Gaussovi cijeli brojevi

Novotny, Martina

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Martina Novotny

GAUSSOVI CIJELI BROJEVI

Diplomski rad

Voditelj rada:
izv.prof.dr.sc. Zrinka Franušić

Zagreb, 2022.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Zahvaljujem mentorici izv.prof.dr.sc. Zrinki Franušić na stručnom vodstvu, podršci i razumijevanju tijekom pisanja diplomskog rada.
Zahvaljujem svojoj obitelji, roditeljima, sestri i bratu na neizmjernoj ljubavi i strpljivoj podršci tijekom studija.
Zahvaljujem se svim prijateljima koji su učinili da vrijeme studiranja ne padne u zaborav.
I konačno, zahvaljujem zaručniku Krešimiru na svakoj riječi ohrabrenja u teškim trenutcima, vjeri u mene, gorljivim molitvama i pruženoj ljubavi.
1 Kor (13, 8-13)

Diplomski rad napravljen je u sklopu aktivnosti Projekta KK.01.1.1.01.0004 - Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Liejevih algebri.

Sadržaj

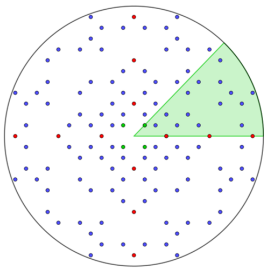
Uvod

Carl Friedrich Gauss (1777. - 1855.) bio je njemački matematičar koji je ostavio brojne doprinose u različitim područjima matematike. U monografiji *Theoria Residuorum Biquadraticorum* iz 1832. godine, Gauss je postavio temelje moderne teorije brojeva, među koje se svrstava i skup brojeva koji su njemu u čast prozvani *Gaussovi cijeli brojevi*.

U ovom diplomskom radu bavimo se Gaussovim cijelim brojevima s naglaskom na geometrijske interpretacije definicija, tvrdnji, primjera i problema koji su prikazani slikama napravljenim u matematičkom softverskom alatu *GeoGebra*. Iako su mnogi problemi Gaussovih cijelih brojeva algebarske i aritmetičke prirode, korištenje ilustracija i vizualnih interpretacija olakšava razumijevanje i poboljšava pamćenje.

Gaussovi cijeli brojevi kompleksni su brojevi oblika $a+bi$, gdje su a i b cijeli brojevi, a skup svih takvih brojeva označava se sa $\mathbb{Z}[i]$. Uz operacije zbrajanja i množenja kompleksnih brojeva, Gaussovi cijeli brojevi imaju strukturu komutativnog prstena s jedinicom. U prstenu Gaussovih cijelih brojeva možemo definirati analogne pojmove onima iz prstena cijelih brojeva. To se u prvom redu odnosi na pojam djeljivosti i pojam prostog broja. Za karakterizaciju prostosti u $\mathbb{Z}[i]$ koristi se norma Gaussovog cijelog broja $N(a+bi) = a^2+b^2$ koja ih povezuje sa sumama kvadrata cijelih brojeva. Pokazujemo da vrijede mnoge analogne tvrdnje onima iz prstena cijelih brojeva kao što su Teorem o dijeljenju s ostatkom, Euklidov algoritam, Teorem o jedinstvenoj faktorizaciji na proste djelitelje.

U radu se spominju i neki zanimljivi problemi koji uz sebe vežu još mnoga otvorena pitanja. To su, na primjer, Gaussov problem kruga i problemi vezani u distribuciju Gaussovih prostih brojeva.



Poglavlje 1

Osnovne algebarske strukture

U ovom poglavlju ponovit ćemo definicije i glavna svojstva nekih osnovnih algebarskih struktura kao što su *grupa*, *prsten* i *polje*.

Neka je G neprazan skup. Ako operacija $\cdot$ zadana na $G \times G = \{(x, y) : x, y \in G\}$ zadovoljava sljedeća svojstva:

1. *zatvorenost*:
$$x \cdot y \in G \text{ za sve } x,\ y \in G,$$
2. *asocijativnost*:
$$(x \cdot y) \cdot z = x \cdot (y \cdot z) \text{ za sve } x, y, z \in G,$$
3. postojanje *neutralnog elementa*:
$$\text{postoji } e \in G \text{ takav da je } e \cdot x = x \cdot e = x \text{ za sve } x \in G,$$
4. postojanje *inverznog elementa*:
$$\text{za svaki } x \in G \text{ postoji } y \in G \text{ takav da je } x \cdot y = y \cdot x = e,$$

onda se uređeni par $(G,\ \cdot)$ zove **grupa**.

Ako vrijedi i

5. komutativnost:
$$x \cdot y = y \cdot x \text{ za sve } x, y \in G,$$

onda se $(G,\ \cdot)$ zove **komutativna** ili **Abelova grupa**. Još kažemo da je G **grupa** (ili Abelova grupa) **s obzirom na operaciju** $\cdot$.

Uobičajeno je operaciju u grupi označiti s $\cdot$ ili $+$ pri čemu se ne misli nužno na standarno množenje ili standardno zbrajanje. U strukturi $(G, \cdot)$ često niti ne pišemo oznaku za operaciju, tj. pišemo $x \cdot y = xy$.

Neutralni element grupe G, odnosno e naziva se i **jedinica**, odnosno **nula** ako je operacija na $G \times G$ aditivna $(+)$. Lako se pokazuje: ako neutralni element postoji, on je jedinstven.

Inverz elementa $x \in G$, odnosno element za koji $x \cdot y = y \cdot x = e$ također je jedinstven. Označava se s x^{-1} ili s $-x$ u aditivnoj grupi $(G, +)$ gdje ga se zove **suprotnim** elementom od x.

Vrlo često struktura $(G, \cdot)$ ne zadovoljava sva svojstva grupe, već samo neka od njih. Ako je zadovoljeno samo svojstvo zatvorenosti operacije, onda se $(G, \cdot)$ naziva **grupoid**. Ako u grupoidu $(G, \cdot)$ vrijedi i asocijativnost, govorimo o **polugrupi**. Konačno, ako u polugrupi $(G, \cdot)$ postoji neutralni element, onda strukturu zovemo **monoidom** ili **polugrupom s jedinicom**. U slučaju kada je operacija $\cdot$ komutativna, govorimo o *komutativnom* grupoidu, *komutativnoj* polugrupi i *komutativnom* monoidu.

Neka je $(G, \cdot)$ grupa i H neprazan podskup od G. Kažemo da je H **podgrupa** od G ako je H i sam grupa u odnosu na istu binarnu operaciju $\cdot$ koja G čini grupom te pišemo $H \leq G$. Ako je H podgrupa od G lako se pokaže da to vrijedi ako i samo ako

$$x \cdot y \in H, x^{-1} \in H \ ,$$

za sve $x,\ y \in H$. Neka je R neprazan skup na kojem su definirane dvije binarne operacije $+$ i $\cdot$. Kažemo da je uređena trojka $(R, +, \cdot)$ **prsten** ako vrijedi:

1. $(R, +)$ je Abelova grupa,
2. $(R, \cdot)$ je polugrupa,
3. svojstvo distributivnosti operacije $\cdot$ obzirom na operaciju $+$:

$$x(y + z) = xy + xz, \ \ (x + y)z = xz + yz, .$$

za sve $x,\ y,\ z \in R$.

Prsten u kojem je $(R, \cdot)$ je monoid, tj. postoji neutralni element operacije $\cdot$, naziva se **prsten s jedinicom**. Ako je operacija $\cdot$ komutativna, $(R, \cdot)$ je **komutativni prsten**.

Komutativni prsten s jedinicom u kojem je svaki element različit od nule (tj. neutralnog elementa zbrajanja) invertibilan, naziva se **polje**. Uobičajeno je polje označiti s $\mathbb{F}$. Dakle, $(\mathbb{F}, +, \cdot)$ je polje ako vrijedi:

1. $(\mathbb{F}, +)$ je Abelova grupa,
2. $(\mathbb{F}\backslash\{0\}, \cdot)$ je Abelova grupa,
3. svojstvo distributivnosti operacije $\cdot$ obzirom na operaciju $+$.

Poglavlje 2

Gaussovi cijeli brojevi

2.1 Skup kompleksnih brojeva

Definicija 2.1.1. *Neka je* $\mathbb{R}\times\mathbb{R}$ *skup svih uređenih parova* (a,b) *gdje su* $a,b\in\mathbb{R}$*. Na skupu* $\mathbb{R}\times\mathbb{R}$ *definiramo operaciju zbrajanja*

$$+ : (\mathbb{R}\times\mathbb{R})\times(\mathbb{R}\times\mathbb{R}) \to \mathbb{R}\times\mathbb{R},$$

$$(a,b)+(c,d) = (a+c, b+d),\ \forall (a,b),(c,d)\in\mathbb{R}\times\mathbb{R}, \tag{2.1}$$

te operaciju množenja

$$\cdot : (\mathbb{R}\times\mathbb{R})\times(\mathbb{R}\times\mathbb{R}) \to \mathbb{R}\times\mathbb{R},$$

$$(a,b)\cdot(c,d) = (a\cdot c - b\cdot d, a\cdot d + b\cdot c),\ \forall (a,b),(c,d)\in\mathbb{R}\times\mathbb{R}. \tag{2.2}$$

Skup $\mathbb{R}\times\mathbb{R}$ *s operacijama zbrajanja (2.1) i množenja (2.2) nazivamo* ***skup kompleksnih brojeva*** *i označavamo s* $\mathbb{C}$*.*

Najprije uočimo da je

$$(1,0)\cdot(1,0) = (1,0),\ (0,1)\cdot(0,1) = (-1,0),$$

te

$$(a,b)\cdot(1,0) = (1,0)\cdot(a,b) = (a,b),$$
$$(a,b)\cdot(0,1) = (0,1)\cdot(a,b) = (-b,a),$$

za sve $(a,b)\in\mathbb{C}$. Zato je

$$(a,b) = (a,0)\cdot(1,0) + (b,0)\cdot(0,1).$$

Skup svih kompleksnih brojeva oblika $(a, 0)$, $a \in \mathbb{R}$ očito se može identificirati sa skupom realnih brojeva pa prethodnu relaciju zapisujemo kao

$$(a, b) = a \cdot 1 + b \cdot i = a + bi,$$

gdje smo kompleksni broj $(0, 1)$ označili s i, a zovemo ga **imaginarna jedinica**. Stoga skup svih komplesnih brojeva obično označavamo kao

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}, i^2 = -1\}.$$

Uz te oznake, zbrajanje dano s (2.1) i množenje dano s (2.2) dvaju kompleksnih brojeva zapisujemo kao

$$(a + bi) + (c + di) = (a + c) + (b + d)i, \tag{2.3}$$

$$(a + bi) \cdot (c + di) = (a \cdot c - b \cdot d) + (a \cdot d + b \cdot c)i. \tag{2.4}$$

Za svaki kompleksni broj $z \in \mathbb{C}$ postoje jedinstveni realni brojevi x i y za koje je

$$z = x + yi.$$

Taj prikaz naziva se **standarni** ili **algebarski zapis** kompleksnog broja z, a realni brojevi x i y su njegov **realni**, odnosno **imaginarni dio** što zapisujemo kao

$$\mathrm{Re}(z) = x, \ \mathrm{Im}(z) = y.$$

Napomena 2.1.2. *Budući da je $i^2 = i \cdot i = -1$, slijedi da je broj i jedno rješenje jednadžbe*

$$x^2 + 1 = 0.$$

Stoga se o skupu kompleksnih brojeva govori i kao proširenju *skupa realnih brojeva kako bi svaka kvadratna jednadžba imala rješenje.*

Ponekad se broj i još naziva (kvadratni) korijen *iz -1.*

Teorem 2.1.3. *Skup svih kompleksnih brojeve uz operacije zbrajanja i množenja definirane s* (2.1) *i* (2.2) *(odnosno* (2.3) *i* (2.4)*) ima strukturu polja.*

Dokaz. Operacije zbrajanja i množenja po definiciji su zatvorene, a raspisivanjem se provjeri da zadovaljavaju svojstvo komutativnosti, asocijativnosti i distributivnosti. Neutralni element zbrajanja je $(0, 0) = 0$, a množenja $(1, 0) = 1$. Suprotni element od $a + bi$ je $-a + (-b)i$, a inverzni element od $a + bi \neq 0$ je $\dfrac{a}{a^2 + b^2} + \dfrac{-b}{a^2 + b^2}i$. □

S obzirom na prethodni teorem skup $\mathbb{C}$ nazivamo **polje kompleksnih brojeva**.

2.2 Prsten Gaussovih cijelih brojeva

Definicija 2.2.1. ***Skup Gaussovih cijelih brojeva****, u oznaci* $\mathbb{Z}[i]$*, skup je svih kompleksnih brojeva kojima je realni i imaginarni dio cijeli broj, tj.*

$$\mathbb{Z}[i] = \{x + yi : x, y \in \mathbb{Z}\}.$$

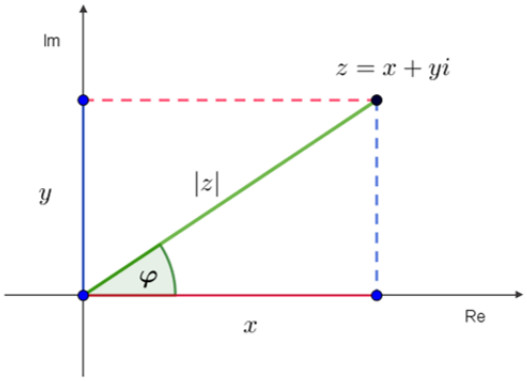
Teorem 2.2.2. *Skup svih Gaussovih cijelih brojeva uz operacije zbrajanja i množenja dane s* (2.3) *i* (2.4)*) ima strukturu komutativnog prstena s jedinicom.*

Dokaz. Očito je $(\mathbb{Z}[i], +)$ podgrupa od $(\mathbb{C}, +)$ jer je zbroj dva Gaussova cijela broja također Gaussov cijeli broj, a i suprotni element svakog Gaussovog cijelog broja je iz $\mathbb{Z}[i]$. $(\mathbb{Z}[i], \cdot)$ ima stukturu komutativnog monoida jer je umnožak dva Gaussova cijelog broja iz $\mathbb{Z}[i]$. No, lako se vidi da Gaussov cijeli broj (različit od nule) ne mora posjedovati inverz u $\mathbb{Z}[i]$. Na primjer, $(1 + i)^{-1} = \frac{1}{2} - \frac{1}{2}i \notin \mathbb{Z}[i]$. □

Skup $\mathbb{Z}[i]$ zovemo **prsten Gaussovih cijelih brojeva**.

