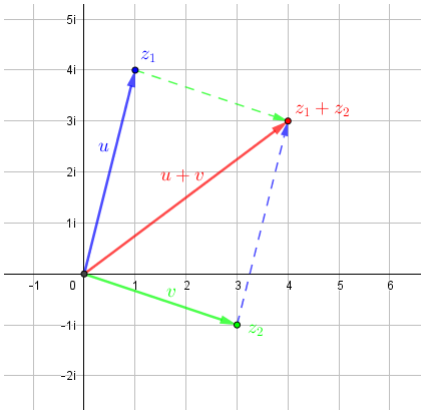
Geometrické znázornění opačného čísla $-z$ Gaussova celého čísla $z = a + bi$ je obraz M'$[-a, -b]$ vzoru M$[a, b]$. Jedná se o zobrazení Gaussova celého čísla z ve středové souměrnosti se středem v počátku $O = 0 + 0i$ Gaussovy roviny. Grafickou interpretaci můžeme vidět na obrázku 4.3, kde vzor Gaussova celého čísla z_1 je zvýrazněn modrou barvou a k němu opačné číslo z_v má červenou barvu.

Úloha 3. K procvičení geometrického znázornění komplexně sdruženého a opačného čísla ke Gaussovu celému číslu využijme **Applet č. 3**. Bližší popis daného appletu nalezneme v kapitole 7 s názvem Applety (přesněji 7.5.3).



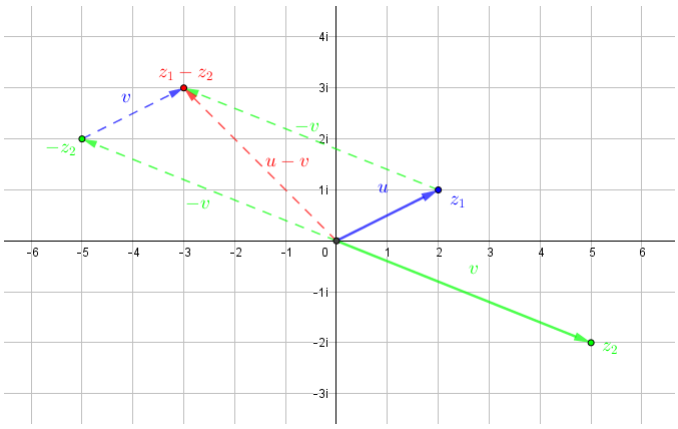
Obrázek 4.3: Grafické znázornění opačného čísla

4.5 Sčítání a odčítání Gaussových celých čísel



Obrázek 4.4: Sčítání dvou Gaussových celých čísel jako vektory

V předchozí kapitole jsme si řekli, jak algebraicky sčítáme dvě Gaussova celá čísla $z_1 + z_2$ (viz definice 3 (2.1)). Nyní se podíváme na operaci sčítání z pohledu grafické interpretace dvou Gaussovo celých čísel vyjádřených jako body (nebo vektory) komplexní roviny. Součet dvou Gaussových celých čísel $z_1 + z_2$ je dán pravidlem rovnoběžníku jako u sčítání dvou běžných vektorů. Úhlopříčka daného rovnoběžníku představuje výsledný vektor (řešení součtu). Grafické znázornění součtu dvou Gaussových čísel můžeme vidět na obrázku 4.4. [31]



Obrázek 4.5: Odčítání dvou Gaussových celých čísel jako vektory

Operaci odčítání dvou Gaussových celých čísel $z_1 - z_2$ můžeme převést na Gaussovo celé číslo z_1 a přičíst k němu opačné Gaussovo celé číslo $-z_2$: $z_1 + (-z_2)$. Jak řešíme součet dvou Gaussových celých čísel, jsme již popsali výše. Grafická interpretace rozdílu dvou Gaussových čísel můžeme vidět na obrázku 4.5.

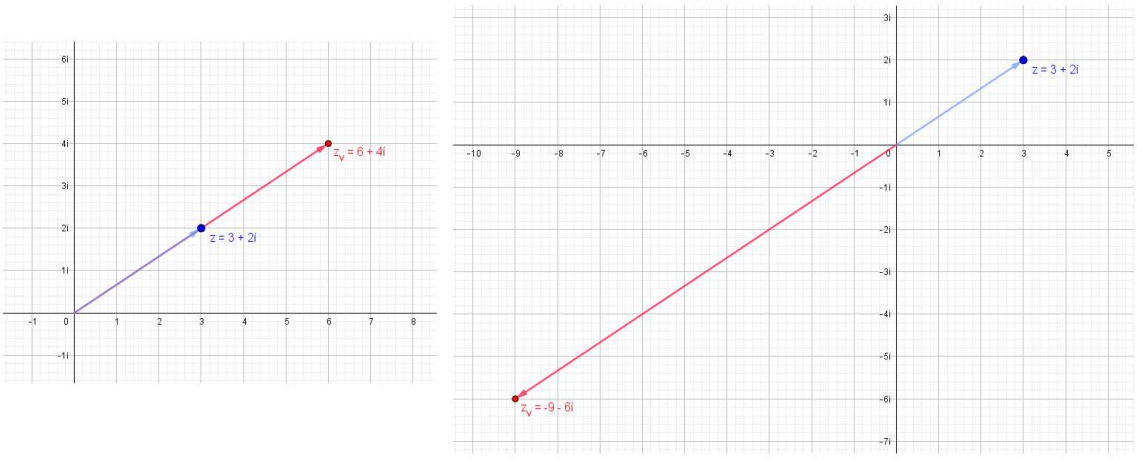
Úloha 4. Pro procvičení sčítání a odčítání Gaussových celých čísel interpretovaných geometricky v komplexní rovině využijme **Applet č. 4**. Bližší informace o daném appletu nalezneme v kapitole 7 s názvem Applety (přesněji 7.5.4).

4.6 Násobení Gaussových celých čísel

Početní řešení součinu dvou Gaussových celých čísel jsme již definovali v předchozí kapitole (viz definice 3 (2.2)). Nyní se zaměříme na tuto operaci z grafického pohledu. Tedy jak ovlivňuje vynásobení Gaussova celého čísla číslem celým, ryze imaginárním a Gaussovým celým.

4.6.1 Vynásobení Gaussova celého čísla číslem celým ($\mathbb{Z}$)

Pokud je Gaussovo celé číslo z vynásobeno celým[1] číslem c, délka vektoru z je vynásobena $|c|$ (absolutní hodnotou čísla c). Pokud je c kladné, směr vektoru cz je stejný jako směr vektoru z. V případě, že c je záporné, vektor cz má opačný směr než vektor z. Grafickou interpretaci součinu Gaussova celého čísla $z = 3+2i$ s celým kladným číslem 2 můžeme vidět na obrázku 4.6 (vlevo). Součinu Gaussova celého čísla $z = 3 + 2i$ s celým záporným číslem -3 lze vidět na obrázku 4.6 (vpravo). [3]



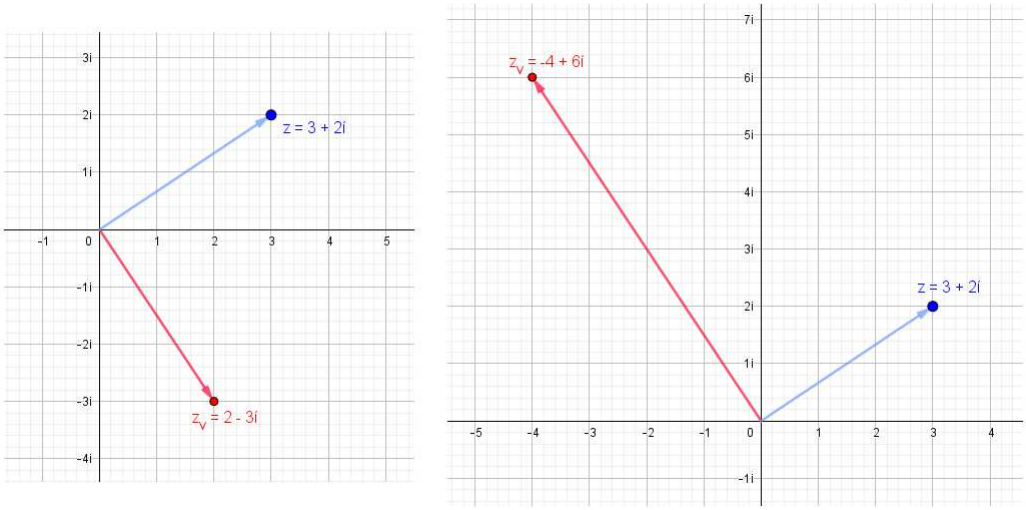
Obrázek 4.6: Násobení Gaussova celého čísla celým číslem

[1] Omezili jsme se pouze na násobení celým číslem z důvodu jednoduší interpretace v Gaussově rovině a přehlednějšího řešení. Jinak samozřejmě násobení reálným číslem funguje stejně jako násobení číslem celým.

4.6.2 Vynásobení Gaussova celého čísla číslem ryze imaginárním

Pokud vynásobíme Gaussovo celé číslo z imaginární jednotkou i, dostaneme vektor z otočený o 90° proti směru chodu hodinových ručiček beze změny délky vektoru.

V případě, že násobíme Gaussovo celé číslo z ryze imaginárním číslem bi, kde $b \in \mathbb{Z}$, dostaneme vektor z otočený o 90° proti směru chodu hodinových ručiček se změnou délky vektoru.[1] Geometrické znázornění součinu Gaussova celého čísla $z = 3 + 2i$ s ryze imaginárním číslem $-i$ můžeme vidět na obrázku 4.7 (vlevo). Součin Gaussova celého čísla $z = 3 + 2i$ s ryze imaginárním číslem $2i$ lze vidět na obrázku 4.7 (vpravo). [3]



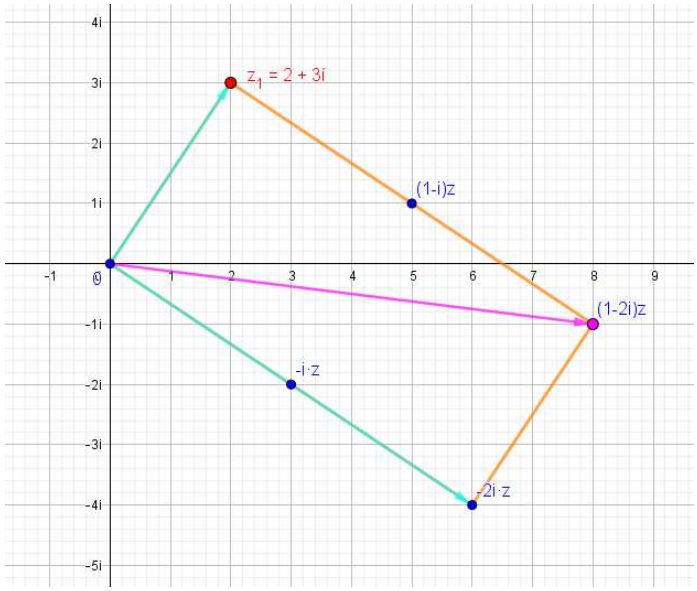
Obrázek 4.7: Násobení Gaussova celého čísla číslem ryze imaginárním

Grafické násobení Gaussova celého čísla celým (resp. ryze imaginárním) číslem můžeme ověřit (prozkoumat) pomocí **Appletu č. 5**. Bližší informace k danému appletu získáme v kapitole 7 s názvem Applety (přesněji 7.5.5).

4.6.3 Vynásobení Gaussova celého čísla Gaussovým celým číslem

Při vynásobení Gaussova celého čísla z_1 jiným Gaussovým celým číslem z_2, které má nenulovou reálnou i imaginární část, zjistíme výsledek tak, že rozdělíme násobení těchto čísel na dvě části. První část bude tvořit násobek čísla z_1 s reálnou částí z_2. Druhou částí pak bude násobek čísla z_1 s imaginární částí z_2. V komplexní rovině dostaneme dvě čísla, která když geometricky sečteme (viz 4.5) dostaneme výsledek součinu z_1 a z_2. Geometrickou interpretaci součinu Gaussova celého čísla $z_1 = 2 + 3i$ s Gaussovým celým číslem $z_2 = 1 - 2i$ můžeme vidět na obrázku 4.8, kde součin (výsledek) je zvýrazněn růžovou barvou.

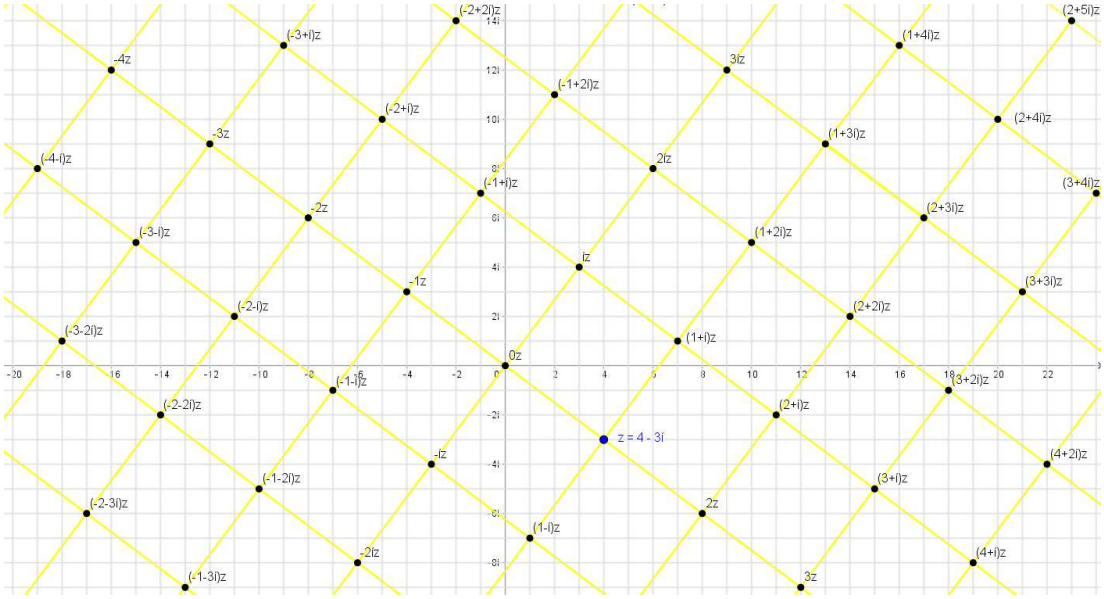
[1] Jestliže $b \in \mathbb{Z}$ je záporné, získáme vektor z otočený o 90° po směru chodu hodinových ručiček se změnou délky vektoru.



Obrázek 4.8: Násobení Gaussova celého čísla s Gaussovým celým číslem

Geometrické násobení Gaussova celého čísla s Gaussovým celým číslem lze vyzkoušet pomocí **Appletu č. 6**. Bližší informace k danému appletu získáme v kapitole 7 (přesněji 7.5.6).

Kdybychom vynásobili Gaussovo celé číslo $z = a + bi$ všemi Gaussovy celými čísly komplexní roviny, došlo by k vykreslení mřížové mapy. Ta ukazuje, jak se dostat z původního Gaussova celého čísla z k jakémukoliv násobku z. Násobky čísla z jsou ve vrcholech čtvercové mříže s délkou strany $|z|$.[1] Část mříže s násobky Gaussova celého čísla $z = 4 - 3i$ můžeme vidět na obrázku 4.9. [3]



Obrázek 4.9: Mříž s násobky Gaussova celého čísla

[1] Mříž (násobky Gaussova celého čísla $z = a + bi$) můžeme také získat otočením roviny souřadnic kolem počátku o úhel θ, kde $\tan(\theta) = \frac{b}{a}$, a následným zvětšením z počátku souřadnic s měřítkem $\sqrt{a^2 + b^2}$. [33]

Kapitola 5

Dělitelnost a dělení v komplexní rovině

V této kapitole budeme pomocí úloh odvozovat geometrickou interpretaci dělitelnosti, dělení Gaussových celých čísel se zbytkem a největší společný dělitel Gaussových celých čísel, které jsme teoreticky shrnuli v kapitole 2. Řešení úloh je doplněné o obrázky z autorových appletů.

5.1 Dělitelnost Gaussových celých čísel

Ve třech úlohách si ukážeme, jak jednoduše můžeme zjistit v Gaussově rovině, zda Gaussovo celé číslo $z = a+bi$ dělí (je dělitelem) Gaussovo celé číslo $z_2 = c+di$.

Úloha 5. Pomocí grafického znázornění rozhodněte, zda Gaussovo celé číslo $z = 3 - 2i$ dělí (je dělitelem) Gaussovo celé číslo $z_2 = -1 + 5i$.

Řešení. Nejprve zobrazíme Gaussova celá čísla v komplexní rovině. Následně Gaussovo celé číslo z vynásobíme celými, ryze imaginárními, případně Gaussovými celými čísly. Tím zjistíme celočíselné násobky čísla z. Jak už jsme si říkali v kapitole 4 v podkapitole Násobení Gaussových celých čísel (viz 4.6), tyto násobky tvoří vrcholy čtvercové mříže s délkou hrany

$$|z| = \sqrt{a^2 + b^2} = \sqrt{(3)^2 + (-2)^2} = \sqrt{13}.$$

Z kapitoly 2 a z definice 6 víme, že dělitelnost se vyjadřuje vztahem

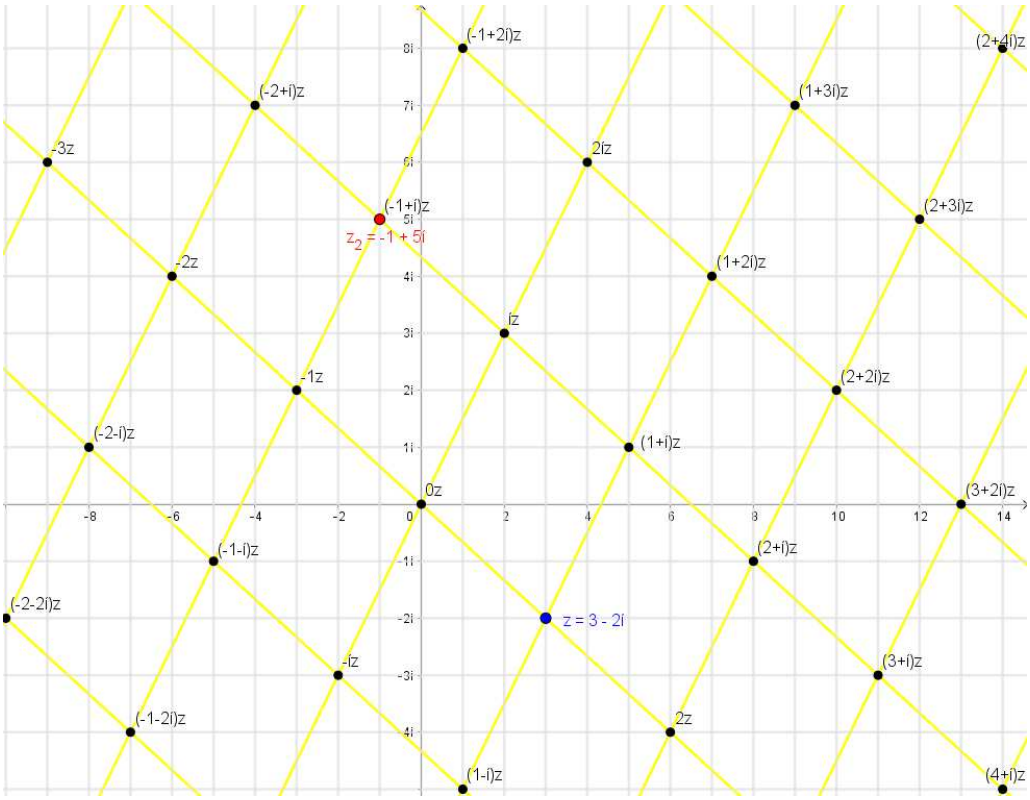
$$z_2 = k \cdot z.$$

Z toho vyplývá, že pokud splývá Gaussovo celé číslo z_2 s některým celočíselným násobkem Gaussova celého čísla z (neboli leží v některém vrcholu čtvercové mříže). Potom Gaussovo celé číslo z_2 je dělitelné Gaussovým celým číslem z. Grafické řešení můžeme vidět na obrázku 5.1, kde čtvercová mříž je zbarvena žlutě, Gaussovo celé číslo z je vykresleno modrou barvou, Gaussovo celé číslo z_2 červenou barvou a násobky Gaussova celého čísla z černou barvou.

Náš závěr si ověříme pomocí početního řešení

$$\frac{z_2}{z} = \frac{-1+5i}{3-2i} = \frac{-1+5i}{3-2i} \cdot \frac{3+2i}{3+2i} = \frac{-13+13i}{13} = -1+i.$$

Z numerického řešení je vidět, že výsledkem je Gaussovo celé číslo, a proto dělitelnost můžeme vyjádřit následovně: $-1+5i=(-1+i)(3-2i)$. Na obrázku 5.1 lze vidět, že Gaussovo celé číslo $-1+5i$ jsme vyjádřili stejným součinem (celočíselným násobkem čísla z).



Obrázek 5.1: Dělitelnost Gaussových celých čísel (a)

Úloha 6. Pomocí grafického znázornění rozhodněte, zda Gaussovo celé číslo $z=-3+2i$ dělí (je dělitelem) Gaussovo celé číslo $z_2=5+5i$.

Řešení. Budeme postupovat stejným způsobem jako v předchozí úloze 5. Zobrazíme Gaussova celá čísla v komplexní rovině a následně vykreslíme celočíselné násobky čísla z. Zobrazení dané situace můžeme vidět na obrázku 5.2.

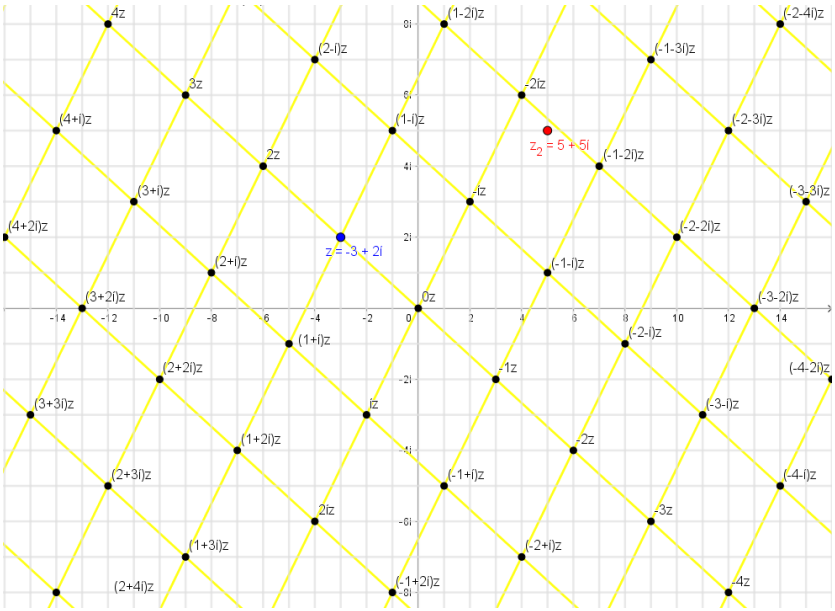
Zároveň si můžeme všimnout, že Gaussovo celé číslo z_2 neleží v žádném vrcholu (v celočíselném násobku čísla z) čtvercové mříže, a proto nejsme schopni dané číslo vyjádřit vztahem z definice 6 v kapitole 2

$$z_2 = k \cdot z.$$

Proto Gaussovo celé číslo z není dělitelem (nedělí) Gaussovo celé číslo z_2.
Nyní si ověříme náš závěr pomocí početního řešení.

$$\frac{z_2}{z}=\frac{5+5i}{-3+2i}=\frac{7+4i}{-3+2i}\cdot\frac{-3-2i}{-3-2i}=\frac{-5+-25i}{13}$$

Z numerického řešení vidíme, že výsledkem není Gaussovo celé číslo, protože reálná ani imaginární část není celé číslo (viz definice 1), a proto Gaussovo celé číslo z nedělí Gaussovo celé číslo z_2.

