Prsten Gaussovih cijelih brojeva i primjene

Novak, Iva

Prsten Gaussovih cijelih brojeva i primjene

Novak, Iva

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Iva Novak

PRSTEN GAUSSOVIH CIJELIH BROJEVA I PRIMJENE

Diplomski rad

Voditelj rada:
prof. dr. sc. Goran Muić,
dr. sc. Sonja Žunar

Zagreb, 2020.

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. _____

Sadržaj

Uvod

U ovom diplomskom radu bavit ćemo se Gaussovim cijelim brojevima i primjenom istih u matematici. Johann Carl Friedrich Gauss bio je njemački matematičar i astronom čiji je rad u matematici vrlo cijenjen, a to se najviše može vidjeti u području algebre, teorije brojeva i diferencijalnoj geometriji.
Prsten Gaussovih cijelih brojeva, u oznaci $\mathbb{Z}[i]$, generalizacija je prstena cijelih brojeva $\mathbb{Z}$ pa su kao takvi Gaussovi cijeli brojevi zadržali većinu svojstava cijelih brojeva. Konkretno rečeno, svaki element prstena $\mathbb{Z}[i]$ ima jedinstven rastav na proste faktore. Također, prsten $\mathbb{Z}[i]$ od velike je koristi za proučavanje sume dvaju kvadrata. To je zato što u $\mathbb{Z}[i]$ možemo faktorizirati sumu dvaju kvadrata cijelih brojeva u linearne faktore, tj. za sve $x, y \in \mathbb{Z}$ imamo $x^2 + y^2 = (x - yi)(x + yi)$.
U ovom diplomskom radu definirat ćemo Gaussove cijele brojeve i proučiti njihova svojstva. Govorit će se o njihovoj normi i invertibilnosti, a pomoću primjera vidjet će se njihova razlika u odnosu na cijele brojeve.
U drugom dijelu riječ će biti o dijeljenju (bez i s ostatkom) u $\mathbb{Z}[i]$, a u tu svrhu osvrnut ćemo se i na Euklidov algoritam te Bezoutov teorem.
U trećem dijelu govorit će se o faktorizaciji Gaussovih cijelih brojeva. Definirat će se prosti i složeni Gaussovi cijeli brojevi te će se iskazati i dokazati teorem o jedinstvenoj faktorizaciji.
Na kraju, dat će se nekoliko primjena $\mathbb{Z}[i]$ na aritmetiku u $\mathbb{Z}$. Konkretno, promatrat ćemo proste brojeve u $\mathbb{Z}$ te iskoristiti Gaussove cijele brojeve za dokazivanje tvrdnje da se prost broj u $\mathbb{Z}$ može zapisati kao suma dvaju kvadrata najviše na jedan način. Govorit će se i o primjeni $\mathbb{Z}[i]$ na klasifikaciju primitivnih Pitagorinih trojki te na određivanje cjelobrojnih rješenja jednadžbi $a^2 + b^2 = c^3$ i $y^2 + 1 = x^3$.

Poglavlje 1

Osnovni pojmovi

U ovom poglavlju navodimo pojmove koji su važni za razumijevanje ovog rada.

Definicija 1.0.1. *Neprazan skup $R = (R, +, \cdot)$ zovemo **prsten** ukoliko za operacije zbrajanja $+ : R \times R \to R$ i množenja $\cdot : R \times R \to R$ vrijedi:*

- *$(R, +)$ je komutativna grupa s neutralom $0 = 0_R$*
- *$(R, \cdot)$ je polugrupa, odnosno množenje je asocijativno*
- *vrijedi distributivnost množenja prema zbrajanju:*

$$x \cdot (y + z) = x \cdot y + x \cdot z, \ \forall x, y, z \in R$$

$$(x + y) \cdot z = x \cdot z + y \cdot z, \ \forall x, y, z \in R$$

Element $0 = 0_R$, neutral u grupi $(R, +)$, zovemo nula prstena R.
Ako postoji jedinični element (jedinica) $1 = 1_R \in R$ takav da je

$$1 \cdot x = x \cdot 1 = x, \ \forall x \in R,$$

*tada kažemo da je R **prsten s jedinicom**.*
*Prsten R je **komutativan prsten** ako je*

$$x \cdot y = y \cdot x, \ \forall x, y \in R,$$

inače govorimo o nekomutativnom prstenu.

