# Gaussovi cijeli brojevi

**Petrić, Ines**

**Undergraduate thesis / Završni rad**

**2016**

*Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj:* **Josip Juraj Strossmayer University of Osijek, Department of Mathematics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku**

*Permanent link / Trajna poveznica:* https://urn.nsk.hr/urn:nbn:hr:126:587525

*Rights / Prava:* In copyright / Zaštićeno autorskim pravom.

*Download date / Datum preuzimanja:* **2024-03-29**



*Repository / Repozitorij:*

Repository of School of Applied Mathematics and Computer Science









Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku

**Ines Petrić**

# Gaussovi cijeli brojevi

Završni rad

Osijek, 2016.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku

**Ines Petrić**

# Gaussovi cijeli brojevi

Završni rad

Voditelj: doc. dr. sc. Mirela Jukić Bokun

Osijek, 2016.

# Sadržaj

**Uvod** **1**

**1. Skup $\mathbb{Z}[i]$** **2**

1.1. Norma na $\mathbb{Z}[i]$ . . . . . 2

1.2. Invertibilni elementi u $\mathbb{Z}[i]$ . . . . . 3

**2. Djeljivost u $\mathbb{Z}[i]$** **4**

2.1. Djeljivost . . . . . 4

2.2. Teorem o dijeljenju s ostatkom . . . . . 5

2.3. Euklidov algoritam . . . . . 8

2.4. Bezoutov teorem . . . . . 10

**3. Faktorizacija Gaussovih cijelih brojeva** **13**

3.1. Prosti Gaussovi cijeli brojevi . . . . . 13

3.2. Jedinstvenost faktorizacije Gaussovih cijelih brojeva . . . . . 14

3.3. Primjene . . . . . 16

**Literatura** **18**

**Sažetak:** U ovom radu bavit ćemo se Gaussovim cijelim brojevima. Reći ćemo nešto općenito o tom skupu, definirat ćemo normu i navesti invertibilne elemente. Također ćemo reći nešto o djeljivosti u skupu Gaussovih cijelih brojeva gdje ćemo iskazat važan Teorem o dijeljenju s ostatkom, Euklidov algoritam i Bezoutov teorem. Na kraju ćemo se upoznati s faktorizacijom Gaussovih cijelih brojeva i vidjeti njihovu primjenu.

**Ključne riječi:** norma, invertibilni elementi, djeljivost, Teorem o dijeljenju s ostatkom, Euklidov algoritam, relativno prosti Gaussovi cijeli brojevi, složeni i prosti Gaussovi cijeli brojevi, jedinstvena faktorizacija.

**Abstract:** In this article we will cover the Gaussian integers. We will say something in general about this set, define the norm and specify invertible elements. Also, we will say something about divisibility in $\mathbb{Z}[i]$ where we will demonstrate an important the Divison theorem, Euclidean algorithm and Bezout's theorem. We will get acquainted with the factorization of Gaussian integers and see some of their application.

**Key words:** norm, invertible elements, divisibility, the Division theorem, the Euclidean algorithm, relatively prime the Gaussian integers, composite and prime the Gaussian integers, unique factorization.

# Uvod

Skup Gaussovih cijelih brojeva predstavlja proširenje skupa cijelih brojeva. Uveo ih je njemački matematičar Carl Friedrich Gauss prilikom proučavanja diofantskih jednadžbi $a^2 + b^2 = n$, gdje Gaussovi cijeli brojevi omogućuju faktorizaciju lijeve strane navedene jednadžbe. Skup $\mathbb{Z}[i]$ posjeduje mnoga svojstva koja pomažu pri rješavanju različitih problema u teoriji brojeva.

U prvom poglavlju upoznat ćemo se s pojmovima norme, invertibilnog i asociranog elementa. U drugom poglavlju reći ćemo nešto o djeljivosti u skupu Gaussovih cijelih brojeva, iskazat i dokazat ćemo Teorem o dijeljenju s ostatkom, Euklidov algoritam i Bezoutov teorem, dok u trećem poglavlju očekuju nas prosti Gaussovi cijeli brojevi i jedinstvena faktorizacija složenog Gaussovog broja.

# 1. Skup $\mathbb{Z}[i]$

U Uvodu smo već spomenuli da je skup Gaussovih cijelih brojeva proširenje skupa cijelih brojeva. To je skup

$$\mathbb{Z}[i] = \{a_1 + a_2 i : a_1, a_2 \in \mathbb{Z}\} \supset \mathbb{Z}.$$

Prirodni brojevi $n$ koji se mogu prikazati u obliku sume dvaju kvadrata u uskoj su vezi s Gaussovim cijelim brojevima jer vrijedi

$$n = n_1^2 + n_2^2 = (n_1 + n_2 i)(n_1 - n_2 i).$$

**Primjer 1.1.** *Vrijedi*

$$5 = 2^2 + 1^2 = (2 + i)(2 - i).$$

## 1.1. Norma na $\mathbb{Z}[i]$

**Definicija 1.1.** *Preslikavanje* $\mathcal{N} : \mathbb{Z}[i] \longrightarrow \mathbb{N} \cup \{0\}$ *zadano s*

$$\mathcal{N}(a) = a\bar{a} = (a_1 + a_2 i)(a_1 - a_2 i) = a_1^2 + a_2^2 = \mid a \mid^2$$

*nazivamo normom na* $\mathbb{Z}[i]$.

Za tako zadanu funkciju vrijedi:

1. $\mathcal{N}(a) > 0$, $\forall a \in \mathbb{Z}[i] \backslash \{0\}$,
2. $\mathcal{N}(a) = 0 \Leftrightarrow a = 0$.

Sljedeća lema govori o multiplikativnosti norme.

**Lema 1.1.** *Za* $a, b \in \mathbb{Z}[i]$ *vrijedi* $\mathcal{N}(ab) = \mathcal{N}(a)\mathcal{N}(b)$.

*Dokaz.*

$$\mathcal{N}(ab) = (ab)\overline{(ab)} = a\bar{a}b\bar{b} = \mathcal{N}(a)\mathcal{N}(b).$$

□

Neka su $a, b \in \mathbb{Z}[i]$, $a = a_1 + a_2 i$, $b = b_1 + b_2 i$. Prema Lemi 1.1 znamo da je:

$$\mathcal{N}(ab) = \mathcal{N}(a)\mathcal{N}(b),$$

pa raspisivanjem dobivamo:

$$(a_1 a_2 - b_1 b_2)^2 + (a_1 b_2 + b_1 a_2)^2 = (a_1^2 + a_2^2)(b_1^2 + b_2^2). \tag{1}$$

Jednakost (1) nazivamo Diofantov identitet.

**Napomena 1.1.** *Primjetimo da svaki pozitivan cijeli broj nije norma nekog Gaussovog cijelog broja. Normu smo definirali kao sumu kvadrata dvaju cijelih brojeva, a kako je suma dvaju kvadrata kongruentno* 0, 1 *ili* 2 *modulo* 4, *odmah možemo zaključiti da prirodni brojevi koji su kongruentni* 3 *modulo* 4 *ne mogu biti norme nekog Gaussovog cijelog broja.*

## 1.2. Invertibilni elementi u $\mathbb{Z}[i]$

Važna primjena Leme 1.1. je kod određivanja Gaussovih cijelih brojeva koji imaju multiplikativni inverz u $\mathbb{Z}[i]$.

**Definicija 1.2.** *Element $a \in \mathbb{Z}[i]$ nazivamo invertibilnim elementom ako postoji $b \in \mathbb{Z}[i]$ takav da je $ab = ba = 1$. $b$ označavamo s $a^{-1}$ i nazivamo ga multiplikativni inverz od $a$.*

Sljedeća propozicija točno će nam odrediti koji su to invertibilni elementi u $\mathbb{Z}[i]$.