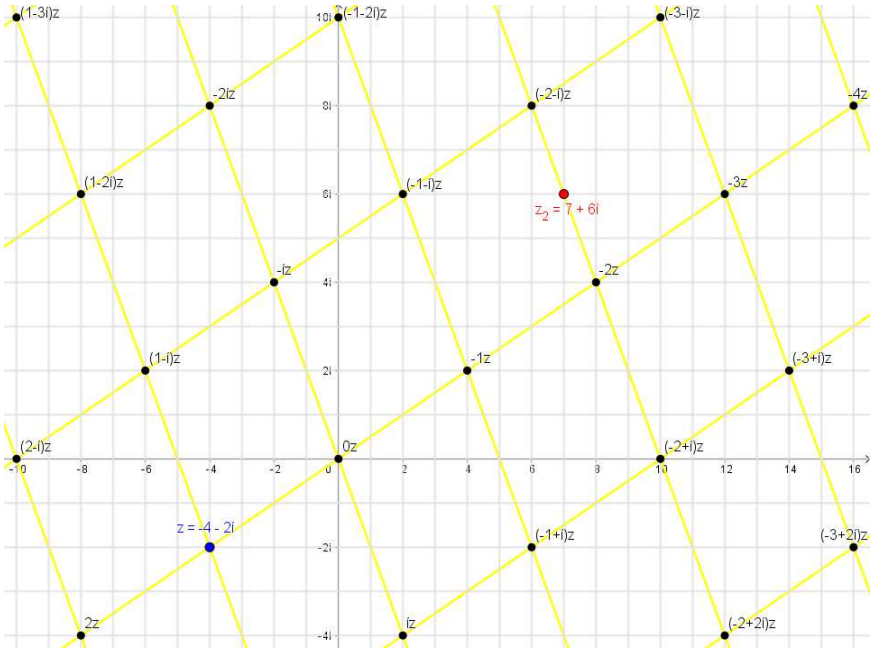


Obrázek 5.2: Dělitelnost Gaussových celých čísel (b)

Na závěr si ukážeme, jak je to s dělitelností dvou Gaussovo celých čísel, když Gaussovo celé číslo z_2 leží na hraně (ne ve vrcholu) žluté čtvercové mříže, která vznikla z celočíselných násobků čísla z.

Úloha 7. Pomocí grafického znázornění rozhodněte, zda Gaussovo celé číslo $z = -4 - 2i$ dělí Gaussovo celé číslo $z_2 = 7 + 6i$.

Řešení. Budeme řešit stejně jako v předchozích dvou úlohách. Vyobrazíme Gaussova celá čísla v komplexní rovině a následně znázorníme celočíselné násobky čísla z. Grafickou interpretaci lze vidět na obrázku 5.3.



Obrázek 5.3: Dělitelnost Gaussových celých čísel (c)

Z obrázku 5.3 je zřejmé, že Gaussovo celé číslo z_2 leží na hraně čtvercové mříže. Z toho důvodu nejsme schopni dané číslo vyjádřit vztahem z definice 6 v kapitole 2

$$z_2 = k \cdot z.$$

A tedy Gaussovo celé číslo z nedělí Gaussovo celé číslo z_2.
Náš závěr zkontrolujeme ještě početně.

$$\frac{z_2}{z} = \frac{7+6i}{-4-2i} = \frac{7+6i}{-4-2i} \cdot \frac{-4+2i}{-4+2i} = \frac{-40-10i}{20} = -2 - \frac{1}{2}i$$

Z početního řešení vidíme, že imaginární část Gaussova celého čísla není celé číslo, a proto Gaussovo celé číslo z nedělí Gaussovo celé číslo z_2.

Úloha 8. K procvičení dělitelnosti dvou Gaussových celých čísel z geometrického hlediska v komplexní rovině můžeme použít **Applet č. 7**. Bližší informace o daném appletu nalezneme v kapitole 7 s názvem Applety (přesněji 7.5.7).

5.2 Dělení Gaussových celých čísel se zbytkem

Již v některých řešených úlohách předchozí podkapitoly o dělitelnosti Gaussových celých čísel jsme si mohli všimnout, že operace dělení v $\mathbb{Z}[i]$ je pouze částečná. A tedy některá Gaussova celá čísla dělit nelze, např. Gaussovo celé číslo $z_2 = 10 + 4i$ nedělí Gaussovo celé číslo $z = -1 - 5i$. Proto jsme v kapitole 2 zavedli větu 8 o dělení se zbytkem, ve které máme dvě operace. Jedna operace dává podíl těchto čísel v $\mathbb{Z}[i]$ a druhou operací je ten zbytek ze $\mathbb{Z}[i]$. Nyní se podíváme na geometrickou interpretaci dělení dvou Gaussových celých čísel se zbytkem, které jsme uvedli jako příklad v odstavci výše.

Úloha 9. Určete grafickou interpretaci $\frac{z_2}{z}$ dvou Gaussových celých čísel $z = -1 - 5i$ a $z_2 = 10 + 4i$.

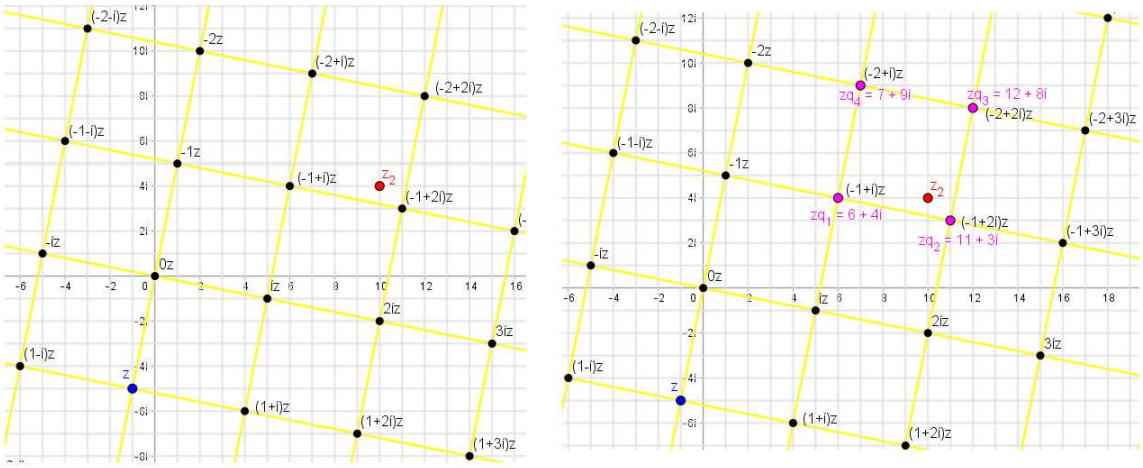
Řešení. Na začátku budeme úlohu řešit stejně jako úlohy uvedené u dělitelnosti v této kapitole. Nejprve zobrazíme Gaussova celá čísla v komplexní rovině. Následně Gaussovo celé číslo z vynásobíme celými, ryze imaginárními, případně Gaussovými celými čísly a získáme celočíselné násobky z, které tvoří vrcholy čtvercové mříže s délkou hrany

$$|z| = \sqrt{a^2 + b^2} = \sqrt{(-1)^2 + (-5)^2} = \sqrt{26}.$$

Gaussovo celé číslo z_2 se nachází v jednom z těchto čtverců čtvercové mříže. Následující znázornění můžeme vidět na obrázku 5.4 (vlevo), kde čtvercová mříž je zbarvena žlutě, Gaussovo celé číslo z je vykresleno modrou barvou a Gaussovo celé číslo z_2 červenou barvou.

Nyní hledáme, který z vrcholů (Gaussovy celočíselné násobky qz) tohoto čtverce je řešením vztahu $z_2 = qz + r$ z věty 8 v kapitole 2 tak, aby platilo, že

$$N(r) < N(z).$$



Obrázek 5.4: Dělení Gaussových celých čísel se zbytkem

Předpokládáme, že řešením jsou všechny vrcholy daného čtverce, a vypočteme jejich hodnoty (souřadnice těchto Gaussových celých čísel):

$$\begin{aligned} q_1 z &= (-1+i)z = (-1+i)(-1-5i) = 6+4i, \\ q_2 z &= (-1+2i)z = (-1+2i)(-1-5i) = 11+3i, \\ q_3 z &= (-2+2i)z = (-2+2i)(-1-5i) = 12+8i, \\ q_4 z &= (-2+i)z = (-2+i)(-1-5i) = 7+9i. \end{aligned}$$

Případně konkrétní hodnoty (souřadnice) vrcholů čtverce můžeme získat pomocí geometrické interpretace násobení Gaussovo celých čísel viz obrázek 5.4 (vpravo), které jsou zde zvýrazněny růžovou barvou.

Gaussovo celé číslo r získáme následovně $r = z_2 - qz$ (upravený dříve zmíněný vztah):

$$\begin{aligned} r_1 &= z_2 - q_1 z = 10+4i-(6+4i) = 4+0i, \\ r_2 &= z_2 - q_2 z = 10+4i-(11+3i) = -1+i, \\ r_3 &= z_2 - q_3 z = 10+4i-(12+8i) = -2-4i, \\ r_4 &= z_2 - q_4 z = 10+4i-(7+9i) = 3-5i. \end{aligned}$$

Nejprve vypočteme $N(z)$ a $N(r)$:

$$\begin{aligned} N(z) &= a^2+b^2 = (-1)^2+(-5)^2 = 26, \\ N(r_1) &= a^2+b^2 = (4)^2+(0)^2 = 16, \\ N(r_2) &= a^2+b^2 = (-1)^2+(1)^2 = 2, \\ N(r_3) &= a^2+b^2 = (-2)^2+(-4)^2 = 20, \\ N(r_4) &= a^2+b^2 = (7)^2+(9)^2 = 137. \end{aligned}$$

Nyní musíme zkontrolovat, že platí $N(r) < N(z)$.

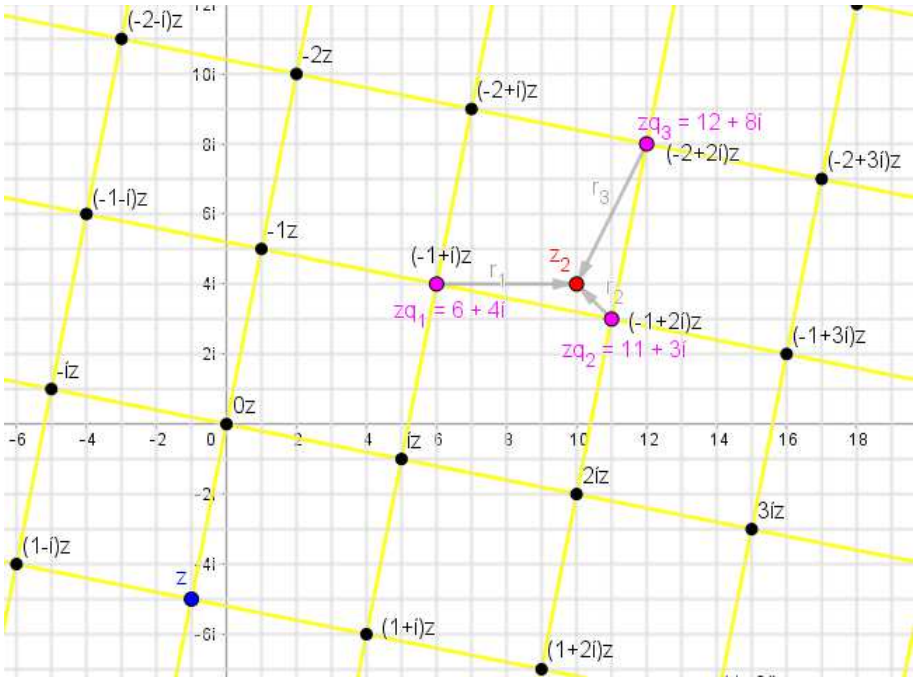
$$\begin{aligned} 16 &< 26, \\ 2 &< 26, \\ 20 &< 26, \\ 137 &< 26. \end{aligned}$$

Z toho vidíme, že poslední nerovnost neplatí, a proto $q_4 z$ nemůže být řešením daného příkladu.

Daná úloha má tedy 3 řešení, jejichž vztahy jsou následující:

$$10 + 4i = 6 + 4i + (4 + 0i),$$
$$10 + 4i = 11 + 3i + (-1 + i),$$
$$10 + 4i = 12 + 8i + (-2 - 4i).$$

Grafickou interpretaci řešení lze vidět na obrázku 5.5



Obrázek 5.5: Dělení Gaussových celých čísel se zbytkem (řešení)

5.3 Počet řešení pro dvojici (q,r) při dělení Gaussových celých čísel se zbytkem

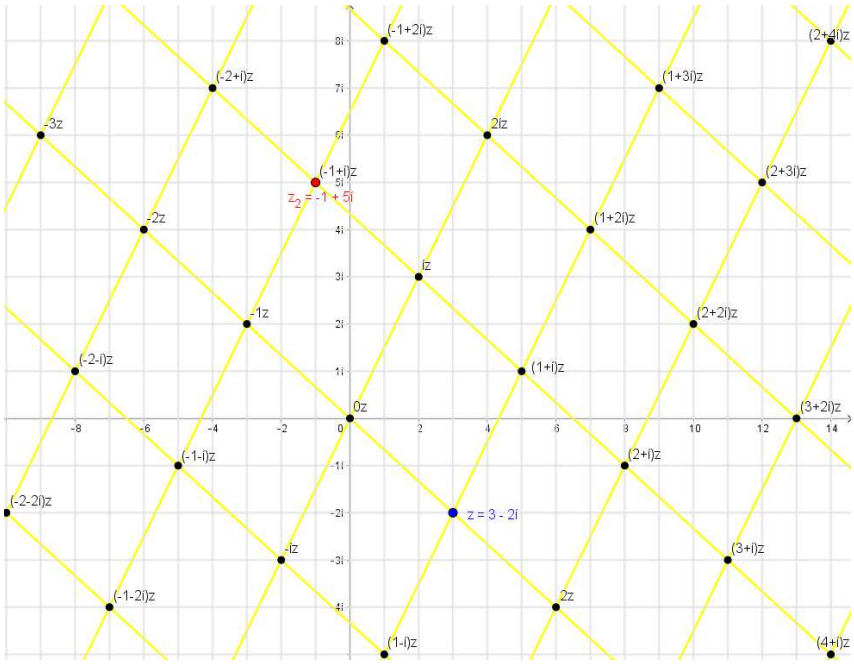
Z předchozích úloh na dělitelnost a dělení se zbytkem docházíme k závěru: *„V závislosti na poloze mřížového bodu z_2, který leží v rámci jednoho čtverce, který je součástí čtvercové mříže, jež vznikla jako násobky Gaussova celého čísla z, může existovat **jedno**, **dvě**, **tři**, nebo **čtyři řešení pro dvojici (q,r)**, která vyhovuje větě 8 o dělení se zbytkem, kterou jsme uváděli v kapitole 2.“*

Poznámka. Abychom nemuseli počítat, který zbytek r splňuje podmínku

$$N(r) < N(z) \tag{5.1}$$

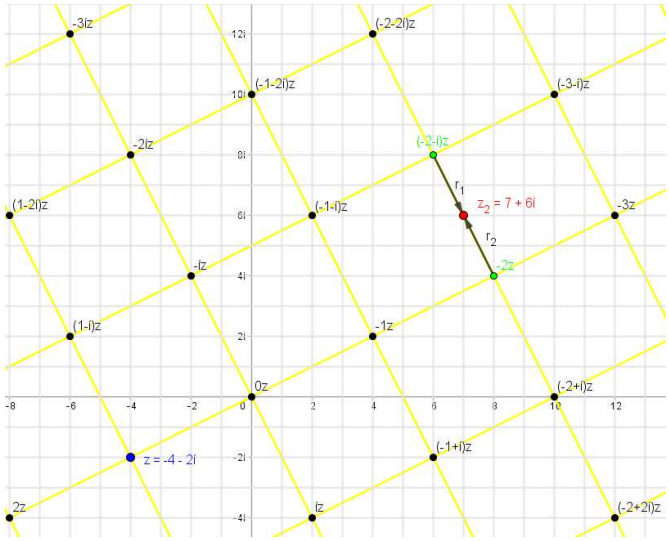
uvedenou ve větě 8 o dělení se zbytkem, využijeme geometrického řešení. Nejprve sestrojíme kružnici se středem v bodě z_2 a poloměrem $|z|$ a následně zjistíme z grafického znázornění, které vrcholy čtverce čtvercové mříže vyhovují podmínce (5.1). Danou kružnici budeme využívat v případě potřeby v následujících příkladech. Kružnici budeme značit k a bude oranžově znázorněna.

Nyní se na jednotlivé případy více podíváme. Pokud z_2 leží v jednom z vrcholů čtverce čtvercové mříže (žlutě zvýrazněná na obrázku 5.6), potom má věta 8 o dělení se zbytkem pouze jedno řešení pro dvojici (q,r) a $r = 0+0i$. Danou situaci můžeme vidět na obrázku 5.6. S řešenou úlohu jsme se mohli setkat v podkapitole 5.1 (přesněji úloha 5).

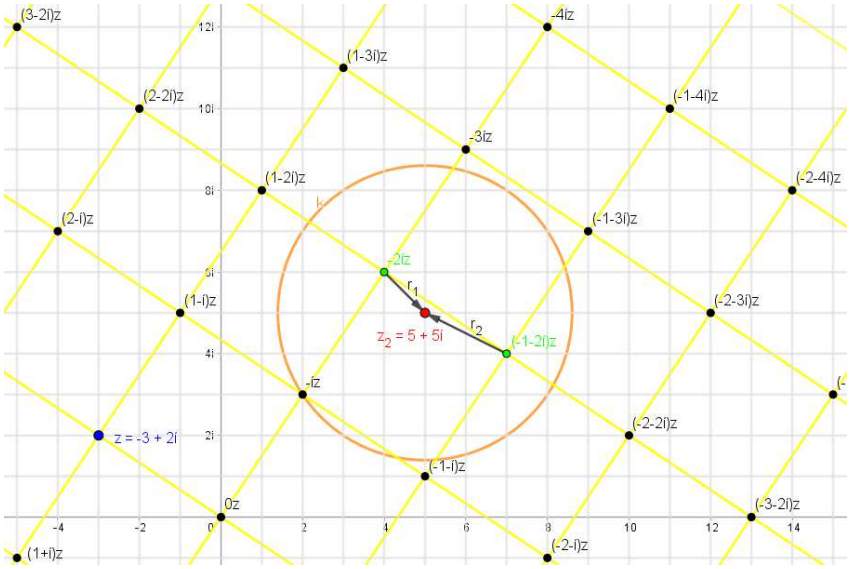


Obrázek 5.6: 1 řešení pro dvojici (q,r)

V případě, že z_2 leží na jedné hraně čtverce čtvercové mříže (viz obrázek 5.7) nebo z_2 leží uvnitř čtverce tak, že po sestrojení kružnice k pouze dva násobky čísla z (zeleně zvýrazněny v obrázku 5.8)a tedy jejich zbytky r splňují nerovnost (5.1)z věty 8 o dělení se zbytkem (viz obrázek 5.8), potom nalezneme dvě řešení pro dvojici (q,r).

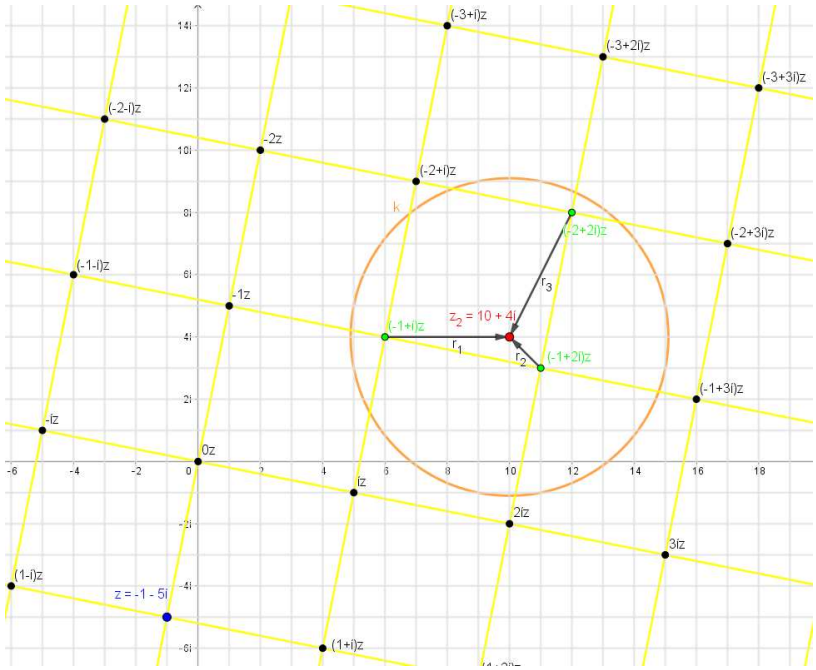


Obrázek 5.7: 2 řešení pro dvojici (q,r) (a)



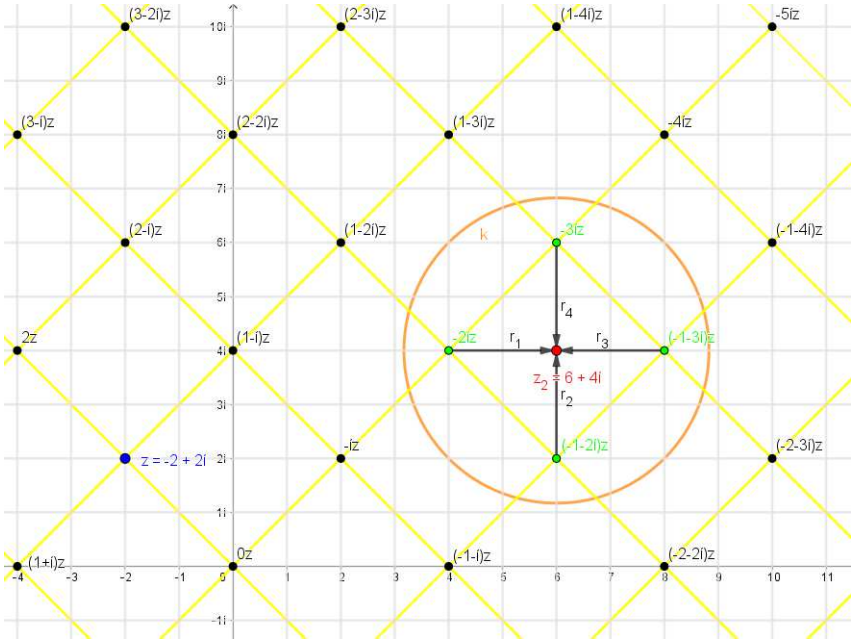
Obrázek 5.8: 2 řešení pro dvojici (q,r) (b)

Jestliže z_2 leží uvnitř čtverce čtvercové mříže tak, že po sestrojení kružnice k pouze tři násobky čísla z (zeleně zvýrazněny v obrázku 5.9) a tedy jejich zbytky r splňují nerovnost (5.1) z věty 8 o dělení se zbytkem, potom lze nalézt tři řešení pro dvojici (q,r). S řešenou úlohu jsme se mohli setkat v podkapitole 5.2 (přesněji úloha 9).



