Gaussovi cijeli brojevi

Pešut, Maja

Undergraduate thesis / Završni rad

2024

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Rijeka / Sveučilište u Rijeci**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:196:321347

Sveučilište u Rijeci

Fakultet za matematiku

Sveučilišni prijediplomski studij Matematika

Maja Pešut

Gaussovi cijeli brojevi

Završni rad

Rijeka, srpanj 2024.

Sveučilište u Rijeci

Fakultet za matematiku

Sveučilišni prijediplomski studij Matematika

Maja Pešut

Gaussovi cijeli brojevi

Završni rad

Mentor: doc. dr. sc. Sanda Bujačić Babić

Rijeka, srpanj 2024.

Sažetak U završnom radu ćemo razmatrati skup Gaussovih cijelih brojeva. U prvom dijelu će se govoriti o normi elemenata tog skupa te njegovoj algebarskoj strukturi. U drugom dijelu ćemo proučavati svojstva djeljivosti u skupu $\mathbb{Z}[i]$. U trećem dijelu ćemo definirati proste Gaussove cijele brojeve i utvrditi da Gaussovi cijeli brojevi imaju jedinstveni rastav na proste faktore. Za kraj, bit će uvedena relacija kongruencije te će biti navedene neke primjene skupa Gaussovih cijelih brojeva na aritmetiku skupa $\mathbb{Z}$.

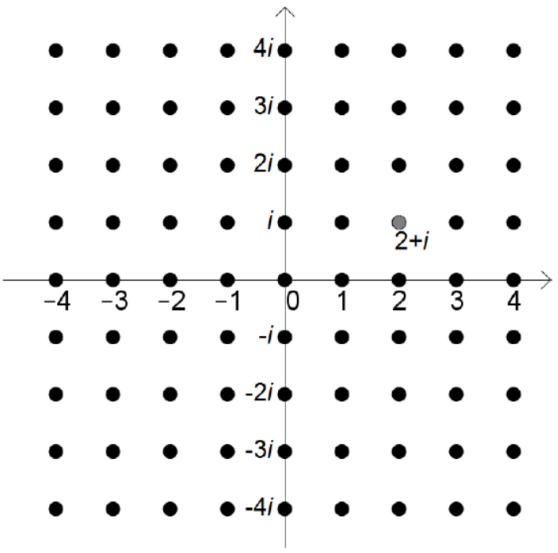
Sadržaj

Uvod

Promatramo skup Gaussovih cijelih brojeva, odnosno skup oblika

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

Gaussovi cijeli brojevi predstavljaju generalizaciju cijelih brojeva na kompleksnu ravninu, zadržavajući većinu svojstava klasičnih cijelih brojeva. Kao i skup cijelih brojeva $\mathbb{Z}$, skup $\mathbb{Z}[i]$ s operacijama zbrajanja i množenja je komutativni prsten s jedinicom. Gaussove cijele brojeve je uveo njemački matematičar Carl F. Gauss 1832. godine u knjizi *Theoria Residuorum Biquadraticorum*([6]). U ovom radu definiramo Gaussove cijele brojeve i istražujemo njihova svojstva, uključujući normu i invertibilnost te naglašavamo razlike u odnosu na skup cijelih brojeva. Drugi dio rada fokusira se na dijeljenje u prstenu $\mathbb{Z}[i]$, osvrćući se i na Euklidov algoritam i Bezoutov teorem. U trećem dijelu istražujemo faktorizaciju Gaussovih cijelih brojeva te definiramo proste i složene Gaussove cijele brojeve. Nakon toga, definiramo relaciju kongruencije te na kraju koristimo skup Gaussovih cijelih brojeva kako bi lakše dokazali neke rezultate u skupu $\mathbb{Z}$.



Slika 1: Gaussovi cijeli brojevi u kompleksnoj ravnini ([3])

1 Norma

Definicija 1.1. *Za $\alpha = a + bi \in \mathbb{Z}[i]$ definiramo normu kao*

$$N(\alpha) = \alpha\bar{\alpha} = (a + bi)(a - bi) = a^2 + b^2.$$

Možemo primijetiti da norma za Gaussov cijeli broj nije definirana kao norma za kompleksni broj. Norma kompleksnog broja $z = x + yi \in \mathbb{C}$ jednaka je $\sqrt{x^2 + y^2}$. Činjenica da je u skupu $\mathbb{Z}[i]$ norma uvijek nenegativan cijeli broj, pokazat će se korisnom kod ispitivanja svojstva djeljivosti skupa $\mathbb{Z}[i]$.
Norma Gaussovog cijelog broja se često koristi ako želimo pokazati da neka tvrdnja vrijedi za sve Gaussove cijele brojeve, odnosno, dokaze možemo provoditi indukcijom po normi.

Definicija 1.2. *Skalarna funkcija f je multiplikativna ako je $f(a \cdot b) = f(a) \cdot f(b)$, za sve a, b iz domene funkcije f.*

Propozicija 1.1. *Norma u skupu $\mathbb{Z}[i]$ je multiplikativna, odnosno, vrijedi:*
$N(\alpha\beta) = N(\alpha)N(\beta),\ \forall \alpha, \beta \in \mathbb{Z}[i]$.

Dokaz. Neka su $\alpha = a + bi, \beta = c + di \in \mathbb{Z}[i]$.
Tada je $\alpha\beta = (a + bi)(c + di) = ac - bd + (ad + bc)i$. Odredimo $N(\alpha\beta)$ i $N(\alpha)N(\beta)$.

$$\begin{aligned} N(\alpha\beta) &= N(ac - bd + (ad + bc)i) \\ &= (ac - bd)^2 + (ad + bc)^2 \\ &= (ac)^2 - 2acbd + (bd)^2 + (ad)^2 + 2adbc + (bc)^2 \\ &= (ac)^2 + (bd)^2 + (ad)^2 + (bc)^2, \end{aligned}$$

$$N(\alpha)N(\beta) = (a^2 + b^2)(c^2 + d^2) = (ac)^2 + (bd)^2 + (ad)^2 + (bc)^2.$$

Zaključujemo:

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

□

Primjer 1. *Neka su $\alpha = 2 + 3i$ i $\beta = -1 - 2i$ Gaussovi cijeli brojevi.*
$N(\alpha) = 2^2 + 3^2 = 13, \quad N(\beta) = (-1)^2 + (-2)^2 = 5$
$N(\alpha\beta) = N((2 + 3i)(-1 - 2i)) = N(4 - 7i) = 4^2 + (-7)^2 = 65 = 13 \cdot 5 = N(\alpha)N(\beta)$

Jedna posljedica multiplikativnosti norme je idući korolar.

Korolar 1.2. *Jedini invertibilni elementi skupa* $\mathbb{Z}[i]$ *su* ± 1 *i* $\pm i$.

Dokaz. Pretpostavimo da je neki $\alpha = a + bi \in \mathbb{Z}[i]$ invertibilan i da je $\alpha\beta = 1$, za neki $\beta \in \mathbb{Z}[i]$. Primjenom Propozicije 1.1 na jednadžbu $\alpha\beta = 1$ dobivamo $N(\alpha) \cdot N(\beta) = 1$. Kako su $N(\alpha), N(\beta) \in \mathbb{Z}_0^+$, zaključujemo da je $N(\alpha) = 1$. Dobivamo jednadžbu $a^2+b^2 = 1$ čija su rješenja $(a, b) \in \{(1, 0), (-1, 0), (0, 1), (0, -1)\}$. Dakle, $\alpha \in \{\pm 1, \pm i\}$. □

Napomena 1.3. 1 *i* -1 *su sami svoji inverzi, a inverz od* i *je* $-i$*, i obrnuto. Jedini invertibilni elementi skupa* $\mathbb{Z}$ *su 1 i -1.*

U skupu $\mathbb{Z}$ vrijedi da, ako je $|m| = |n|$, onda je $m = \pm n$ tj. m se može dobiti kao umnožak invertibilnog elementa iz $\mathbb{Z}$ s n.
Analogna tvrdnja ne vrijedi u $\mathbb{Z}[i]$: Ako je $N(\alpha) = N(\beta)$ ne vrijedi općenito da je $\alpha = \beta \cdot u$, za neki $u \in \{\pm 1, \pm i\}$.