**Propozicija 1.1.** *$a \in \mathbb{Z}[i]$ je invertibilan ako i samo ako je $\mathcal{N}(a) = 1$. Jedini invertibilni elementi u $\mathbb{Z}[i]$ su $\pm 1$ i $\pm i$.*

*Dokaz.* Pretpostavimo da je $a \in \mathbb{Z}[i]$ invertibilan element. Po Definiciji 1.2. postoji $b \in \mathbb{Z}[i]$ takav da je $ab = 1$. Uočimo da je $a \neq 0$ i $b \neq 0$. Kako je

$$\mathcal{N}(ab) = \mathcal{N}(a)\mathcal{N}(b) = \mathcal{N}(1) = 1$$

i $\mathcal{N}(a), \mathcal{N}(b) \in \mathbb{N}$ dobivamo

$$\mathcal{N}(a) = \mathcal{N}(b) = 1.$$

Pogledajmo drugi smjer. Pretpostavimo da je $\mathcal{N}(a) = 1$, tada je $a\bar{a} = 1$. Iz toga vidimo da je $\bar{a} = \dfrac{1}{a}$, odnosno da je $\bar{a} = a^{-1}$. Pokazali smo prvi dio propozicije.
Odredimo sve invertibilne Gaussove cijele brojeve, odnosno sve $a \in \mathbb{Z}[i]$ koji imaju normu 1. Za $a = a_1 + a_2 i$ sa svojstvom da je

$$\mathcal{N}(a) = a_1^2 + a_2^2 = 1,$$

mogućnosti su sljedeće:

- $a_1^2 = 1$ i $a_2^2 = 0$, tada je $a_1 = \pm 1$ i $a_2 = 0$,
- $a_1^2 = 0$ i $a_2^2 = 1$, tada je $a_1 = 0$ i $a_2 = \pm 1$.

Dobivamo da je $a = 1$, $a = -1$, $a = i$ ili $a = -i$, odnosno da su jedini invertibilni elementi u $\mathbb{Z}[i]$: $\pm 1$ i $\pm i$. □

Invertibilne elemente u $\mathbb{Z}[i]$ nazivamo još i jedinice.
Ako je $b = \varepsilon a$, $a \in \mathbb{Z}[i]$, $\varepsilon \in \{\pm 1, \pm i\}$, kažemo da su $a$ i $b$ asocirani.

**Primjer 1.2.** *Neka je $a = -4 + 3i$, a $b = i(-4 + 3i) = -3 - 4i$, tada su $a$ i $b$ asocirani. Također, elementi asocirani elementu $a$ su i:*

$$\begin{aligned} c &= -1(-4 + 3i) = 4 - 3i, \\ d &= -i(-4 + 3i) = 3 + 4i, \\ a &= -4 + 3i. \end{aligned}$$

U skupu $\mathbb{Z}$ norma predstavlja apsolutnu vrijednost broja, inverzni elementi su $\pm 1$ i iz $\mid a \mid = \mid b \mid$, $a, b \in \mathbb{Z}$ slijedi $a = \pm b$.
Drugačije je u $\mathbb{Z}[i]$. Ako je $\mathcal{N}(a) = \mathcal{N}(b)$, $a, b \in \mathbb{Z}[i]$, kao što ćemo vidjeti u sljedećem primjeru ne mora značiti da se $a$ i $b$ razlikuju samo do na množenje invertibilnim elementom.

**Primjer 1.3.** *Za $a = 4 + 5i$ i $b = 5 - 4i$ je $\mathcal{N}(a) = \mathcal{N}(b) = 41$, ali $a$ i $b$ nisu asocirani elementi, odnosno ne postoji $\varepsilon \in \{\pm 1, \pm i\}$ takav da je $a = \varepsilon b$.*

# 2. Djeljivost u $\mathbb{Z}[i]$

## 2.1. Djeljivost

Djeljivost u $\mathbb{Z}[i]$ definirana je na prirodan način.

**Definicija 2.1.** *Neka su $a, b \in \mathbb{Z}[i]$, $b \neq 0$. Ako postoji $c \in \mathbb{Z}[i]$ takav da je $a = bc$, kažemo da $b$ dijeli $a$. Pišemo: $b \mid a$.*

U ovom slučaju $a$ zovemo djeljenik, dok $b$ nazivamo djelitelj. Rezultat pri dijeljenju nazivamo količnik.

**Primjer 2.1.** *Kako je*

$$11 + 13i = (2 + 5i)(3 - i)$$

*zaključujemo da $(2 + 5i) \mid (11 + 13i)$.*

**Primjer 2.2.** *Provjerimo je li $15 + 7i$ djeljiv s $3 + i$.*
*Kako je*

$$\frac{15 + 7i}{3 + i} = \frac{15 + 7i}{3 + i} \cdot \frac{3 - i}{3 - i} = \frac{52 + 6i}{10} = \frac{52}{10} + \frac{6}{10}i \notin \mathbb{Z}[i]$$

*slijedi da $(3 + i) \nmid (15 + 7i)$.*

**Primjer 2.3.** *Provjerimo je li $52 - 16i$ djeljiv s $7 - 5i$.*
*Kako je*

$$\frac{52 - 16i}{7 - 5i} = \frac{52 - 16i}{7 - 5i} \cdot \frac{7 + 5i}{7 + 5i} = \frac{444 + 148i}{74} = \frac{444}{74} + \frac{148}{74}i = 6 + 2i \in \mathbb{Z}[i]$$

*zaključujemo da $(52 - 16i) \mid (7 - 5i)$.*

Sljedeći teorem govori nam kada je Gaussov cijeli broj djeljiv cijelim brojem.

**Teorem 2.1.** *Gaussov cijeli broj $a = a_1 + a_2 i$ djeljiv je s cijelim brojem $b \in \mathbb{Z}$ ako $b \mid a_1$ i $b \mid a_2$.*

*Dokaz.* Neka je Gaussov cijeli broj $a = a_1 + a_2 i$ djeljiv s $b \in \mathbb{Z} \subset \mathbb{Z}[i]$. Po definiciji djeljivosti postoji $c = c_1 + c_2 i \in \mathbb{Z}[i]$ takav da je $a = bc = b(c_1 + c_2 i)$. Tada je

$$a = a_1 + a_2 i = bc_1 + (bc_2)i.$$

Izjednačavanjem realnog dijela s realnim i imaginarnog dijela s imaginarnim dobivamo:

$$a_1 = bc_1 \ \ i \ \ a_2 = bc_2,$$

iz čega zaključujemo da $b \mid a_1$ i $b \mid a_2$. □

**Napomena 2.1.** *Ako u Teoremu 2.1. stavimo da je $a_2 = 0$, dobivamo da se dijeljenje između cijelih brojeva ne mijenja kada smo u $\mathbb{Z}[i]$, tj. za $a, c \in \mathbb{Z}$, $c \mid a$ u $\mathbb{Z}[i]$ ako i samo ako $c \mid a$ u $\mathbb{Z}$.*

**Teorem 2.2.** *Neka su $a, b \in \mathbb{Z}[i]$. Ako $b$ dijeli $a$ u $\mathbb{Z}[i]$, onda $\mathcal{N}(b)$ dijeli $\mathcal{N}(a)$ u $\mathbb{Z}$.*

*Dokaz.* Neka su $a, b \in \mathbb{Z}[i]$ i $b \mid a$. Po definiciji djeljivosti $a = bc$ za neki $c \in \mathbb{Z}[i]$. Tada je

$$\mathcal{N}(a) = \mathcal{N}(bc) = \mathcal{N}(b)\mathcal{N}(c),$$

iz čega vidimo da $\mathcal{N}(b) \mid \mathcal{N}(a)$. □

**Primjer 2.4.** *Neka je $a = 4 + i$ i $b = 6 - 4i$. Kako je $\mathcal{N}(a) = 17$, $\mathcal{N}(b) = 52$, a $17 \nmid 52$, slijedi da $a \nmid b$.*