2.3 Gaussova ravnina

Gaussova ili **kompleksna ravnina** je ravnina u kojoj prikazujemo kompleksne brojeve. Realni dio kompleksnog broja prikazujemo na osi apscisa, a imaginarni dio na osi ordinata Kartezijevog koordinatnog sustava. Dakle, kompleksni broj $z = x + yi$ prikazuje se kao točka (x, y).

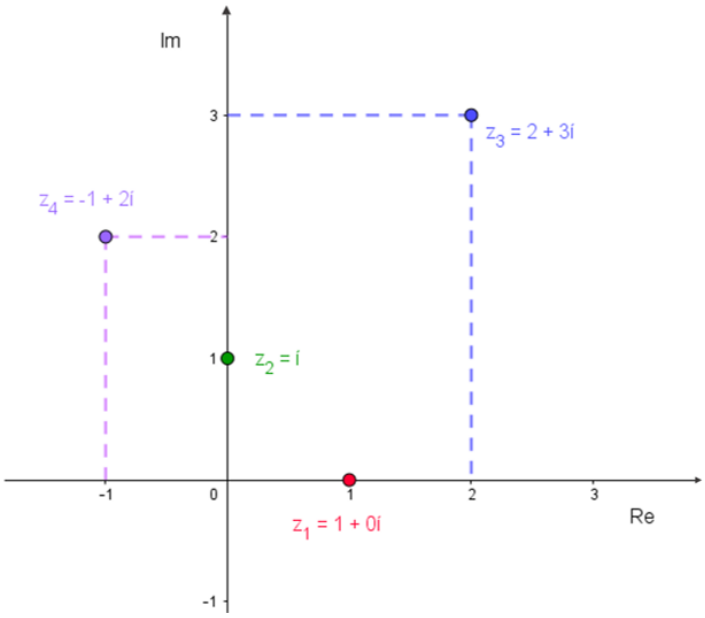


Slika 2.1: Općeniti prikaz kompleksnog broja u Gaussovoj ravnini

Primjer 2.3.1. *U Gaussovoj ravnini prikažite brojeve:*

$$z_1 = 1,\ z_2 = i,\ z_3 = 2 + 3i,\ z_4 = -1 + 2i.$$

Rješenje. Vidi sliku 2.2. □



Slika 2.2: Prikaz broja $z = x + yi$ u Gaussovoj ravnini

Apsolutna vrijednost ili **modul** kompleksnog broja $z = x + yi$ je

$$|z| = r = \sqrt{x^2 + y^2},$$

odnosno udaljenost točke (x, y) od ishodišta (slika 2.1).

Argument je kompleksnog broja z kut $\varphi \in [0, 2\pi\rangle$, u oznaci $\varphi = \arg(z)$, kojeg polupravac Oz zatvara s pozitivnim dijelom realne osi. Primjenom trigonometrije na pravokutan trokut (slika 2.1) slijedi da je

$$x = r \cdot \cos\varphi,$$

$$y = r \cdot \sin\varphi$$

pa kompleksni broj z zapisujemo u tzv. **trigonometrijskom obliku**:

$$z = r \cdot (\cos\varphi + i \sin\varphi).$$

Taj oblik još se naziva i **polarni** jer kompleksni broj u polarnom koordinatnom sustavu, određen s pozitivnim dijelom realne osi, ima koordinate (r, φ).

Napomena 2.3.1. *Modul kompleksog broja još se naziva i* euklidska norma *kompleksnog broja. Naime,* norma *je općenito preslikavanje definirano na vektorskom prostoru X (nad poljem* $\mathbb{C}$*)* $\|\cdot\| : X \to \mathbb{R}$ *sa sljedećim svojstvima:*

1. $\|x\| \geq 0,\ \forall x \in X$ *(pozitina definitnost);*
2. $\|x\| = 0 \iff x = 0$ *(strogost);*
3. $\|\alpha x\| = |\alpha| \cdot \|x\|,\ \forall \alpha \in \mathbb{C},\ \forall x \in X$ *(homogenost);*
4. $\|x + y\| \leq \|x\| + \|y\|,\ \forall x,\ y \in X$ *(nejednakost trokuta).*

Uređeni par $(X, \|\cdot\|)$ *naziva se normiranim prostorom.*

Očito je da modul kompleksnog broja zadovoljava prva tri svojstva norme. Pokažimo da vrijedi i četvrto svojstvo – nejednakost trokuta. Za $z, w \in \mathbb{C}$ *vrijedi*

$$|z + w|^2 = (z + w)(\overline{z} + \overline{w}) = |z|^2 + 2\,\mathrm{Re}(z\overline{w}) + |w|^2 \leq |z|^2 + 2|z||w| + |w|^2 = (|z| + |w|)^2,$$

pa je $|z + w| \leq |z| + |w|$.

2.4 Računske operacije u Gaussovoj ravnini

Zbrajanje

Kompleksni brojevi zbrajaju se prema (2.3) na način da se posebno zbroje realni dijelovi, a posebno imaginarni. U Gaussovoj ravnini zbrajanje kompleksnih brojeva može se interpetirati kao zbrajanje odgovarajućih radijvektora. Konkretno, ako su kompleksni brojevi $z_1 = a + bi$ i $z_2 = c + di$ u kompleksnoj ravnini označeni točkama $T_1(a, b)$ i $T_2(c, d)$, tada kompleksni broj $z_1 + z_2$ pripada točki $T(a + c, b + d)$ za koju vrijedi

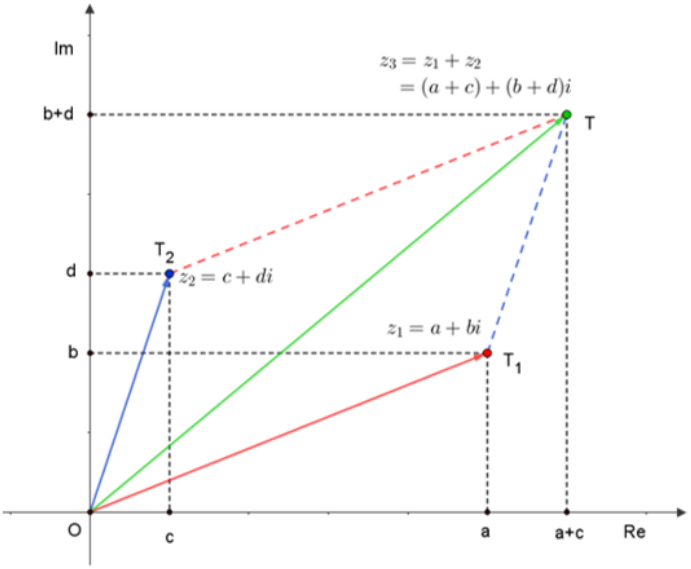
$$\overrightarrow{OT} = \overrightarrow{OT_1} + \overrightarrow{OT_2}.$$

Na slici 2.3 prikazana je geometrijska interpretacija kompleksnih brojeva kao zbrajanje dvaju vektora prema pravilu paralelograma.

Množenje

Najprije uočimo da se množenje kompleksnog broja $z = a + bi$ imaginarnom jedinicom u kompleksnoj ravnini realizira kao rotacija oko ishodišta za 90°:

$$z \cdot i = (a + bi) \cdot i = -b + ai.$$



Slika 2.3: Zbrajanje kompleksnih brojeva u Gaussovoj ravnini

Zaista, tangens kuta α_1 kojeg polupravac Oz zatvara s pozitivnim dijelom realne osi je $\frac{b}{a}$, a tangens kuta α_2 kojeg polupravac Oz_1 ($z_1 = z \cdot i$) zatvara s pozitivnim dijelom realne osi je $-\frac{a}{b}$ pa je kut između ova dva polupravca jednak 90° jer je $1 + \frac{b}{a} \cdot \left(-\frac{a}{b}\right) = 0$.

Nadalje, množenjem s $i^2 = -1$, z rotira oko ishodišta za 180°, a množenjem s $i^3 = -i$ za 270°,

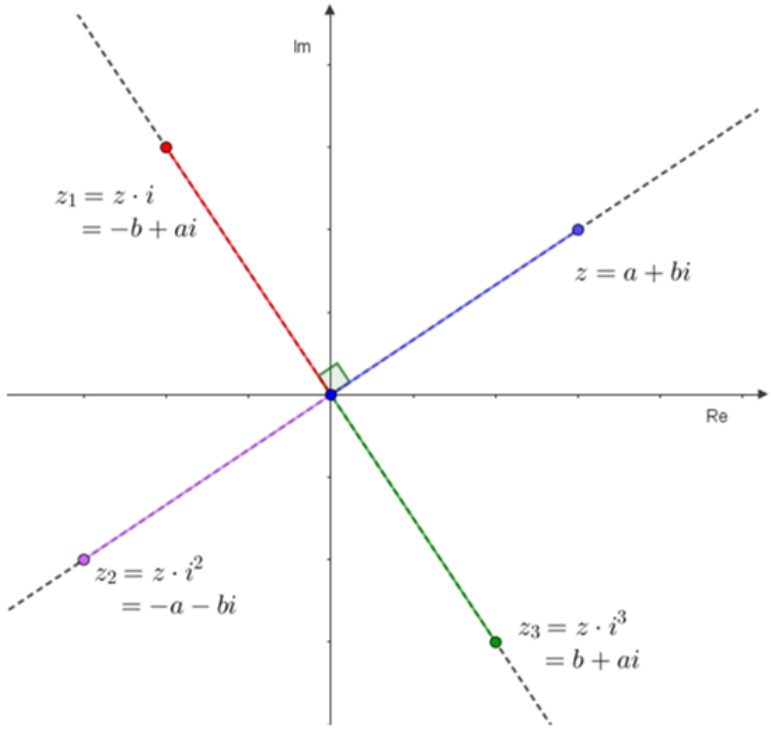
$$z \cdot i^2 = -a + bi,\ z \cdot i^3 = b - ai.$$

Da bismo geometrijski razumijeli množenje bilo koja dva kompleksna broja, potrebni su nam trigonometrijski zapisi tih kompleksnih brojeva. Ako su $z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1)$ i $z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$, tada je njihov umnožak jednak

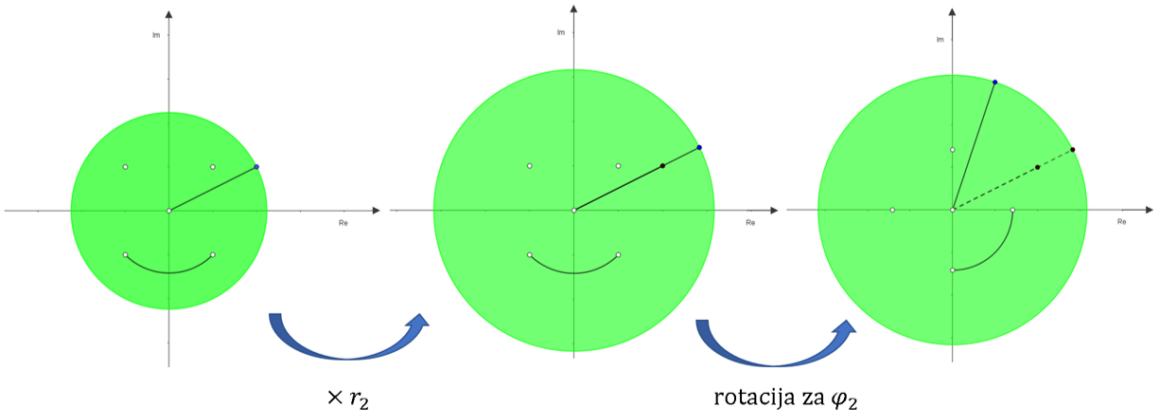
$$\begin{aligned} z_1 \cdot z_2 &= r_1(\cos\varphi_1 + i\sin\varphi_1) \cdot r_2(\cos\varphi_2 + i\sin\varphi_2) \\ &= r_1 \cdot r_2(\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2 + i(\sin\varphi_1\cos\varphi_2 + \cos\varphi_1\sin\varphi_2) \\ &= r_1 \cdot r_2(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)), \end{aligned}$$

pri čemu posljednja jednakost slijedi iz adicijskih formula za sinus i kosinus.

Na slici 2.5 prikazano je množenje dva kompleksna broja u dva koraka. U prvom koraku broj z_1, odnosno vektor $\overrightarrow{OT_1}$ skaliramo modulom broja z_2, a u drugom ga rotiramo za argument od z_2.

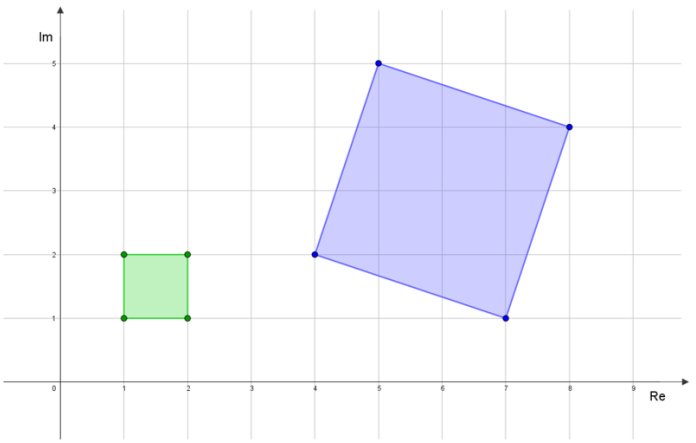


Slika 2.4: Množenje kompleksnog broja imaginarnom jedinicom



Slika 2.5: Množenje kompleksnim brojem

Primjer 2.4.1. *Kompleksni brojevi koji se nalaze u vrhovima zelenog kvadrata površine jedan pomnoženi su sa $z = 3-i$. Pomnoženi brojevi nalaze se ponovno u vrhovima kvadrata koji je zarotiran za argument od z i skaliran za modul broja z (slika 2.6).*



Slika 2.6: Višekratnici kompleksnog broja

Općenito, vrijedi da se višekratnici Gaussovih cijelih brojeva raspoređuju u ravnini na način da čine pravilnu kvadratnu mrežu.