Definicija 1.0.2. *Skup $S \subseteq R$, gdje je R neki prsten, je **potprsten** or R ako je $S = (S, +, \cdot)$ i sam prsten. Drugim riječima, S je potprsten od R ako vrijede sljedeća dva uvjeta:*

- *$(\forall x, y \in S)$: $x - y \in S$ (tj., (S,+) je grupa);*
- *$(\forall x, y \in S)$: $x \cdot y \in S$ (tj., $(S, \cdot)$ je grupoid).*

Definicija 1.0.3. *Neka je R prsten. Element $0 \neq \lambda \in R$ (tj. $0 \neq \rho \in R$) takav da je*

$$\lambda x = 0 \quad (\text{tj. } x\rho = 0), \quad \text{za neki } 0 \neq x \in R$$

zove se lijevi (tj. desni) djelitelj nule.
*R je **integralna domena (domena)**, ako nema ni lijevih ni desnih djelitelja nule.*

U nastavku, neka je $\mathcal{A}$ komutativan prsten s jedinicom.

Definicija 1.0.4. *Prsten $\mathcal{A}$ je **Euklidova domena** ako je integralna domena i ako postoji neka funkcija $\lambda : \mathcal{A} \setminus 0 \to \mathbb{N}_0$ takva da za nju vrijedi:*
Ako su elementi $A,\ B \in \mathcal{A}$, gdje je $B \neq 0$, onda postoje neki elementi $C,\ D \in \mathcal{A}$ takvi da je $A = BC + D$, gdje je $D = 0$ ili $\lambda(D) < \lambda(B)$.

Napomena 1.0.5. *Ako je prsten $\mathcal{A}$ Euklidova domena, postoji "konstruktivna metoda" traženja najvećeg zajedničkog djelitelja dvaju elementa $a,\ b \in \mathcal{A}$. Ta metoda je Euklidov algoritam.*

Definicija 1.0.6. *Za elemente $x,\ y \in \mathcal{A},\ y \neq 0$, kažemo da "y dijeli x", pišemo $y \mid x$ ako*

$$\exists\, c \in \mathcal{A} :\ x = yc.$$

Element $c \in \mathcal{A}$ je **ireducibilan** ako je ispunjeno:

- $0 \neq c \notin \mathcal{A}^x$,
- Ako je $c = ab$, onda je ili $a \in \mathcal{A}^x$ ili je $b \in \mathcal{A}^x$.

Odnosno, element je ireducibilan ako je nenul neinvertibilan element koji se ne može zapisati kao produkt dva neinvertibilna elementa.

Napomena 1.0.7. *$\mathcal{A}^x :=$ grupa invertibilnih elemenata u prstenu $\mathcal{A}$.*

Element $p \in \mathcal{A}$ je **prost** ako je ispunjeno:

- $0 \neq p \notin \mathcal{A}^x$,
- Ako $p \mid ab$, onda ili $p \mid a$ ili $p \mid b$.

Odnosno, element je prost ako je nenul neinvertibilan element koji ima svojstvo da ako dijeli produkt dva elementa, onda on dijeli barem jedan od faktora.

Definicija 1.0.8. *Kažemo da su elementi $a, b \in \mathcal{A}$* ***asocirani*** *i koristimo oznaku $a \sim b$, ako:*

$$\exists\, u \in \mathcal{A}^x \ : \ a = ub.$$

Definicija 1.0.9. *Integralna domena $\mathcal{A}$ je* ***faktorijalan prsten (faktorizacijski prsten, domena jedinstvene faktorizacije)*** *ako vrijedi:*

- *(Egzistencija rastava)*
  Za svaki $a \in \mathcal{A},\ 0 \neq a \notin \mathcal{A}^x$, postoji rastav

  $$a = c_1 \cdots c_n,$$

  gdje su $c_i \in \mathcal{A}$ ireducibilni elementi.

- *(Jedinstvenost rastava)*
  Ako imamo dva rastava $a = c_1 \cdots c_n = e_1 \cdots e_m$, onda je $m = n$ i postoji neka permutacija $\sigma \in S_n$ tako da je $c_i \sim e_{\sigma(i)}$.