**Napomena 2.2.** *Obrat Teorema 2.2. ne vrijedi.*

**Primjer 2.5.** *Neka je $a = 12 + 11i$ i $b = 1 + 2i$. Tada je $\mathcal{N}(a) = 265$, $\mathcal{N}(b) = 5$. Vidimo da $\mathcal{N}(b) \mid \mathcal{N}(a)$, međutim*

$$\frac{12 + 11i}{1 + 2i} = \frac{12 + 11i}{1 + 2i} \cdot \frac{1 - 2i}{1 - 2i} = \frac{34}{5} - \frac{13}{5}i \notin \mathbb{Z}[i]$$

*pa $b \nmid a$.*

**Korolar 2.1.** *Gaussov cijeli broj ima parnu normu ako i samo ako je višekratnik od $1 + i$.*

*Dokaz.* Neka je $a \in \mathbb{Z}[i]$ i neka je $a$ višekratnik od $1+i$, tj. $(1+i) \mid a$. Tada $\mathcal{N}(1+i) \mid \mathcal{N}(a)$, iz čega vidimo da $2 \mid \mathcal{N}(a)$, odnosno da je $\mathcal{N}(a)$ paran broj.
Pretpostavimo sada da Gaussov cijeli broj $a = a_1 + a_2 i$ ima parnu normu, tj.

$$a_1^2 + a_2^2 \equiv 0 \pmod 2.$$

Tada su $a_1$, $a_2$ parni ili $a_1$, $a_2$ neparni brojevi, što u oba slučaja znači da je

$$a_1 \equiv a_2 \pmod 2.$$

Želimo Gaussov cijeli broj $a$ napisati kao $a_1 + a_2 i = (1 + i)(b_1 + b_2 i)$, $b_1, b_2 \in \mathbb{Z}$. To nam je isto kao i:

$$a_1 + a_2 i = (b_1 - b_2) + (b_1 + b_2 i)i.$$

Ako uzmemo da nam je $b_1 = \dfrac{a_1 + a_2}{2}$ i $b_2 = \dfrac{a_2 - a_1}{2}$, dobijemo upravo ono što smo trebali i $(1 + i) \mid a$. □

**Primjer 2.6.** *Norma od $2 + 6i$ jednaka je 40 i $2 + 6i = (1 + i)(4 + 2i)$.*

## 2.2. Teorem o dijeljenju s ostatkom

**Teorem 2.3** (Teorem o dijeljenju s ostatkom)**.** *Za $a, b \in \mathbb{Z}[i]$, $b \neq 0$ postoje $c, d \in \mathbb{Z}[i]$ takvi da je $a = bc + d$, $\mathcal{N}(d) < \mathcal{N}(b)$. Zapravo, možemo izabrati $d$ takav da je $\mathcal{N}(d) \leq \dfrac{1}{2}\mathcal{N}(b)$.*

Gaussov cijeli broj $c$ je količnik, a $d$ nazivamo ostatak. Norma ostatka je omeđena, tj. $0 \leq \mathcal{N}(d) < \mathcal{N}(b)$. Slijede nam primjer, iskaz i dokaz teorema koji će nam pomoći kako bi dokazali Teorem o dijeljenju s ostatkom.

**Primjer 2.7.** *Neka je* $a = 27 - 23i$ *i* $b = 8 + i$*. Odredimo* $c, d$ *takve da je* $a = bc + d$*. Kako je*

$$\frac{a}{b} = \frac{27-23}{8+i} = \frac{193-211i}{65} = \frac{193}{65} - \frac{211}{65}i.$$

*Koristeći teorem o dijeljenju s ostatkom u skupu* $\mathbb{Z}$ *dobivamo:*

$$193 : 65 = 26 \cdot 2 + 63, \tag{2}$$
$$-211 : 65 = 65 \cdot (-4) + 49. \tag{3}$$

*Iz* (2) *i* (3) *uzmemo količnike i dobivamo* $c = 2 - 4i$*. Izračunajmo ostatak:*

$$d = a - bc = (27 - 23i) - (8 + i)(2 - 4i) = 7 + 7i,$$

*ali uočimo da je:*

$$\mathcal{N}(d) = 98 > \mathcal{N}(b) = 65.$$

*Jedna od prednosti ovog teorema upravo je mali ostatak. Izbor ovakvog* $c$ *i* $d$ *nije dobar. Pokušajmo sada drugačiji pristup. Probajmo zamijeniti* $193 : 65 = 2.969$ *i* $-211 : 65 = -3.246$ *s najbližim cijelim brojevima. Uočimo da je* $2.969$ *bliže* $3$ *nego* $2$*,* $a$ $-3.246$ *je bliže* $-3$ *nego* $-4$*, pa nam je* $c = 3 - 3i$*. Ostatak bi u tom slučaju iznosio* $d = a - bc = -2i$*, a norma tog ostatka je* $4 < \mathcal{N}(b) = 65$*. Znači,* $c = 3 - 3i$*, a ostatak* $d = -2i$*.*

U standardnom teoremu o dijeljenju s ostatkom u $\mathbb{Z}$ ostatak nam je uvijek nenegativan broj. Postupak opisan u prethodnom primjeru dopušta da ostatak bude negativan cijeli broj i to je tako zvani modificirani teorem o dijeljenju s ostatkom. Ostatak dobiven modificiranim teoremom po apsolutnoj je vrijednosti manji ili jednak od ostatka koji se dobije kada bismo radili na standardan način. Preciznije ćemo to iskazati sljedećim teoremom.

**Teorem 2.4** (Modificirani teorem o dijeljenju s otatkom u $\mathbb{Z}$)**.** *Neka je* $a \in \mathbb{Z}$ *i* $b \in \mathbb{N}$*. Tada postoje cijeli brojevi* $q$ *i* $r$ *takvi da vrijedi*

$$a = bq + r, \quad |r| \leq \frac{1}{2}b.$$

*Dokaz.* Neka je $q$ najbliži cijeli broj broju $\frac{b}{a}$. Tada je

$$\left| q - \frac{b}{a} \right| \leq \frac{1}{2}.$$

Imamo sljedeće slučajeve:

- Ako je $q - \frac{b}{a} \leq \frac{1}{2}$, definiramo da je $r = b\left(q - \frac{a}{b}\right) = bq - a$ pa je zbog prethodne nejednakosti $|r| \leq \frac{1}{2}b$.
- Analogno, ako je $\frac{b}{a} - q \leq \frac{1}{2}$, stavimo da je $r = b\left(\frac{a}{b} - q\right) = a - bq$, a onda je $|r| \leq \frac{1}{2}b$.

□

Konačno, slijedi dokaz Teorema o dijeljenju s ostatkom.

*Dokaz Teorema 2.3.* Neka su $a, b \in \mathbb{Z}[i]$, $b \neq 0$. Želimo konstruirati $c, d \in \mathbb{Z}[i]$ takve da je $a = bc + d$, $\mathcal{N}(d) \leq \frac{1}{2}\mathcal{N}(b)$. Neka je

$$\frac{a}{b} = \frac{a\bar{b}}{b\bar{b}} = \frac{m_1 + m_2 i}{\mathcal{N}(b)}, \quad a\bar{b} = m_1 + m_2 i. \tag{4}$$

Podijelimo li $m_1$ i $m_2$ s $\mathcal{N}(b)$ koristeći modificirani teorem o dijeljenju s ostatkom u $\mathbb{Z}$ dobivamo

$$m_1 = \mathcal{N}(b)q_1 + r_1, \;\; q_1 \in \mathbb{Z}, \;\; 0 \leq \mid r_1 \mid \leq \frac{1}{2}\mathcal{N}(b),$$

$$m_2 = \mathcal{N}(b)q_2 + r_2, \;\; q_2 \in \mathbb{Z}, \;\; 0 \leq \mid r_2 \mid \leq \frac{1}{2}\mathcal{N}(b).$$

Tako dobivene $m_1$ i $m_2$ vratimo u (4):

$$\frac{a}{b} = \frac{\mathcal{N}(b)q_1 + r_1 + (\mathcal{N}(b)q_2 + r_2)i}{\mathcal{N}(b)} = q_1 + q_2 i + \frac{r_1 + r_2 i}{\mathcal{N}(b)}.$$