Konjugiranje

Definicija 2.4.1. ***Konjugirano kompleksni broj*** *od $z = x + yi$, $x, y \in \mathbb{R}$ definira se izrazom*

$$\overline{z} = x - yi\ . \tag{2.5}$$

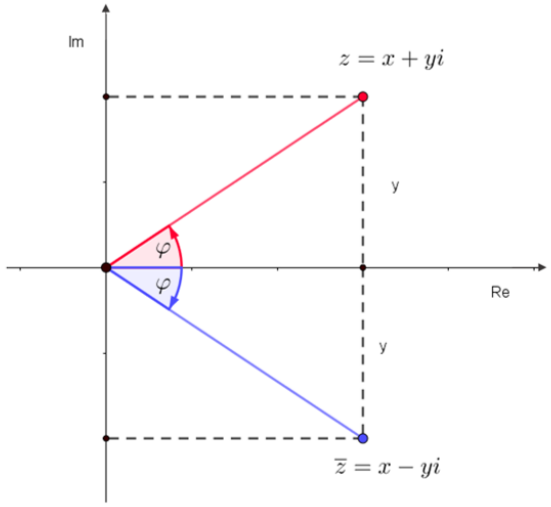
U Gaussovoj ravnini konjugirano kompleksni broj prikazan je točkom koja je simetrična s obzirom na os apscisa. Apsolutna vrijednost broja ostaje ista, a kut je po mjeri isti, ali ako se promatra u suprotnom smjeru od dogovorenog (tj. u smjeru kazaljke na satu).

Propozicija 2.4.2. *Za sve kompleksne brojeve z i w vrijedi:*

$$\overline{z} + \overline{w} = \overline{z + w}$$

$$\overline{z} - \overline{w} = \overline{z - w}$$

$$\overline{z} \cdot \overline{w} = \overline{zw}.$$



Slika 2.7: Kompleksno konjugiran broj u Gaussovoj ravnini

Dokaz. Neka su $z = a + bi$ i $w = c + di$, $a, b, c, d \in \mathbb{R}$. Tada

$$\overline{z} + \overline{w} = (a - bi) + (c - di) = (a + c) - (b + d)i = \overline{(a + c) + (b + d)i} = \overline{x + w}.$$

Analogno bismo dokazali i ostala svojstva iz propozicije 2.4.2. □

Propozicija 2.4.3. *Modul kompleksnog broja jednak je umnošku tog kompleksnog broja i njegovog konjugata, to jest*

$$|z|^2 = z \cdot \overline{z}.$$

Dokaz. Neka je $z = a + bi$ i $\overline{z} = a - bi$, tada računamo

$$z \cdot \overline{z} = (a + bi)(a - bi) = a^2 - abi + abi - b^2(i \cdot i) = a^2 + b^2 = |z|^2.$$

□

2.5 Norma Gaussovog cijelog broja

Definicija 2.5.1. *Neka je $z = a + bi \in \mathbb{Z}[i]$.* ***Norma Gaussovog cijelog broja*** *broja z definira se s*

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

Norma Gaussovog cijelog broja zapravo je kvadrat modula kompleksnog broja. Razlog zašto se radije bavimo normama na $\mathbb{Z}[i]$ umjesto apsolutnim vrijednostima na $\mathbb{Z}[i]$ je taj što

su norme nenegativni cijeli brojevi (a ne kvadratni korijeni), a svojstva djeljivosti normi u $\mathbb{N}_0$ pružit će važne informacije o svojstvima djeljivosti u $\mathbb{Z}[i]$. Ovo se temelji na sljedećem algebarskom svojstvu norme.

Teorem 2.5.2. *Neka su* $z_1,\ z_2 \in \mathbb{Z}[i]$. *Tada vrijedi*

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

odnosno norma je multiplikativna.

Dokaz. Neka su $z_1 = a + bi$ i $z_2 = c + di$, $a, b, c, d \in \mathbb{Z}$. Tada je njihov umnožak jednak

$$z_1 \cdot z_2 = (a \cdot c - b \cdot d) + (a \cdot d + b \cdot c)i. \tag{2.6}$$

Računamo sada $N(z_1) \cdot N(z_2)$ i $N(z_1 \cdot z_2)$:

$$N(z_1) \cdot N(z_2) = (a^2 + b^2)(c^2 + d^2) = (ac)^2 + (ad)^2 + (bc)^2 + (bd)^2 \tag{2.7}$$

i

$$\begin{aligned} N(z_1 \cdot z_2) &= (a \cdot c - b \cdot d)^2 + (a \cdot d + b \cdot c)^2 \\ &= (ac)^2 - 2abcd + (bd)^2 + (ad)^2 + 2abcd + (bc)^2 \\ &= (ac)^2 + (ad)^2 + (bc)^2 + (bd)^2. \end{aligned} \tag{2.8}$$

Iz (2.7) i (2.8) slijedi da je $N(z_1 \cdot z_2) = N(z_1) \cdot N(z_2)$. □

Napomena 2.5.3. *Jasno je da prethodni teorem vrijedi i za sve kompleksne brojeve, tj.* $N(z_1z_2) = N(z_1)N(z_2)$ *za sve* $z_1, z_2 \in \mathbb{C}$.

Nadalje, prethodni teorem povlači i da je

$$|z_1||z_2| = |z_1z_2|,\ \forall z_1, z_2 \in \mathbb{C}.$$

Norma svakog Gaussovog cijelog broja je nenegativan cijeli broj, ali nije točno da je svaki nenegativan cijeli broj norma nekog Gaussovog cijelog broja. Naime, norma Gaussovog cijelog broja oblika je $a^2 + b^2$, a postoje brojevi koji se ne mogu prikazati suma dva kvadrata cijelih brojeva. Na primjer, ne postoje Gaussovi cijeli brojevi čija je norma jednaka 3 ili 7. Općenito se prirodan broj može prikazati u obliku sume kvadrata dva cijela broja ako i samo ako mu se u rastavu na proste faktore svi prosti brojevi oblika $4k + 3$ pojavljuju s parnom potencijom. O tome će još biti govora u sljedećim poglavljima (npr. vidjeti teorem 4.2.8).

2.6 Dijeljenje kompleksnih brojeva

Kompleksne brojeve možemo dijeliti koristeći se postupkom analognom onom kod racionalizacije iracionalnih izraza pri čemu ćemo se sada koristiti kompleksno konjugiranim brojevima. Neka su $z_1 = a + bi$ i $z_2 = c + di \neq 0$ kompleksni brojevi, tada njihov kvocijent računamo na sljedeći način:

$$\frac{z_1}{z_2} = \frac{a+bi}{c+di} \cdot \frac{c-di}{c-di} = \frac{(a+bi)(c-di)}{c^2+d^2} = \frac{(ac+bd)}{c^2+d^2} + \frac{(bc-ad)}{c^2+d^2} i. \tag{2.9}$$

Analogno kao za množenje dva kompleksna broja, možemo promatrati kvocijent dva kompleksna broja zapisana u trigonometrijskom obliku. Ako je

$$z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1),\ z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2),\ r_2 \neq 0,$$

onda prema (2.9) i adicijskim formulama za sinus i kosinus imamo

$$\begin{aligned} \frac{z_1}{z_2} &= \frac{r_1 r_2(\cos\varphi_1\cos\varphi_2 + \sin\varphi_1\sin\varphi_2)}{r_2^2} + \frac{(\sin\varphi_1\cos\varphi_2 - \cos\varphi_1\sin\varphi_2)}{r_2^2} i \\ &= \frac{r_1}{r_2}\left(\cos(\varphi_1-\varphi_2) + i\sin(\varphi_1-\varphi_2)\right). \end{aligned}$$

Iz gornjih formula jasno je da kvocijent dva Gaussova cijela broja ne mora uvijek biti Gaussov cijeli broj (npr. $\frac{2+3i}{1-2i} = -\frac{4}{5} + \frac{7}{5}i \notin \mathbb{Z}[i]$).

Poglavlje 3

Dijeljenje u prstenu Gaussovih cijelih brojeva

3.1 Djeljivost u $Z[i]$

Definicija 3.1.1. *Neka su $z_1, z_2 \in Z[i]$ i $z_2 \neq 0$. Kažemo da z_2 **dijeli** z_1, odnosno da je z_1 **djeljiv** sa z_2, ako postoji broj $w \in Z[i]$ takav da je $z_1 = w \cdot z_2$.*

Oznake: $z_2 \mid z_1$ (ako z_2 dijeli z_1), odnosno $z_2 \nmid z_1$ (ako z_2 ne dijeli z_1).

Propozicija 3.1.2. *Ako $z_2 \mid z_1$ i $z_1 \neq 0$, tada je $|z_2| \leq |z_1|$.*

Dokaz. Budući da je $z_2 \mid z_1$, postoji $w \in \mathbb{Z}[i]$ takav da je $z_1 = z_2 w$. Nadalje, $w \neq 0$ jer je $z_1 \neq 0$ i zato je $|w| \geq 1$. Stoga,

$$|z_2| = |z_2| \cdot 1 \leq |z_2| \cdot |w| = |z_1|.$$

□

Primjer 3.1.1. *Broj $14 - 5i$ djeljiv je s $3 - 2i$, ali nije djeljiv s $2 + 2i$. Zaista,*

$$\frac{14 - 5i}{3 - 2i} = \frac{(14 - 5i)(3 + 2i)}{(3 - 2i)(3 + 2i)} = \frac{52 + 13i}{13} = 4 + i \in \mathbb{Z}[i],$$

no

$$\frac{14 - 5i}{2 + 2i} = \frac{(14 - 5i)(2 - 2i)}{(8)} = \frac{18 - 38i}{18} = \frac{9}{4} - \frac{19}{4} i \notin \mathbb{Z}[i].$$

U nastavku ćemo pokazati je li baš uvijek potrebno dijeliti dva Gaussova cijela broja da bi se ispitala djeljivost.

Teorem 3.1.3. *Broj $\alpha \in \mathbb{Z}$, $\alpha \neq 0$, dijeli broj $z = a + bi \in \mathbb{Z}[i]$ ako i samo $\alpha \mid a$ i $\alpha \mid b$ u $\mathbb{Z}$.*

Dokaz. Broj α dijeli z ako i samo ako je $a+bi = \alpha(c+di)$ za neke $c, d \in \mathbb{Z}$. Izjednačavanjem realnih i imaginarnih dijelova dobivamo da je $a = \alpha c$ i $b = \alpha d$, tj. $\alpha \mid a$ i $\alpha \mid b$. □

Teorem 3.1.4. *Neka su $z_1, z_2 \in \mathbb{Z}[i]$, $z_2 \neq 0$. Ako $z_2 \mid z_1$ u $\mathbb{Z}[i]$, onda $N(z_2) \mid N(z_1)$ u $\mathbb{Z}$.*

Dokaz. Kako $z_2 \mid z_1$, postoji $w \in \mathbb{Z}[i]$ takav da $z_1 = wz_2$. Otuda je $N(z_1) = N(wz_2)$. S obzirom na to da je norma multiplikativna (teorem 2.5.2) slijedi

$$N(z_1) = N(w)N(z_2),$$

a to znači da $N(z_2) \mid N(z_1)$ u $\mathbb{Z}$ (jer je norma Gaussovog cijelog broja nenegativan cijeli broj). □

Prethodni teorem je od koristi kada želimo ustanoviti da z_2 ne dijeli z_1. Iz primjera 3.1.1: $N(14 - 5i) = 221$ ne dijeli $N(2 + 2i) = 8$, pa $2 + 2i \nmid 14 - 5i$. Tu smo primijenili obrat po kontrapoziciji tvrdnje iz teorema 3.1.4, što možemo općenito zapisati kao:

Korolar 3.1.5. *Neka su $z_1, z_2 \in \mathbb{Z}[i]$, $z_2 \neq 0$. Ako $N(z_2) \nmid N(z_1)$ u $\mathbb{Z}$, onda $z_2 \nmid z_1$ u $\mathbb{Z}[i]$.*

Važno je napomenuti da obrat teorema 3.1.4 ne vrijedi.

Primjer 3.1.2. *Broj $3 + 2i$ ne dijeli $14 - 5i$ jer je*

$$\frac{14 - 5i}{3 + 2i} = \frac{32}{13} - \frac{43}{13}i.$$

No $N(14 - 5i) = 221$ je djeljivo s $N(3 + 2i) = 13$ ($221 = 13 \cdot 17$).

U svakom prstenu s jedinicom smisleno je govoriti o tzv. invertibilnim elementima. Gaussov cijeli broj z je *invertibilan* u $\mathbb{Z}[i]$ ako postoji $w \in \mathbb{Z}[i]$ takav da je $zw = wz = 1$. Broj w nazivamo *multiplikativni inverz* od z u $\mathbb{Z}[i]$ i označavamo sa z^{-1}.

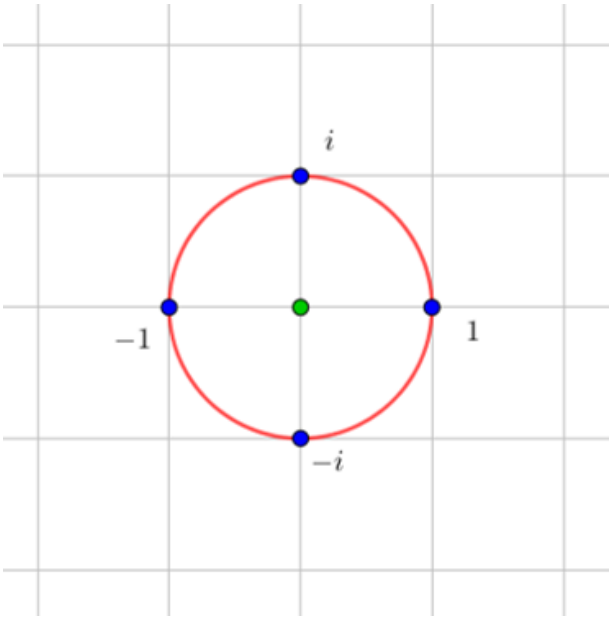
Propozicija 3.1.6. *Gaussov cijeli broj z je invertibilan u $\mathbb{Z}[i]$ ako i samo ako je $N(z) = 1$.*

Dokaz. Ako je $z \in \mathbb{Z}[i]$ invertibilan, onda je $zw = 1$ za neki $w \in \mathbb{Z}[i]$. Prema teoremu 2.5.2 je $N(z)N(w) = 1$ pa je $N(z) = N(w) = 1$ jer su $N(z), N(w) \in \mathbb{N}$.