Iz [3, Propozicija 3.8] slijedi sljedeća propozicija:

Propozicija 1.0.10. *Neka je $\mathcal{A}$ faktorijalan prsten. Tada je $a \in \mathcal{A}$ ireducibilan ako i samo ako je prost.*

Sve definicije i tvrdnje preuzete su iz [5].

Poglavlje 2

Prsten Gaussovih cijelih brojeva

Prsten Gaussovih cijelih brojeva je potprsten

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

od $\mathbb{C}$, gdje je $i = \sqrt{-1}$.
Kao njegovu prvu prednost u odnosu na prsten $\mathbb{Z}$ primijetimo sljedeće: polinom $x^2 + y^2$ ne može se zapisati kao produkt linearnih polinoma s koeficijentima u $\mathbb{Z}$, ali može se zapisati kao produkt

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

linearnih polinoma s koeficijentima u $\mathbb{Z}[i]$.
Pogledajmo na primjeru. Neka je zadan prirodan broj 5. Vrijedi:

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

Iz ove jednostavne činjenice proizlaze neke važne primjene prstena $\mathbb{Z}[i]$ u teoriji brojeva, neke od kojih ćemo proučiti u ovom radu.

2.1 Norma

Definicija 2.1.1. *Neka je $\alpha = a + bi \in \mathbb{Z}[i]$. Preslikavanje $\mathcal{N} : \mathbb{Z}[i] \to \mathbb{N} \cup \{0\}$ zadano s*

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

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

Za tako definiranu funkciju vrijedi:
1. $\mathcal{N}(\alpha) > 0, \forall \alpha \in \mathbb{Z}[i]\backslash\{0\}$,
2. $\mathcal{N}(\alpha) = 0 \Leftrightarrow \alpha = 0$.

Primjerice ako imamo $\alpha = 3 + 8i$, tada norma iznosi $\mathcal{N}(3 + 8i) = 3^2 + 8^2 = 9 + 64 = 73$.
Općenito, za svaki $m \in \mathbb{Z}$ je $\mathcal{N}(m) = m^2$. Posebno, $\mathcal{N}(1) = 1$.

Sljedeći teorem govori o svojstvu multiplikativnosti norme.

Teorem 2.1.2. *Za sve $\alpha, \beta \in \mathbb{Z}[i]$ vrijedi: $\mathcal{N}(\alpha\beta) = \mathcal{N}(\alpha)\mathcal{N}(\beta)$, odnosno, norma je multiplikativna.*

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

$$\mathcal{N}(\alpha\beta) = (\alpha\beta)\overline{(\alpha\beta)} = (\alpha\beta)(\overline{\alpha}\overline{\beta}) = (\alpha\overline{\alpha})(\beta\overline{\beta}) = \mathcal{N}(\alpha)\mathcal{N}(\beta).$$

□

Neka su $\alpha = a + bi$, $\beta = c + di \in \mathbb{Z}[i]$. Prema teoremu 2.1.2. znamo da vrijedi:

$$\mathcal{N}(\alpha\beta) = \mathcal{N}(\alpha)\mathcal{N}(\beta).$$

Uvrštavanjem α i β u gornju jednakost i njezinim sređivanjem dobivamo

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

Gornju jednakost nazivamo Diofantov identitet. Diofant[1] se bavio teorijom brojeva, posebice sumom dvaju kvadrata. Znao je da je produkt suma dvaju kvadrata opet suma dvaju kvadrata. Ovdje se može primijetiti da neka svojstva prstena $\mathbb{Z}[i]$ imaju daleke korijene, jer ih je poznavao Diofant koji je živio u 3. st. nove ere.

2.2 Invertibilnost

Definicija 2.2.1. *Element $\alpha \in \mathbb{Z}[i]$ zovemo invertibilnim elementom ako postoji $\beta \in \mathbb{Z}[i]$ takav da vrijedi $\alpha\beta = \beta\alpha = 1$. Element β označavamo sa α^{-1}, tj. $\beta = \alpha^{-1}$, i nazivamo ga multiplikativni inverz od α.*

Važna primjena teorema 2.1.2., koji smo spomenuli u prethodnom poglavlju, je pri određivanju Gaussovih cijelih brojeva koji imaju multiplikativni inverz u $\mathbb{Z}$. Ideja je iskoristiti normu kako bi se odredili invertibilni elementi.