Kako je $\mathcal{N}(b) = b\bar{b}$, postavimo li da je $c = q_1 + q_2 i$ slijedi

$$\frac{a}{b} = c + \frac{r_1 + r_2 i}{b\bar{b}}.$$

Pomnožimo li ovu jednakost s $b$ dobivamo:

$$a = cb + \frac{r_1 + r_2 i}{\bar{b}}$$

iz čega slijedi da je

$$a - cb = \frac{r_1 + r_2 i}{\bar{b}}.$$

Kako su $a, b, c \in \mathbb{Z}[i]$, onda je i $\dfrac{r_1 + r_2 i}{\bar{b}} \in \mathbb{Z}[i]$. Ostatak označimo s $d = a - cb = \dfrac{r_1 + r_2 i}{\bar{b}}$. Pokažimo još da je $\mathcal{N}(d) \leq \frac{1}{2}\mathcal{N}(b)$. Kako je

$$a - cb = \frac{r_1 + r_2 i}{\bar{b}},$$

zaključujemo da

$$\mathcal{N}(a - cb) = \mathcal{N}\left(\frac{r_1 + r_2 i}{\bar{b}}\right).$$

Znamo da je $\mathcal{N}(b) = \mathcal{N}(\bar{b})$, dakle imamo:

$$\mathcal{N}(a - cb) = \frac{r_1^2 + r_2^2}{\mathcal{N}(b)}.$$

Budući da nam je

$$0 \leq \mid r_i \mid \leq \frac{1}{2}\mathcal{N}(b), \;\; i = 1, 2,$$

slijedi:

$$\mathcal{N}(a - cb) \leq \frac{\frac{1}{4}\mathcal{N}(b)^2 + \frac{1}{4}\mathcal{N}(b)^2}{\mathcal{N}(b)} = \frac{1}{2}\mathcal{N}(b).$$

Time je teorem dokazan. □

Pogledajmo sljedeći primjer.

**Primjer 2.8.** *Neka je $a = 24 - 7i$ i $b = 5 + i$. Nađimo $c, d \in \mathbb{Z}[i]$ takve da je $a = bc + d$. Kako je*

$$\frac{a}{b} = \frac{24 - 7i}{5 + i} \cdot \frac{5 - i}{5 - i} = \frac{113 - 59i}{26},$$
$$113 : 26 = 4.35 \; i \;\; - 59 : 26 = -2.27.$$

*Slijedi nam da je $c = 4 - 2i$, a ostatak $d = (24 - 7i) - (5 + i)(4 - 2i) = 2 - i$. Naravno, važno je prokomentirati da je $\mathcal{N}(d) = 5 < \frac{1}{2}\mathcal{N}(b) = \frac{26}{2}$.*

## 2.3. Euklidov algoritam

**Definicija 2.2.** *Zajednički djelitelj Gaussovih cijelih brojeva $a$ i $b$ je svaki $c \in \mathbb{Z}[i]$ sa svojstvom da $c \mid a$ i $c \mid b$.*

Sljedeće što ćemo definirati najveći je zajednički djelitelj dvaju Gaussovih cijelih brojeva.

**Definicija 2.3.** *Najveći zajednički djelitelj brojeva $a, b \in \mathbb{Z}[i]$ zajednički je djelitelj od $a$ i $b$ s najvećom normom.*

Uočimo da ako je $c \in \mathbb{Z}[i]$ najveći zajednički djelitelj brojeva $a, b \in \mathbb{Z}[i]$, onda su to i asocirani elementi od $c$.

**Definicija 2.4.** *Kažemo da su $a, b \in \mathbb{Z}[i]$ relativno prosti ako su im jedini zajednički djelitelji invertibilni elementi.*

Problem nam je kako odrediti najveći zajednički djelitelj dvaju Gaussovih cijelih brojeva. Odgovor nam, kao i u slučaju skupa $\mathbb{Z}$, daje Euklidov algoritam.

**Teorem 2.5** (Euklidov algoritam)**.** *Neka su $a, b \in \mathbb{Z}[i]$, $a, b \neq 0$. Uzastopnom primjenom teorema o dijeljenju s ostatkom na $a$ i $b$ pa na djeljenik i ostatak sve dok ostatak nije nula dobivamo sljedeći niz jednakosti:*

$$\begin{aligned}
a &= bc_1 + d_1, && \mathcal{N}(d_1) < \mathcal{N}(b), && (5)\\
b &= d_1c_2 + d_2, && \mathcal{N}(d_2) < \mathcal{N}(d_1), && (6)\\
d_1 &= d_2c_3 + d_3, && \mathcal{N}(d_3) < \mathcal{N}(d_2), && (7)\\
&\vdots && && \\
d_{n-2} &= d_{n-1}c_n + d_n, && \mathcal{N}(d_n) < \mathcal{N}(d_{n-1}), && (8)\\
d_{n-1} &= d_nc_{n+1} + 0. && && (9)
\end{aligned}$$

*Zadnji ostatak različit od nule najveći je zajednički djelitelj brojeva $a$ i $b$.*

*Dokaz.* Iz (5) zaključujemo da svaki zajednički djelitelj od $a$ i $b$ dijeli $d_1$. Primijenimo li ovaj zaključak na (6), zaključujemo da svaki zajednički djelitelj od $a$ i $b$ dijeli $d_2$. Analognim zaključivanjem iz preostalog niza jednakosti slijedi da svaki zajednički djelitelj od $a$ i $b$ dijeli svaki $d_j$, $j = 1, \ldots, n$. Posebno, svaki zajednički djelitelj od $a$ i $b$ dijeli $d_n$. S druge strane, iz (9) slijedi da $d_n$ dijeli $d_{n-1}$ pa iz (8) slijedi da $d_n$ dijeli $d_{n-2}$. Analognim zaključivanjem kroz čitav niz jednakosti zaključujemo da je $d_n$ zajednički djelitelj od $a$ i $b$. Kako je on zajednički djelitelj koji je djeljiv sa svakim drugim zajedničkim djeliteljem brojeva $a$ i $b$, onda je maksimalne norme i time je teorem dokazan. □

**Primjer 2.9.** *Odredimo najveći zajednički djeljitelj brojeva* $a = 11 + 3i$ *i* $b = 1 + 8i$.

$$\begin{aligned} 11 + 3i &= (1 + 8i)(1 - i) + (2 - 4i), \\ 1 + 8i &= (2 - 4i)(-1 + i) + (-1 + 2i), \\ 2 - 4i &= (-1 + 2i)(-2) + 0. \end{aligned}$$

*Najveći zajednički djelitelj od* $a$ *i* $b$ *zadnji je ostatak različit od nule, odnosno* $-1 + 2i$. *Ako u drugoj jednakosti napravimo promjenu, tj. ako je zapišemo na ovaj način:*

$$\begin{aligned} 1 + 8i &= (2 - 4i)(-2 + i) + (1 - 2i), \\ 2 - 4i &= (1 - 2i)(2) + 0, \end{aligned}$$

*vidimo da je tada najveći zajednički djelitelj od* $a$ *i* $b$ *jednak* $1 - 2i$. *Dobili smo dva različita najveća zajednička djelitelja brojeva* $a$ *i* $b$. *Ako bolje pogledamo, vidimo da su oni asocirani, tj.* $-1 + 2i = (-1)(1 - 2i)$.