Primjer 2. *Uzmimo brojeve* $4 + 5i$ *i* $4 - 5i$*. Vrijedi da je* $N(4 + 5i) = 41 = N(4 - 5i)$*, ali ako* $4 + 5i$ *pomnožimo s* ± 1 *i* $\pm i$ *dobivamo brojeve* $4 + 5i, -4 - 5i, -5 + 4i, 5 - 4i$*, a ni jedan od njih nije* $4 - 5i$*.*

Primijetimo da svaki nenegativan cijeli broj nije norma nekog Gaussovog cijelog broja. Ta činjenica slijedi iz toga da se ne može svaki prirodni broj napisati kao suma dva kvadrata. O tome govori Fermatov teorem: Prirodni broj n se može prikazati kao zbroj kvadrata dva cijela broja ako i samo ako nekvadratni dio[1] od n nema prostog djelitelja p oblika $p \equiv 3 \pmod 4$.

Primjer 3.

$$2340 = 36 \cdot 65 = 6^2 \cdot 13 \cdot 5$$

Vrijedi: $13 \equiv 1 \pmod 4$, $5 \equiv 1 \pmod 4$ *pa se* 2340 *može zapisati kao zbroj dva kvadrata. Kako je* $65 = 8^2 + 1^2$*, onda je* $2340 = 6^2 \cdot (8^2 + 1^2) = (6 \cdot 8)^2 + (6 \cdot 1)^2 = 48^2 + 6^2$*. Znači, postoji Gaussov cijeli broj kojemu je norma jednaka* 2340*. Jedan od njih je* $48 + 6i$*.*

Primjer 4. *Neki od brojeva koji nisu norma ni jednog Gaussovog cijelog broja su* 3 *i* 63*:* $3 \equiv 3 \pmod 4$, $\quad 63 = 3^2 \cdot 7 \quad$ *te je* $\ 7 \equiv 3 \pmod 4$.

Zaključujemo, cijeli broj je norma nekog Gaussovog cijelog broja ako i samo ako se može zapisati kao zbroj dva kvadrata.

[1]Neka je $n = m^2 \cdot n_0, \ \ m, n_0 \in \mathbb{N}_0$. Ako n_0 nije djeljiv s niti jednim kvadratom prirodnog broja (osim 1), onda kažemo da je n_0 nekvadratni dio od n.

2 Algebarska struktura $(\mathbb{Z}[i], +, \cdot)$

Definicija 2.1. *Prsten $(R, +, \cdot)$ je skup R s operacijama $+$ i $\cdot$ takvim da vrijedi:*

1. *$(R, +)$ je Abelova grupa,*
2. *$(R, \cdot)$ je polugrupa,*
3. *Vrijede zakoni distributivnosti: $(a+b)\cdot c = a\cdot c + b\cdot c, \;\; c\cdot(a+b) = c\cdot a + c\cdot b, \; \forall a, b, c \in R.$*

Ako vrijedi da je $b \cdot a = a \cdot b, \forall a, b \in R$, tada kažemo da je R komutativan. Ako postoji $e \in R$ takav da je $a \cdot e = e \cdot a, \forall a \in R$, tada kažemo da je R prsten s jedinicom.

Teorem 2.1. *Skup Gaussovih cijelih brojeva $(\mathbb{Z}[i], +, \cdot)$ u odnosu na standardne operacije zbrajanja i množenja je komutativni prsten s jedinicom.*

Dokaz. Prvo dokažimo da je $(\mathbb{Z}[i], +)$ Abelova grupa.
Neka su $\alpha = a+bi, \beta = c+di \in \mathbb{Z}[i]$. Tada je $\alpha+\beta = a+c+(b+d)i \in \mathbb{Z}[i]$ jer su $a+c$ i $b+d$ cijeli brojevi. $\mathbb{Z}[i] \subseteq \mathbb{C}$ pa se asocijativnost i komutativnost zbrajanja nasljeđuju iz skupa kompleksnih brojeva. Neutral za zbrajanje je $\epsilon = 0+0i$ jer je $\alpha+\epsilon = 0+a+(0+b)i = \alpha$. Inverz za zbrajanje od $\alpha = a+bi$ je $\alpha^{-1} = -a-bi \in \mathbb{Z}[i]$ (jer $\alpha+\alpha^{-1} = 0 \implies \alpha^{-1} = -\alpha$.)
Još moramo pokazati da je $(\mathbb{Z}[i], \cdot)$ komutativni monoid.
Kako je skup $\mathbb{Z}$ zatvoren s obzirom na množenje i zbrajanje, onda je $\alpha \cdot \beta = ac + bd + (ad - bc)i \;\; \in \mathbb{Z}[i]$. $\mathbb{Z}[i] \subseteq \mathbb{C}$ pa se asocijativnost i komutativnost množenja nasljeđuju iz skupa kompleksnih brojeva. Neutral za množenje je $\epsilon = 1$ jer je $\alpha \cdot 1 = \alpha, \; \forall \alpha \in \mathbb{Z}[i]$. □

Definicija 2.2. *Neka je $(R, +, \cdot)$ prsten. Ako za $a, b \in R, \; a, b \neq 0$ vrijedi da je $a \cdot b = 0$, onda kažemo da je a lijevi, a b desni djelitelj nule. Ako je 0 jedini djelitelj nule, onda kažemo da je R prsten bez djelitelja nule.*

Definicija 2.3. *Ako je R komutativan prsten bez djelitelja nule, onda kažemo da je R integralna domena.*

Propozicija 2.2. *$(\mathbb{Z}[i], +, \cdot)$ je integralna domena.*

Dokaz. Iz Teorema 2.1 znamo da je $(\mathbb{Z}[i], +, \cdot)$ komutativan prsten. Pretpostavimo da postoje $\alpha, \beta \in \mathbb{Z}[i], \; \alpha, \beta \neq 0$ takvi da je $\alpha \cdot \beta = 0$. Djelovanjem norme slijedi, $N(\alpha)N(\beta) = 0$. To može biti jedino ako je α ili β jednako 0, što je kontradikcija s pretpostavkom da su $\alpha, \beta \neq 0$. Dakle, 0 je jedini djelitelj nule u $(\mathbb{Z}[i], +, \cdot)$ pa je $(\mathbb{Z}[i], +, \cdot)$ integralna domena, što je i trebalo pokazati. □

3 Djeljivost

U ovom poglavlju istražit ćemo svojstva djeljivosti u skupu $\mathbb{Z}[i]$ i vidjeti kako su povezana s djeljivošću u skupu cijelih brojeva. Definicija djeljivosti Gaussovih cijelih brojeva je analogna uobičajenoj definiciji djeljivosti.

Definicija 3.1. *Kažemo da $\beta \in \mathbb{Z}[i]$ dijeli $\alpha \in \mathbb{Z}[i]$ i pišemo $\beta|\alpha$, ako je $\alpha = \beta\gamma$, za neki $\gamma \in \mathbb{Z}[i]$.*

Primjer 5. $-10 - 10i = (1 + 3i)(-4 + 2i)$
Dakle, $1 + 3i$ i $-4 + 2i$ su brojevi koji dijele $-10 - 10i$.
Dodatno, provjerimo još ako je $-4 + 2i$ djeljiv s $1 + 3i$.

$$\frac{-4+2i}{1+3i} = \frac{-4+2i}{1+3i} \cdot \frac{1-3i}{1-3i} = \frac{2+14i}{10} = \frac{1}{5} + \frac{7}{5}i.$$

Zaključujemo da $-4 + 2i$ nije djeljiv s $1 + 3i$ u skupu $\mathbb{Z}[i]$ jer smo kao rezultat dobili broj koji nije element tog skupa.

Jedini siguran način za provjeru dijeli li jedan broj drugi je provedba postupka kao u primjeru, to jest, racionalizacija nazivnika nakon koje provjerimo je li rezultat Gaussov cijeli broj. U nekim primjerima ne moramo provoditi taj postupak, već nam neki od idućih rezultata mogu pomoći.