Obratno, ako je $N(z) = 1$, onda vrijedi $z\bar{z} = 1$. Kako je $\bar{z} \in \mathbb{Z}[i]$, zaključujemo da je z invertibilan u $\mathbb{Z}[i]$ i $z^{-1} = \bar{z}$. □

Korolar 3.1.7. *Skup svih invertibilnih elementata u prstenu Gaussovih cijelih brojeva je $\{1, -1, i, -i\}$.*

Dokaz. Prema propoziciji 3.1.6 $z = a + bi \in \mathbb{Z}[i]$ je invertibilan u $\mathbb{Z}[i]$ ako i samo ako je $a^2 + b^2 = 1$. Jedina rješenja ove jednadžbe u $\mathbb{Z}$ su $(a, b) \in \{(1, 0), (-1, 0), (0, 1), (0, -1)\}$ i ona odgovaraju brojevima $1, -1, i, -i$. □



Slika 3.1: Invertibilni Gaussovi cijeli brojevi

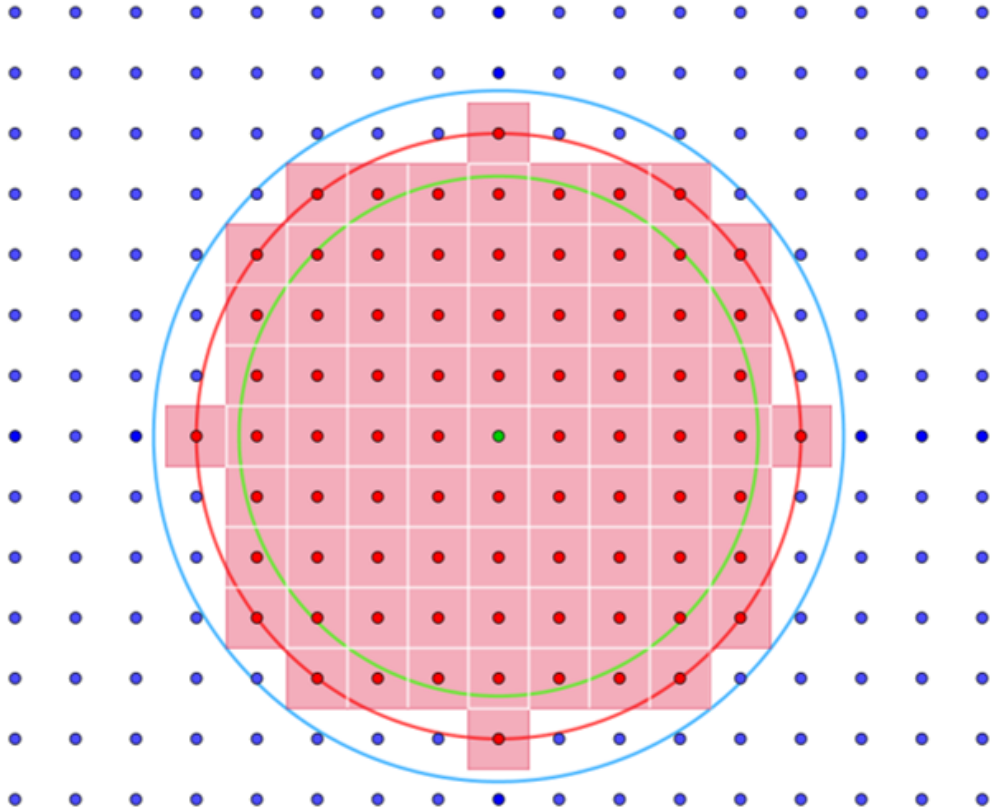
Na slici 3.1 plavim točkama prikazani su jedini Gaussovi cijeli brojevi koji su invertibilni. Spomenute točke leže na kružnici radijusa 1 sa središtem u nuli. Unutar te kružnice ne postoji niti jedan Gaussov cijeli broj različit od nule. To nas navodi na pitanje koliko Gaussovih cijelih brojeva leži na krugu radijusa r oko nule. Ono se svodi na određivanje broja rješavanja nejednadžbe

$$a^2 + b^2 \leq r^2$$

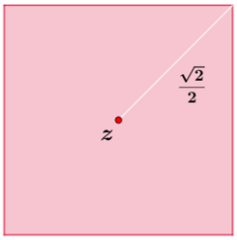
u prstenu cijelih brojeva $\mathbb{Z}$. No, ideja je taj broj aproksimirati površinom kružnice i što točnije ograničiti pogrešku – razliku broja točaka unutar kruga i površine kruga. Taj se problem još naziva i *problem Gaussovog kruga*.

Na slici 3.2 crvenom bojom označena je kružnica radijusa $r = 5$, a crvenim točkama označeni su Gaussovi cijeli brojevi z koji leže na toj kružnici i unutar nje, tj. oni za koje je $|z| \leq r$. Nadalje, oko svake crvene točke, tj. oko svakog Gaussovog cijelog broja koji leži na zadanom krugu nacrtan je kvadrat površine 1 čije su stranice paralelne s koordinatnim osima. Gaussov cijeli broj nalazi se u središtu kvadrata, a udaljenost do vrhova jednaka je duljini pola dijagonale, odnosno $\frac{\sqrt{2}}{2}$ (slika 3.3). Zelenom bojom označena je kružnica radijusa $r - \frac{\sqrt{2}}{2}$, a plavom ona radijusa $r + \frac{\sqrt{2}}{2}$.

Označimo s $G(r)$ broj Gaussovih cijelih brojeva koji leže na krugu radijusa r. Površina lika koji se sastoji od svih kvadratića čija središta leže na krugu radijusa r jednaka je $G(r) \cdot 1 = G(r)$. Nadalje, ta je površina manja ili jednaka od površine kruga radijusa $r + \frac{\sqrt{2}}{2}$, a veća ili jednaka od površine kruga radijusa $r - \frac{\sqrt{2}}{2}$ (primjetimo da je krug sa zelenom



Slika 3.2: Gaussovi cijeli brojevi na krugu radijusa $r = 5$



Slika 3.3: Kvadrat površine 1 oko Gaussovog cijelog broja z

kružnicom čitav pokriven kvadratima, a svi kvadrati leže na krugu s plavom kružnicom).

Uspoređivanjem površina navedenih likova imamo:

$$\pi\left(r-\frac{\sqrt{2}}{2}\right)^2 \leq G(r) \leq \pi\left(r+\frac{\sqrt{2}}{2}\right)^2,$$

$$\pi r^2 - \pi\sqrt{2}r + \frac{\pi}{2} \leq G(r) \leq \pi r^2 + \pi\sqrt{2}r + \frac{\pi}{2},$$

$$-\pi\sqrt{2}r + \frac{\pi}{2} \leq G(r) - \pi r^2 \leq \pi\sqrt{2}r + \frac{\pi}{2}.$$

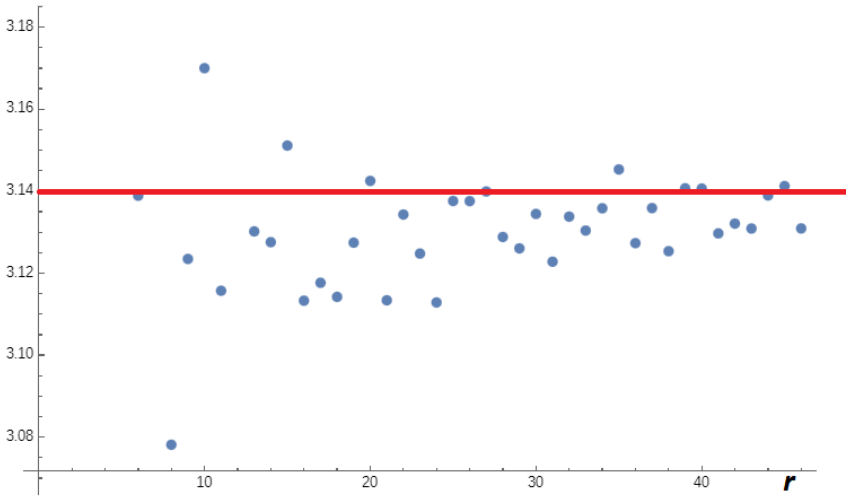
Iz zadnje nejednakosti slijedi

$$|G(r) - \pi r^2| \leq \pi\sqrt{2}\cdot r + \frac{\pi}{2},$$

što znači da smo tzv. pogrešku aproksimacije broja Gaussovih cijelih brojeva koji leže na krugu radijusa r s površinom kružinice, tj.

$$E(r) = |G(r) - \pi r^2|$$

ograničili linearnom funkcijom u r ($r \mapsto \pi\sqrt{2}\cdot r + \frac{\pi}{2}$). Ipak, sluti se da je pogreška $E(r)$ bitno manja i da se može ograničiti funkcijom koja sporije raste od linearne funkcije (približno s $\sqrt{r}$).



Slika 3.4: Graf $r \mapsto G(r)/r^2$ za $r = 1, 2, \ldots, 46$

Slutnja 3.1.8 (Gaussov problem kruga)**.** *Za svaki pozitivni realni broj ε, postoji konstanta $K_\varepsilon > 0$ za koju je*

$$|G(r) - \pi r^2| \leq K_\varepsilon r^{\frac{1}{2}+\varepsilon},$$

za $r > 0$.

r	1	2	3	4	5	6	7	8	9	10	11	12
$G(r)$	5	13	29	49	81	113	149	197	253	317	377	441
πr^2	3.1	12.6	28.3	50.3	78.5	113.1	153.9	201.1	254.5	314.2	380.1	452.4

Tablica 3.1: Aproksimacija broja $G(r)$ s površinom kruga radijusa r

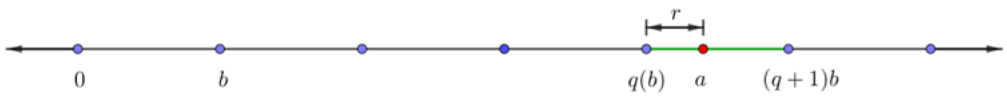
3.2 Dijeljenje s ostatkom

Teorem 3.2.1. (Teorem o dijeljenju s ostatkom). *Za proizvoljan prirodan broj b i cijeli broj a postoje jedinstveni cijeli brojevi q i r takvi da je*

$$a = qb + r \ \ i \ \ 0 \leq r < b.$$

Dokaz. Promatramo skup $B = \{a - bm : m \in \mathbb{Z}\}$. Označimo s r najmanji nenegativni član skupa B. Tada je po definiciji $0 \leq r < b$ i postoji $q \in \mathbb{Z}$ takav da je $a - qb = r$, odnosno $a = qb + r$. Jedinstvenost od $q,\ r$ pokazujemo tako da pretpostavimo da postoji još jedan par $q_1,\ r_1$ koji zadovoljavaju iste uvjete. Pretpostavimo da je $r < r_1$. Tada $0 < r_1 - r < b$, ali istovremeno i $r_1 - r = b(q - q_1) \geq b$. Prema tome $r_1 = r$, pa je i $q_1 = q$. □

Teorem 3.2.1 možemo interpretirati na geometrijski način. Višekratnici od b dijele brojevnu crtu na intervale duljine b. Kvocijent q govori o tome u kojem se intervalu nalazi a, a ostatak r gdje se u tom intervalu nalazi a (slika 3.5). Slično, ako je $b \in \mathbb{Z}[i]$ različit



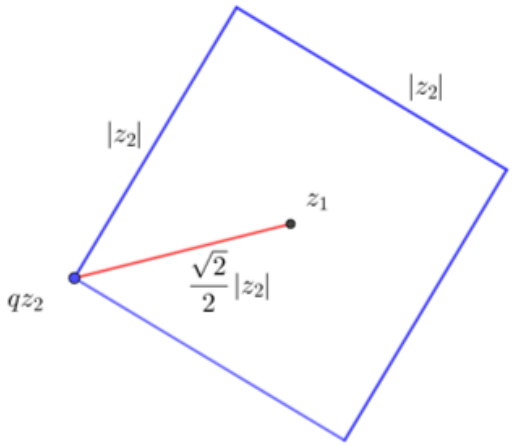
Slika 3.5: Geometrijska interpretacija teorema o dijeljenju s ostatkom u $\mathbb{Z}$

od nule, tada višekratnici od b dijele Gaussovu ravninu na kvadrate stranice duljine $|b|$. Ako želimo analogiju s prstenom cijelih brojeva, onda bi se izraz $a = qb + r$ u $\mathbb{Z}[i]$ trebao intrepretirati na način da q govori u kojem se kvadratu a nalazi, a r gdje se a nalazi unutar kvadrata (slika 3.6).

Teorem 3.2.2. *Neka su $z_1,\ z_2 \in \mathbb{Z}[i]$ i $z_2 \neq 0$. Tada postoje $q,\ r \in \mathbb{Z}[i]$ takvi da vrijedi*

$$z_1 = qz_2 + r \ \ i \ |r| \leq \frac{\sqrt{2}}{2}|z_2|.$$

Dokaz. Višekratnici broja z_2 dijele ravninu na kvadrate kojima je duljina stranica jednaka $|z_2|$. Neka je qz_2 višekratnik od z_2 koji je najbliže točki z_1. Tada je z_1 element kvadrata s vrhom qz_2, a najveća udaljenost od qz_2 do z_1 jednaka je duljini pola dijagonale, to jest $\frac{\sqrt{2}}{2}|z_2|$ (slika 3.6). Sada je $r = z_1 - qz_2$, pa prema tome slijedi da je $z_1 = qz_2 + r$, i $|r|$ je udaljenost između z_1 i qz_2 takva da $|r| \leq \frac{\sqrt{2}}{2}|z_2|$. □



Slika 3.6: Geometrijska interpretacija teorema o dijeljenju s ostatkom u $\mathbb{Z}[i]$

Razumljivo se pitati kako efektivno pronaći kvocijent i ostatak pri dijeljenju dva Gaussova cijela broja. Jedan od pristupa je geometrijski (kao iz dokaza teorema 3.2.2), a za drugi – algebarski pristup treba nam varijanta teorema o dijeljenju s ostatkom:

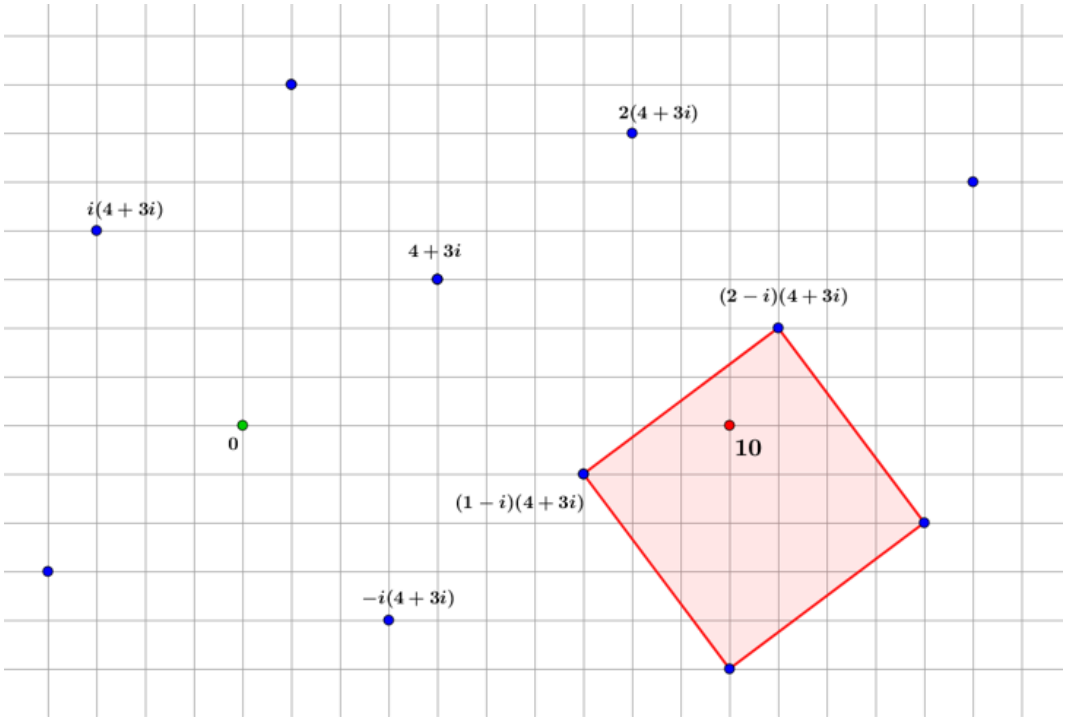
Teorem 3.2.3. *Za $a \in \mathbb{Z}$ i $b \in \mathbb{N}$ postoje jedinstveni cijeli brojevi q i r takvi da je*

$$a = qb + r \;\; i \;\; |r| < b.$$

Primjer 3.2.4. *Pronađite kvocijent i ostatak pri dijeljenju 10 s $4 + 3i$ koji zadovoljavaju teorem 3.2.2.*

Rješenje. Potrebno je pronaći $q,\ r \in \mathbb{Z}[i]$ takvi da $10 = q(4 + 3i) + r$ i $|r|$ bude što manji mogući, tj. $|r| \leq \frac{\sqrt{2}}{2}|4 + 3i|$. Najbliži višekratnik do 10 je $(2 - i)(4 + 3i)$, odnosno $q = 2 - i$ pa je $r = -1 - 2i$. Provjerimo još zadovoljava li novi r uvjete teorema 3.2.2

$$|r| = \sqrt{5} \approx 2.236,\ \frac{\sqrt{2}}{2}|4 + 3i| = \frac{\sqrt{2}}{2}5 \approx 3.536.$$



Slika 3.7: Geometrijska interpretacija teorema o dijeljenju s ostatkom u $\mathbb{Z}[i]$

Ostatak zadovoljava uvjete pa konačno možemo zapisati

$$10 = (2 - i)(4 + 3i) + (-1 - 2i).$$

Sada pogledajmo što dobijemo kad standarnim postupkom podijelimo dane brojeve,

$$\frac{10}{4 + 3i} = \frac{10(4 - 3i)}{(4 + 3i)(4 - 3i)} = \frac{8}{5} - \frac{6}{5}i. \tag{3.1}$$

Na brojeve 8 i 5 te -6 i 5 primijenimo teorem 3.2.3 o dijeljenju s ostatkom u $\mathbb{Z}$:

$$8 = 2 \cdot 5 - 2,$$

$$-6 = (-1) \cdot 5 - 1.$$

Uvrštavanjem u (3.3) dobivamo

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

te množenjem prethodne jednakosti s $4 + 3i$ slijedi

$$10 = (2 - i)(4 + 3i) + \frac{4 + 3i}{5}(-2 - i) = (2 - i)(4 + 3i) + (-1 - 2i).$$

Možemo se pitati što bismo dobili kad bismo na brojeve 8 i 5 te -6 i 5 primijenili *standarni* teorem 3.2.1 o dijeljenju s ostatkom u $\mathbb{Z}$:

$$8 = 1 \cdot 5 + 3,$$

$$-6 = (-2) \cdot 5 + 4.$$

Uvrštavanjem u (3.3) dobivamo

$$\frac{10}{4+3i} = \frac{1}{5}\left(1 \cdot 5 + 3 + ((-2) \cdot 5 + 4)i\right).$$

Otuda je

$$10 = (1-2i)(4+3i) + \frac{4+3i}{5}(3+4i) = (1-2i)(4+3i) + 5i.$$

Ostatak dobiven na ovaj način ($5i$) očito ne zadovoljava uvjete teorema 3.2.2. □

Primjer 3.2.1. *Pronađite kvocijent i ostatak pri dijeljenju 10 s 4.*

Dokaz. U skupu $\mathbb{Z}$ dani primjer ima jedinstveno rješenje koje glasi

$$10 = 4 \cdot 2 + 2,$$

budući da po teoremu 3.2.1 slijedi da ostatak mora biti nenegativni cijeli broj. Međutim, 10 smo mogli zapisati i na drugačiji način

$$10 = 4 \cdot 3 - 2,$$

pri čemu je sada ostatak negativan. Ako pogledamo u višekratnike u Gaussovoj ravnini na slici 3.8 i gdje se nalazi broj 10, uočavamo da se nalazi na polovištu između brojeva $4 \cdot 2$ i $4 \cdot 3$ pa i ostatak 2 i ostatak -2 zadovoljavaju uvjete teorema 3.2.2. Ovakav zaključak nas navodi da teorem o dijeljenju s ostatkom u $\mathbb{Z}[i]$ nema jedinstven kvocijent i ostatak. □

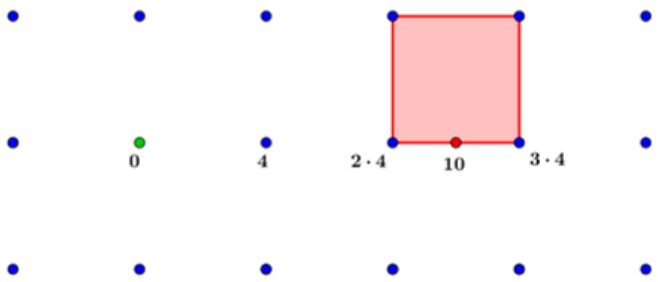
Teorem 3.2.5. *Neka su $z_1,\ z_2 \in \mathbb{Z}[i]$ i $z_2 \neq 0$. Tada postoje $q,\ r \in \mathbb{Z}[i]$ takvi da*

$$z_1 = qz_2 + r \ \ i\ N(r) < N(z_2).$$

Štoviše, $N(r) < \frac{1}{2}N(z_2)$.

Dokaz. Standardnim putem podijelimo z_1 sa z_2

$$\frac{z_1}{z_2} = \frac{z_1\overline{z_2}}{z_2\overline{z_2}} = \frac{x+yi}{N(z_2)}, \tag{3.2}$$



Slika 3.8: Geometrijska interpretacija teorema o dijeljenju s ostatkom u $\mathbb{Z}[i]$

gdje je produkt $z_1\overline{z_2}$ jednak $x + yi \in \mathbb{Z}[i]$. Nadalje, brojeve x i y podijelimo s $N(z_2)$ koristeći se teoremom o dijeljenju s ostatkom 3.2.1.

$$x = N(z_2)q_1 + r_1, \quad y = N(z_2)q_2 + r_2, \tag{3.3}$$

gdje su q_1 i q_2 kvocijenti u $\mathbb{Z}$, a r_1 i r_2 ostatci za koje vrijedi

$$0 \leq r_i < \frac{1}{2}N(z_2), \quad i \in \{1,\ 2\}. \tag{3.4}$$

U jednadžbu (3.2) uvrstimo dobivene izraze iz (3.4)

$$\frac{z_1}{z_2} = \frac{N(z_2)q_1 + r_1 + (N(z_2)q_2 + r_2)i}{N(z_2)} = q_1 + q_2 i + \frac{r_1 + r_2 i}{N(z_2)}.$$

Neka je $w = q_1 + q_2 i$. Nastavljamo računati dalje

$$\begin{aligned} \frac{z_1}{z_2} &= w + \frac{r_1 + r_2 i}{z_2\overline{z_2}} \quad / \cdot z_2\ , \\ z_1 &= z_2 w + \frac{r_1 + r_2 i}{\overline{z_2}}, \\ z_1 - z_2 w &= \frac{r_1 + r_2 i}{\overline{z_2}}. \end{aligned} \tag{3.5}$$

Pokažimo sada da je $N(z_1 - z_2 w) \leq \frac{1}{2}N(z_2)$ tako da djelujemo normom na jednadžbu (3.5) i pri tome koristimo svojstvo norme da je $N(\overline{z_2}) = N(z_2)$

$$N(z_1 - z_2 w) = \frac{{r_1}^2 + {r_2}^2}{N(z_2)}.$$

Sada koristimo omeđenost koju smo dobili u (3.4)

$$N(z_1 - z_2 w) \leq \frac{\frac{1}{4}N(z_2)^2 + \frac{1}{4}N(z_2)^2}{N(z_2)} = \frac{1}{2}N(z_2),$$

pa je tvrdnja dokazana. □

3.3 Euklidov algoritam

Euklidov algoritam u $\mathbb{Z}[i]$ analogon je Euklidovog algoritma u $\mathbb{Z}$ u kojem se uzastopnom primjernom teorema o dijeljenju s ostatkom dolazi do najvećeg zajedničkog djelitelja.

Definicija 3.3.1. *Neka su* $z_1,\ z_2 \in \mathbb{Z}[i]$.

- ***Zajednički djelitelj*** *brojeva* $z_1,\ z_2$ *je broj* $w \in \mathbb{Z}[i]$ *takav da* $w \mid z_1$ *i* $w \mid z_2$.
- ***Najveći zajednički djelitelj*** *brojeva* $z_1,\ z_2$ *zajednički je djeljitelj* z_1 *i* z_2 *s najvećom normom.*
  Oznaka: $\mathrm{NZD}(z_1,\ z_2)$.
- *Ako je norma najvećeg zajedničkog djelitelja brojeva* z_1 *i* z_2 *jednaka jedan, tada su* z_1 *i* z_2 ***relativno prosti*** *brojevi.*

Teorem 3.3.2. *Neka su* $z_1,\ z_2 \in \mathbb{Z}[i]$*, različiti od nule. Pretpostavimo da je uzastopnom primjenom teorema o dijeljenju s ostatkom 3.2.5 dobiven niz jednakosti*

$$\begin{aligned}
z_1 &= z_2 q_1 + r_1, \quad && N(r_1) < N(z_2),\\
z_2 &= r_1 q_2 + r_2, \quad && N(r_2) < N(r_1),\\
r_1 &= r_2 q_3 + r_3, \quad && N(r_3) < N(r_2),\\
&\vdots\\
r_{j-2} &= r_{j-1} q_j + r_j, \quad && N(r_j) < N(r_{j-1}),\\
r_{j-1} &= r_j q_{j+1} + 0.
\end{aligned}$$

Tada je $\mathrm{NZD}(z_1,\ z_2) = r_j$*, gdje je* r_j *jednak posljednjem ostatku različitom od nule.*

Dokaz. Iz prve jednakosti zaključujemo da svaki zajednički djelitelj brojeva z_1 i z_2 dijeli i ostatak r_1. Provodeći isto zaključivanje kroz sve jednakosti možemo zaključiti da svaki zajednički djelitelj brojeva z_1 i z_2 dijeli i ostatak $r_k, k = 1,\ 2, \ldots,\ j$. Iz posljednje jednakosti zaključujemo i da svaki zajednički djelitelj brojeva z_1 i z_2 dijeli r_j, ali i da r_j dijeli r_{j-1}. Ponovno, prolazeći kroz svaku jednakost zaključujemo da je r_j zajednički djelitelj brojeva z_1 i z_2. Budući da je r_j djeljiv sa svim drugim zajedničnikim djeliteljima brojeva z_1 i z_2, r_j ima maksimalnu normu pa je i najveći zajednički djelitelj brojeva z_1 i z_2. □

Primjer 3.3.1. *Odredimo* $\mathrm{NZD}(10 + 5i,\ 4 - 2i)$.

Rješenje. Prvo podijelimo dane brojeve kako bismo mogli odrediti q_1, potom i r_1 pa računamo

$$10 + 5i = (4 - 2i)(2 + 2i) + (-2 + i),$$

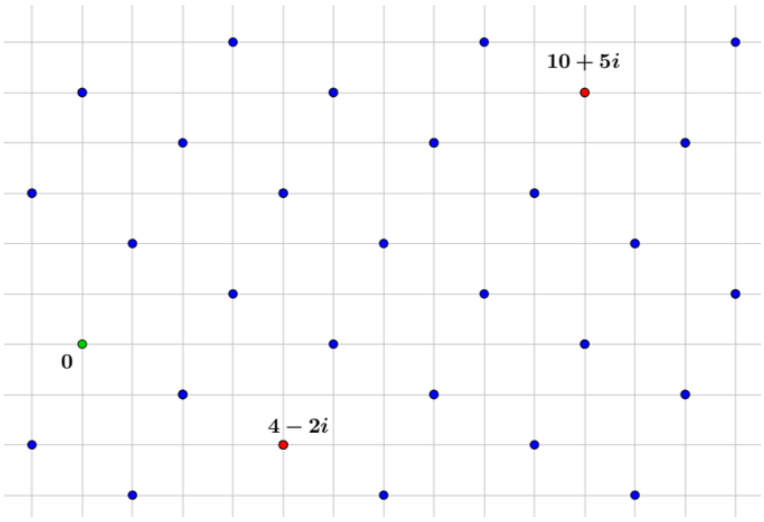
$$4 - 2i = (-2 + i)(-2) + 0.$$

Dakle, NZD$(10+5i,\ 4-2i) = -2+i$. Uočimo da smo mogli i drugačije provoditi algoritam

$$10 + 5i = (4 - 2i)(1 + 2i) + 2 - i,$$

$$4 - 2i = (2 - i)(2) + 0,$$

pa slijedi da je NZD$(10 + 5i,\ 4 - 2i) = 2 - i$. Dobili smo dva različita najveća zajednička djelitelja, ali uočavamo da je $2 - i = (-1)(-2 + i)$. Na slici 3.9 prikazani su višekratnici od $-2 + i$ gdje se vidi da su $10 + 5i$ i $4 - 2i$ višekratnici njihovog najvećeg zajedničkog djelitelja. □



Slika 3.9: Višekratnici od $-2 + i$

Primjer 3.3.2. *Odredimo* NZD$(3 + 2i,\ 3 - 2i)$.