Obrázek 5.9: 3 řešení pro dvojici (q,r)

Pokud z_2 leží v průsečíku úhlopříček čtverce čtvercové mříže, potom jsme schopni nalézt 4 řešení pro dvojici (q,r), které splňují větu 8 o dělení se zbytkem. Danou situaci můžeme vidět na obrázku 5.10.



Obrázek 5.10: 4 řešení pro dvojici (q,r)

Pro další geometrickou interpretaci dělení dvou Gaussových celých čísel se zbytkem můžeme využít **Applet č. 8**. Bližší informace k danému appletu získáme v kapitole 7 s názvem Applety (přesněji 7.5.8).

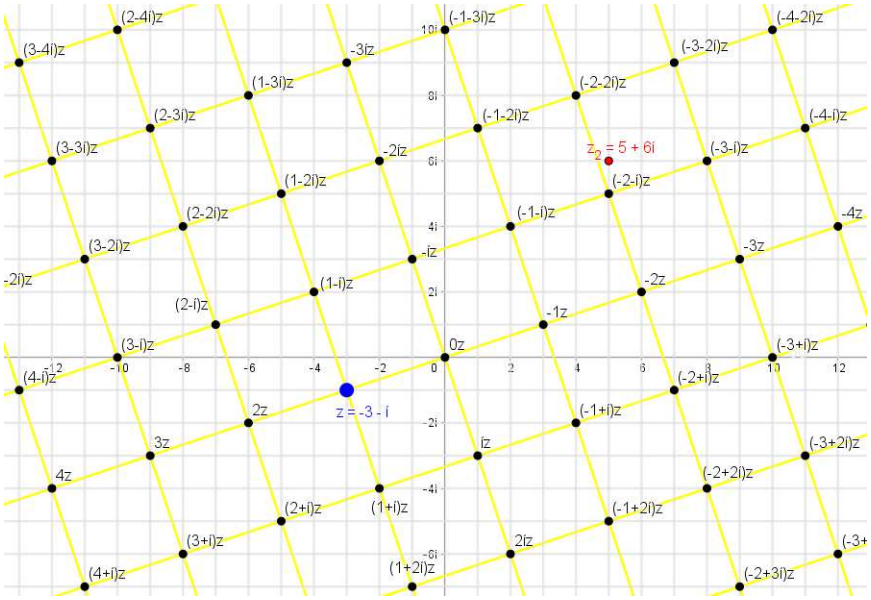
5.4 Největší společný dělitel Gaussových celých čísel

Již v kapitole 2 jsme uváděli větu 10 o Euklidově algoritmu, pomocí kterého dokážeme nalézt největší společný dělitel dvou Gaussových celých nenulových čísel. Grafické znázornění a aplikaci daného algoritmu si ukážeme na konkrétní úloze.

Úloha 10. Mějme Gaussova celá čísla $z = -3 - i$ a $z_2 = 5 + 6i$, pro která platí, že z dělí z_2. Určete největšího společného dělitele (NSD) těchto dvou čísel v komplexní rovině.

Řešení. Nejprve vyobrazíme Gaussova celá čísla z a z_2 v Gaussovo rovině. Následně znázorníme násobky Gaussova celého čísla z jako u předchozích úloh, které vytvoří čtvercovou mříž (žlutě zvýrazněno na obrázku 5.11). Hrana čtverců má délku

$$|z| = \sqrt{a^2 + b^2} = \sqrt{(3)^2 + (-1)^2} = \sqrt{10}.$$

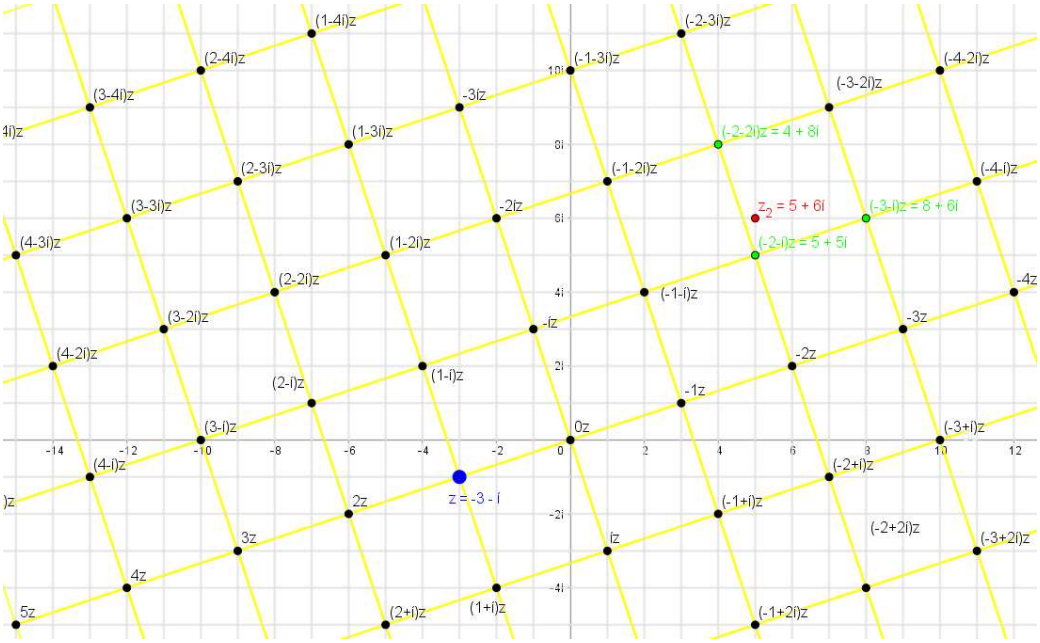


Obrázek 5.11: Největší společný dělitel (1)

Z obrázků 5.11 je patrné, že Gaussovo celé číslo z_2 se zobrazilo do jednoho ze čtverců žluté čtvercové mříže.

Z úlohy 9 a z věty 8 z kapitoly 2 již víme, že musí platit následující vztah $z_2 = qz + r$ s touto podmínkou

$$N(r) < N(z). \tag{5.2}$$



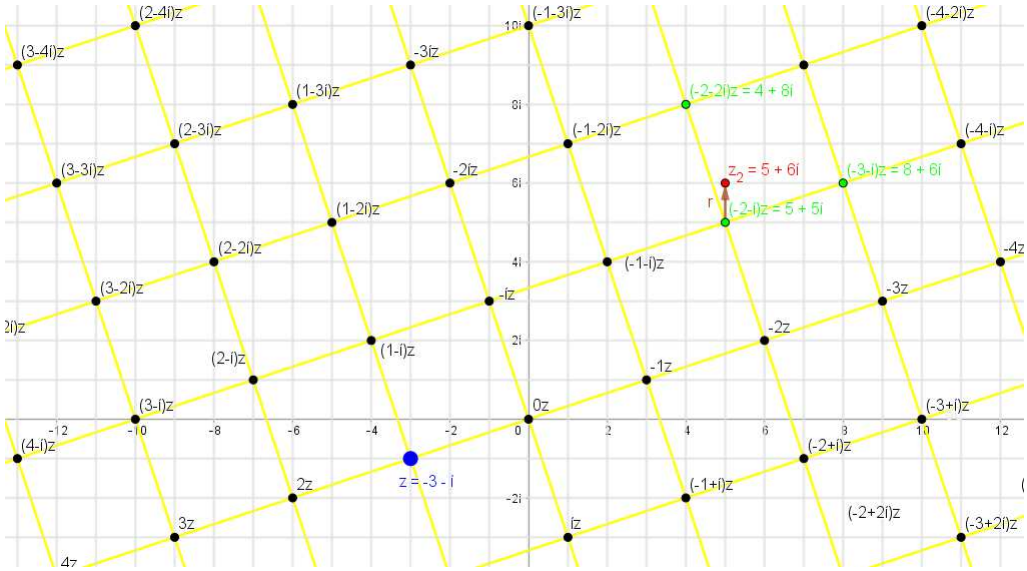
Obrázek 5.12: Největší společný dělitel (2)

Z grafického znázornění 5.12 vidíme, že pouze tři body splňují podmínku (5.2) (zeleně zvýrazněny). Jak jsme uváděli v poznámce podkapitoly 2.5 o **Euklidově algoritmu**, při hledání největšího společné dělitele Gaussových celých čísel se budeme snažit vzít násobek z takový, aby zbytek r měl co nejmenší normu (pokud

to budeme možné). Vidíme, že v tomto případě to lze. Proto vybereme zeleně zvýrazněný bod $qz = (-2 - i)z$ a dostáváme

$$5 + 6i = (-2 - i)(-3 - i) + (0 + i), \qquad 1 < 10$$

Ze vztahu dostáváme zbytek $r = 0 + i$, jenž je graficky vyobrazen na 5.13.

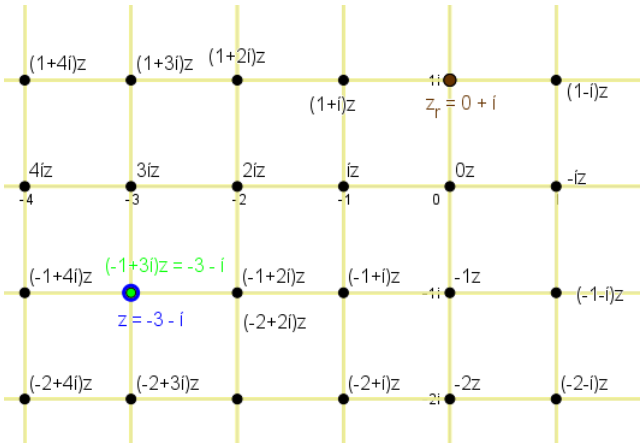


Obrázek 5.13: Největší společný dělitel (3)

Nyní budeme znovu aplikovat větu 8 z kapitoly 2, protože z věty 10 víme, že Euklidův algoritmus provádíme do té doby, než získáme nulový zbytek. Na obrázku 5.14 jsou vyobrazeny násobky čísla r a zároveň vidíme, že bod z leží ve vrcholu násobku r (tj. $q_1 r = (-1 + 3i)r$)[1] čtvercové mříže. Proto dostáváme

$$-3 - i = (-1 + 3i)(0 + i) + (0 + 0i), \qquad 0 < 1,$$

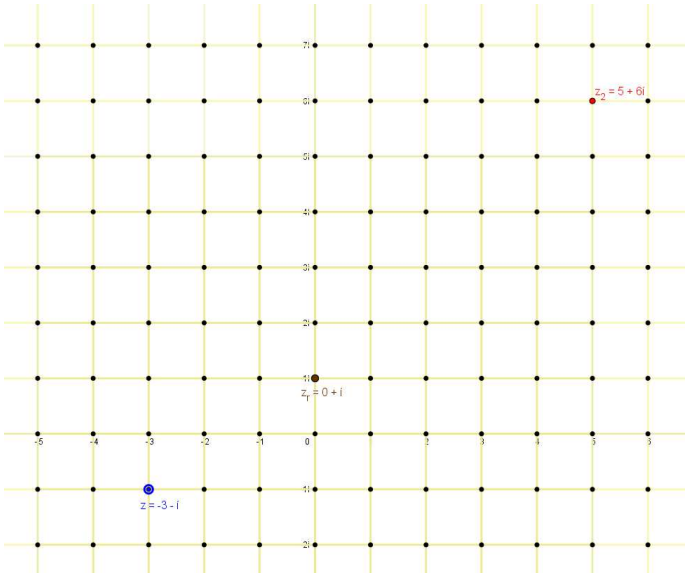
a tedy NSD(z, z_2)$= 0 + i$.



Obrázek 5.14: Největší společný dělitel (4)

[1] V obrázku 5.14 je u zeleného bodu $(-1 + 3i)z$, protože GeoGebra neumožňuje zástupný symbol, proto je použito univerzálně z.

Z obrázku 5.15 je zřejmé, že Gaussova celá čísla z a z_2 leží v mřížových bodech čtvercové sítě, která vznikla jako násobky čísla r. A tedy potvrzují náš výsledek největšího společného dělitele těchto čísel



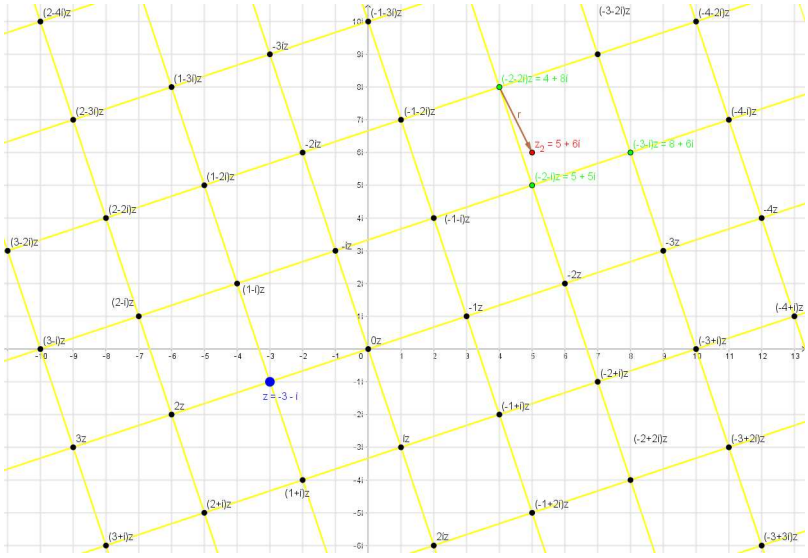
Obrázek 5.15: Největší společný dělitel (5)

Nyní se v této úloze vrátíme do první části řešení, kdy jsme jasně řekli, který násobek Gaussova celého čísla z vybereme ($qz = (-2 - i)z$). A nyní zvolíme násobek čísla z takový, že zbytek r nebudeme mít nejmenší normu, abychom zjistili, jaký vliv to má na výsledek úlohy.

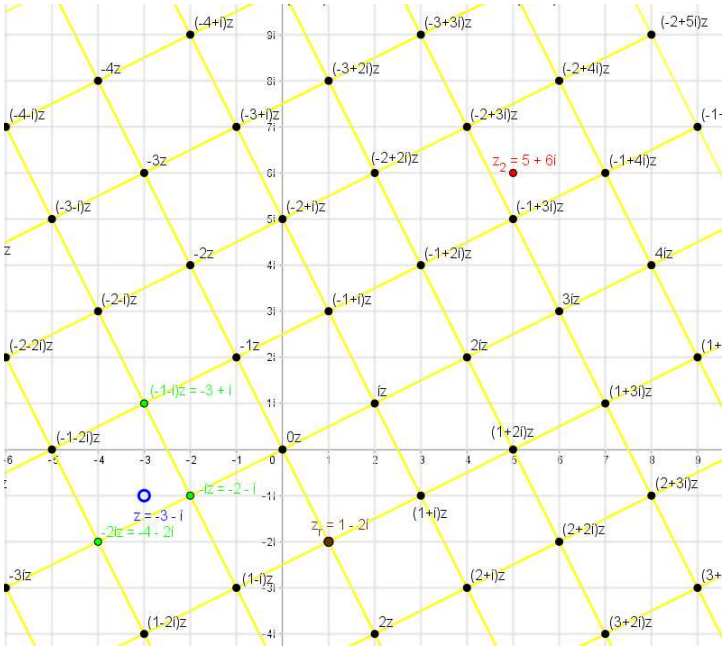
Vybereme si např. $qz = (-2 - 2i)z$ (viz obrázek 5.12). Tím získáme

$$5 + 6i = (-2 - 2i)(-3 - i) + (1 - 2i), \qquad 5 < 10$$

Vidíme, že zbytek je $r = 1 - 2i$ (viz obrázek 5.16).



Obrázek 5.16: Největší společný dělitel (6)



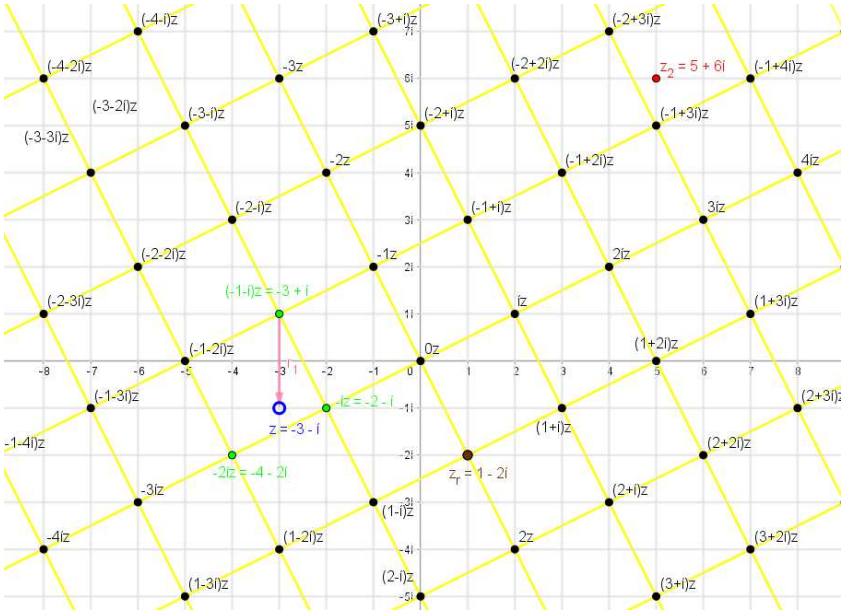
Obrázek 5.17: Největší společný dělitel (7)

Z prvního postupu víme, že Euklidův algoritmus aplikujeme tak dlouho, dokud nedostaneme nulový zbytek. Po zobrazení násobků $r = 1 - 2i$ (viz obrázek 5.17) zjišťujeme, že číslo z leží ve čtverci čtvercové mříže a zároveň dostáváme nové zelené body, které splňují podmínku $N(r_1) < N(r)$.

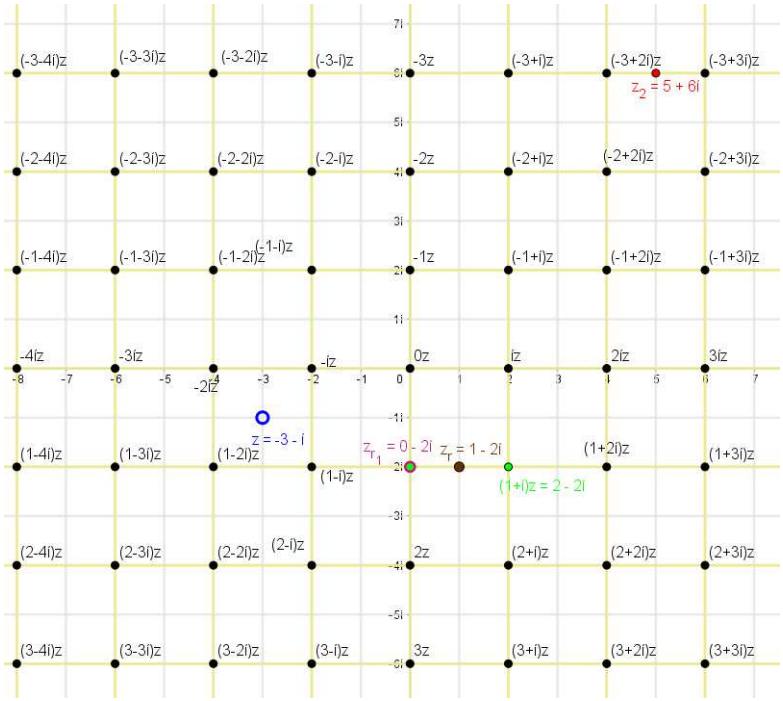
Znovu náhodně volíme například $q_1 r = (-1 - i)r$ a dostáváme

$$-3 - i = (-1 - i)(1 - 2i) + (0 - 2i), \qquad 4 < 5.$$

Ze vztahu vidíme, že zbytek $r_1 = 0 - 2i$ (viz obrázek 5.18).



Obrázek 5.18: Největší společný dělitel (8)

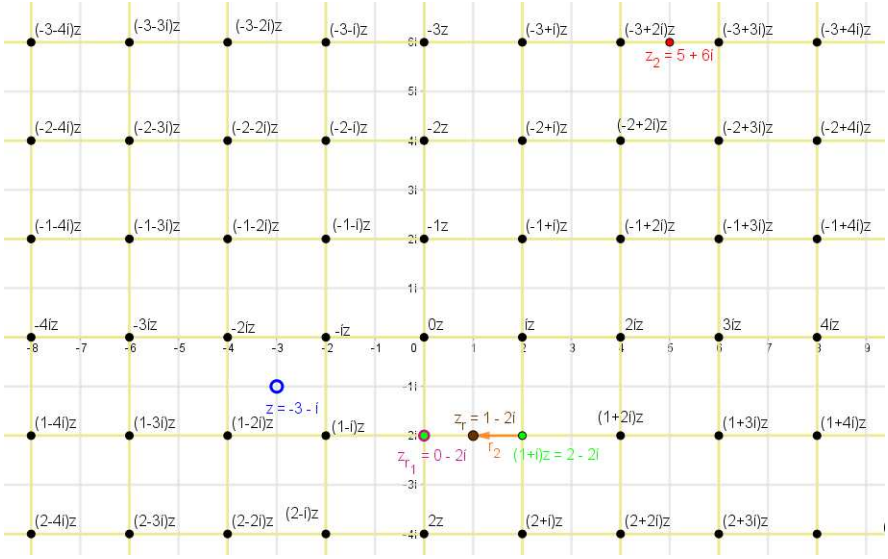


Obrázek 5.19: Největší společný dělitel (9)

Po vyobrazení násobků r_1 je z obrázku 5.19 zřejmé, že si můžeme vybrat ze dvou zelených bodů. Naší volbou nyní bude $q_2 r_1 = (-2 - i)r$ a dostaneme

$$1 - 2i = (1 + i)(0 - 2i) + (-1 + 0i), \qquad 1 < 4.$$

Ze vztahu získáváme zbytek $r_2 = -1 + 0i$ (viz obrázek 5.20).