Teorem 3.1. *Gaussov cijeli broj $\alpha = a + bi$ je djeljiv s $c \in \mathbb{Z}$ ako i samo ako $c|a$ i $c|b$.*

Dokaz. Neka $c \in \mathbb{Z}$ dijeli $\alpha = a+bi \in \mathbb{Z}[i]$. To znači da možemo pisati $a+bi = c(m+ni)$, gdje su $m, n \in \mathbb{Z}$. To je ekvivalentno tome da je $a+bi = cm+cni$, to jest $a = cm, b = cn$. Dakle, $c|a$ i $c|b$. □

Ako uzmemo da je $b = 0$ u iskazu prethodnog teorema, vidimo da se djeljivost između cijelih brojeva ne mijenja kada ih promatramo u skupu $\mathbb{Z}[i]$: za $c, a \in \mathbb{Z}$, $c|a$ u $\mathbb{Z}[i]$ ako i samo ako $c|a$ u $\mathbb{Z}$.
Mutiplikativnost norme nam daje idući rezultat koji je u nekim slučajevima koristan da lako provjerimo djeljivost dva Gaussova cijela broja.

Teorem 3.2. *Neka su $\alpha, \beta \in \mathbb{Z}[i]$. Ako $\beta|\alpha$ (u $\mathbb{Z}[i]$), onda $N(\beta)$ dijeli $N(\alpha)$ (u $\mathbb{Z}$).*

Dokaz. $\beta|\alpha \implies \alpha = \beta\gamma,\ \gamma \in \mathbb{Z}[i]$. Djelovanjem norme dobivamo $N(\alpha) = N(\beta)N(\gamma)$ iz čega zaključujemo $N(\beta)|N(\alpha)$. □

Napomena 3.2. *Primijetimo da obrat Teorema 3.2 ne vrijedi općenito. Naime, uzmimo za* $\alpha = 3 - i$*, a za* $\beta = 1 + 2i$*.* $N(\alpha) = 10, N(\beta) = 5$ *pa vidimo da vrijedi da* $N(\beta)$ *dijeli* $N(\alpha)$*, ali* β *ne dijeli* α *(*$\frac{\alpha}{\beta} = \frac{1}{5} - \frac{7}{5}i \notin \mathbb{Z}[i]$*).*

Teorem 3.2 je dobar alat za dokazivanje toga da jedan broj ne dijeli drugi. Ako uzmemo $\alpha, \beta \in \mathbb{Z}[i]$ i za njih vrijedi da $N(\beta)$ ne dijeli $N(\alpha)$, onda odmah možemo zaključiti da $\beta \nmid \alpha$. Dakle, provjera djeljivosti normi u $\mathbb{Z}$ je nužan uvjet za djeljivost u $\mathbb{Z}[i]$ (kada ne vrijedi djeljivost normi, onda ne vrijedi ni djeljivost brojeva u $\mathbb{Z}[i]$), ali to nije dovoljan uvjet.

Korolar 3.3. *Norma Gaussovog cijelog broja je parna ako i samo ako je taj broj djeljiv s* $1 + i$*.*

Dokaz. Ako $1 + i$ dijeli $\alpha \in \mathbb{Z}[i]$, onda $N(1 + i) = 2$ dijeli $N(\alpha)$ pa je norma od α parna. Obratno, pretpostavimo da $a + bi \in \mathbb{Z}[i]$ ima parnu normu tj. $a^2 + b^2 \equiv 0 \pmod 2$. Slijedi da su a i b ili, oba parni, ili, oba neparni. Tada $2|(a - b)$ tj. $a \equiv b \pmod 2$. Želimo naći neke $m, n \in \mathbb{Z}$ takve da možemo napisati $a + bi = (1 + i)(m + ni)$, odnosno, $a + bi = (m - n) + (m + n)i$. Stavimo da je $m = \frac{a+b}{2}$, $n = \frac{a-b}{2}$. Takvi m i n su iz $\mathbb{Z}$ jer je $a \equiv b \pmod 2$ i $a + bi = (1 - i)(\frac{a+b}{2} + \frac{a-b}{2}i)$. Dakle, $(1 + i)|(a + bi)$. □

Primijetimo da su svi Gaussovi cijeli brojevi djeljivi s invertibilnim elementima $1, -1, i$ te $-i$.

Lema 3.4. *Za* $\alpha \in \mathbb{Z}[i], \alpha \neq 0$ *bilo koji djelitelj od* α *kojemu je norma jednaka* $N(\alpha)$ *je umnožak invertibilnog elementa s* α*.*

Dokaz. Neka $\beta|\alpha$ i $N(\beta) = N(\alpha)$. Kako $\beta|\alpha$, onda je $\alpha = \beta\gamma$, $\gamma \in \mathbb{Z}[i]$. Djelovanjem norme dobivamo $N(\alpha) = N(\alpha) \cdot N(\gamma)$ iz čega slijedi $N(\gamma) = 1$ pa je $\gamma \in \{\pm 1, \pm i\}$. Dakle, β mora biti $\pm\alpha$ ili $\pm i\alpha$. □

Prema Lemi 3.4, $\pm\alpha$ i $\pm i\alpha$ su jedini djelitelji od α s normom $N(\alpha)$. Taj rezultat ćemo koristiti u poglavlju o prostim brojevima i faktorizaciji. Dokaz idućeg teorema može se pronaći u [1].

Teorem 3.5 (O dijeljenju s ostatkom)**.** *Za svaka dva Gaussova cijela broja* $\alpha, \beta \in \mathbb{Z}[i]$*,* $\beta \neq 0$*, postoje* $\gamma, \rho \in \mathbb{Z}[i]$ *takvi da je* $\alpha = \gamma \cdot \beta + \rho$ *i* $N(\rho) < N(\beta)$*. Dodatno, možemo izabrati* ρ *tako da vrijedi* $N(\rho) \leq \frac{1}{2}N(\beta)$*.*

Definicija 3.3. *Brojevi γ i ρ se nazivaju kvocijent i ostatak, pri čemu je ostatak ograničen normom djelitelja β.*

Problemi koji se mogu javiti kod računanja brojeva γ i ρ najbolje je ilustrirati jednim primjerom.

Primjer 6. *Neka je $\alpha = 25 - 13i$ i $\beta = 6 + i$. Pokušajmo pronaći γ i ρ tako da je $\alpha = \gamma\beta + \rho$, gdje je $N(\rho) < 37 = N(\beta)$.*

Promotrimo:

$$\frac{\alpha}{\beta} = \frac{\alpha}{\beta} \cdot \frac{\bar{\beta}}{\bar{\beta}} = \frac{137 - 103i}{37} = \frac{137}{37} - \frac{103}{37}i$$

$$\frac{137}{37} = 3.7027, \quad \frac{-103}{37} = -2.783$$

pa stavimo da je $\gamma = 3 - 2i$.

$$\rho = \alpha - \gamma\beta \implies \rho = 5 + 4i, \;\; N(\rho) = 41 \not< 37.$$

Vidimo da smo dobili ρ koji ima puno veću normu od željene pa moramo promijeniti način biranja broja γ.

Iskoristimo teorem o dijeljenju s ostatkom u skupu cijelih brojeva:

$$\frac{137}{37} = 3 + \frac{26}{37}, \quad \frac{-103}{37} = -3 + \frac{8}{37}.$$

Sada stavimo da je $\gamma = 3 - 3i$. Tada je $\rho = 4 + 2i$, što nam odgovara jer je $N(4+2i) = 20$. Očito je teorem o dijeljenju s ostatkom u skupu cijelih brojeva dobar alat kako bi odabrali broj γ.

Ali, Teorem 3.5 nam tvrdi i da postoje γ i ρ takvi da je $N(\rho) \leq \frac{1}{2}N(\beta)$. Uistinu, ako za γ uzmemo $4 - 3i$ dobit ćemo $\rho = -2 + i$, a za njega je norma jednaka $5 < \frac{1}{2} \cdot 37$. (Ovdje smo za γ uzeli onaj broj koji je najbliži[2] broju $\frac{\alpha}{\beta}$.)

Zanimljiva razlika između Teorema o dijeljenju s ostatkom u skupu $\mathbb{Z}$ i skupu $\mathbb{Z}[i]$ je ta da verzija teorema za cijele brojeve garantira jedinstvenost kvocijenta i ostatka, što za Gaussove cijele brojeve nije istina. No, ta činjenica ne smanjuje djelotvornost tog teorema u primjeni.