Propozicija 2.2.2. *$\alpha \in \mathbb{Z}[i]$ je invertibilan akko je $\mathcal{N}(\alpha) = 1$.*

Dokaz. Neka je $\alpha \in \mathbb{Z}[i]$ invertibilni element. Prema definiciji 2.2.1. znamo da postoji $\beta \in \mathbb{Z}[i]$ td. vrijedi $\alpha\beta = 1$. Uočimo da mora vrijediti da su $\alpha \neq 0$ i $\beta \neq 0$.
Prema teoremu 2.1.2. imamo

$$\mathcal{N}(\alpha)\mathcal{N}(\beta) = \mathcal{N}(\alpha\beta) = \mathcal{N}(1) = 1$$

[1] Diofant (3. st. n. e.) - starogrčki matematičar

i $\mathcal{N}(\alpha), \mathcal{N}(\beta) \in \mathbb{N}$ pa slijedi da je

$$\mathcal{N}(\alpha) = \mathcal{N}(\beta) = 1.$$

Obratno, pretpostavimo da je $\mathcal{N}(\alpha) = 1$. Tada vrijedi da je $\alpha\overline{\alpha} = 1$. Sada slijedi da je $\overline{\alpha} = \alpha^{-1}$. Prema definiciji 2.2.1. slijedi da je $\alpha \in \mathbb{Z}[i]$ invertibilan. □

Korolar 2.2.3. *Jedini invertibilni elementi u* $\mathbb{Z}[i]$ *su* ± 1 *i* $\pm i$.

Dokaz. Trebamo pokazati da su ± 1 i $\pm i$ jedini invertibilni elementi. Neka je $\alpha \in \mathbb{Z}[i]$, $\alpha = a + bi$, invertibilan. Tada po propoziciji 2.2.2. vrijedi $\mathcal{N}(\alpha) = 1$, odnosno

$$1 = \mathcal{N}(\alpha) = \mathcal{N}(\alpha)\mathcal{N}(\overline{\alpha}) = (a + bi)(a - bi) = a^2 + b^2.$$

Uočimo da mora vrijediti $a = 0$ ili $b = 0$. U protivnom, ako je $a \neq 0$ i $b \neq 0$, tada bi imali $|a + bi| > 1$ i $|a - bi| > 1$. To bi značilo da je $(a + bi)(a - bi) \geq 2$ što nije moguće. Sada razlikujemo dva slučaja:

1. slučaj: $a = 0$ i $b = \pm 1$, tada je $\alpha = i$ ili $\alpha = -i$
2. slučaj: $a = \pm 1$ i $b = 0$, tada je $\alpha = 1$ ili $\alpha = -1$.

Znači da su jedini invertibilni elementi u $\mathbb{Z}[i] \pm 1$ i $\pm i$. □

Invertibilne elemente u $\mathbb{Z}[i]$ iz prethodnog korolara još zovemo jedinice.

Sada možemo usporediti prsten cijelih brojeva $\mathbb{Z}$ i prsten Gaussovih cijelih brojeva $\mathbb{Z}[i]$.
U prstenu $\mathbb{Z}$, analogon norme je apsolutna vrijednost broja, a invertibilni elementi su -1 i 1. Iz činjenice da je $|\alpha| = |\beta|$ za $\alpha, \beta \in \mathbb{Z}$ slijedi da je $\alpha = \pm\beta$.
Međutim, situacija je drugačija u $\mathbb{Z}[i]$. Ako je $\mathcal{N}(\alpha) = \mathcal{N}(\beta)$ za $\alpha, \beta \in \mathbb{Z}[i]$, ne mora značiti da je $\alpha = n \cdot \beta$, gdje je $n \in \{-1, 1, -i, i\}$.

Primjer 2.2.4. *Neka je* $\alpha = 2 + 6i$*, a* $\beta = 2 - 6i$*. Jednostavnim računom dobivamo da je* $\mathcal{N}(\alpha) = \mathcal{N}(\beta) = 40$*, ali ne postoji* $n \in \{-1, 1, -i, i\}$ *tako da je* $\alpha = n \cdot \beta$.