Obrázek 5.20: Největší společný dělitel (10)

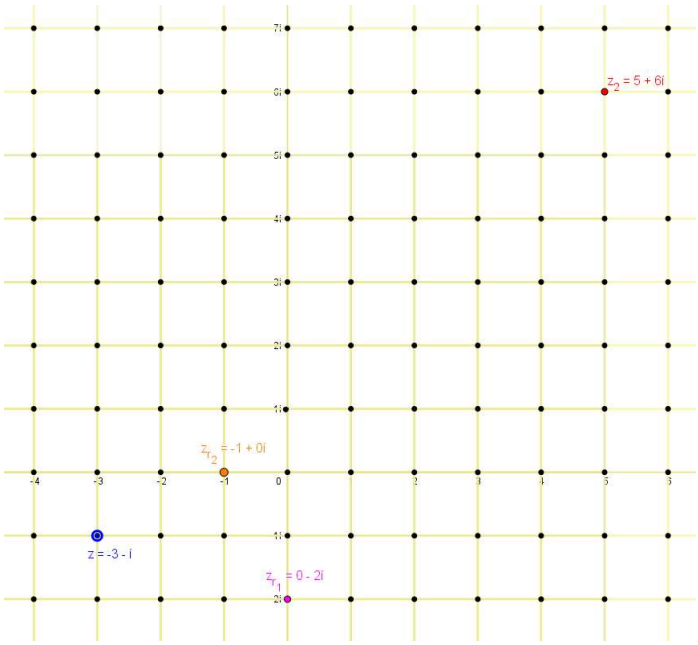
Následně vyobrazíme v komplexní rovině násobky r_2 a z obrázku 5.21 zjistíme, že bod r_1 leží ve vrcholu čtvercové mříže, a proto

$$0 - 2i = (0 + 2i)(-1 + 0i) + (0 + 0i), \qquad 0 < 1.$$

Tudíž NSD(z, z_2)$= -1 + 0i$. Proto Gaussova celá čísla z a z_2 leží ve vrcholech čtvercové sítě (žlutá), která vznikla jako násobky čísla r_2.

Nyní se podíváme na NSD_1 získaný prvním způsobem a na NSD_2 získaný druhým způsobem. Vidíme, že $NSD_1(z, z_2) = 0+i$ a $NSD_2(z, z_2) = -1+0i$ nejsou stejné, neboli liší se o násobek jednotky, což už jsme uvedli v podkapitole 2.5 v důsledku **Euklidova algoritmu**, a proto největší společný dělitel Gaussových celých čísel je určen jednoznačně až na násobek jednotky.

Z věty 12 v kapitole 2 víme, že Gaussova celá čísla z a z_2 jsou čísla nesoudělná (viz definice 10 v kapitole 2).



Obrázek 5.21: Největší společný dělitel (11)

Poznámka. Volba násobků čísla z a zbytku r má vliv na to, který výsledek vyjde z asociované čtveřice největšího společného dělitele Gaussových celých čísel, ale také na počet kroků v Euklidově algoritmu. Pokud volíme zbytky r s nejmenší normou, potom je nejméně kroků v Euklidově algoritmu.

Dané tvrzení si můžeme vyzkoušet pomocí **Applet č. 9**. Bližší informace k danému appletu získáme v kapitole 7 s názvem Applety (přesněji 7.5.9).

Kapitola 6

Prvočísla a rozklad v Gaussově rovině

Do této kapitoly jsme spojili téma prvočísel a případný rozklad složených Gaussových celých čísel z pohledu geometrického znázornění. Toto spojení je záměrné, protože pokud zjistíme, že se nejedná o Gaussovo prvočíslo, budeme hledat rozklad tohoto čísla. Určování, zda se jedná o Gaussovo prvočíslo nebo ne, si ukážeme v několika úlohách, u kterých uvedeme podrobný popis řešení doplněné o obrázky z Gaussovo roviny, které byly pořízeny z autorových appletů.

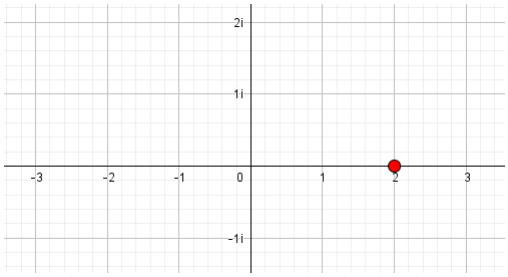
6.1 Přirozená čísla

Nejprve se ptáme, zda platí: *„Pokud máme přirozené prvočíslo (v* $\mathbb{N}$*), tak potom je toto číslo automaticky Gaussovým prvočíslem (prvočíslem v* $\mathbb{Z}[i]$*)?“*

Číslo 0 nebudeme geometricky demonstrovat, protože je zřejmé, že toto číslo nesplňuje podmínku v definici 13 z kapitoly 3. Ani číslo 1 nebudeme řešit grafickou formou, jelikož víme, že určitě nesplňuje podmínku uvedenou ve stejné definici, kterou jsme uváděli u čísla 0, tj. 13. A zároveň lze říci, že nesplňují další definice 11 a 12 ze stejné kapitoly.

Úloha 11. Rozhodněte, zda přirozené prvočíslo 2 je Gaussovým prvočíslem. Pokud není prvočíslem v $\mathbb{Z}[i]$, určete rozklad činitelů tohoto čísla.

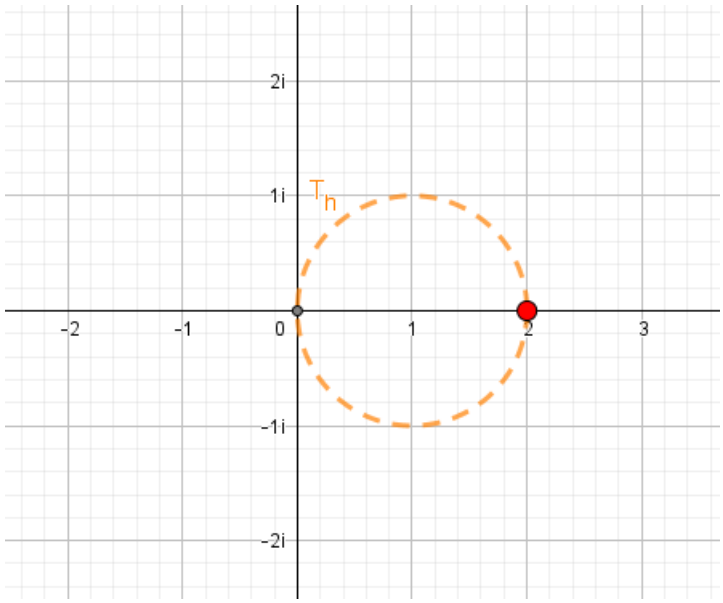
Řešení. Ze zadání je zřejmé, že číslo 2 je reálné Gaussovo celé číslo, protože imaginární část tohoto čísla je rovna 0. Znázornění tohoto čísla v komplexní rovině můžeme vidět na obrázku 6.1, kde je zvýrazněno červenou barvou.



Obrázek 6.1: Prvočíselný rozklad čísla 2 (a)

Při řešení vycházíme z věty 27 o reálných Gaussových prvočíslech, ze které víme, že Gaussovo prvočíslo nelze vyjádřit součtem dvou čtverců. Budeme předpokládat, že číslo 2 není Gaussovo prvočíslo, a proto jej lze vyjádřit vztahem uvedeném u věty výše. Z geometrie známe Pythagorovu větu[1], která vyjadřuje právě daný vztah.

Řekneme, že přeponou bude vzdálenost bodu (čísla 2) od počátku v komplexní rovině (neboli absolutní hodnota Gaussova celého čísla 2). Potřebujeme zjistit, jestli lze najít odvěsny, které by splňovaly tuto rovnost. Aby platila Pythagorova věta a mohli jsme hledat odvěsny, potřebujeme pravoúhlý trojúhelník, ten dokážeme nalézt pomocí Thaletovy kružnice[2]. Jejího zobrazení v komplexní rovině si lze všimnout na obrázku 6.2.



Obrázek 6.2: Prvočíselný rozklad čísla 2 (b)

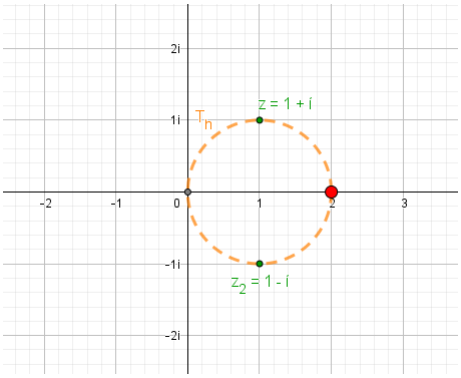
Nyní je otázkou, které body z této kružnice můžeme využít při rozkladu čísla 2, abychom získali součin činitelů ze $\mathbb{Z}[i]$. Jinými slovy potřebujeme dostat následující vztah

$$z = a^2 + b^2 = (a + bi)(a - bi).$$

Z toho vidíme, že hledáme body (Gaussova celá čísla), které mají celočíselné souřadnice, a tedy jsou mřížovými body. Když se podíváme na obrázek 6.3, vidíme, že pouze dva body $z = 1 + i$ a $z_2 = 1 - i$ (zvýrazněné zeleně) leží na Thaletově kružnici a zároveň jsou mřížovými body. Tato dvě Gaussova celá čísla z a z_2 jsou navzájem komplexně sdružená Gaussova celá čísla (viz 4.3), a proto se omezíme pouze na I. kvadrant komplexní roviny.

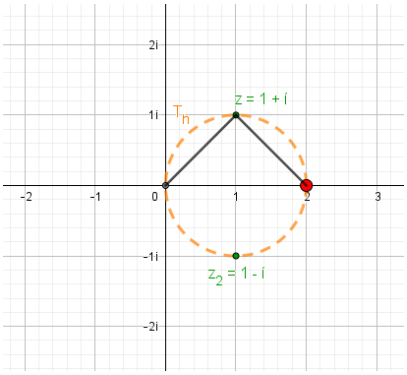
[1] **Pythagorova věta:** „Obsah čtverce sestrojeného nad přeponou pravoúhlého trojúhelníku je roven součtu obsahu čtverců sestrojených nad oběma jeho odvěsnami.“ [34]

[2] **Thaletova věta:** *„Všechny trojúhelníky, jejichž střed kružnice opsané půlí nejdelší stranu, jsou pravoúhlé.“*
Jiné znění: *„Sestrojíme-li libovolnou kružnici s průměrem. Koncové body jejího průměru označíme A a B a zvolíme libovolný bod C na kružnici. Pak platí, že trojúhelník ABC je pravoúhlý a má pravý úhel u vrcholu C.“*
Kružnice, která vznikne při konstrukci Thaletovy věty, bývá označována jako **Thaletova kružnice**. [35] [36]



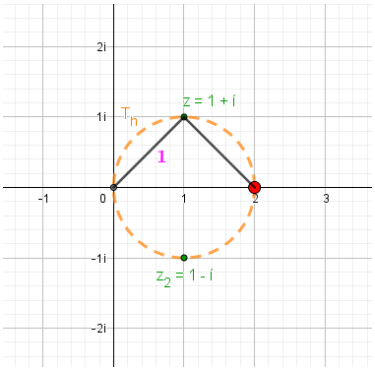
Obrázek 6.3: Prvočíselný rozklad čísla 2 (c)

Pokud propojíme jednotlivé body, získáme pravoúhlý trojúhelník s vrcholy 2, $z = 1 + i$ a 0 (viz obrázek 6.4).



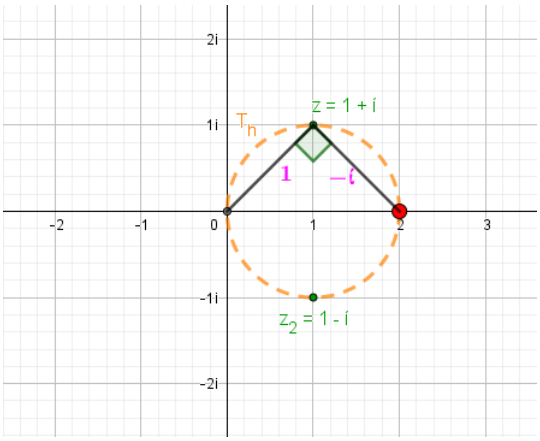
Obrázek 6.4: Prvočíselný rozklad čísla 2 (d)

Z počátku Gaussovy roviny se dostaneme do Gaussova celého čísla z vynásobením Gaussova celého čísla z číslem 1 (viz obrázek 6.5).



Obrázek 6.5: Prvočíselný rozklad čísla 2 (e)

Nyní jsme v bodě z a potřebovali bychom skončit v čísle 2. Z obrázku 6.6 si můžeme všimnout, že u bodu (vrcholu trojúhelníka) z je pravý úhel. Z násobení Gaussových celých čísel známe (viz 4.6.2), že otočení o 90° v komplexní rovině získáme vynásobením čísla číslem $-i$. Proto se z bodu z do čísla 2 dostaneme součinem $-i \cdot z$.



Obrázek 6.6: Prvočíselný rozklad čísla 2 (f)

Dále víme, že násobení dvou Gaussových celých čísel můžeme rozložit na dva případy (vynásobení Gaussova celého čísla reálnou částí druhého Gaussova celého čísla a vynásobení Gaussova celého čísla imaginární částí druhého Gaussova celého čísla) a následně dané výsledky geometricky sečteme (viz 4.6.3).

Z předchozích informací se dostáváme k závěru, že číslo 2 lze zapsat pomocí součinu dvou Gaussových celých čísel

$$2 = (1 + i)(1 - i), \tag{6.1}$$

tudíž dané číslo není Gaussovým prvočíslem. Ze 6.1 je zřejmé, že se jedná o součin dvou komplexně sdružených Gaussových celých čísel, a proto se nebudeme zabývat bodem (číslem) $z_2 = 1 - i$, protože výsledek by byl stejný jako ten, který jsme již uvedli.

Navíc tvrdíme, že (6.1) je prvočíselným rozkladem čísla 2 v $\mathbb{Z}[i]$ a neexistuje žádný další způsob rozkladu daného čísla. Ověření, že Gaussovo celé číslo $1 + i$ (případně $1 - i$) je Gaussovým prvočíslem, si ukážeme v rámci úlohy 14.

Řešení dané úlohy si můžeme projít pomocí **Appletu č. 13**, ve kterém je použitá kroková konstrukce. Bližší informace o daném appletu nalezneme v kapitole 7 s názvem Applety (přesněji 7.5.13).

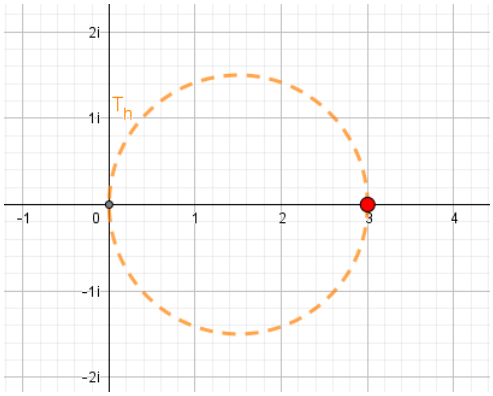
Úloha 12. Rozhodněte, zda přirozené prvočíslo 3 je Gaussovým prvočíslem. Pokud není prvočíslem v $\mathbb{Z}[i]$, určete rozklad činitelů tohoto čísla.

Řešení. Při řešení budeme postupovat stejným způsobem jako u úlohy 11. Nejprve zobrazíme reálné Gaussovo celé číslo v Gaussově rovině. Následně sestrojíme Thaletovu kružnici, která prochází bodem (číslem) 3 a počátkem komplexní roviny (viz obrázek 6.7).

Z obrázku 6.7 je vidět, že daná kružnice neprotíná žádné další mřížové body (pouze počátek 0 a číslo 3), a proto nedokážeme nalézt žádný pravoúhlý trojúhelník s vrcholem na Thaletově kružnici a celočíselnými souřadnicemi. Kvůli tomu nemůžeme číslo 3 vyjádřit pomocí vztahu z věty 27

$$z = a^2 + b^2 = (a + bi)(a - bi).$$

Z toho důvodu je číslo 3 Gaussovým prvočíslem.



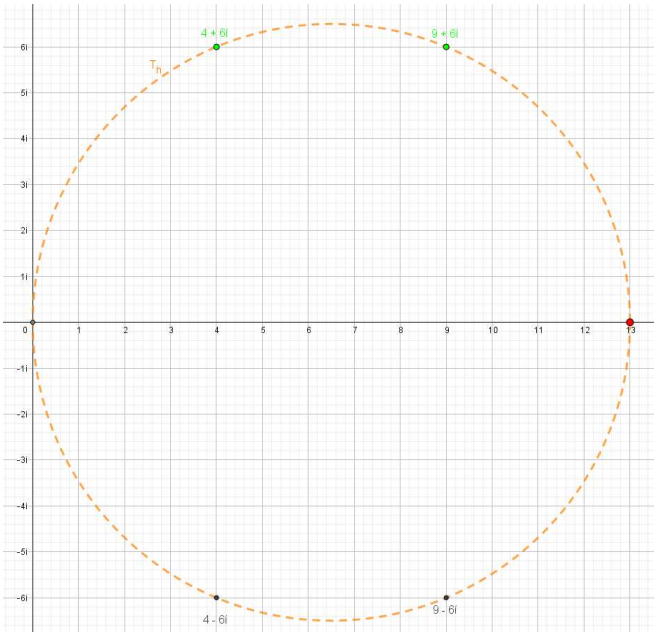
Obrázek 6.7: Přirozené prvočíslo 3 v komplexní rovině

Řešení daného úlohy si lze projít pomocí **Appletu č. 14**, ve kterém je použitá kroková konstrukce. Bližší informace o daném appletu nalezneme v kapitole 7 s názvem Applety (přesněji 7.5.14).

Úloha 13. Rozhodněte, zda přirozené prvočíslo 13 je Gaussovým prvočíslem. Pokud není prvočíslem v $\mathbb{Z}[i]$, určete rozklad činitelů tohoto čísla.

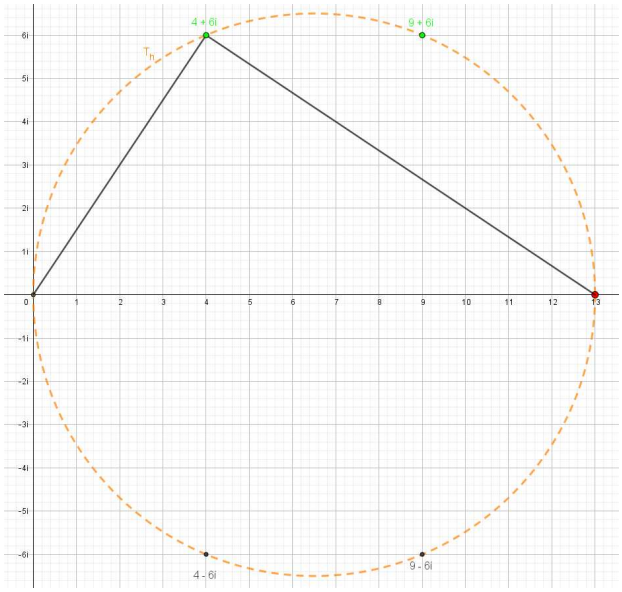
Řešení. Dané zadání jsme zvolili záměrně, abychom si ukázali, jakým způsobem se řeší úloha, ve kterém leží více mřížových bodů na Thaletově kružnici. Z toho je jasné, že jsme již prozradili, že číslo 13 není Gaussovým prvočíslem.

Z předchozích dvou řešených úloh víme, že nejprve dané číslo vyobrazíme v Gaussově rovině, následně sestrojíme Thaletovu kružnici a zjišťujeme, zda na dané kružnici nalezneme mřížový bod (viz obrázek 6.8).



Obrázek 6.8: Prvočíselný rozklad čísla 13 (a)

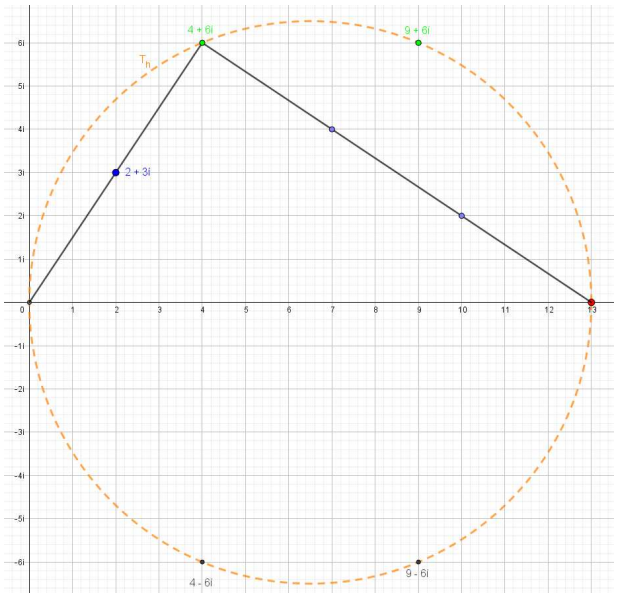
Z obrázku 6.8 je patrné, že na Thaletově kružnici leží 4 mřížové body ($4+6i$, $9+6i$, $4-6i$ a $9-6i$). Nejdříve se zaměříme na body z I. kvadrantu. Vybereme



Obrázek 6.9: Prvočíselný rozklad čísla 13 (b)

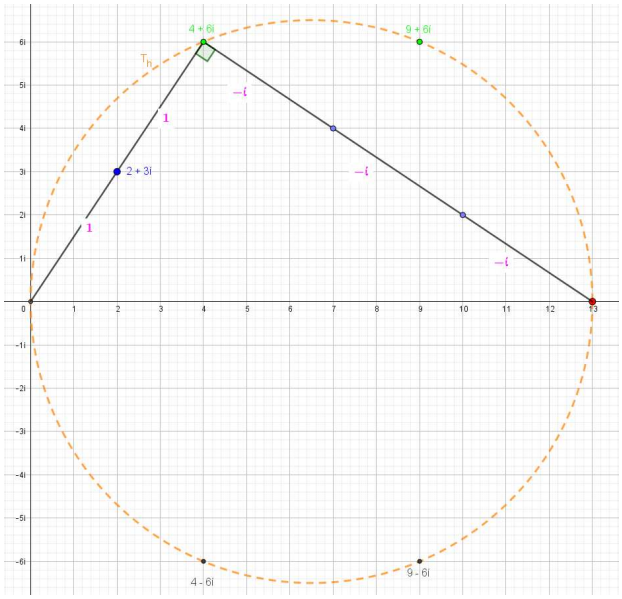
nejprve mřížový bod $4 + 6i$ a postupujeme stejným způsobem jako v úloze 11. Sestrojíme trojúhelník s vrcholy počátek, $4 + 6i$, číslo 13 (viz obrázek 6.9).

Z konstrukce (obrázek 6.10) zjišťujeme, že na stranách daného trojúhelníku leží další mřížové body ($2 + 3i$, $7 + 4i$, $10 + 2i$), které jsou zvýrazněny modře. Vidíme, že získané body rozdělují strany trojúhelníku na jednotlivé dílky, které mají stejnou velikost.



Obrázek 6.10: Prvočíselný rozklad čísla 13 (c)

Z počátku se chceme dostat do bodu $4+6i$. To lze provést přes bod $2+3i$, jež vynásobíme číslem 2, protože číslo $2+3i$ leží ve středu strany trojúhelníku. Jsme v námi požadovaném bodě a vidíme z obrázků, že u daného vrcholu je pravý úhel. Z úlohy 11 víme, že rotaci o 90° získáme vynásobením čísla číslem $-i$. Tím se dostaneme do bodu $7 + 4i$, ale my potřebujeme skončit v čísle 13.