**Primjer 2.10.** *Primjenom Euklidovog algoritma odredimo najveći zajednički djelitelj brojeva* $a = 32 + 9i$ *i* $b = 4 + 11i$.

$$\begin{aligned} 32 + 9i &= (4 + 11i)(2 - 2i) + (2 - 5i), \\ 4 + 11i &= (2 - 5i)(-2 + i) + (3 - i), \\ 2 - 5i &= (3 - i)(1 - i) - i, \\ 3 - i &= (-i)(1 + 3i) + 0. \end{aligned}$$

*Slijedi da je najveći zajednički djelitelj brojeva* $a$ *i* $b$ *jednak* $-i$, *odnosno da su* $a$ *i* $b$ *relativno prosti.*

**Napomena 2.3.** *Najveći zajednički djelitelj brojeva* $a$ *i* $b$ *u skupu* $\mathbb{Z}$ *označavat ćemo s* $(a, b)$.

**Napomena 2.4.** *Ako je* $c$ *najveći zajednički djelitelj Gaussovih cijelih brojeva* $a$ *i* $b$, *onda* $\mathcal{N}(c)$ *dijeli* $\mathcal{N}(a)$ *i* $\mathcal{N}(b)$. *Može se dogoditi da je* $\mathcal{N}(c) < (\mathcal{N}(a), \mathcal{N}(b))$.

**Primjer 2.11.** *Pogledajmo Primjer 2.9. Vidimo da je* $\mathcal{N}(a) = 130$ *i* $\mathcal{N}(b) = 65$ *pa je*

$$(\mathcal{N}(a), \mathcal{N}(b)) = (130, 65) = 65.$$

*Najveći zajednički djelitelj od* $a$ *i* $b$ *je* $-1 + 2i$ *i njegova norma iznosi* 5. *Očito je da:*

$$\mathcal{N}(-1 + 2i) = 5 < 65 = (\mathcal{N}(a), \mathcal{N}(b)).$$

**Napomena 2.5.** *Pretpostavimo da za Gaussove cijele brojeve* $a$ *i* $b$ *vrijedi da su njihove norme relativno proste u skupu* $\mathbb{Z}$, *tj.* $(\mathcal{N}(a), \mathcal{N}(b)) = 1$, *te da je* $c$ *najveći zajednički djelitelj od* $a$ *i* $b$. *Tada* $c \mid a$ *i* $c \mid b$, *iz čega nam slijedi da* $\mathcal{N}(c) \mid \mathcal{N}(a)$ *i* $\mathcal{N}(c) \mid \mathcal{N}(b)$ *te zaključujemo da je* $\mathcal{N}(c) = 1$, *odnosno* $c = \varepsilon$, $\varepsilon \in \{\pm 1, \pm i\}$.

**Primjer 2.12.** *Neka je* $a = 32 + 9i$ *i* $b = 4 + 11i$. *Vidimo da je:*

$$\mathcal{N}(a) = 1105, \ \ \mathcal{N}(b) = 137.$$

*Uočimo da je* $(1105, 137) = 1$ *i po prethodnoj napomeni najveći zajednički djeljitelj brojeva* $a$ *i* $b$ *je* $\varepsilon$, $\varepsilon \in \{\pm 1, \pm i\}$. *U Primjeru 2.10. pokazali smo upravo da su* $a$ *i* $b$ *relativno prosti, odnosno da je najveći zajednički djelitelj* $a$ *i* $b$ *jednak* $-i$.

Sljedeći korolar koji ćemo iskazati i kojim ćemo ujedno i završiti s Euklidovim algoritmom govori nam da je najveći zajednički djelitelj dvaju Gaussovih cijelih brojeva jedinstven do na množenje invertibilnim elementom.

**Korolar 2.2.** *Neka su $a, b \in \mathbb{Z}[i]$, $a, b \neq 0$ i neka je $c$ najveći zajednički djelitelj brojeva $a$ i $b$ dobiven Euklidovim algoritmom. Bilo koji najveći zajednički djelitelj $d$ od $a$ i $b$ oblika je $d = \varepsilon c$, $\varepsilon \in \{\pm 1, \pm i\}$.*

*Dokaz.* Neka je $c$ najveći zajednički djelitelj Gaussovih cijelih brojeva $a$ i $b$ dobiven Euklidovim algoritmom i neka je $d$ najveći zajednički djelitelj brojeva $a$ i $b$. Znamo da $d \mid c$, tj. postoji Gaussov cijeli broj $e$ takav da je $c = de$ što implicira $\mathcal{N}(c) = \mathcal{N}(d)\mathcal{N}(e)$. Kako je $\mathcal{N}(c) = \mathcal{N}(d)$, to nam pokazuje da je $\mathcal{N}(e) = 1$, odnosno da je $e = \varepsilon$, $\varepsilon \in \{\pm 1, \pm i\}$. □

## 2.4. Bezoutov teorem

**Teorem 2.6** (Bezoutov teorem)**.** *Neka je $d$ najveći zajednički djelitelj brojeva $a, b \in \mathbb{Z}[i]$, $a, b \neq 0$. Tada postoje $x, y \in \mathbb{Z}[i]$ takvi da je $c = ax + by$.*

*Dokaz.* Prisjetimo se Teorema 2.4. Iz (5) vidimo da je:

$$d_1 = a - bc_1.$$

Ako ovu jednakost vratimo u (6), dobivamo sljedeće:

$$d_2 = b - (a - bc_1)c_1 = b(1 + c_1c_2) - ac_2.$$

Uočimo da smo ostatak $d_1$ i $d_2$ prikazali kao linearnu kombinaciju od $a$ i $b$. Nastavljajući analogno dalje, dobivamo da je svaki $d_i$ linearna kombinacija od $a$ i $b$. Posebno, najveći zajednički djelitelj od $a$ i $b$ je linearna kombinacija od $a$ i $b$. □

**Korolar 2.3.** *$a, b \in \mathbb{Z}[i]$, $a, b \neq 0$ relativno su prosti ako i samo ako je*

$$ax + by = 1,$$

*za neke $x, y \in \mathbb{Z}[i]$.*

*Dokaz.* Ako su Gaussovi cijeli brojevi $a$ i $b$ relativno prosti, po Bezoutovom teoremu postoje $x, y \in \mathbb{Z}[i]$ takvi da je $ax + by = 1$.
S druge strane, ako je $ax + by = 1$, za neke Gaussove cijele brojeve $x$ i $y$ tada bilo koji zajednički djelitelj od $a$ i $b$ dijeli 1. Invertibilni elementi su jedini koji dijele 1 i iz tog nam slijedi da su $a$ i $b$ relativno prosti. □

**Primjer 2.13.** *U Primjeru 2.12. pokazali smo da je $-i$ najveći zajednički djelitelj brojeva $a = 32+9i$ i $b = 4+11i$. Prikažimo $-i$ kao linearnu kombinaciju od $a$ i $b$. Koristeći povratne supstitucije u Euklidovom algoritmu imamo:*

$$\begin{aligned}
-i &= (2-5i) - (3-i)(1-i) \\
&= (2-5i) - (4+11i-(2-5i)(-2+i))(1-i) \\
&= (2-5i)(1+(-2+i)(1-i)) - (4+11i)(1-i) \\
&= (2-5i)(3i) - (4+11i)(1-i) \\
&= (32+9i-(4+11i)(2-2i))(3i) - (4+11i)(1-i) \\
&= (32+9i)(3i) - (4+11i)(7+5i) \\
&= a(3i) - b(7+5i).
\end{aligned}$$

*Dobili smo da je:*

$$-i = a(3i) - b(7 + 5i). \tag{10}$$

*Ako* (10) *pomnožimo s i imamo:*

$$1 = a(-3) + b(5 - 7i).$$

U nastavku pogledajmo još neke primjere.