Rješenje.

$$3 + 2i = (3 - 2i)i + 1 - i,$$

$$3 - 2i = (1 - i)(3 + i) - 1,$$

$$1 - i = -1(-1 + i) + 0.$$

Određivanjem najvećeg zajedničkog djelitelja $3 + 2i$ i $3 - 2i$ pokazali smo da je dani par konjugiranih brojeva relativno prost (NZD$(3 + 2i,\ 3 - 2i) = -1$). Taj zaključak ne vrijedi za svaki par konjugiranih brojeva je npr. NZD$(7 + 3i,\ 7 - 3i) = -1 + i$). □

Poglavlje 4

Prosti brojevi i faktorizacija u prstenu $\mathbb{Z}[i]$

4.1 Prosti brojevi

Definicija 4.1.1. *Prirodan broj $p > 1$ je **prost** ako p nema niti jednog djelitelja d takvog da je $1 < d < p$. Ako prirodan broj $a > 1$ nije prost, onda kažemo da je **složen**.*

Prethodna definicija 4.1.1 rekla je da je broj p prost ako su mu jedini djelitelji 1 ili on sam. Kako prirodno možemo poopćiti ovu definiciju na prsten cijelih brojeva? U $\mathbb{Z}$ je prosti broj p djeljiv s -1, 1, p i $-p = (-1)p$. Brojevi -1 i 1 jedini su invertibilni elementi u prstenu $\mathbb{Z}$, a uobičajeno je da ih nazivamo *jedinice*. Njih ne smatramo niti prostim niti složenim brojevima u $\mathbb{Z}$.

Definicija 4.1.2. *Broj $p \in \mathbb{Z}$ je **prost** broj ako zadovoljava sljedeće uvjete:*

1. *p nije jedinica;*
2. *ako su $x,\ y \in \mathbb{Z}$ i $xy = p$, tada je x ili y jednak jedinici.*

Na analogan način, poopćimo definiciju na proste brojeve u prstenu $\mathbb{Z}[i]$ gdje postoje točno četiri jedinice: $1, -1, i, -i$ (korolar 3.1.7).

Definicija 4.1.3. *Gaussov cijeli broj w je **prost** ako vrijedi:*

1. *w nije jedinica;*
2. *ako su $z_1,\ z_2 \in \mathbb{Z}[i]$ i $z_1 z_2 = w$, tada je z_1 ili z_2 jednak jedinici.*

*U suprotnom je w **složen** broj.*

Napomena 4.1.4. *Ako Gaussov cijeli broj z nije jednak jedinici, što znači da je $N(z) > 1$, i ako z možemo napisat kao umnožak dva Gaussova cijela broja od kojih niti jedan nije jednak jedinici, tada je z* ***složen*** *broj.*

Primjer 4.1.1. *Gaussov cijeli broj $9 + 5i$ je složen broj budući da postoji netrivijalna faktorizacija*

$$9 + 5i = (1 - i)(2 + 7i).$$

Lako se vidi da uvijek postoji više trivijalnih faktorizacija

$$9 + 5i = i(5 - 9i) = -1(-9 - 5i) = 1(9 + 5i) = -i(-5 + 9i),$$

ali i netrivijalnih faktorizacija

$$9 + 5i = (1 - i)(2 + 7i) = (-1 + i)(-2 - 7i) = (-1 - i)(-7 + 2i) = (1 + i)(7 - 2i).$$

Teorem 4.1.5. *Neka je $w = a + bi \in \mathbb{Z}[i]$, pri čemu su $a \neq 0$ i $b \neq 0$. Broj w je prost u $\mathbb{Z}[i]$ ako i samo ako je $N(w)$ prosti broj u $\mathbb{N}$.*

Dokaz. Pretpostavimo da je $w = a + bi \in \mathbb{Z}[i]$, $a, b \neq 0$, prosti broj. Tada je $N(w) = w\overline{w}$ pa w dijeli $N(w) \in \mathbb{N}$. Stoga, postoji prosti broj $p \in \mathbb{N}$ (iz faktorizacije od $N(w)$) takav da $w \mid p$. Nadalje, $p = w \cdot z$ za neki $z \in \mathbb{Z}[i]$ pa je

$$N(p) = p^2 = N(w) \cdot N(z).$$

Prethodna faktorizacija u skupu prirodnih brojeva može vrijediti samo za $N(w) = p^2$ ili $N(w) = p$ (jer w nije jedinica). No, prva mogućnost ne može vrijediti jer je $N(w) = a^2 + b^2$ i $a, b \neq 0$. Stoga je $N(w) = p$.

Sada pretpostavimo da je $N(w) = a^2 + b^2 \in \mathbb{N}$ prosti broj. Zapišemo w kao umnožak faktora $z_1,\ z_2 \in \mathbb{Z}[i]$, $w = z_1 z_2$. Tada je

$$N(w) = N(z_1)N(z_2).$$

Budući da je nova jednažba u $\mathbb{N}_0$ i $N(w)$ prost broj, prema definiciji 4.1.3 slijedi da je $N(z_1)$ ili $N(z_2)$ jednak 1. Znači da je z_1 ili z_2 jednak jedinici pa zaključujemo da w nema netrivijalnu faktorizaciju. Broj w je prost. □

Napomena 4.1.6. *Prema teoremu 4.1.5 Gaussov cijeli broj $w = a + bi$ kojem su realni i imaginarni dio različiti od nule je prost ako i samo je suma kvadrata $a^2 + b^2$ prosti broj u $\mathbb{N}$.*

Teorem 4.1.5 nam omogućava da odredimo je li neki Gaussov cijeli broj prost s obzirom na njegovu normu ako je prosti broj. Na primjer, broj $3+2i$ je prost zato što je $N(3+2i) = 13$ prost broj u $\mathbb{Z}$. No, pitanje je što u slučaju kad norma nije prost broj u $\mathbb{Z}$, odnosno je li onda nužno Gaussov cijeli broj složen? Promatramo li broj 2 u $\mathbb{Z}[i]$, on se može napisati $2 = (1 + i)(1 - i)$ pa slijedi da je 2 složen broj, a njegova norma jednaka je 4, što nije prost broj u $\mathbb{Z}$. S druge strane, broj 3 je prost broj u $\mathbb{Z}[i]$, ali njegova norma jednaka je 9, a 9 nije prost broj u $\mathbb{Z}$. Tvrdnja će se obrazložiti u sljedećem odjeljku.

4.2 Veza sume kvadrata i Gaussovih cijelih brojeva

Teorem 4.2.1. *Prost broj $p \in \mathbb{N}$ je složen u $\mathbb{Z}[i]$ ako i samo ako se može prikazati kao suma dva kvadrata dva prirodna broja.*

Dokaz. Ako je prosti broj $p \in \mathbb{N}$ složen u $\mathbb{Z}[i]$, onda postoje $z_1, z_2 \in \mathbb{Z}[i]$ takvi da je $N(z_1), N(z_2) > 1$ i $p = z_1 z_2$. Otuda je

$$p^2 = N(z_1)N(z_2).$$

Očito je jedino moguće $N(z_1) = p$ pa je $p = a^2 + b^2$ gdje su $a, b \neq 0$.

Ako je $p = a^2 + b^2$ za neke $a, b \in \mathbb{N}$, tada je

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

pa je p složen broj u $\mathbb{Z}[i]$ (jer očito da $a \pm bi$ nisu jedinice). □

Možemo sada povezati definiciju 2.2.1 skupa Gaussovih cijelih brojeva s proširenjem prstenu $\mathbb{Z}$. Ako promatramo polinom $x^2 + y^2$, primjetit će se da se ne može napisati kao produkt linearnih polinoma s koeficijentim u $\mathbb{Z}$, ali može se zapisati kao produkt

$$x^2 + y^2 = (x - yi)(x + yi)$$

linearnih polinoma s koeficijentima u $\mathbb{Z}[i]$.

U nastavku ćemo pokazati i iskazati neke tvrdnje o prikazivosti prirodnih brojeva kao sumu dvaju kvadrata cijelih brojeva.

Teorem 4.2.2. *Ako je p oblika $p = 4n + 3$, tada se p ne može napisati kao suma dva kvadrata.*

Dokaz. Tvrdnja teorema ekvivalentna je sljedećem izrazu

$$a^2 + b^2 \not\equiv 3 \pmod 4.$$

Znamo da ostatak pri dijeljenju s 4 nekog broja na kvadrat može biti ili 0 ili 1. Slijedi da $a^2 + b^2 \equiv 0,\ 1,\ 2 \pmod 4$. □

Lema 4.2.3 (Langrangeova lema)**.** *Prost broj oblika* $p = 4n+1$ *dijeli* m^2+1 *za neki* $m \in \mathbb{Z}$*.*

Teorem 4.2.4 (Fermatov teorem o dva kvadrata)**.** *Ako je* $p = 4n + 1$ *prost broj, tada je* $p = a^2 + b^2$*, za neke* $a,\ b \in \mathbb{Z}$*.*

Dokaz. Za dani p prost broj neka je $m \in \mathbb{Z}$ takav da $p \mid m^2 + 1$ (lema 4.2.3). U $\mathbb{Z}[i]$ broj $m^2 + 1$ može se faktorizirati na sljedeći način

$$m^2 + 1 = (m + i)(m - i).$$

Iako p dijeli $m^2 - 1$, $p \nmid m + i$ te $p \nmid m - i$ jer kvocijenti nisu u $\mathbb{Z}[i]$, odnosno $\frac{m}{p} + \frac{i}{p}$ i $\frac{m}{p} - \frac{i}{p}$ nisu Gaussovi cijeli brojevi. Slijedi da p nije prost Guassov cijeli broj, pa prema teoremu 4.2.1 složen broj se može napisati kao $p = a^2 + b^2$. □

Kao posljedicu prethodnih tvrdnji imamo sljedeću karakterizaciju prostih brojeva oblika $a \in \mathbb{Z}$ u $\mathbb{Z}[i]$.

Teorem 4.2.5. *Broj* $a \in \mathbb{Z}$ *je prost u* $\mathbb{Z}[i]$ *ako i samo ako je* $|a|$ *prost u* $\mathbb{N}$ *i* $|a| \equiv 3 \pmod 4$.

Napomena 4.2.6. *Prema teoremu 4.2.5 jasno je da vrijedi da je broj* $ib \in \mathbb{Z}[i]$ *prost u* $\mathbb{Z}[i]$ *ako i samo ako je* $|b|$ *prost u* $\mathbb{N}$ *i* $|b| \equiv 3 \pmod 4$.

Teorem 4.2.7 (Diofantov identitet)**.** *Produkt dvije sume kvadrata jednak je sumi kvadrata, odnosno*

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ac + bd)^2.$$

Dokaz. Neka su $z_1,\ z_2 \in \mathbb{Z}[i]$, takvi da je $z_1 = a + bi$, a $z_2 = c + di$ pa računamo

$$\begin{aligned}(a^2 + b^2)(c^2 + d^2) &= (a - bi)(a + bi)(c + di)(c - di)\\ &= (a - bi)(c - di)(a + bi)(c + di)\\ &= (ac - bd - (ad + bc)i) \cdot (ac - bd + (ad + bc)i)\\ &= (ac - bd)^2 + (ad + bc)^2.\end{aligned} \tag{4.1}$$

□

Iz teorema 4.2.2, 4.2.3, 4.2.7 slijedi sljedeća važna tvrdnja.

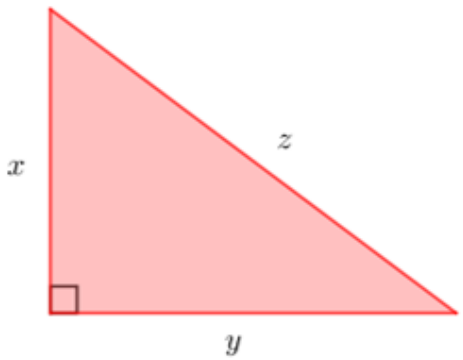
Teorem 4.2.8. *Prirodan broj može se prikazati u obliku sume kvadrata dva cijela broja ako i samo ako mu se u rastavu na proste faktore svi prosti brojevi oblika* $4k + 3$ *pojavljuju s parnom potencijom.*

Pitagorine trojke

Definicija 4.2.9. *Uređenu trojku prirodnih brojeva* $(x,\ y,\ z)$ *zovemo Pitagorina trojka ako su* $x,\ y$ *katete, a* z *hipotenuza nekog pravokutnog trokuta, tj. ako vrijedi*

$$x^2 + y^2 = z^2.$$

Ako su $x,\ y,\ z$ *relativno prosti, onda kažemo da je* $(x,\ y,\ z)$ *primitivna Pitagorina trojka.*



Slika 4.1: Pravokutni trokut s duljinama stranica $x,\ y,\ z$

Primjer 4.2.1. *Neke Pitagorine trojke su*

$$(3,\ 4,\ 5),\ (5,\ 12,\ 13),\ (9,\ 40,\ 41),\ (7,\ 24,\ 25),\ (11,\ 60,\ 61).$$

Korolar 4.2.10. *Ako su trojke* $(a,\ b,\ e)$ *i* $(c,\ d,\ f)$ *Pitagorine, onda je i* $(ac-bd,\ ad+bc,\ ef)$ *Pitagorina trojka.*

Dokaz. Za Pitagorine trojke $(a,\ b,\ e)$ i $(c,\ d,\ f)$ vrijedi

$$a^2 + b^2 = e^2\ ,\ c^2 + d^2 = f^2.$$

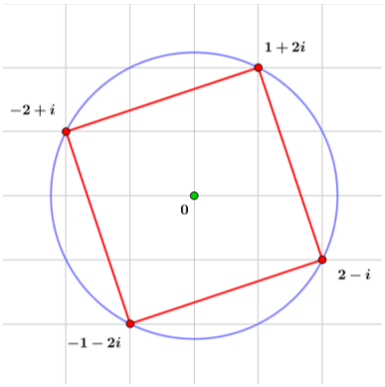
Tada slijedi

$$\begin{aligned}(ef)^2 = e^2f^2 &= (a^2 + b^2)(c^2 + d^2)\\ &= (ac - bd)^2 + (ad + bc)^2,\end{aligned} \tag{4.2}$$

pri čemu zadnja jednakost slijedi iz teorema 4.2.7. □

4.3 O distribuciji Gaussovih prostih brojeva

Distribucija Gaussovih prostih brojeva uključuje mnoge otvorene probleme. Na primjer, na realnoj i imaginarnoj osi nalazi se beskonačno monogo prostih Gaussovih brojeva ($3, 7, 11, 19, \ldots$ i njima asociranim $-3, -7, -11, -19, \ldots, \pm i3, \pm i7, \pm i11, \pm i19, \ldots$). Postoje li još neki pravci Gaussove ravnine na kojima leži beskonačno mnogo Gausovih prostih brojeva? Konkretno, postoji li beskonačno mnogo Gaussovih prostih brojeva oblika $1+bi$? Nadalje, je li moguće hodati koracima ograničene duljine koristeći se samo Gaussovim prostim brojevima u beskonačnost? Ovo je poznato kao *Gaussov problem jarka* (engl. Gaussian moat problem[1]). U ovom radu neće biti govora o složenim problemima distribucije prostih brojeva već o njezinoj vizualnoj *ljepoti*.