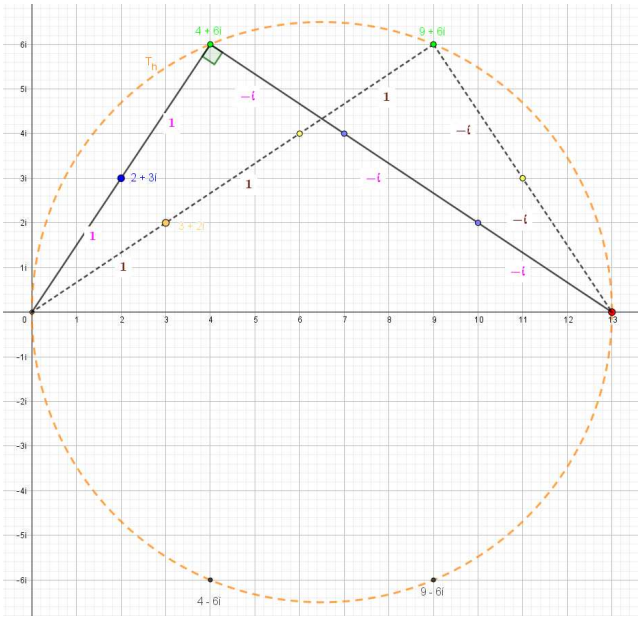


Obrázek 6.11: Prvočíselný rozklad čísla 13 (d)

Z obrázku 6.11 lze vidět, že do daného čísla se dostaneme vynásobením $-2i$. Tedy z bodu $2 + 3i$ se dostaneme do čísla 13 vynásobením čísla $2 + 3i$ číslem $2 - 3i$, proto číslo 13 lze rozložit

$$13 = (2 + 3i)(2 - 3i) \tag{6.2}$$

a tudíž 13 není Gaussovým prvočíslem.



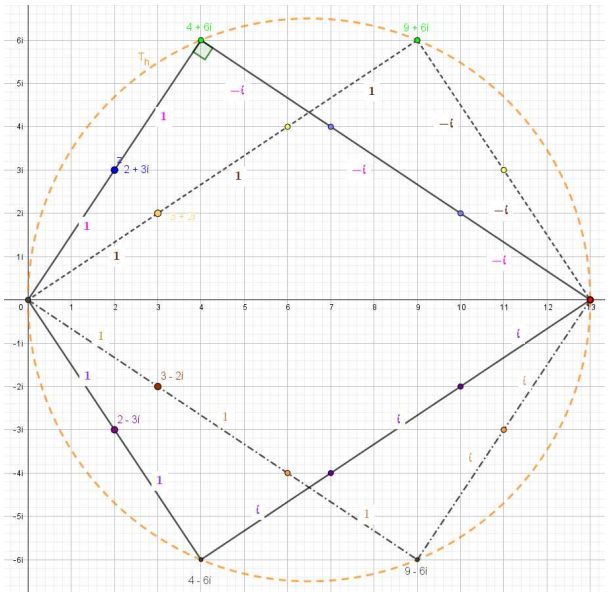
Obrázek 6.12: Prvočíselný rozklad čísla 13 (e)

Nyní se vrátíme zpátky k mřížovému bodu na kružnici z I. kvadrant $(9 + 6i)$ a řešíme stejným způsobem jako pro bod $4 + 6i$. Tím získáme následující grafické znázornění 6.12.

Ze kterého dostáváme tento rozklad

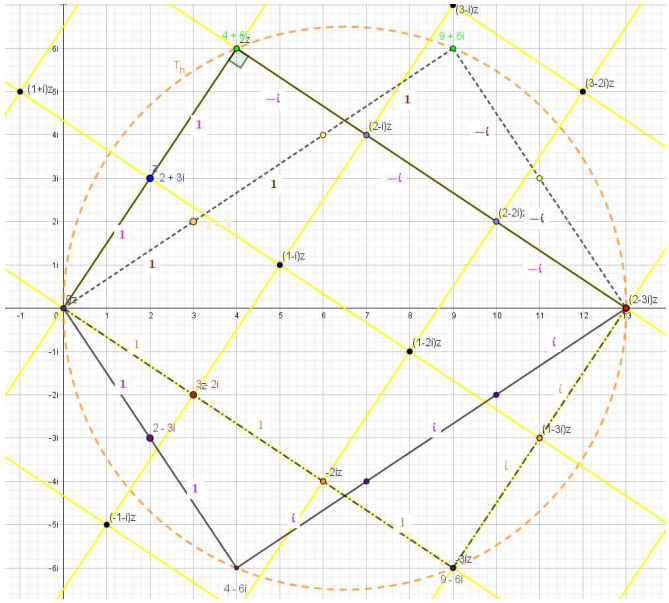
$$13 = (3 + 2i)(3 - 2i),$$

ale ten je stejný s (6.3), protože se jedná o asociovaná čísla v $\mathbb{Z}[i]$ (viz definice 9 v kapitole 2).



Obrázek 6.13: Prvočíselný rozklad čísla 13 (f)

Z obrázku 6.13 je zřejmé, že Gaussova celá čísla (body) ze IV. kvadrantu, která jsou komplexně sdružená s Gaussovým celými čísly z I. kvadrantu (osově souměrná podle reálné osy) mají stejný rozklad jako (6.3).



Obrázek 6.14: Prvočíselný rozklad čísla 13 (g)

Pokud se podíváme na obrázek 6.14, vidíme, že mřížové body $4 + 6i$, $4 - 6i$ na kružnici a mřížové body, které dělí strany trojúhelníků s vrcholem $4 + 6i$ a $4 - 6i$ na dílky stejné velikosti, jsou násobkem Gaussova celého čísla $2 - 3i$.

Řešení dané úlohy si můžeme projít pomocí **Appletu č. 15**, ve kterém je použitá kroková konstrukce. Bližší informace o daném appletu nalezneme v kapitole 7 s názvem Applety (přesněji 7.5.15).

Stejným způsobem bychom zjistili, že z přirozených prvočísel do 20 jsou ještě čísla 7, 11 a 19 Gaussovými prvočísly. Naopak čísla 5 a 17 nejsou prvočísly v $\mathbb{Z}[i]$. K ověření této věty můžeme využít **Applet č. 11**, který rozhoduje, zda je Gaussovo celé číslo prvočíslem či nikoliv. Bližší informace o daném appletu nalezneme v kapitole 7 s názvem Applety (přesněji 7.5.11).

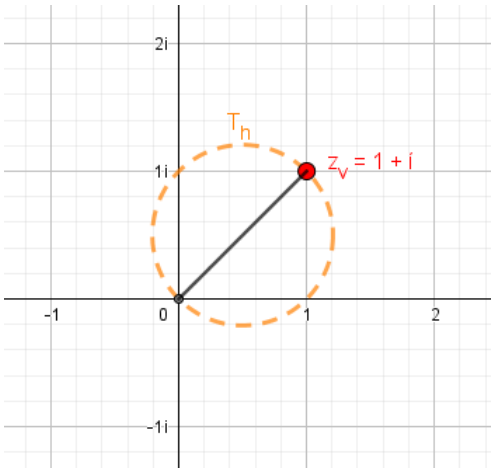
Z řešení předchozích úloh na přirozená čísla docházíme k závěru: *„Pokud dokážeme sestrojit Thaletovu kružnici, která prochází kromě počátku a daného přirozeného čísla jiným mřížovým bodem. Potom dané číslo z* $\mathbb{N}$ *není Gaussovým prvočíslem. V opačném případě je prvočíslem v* $\mathbb{Z}[i]$*.“*

6.2 Gaussova celá čísla

Nyní ověříme, zda můžeme řešení pomocí Thaletovy kružnice využít pro jakékoliv Gaussovo celé číslo.

Úloha 14. Rozhodněte, zda číslo $z_v = 1 + i$ je Gaussovým prvočíslem. Pokud není prvočíslem v $\mathbb{Z}[i]$, určete rozklad činitelů tohoto čísla.

Řešení. Řešíme stejným postupem jako u předchozí úlohy. Nejprve znázorníme Gaussovo celé číslo v komplexní rovině. Následně sestrojíme Thaletovu kružnici (obrázek 6.15).



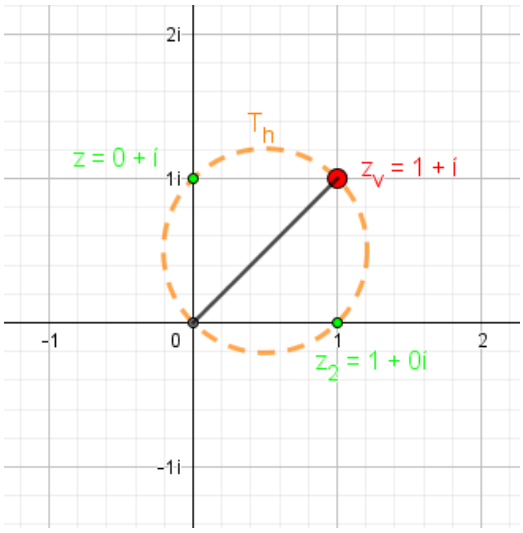
Obrázek 6.15: Gaussovo celé číslo $z_v = 1 + i$ v komplexní rovině (1)

Na obrázku 6.16 vidíme, že na kružnici leží 2 mřížové body ($z = 0 + i$, $z_2 = 1 + 0i$). Pokud zvolíme prvně zmíněné Gaussovo celé číslo, získáváme

$$z_v = i(1 - i) = (1 + i). \tag{6.3}$$

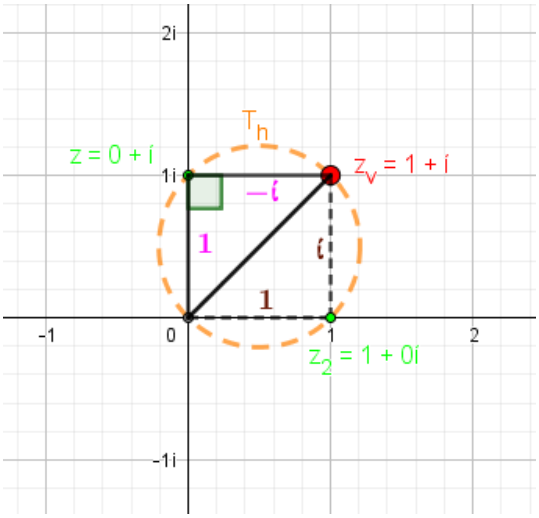
Při výběru druhého čísla $z_2 = 1 + 0i$, dostáváme

$$z_v = 1(1 + i) = (1 + i). \tag{6.4}$$



Obrázek 6.16: Gaussovo celé číslo $z_v = 1 + i$ v komplexní rovině (2)

Grafické znázornění těchto vyjádření lze vidět na obrázku 6.17. A tyto zápisy (6.3),(6.4) jsou totožné. Navíc splňují definici 11 z kapitoly 3, a proto je Gaussovo celé číslo $z = 1 + i$ prvočíslem v $\mathbb{Z}[i]$.

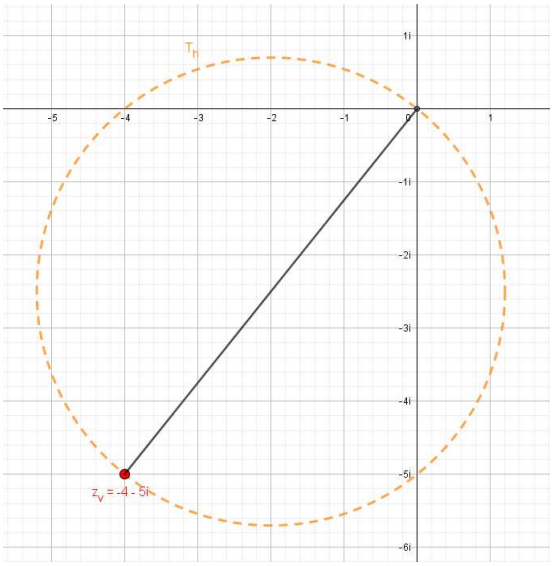


Obrázek 6.17: Gaussovo celé číslo $z_v = 1 + i$ v komplexní rovině (3)

Řešení dané úlohy si lze projít pomocí **Appletu č. 16**, ve kterém je použitá kroková konstrukce. Bližší informace o daném appletu nalezneme v kapitole 7 s názvem Applety (přesněji 7.5.16).

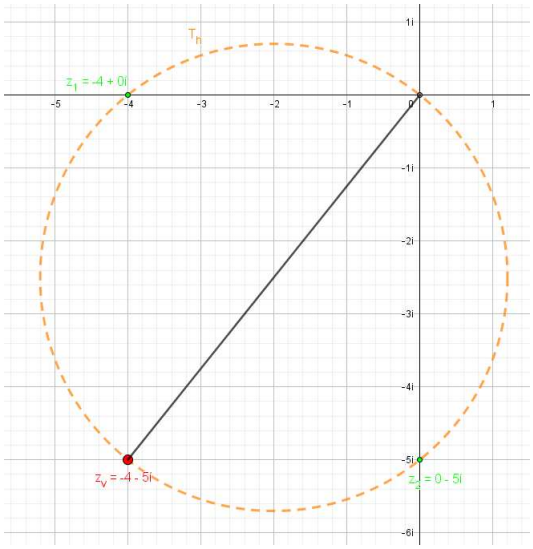
Úloha 15. Rozhodněte, zda číslo $z_v = -4 - 5i$ je Gaussovým prvočíslem. Pokud není prvočíslem v $\mathbb{Z}[i]$, určete rozklad činitelů tohoto čísla.

Řešení. V komplexní rovině vyobrazíme Gaussovo celé číslo $z_v = -4 - 5i$ a zkonstruujeme Thaletovu kružnici, která prochází počátkem a zadaným číslem z_v (obrázek 6.18).



Obrázek 6.18: Gaussovo celé číslo $z_v = -4 - 5i$ v komplexní rovině (1)

Na obrázku 6.19 vidíme, že získáváme dva mřížové body $z_1 = -4$ a $z_2 = -4$, které leží na Thaletově kružnici a na reálné (imaginární) ose Gaussovy roviny.



Obrázek 6.19: Gaussovo celé číslo $z_v = -4 - 5i$ v komplexní rovině (2)

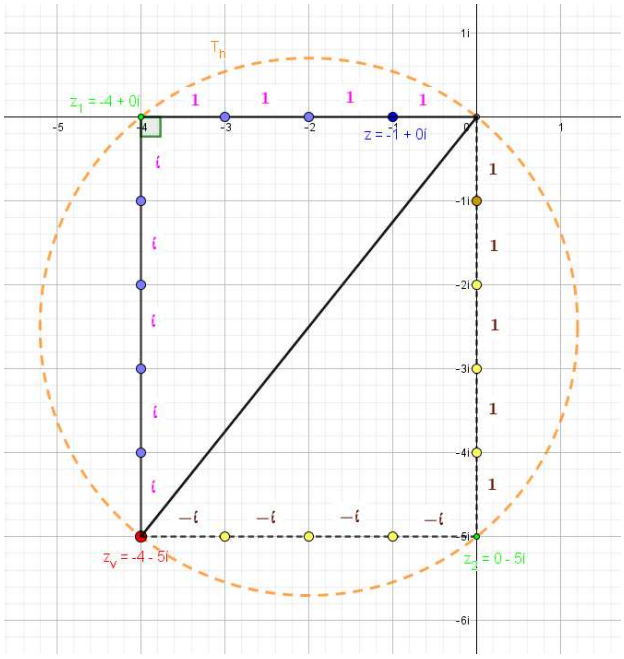
Z obrázku 6.20 je zřejmé, že číslo $z_v = -4 - 5i$ lze vyjádřit

$$z_v = (-1 + 0i)(4 + 5i) = -4 - 5i \tag{6.5}$$

a

$$z_v = (0 - i)(5 - 4i) = -4 - 5i. \tag{6.6}$$

Vztahy (6.5) a (6.7) říkají, že se jedná o Gaussovo prvočíslo (viz definice 11 z kapitoly 3).

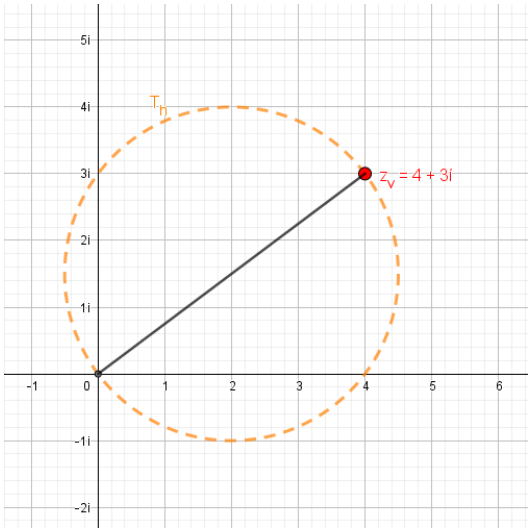


Obrázek 6.20: Gaussovo celé číslo $z_v = -4 - 5i$ v komplexní rovině (3)

Po krocích můžeme zhlédnout řešení dané úlohy pomocí **Appletu č. 17**, ve kterém je použitá kroková konstrukce. Bližší informace o daném appletu nalezneme v kapitole 7 s názvem Applety (přesněji 7.5.17).

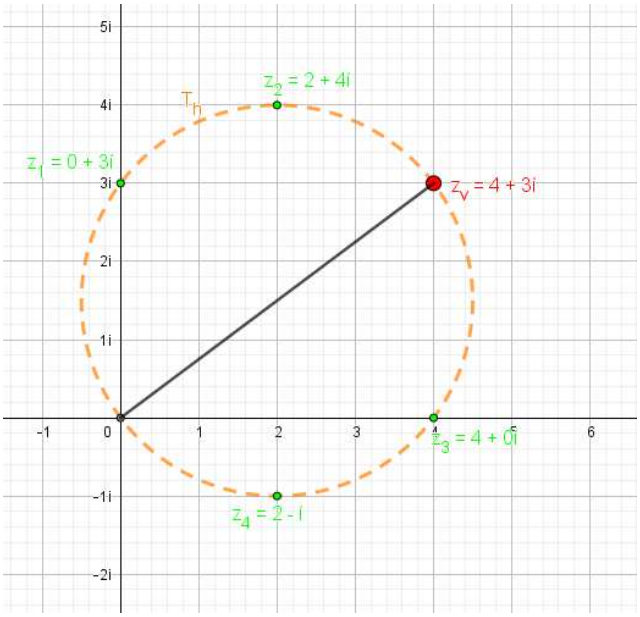
Úloha 16. Rozhodněte, zda číslo $z_v = 4 + 3i$ je Gaussovým prvočíslem. Pokud není prvočíslem v $\mathbb{Z}[i]$, určete rozklad činitelů tohoto čísla.

Řešení. V Gaussově rovině mějme zobrazené Gaussovo celé číslo z_v a sestrojenou Thaletovu kružnici (obrázek 6.21).



Obrázek 6.21: Gaussovo celé číslo $z_v = 4 + 3i$ v komplexní rovině (a)

Na kružnici nalezneme 4 mřížové body $z_1 = 3i$, $z_2 = 1 + 4i$, $z_3 = 4$ a $z_4 = 2 - i$ (zeleně zbarvené)(viz obrázek 6.22).



Obrázek 6.22: Gaussovo celé číslo $z_v = 4 + 3i$ v komplexní rovině (b)

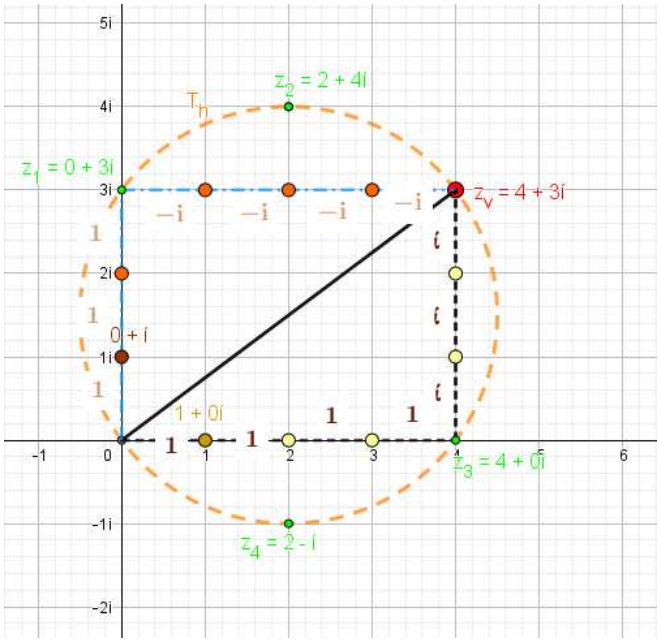
Vybereme mřížové body $z_1 = 0 + 3i$, $z_3 = 4 + 0i$ a z obrázku 6.23 jsou zřejmé následující vztahy

$$z_v = i(3 - 4i) = 4 + 3i \tag{6.7}$$

a

$$z_v = 1(4 + 3i) = 4 + 3i.$$

Z definice 9 z kapitoly 2 víme, že se jedná o asociovaná čísla.



Obrázek 6.23: Gaussovo celé číslo $z_v = 4 + 3i$ v komplexní rovině (c)

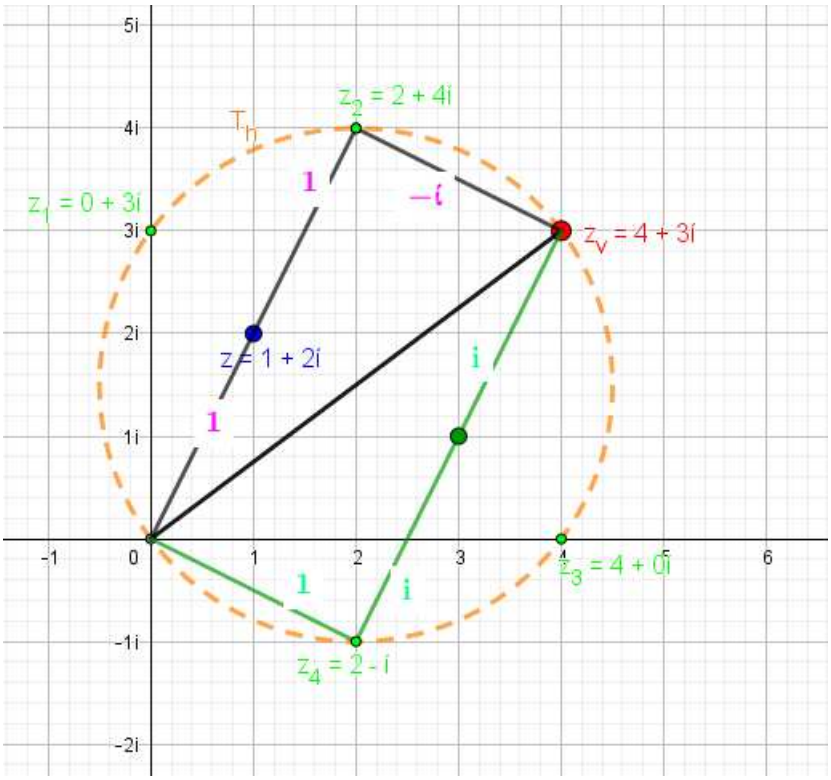
Nyní vezmeme Gaussova celá čísla $z_2 = 1 + 4i$ a $z_4 = 2 - i$. Z grafického znázornění na obrázku 6.24 je vidět, že čísla můžeme rozložit

$$z_v = (1 + 2i)(2 - i) = 4 + 3i$$

a

$$z_v = (2 - i)(1 + 2i) = 4 + 3i.$$

Oba tyto rozklady jsou stejné. To ale nic nemění na tom, že Gaussovo celé číslo $z_v = 4 + 3i$ není Gaussovým prvočíslem, protože ho jsme schopni rozložit (viz (6.7)).