**Primjer 2.14.** *Neka je $a = 4+5i$ i $b = 4-5i$. Prikažimo najveći zajednički djelitelj brojeva $a$ i $b$ kao njihovu linearnu kombinaciju. Prvo ćemo Euklidovim algoritmom odrediti najveći zajednički djelitelj.*

$$\begin{aligned} 4 + 5i &= (4 - 5i)(i) - (1 - i), \\ 4 - 5i &= -(1 - i)(-4) - i, \\ -1 + i &= (-i)(1 + i) + 0. \end{aligned}$$

*Vidimo da je najveći zajednički djelitelj brojeva $a$ i $b$ jednak $-i$. Sada ćemo $-i$ prikazati kao linearnu kombinaciju od $a$ i $b$.*

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

*Opet množenjem s i imamo:*

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

**Napomena 2.6.** *Uočimo da je u Primjeru 2.14. $\mathcal{N}(a) = \mathcal{N}(b) = 41$, i norme nisu relativno proste u $\mathbb{Z}$, ali Gaussovi cijeli brojevi $a$ i $b$ relativno su prosti u $\mathbb{Z}[i]$.*

**Primjer 2.15.** *U Primjeru 2.9. pokazali smo da je najveći zajednički djelitelj Gaussovih cijelih brojeva $a = 11 + 3i$ i $b = 1 + 8i$ jednak $-1 + 2i$. Prikažimo $-1 + 2i$ kao linearnu kombinaciju od $a$ i $b$.*

$$\begin{aligned} -1 + 2i &= (1 + 8i) - (2 - 4i)(-1 + i) \\ &= (1 + 8i) - (11 + 3i - (1 + 8i)(1 - i))(-1 + i) \\ &= (11 + 3i)(1 - i) + (1 + 8i)(1 + (1 - i)(-1 + i)) \\ &= (11 + 3i)(1 - i) + (1 + 8i)(1 + 2i) \\ &= a(1 - i) + b(1 + 2i). \end{aligned}$$

Sljedeće što ćemo pokazati neke su posljedice Bezoutovog teorema.

**Korolar 2.4.** *Neka su $a, b, c \in \mathbb{Z}[i]$ i neka su $a$ i $b$ relativno prosti. Ako $a \mid bc$, tada $a \mid c$.*

*Dokaz.* Kako $a \mid bc$, onda je $bc = ad$ za neki Gaussov cijeli broj $d$. Po pretpostavci su $a$ i $b$ relativno prosti. Koristeći Bezoutov teorem slijedi da postoje $x, y \in \mathbb{Z}[i]$ takvi da je:

$$ax + by = 1. \tag{11}$$

Ako (11) pomnožimo s $c$ imamo:

$$acx + bcy = c.$$

Kako je

$$bc = ad,$$

slijedi da je

$$acx + ady = c,$$

odnosno

$$a(cx + dy) = c,$$

pa vrijedi $a \mid c$. □

**Korolar 2.5.** *Neka su $a$ i $b$ relativno prosti Gaussovi cijeli brojevi. Ako $a \mid c$ i $b \mid c$ u $\mathbb{Z}[i]$, tada i $ab \mid c$.*

*Dokaz.* Ako $a \mid c$, onda je $c = ad_1$, $d_1 \in \mathbb{Z}[i]$. Ako $b \mid c$, onda je $c = bd_2$, $d_2 \in \mathbb{Z}[i]$. Kako su $a$ i $b$ relativno prosti, postoji $x, y \in \mathbb{Z}[i]$ takvi da je

$$ax + by = 1. \tag{12}$$

Jednakost (12) pomnožimo s $c$ i onda imamo:

$$acx + bcy = c,$$

pa je

$$abd_2x + bad_1y = c,$$

tj.

$$ab(d_2x + d_1y) = c,$$

iz čega slijedi da $ab \mid c$. □

**Korolar 2.6.** *Neka su $a, b, c \in \mathbb{Z}[i]$, $a, b, c \neq 0$. Ako su $a$ i $c$ relativno prosti i $b$ i $c$ relativno prosti, onda su i $ab$ i $c$ relativno prosti.*

*Dokaz.* Kako su $a$ i $c$ relativno prosti, postoje Gaussovi cijeli brojevi $x_1$ i $y_1$ takvi da je:

$$ax_1 + cy_1 = 1. \tag{13}$$

Kako su $b$ i $c$ relativno prosti, postoje Gaussovi cijeli brojevi $x_2$ i $y_2$ takvi da je:

$$bx_2 + cy_2 = 1. \tag{14}$$

Ako (13) i (14) pomnožimo međusobno, onda imamo:

$$abx_1x_2 + acx_1y_1 + cby_1x_2 + c^2y_1y_2 = 1.$$

Odavde je

$$ab(x_1x_2) + c(ax_1y_1 + by_1y_2 + cy_1y_2) = 1,$$

iz čega proizlazi da su $ab$ i $c$ relativno prosti. □

# 3. Faktorizacija Gaussovih cijelih brojeva

## 3.1. Prosti Gaussovi cijeli brojevi

**Lema 3.1.** *Neka je $a$ Gaussov cijeli broj, $a \neq 0$. Bilo koji djelitelj od $a$ čija je norma 1 ili $\mathcal{N}(a)$ je invertibilni element ili invertibilni element pomnožen s $a$.*

*Dokaz.* Ako $b \mid a$, onda $\mathcal{N}(b) \mid \mathcal{N}(a)$ i $\mathcal{N}(b) = 1$. Iz toga nam slijedi da je $b = \pm 1$ i $b = \pm i$. Ako $b \mid a$ i $\mathcal{N}(a) = \mathcal{N}(b)$, onda je $a = bc$, $c \in \mathbb{Z}[i]$. Vidimo da je $\mathcal{N}(a) = \mathcal{N}(b)\mathcal{N}(c)$, iz čega slijedi da je $\mathcal{N}(c) = 1$, odnosno da je $c = \pm 1$ i $c = \pm i$ i $b = \pm a$ i $b = \pm ia$. □

Prethodna lema pokazuje da su jedini Gaussovi cijeli brojevi koji dijele $a \in \mathbb{Z}[i]$ i imaju normu jednaku kao $a$ upravo $\pm a$ i $\pm ia$. Ako je norma Gaussovog cijelog broja $a$ veća od 1, tada on uvijek ima barem osam djelitelja od $a$: $\pm 1$, $\pm i$, $\pm a$ i $\pm ia$. Ove djelitelje ćemo zvati trivijalni djelitelji ili trivijalni faktori. Norma netrivijalnih faktora strogo je između 1 i $\mathcal{N}(a)$.

**Definicija 3.1.** *Neka je $a \in \mathbb{Z}[i]$ i $\mathcal{N}(a) > 1$. Broj $a$ složen je Gaussov broj ako ima barem jedan netrivijalni djelitelj. Ako ima samo trivijalne djelitelje, onda kažemo da je $a$ prost Gaussov cijeli broj.*

**Napomena 3.1.** *Ako je $a = bc$ uz uvjet $1 < \mathcal{N}(b) < \mathcal{N}(a)$, uočimo da je onda i $\mathcal{N}(c) > 1$. Prikaz Gaussovog cijelog broja $a$ u obliku produta Gaussovih cijelih brojeva norme veće od 1 zvat ćemo netrivijalna faktorizacija.*

**Primjer 3.1.** *Netrivijalna faktorizacija od $5 + 5i$ bi bila $(3 - i)(1 + 2i)$, dok bi $i(5 - 5i)$ bila trivijalna faktorizacija.*

**Primjer 3.2.** *Netrivijalna faktorizacija od 5 je $(1 - 2i)(1 + 2i)$. Znamo da je 5 prost broj u $\mathbb{Z}$, dok je složen u $\mathbb{Z}[i]$. Broj 2 također je složen u $\mathbb{Z}[i]$ jer je $2 = (1 + i)(1 - i)$.*

**Primjer 3.3.** *Pokažimo da je 3 prost broj u $\mathbb{Z}[i]$. Pretpostavimo suprotno, neka je 3 složen, tj. $3 = ab$. Vidimo da je $9 = \mathcal{N}(a)\mathcal{N}(b)$, $\mathcal{N}(a), \mathcal{N}(b) > 1$ jer je ovo netrivijalna faktorizacija. Stoga je $\mathcal{N}(a) = 3$, odnosno za $a = a_1 + a_2 i \in \mathbb{Z}[i]$ vrijedi $a_1^2 + a_2^2 = 3$. To je kontradikcija jer takvi $a_1$ i $a_2$ ne postoje u $\mathbb{Z}$. Zaključujemo da broj 3 ima samo trivijalne faktore u $\mathbb{Z}[i]$ pa je on prost broj u $\mathbb{Z}[i]$.*

Sljedeći teorem govori kako prepoznati proste Gaussove cijele brojeve koristeći njihovu normu.