[2]Ovdje se misli na udaljenost dva kompleksna broja $z_1 = a_1 + b_1 i$ i $z_2 = a_2 + b_2 i$ što se računa po formuli $\sqrt{(a_1 - a_2)^2 + (b_1 - b_2)^2}$.

Primjer 7. *U ovom primjeru uzmimo da je* $\alpha = 1 + 8i,\ \beta = 2 - 4i.$

$$\frac{\alpha}{\beta} = \frac{-3}{2} + i$$

Kako je $\frac{-3}{2}$ *točno između* -2 *i* -1 *za* γ *možemo uzeti* $-2 + i$ *ili* $-1 + i$.
Koristeći prvu opciju dobivamo $\alpha = (-2 + i)\beta + 1 - 2i$, *iz druge* $\alpha = (-1 + i)\beta - 1 + 2i$.
U oba slučaja je $N(\rho) = 5 < 20 = N(\beta)$.

3.1 Euklidov algoritam

Euklidov algoritam je metoda za pronalaženje najvećeg zajedničkog djelitelja dvaju brojeva a i b, u oznaci $M(a, b)$. Kako u $\mathbb{Z}[i]$ nemamo definiran uređaj, točnije relaciju $\leq$, podrazumijevamo da je najveći zajednički djelitelj onaj koji ima najveću normu. Odmah možemo primijetiti da, ako je δ najveći zajednički djelitelj brojeva α i β, onda su to i brojevi $-\delta$, $i\delta$, $-i\delta$, a možda ima i drugih.

Definicija 3.4. *Za* $\alpha, \beta \in \mathbb{Z}[i]$ *kažemo da su relativno prosti ako su im jedini zajednički djelitelji* $1, -1, i$ *te* $-i$.

Teorem 3.6 (Euklidov algoritam)**.** *Neka su* $\alpha, \beta \in \mathbb{Z}[i],\ \alpha, \beta \neq 0$. *Pretpostavimo da je uzastopnom primjenom Teorema o dijeljenju s ostatkom u* $\mathbb{Z}[i]$ *dobiven niz jednakosti:*

$$\begin{aligned} \alpha &= \beta \cdot \gamma_1 + \rho_1, & N(\rho_1) &< N(\beta) \\ \beta &= \rho_1 \cdot \gamma_2 + \rho_2, & N(\rho_2) &< N(\rho_1) \\ \rho_1 &= \rho_2 \cdot \gamma_3 + \rho_3, & N(\rho_3) &< N(\rho_2) \\ &\vdots \end{aligned}$$

Posljednji ostatak različit od nule djeljiv je sa svim zajedničkim djeliteljima od α *i* β *te je i sam njihov zajednički djelitelj pa je najveći zajednički djelitelj brojeva* α *i* β.

Dokaz. Krenuvši od prve jednadžbe nadalje, zaključujemo da svaki zajednički djelitelj od α i β dijeli posljednji nenul ostatak. Ako krenemo obrnuto, od zadnje jednadžbe prema prvoj, zaključimo da je posljednji nenul ostatak zajednički djelitelj od α i β. Stoga, taj posljednji nenul ostatak je djeljiv sa svim ostalim zajedničkim djeliteljima brojeva α i β pa među zajedničkim djeliteljima ima maksimalnu normu. Prema tome, posljednji nenul ostatak je najveći zajednički djelitelj brojeva α i β. □

Primjer 8. *Pronađimo najveći zajednički djelitelj brojeva* $\alpha = 32 + 11i$ *i* $\beta = 8 + 9i$.

$$32 + 11i = (8 + 9i)(2 - i) + 7 + i$$

$$8 + 9i = (7 + i)(1 + i) + 2 + i$$

$$7 + i = (2 + i)(3 - i) + 0.$$

Posljednji nenul ostatak je $2 + i$ *pa je taj broj najveći zajednički djelitelj od* $\alpha = 32 + 11i$ *i* $\beta = 8 + 9i$*, to jest,* $M(\alpha, \beta) = 2 + i$.

Primjer 9. *Dokažimo da su* $4 - 5i$ *i* $4 + 5i$ *relativno prosti:*

$$4 - 5i = (4 + 5i)(-i) - 1 - i$$

$$4 + 5i = (-1 - i)(-5 - i) - i$$

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

Posljednji nenul ostatak je $-i$*, odnosno za brojeve* $4-5i$ *i* $4+5i$ *jedini zajednički djelitelji su* $1, -1, i$ *te* $-i$ *pa zaključujemo da su* $4 - 5i$ *i* $4 + 5i$ *relativno prosti.*

U prethodnom primjeru drugu jednadžbu smo mogli napisati i drugačije:
$4 + 5i = (-1 - i)(-5) - 1, \quad 4 + 5i = (-1 - i)(-4) + i, \quad 4 + 5i = (-1 - i)(-4 - i) + 1.$
U svakom od tih slučajeva posljednji nenul ostatak je jedan od invertibilnih elemenata te bi iz bilo kojeg od njih došli do istog zaključka.

Napomena 3.5. *Iz Teorema 3.2 slijedi: Ako je* $M(\alpha, \beta) = \delta$*, onda* $N(\delta)$ *dijeli* $N(\alpha)$ *i* $N(\beta)$ *pa dijeli i* $M(N(\alpha), N(\beta))$.

U Primjeru 8 je $N(\alpha) = 1145 = 229 \cdot 5$ i $N(\beta) = 145 = 29 \cdot 5$ pa je $M(N(\alpha), N(\beta)) = 5 = N(\delta)$. Naravno, može biti i da je $N(\delta) < M(N(\alpha), N(\beta))$ kao u Primjeru 9, gdje su $4 - 5i$ i $4 + 5i$ ($N(4 \pm 5i) = 41$) relativno prosti pa im najveći zajednički djelitelj ima normu 1.
Pretpostavimo da je $M(N(\alpha), N(\beta)) = 1$. U tom slučaju bilo koji djelitelj od α i β mora imati normu koja dijeli 1 pa su jedini djelitelji od α i β invertibilni elementi (jedino $1, -1, i$ te $-i$ imaju normu jednaku 1). Dakle, Gaussovi cijeli brojevi koji imaju relativno proste norme su relativno prosti. (Obrat ne vrijedi, kao što je prikazano u Primjeru 9 za $4 \pm 5i$.) Koristeći tu tvrdnju, ako pokažemo da je $M(N(\alpha), N(\beta)) = 1$, onda odmah znamo da su α i β relativno prosti u $\mathbb{Z}[i]$.

Idući korolar Euklidovog algoritma nam kaže da je najveći zajednički djelitelj dvaju brojeva u $\mathbb{Z}[i]$ jedinstven do na umnožak s invertibilnim elementima.

Korolar 3.7. *Neka su α i β nenul elementi iz $\mathbb{Z}[i]$ i neka je δ njihov najveći zajednički djelitelj dobiven Euklidovim algoritmom. Tada je bilo koji najveći zajednički djelitelj od α i β jednak $\delta \cdot u$, gdje je $u \in \{\pm 1, \pm i\}$.*

Dokaz. Neka je $\delta' \in \mathbb{Z}[i]$ najveći zajednički djelitelj od α i β. Iz dokaza Euklidovog algoritma imamo da $\delta' | \delta$, to jest, $\delta = \delta'\gamma$ pa je $N(\delta) = N(\delta')N(\gamma) \geq N(\delta')$. Zato što je δ' najveći zajednički djelitelj, njegova norma je maksimalna među normama svih zajedničkih djelitelja. Iz toga slijedi da mora biti $N(\delta) = N(\delta')$. Slijedi $N(\gamma) = 1$ pa je $\gamma \in \{\pm 1, \pm i\}$. Dakle, $\delta' = \delta \cdot \gamma$, pri čemu je $\gamma \in \{\pm 1, \pm i\}$. □

3.2 Bezoutov identitet

Bezoutov identitet (ili Bezoutova lema) je fundamentalni rezultat u teoriji brojeva, a kaže da za bilo koja dva nenul cijela broja a i b postoje $x, y \in \mathbb{Z}$ takvi da je $M(a, b) = ax + by$. Analogon te tvrdnje vrijedi i u skupu Gaussovih cijeli brojeva.