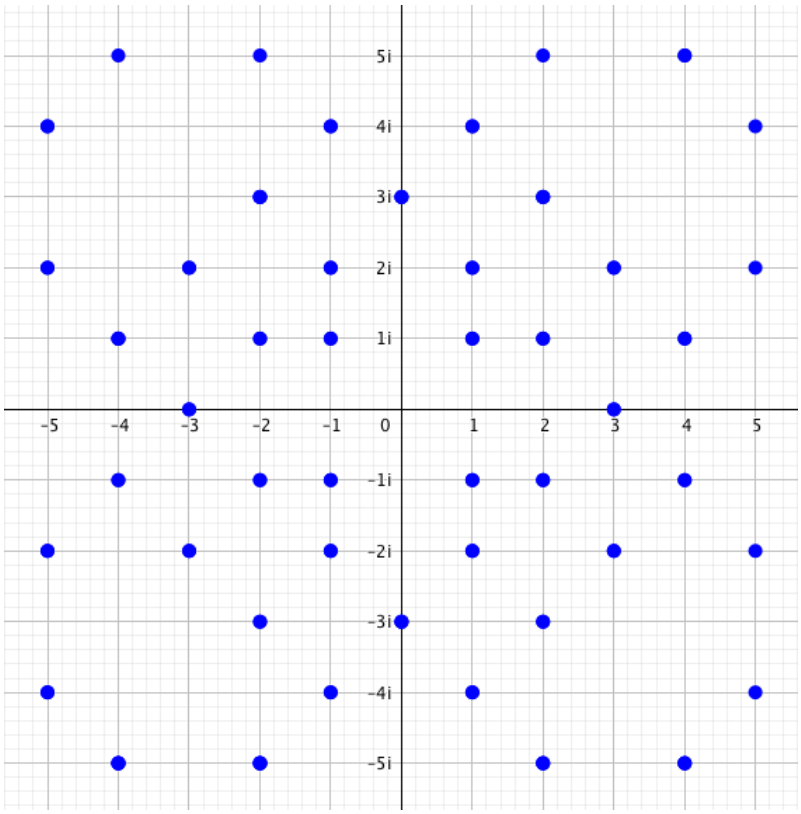
Obrázek 6.24: Gaussovo celé číslo $z_v = 4 + 3i$ v komplexní rovině (d)

Řešení dané úlohy si můžeme projít pomocí **Appletu č. 18**, ve kterém je použitá kroková konstrukce. Bližší informace o daném appletu nalezneme v kapitole 7 s názvem Applety (přesněji 7.5.18).

Poznámka. Z předchozích úloh zjišťujeme, že pomocí Thaletovy kružnice lze zjistit, zda jakékoliv nenulové Gaussovo celé číslo je Gaussovým prvočíslem, či nikoliv.

6.3 Prvočísla v komplexní rovině

Na obrázku 6.25 můžeme vidět vyobrazenou část komplexní roviny s prvočísly v $\mathbb{Z}[i]$. Pokud se zadíváme více na toto zobrazení, můžeme říci, že prvočísla v Gaussově rovině jsou osově souměrná podle reálné a imaginární osy. Protože tyto osy jsou na sebe kolmé, můžeme říct, že Gaussova prvočísla jsou i středově souměrná podle počátku komplexní roviny.



Obrázek 6.25: Prvočísla v komplexní rovině

Zobrazení prvočísel v Gaussově rovině si můžeme vyzkoušet v rámci **Appletu č. 12**. Bližší informace o daném appletu nalezneme v kapitole 7 s názvem Applety (přesněji 7.5.12).

Kapitola 7

Applety

V první části kapitoly seznamujeme čtenáře s obecnými informacemi (význam slova applet, využití, ...). V druhé části je uveden odkaz k nalezení appletů, které vytvořil autor této práce, a popis jednotlivých appletů demonstrujících vybrané vlastnosti Gaussových celých čísel.

7.1 Obecně o appletech

Applet[1] je softwarová komponenta, která běží v kontextu jiného programu, např. v rámci webového prohlížeče. Tento pojem byl zaveden v rámci AppleScriptu[2] v roce 1993. Většinou se orientuje na plnění konkrétní funkce.

Applet je napsán v jazyce, který se liší od skriptovacího jazyka nebo jazyka HTML[3], který jej vyvolává. Applet je napsán v kompilovaném jazyce[4], zatímco skriptovací jazyk kontejneru je jazyk interpretovaný[5], a proto je vyšší výkon a funkčnost appletu.

Někdy se výraz applet alternativně používá k popisu malé samostatné aplikace, například program kalkulačka a další, které jsou typicky dodávány s operačními systémy.

7.2 Výhody appletů

Mezi výhody appletů patří následující vlastnosti:

- pracuji na straně klienta, proto je kratší odezva,
- zabezpečení,

[1] Velmi často se používá spojení **Java applet**, což je malá aplikace, která je napsána v objektově orientovaném programovacím jazyce Java.

[2] **AppleScript** je skriptovací jazyk vyvinutý firmou Apple Inc., který byl zakomponován do jejich operačních systémů Mac OS. [37]

[3] HyperText Markup Language (zkratka HTML) je značkovací jazyk, který se používá pro tvorbu webových stránek, jež jsou propojeny hypertextovými odkazy. [38]

[4] **Kompilovaný jazyk** je programovací jazyk, pro který je potřeba zdrojový kód, v němž je napsaný, nejprve přeložit pomocí překladače do strojového kódu a až poté můžeme program spustit. [39]

[5] **Interpretovaný jazyk** je programovací jazyk, který lze spustit pomocí zdrojového kódu a zvláštního programu tzv. interpretu. Tento program zdrojový kód interpretuje (provádí). [40]

- jsou spouštěny v rámci webového prohlížeče, který běží na mnoha platformách, včetně Linuxu, Windows, Mac OS atd.

7.3 Nevýhody appletů

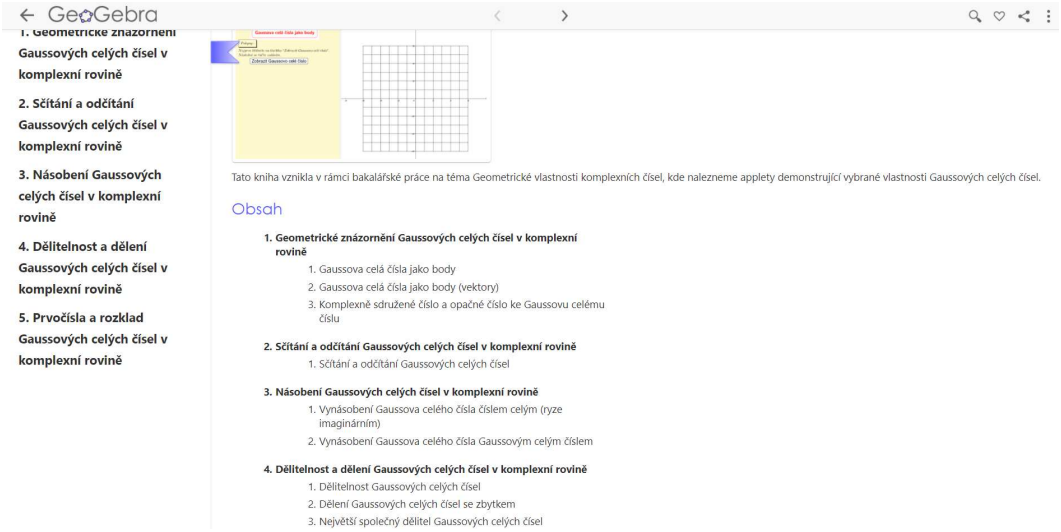
Ke spuštění appletů jsou nejčastěji vyžadovány pluginy v klientském prohlížeči.

7.4 Využití

Applety jsou nejčastěji používány jako pluginy pro zobrazování 3D modelů, které umožňují otáčení a zvětšení zobrazeného modelu skrze webový prohlížeč, jako dále demonstrační programy atd. Na bázi appletů jsou vyvinuty některé webové hry. [41]

7.5 Matematické applety

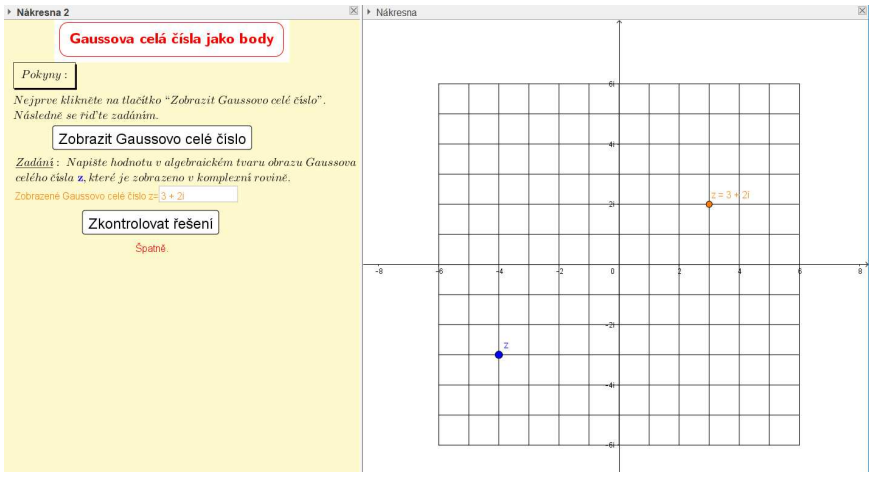
Applety, které byly vytvořeny v programu GeoGebra v rámci bakalářské práce a jež demonstrují vybrané vlastnosti Gaussovo celých čísel nalezneme na následujícím odkazu https://ggbm.at/rusK9KPN, který jsme již uváděli v úvodu práce. Pro publikování appletů na internetu jsme využili GeoGebru, která umožňuje vytvořit **Knihu** na GeoGebraTube. Do této knihy můžeme nahrát vlastní applety (soubory vytvořené v GeoGebře), jež můžeme opatřit popisky (textem), nastavit formu sdílení, případně konkrétní applet stáhnout. Po otevření odkazu výše se zobrazí úvodní obrazovka se vzhledem, který lze vidět na obrázku **obr10:app1**.



Obrázek 7.1: GeoGebra Book

7.5.1 Applet č. 1

- **Téma:** Souřadnice Gaussova celého čísla v Gaussově rovině
- **Účel:** Uživatel si procvičí vyčíst (správně určit) souřadnice (zápis v algebraickém tvaru) pro dané Gaussovo celé číslo.
- **Předpokládané znalosti:** Gaussovo celé číslo (algebraický zápis), komplexní rovina
- **Popis:** Při zahájení appletu se zobrazí okno s pokyny, tlačítkem a Gaussovou rovinou. Po poklepání na tlačítko "Zobrazit Gaussovo celé číslo"se zobrazí text se zadáním a Gaussovo celé číslo v Gaussově rovině. Po určení souřadnic (algebraického tvaru) Gaussova celého čísla klikneme na tlačítko "Zkontrolovat řešení". Následně se vyobrazí text s informací, zda jsme hodnotu určili správně či nikoliv.



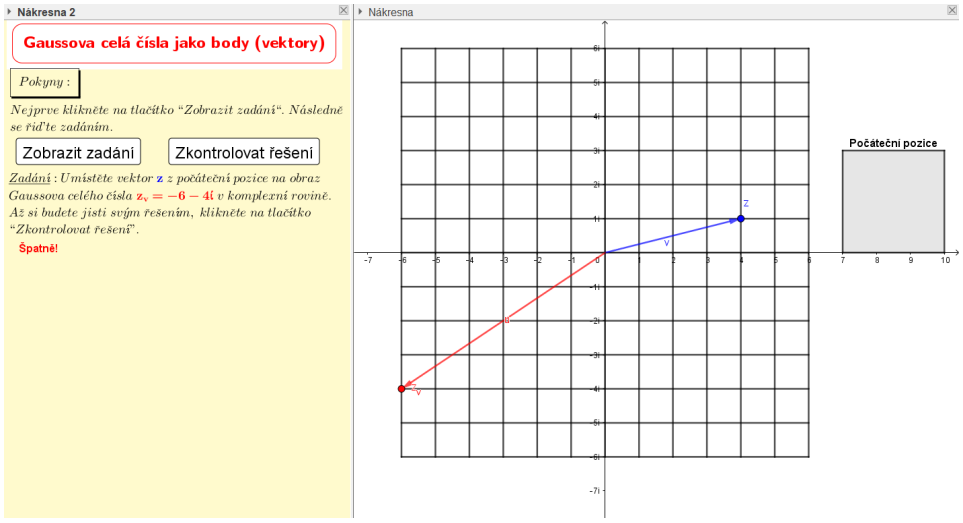
Obrázek 7.2: Applet č. 1

Jestliže znovu klikneme na tlačítko "Zobrazit Gaussovo celé číslo", vygeneruje se náhodně zcela nové zadání.

7.5.2 Applet č. 2

- **Téma:** Gaussova celá čísla jako body (vektory) komplexní roviny
- **Účel:** Applet slouží k procvičení grafické interpretace Gaussových celých čísel jako body (vektory) v Gaussově rovině.
- **Předpokládané znalosti:** Gaussovo celé číslo (algebraický zápis tohoto čísla), komplexní rovina, vektor
- **Popis:** Po spuštění appletu se zobrazí okno s pokyny a s komplexní rovinou. Po kliknutí na tlačítko "Zobrazit zadání"se vyobrazí zadání, ve kterém máme umístit Gaussovo celé číslo jako bod nebo jako vektor v Gaussově rovině s přesnými instrukcemi. Po přesunutí bodu z (vektoru v) do vyznačené oblasti (komplexní roviny) se zobrazí tlačítko "Zkontrolovat řešení". Po následném kliknutí na toto tlačítko se objeví text s informací, zda jsme

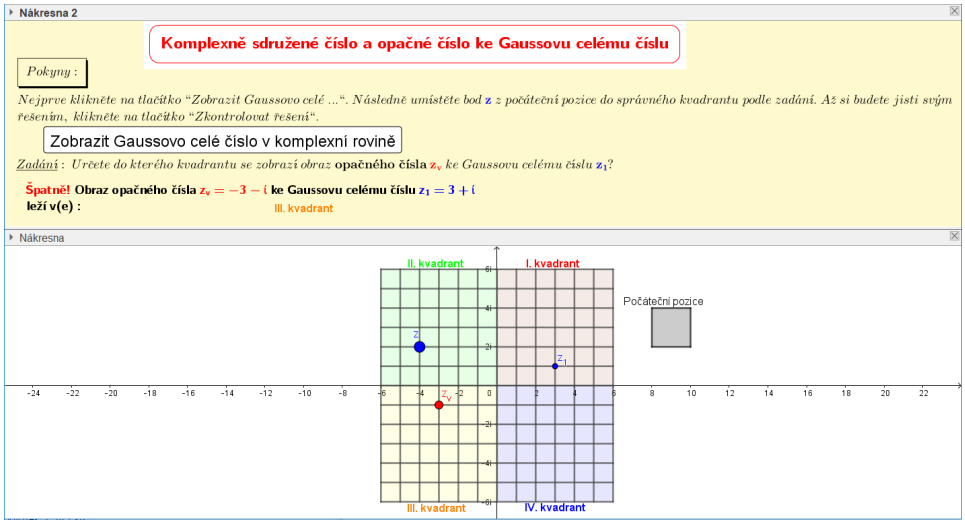
úkol vykonali správně či nikoliv. Zároveň se vykreslí grafické řešení našeho zadání.



Obrázek 7.3: Applet č. 2

Po kliknutí znovu na tlačítko "Zobrazit zadání"se náhodně vygeneruje zcela nové zadání.

7.5.3 Applet č. 3



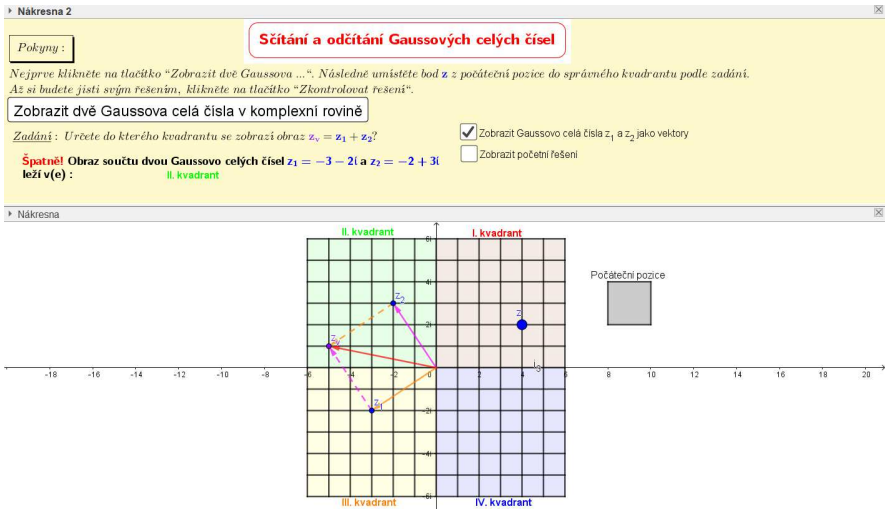
Obrázek 7.4: Applet č. 3

- **Téma:** Komplexně sdružené a opačné číslo ke Gaussovu celému číslu
- **Účel:** Uživatel si procvičí geometrické zobrazení obrazu komplexně sdruženého a opačného čísla ke Gaussovu celému číslu v Gaussově rovině.
- **Předpokládané znalosti:** Gaussovo celé číslo, komplexně sdružené číslo, opačné číslo, komplexní rovina

- **Popis:** Při zahájení appletu se zobrazí okno s pokyny a s komplexní rovinou rozdělenou do jednotlivých kvadrantů. Po kliknutí na tlačítko "Zobrazit Gaussovo celé číslo v komplexní rovině"se zobrazí text se zadáním, ve kterém máme určit, do jakého kvadrantu Gaussovy roviny se zobrazí obraz komplexně sdruženého čísla (nebo opačného čísla) ke Gaussovu celému číslu. Při přesunutí bodu z do některého barevně zvýrazněného kvadrantu se zobrazí tlačítko "Zkontrolovat řešení". Po následném klepnutí na předchozí tlačítko se vyobrazí text (správně/špatně) i se správným řešením. Při opětovném kliknutí na tlačítko "Zobrazit Gaussovo celé číslo v komplexní rovině"se náhodně vygeneruje zcela nové zadání.

7.5.4 Applet č. 4

- **Téma:** Grafické sčítání a odčítání Gaussovo celých čísel
- **Účel:** Daný applet slouží k procvičení grafického sčítání a odčítání dvou Gaussových celých čísel v komplexní rovině.
- **Předpokládané znalosti:** Gaussovo celé číslo, komplexní rovina, vektor, operace sčítání a odčítání

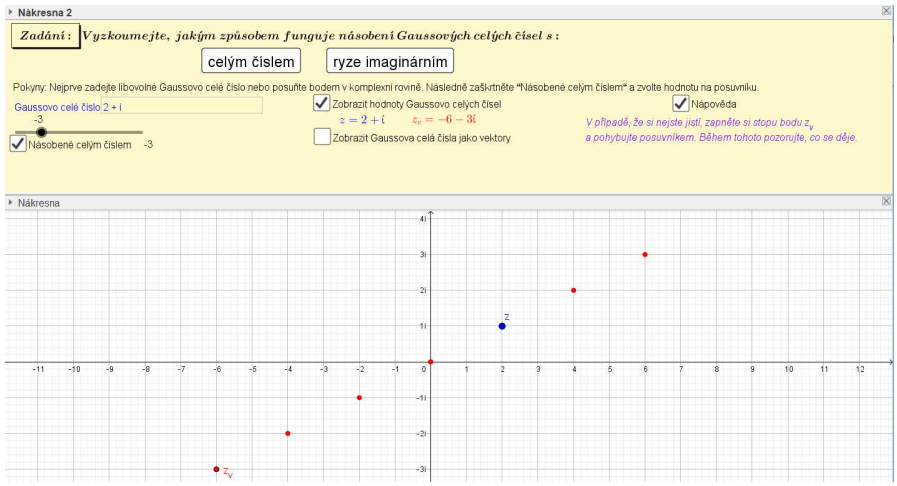


Obrázek 7.5: Applet č. 4

- **Popis:** Při úvodním spuštění daného appletu se uživateli zobrazí okno s pokyny a s Gaussovou rovinou, jež je rozdělena do jednotlivých barevných kvadrantů. Po kliknutí na tlačítko "Zobrazit dvě Gaussova celá čísla v komplexní rovině"se zobrazí zadaní, u kterého se mohou objevit dvě možnosti (sčítání nebo odčítání dvou Gaussových celých čísel). Zároveň se vyobrazí tlačítko "Zkontrolovat řešení"a zaškrtávací políčko "Zobrazit Gaussova celá čísla jako vektory". Po přemístění bodu z do některého barevně zvýrazněného kvadrantu a po klepnutí na tlačítko "Zkontrolovat řešení"se zobrazí text s informací, zda jsme správně určili řešení. U obou variant textů (správné/nesprávné řešení) se vykreslí grafické řešení daného zadání. Máme i možnost si zobrazit početní řešení daného zadání. V případě nesprávného

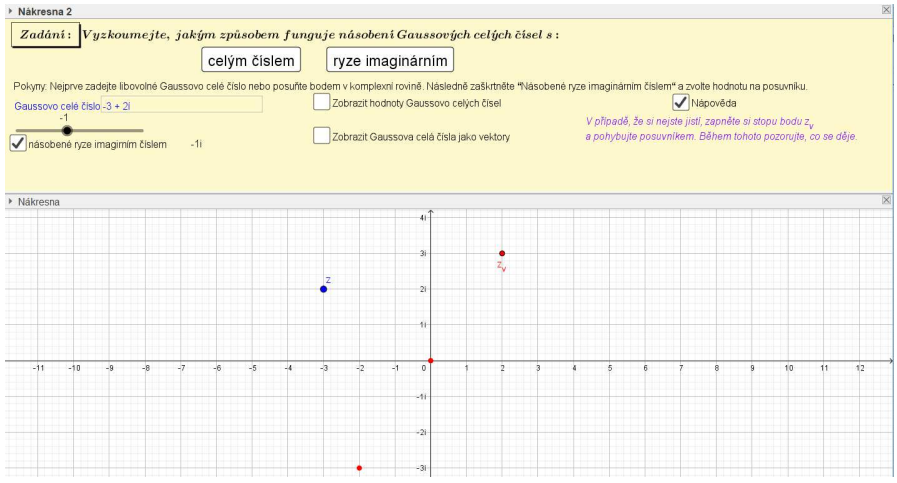
řešení se navíc zobrazí v textu správný kvadrant řešení. Při opětovném kliknutí na tlačítko "Zobrazit dvě Gaussova celá čísla v komplexní rovině"se náhodně vygeneruje zcela nové zadání.