Slika 4.2: Primagon generiran s $w = 1 + 2i$

Propozicija 4.3.1. *Ako je $w \in \mathbb{Z}[i]$ prost broj i $e \in \{-1,\ 1,\ -i,\ i\}$, tada je $ew \in \mathbb{Z}[i]$ prost broj.*

Dokaz. Neka je w prost broj što znači da w nije jedinica, pa ni umnožak ew nije jednak jedinici. Ako je $ew = z_1 z_2$ tada je $w = (e^{-1}z_1)z_2$ (e je invertibilan element u $\mathbb{Z}[i]$). Slijedi da ili $e^{-1}z_1$ jedinica ili z_2 jedinica. Uzmemo li da je $e^{-1}z_1$ jedinica, zaključujemo da je z_1 jedinica. Dakle, ili je z_1 ili z_2 jedinica pa je ew prost broj. □

Propozicija 4.3.2. *Ako je $z \in \mathbb{Z}[i]$ prost, tada je i $\overline{z} \in \mathbb{Z}[i]$ prost.*

Dokaz. Neka je z prost, što znači da nije jedinica, pa slijedi da ni konjugat $\overline{z}$ nije jedinica. Ako je $\overline{z} = z_1 z_2$, onda je $z = \overline{\overline{z}} = \overline{z_1}\ \overline{z_2}$. Kako je z prost, $\overline{z_1}$ ili $\overline{z_2}$ mora biti jednak jedinici. Zato će z_1 ili z_2 biti jednak jedinici. Zaključujemo, $\overline{z}$ je prost. □

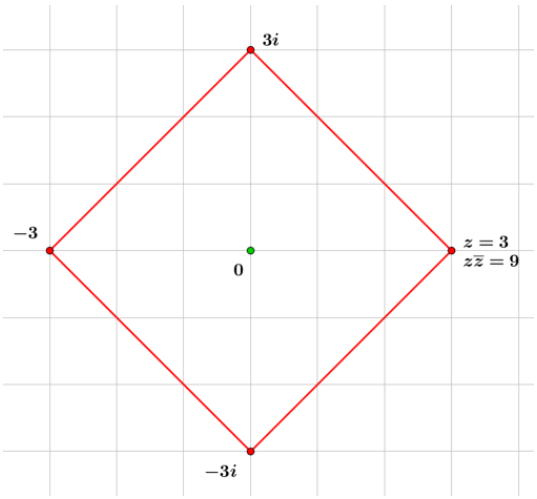
[1] Postavio ga je 1962. Basil Gordon i za sada je neriješen

Prema propoziciji 4.3.1 i 4.3.2 slijedi da Gaussovi prosti brojevi dolaze u skupinama po 4 ili 8 s istom normom. Naime, ako je w Gaussov prosti broj, onda su to i tzv. pridruženi brojevi $-w, iw, -iw$. Skup $\{w, -w, iw, -iw\}$ u ravnini čini vrhove kvadrata kojeg ćemo nazvati *primagon* (slika 4.2). Nadalje, ako su realni ili imaginarni dio od w različiti od nule, onda su i $\overline{w}, -\overline{w}, i\overline{w}, -i\overline{w}$ prosti (do istog zaključka moglo se doći i korištenjem napomene 4.1.6).

Primagone možemo podijeliti u tri skupine s obzirom na prosti broj w koji ih generira.

1. Primagon generiran s w koji se poklapa s primagonom generiranim s $\overline{w}$, a

   $z\bar{z}$ je jednak kvadratu cijelog broja. Stranice kvadrata leže na pravcima čiji je nagib ± 1. Ovaj primagon je *inertan*.

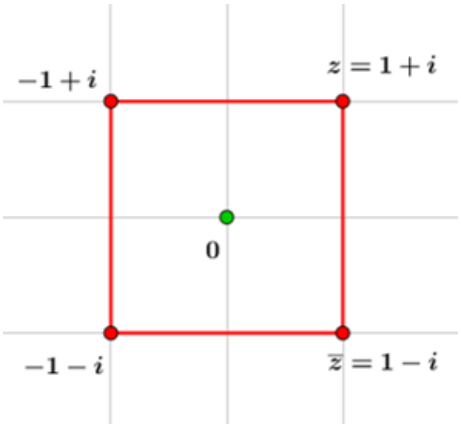


Slika 4.3: Inertni primagon

2. Primagon generiran s w koji se poklapa s primagonom generiranom s $\overline{w}$, ali $z\bar{z}$ nije jednak kvadratu cijelog broja.

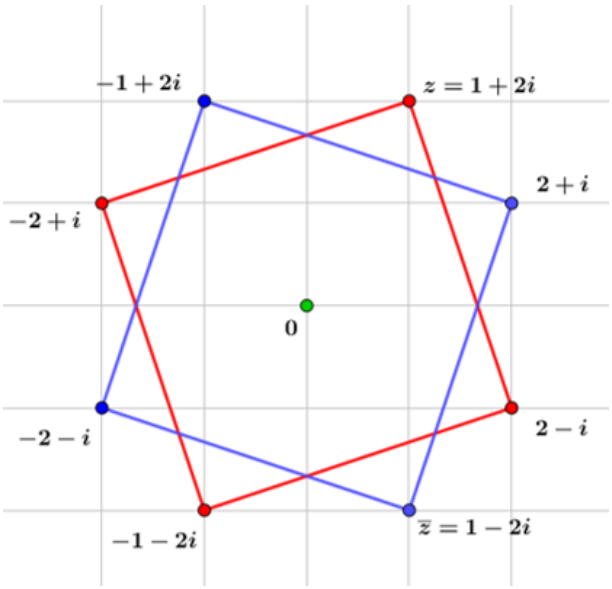
   Stranice kvadrata leže na pravcima koji su paralelni s koordinatnim osima. Za taj primagon od w kažemo da je razgranat[2].

[2]Vrijedi $2 = (1+i)(1-i) = i(1-i)^2$, tj. 2 je prosti broj u $\mathbb{Z}$ koji se grana ("ramificira") na dva ista (ili ekvivalentna) prosta broja



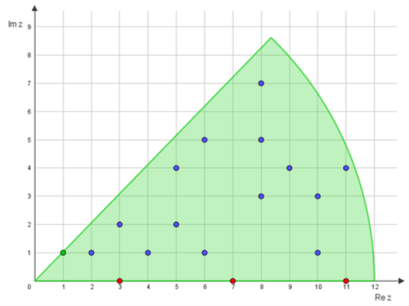
Slika 4.4: Razgranati primagon

3. Primagon generiran s w nije jednak primagonu generiranim s $\overline{w}$. Ta dva primagona sadrže sve proste brojeve čija je norma $N(w)$. Zrcalno su simetrični s obzirom na koordinatne osi. Za opisani primagon od w kažemo da je *podijeljen*.



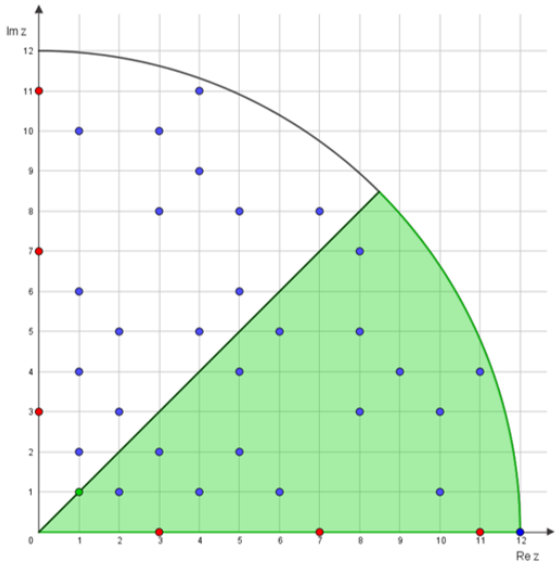
Slika 4.5: Podijeljeni primagon

Recimo sada nešto o Gaussovim prostim brojevima unutar kruga radijusa r. Iz svega prethodno navedenog možemo zaključiti da struktura Gaussovih prostih brojeva ima induciranu osmerostruku simetriju, tj. ako je $a + bi$ prost onda su i brojevi $\pm a \pm bi$ i $\pm b \pm ai$ prosti. Stoga ako želimo odrediti sve Gaussove proste brojeve koji leže na krugu radijusa

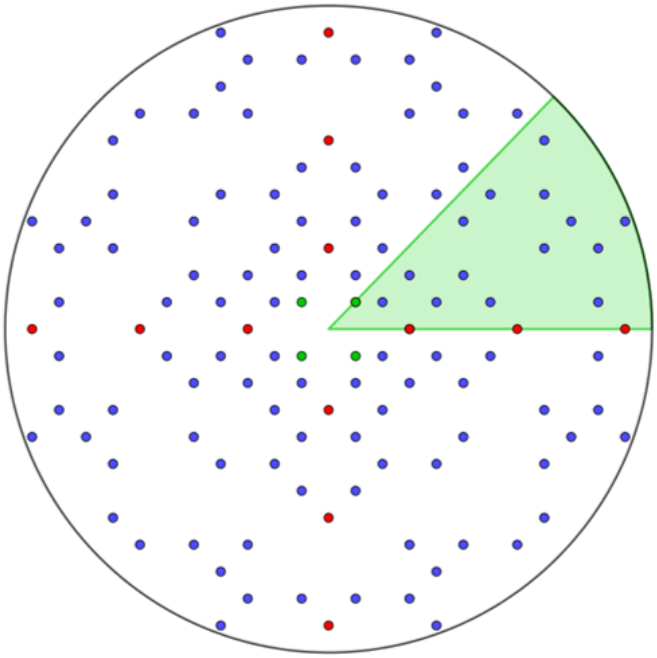


Slika 4.6: Gaussovi prosti cijeli brojevi u „fundamentalnoj domeni”

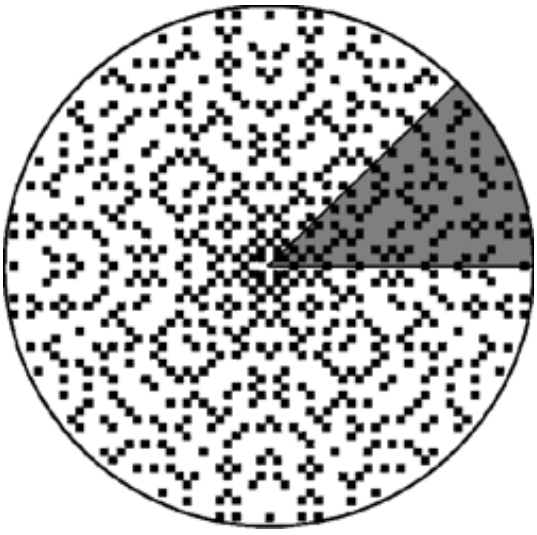
12, odnosno čija je apsolutna vrijednost manja ili jednaka 12, dovoljno ih je gledati na takozvanoj „fundamentalnoj domeni” – kružnom isječku sa pripadnim središnjim kutom $\frac{\pi}{4}$ (slika 4.7). Sve ostale točke možemo dobiti zrcaljenjem s obzirom na odgovarajuće pravce. Na primjer, zrcaljenjem oko pravca $x = y$ prikazano je na slici 4.7, a svi Gaussovi cijeli brojevi koji su prosti unutar kruga radijusa 12 (njih 128) na slici 4.8. Nadalje, na slici 4.8 crvene točke su brojevi koji se poklapaju s prostim brojevima u prstenu $\mathbb{Z}$. Zelene točke dio su skupine koju smo ranije opisali kao razgranati primagon. Ostale plave točke pripadaju ili inertnom ili podijeljenom primagonu.



Slika 4.7: Zrcaljenje „fundamentalne domene” oko pravca $x = y$



Slika 4.8: Gaussovi prosti cijeli brojevi unutar kruga radijusa 12



Slika 4.9: Gaussovi prosti cijeli brojevi norme manje od 1000, [3]

4.4 Jedinstvena faktorizacija

Faktorizacija brojeva podrazumijeva prikazivanje broja kao produkt jednog ili više prostih brojeva. Na slici 4.10 prikazan je rastav broja 550 na proste faktore. Možemo uočiti da se broj može rastaviti na više načina, ali da je konačan rastav jedanak $550 = 2 \cdot 5^2 \cdot 11$. O jedinstvenosti rastava prirodnog broja na proste faktore govori sljedeći teorem.

Teorem 4.4.1 (Osnovni teorem aritmetike)**.** *Prikaz svakog prirodnog broja većeg od 1 u obliku produkta prostih faktora jedinstven je do na poredak faktora.*

Dokaz. Prvo ustanovimo da se svaki prirodan broj $n > 1$ može prikazati kao umnožak prostih faktora. Koristimo princip matematičke indukcije. Broj 2 je prost. Pretpostavimo da se svi prirodni brojevi manji od n mogu prikazati kao umnožak prostih brojeva. Broj n je ili prost ili složen. Ako je n prost onda za njega vrijedi tvrdnja, a ako je složen onda je $n = n_1 n_2$ i $n_1, n_2 < n$. Prema pretpostavci n_1, n_2 se mogu prikazati kao produkt prostih faktora pa se može i broj n.