Teorem 3.8 (Bezoutov identitet)**.** *Neka je δ bilo koji najveći zajednički djelitelj nenul brojeva $\alpha, \beta \in \mathbb{Z}[i]$. Tada je $\delta = \alpha x + \beta y$, za neke $x, y \in \mathbb{Z}[i]$.*

Korolar 3.9. *Nenul Gaussovi cijeli brojevi α i β su relativno prosti ako i samo ako je $1 = \alpha x + \beta y$, za neke $x, y \in \mathbb{Z}[i]$.*

Brojevi x i y zovu se Bezoutovi koeficijenti, a lako se pronađu tako da provedemo Euklidov algoritam "unatrag". Često se taj postupak naziva prošireni Euklidov algoritam. Jasno je da koeficijenti x i y, kao i najveći zajednički djelitelj, nisu jedinstveni.

Primjer 10. *U primjeru 8 Euklidovim algoritmom smo izračunali da je $2 + i$ najveći zajednički djelitelj brojeva $32 + 11i$ i $8 + 9i$. Sada možemo provesti taj postupak unatrag da bi $2 + i$ izrazili u obliku $2 + i = \alpha x + \beta y$.*

$$\begin{aligned}
2 + i &= 8 + 9i - (7 + i)(1 + i) \\
&= 8 + 9i - ((32 + 11i) - (8 + 9i)(2 - i))(1 + i) \\
&= 8 + 9i - (32 + 11i)(1 + i) + (8 + 9i)(2 - i)(1 + i) \\
&= -\alpha(1 + i) + \beta(1 + (2 - i)(1 + i)) \\
&= \alpha(-1 - i) + \beta(4 + i).
\end{aligned}$$

Primjer 11. *U primjeru 9 vidjeli smo da su* $4-5i$ *i* $4+5i$ *relativno prosti. Vrijedi:*

$$\begin{aligned}-i &= 4+5i-((-1-i)(-5-i))\\ &= 4+5i-((4-5i)-(4+5i)(-i))(-5-i)\\ &= (4+5i)(1+(-i)(-5-i))-(4-5i)(-5-i)\\ &= (4+5i)(5i)+(4-5i)(5+i).\end{aligned}$$

Množeći posljednju jednadžbu s i dobivamo:

$$1 = (4+5i)(-5)+(4-5i)(-1+5i).$$

4 Prosti brojevi i faktorizacija

Prosti brojevi u skupu cijelih brojeva su oni koji su djeljivi samo s 1 i sa samim sobom. Brojeve $a_1, a_2, ..., a_n$ takve da je $a = a_1 \cdot a_2 \cdot ... \cdot a_n$ zovemo faktorima od a. Dakle, cijeli broj a je prost ako su jedini njegovi faktori ± 1 i $\pm a$. Analogno tome ćemo uvesti proste brojeve u skupu $\mathbb{Z}[i]$.

Kada je $N(\alpha) > 1$, za $\alpha \in \mathbb{Z}[i]$, 8 očitih faktora je $\pm 1, \pm i, \pm\alpha, \pm i\alpha$. Njih zovemo trivijalnim faktorima. Bilo koji drugi faktor od α naziva se netrivijalan. Po Lemi 3.4, svi netrivijalni faktori od α imaju normu veću od 1 i manju od $N(\alpha)$. Shodno tome, razlikujemo trivijalnu i netrivijalnu faktorizaciju. Ako je $\alpha = \beta\gamma$, pri čemu je $N(\beta), N(\gamma) > 1$, onda je ta faktorizacija netrivijalna.

Definicija 4.1. *Neka je* α *Gaussov cijeli broj takav da je* $N(\alpha) > 1$. *Kažemo da je* α *prost ako ima samo trivijalne faktore. Inače kažemo da je složen.*

Primjer 12. *Trivijalna faktorizacija od* $9+2i$ *je* $i(2-9i)$, *a netrivijalna* $(1-2i)(1+4i)$.

Zanimljivo je uočiti da neki brojevi koji su prosti u $\mathbb{Z}$, to neće biti u $\mathbb{Z}[i]$.

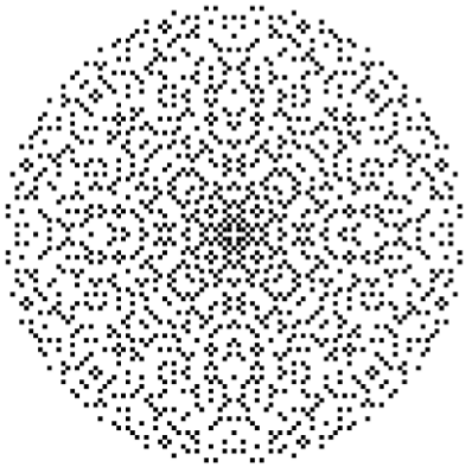
Primjer 13. *Broj* 5 *je u skupu* $\mathbb{Z}$ *prost, ali u* $\mathbb{Z}[i]$ *nije. Primijetimo da možemo pisati* $5 = (1+2i)(1-2i)$. *Također, i broj* 2 *je složen u* $\mathbb{Z}[i]$ *jer je* $2 = (1+i)(1-i)$. *No, broj* 3 *ostaje prost i kao Gaussov cijeli broj.*

Za provjeru prostosti Gaussovog cijelog broja, korisnom se pokazuje norma zahvaljujući kojoj taj problem promatramo u skupu cijelih brojeva u kojem nam je praktičnije raditi.

Teorem 4.1. *Ako je norma Gaussovog cijelog broja $\alpha = a + bi$, pri čemu je $a, b \neq 0$, prost broj u $\mathbb{Z}$, onda je α prost u $\mathbb{Z}[i]$.*

Dokaz. Neka je $p = N(\alpha)$ prost broj i $\alpha = \beta\gamma,\ \beta, \gamma \in \mathbb{Z}[i]$. Primjenom norme dobivamo $p = N(\beta)N(\gamma)$. p, $N(\beta)$ i $N(\gamma)$ su nenegativni cijeli brojevi i p je prost pa je jedan od brojeva $N(\beta)$ i $N(\gamma)$ jednak 1. Odnosno, jedan od β i γ je invertibilni element. Zaključujemo da α nema netrivijalnu faktorizaciju. □

Napomena 4.2. *Obrat Teorema 4.1 ne vrijedi, odnosno, ako je Gaussov cijeli broj prost, to ne znači da je njegova norma prost broj. Primjerice, 3 je prost u $\mathbb{Z}[i]$, ali njegova norma, koja je jednaka 9, je složen cijeli broj.*



Slika 2: Gaussovi prosti brojevi s normom manjom od 1000 ([4])

Teorem 4.2. *Svaki $\alpha \in \mathbb{Z}[i]$ takav da je $N(\alpha) > 1$ se može prikazati kao produkt prostih brojeva iz $\mathbb{Z}[i]$.*

Dokaz. Dokaz provodimo indukcijom po $N(\alpha)$. Neka je $N(\alpha) = 2$. Po teoremu 4.1 je α prost. Pretpostavimo da tvrdnja vrijedi za sve Gaussove cijele brojeve s normom jednakom k, za neki $k \in \mathbb{N}$. Neka je sada $N(\alpha) = k+1$. Ako ne postoji $\alpha \in \mathbb{Z}[i]$ takav da je $N(\alpha) = k + 1$, onda nemamo što pokazati. Pretpostavimo da postoji $\alpha \in \mathbb{Z}[i]$ takav da je $N(\alpha) = k+1$. Ako je α prost, onda je on produkt prostih brojeva iz $\mathbb{Z}[i]$. Ako je α složen, onda ga možemo zapisati kao $\alpha = \beta\gamma,\ \beta, \gamma \in \mathbb{Z}[i]$, pri čemu je $N(\beta), N(\gamma) < N(\alpha) = k+1$. Po pretpostavci indukcije, β i γ se mogu prikazati kao produkti prostih faktora u $\mathbb{Z}[i]$. Prema tome, njihov produkt, koji je jednak α, je produkt prostih brojeva iz $\mathbb{Z}[i]$. □

Sad kad smo pokazali egzistenciju faktorizacije na proste faktore, želimo doći do jedinstvenosti te faktorizacije. Međutim, ta jedinstvenost nije jedinstvenost u doslovnom smislu. Ovdje ćemo dobiti jedinstvenost do na umnožak s invertibilnim elementima.