7.5.5 Applet č. 5



Obrázek 7.6: Applet č. 5 (a)

- **Téma:** Grafické násobení Gaussova celého čísla celým (ryze imaginárním) číslem
- **Účel:** Uživatel sám zkusí přijít na princip grafického násobení Gaussova celého čísla celým (resp. ryze imaginárním) číslem v komplexní rovině. Daný applet je především určen pro uživatele, kteří se neseznámili s textem v kapitole 4 (přesněji 4.6.1 a 4.6.2) nebo s danou problematikou někde jinde.
- **Předpokládané znalosti:** Gaussovo celé číslo, celé číslo, ryze imaginární číslo, komplexní rovina

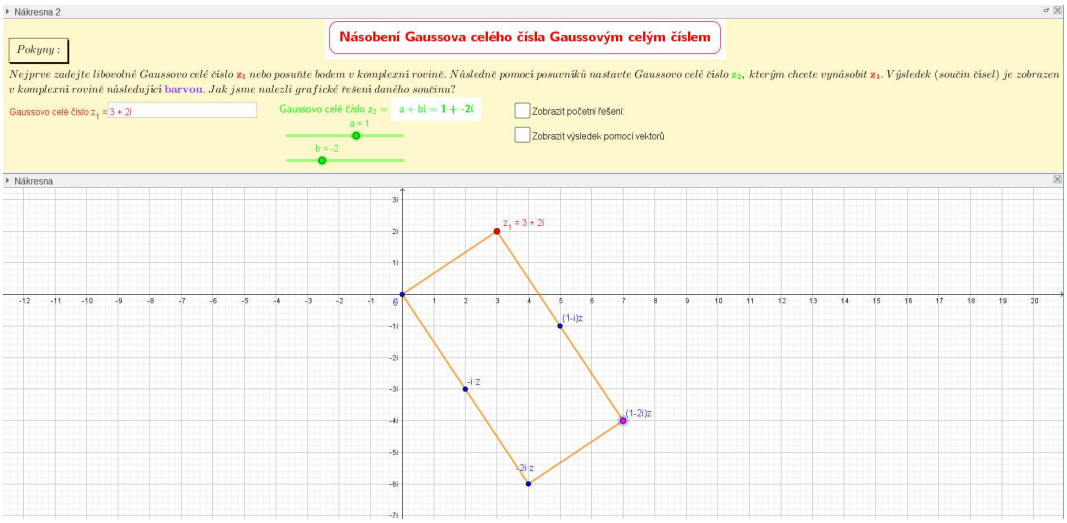


Obrázek 7.7: Applet č. 5 (b)

- **Popis:** Při spuštění appletu se zobrazí okno se zadáním, dvěma tlačítky a s komplexní rovinou. U tlačítek můžeme zvolit, zda Gaussovo celé číslo chceme vynásobit celým (resp. ryze imaginárním) číslem. Po zvolení jedné varianty (klepnutí na dané tlačítko) se zobrazí pokyny, zaškrtávací políčka, možnost zadání Gaussova celého čísla (případně můžeme posunout bodem v komplexní rovině) a zároveň jakým číslem bude násobeno (zvolení hodnoty na posuvníku). Následně se vykreslí námi zvolený součin čísel v Gaussově rovině. Pokud by uživatel z daného vyobrazení nic nezjistil, má možnost si zobrazit nápovědu pomocí zaškrtávacího políčka "Nápověda". Uživatel by měl přijít na vlastnosti (princip), které jsou uvedeny v kapitole 4 (přesněji 4.6.1 a 4.6.2).

7.5.6 Applet č. 6

- **Téma:** Grafické násobení Gaussova celého čísla s Gaussových celým číslem
- **Účel:** Uživatel sám zkusí zjistit, jakým způsobem funguje grafické násobení Gaussova celého čísla Gaussovým celým číslem v komplexní rovině. Daný applet je především určen pro uživatele, kteří se neseznámili s textem v kapitole 4 (přesněji 4.6.3) nebo s danou problematikou někde jinde.
- **Předpokládané znalosti:** Gaussovo celé číslo, grafické sčítání těchto čísel, komplexní rovina

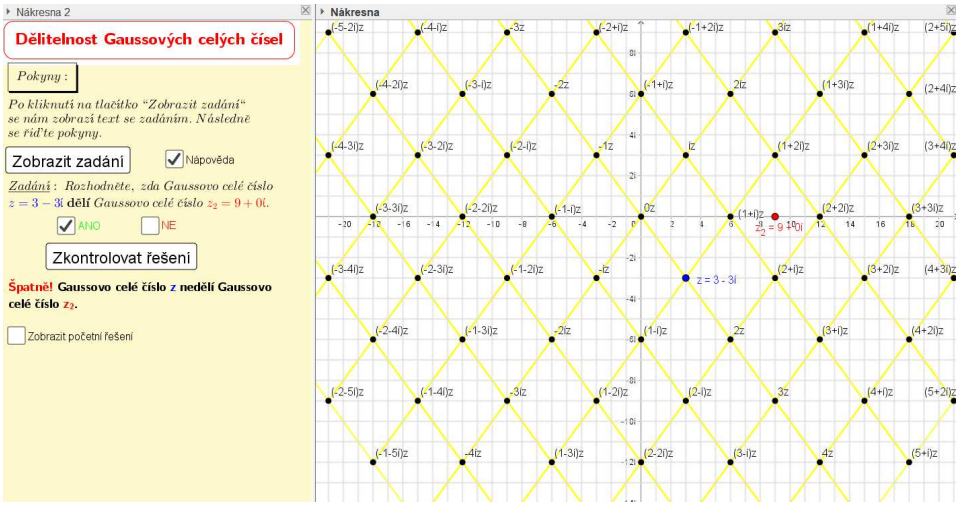


Obrázek 7.8: Applet č. 6

- **Popis:** Při spuštění appletu se zobrazí okno s pokyny, s zaškrtávacími políčky, s možností zadat Gaussovo celé číslo (případně můžeme posunout bodem v komplexní rovině) a zároveň posuvníky, kterými zvolíme, jakým Gaussovým celým číslem bude násobeno Gaussovo celé číslo. Následně se vyobrazí řešení v Gaussově rovině. Dalšími změnami jednotlivých čísel (zadáním) se bude měnit naše vyobrazení v komplexní rovině. Kdybychom zvolili reálnou (resp. imaginární) část nulovou, převedli bychom problematiku na předchozí applet 7.5.4.

7.5.7 Applet č. 7

- **Téma:** Grafická interpretace dělitelnosti Gaussových celých čísel
- **Účel:** Applet slouží k procvičení dělitelnosti dvou Gaussových celých čísel z hlediska geometrické interpretace.
- **Předpokládané znalosti:** Gaussovo celé číslo, dělitelnost v $\mathbb{Z}[i]$ (viz definice 6, norma Gaussových celých čísel (viz definice 5), komplexní rovina
- **Popis:** Po spuštění appletu se zobrazí okno s textem, ve kterém jsou napsány pokyny, a tlačítko "Zobrazit zadání". Po klepnutí na dané tlačítko se vyobrazí zadání společně se třemi zaškrtávacími políčky ("Nápověda", ANO, NE) a zároveň Gaussova celá čísla v komplexní rovině. Při zaškrtnutí políčka "Nápověda"se zobrazí násobky čísla z. Po výběru jedné z možností ANO/NE se vykreslí tlačítko "Zkontrolovat řešení". Po následném kliknutí na toto tlačítko se objeví text s informací o správnosti řešení a se zaškrtávacím políčkem "Zobrazit početní řešení". Při opětovném klepnutí na "Zobrazit zadání"se vygeneruje nové zadání.

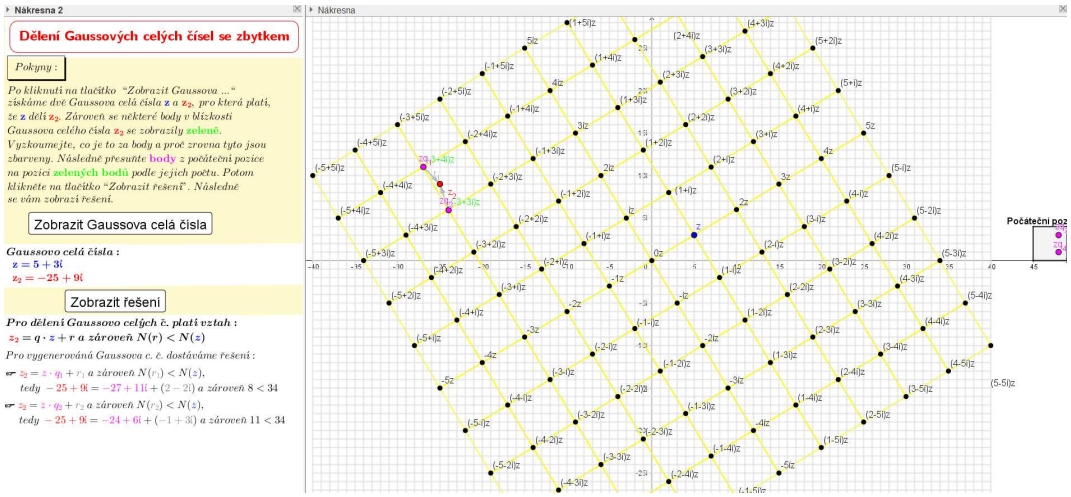


Obrázek 7.9: Applet č. 7

7.5.8 Applet č. 8

- **Téma:** Grafické dělení Gaussových celých čísel se zbytkem
- **Účel:** Applet demonstruje grafické dělení dvou Gaussových celých čísel se zbytkem v komplexní rovině.
- **Předpokládané znalosti:** Gaussovo celé číslo, dělení se zbytkem v $\mathbb{Z}[i]$ (viz věta 3), norma Gaussových celých čísel (viz definice 5), komplexní rovina
- **Popis:** Při spuštění appletu se zobrazí okno s pokyny, tlačítkem a Gaussovou rovinou. Po kliknutí na tlačítko "Zobrazit Gaussova celá čísla"se vykreslí dvě Gaussova celá čísla, násobky jednoho z těchto čísel (tvoří

žlutá mřížka) a některé body zbarvené zeleně v komplexní rovině. Tyto zelené body jsou řešením daného dělení. Pokud přemístíme některý z fialových bodů na zeleně zbarvený, zviditelní se tlačítko "Zobrazit řešení". Po následném klepnutí na něj se zobrazí celkové řešení společně s algebraickým (početním).

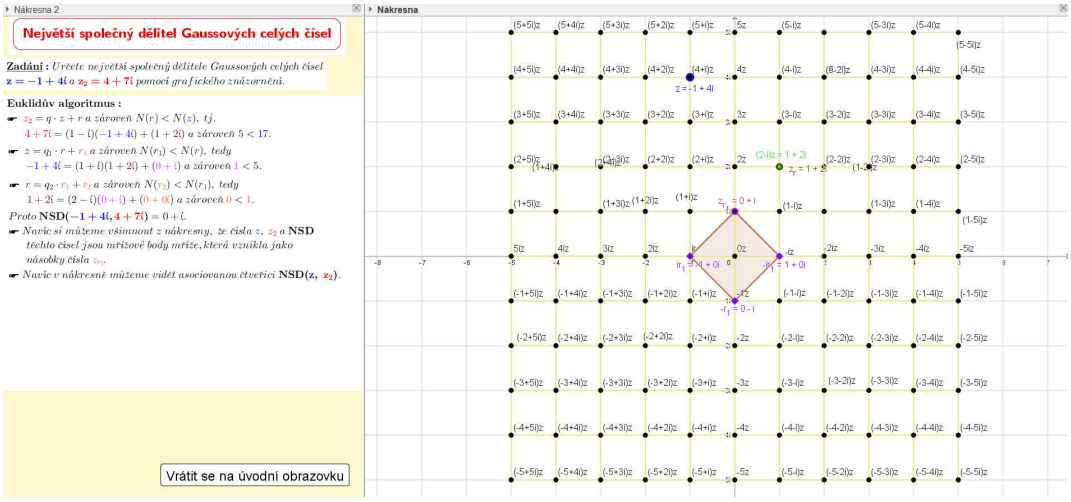


Obrázek 7.10: Applet č. 8

V případě, že znovu klikneme na tlačítko "Zobrazit Gaussova celá čísla", vygeneruje se náhodně nové zadání.

7.5.9 Applet č. 9

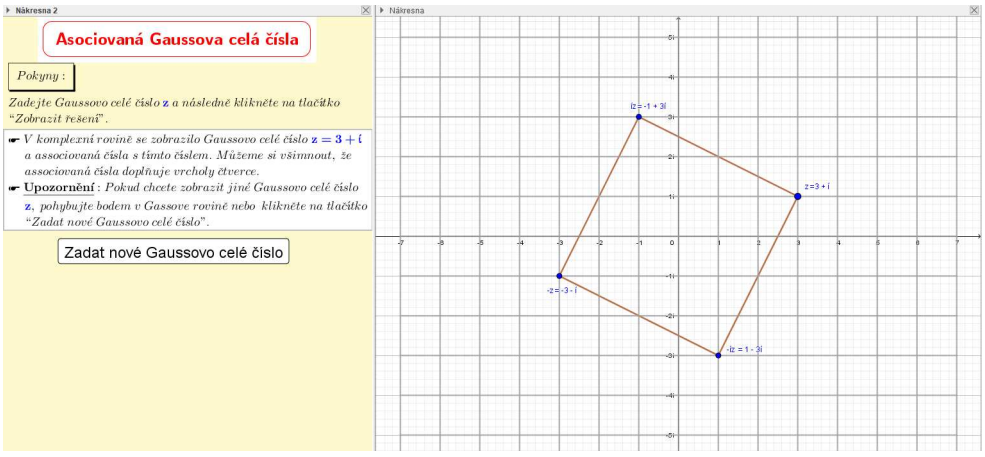
- **Téma:** Největší společný dělitel Gaussových celých čísel v komplexní rovině
- **Účel:** Pomocí appletu je možné vyzkoušet si hledání (určení) největšího společného dělitele dvou Gaussových celých čísel v komplexní rovině.
- **Předpokládané znalosti:** Gaussovo celé číslo, dělení se zbytkem v $\mathbb{Z}[i]$ (viz věta 3), Euklidův algoritmus v $\mathbb{Z}[i]$ (viz věta 10), největší společný dělitel v $\mathbb{Z}[i]$ (viz definice 8), norma Gaussových celých čísel (viz definice 5), komplexní rovina
- **Popis:** Po spuštění appletu se zobrazí okno se zadáním, pokyny, dvěma posuvníky, textovým polem a tlačítkem. Po zvolení Gaussových celých čísel (z, z_2) klikneme na tlačítko "Zobrazit Gaussova celá čísla". Následně se vyobrazí Gaussova celá čísla společně s násobky čísla z v komplexní rovině. A zároveň se označí násobky z, které vyhovují podmínce uvedené ve větě 3. Následně je po uživateli vyžadováno zadání jednoho z těchto vyhovujících násobků. Po zadání vyhovující násobku se zobrazí první krok v Euklidově algoritmu s případným požadavkem na zadání konkrétního zbytku (pokud po vydělení čísla z_2 číslem z získáme nenulový zbytek). Následně se v Gaussově rovině zobrazí násobky zbytku r a zbarvené vyhovující násobky r. Uživatel znovu zadá svoji volbu. Tímto způsobem pokračujeme do té doby než získáme nulový zbytek a tedy největší společný dělitel Gaussových celých čísel z a z_2.



Obrázek 7.11: Applet č. 9

7.5.10 Applet č. 10

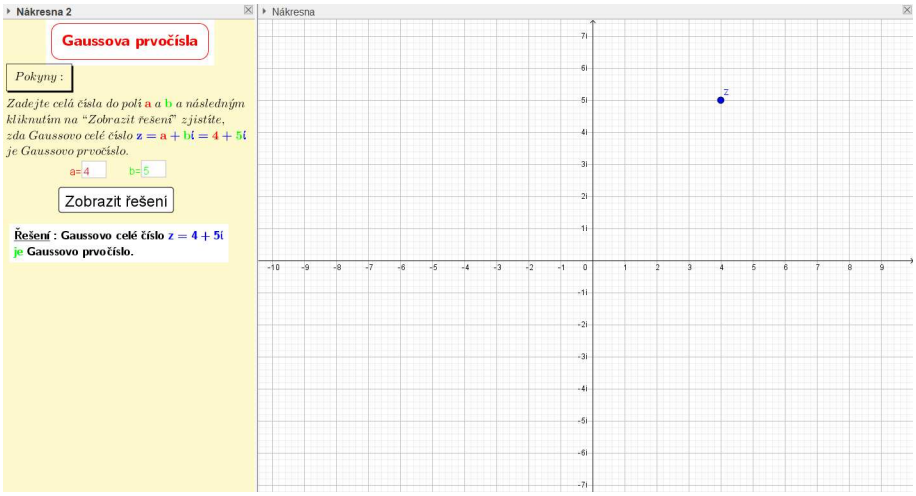
- **Téma:** Grafická interpretace asociovaných Gaussových celých čísel
- **Účel:** Applet slouží ke geometrické interpretaci asociovaných Gaussových celých čísel v komplexní rovině.
- **Předpokládané znalosti:** Gaussovo celé číslo, asociovaná čísla v $\mathbb{Z}[i]$ (viz definice 9), komplexní rovina
- **Popis:** Po spuštění appletu se vyobrazí okno s pokyny, tlačítkem a polem pro zadání Gaussova celého čísla z. Po vyplnění čísla z a následném klepnutí na "Zobrazit řešení"se vykreslí asociovaná čísla ke Gaussovu celému číslu z v Gaussově rovině, text s informacemi a tlačítkem "Zadat nové Gaussovo celé číslo".



Obrázek 7.12: Applet č. 10

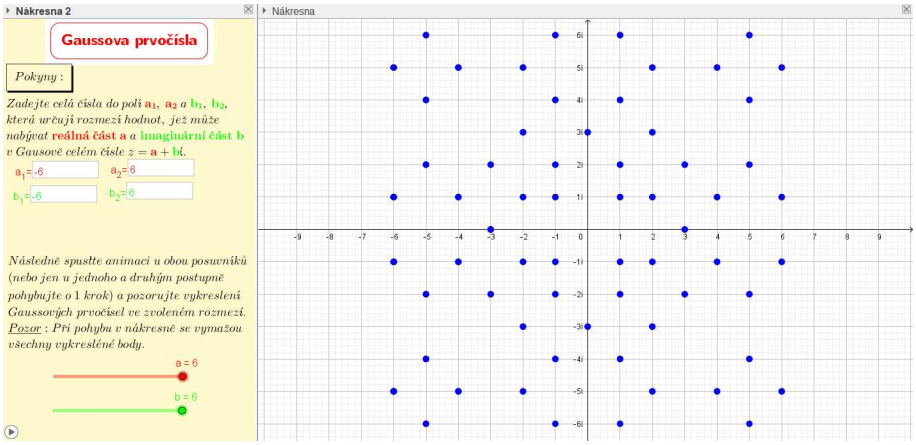
7.5.11 Applet č. 11

- **Téma:** Prvočísla v $\mathbb{Z}[i]$
- **Účel:** Applet rozhodne o číslu ze $\mathbb{Z}[i]$, zda je Gaussovým prvočíslem.
- **Předpokládané znalosti:** Gaussovo celé číslo, prvočíslo v $\mathbb{Z}[i]$
- **Popis:** Po spuštění appletu se zobrazí text s pokyny, textová pole a tlačítko. Po zadání Gaussova celého čísla z (zadání hodnot do textových polí) a klepnutí na tlačítko "Zobrazit řešení"se zobrazí text s informací, zda Gaussovo celé číslo z je nebo není Gaussovým prvočíslem.



Obrázek 7.13: Applet č. 11

7.5.12 Applet č. 12



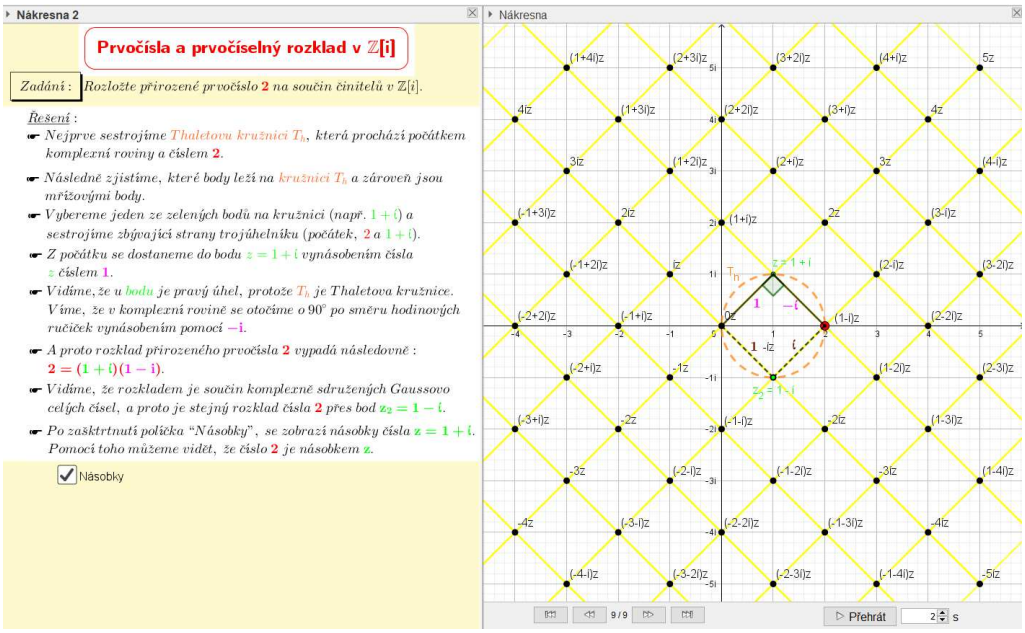
Obrázek 7.14: Applet č. 12

- **Téma:** Prvočísla v Gaussově rovině
- **Účel:** Applet slouží k vyobrazení Gaussových prvočísel v komplexní rovině.

- **Předpokládané znalosti:** Gaussovo celé číslo, Gaussovo prvočíslo, komplexní rovina
- **Popis:** Po spuštění appletu se zobrazí text s pokyny, textovými poli a posuvníky. Zadáním hodnot do textových polí určíme rozmezí jednotlivých posuvníků. Následně spustíme animaci jednoho nebo obou posuvníků a sledujeme vykreslování Gaussových prvočísel v komplexní rovině. Pokud bychom zadali do textových polí nesmyslné rozmezí jednotlivých posuvníků, vyobrazí se text s informací, abychom dané rozmezí upravili.