Poglavlje 3

Dijeljenje u $\mathbb{Z}[i]$

3.1 Djeljivost

Pitanje djeljivosti u prstenu $\mathbb{Z}[i]$ možemo proučavati na isti način kao pitanje djeljivosti u prstenu $\mathbb{Z}$. Djeljivost se definira na prirodan način, sljedećom definicijom koja je poseban slučaj Definicije 1.0.6.

Definicija 3.1.1. *Neka su $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$. Ako postoji $\gamma \in \mathbb{Z}[i]$ takav da je $\alpha = \beta\gamma$, onda kažemo da β dijeli α ili da je α djeljiv sa β, i pišemo $\beta \mid \alpha$.*

Element α iz definicije nazivamo djeljenik, a element β nazivamo djelitelj. Njihov rezultat γ pri dijeljenju nazivamo količnik.
Sada ćemo kroz tri primjera vidjeti situacije kada $\alpha \in \mathbb{Z}[i]$ jest odnosno nije djeljiv sa $\beta \in \mathbb{Z}[i]$.

Primjer 3.1.2. *Kako je*

$$10 + 5i = (3 + 4i)(2 - i)$$

zaključujemo da $(3 + 4i) \mid (10 + 5i)$.

Primjer 3.1.3. *Provjerimo je li $\alpha = 19 + 7i$ djeljiv s $\beta = 4 + i$.*
Imamo:

$$\frac{19 + 7i}{4 + i} = \frac{19 + 7i}{4 + i} \cdot \frac{4 - i}{4 - i} = \frac{83 + 9i}{17} = \frac{83}{17} + \frac{9}{17}i \notin \mathbb{Z}[i].$$

Realni i imaginarni dio su $\frac{83}{17}$ i $\frac{9}{17}$, a to nisu cijeli brojevi. Zaključujemo da $\beta \nmid \alpha$.

Primjer 3.1.4. *Provjerimo je li $\alpha = 31 + 34i$ djeljiv s $\beta = 5 - 2i$.*
Imamo:

$$\frac{31+34i}{5-2i} = \frac{31+34i}{5-2i} \cdot \frac{5+2i}{5+2i} = \frac{87+232i}{29} = \frac{87}{29} + \frac{232}{29}i = 3 + 8i.$$

Realni i imaginarni dio su cijeli brojevi pa zaključujemo da $\beta \mid \alpha$.

Sljedeći teorem dat će odgovor na pitanje kada je Gaussov cijeli broj djeljiv cijelim brojem.

Teorem 3.1.5. *Gaussov cijeli broj $\alpha = a + bi$ djeljiv je cijelim brojem $c \in \mathbb{Z}$ akko $c \mid a$ i $c \mid b$ u $\mathbb{Z}$.*

Dokaz. Neka je Gaussov cijeli broj $\alpha = a+bi$ djeljiv s $c \in \mathbb{Z} \subset \mathbb{Z}[i]$. Po definiciji djeljivosti, znamo da postoji $\beta = d + ei \in \mathbb{Z}[i]$ takav da je $\alpha = c\beta = c(d + ei)$. Tada je

$$\alpha = a + bi = cd + (ce)i.$$

Sada izjednačimo realni dio s realnim te imaginarni dio s imaginarnim i dobivamo:

$$a = cd \text{ i } b = ce,$$

iz čega možemo zaključiti da $c \mid a$ i $c \mid b$ u $\mathbb{Z}$.
Obrat trivijalno vrijedi. □

Napomena 3.1.6. *Ako u teoremu 3.1.5. uzmemo da je $b = 0$, odnosno $\alpha = a$, dobivamo da se dijeljenje između cijelih brojeva ne mijenja kada smo u prstenu $\mathbb{Z}[i]$. Preciznije rečeno, za $\alpha, \beta \in \mathbb{Z}$, $\beta \mid \alpha$ u $\mathbb{Z}[i]$ akko $\beta \mid \alpha$ u $\mathbb{Z}$.*

Teorem 3.1.7. *Neka su $\alpha, \beta \in \mathbb{Z}[i]$. Ako β dijeli α u $\mathbb{Z}[i]$, onda $N(\beta)$ dijeli $N(\alpha)$ u $\mathbb{Z}$.*