Primjer 14. $5 = (1+2i)(1-2i) = (2-i)(2+i)$. *Svi ovi faktori su prosti pa bi mogli zaključiti da broj* 5 *nema jedinstvenu prostu faktorizaciju. Ali, primijetimo da je* $1+2i = (2-i)i \;\; i \;\; 1-2i = (2+i)(-i)$.

Dokaz idućeg teorema može se pronaći u [1].

Teorem 4.3. *Svaki* $\alpha \in \mathbb{Z}[i]$ *s normom većom od* 1 *ima jedinstveni rastav na proste faktore u sljedećem smislu: Ako je*

$$\alpha = \pi_1\pi_2...\pi_r = \pi_1'\pi_2'...\pi_s',$$

gdje su π_i, π_j' *prosti u* $\mathbb{Z}[i]$, *za* $i \in \{1,2,...,r\}, \;\; j \in \{1,2,...,s\}$, *onda je* $r = s$ *i svaki* π_i *je umnožak nekog* π_j' *s invertibilnim elementom.*

Za određivanje rastava Gaussovog cijelog broja na proste faktore poslužit ćemo se normom, to jest, činjenicom da, ako je $\alpha = \beta\gamma$, onda je i $N(\alpha) = N(\beta)N(\gamma)$.

Primjer 15. *Uzmimo za* α *broj* $4+3i$. $N(\alpha) = 25 = 5 \cdot 5$. *Gaussovi cijeli brojevi s normom* 5 *su* $1+2i$ *i* $1-2i$ *te njihovi umnošci s invertibilnim elementima. Pokušajmo* $4+3i$ *zapisati kao umnožak nekih od njih.*

$$(1+2i)(1-2i) = 5, \quad (1+2i)(2+i) = 5i, \quad (1+2i)(-2+i) = -4-3i.$$

Uočimo da je posljednji umnožak jednak $-\alpha$ *pa je* $-(-4-3i) = -(1+2i)(-2+i)$. *Dobivamo da je* $(1+2i)(2-i)$ *rastav od* $4+3i$ *na proste faktore.*

5 Modularna aritmetika

U ovom poglavlju ćemo se pozabaviti relacijom kongruencije. Teoriju kongruencija je uveo C.F. Gauss u djelu *Disquisitiones arithmeticae* čiji se naslov prevodi kao Aritmetičke rasprave. Analogno kao u skupu cijelih brojeva definiramo relaciju kongruencije za Gaussove cijele brojeve.

Definicija 5.1. *Neka su* $\alpha, \beta, \gamma \in \mathbb{Z}[i]$. *Kažemo da je* α *kongruentno s* β *modulo* γ *ako* $\gamma | (\alpha - \beta)$. *Pišemo:* $\alpha \equiv \beta \pmod{\gamma}$ *ili* $\alpha \equiv_\gamma \beta$.

Napomena 5.2. *Primijetimo da* $\alpha \equiv 0 \pmod{\gamma}$ *znači da je* α *djeljivo s* γ.

Primjer 16. *Provjerimo vrijedi li* $1 + 12i \equiv 2 - i \pmod{3 + i}$.

$$\frac{1 + 12i - (2 - i)}{3 + i} = \frac{-1 + 13i}{3 + i} = 1 + 4i.$$

Rezultat je u $\mathbb{Z}[i]$ *pa možemo reći da je* $1 + 12i$ *kongruentno s* $2 - i$ *modulo* $3 + i$.

Propozicija 5.1. *Relacija "biti kongruentno modulo* γ*" je relacija ekvivalencije.*

Dokaz. Neka su $\alpha, \beta \in \mathbb{Z}[i]$.

- refleksivnost: $\alpha \equiv \alpha \pmod{\gamma}$ jer $\gamma | 0, \ \forall \gamma \in \mathbb{Z}[i]$.
- simetričnost: Pretpostavimo da je $\alpha \equiv \beta \pmod{\gamma}$. Tada $\gamma | (\alpha - \beta)$ odnosno postoji $\delta \in \mathbb{Z}[i]$ takav da je $\delta\gamma = \alpha - \beta$. Pomnožimo tu jednadžbu s -1 i dobijemo $-\delta\gamma = \beta - \alpha$ pa kako je $-\delta \in \mathbb{Z}[i]$ onda $\gamma | (\beta - \alpha)$ što znači da je $\beta \equiv \alpha \pmod{\gamma}$.
- tranzitivnost: Pretpostavimo da je $\alpha \equiv \beta \pmod{\gamma}$ i $\beta \equiv \epsilon \pmod{\gamma}$. To znači da $\gamma | (\alpha - \beta)$ i $\gamma | (\beta - \epsilon)$ pa postoje $\delta_1, \delta_2 \in \mathbb{Z}[i]$ takvi da je $\delta_1\gamma = \alpha - \beta$ i $\delta_2\gamma = \beta - \epsilon$. Posljednje dvije jednadžbe možemo zbrojiti. Dobivamo da je $(\delta_1 + \delta_2)\gamma = \alpha - \epsilon$. Vrijedi $\delta_1 + \delta_2 \in \mathbb{Z}[i]$ pa slijedi da $\gamma | \alpha - \epsilon$ pa zaključujemo da je $\alpha \equiv \epsilon \pmod{\gamma}$

□

Budući da relacija ekvivalencije dijeli skup na kojem je definirana na klase ekvivalencije znamo da je relacijom kongruencije definiran kvocijentni skup $\mathbb{Z}[i]/_{\equiv_\gamma}$. Gaussovi cijeli brojevi α i β se nalaze u istoj klasi ekvivalencije ako je $\alpha \equiv_\gamma \beta$.
Gaussov cijeli broj možemo "reducirati" modulo γ tako da ga podijelimo s γ i promotrimo ostatak. Time dobivamo Gaussov cijeli broj kongruentan početnom, ali s manjom normom.

Primjer 17. *Reducirajmo* $1+8i$ *modulo* $2-4i$. *U Primjeru 7 te smo brojeve već podijelili i dobili dvije mogućnosti:*

$$1 + 8i = (2 - 4i)(-2 + i) + 1 - 2i, \qquad 1 + 8i = (2 - 4i)(-1 + i) - 1 + 2i.$$

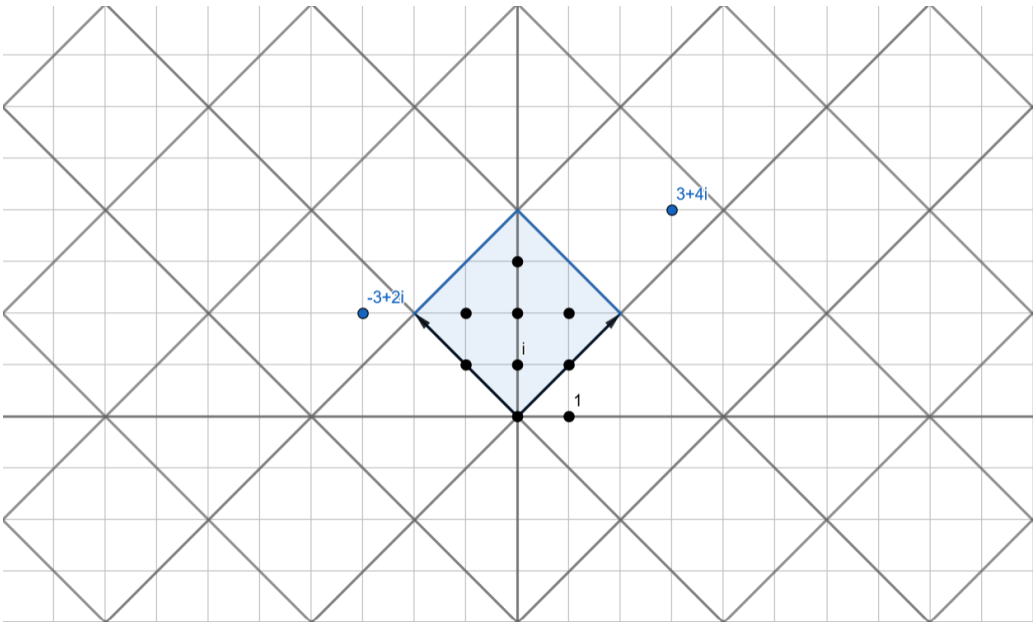
Dakle, $1 + 8i \equiv 1 - 2i \pmod{2 - 4i}$ *i* $1 + 8i \equiv -1 + 2i \pmod{2 - 4i}$

Postoji interesantan način kojim se može slikovito prikazati kako djeluje modularna aritmetika u $\mathbb{Z}[i]$.