**Teorem 3.1.** *Neka je $\varepsilon$ invertibilan element u $\mathbb{Z}[i]$. Tada su sljedeći brojevi prosti Gaussovi cijeli brojevi:*

1. *$\varepsilon(1 + i)$,*
2. *$\varepsilon(a_1 + a_2 i)$, gdje je $a_1^2 + a_2^2 = p$, $p$ prost broj u $\mathbb{Z}$ i $p \equiv 1 \pmod 4$,*
3. *$\varepsilon q$, gdje je $q$ prost broj u $\mathbb{Z}$ takav da je $q \equiv 3 \pmod 4$.*

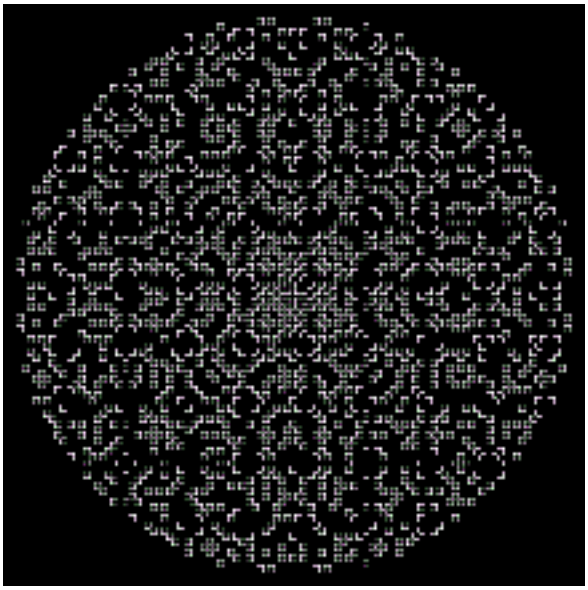
*Dokaz.*

1. Norma Gaussovog cijelog broja $\varepsilon(1 + i)$ jednaka je 2, a kako je 2 prost broj u skupu $\mathbb{Z}$ slijedi da je $\varepsilon(1 + i)$ prost broj u skupu $\mathbb{Z}[i]$.
2. Za Gaussov cijeli broj $\varepsilon(a_1 + a_2 i)$ vrijedi da je $\mathcal{N}(\varepsilon(a_1 + a_2 i)) = a_1^2 + a_2^2 = p$, $p \equiv 1 \pmod 4$ iz čega proizlazi da je $\varepsilon(a_1 + a_2 i)$ prost broj.

3. Za $\varepsilon q$ norma je jednaka $q^2 = qq$. Pretpostavimo da je $\varepsilon q = bc$ netrivijalna faktorizacija Gaussovog cijelog broja $\varepsilon q$, gdje su $b, c \in \mathbb{Z}[i]$. Slijedi nam da je $\mathcal{N}(b) = \mathcal{N}(c) = q$, a kako je $q \equiv 3 \pmod 4$ prema Napomeni 1.1. zaključujemo da ne postoji Gaussov cijeli broj norme $q$ odnosno da je $\varepsilon q$ je prost Gaussov cijeli broj.

□

Može se pokazati da vrijedi i obrat ovog teorema (vidi [1, str. 12]). Slika 1 prikazuje proste Gaussove cijele brojeve u kompleksnoj ravnini. Ako je $a_1 + a_2 i \in \mathbb{Z}[i]$ prost tada su i $a_2 + a_1 i$, $\varepsilon(a_1 + a_2 i)$, $\varepsilon(a_2 + a_1 i)$, $\varepsilon \in \{\pm 1, \pm i\}$ također prosti Gaussovi cijeli brojevi i to je razlog simetriji koju vidimo na slici.



Slika 1: Prosti Gaussovi cijeli brojevi u kompleksnoj ravnini

**Teorem 3.2.** *Svaki Gaussov cijeli broj $a$ s normom većom od* 1 *produkt je prostih Gaussovih cijelih brojeva.*

*Dokaz.* Neka je $a \in \mathbb{Z}[i]$ i $\mathcal{N}(a) > 1$. Dokaz ide indukcijom po normi od $a$. Ako je $\mathcal{N}(a) = 2$, onda je $a = 1 \pm i$ ili $a = -1 \pm i$, što su prosti Gaussovi cijeli brojevi. Neka je $n \geq 3$. Pretpostavimo da je svaki Gaussov cijeli broj $a$ norme veće ili jednake od 3 i manje od $n$ produkt prostih Gaussovih cijelih brojeva. Sada pokažimo da je svaki Gaussov cijeli broj $a$ norme $n$ produkt prostih Gaussovih cijelih brojeva. Ako ne postoji $a$ takav da je $\mathcal{N}(a) = n$, onda nemamo što dokazati. Zato pretpostavimo da postoji Gaussov cijeli broj $a$ norme $n$, $n$ složen broj i neka je $a = bc$ netrivijalna faktorizacija od $a$. Tada je $\mathcal{N}(b), \mathcal{N}(c) < n$ pa po pretpostavci indukcije, $b$ i $c$ su produkti prostih Gaussovih cijelih brojeva. □

## 3.2. Jedinstvenost faktorizacije Gaussovih cijelih brojeva

Pokazali smo da svaki složen Gaussov cijeli broj možemo prikazati kao produkt prostih Gaussovih cijelih brojeva. Sljedeći cilj nam je jedinstvenost tog prikaza. Prije toga ćemo iskazati i dokazati jednu lemu.

**Lema 3.2.** *Neka je $p$ prost Gaussov cijeli broj i $a_1, \ldots, a_r \in \mathbb{Z}[i]$. Ako $p \mid a_1 \cdots a_r$, tada $p \mid a_j$ za neki $j = 1, \ldots, r$.*

*Dokaz.* Dokaz ćemo raditi indukcijom po $r$. Za $r = 2$, pretpostavimo da $p \nmid a_1$. Tada su $p$ i $a_1$ relativno prosti i po Korolaru 2.4. $p \mid a_2$. Neka $p \mid a_1 \cdots a_r$ i pretpostavimo da $p \mid a_j$, za neki $j = 1, \ldots, r$. Sada pokažimo da ako vrijedi:

$$p \mid a_1 \cdots a_{r+1},$$

onda $p \mid a_j$ za neki $j = 1, \ldots, r+1$. Ako s $b$ označimo produkt $a_1 \cdots a_r$, tada

$$p \mid ba_{r+1}.$$

Ako $p \nmid b$, onda $p \mid a_{r+1}$. U suprotnom, $p \mid b$ te po pretpostavci indukcije slijedi da $p \mid a_j$ za neki $j = 1, \ldots, r$. □

Sada smo spremni za jedinstvenu faktorizaciju u $\mathbb{Z}[i]$. Prije toga pogledajmo primjer.