7.5.13 Applet č. 13

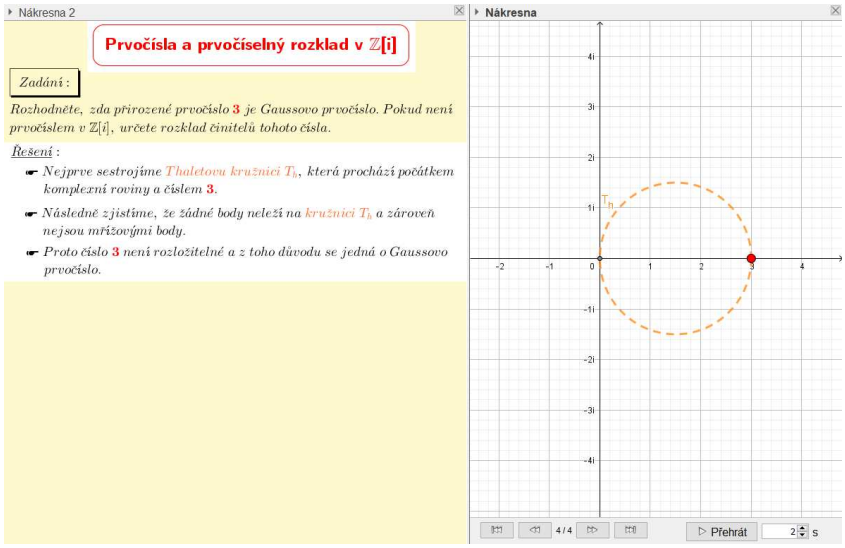
- **Téma:** Prvočíselný rozklad čísla 2 v $\mathbb{Z}[i]$ a v Gaussově rovině
- **Účel:** Daný applet ukazuje geometrickou interpretaci prvočíselného rozkladu v komplexní rovině.
- **Předpokládané znalosti:** Gaussovo celé číslo, prvočíslo a prvočíselný rozklad v $\mathbb{Z}[i]$, komplexní rovina, Thaletova kružnice
- **Popis:** Po spuštění appletu se zobrazí okno se zadáním. Navíc v pravém dolním rohu najdeme nový panel, který slouží k ovládání krokové konstrukce v programu GeoGebra. Díky těmto tlačítkům můžeme procházet konstrukcí tam a zpátky, případně lze spustit jako animace. Pokud existují násobky některého Gaussova celého čísla zobrazí se zaškrtávací políčko "Násobky"v posledním kroku konstrukce.



Obrázek 7.15: Applet č. 13

7.5.14 Applet č. 14

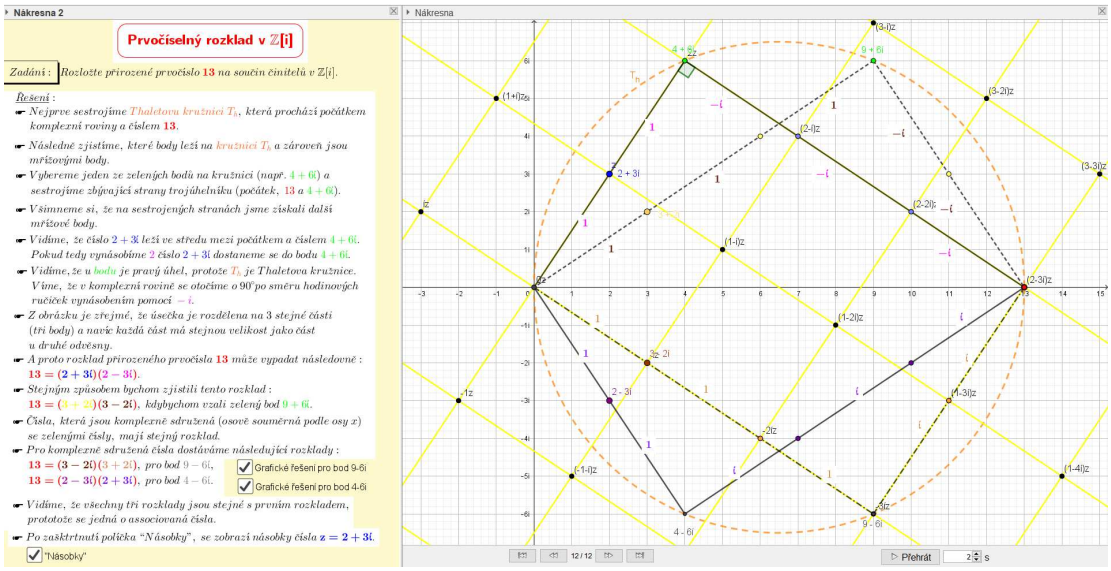
- **Téma:** Prvočíslo 3 v $\mathbb{Z}[i]$ a v komplexní rovině
- Další body nebudeme vyplňovat, protože applet je téměř totožný jako applet jako 7.5.13.



Obrázek 7.16: Applet č. 14

7.5.15 Applet č. 15

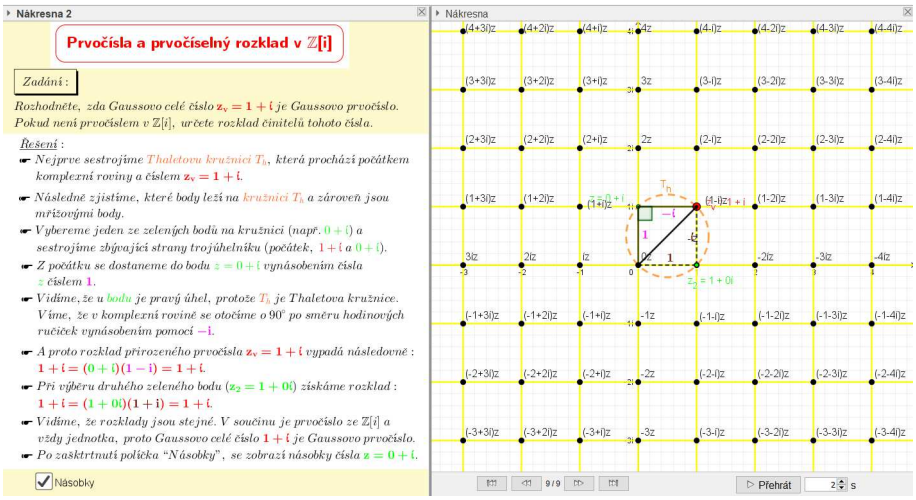
- **Téma:** Prvočíselný rozklad čísla 13 v $\mathbb{Z}[i]$ a v komplexní rovině
- Další body nebudeme uvádět, jelikož applet je podobný s appletem 7.5.13.



Obrázek 7.17: Applet č. 15

7.5.16 Applet č. 16

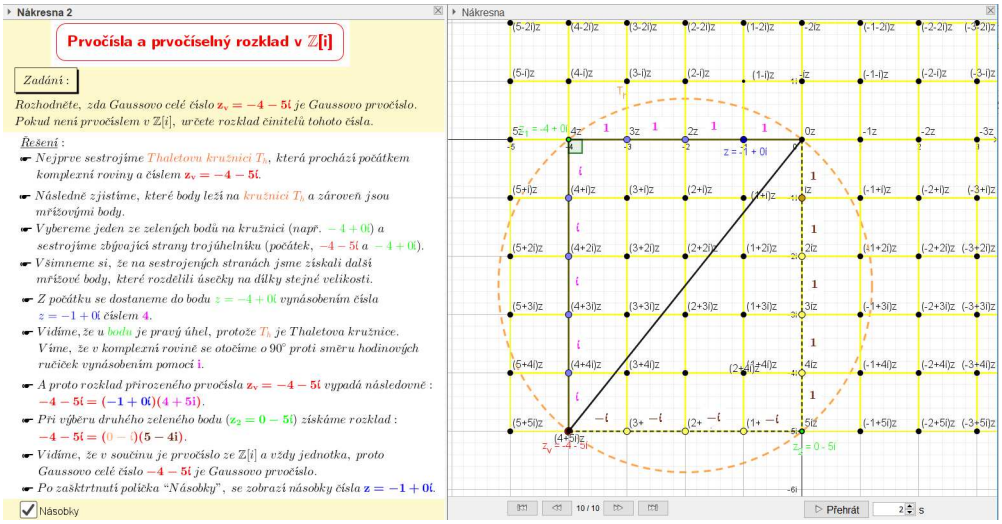
- **Téma:** Prvočíslo $z = 1 + i$ v $\mathbb{Z}[i]$ a v Gaussově rovině
- Další body nebudeme popisovat jako u jiných appletů, jelikož applet je podobný s 7.5.13.



Obrázek 7.18: Applet č. 16

7.5.17 Applet č. 17

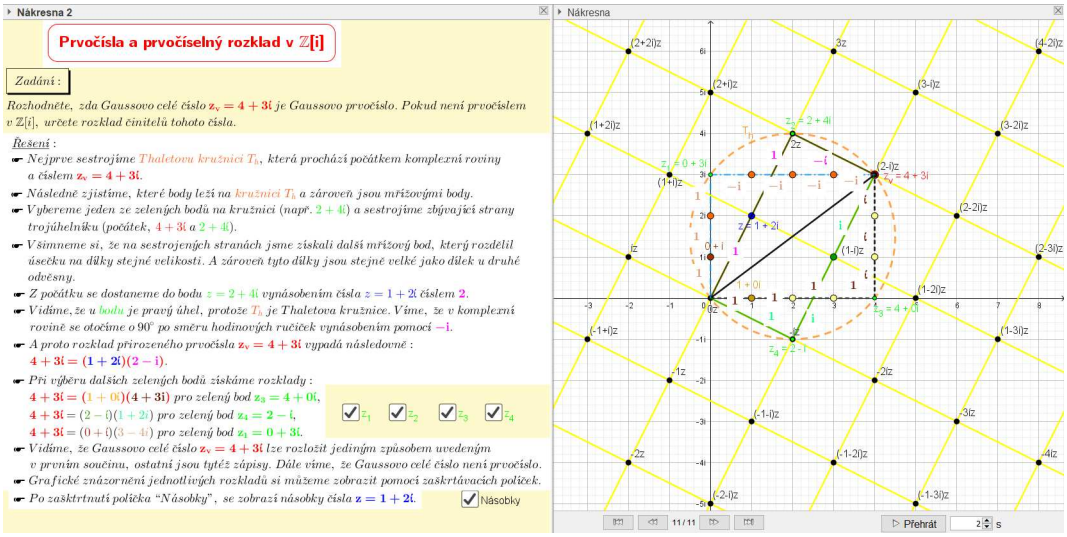
- **Téma:** Prvočíslo $z = -4 - 5i$ v $\mathbb{Z}[i]$ a v komplexní rovině
- Další body nebudeme uvádět jako u jiných appletů, protože applet je podobný s 7.5.13.



Obrázek 7.19: Applet č. 17

7.5.18 Applet č. 18

- **Téma:** Prvočíselný rozklad $z = 4 + 3i$ v $\mathbb{Z}[i]$ a v Gaussově rovině
- Další body nebudeme vyplňovat, jelikož applet je podobný s appletem 7.5.13.



Obrázek 7.20: Applet č. 18

Závěr

Cílem bakalářské práce bylo prostudovat si vlastnosti Gaussovo celých čísel a vytvoření appletů demonstrujících vybrané geometrické vlastnosti těchto čísel.

Autor se domnívá, že práce má několik předností a přínosů, které si zformulujeme do několika bodů.

- Odvození a ukázka vybraných vlastností pomocí geometrické interpretace skrze řešené úlohy (kapitoly 4, 5 a 6).
- Vytvoření interaktivních appletů v programu GeoGebra demonstrujících geometrické vlastnosti.
- Zpracování uceleného teoretického textu, který vychází především z cizojazyčné literatury, a je uveden v prvních třech kapitolách. Ty by šly využít jako pomocný studijní materiál při výuce na některých typech středních nebo vysokých škol.
- Práci by šlo rozšířit o pedagogický výzkum v rámci diplomové práce, jenž by se zabýval zařazením appletů do výuky. Zajímavé by bylo zjišťování, jaký vliv má právě využití appletů ve výuce. Zda žáci lépe porozumí dané problematice, případně zda se zvýší zájem žáků skrze applety o matematiku.

Autora mrzí, že nedokázal vytvořit některé applety více interaktivní (např. prvočíselný rozklad v $\mathbb{Z}[i]$) tak, jak by chtěl. Je to z důvodu omezenosti programu GeoGebra.

Literatura

[1] Daniel Shanks. *Solved and unsolved problems in number theory*, volume 297. American Mathematical Soc., 2001.

[2] Pavel Boháč. *Základy geometrie komplexních čísel.* PhD thesis, Masarykova univerzita, Přírodovědecká fakulta, 2013. Dostupné z: `https://is.muni.cz/th/gwht9/rigo.pdf`.

[3] James Pommersheim, Tim K Marks, and Erica Flapan. *Number theory: a lively introduction with proofs, applications, and stories.* Wiley, 2010.

[4] John B Fraleigh. *A first course in abstract algebra.* Pearson Education India, 2003.

[5] Wikipedie. *Okruh (algebra) — Wikipedie: Otevřená encyklopedie*, [Online; navštíveno 1. 03. 2018]. Dostupné z: `https://cs.wikipedia.org/w/index.php?title=Okruh_(algebra)`.

[6] Titu Andreescu, Dorin Andrica, et al. *Complex Numbers from A to... Z*, volume 165. Springer, 2006.

[7] Miloš Ráb. *Komplexní čísla v elementární matematice.* Masarykova univerzita, Přírodovědecká fakulta, 1996.

[8] Richard Earl. Mathematical institute, oxford, ox1 2lb, august 2003. 2003.

[9] Margaret F. Willerding. Divisibility and factorization of gaussian integers. *The Mathematics Teacher*, 59(7), 1966.
Dostupné z: `https://www.jstor.org/stable/27957439`.

[10] Lee A. Butler. A classification of gaussian primes. Dostupné z: `http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.568.1607`.

[11] Serge Tabachnikov. *Kvant selecta: algebra and analysis*, volume 1. Universities Press, 1999.
Dostupné z: `https://books.google.cz/books?id=001rPuunBLcC`.

[12] Frederick Michael Hall. *An introduction to abstract algebra.* CUP Archive, 1966. Dostupné z: `https://books.google.cz/books?id=LYg4AAAAIAAJ`.

[13] Theodore Shifrin. *Abstract algebra: A geometric approach.* Prentice Hall, 1996.

[14] James Kraft and Lawrence Washington. *An Introduction to Number Theory with Cryptography*. Chapman and Hall/CRC, 2018. Dostupné z: https://books.google.cz/books?id=zy9KDwAAQBAJ.

[15] Ronald Solomon. *Abstract Algebra*, volume 9. American Mathematical Soc., 2003. Dostupné z: https://books.google.cz/books?id=ouvZKQiykf4C.

[16] Giancarlo Travaglini. *Number theory, Fourier analysis and Geometric discrepancy*, volume 81. Cambridge University Press, 2014. Dostupné z: https://books.google.cz/books?id=mIaYAwAAQBAJ.

[17] Keith Conrad. The gaussian integers. *Pre-Print, paper edition*, 2008. Dostupné z: http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/Zinotes.pdf.

[18] Nanxian Chen. *Mobius Inversion in Physics*, volume 1. world Scientific, 2010. Dostupné z: https://books.google.cz/books?id=JmxK6-RoWmsC.

[19] Carl Douglas Olds, Anneli Lax, Giuliana P Davidoff, and Giuliana Davidoff. *The geometry of numbers*, volume 41. Cambridge University Press, 2001. Dostupné z: https://books.google.cz/books?id=Bycut_duHr8C.

[20] Waclaw Sierpinski. *Elementary Theory of Numbers: Second English Edition (edited by A. Schinzel)*, volume 31. Elsevier, 1988. Dostupné z: https://books.google.cz/books?id=ktCZ2MvgN3MC.

[21] Mahima Ranjan Adhikari and Avishek Adhikari. *Basic modern algebra with applications*. Springer, 2016. Dostupné z: https://books.google.cz/books?id=lBO7BAAAQBAJ.

[22] Wikipedie. *Prvočíslo — Wikipedie: Otevřená encyklopedie*, [Online; navštíveno 2. 04. 2018]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Prvo%C4%8D%C3%ADslo.

[23] Liong-shin Hahn. *Mathemagical Buffet*. National Taiwan University Press, 2013. Dostupné z: https://books.google.cz/books?id=rK9PBvtf9XIC.

[24] William Judson LeVeque. *Elementary theory of numbers*. Courier Corporation, 1990. Dostupné z: https://books.google.cz/books?id=BYvMAgAAQBAJ.

[25] Jakub Opršel. Gaussovská prvočísla, 2006.

[26] TT Moh. Algebra, series on university mathematics vol. 5, 1992. Dostupné z: https://books.google.cz/books?id=v9Xt77TaeMAC.

[27] Sukumar Das Adhikari. *An introduction to commutative algebra and number theory*. CRC Press, 2001. Dostupné z: https://books.google.cz/books?id=U5fgRF7ekQcC.

[28] John Stillwell. *Elements of number theory*. Springer Science & Business Media, 2002. Dostupné z: https://books.google.cz/books?id=5jsmBQAAQBAJ.

[29] Anthony Vazzana and David Garth. *Introduction to Number Theory, 2nd Edition (Textbooks in Mathematics)*. Chapman and Hall, 2015. Dostupné z: https://books.google.cz/books?id=QpLwCgAAQBAJ.

[30] Milan Hejný a další. *Úvod do studia analytické geometrie*. PedF UK, 2006.

[31] Tristan Needham. *Visual complex analysis*. Oxford University Press, 1998.

[32] Eric W Weisstein. *CRC concise encyclopedia of mathematics*. CRC press, 2002. Dostupné z: https://books.google.cz/books?id=D_XKBQAAQBAJ.

[33] Tristan Roussillon and David Coeurjolly. *Characterization of bijective discretized rotations by Gaussian integers*. PhD thesis, LIRIS UMR CNRS 5205, 2016. Dostupné z: https://hal.archives-ouvertes.fr/hal-01259826/file/RR.pdf.

[34] Michal Čučka. *Pythagorova věta a její důkazy*. PhD thesis, Masarykova univerzita, Pedagogická fakulta, 2007.

[35] Jiří Doležal. Základy geometrie a geometrie. *Ostrava: VŠB-TU*, 2007.

[36] Šárka Voráčová a kolektiv. *Atlas geometrie - Geometrie krásná a užitečná*. Academia, 2012.

[37] Wikipedie. *AppleScript — Wikipedie: Otevřená encyklopedie*, [Online; navštíveno 8. 04. 2018]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=AppleScript.

[38] Wikipedie. *HyperText Markup Language — Wikipedie: Otevřená encyklopedie*, [Online; navštíveno 8. 04. 2018]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=HyperText_Markup_Language.

[39] Wikipedie. *Kompilovaný jazyk — Wikipedie: Otevřená encyklopedie*, [Online; navštíveno 8. 04. 2018]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Kompilovan%C3%BD_jazyk.

[40] Wikipedie. *Interpretovaný jazyk — Wikipedie: Otevřená encyklopedie*, [Online; navštíveno 8. 04. 2018]. Dostupné z: https://cs.wikipedia.org/w/index.php?title=Interpretovan%C3%BD_jazyk.

[41] Wikipedie. *Applet — Wikipedia, The Free Encyclopedia*, 2007. Dostupné z: https://en.wikipedia.org/w/index.php?title=Applet.

Seznam obrázků

1.1 Grafické schéma Gaussových celých čísel 8
1.2 Grafický důkaz trojúhelníkové nerovnosti 16

2.1 Jednotky $\mathbb{Z}[i]$ v komplexní rovině 21
2.2 Grafické znázornění dělení Gaussovo celých čísel 21
2.3 Asociovaná čísla $\mathbb{Z}[i]$ v komplexní rovině 26

4.1 Gaussovo celá čísla jako bod (vlevo) a vektor (vpravo) 36
4.2 Grafické znázornění komplexně sdruženého čísla 37
4.3 Grafické znázornění opačného čísla 38
4.4 Sčítání dvou Gaussových celých čísel jako vektory 38
4.5 Odčítání dvou Gaussových celých čísel jako vektory 38
4.6 Násobení Gaussova celého čísla celým číslem 39
4.7 Násobení Gaussova celého čísla číslem ryze imaginárním 40
4.8 Násobení Gaussova celého čísla s Gaussovým celým číslem 41
4.9 Mříž s násobky Gaussova celého čísla 41

5.1 Dělitelnost Gaussových celých čísel (a) 43
5.2 Dělitelnost Gaussových celých čísel (b) 44
5.3 Dělitelnost Gaussových celých čísel (c) 44
5.4 Dělení Gaussových celých čísel se zbytkem 46
5.5 Dělení Gaussových celých čísel se zbytkem (řešení) 47
5.6 1 řešení pro dvojici (q,r) 48
5.7 2 řešení pro dvojici (q,r) (a) 48
5.8 2 řešení pro dvojici (q,r) (b) 49
5.9 3 řešení pro dvojici (q,r) 49
5.10 4 řešení pro dvojici (q,r) 50
5.11 Největší společný dělitel (1) 51
5.12 Největší společný dělitel (2) 51
5.13 Největší společný dělitel (3) 52
5.14 Největší společný dělitel (4) 52
5.15 Největší společný dělitel (5) 53
5.16 Největší společný dělitel (6) 53
5.17 Největší společný dělitel (7) 54
5.18 Největší společný dělitel (8) 54
5.19 Největší společný dělitel (9) 55
5.20 Největší společný dělitel (10) 55
5.21 Největší společný dělitel (11) 56

6.1 Prvočíselný rozklad čísla 2 (a) 57
6.2 Prvočíselný rozklad čísla 2 (b) 58
6.3 Prvočíselný rozklad čísla 2 (c) 59
6.4 Prvočíselný rozklad čísla 2 (d) 59
6.5 Prvočíselný rozklad čísla 2 (e) 59
6.6 Prvočíselný rozklad čísla 2 (f) 60
6.7 Přirozené prvočíslo 3 v komplexní rovině 61
6.8 Prvočíselný rozklad čísla 13 (a) 61
6.9 Prvočíselný rozklad čísla 13 (b) 62
6.10 Prvočíselný rozklad čísla 13 (c) 62
6.11 Prvočíselný rozklad čísla 13 (d) 63
6.12 Prvočíselný rozklad čísla 13 (e) 63
6.13 Prvočíselný rozklad čísla 13 (f) 64
6.14 Prvočíselný rozklad čísla 13 (g) 64
6.15 Gaussovo celé číslo $z_v = 1 + i$ v komplexní rovině (1) 65
6.16 Gaussovo celé číslo $z_v = 1 + i$ v komplexní rovině (2) 66
6.17 Gaussovo celé číslo $z_v = 1 + i$ v komplexní rovině (3) 66
6.18 Gaussovo celé číslo $z_v = -4 - 5i$ v komplexní rovině (1) 67
6.19 Gaussovo celé číslo $z_v = -4 - 5i$ v komplexní rovině (2) 67
6.20 Gaussovo celé číslo $z_v = -4 - 5i$ v komplexní rovině (3) 68
6.21 Gaussovo celé číslo $z_v = 4 + 3i$ v komplexní rovině (a) 68
6.22 Gaussovo celé číslo $z_v = 4 + 3i$ v komplexní rovině (b) 69
6.23 Gaussovo celé číslo $z_v = 4 + 3i$ v komplexní rovině (c) 69
6.24 Gaussovo celé číslo $z_v = 4 + 3i$ v komplexní rovině (d) 70
6.25 Prvočísla v komplexní rovině 71

7.1 GeoGebra Book 73
7.2 Applet č. 1 74
7.3 Applet č. 2 75
7.4 Applet č. 3 75
7.5 Applet č. 4 76
7.6 Applet č. 5 (a) 77
7.7 Applet č. 5 (b) 77
7.8 Applet č. 6 78
7.9 Applet č. 7 79
7.10 Applet č. 8 80
7.11 Applet č. 9 81
7.12 Applet č. 10 81
7.13 Applet č. 11 82
7.14 Applet č. 12 82
7.15 Applet č. 13 83
7.16 Applet č. 14 84
7.17 Applet č. 15 84
7.18 Applet č. 16 85
7.19 Applet č. 17 85
7.20 Applet č. 18 86