Primjer 18. *Neka je* $\gamma = 2 + 2i$ *i uočimo kako izgledaju umnošci od* γ *s elementima iz* $\mathbb{Z}[i]$*, odnosno, višekratnici od* $2 + 2i$*.*

$$(2 + 2i)(m + ni) = (2 + 2i)m + (2 + 2i)ni = (2 + 2i)m + (-2 + 2i)n, \quad m, n \in \mathbb{Z}.$$

$\mathbb{Z}[i]$*-višekratnici od* $2 + 2i$ *su zapravo linearne kombinacije od* $2 + 2i$ *i* $-2 + 2i$*. Ako ih promatramo kao vektore tj. svaki Gaussov cijeli broj* $x + yi$ *interpretiramo kao vektor* $(x, y) \in \mathbb{R}^2$*, onda ih možemo prikazati u kompleksnoj ravnini. Dobivamo popločavanje ravnine kvadratima koji imaju Gaussove višekratnike od* $2 + 2i$ *kao vrhove.*



Slika 3: $\mathbb{Z}[i]$-višekratnici od $2 + 2i$ ([5])

Ako se dva Gaussova cijela broja nalaze na istoj relativnoj poziciji unutar različitih kvadrata, onda su oni kongruentni modulo $2 + 2i$*. Ovo vrijedi zato što svaki kvadrat dijeli stranice s* 4 *kvadrata pa je pomicanje iz neke pozicije jednog kvadrata na istu poziciju u susjednom kvadratu ekvivalentno translaciji za neki od vektora* $\pm(2 + 2i), \pm(-2 + 2i)$*. Prema tome, sa slike 3 iščitavamo da su* $-3 + 2i$ *i* $3 + 4i$ *kongruentni modulo* $2 + 2i$*. Nadalje, sa slike 3 možemo odrediti kvocijentni skup* $\mathbb{Z}[i]/_{\equiv_{2+2i}}$*. Uzmimo kvadrat koji je obojan plavom bojom i napravimo listu Gaussovih cijelih brojeva koji određuju pozicije unutar njega, pozicije na dvjema susjednim stranicama i jedan vrh tog kvadrata. To su:* $0,\ i,\ 2i,\ 3i,\ 1 + i,\ -1 + i,\ -1 + 2i$ *te* $1 + 2i$*. Svaki Gaussov cijeli broj je kongruentan modulo* $2 + 2i$ *s točno jednim od njih.*

Koristan rezultat modularne aritmetike iz $\mathbb{Z}$ je Fermatov mali teorem koji kaže da za p prost i $a \in \mathbb{N}$ takve da $p \nmid a$ vrijedi $a^{p-1} \equiv 1 \pmod{p}$. Sjetimo se da se $p-1$ u eksponentu pojavio zato što postoji $p-1$ nenul brojeva koji daju različite ostatke pri dijeljenju s p. Imajući to na umu, možemo izreći $\mathbb{Z}[i]$-analogon Fermatovog malog teorema koji navodimo bez dokaza.

Teorem 5.2. *Neka je π prost Gaussov cijeli broj i označimo s $n(\pi)$ broj elemenata u $\mathbb{Z}[i]/_{\equiv_\pi}$. Ako $\pi \nmid \alpha$, onda je $\alpha^{n(\pi)-1} \equiv 1 \pmod{\pi}$.*

Kako bi nam prethodni teorem zapravo bio koristan trebamo formulu za $n(\pi)$ kada je π bilo koji Gaussov cijeli broj. Dokaz idućeg teorema može se pronaći u [1].

Teorem 5.3. *Ako je $\alpha \neq 0$ u $\mathbb{Z}[i]$, onda je $n(\alpha) = N(\alpha)$.*

U primjeru 18 je vidljivo da je $|\mathbb{Z}[i]/_{\equiv_{2+2i}}| = 8$, a s obzirom da je $N(2+2i) = 8$, onda je $n(2+2i) = N(2+2i)$, što je u skladu s prethodnim teoremom.

6 Skup $\mathbb{Z}[i]$ i aritmetika skupa $\mathbb{Z}$

Sve primjene skupa $\mathbb{Z}[i]$ na svojstva u $\mathbb{Z}$ vezane su uz zbroj dva kvadrata. Koristeći formulu $a^2+b^2 = (a+bi)(a-bi)$, sumu kvadrata na lijevoj strani prikazujemo kao umnožak brojeva iz $\mathbb{Z}[i]$. Iz toga je jasno zašto su svojstva skupa Gaussovih cijelih brojeva relevantna kod analize zbroja dva kvadrata u skupu cijelih brojeva.

Teorem 6.1. *Neka je $p \in \mathbb{Z}$ prost broj. Ako je $p = a^2 + b^2$, onda su a^2 i b^2 jedinstveni do na poredak (a i b su jedinstveni do na poredak i predznak).*

Dokaz. Neka je $p = a^2 + b^2$, gdje je p prost cijeli broj i $a, b \in \mathbb{Z}$. U $\mathbb{Z}[i]$ faktorizacija od p je $(a+bi)(a-bi)$. Zbog multiplikativnosti norme je $N(p) = N(a+bi)N(a-bi)$ iz čega slijedi da je $N(a+bi) = p = N(a-bi)$. Po Teoremu 4.1, $a+bi$ i $a-bi$ su prosti u $\mathbb{Z}[i]$. Pretpostavimo da postoje neki $c, d \in \mathbb{Z}$ različiti od a i b takvi da je $p = c^2 + d^2$ tj. $p = (c+di)(c-di)$. Analogno kao za $a \pm bi$, mora biti da su $c+di$ i $c-di$ također prosti u $\mathbb{Z}[i]$. Po Teoremu o jedinstvenoj faktorizaciji u $\mathbb{Z}[i]$ (4.3) imamo:

$$a + bi = u(c + di) \;\; ili \;\; a + bi = u(c - di),$$

gdje je $u \in \{\pm 1, \pm i\}$. Promotrimo slučaj kada je $a + bi = u(c + di)$. Ako je $u = 1$, onda je $c = a$ i $d = b$. Ako je $u = -1$, onda je $c = -a$ i $d = -b$. Ako je $u = i$, onda je $c = b$ i

$d = -a$. Ako je $u = -i$, onda je $c = -b$ i $d = a$. Dakle, c i d su jednaki kao a i b do na poredak i predznak. Analogno bi se pokazalo ako bi uzeli da je $a + bi = u(c - di)$. □

U prethodnom teoremu vidljivo je da svaki $p \in \mathbb{Z}$ prost, možemo na jedinstven način zapisati kao zbroj dva kvadrata, ali to ne vrijedi i za sve složene cijele brojeve. Skup $\mathbb{Z}[i]$ iskoristit ćemo za generiranje cijelih brojeva koji se mogu zapisati kao zbroj dva kvadrata na više načina.

Primjer 19. *Promotrimo faktorizacije* $5 = (1 + 2i)(1 - 2i)$ *i* $13 = (2 + 3i)(2 - 3i)$. *Njihov umnožak možemo zapisati kao:*

$$5 \cdot 13 = ((1 + 2i)(2 + 3i)) \cdot ((1 - 2i)(2 - 3i)),$$

$$5 \cdot 13 = ((1 + 2i)(2 - 3i)) \cdot ((1 - 2i)(2 + 3i)).$$

Iz te dvije jednadžbe dobivamo: $65 = (-4 + 7i) \cdot (-4 - 7i) = (8 + i) \cdot (8 - i)$. *Dakle,* $65 = 4^2 + 7^2 = 8^2 + 1^2$.