Pretpostavimo da n ima dvije različite faktorizacije, $n = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$. Podijeljimo jednakost s prostim brojevima koji su zajednički u obje faktorizacije i dobijemo sljedeću jednakost

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \,,$$

gdje su p_i, q_j prosti brojevi, ne nužno različiti, ali takvi da se niti jedan prost broj s lijeve strane ne pojavljuje na desnoj strani, tj. $p_i \neq q_j$ za sve $i,\ j$. Međutim, to je nemoguće jer iz $p_1 \mid q_1 q_2 ... q_s$, slijedi da p_1 dijeli barem jedan q_j. No, kako su svi p_i i q_j prosti brojevi, to znači da je $p_1 = q_j$. Dolazi se do kontradikcija. □

Napomena 4.4.2. *Svaki prirodan broj n veći od jedan se može prikazati u obliku*

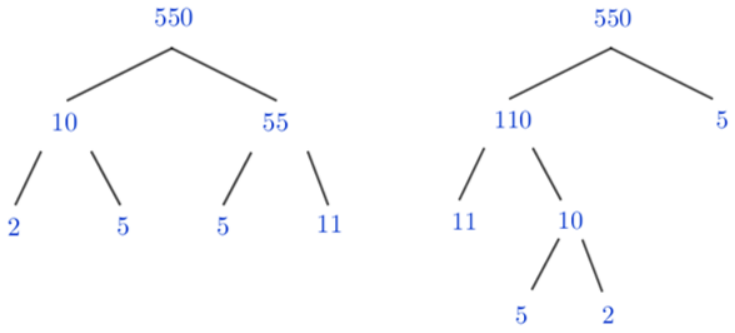
$$n = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k},$$

gdje su $p_1,\ p_2, \ldots,\ p_k$ *različiti prosti brojevi, a* $\alpha_1,\ \alpha_2, \ldots,\ \alpha_k$ *prirodni brojevi. Dani prikaz naziva se* kanonski rastav broja n na proste faktore.

Problem 4.4.1. *Faktorizirajte broj 10 u prstenu Gaussovih cijelih brojeva?*

Rješenje. Broj 10 možemo napisati kao umnožak brojeva 2 i 5, odnosno $10 = 2 \cdot 5$. Kad bismo bili su skupu $\mathbb{Z}$ tu bismo bili gotovi jer su 2 i 5 u tom prstenu prosti brojevi. Međutim, već smo naveli da 2 i 5 nisu prosti Gaussovi cijeli brojevi i zato trebamo razmotrit i na koji način možemo faktorizirati 2 i 5. Za broj 2 potrebno je promatrati Gaussove brojeve čija je apsolutna vrijednost između 1 i $\sqrt{2}$,

$$2 = (1 + i) \cdot (1 - i).$$



Slika 4.10: Rastav broja 550 na proste faktore

Nadalje, za broj 5 tražimo Gaussove brojeve čija je apsolutna vrijednost između 1 i $\sqrt{5}$ i pronalazimo da se 5 može faktorizirati na sljedeći način

$$5 = (2 + i)(2 - i).$$

Konačno,

$$10 = 2 \cdot 5 = (1 + i)(1 - i)(2 + i)(2 - i).$$

Naravno, $(1 - i)$ mogli smo napisati kao $(-i)(1 + i)$ i tako sve ostale faktore, pa je pitanje jesu li sve faktorizacije jednake i postoji li onda jedinstvena faktorizacija za kakvu znamo u $\mathbb{Z}$. □

Teorem 4.4.3. *Neka je $z \in \mathbb{Z}[i]$ i $N(z) > 1$. Svaki z se može napisati kao produkt prostih brojeva u $\mathbb{Z}[i]$.*

Dokaz. Dokaz se provodi matematičkom indukcijom po $N(z)$. Za bazu provjeravamo $N(z) = 2$. Prema teoremu 4.1.5 slijedi da je takav z prost broj, konkretno $z = 1 \pm i$ ili $z = -1 \pm i$. Neka je $n \geq 3$. Pretpostavimo da Gaussove cijele brojeve za koje vrijedi $3 \leq N(z) < n$ možemo napisati kao produkt prostih brojeva u $\mathbb{Z}[i]$. Pokažimo da se $z \in \mathbb{Z}[i]$, $N(z) = n$ i složen može napisati kao produkt prostih Gaussovih cijeli brojeva. Neka je $z_1 z_2$ netrivijalna faktorizacija od z. Kako je $N(z_1) < N(z)$ i $N(z_2) < N(z)$, prema pretpostavci, z_1 i z_2 su produkti prostih Gaussovih cijelih brojeva. Zaključujemo da se z može napisati kao produkt prostih Gaussovih cijelih brojeva. □

Lema 4.4.4. *Neka je $w \in \mathbb{Z}[i]$ prosti broj. Ako $w \mid z_1 z_2 \cdots z_n$, onda postoji $j \in \{1, \ldots, n\}$ takav da w dijeli z_j.*

Dokaz. Pokazujemo slučaj $n = 2$, a za opći n tvrdnja slijedi indukcijom.

Neka je $w \mid z_1 z_2$. Pretpostavimo da w ne dijeli z_1. To znači da su w i z_1 relativno prosti, tj NZD$(w, z_1) = 1$. Stoga, prema teoremu 3.3.2 (Euklidov algoritam) slijedi da je $wx + z_1 y = 1$ za neke $x, y \in \mathbb{Z}[i]$ te otuda $wz_2 x + z_1 z_2 y = z_2$. Očito w dijeli $wz_2 x + z_1 z_2 y$ pa dijeli i z_2. □

Teorem 4.4.5 (Jedinstvena faktorizacija Gaussovih cijelih brojeva)**.** *Neka je* $z \in \mathbb{Z}[i]$ *i* $N(z) > 1$. *Ako je*

$$z = z_1 z_2 \cdots z_m = z'_1 z'_2 \cdots z'_n \,,$$

gdje su $z_1, \ldots z_m, z'_1, \ldots z'_n$ *prosti Gaussovi cijeli brojevi, tada je* $m = n$ *te postoji permutacija* σ *skupa* $\{1, \ldots, m\}$ *takva da je* $z_j = e_j z'_{\sigma(j)}$, $e_j \in \{1, -1, i, -i\}$, *za sve* $j \in \{1, \ldots, m\}$.

Dokaz. U prethodnom teoremu 4.4.3 pokazali smo da se svaki $z \in \mathbb{Z}[i]$, takav da $N(z) > 1$, može faktorizirati. Nadalje, pretpostavimo da je $N(z) > 2$ jer je iz $N(z) = 2$ slijedi da je z prost. Tvrdnju pokazujemo primjenom principa matematičke indukcije po $N(z)$. Pretpostavimo da za sve Gaussove cijele brojeve za koje je $3 \leq N(z) < n$ vrijedi da se mogu jedinstveno faktorizirati (do na poredak faktora i množenje svakog faktora s nekom od jedinica). Neka je $z \in \mathbb{Z}[i]$ takav da je $N(z) = n$ te pretpostavimo da postoje dvije faktorizacije na proste faktore od z:

$$z = z_1 z_2 \cdots z_m = z'_1 z'_2 \cdots z'_n \,.$$

Budući da $z_1 \mid z$, odnosno

$$z_1 \mid z'_1 z'_2 \cdots z'_n \,,$$

prema lemi 4.4.4 slijedi da $z_1 \mid z'_k$ za neki $k \in \{1, \ldots, n\}$. Bez smanjenja općenitosti možemo prepostaviti da je $k = 1$, to jest da $z_1 \mid z'_1$. Kako su z_1 i z'_1 prosti brojevi i nemaju netrivijalnih faktora, slijedi da $z_1 = e_1 z'_1$ za $e_1 \in \{1, -1, i, -i\}$. Dvije faktorizacije za z sada imaju oblik

$$z = e_1 z'_1 z_2 \cdots z_m = z'_1 z'_2 \cdots z'_n \,,$$

kad podijelimo jednakosti sa z'_1

$$w = \frac{z}{z'_1} = e_1 z_2 \cdots z_m = z'_2 \cdots z'_n \,.$$

Za dobiveni $w \in \mathbb{Z}[i]$ očito vrijedi da je $N(w) < N(z) = n$. Nadalje, kako je e_1 jedinica, slijedi da je $e_1 z_2$ prost broj pa iz toga zaključujemo da se na lijevoj strani nalazi $m - 1$ prost broj, a na desnoj strani $n - 1$ prost broj. Imamo zadovoljenu pretpostavku da je $N(w) < n$ pa w ima jedinstvenu faktorizaciju i $m - 1 = n - 1$, tj. $m = n$. □

Nakon ovog teorema možemo zaključiti da za svaki Gaussov cijeli broj postoji jedinstvena faktorizacija na proste Gaussove cijele brojeve do na poredak i množenje jedinicom.

Primjer 4.4.1. *Odredimo rastav na proste Gaussove cijele brojeve od* $z = 36 + 3i$.

Rješenje. Najprije ćemo odrediti normu od z, $N(z) = 36^2 + 3^2 = 1305$, a zatim odrediti rastav norme na proste faktore u $\mathbb{N}$, $1305 = 3^2 \cdot 5 \cdot 29$. Sada se za svaki faktor, odnosno za svaku normu pronađe se broj čija je to norma, a potom i rastav na proste faktore te konačno dobivamo

$$36 + 3i = 3^2 \cdot (1 + 2i) \cdot (1 - 2i) \cdot (2 + 5i) \cdot (2 - 5i).$$

□

Bibliografija

[1] D. Bakić, *Normirani prostori*, skripta, 2017., https://www.pmf.unizg.hr/math/predmet/norpro_a

[2] K. Conrad, *The Gaussin Integers*, https://kconrad.math.uconn.edu/blurbs/ugradnumthy/Zinotes.pdf

[3] M. Das, *Walking through the Gaussian Primes*, arXiv:1901.04549v2 [math.NT],https://doi.org/10.48550/arXiv.1901.04549

[4] A. Dujella, *Teorija brojeva*, Školska kniiga, Zagreb, 2019.

[5] Z. Franušić, J. Šiftar, *Linearna agebra*, skripta, https://web.math.pmf.unizg.hr/~fran/LA-sve-lektura.pdf

[6] Z. Franušić, T. Pejković, *Djeljivost*, nastavni materijali, https://web.math.pmf.unizg.hr/nastava/etb/materijali/predavanje%200.pdf

[7] K. Horvatić, *Linearna algebra*, Golden marketing - Tehnička knjiga, Zagreb, 2004.

[8] D. Ilišević, G. Muić, *Uvod u matematiku*, skripta dostupna na https://www.pmf.unizg.hr/math/predmet/uum

[9] R. S. Irvnig, *Integers, polynomials, and rings*, Springer, 2004.

[10] J. Stillwell, *Elements of number theory*, Springer, 2003.

[11] M. Tevčić, M. Špoljarić, M. Maras, *Kompleksni brojevi u Gaussovoj ravnini*, dostupno na https://hrcak.srce.hr/file/323183

[12] M. H. Weissman, *An Illustrated Theory of Numbers*, American Mathematical Society, 2017.

[13] E. Weisstein, *Gauss's Circle Problem*, From MathWorld–A Wolfram Web Resource. https://mathworld.wolfram.com/GausssCircleProblem.html

[14] *Gauss circle problem*, Wikipedia, https://en.wikipedia.org/wiki/Gauss_circle_problem#cite_note-Hardy-1

[15] *Gaussian Integer Factorization Calculator*, Had to know, https://www.had2know.org/academics/gaussian-integer-factorization.html

[16] *Gaussian Integers*, EuclideanAlgorithmOnline, http://www.maths.surrey.ac.uk/hosted-sites/euclidean/gaussianintegers.html

[17] *Kompleksni brojevi*, Edutorij, https://edutorij.e-skole.hr/share/proxy/alfresco-noauth/edutorij/api/proxy-guest/b9455aeb-16ae-4c3a-a6b1-da720c38c54d/html/1766_Kompleksni_brojevi.html

[18] Project Nayuki, *Factorize Gaussian integer (JavaScript)*, https://www.nayuki.io/page/factorize-gaussian-integer-javascript

[19] *The Arithmetic of the Gaussina Integers*, https://personal.math.ubc.ca/~anstee/math444/GaussianIntegersfinal.pdf

Sažetak

Skup Gaussovih cijelih brojeva označavamo sa $\mathbb{Z}[i] = \{a + bi : a, b \in\}$ i on čini komutativni prsten s jedinicom s obzirom na zbrajanje i množenje kompleksnih brojeva. U radu se obrađuju standardne teme kao što su djeljivost, Gaussovi prosti brojevi, veza sa sumama kvadrata, Euklidov algoritam, jedinstvena faktorizacija, itd. Poseban je naglasak na vizualnim iterpretacijama i ilustracijama koje su izvedene pomoću *GeoGebre*.

Summary

The set of Gaussian integers is denoted by $\mathbb{Z}[i] = \{a+bi : a, b \in\}$ and it forms a commutative ring with the unit in regard to addition and multiplication of complex numbers. The thesis deals with standard topics such as divisibility, Gaussian prime numbers, connection to the sums of squares, Euclid's algorithm, unique factorization, etc. There is a special emphasis on the visual interpretations and illustrations that were performed using GeoGebra.

Životopis

Martina Novotny rođena je 13. kolovoza 1998. godine u Rijeci u Republici Hrvatskoj. Osnovnu školu Ivana Rabljanina Rab upisala je 2005. godine na Rabu, a paralelno s njom pohađala je i Glazbenu školu Ivana Matetića Ronjgova, smjer klavir. Po završetku upisuje opću gimnaziju u Srednjoj školi Markantuna de Dominisa. Ljubav prema matematici stvorila se u nižim razredima osnovne škole gdje je ostvarila plasman na Regionalno natjecanje iz matematike, a nakon dolaska fizike među nastavne predmete, stvorila se povezanost između teorije i primjene matematike te se zato 2017. godine upisuje na Prirodoslovno-matematički fakultet u Zagrebu na nastavnički smjer integriranog studija matematike i fizike. Tijekom srednjoškolskog i fakultetskog obrazovanja, Martina je uz sezonske poslove trenirala dugi niz godina rukomet u RK Rabu, bila aktivna kao volonter u mnogim organizacijama, a za istaknut je pomoć pri učenju za učenike slabijeg imovinskog statusa, organizacija "International Junior Science Olympiad" i sudjelovanje na otvorenim danima PMF-a. Za vrijeme studija obavljala je niz dužnosti u Studentskom zboru Prirodoslovno-matematičkog fakulteta i Studentskom zboru Sveučilišta u Zagrebu, kao članica Fakultetskog vijeća, Vijeća Matematičkog odsjeka, Vijeća prirodoslovnog područja, Etičkog povjerenstva te zamjena u Senatu Sveučilišta u Zagrebu.