**Primjer 3.4.** *Vrijedi*

$$17 = (4+i)(4-i) = (1+4i)(1-4i).$$

*Sve su to prosti faktori u* $\mathbb{Z}[i]$*. Očigledno je da ove dvije faktorizacije nisu jednake, ali ako dopustimo množenje s jedinicom, vidimo da je:*

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

**Napomena 3.2.** *Ključna stvar kod jedinstvene faktorizacije množenje je faktora s invertibilnim elementima.*

**Teorem 3.3.** *Neka je $a$ Gaussov cijeli broj norme veće od 1. Ako je*

$$a = a_1 \cdots a_r = a'_1 \cdots a'_s,$$

*gdje su $a_j$, $j \in \{1, \ldots, r\}$ i $a'_k$, $k \in \{1, \ldots, s\}$ prosti Gaussovi cijeli brojevi, onda je $r = s$ i za svaki $a_j$, $j \in \{1, \ldots, r\}$, postoji $k \in \{1, \ldots, r\}$ i $\varepsilon \in \{\pm 1, \pm i\}$ takav da je $a_j = \varepsilon a'_k$.*

*Dokaz.* Pokazali smo da se svaki Gaussov cijeli broj $a$, $\mathcal{N}(a) > 1$, može faktorizirati. Ako je $a$ prost broj, faktorizacija je očita. Zato pretpostavimo da je $a$ složen. Dokaz radimo indukcijom po normi od $a$. Ako je $\mathcal{N}(a) = 2$, onda je $a$ prost broj. Već smo imali ovakav slučaj u dokazu Teorema 3.2. Pretpostavimo da za svaki Gaussov cijeli broj norme veće ili jednake od 3 vrijedi tvrdnja. Preostaje nam pokazati da Gaussov cijeli broj $a$ norme $n$ ima jedinstvenu faktorizaciju. Pretpostavimo da postoje dvije faktorizacije od $a$,

$$a = a_1 \cdots a_r = a'_1 \cdots a'_s.$$

Kako $a_1 \mid a$, možemo pisati da $a_1 \mid a'_1 \cdots a'_s$. Prema Lemi 3.2. $a_1 \mid a'_j$ za neki $j = 1, \ldots, s$. Bez smanjenja općenitosti možemo pretpostaviti da je $j = 1$, odnosno $a_1 \mid a'_1$. Kako su $a_1$ i $a'_1$ prosti, nemaju netrivijalnih faktora, onda je $a_1 = \varepsilon a'_1$, $\varepsilon \in \{\pm 1, \pm i\}$. Faktorizaciju od $a$ možemo zapisati na sljedeći način:

$$a = \varepsilon a'_1 a_2 \cdots a_r = a'_1 \cdots a'_s.$$

Ako podijelimo s $a'_1$ dobivamo:

$$\frac{a}{a'_1} = b = \varepsilon a_2 \cdots a_r = a'_2 \cdots a'_s.$$

Očigledno je da je $\mathcal{N}(b) = \frac{\mathcal{N}(a)}{\mathcal{N}(a_1')} < \mathcal{N}(a)$. Kako je $\varepsilon$ jedinica, produt $\varepsilon a_2$ je također prost broj. Imamo dvije faktorizacije od $b$ sa $r-1$ i $s-1$ prostih faktora. Kako je $\mathcal{N}(b) < n$ pretpostavka povlači da je $r-1 = s-1$, iz čega slijedi da je $r = s$. Drugi dio pretpostavke povlači tvrdnju da za svaki $a_j$, $j \in \{1, \ldots, r\}$, postoji $k \in \{1, \ldots, r\}$ i $\varepsilon \in \{\pm 1, \pm i\}$ takav da je $a_j = \varepsilon a_k'$. □

**Napomena 3.3.** *Teorem 3.3. nam pokazuje da je faktorizacija Gaussovog cijelog broja norme veće od* 1 *jedinstvena do na poredak i množenje invertibilnim elementima.*

Prirodno nam dolazi pitanje kako faktorizirati neki Gaussov cijeli broj. Pokazat ćemo jedan od načina. Ideja ja da iskoristimo faktorizaciju prirodnih brojeva.

**Primjer 3.5.** *Faktorizirajte Gaussov cijeli broj* $a = 66 + 127i$.
*Kako je*

$$\mathcal{N}(a) = 20485 = 5 \cdot 17 \cdot 241.$$

*Dalje imamo:*

$$\begin{aligned} 5 &= 1^2 + 2^2 = (1+2i)(1-2i), \\ 17 &= 1^2 + 4^2 = (1+4i)(1-4i), \\ 241 &= 15^2 + 4^2 = (15+4i)(15-4i). \end{aligned}$$

*Lako se vidi da je*

$$\frac{66+127i}{1+2i} = 64 - i.$$

*Sada faktoriziramo ovaj Gaussov cijeli broj. Pokazuje se da je*

$$\frac{64-i}{1-4i} = 4 + 15i.$$

*Odavde slijedi*

$$66 + 127i = (1+2i)(1-4i)(4+15i).$$

## 3.3. Primjene

Gaussovi cijeli brojevi se mogu primjeniti za:

1. klasifikaciju (primitivnih) Pitagorinih trojki,
2. klasifikaciju (primitivnih) rješenja diofantskih jednadžbi $a^2 + b^2 = c^3$,
3. dokazivanje tvrdnje da se prost broj u skupu $\mathbb{Z}$ na jedan može zapisati kao suma dvaju kvadrata,
4. sustavno nalaženje prirodnih brojeva koji se mogu zapisati na više načina kao suma dvaju kvadrata.

Detalji o ovim primjenama mogu se naći u [2] i [4]. Mi ćemo ovdje dokazati sljedeći teorem (što je spomenuta treća primjena).

**Teorem 3.4.** *Neka je $p$ prost broj koji se može zapisati u obliku sume dvaju kvadrata, $p = a^2 + b^2$, $a, b \in \mathbb{Z}$, onda su $a$ i $b$ jedinstveni do na poredak i predznak.*

*Dokaz.* Neka je $p$ prost broj, $p = a^2 + b^2$, $a, b \in \mathbb{Z}$. Broj $p$ u skupu $\mathbb{Z}[i]$ možemo zapisati kao $p = (a + bi)(a - bi)$, gdje su $a \pm bi$ prosti Gaussovi cijeli brojevi. Pretpostavimo da $p$ možemo zapisati na još jedan način kao sumu dvaju kvadrata, $p = c^2 + d^2 = (c + di)(c - di)$, $c, d \in \mathbb{Z}$, $c \pm di$ su prosti Gaussovi cijeli brojevi. Zbog teorema o jedinstvenoj faktorizaciji u skupu $\mathbb{Z}[i]$ slijedi da je

$$a + bi = \varepsilon(c + di) \quad ili \quad a + bi = \varepsilon(c - di),$$

gdje je $\varepsilon \in \{\pm 1, \pm i\}$. Promatrat ćemo samo jedan od ova dva prethodna slučaja jer jedina razlika između $c+di$ i $c-di$ je predznak ispred $i$, a cilj nam je pokazati da se $a$ i $b$ podudaraju sa $c$ i $d$ do na predznak i poredak pa ne moramo gledati oba slučaja. Pogledajmo kada je

$$a + bi = \varepsilon(c + di).$$

Ako je $\varepsilon = 1$, onda je $\varepsilon = a$ i $d = b$. Ako je $\varepsilon = -1$ onda je $c = -a$ i $d = -b$. Ako je $\varepsilon = i$, onda je $c = b$ i $d = -a$. Ako je $u = -i$, onda je $c = -b$ i $d = a$. Time smo pokazali da su $c$ i $d$ jednaki $a$ i $b$ do na predznak i poredak. □

**Primjer 3.6.** *Peti Fermatov broj* $2^{2^5} + 1$ *je suma dvaju kvadrata:* $2^{2^5} + 1 = 2^{16^2} + 1^2$. *Fermat je pretpostavljao da je taj broj prost broj, dok je Euler peti Fermatov broj zapisao na drugačiji način kao sumu dvaju kvdrata:*

$$2^{2^5} + 1 = 62264^2 + 20449^2.$$

*Neznajući nijednu netrivijalnu faktorizaciju broja* $2^{2^5} + 1$ *prema prethodnom teoremu možemo zaključiti da* $2^{2^5} + 1$ *nije prost broj.*

# Literatura


[1] Lee A. Butler, *A classification of Gaussian primes*, http://www2.stats.bris.ac.uk/~malab/PDFs/2ndYearEssay.pdf

[2] K. Conrad, *The Gaussian integers*, http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/Zinotes.pdf

[3] A. Dujella, *Uvod u teoriju brojeva*, PMF - Matematički odjel, Sveučilište u Zagrebu (skripta).

[4] I. Matić, *Uvod u teoriju brojeva*, Odjel za matematiku, Sveučilište u Osijeku (skripta).

[5] D. Shanks, *Solved and Unsolved Problems in Number Theory*, Chelsea Publishing company, New York, 1978.

[6] L. Lindahl, *Lectures on Number Theory*, http://www2.math.uu.se/~lal/kompendier/Talteori.pdf