Možemo zaključiti da različiti prikazi cijelog broja kao zbroja dva kvadrata u $\mathbb{Z}$ odgovora preslagivanju prostih faktora u $\mathbb{Z}[i]$. Isti postupak možemo iskoristiti za dobivanje cijelog broja koji je suma dva kvadrata cijelih brojeva na tri različita načina.

Primjer 20. $5 = (1 + 2i)(1 - 2i)$, $13 = (2 + 3i)(2 - 3i)$, $17 = (1 + 4i)(1 - 4i)$.
Uzmimo umnoške:

$$(1 + 2i)(2 + 3i)(1 + 4i) = -32 - 9i,$$

$$(1 - 2i)(2 + 3i)(1 + 4i) = 12 + 31i,$$

$$(1 + 2i)(2 - 3i)(1 + 4i) = 4 + 33i.$$

Sada možemo pisati:

$$5 \cdot 13 \cdot 17 = 1105 = 9^2 + 32^2 = 12^2 + 31^2 = 4^2 + 33^2.$$

Sada ćemo skup Gaussovih cijelih brojeva iskoristiti za klasifikaciju Pitagorinih trojki.

Definicija 6.1. *Uređenu trojku prirodnih brojeva* (x, y, z) *zovemo Pitagorina trojka ako vrijedi da je* $x^2 + y^2 = z^2$ *tj. ako su* x *i* y *duljine kateta, a* z *duljina hipotenuze pravokutnog trokuta. Ako su x, y, z relativno prosti, onda kažemo da je* (x, y, z) *primitivna Pitagorina trojka.([2])*

Ako bilo koja dva od brojeva x, y i z imaju zajednički prosti faktor, onda je to faktor i trećeg. Također, u svakoj primitivnoj Pitagorinoj trojki točno je jedan od brojeva x i y paran, dok je z uvijek neparan. Naime, ako pretpostavimo da su x i y oba parni (tada nisu relativno prosti), onda (x, y, z) ne bi bila primitivna Pitagorina trojka. A ako pretpostavimo da su x i y neparni tada bi vrijedilo $x^2 \equiv 1 \pmod 4$ i $y^2 \equiv 1 \pmod 4$. Relacija kongruencije se dobro ponaša sa zbrajanjem pa slijedi $z^2 = x^2 + y^2 \equiv 2 \pmod 4$, ali to ne može biti jer ne postoji $m \in \mathbb{Z}$ takav da je $m^2 \equiv 2 \pmod 4$.

Teorem 6.2. *Svaka primitivna Pitagorina trojka* (x, y, z), *gdje je* x *neparan, ima oblik:*

$$x = m^2 - n^2, \;\; y = 2mn, \;\; z = m^2 + n^2,$$

pri čemu je $m > n > 0, \;\; m, n \in \mathbb{N}, \;\; M(m, n) = 1.$

Dokaz. Jednadžbu $x^2 + y^2 = z^2$ možemo zapisati u obliku $(x + yi)(x - yi) = z \cdot z$. Neka je δ zajednički djelitelj od $(x + yi)$ i $(x - yi)$ u $\mathbb{Z}[i]$. Tada δ dijeli njihovu sumu i razliku tj. $\delta \mid 2x$ i $\delta \mid 2yi$, odnosno, $\delta \mid 2x$ i $\delta \mid 2y$. Nadalje, $\delta^2 | z^2$ pa $N(\delta)^2 | z^4$, a z^4 je neparan pa je i $N(\delta)$ neparan. Po Korolaru 3.3, $1 + i$ dijeli δ ako i samo ako je $N(\delta)$ parna. Slijedi, $(1 + i) \nmid \delta$, a to je ekvivalentno s tim da je δ relativno prost s 2 (jer je $2 = -i(1 + i)^2$, a $1 + i$ je prost). Sada, možemo pisati $\delta \mid x$ i $\delta \mid y$. Iz toga što su x i y relativno prosti u $\mathbb{Z}$ pa i u $\mathbb{Z}[i]$, slijedi da je $\delta \in \{\pm 1, \pm i\}$. Pokazali smo da su $(x + yi)$ i $(x - yi)$ relativno prosti. U jednadžbi $(x + yi)(x - yi) = z^2$ s lijeve strane su dva relativno prosta Gaussova cijela broja čiji je umnožak kvadrat. Teorem 4.3 kaže da je svaki faktor s lijeve strane također kvadrat pomnožen s invertibilnim elementom. Dakle, može biti:

$$x + yi = (m + ni)^2 \quad ili \quad x + yi = i(m + ni)^2, \quad m + ni \in \mathbb{Z}[i].$$

$$x + yi = (m^2 - n^2) + (2mn)i \quad ili \quad x + yi = -2mn + (m^2 - n^2)\, i.$$

Po pretpostavci teorema, x je neparan pa ostaje samo prva mogućnost.
Iz $x + yi = (m^2 - n^2) + (2mn)i$ slijedi: $x = m^2 - n^2, \quad y = 2mn.$
Stoga, $z^2 = (m^2 - n^2)^2 + (2mn)^2 = m^4 - 2m^2n^2 + n^4 + 4m^2n^2 = (m^2 + n^2)^2$. Zaključujemo, $x = m^2 - n^2, \;\; y = 2mn, \;\; z = m^2 + n^2.$ □

m	2	3	4	5	4
n	1	2	1	2	3
$x = m^2 - n^2$	3	5	15	21	7
$y = 2mn$	4	12	8	20	24
$z = m^2 + n^2$	5	13	17	29	25

Tablica 1: Neke primitivne Pitagorine trojke

Iz dokaza Teorema 6.2 proizlazi lagan način za dobivanje Pitagorinih trojki. Jednostavno uzmemo neki $\alpha \in \mathbb{Z}[i]$ kojemu realni i imaginarni dio nisu 0 te ga kvadriramo. Recimo da je $\alpha^2 = a + bi$. Tada je $(|a|, |b|, N(\alpha))$ Pitagorina trojka.

Primjer 21. *Neka je* $\alpha = 9 + 8i$. *Tada je* $(9 + 8i)^2 = (9^2 - 8^2) - (2 \cdot 9 \cdot 8)i = 17 + 144i$ *i* $N(9 + 8i) = 9^2 + 8^2 = 145$. *Dakle,* $(17, 144, 145)$ *je Pitagorina trojka. Štoviše, to je primitivna Pitagorina trojka jer su* 8 *i* 9 *relativno prosti.*

7 Zaključak

U završnom radu smo uveli skup Gaussovih cijelih brojeva tj. skup $\mathbb{Z}[i]$. Taj skup je proširenje skupa $\mathbb{Z}$ na određene kompleksne brojeve, odnosno, elementi od $\mathbb{Z}[i]$ su brojevi oblika $a + bi,\ a, b \in \mathbb{Z}$. Skup $\mathbb{Z}[i]$ je s operacijama zbrajanja i množenja komutativni prsten s jedinicom. Vidjeli smo i da u $\mathbb{Z}[i]$ vrijede neke tvrdnje analogne onima koje vrijede u $\mathbb{Z}$ kao što su Teorem o dijeljenju s ostatkom, Euklidov algoritam i jedinstvenost rastava na proste faktore. Također, proučili smo primjene skupa $\mathbb{Z}[i]$ na aritmetiku u $\mathbb{Z}$ te modularnu aritmetiku u $\mathbb{Z}[i]$.

Popis slika

Popis tablica

Literatura

[1] K.Conrad, *The Gaussian Integers*, 2013, https://api.semanticscholar.org/CorpusID:17483435

[2] A.Dujella, *Teorija brojeva*, Školska Knjiga, Zagreb, 2019.

[3] https://math.libretexts.org/Bookshelves/Combinatorics_and_Discrete_Mathematics/Elementary_Number_Theory_(Barrus_and_Clark)/01%3A_Chapters/1.13%3A_The_Gaussian_Integers

[4] https://mathworld.wolfram.com/GaussianPrime.html

[5] https://www.geogebra.org/calculator

[6] https://www.sophiararebooks.com/pages/books/6172/carl-friedrich-gauss/theoria-residuorum-biquadraticorum-commentatio-prima-secunda