Dokaz. Neka su $\alpha, \beta \in \mathbb{Z}[i]$ i neka $\beta \mid \alpha$. Po definiciji djeljivosti znamo da postoji neki $c \in \mathbb{Z}[i]$ tako da je $\alpha = c\beta$. Tada je

$$N(\alpha) = N(c\beta) = N(c)N(\beta),$$

a iz ovoga možemo vidjeti da $N(\beta) \mid N(\alpha)$. □

Napomena 3.1.8. *Uočimo da obrat teorema 3.1.7. ne vrijedi. Pogledajmo primjer.*

Primjer 3.1.9. *Neka je $\alpha = 8 + 6i$ i $\beta = 2 + i$. Tada je $\mathcal{N}(\alpha) = 100, \mathcal{N}(\beta) = 5$. Vidimo da $\mathcal{N}(\beta) \mid \mathcal{N}(\alpha)$, ali*

$$\frac{8+6i}{2+i} = \frac{8+6i}{2+i} \cdot \frac{2-i}{2-i} = \frac{22+4i}{5} = \frac{22}{5} + \frac{4}{5}i \notin \mathbb{Z}[i]$$

iz čega slijedi da $\beta \nmid \alpha$.

Korolar 3.1.10. *Gaussov cijeli broj ima parnu normu akko je višekratnik od $1 + i$.*

Dokaz. Neka je $\alpha \in \mathbb{Z}[i]$ i neka je α višekratnik od $1 + i$, odnosno $(1 + i) \mid \alpha$. Iz teorema 3.1.7. slijedi da $\mathcal{N}(1 + i) \mid \mathcal{N}(\alpha)$. Uočimo da je $\mathcal{N}(1 + i) = 2$ iz čega vidimo da $2 \mid \mathcal{N}(\alpha)$, odnosno $\mathcal{N}(\alpha)$ je paran broj.
Obratno, pretpostavimo da Gaussov cijeli broj $\alpha = a + bi$ ima parnu normu, tj.

$$a^2 + b^2 \equiv 0 \pmod 2.$$

Tada su a, b oba parni ili oba neparni brojevi, što u oba slučaja znači da je

$$a \equiv b \pmod 2.$$

Želimo Gaussov cijeli broj α napisati u obliku $a + bi = (1 + i)(c + di),\ c, d \in \mathbb{Z}$.
To je isto kao i:

$$a + bi = (c - d) + (c + d)i.$$

Uzmimo da je $c = \frac{a+b}{2}$ i $d = \frac{b-a}{2}$ i dobijemo upravo ono što smo trebali pokazati, tj. $(1 + i) \mid \alpha$. □

3.2 Dijeljenje s ostatkom

Na početku ćemo iskazati teorem o dijeljenju s ostatkom koji nećemo tada dokazati. Kroz primjere ćemo doći do modificiranog teorema o dijeljenju s ostatkom u $\mathbb{Z}$, koji ćemo i dokazati. Konačno, vratit ćemo se na teorem o dijeljenju s ostatkom te ga dokazati.

Teorem 3.2.1. *Za $\alpha,\ \beta \in \mathbb{Z}[i],\ \beta \neq 0$, postoje $\gamma,\ \delta \in \mathbb{Z}[i]$ takvi da je $\alpha = \beta\gamma + \delta$ i $\mathcal{N}(\delta) < \mathcal{N}(\beta)$. Štoviše, možemo izabrati δ takav da je $\mathcal{N}(\delta) \leq \frac{1}{2}\mathcal{N}(\beta)$.*

Gaussov cijeli broj γ iz teorema zovemo količnik (kvocijent), a δ zovemo ostatak. Norma ostatka je omeđena, preciznije, vrijedi $0 \leq \mathcal{N}(\delta) < \mathcal{N}(\beta)$.

Primjer 3.2.2. *Neka su $\alpha = 27-23i$, $\beta = 8+i$. Trebamo odrediti γ, δ takve da je $\alpha = \beta\gamma+\delta$. Ideja je pogledati omjer $\frac{\alpha}{\beta}$ i racionalizirati nazivnik.*
Imamo:

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\beta\overline{\beta}} = \frac{(27-23i)(8-i)}{65} = \frac{193-211i}{65} = \frac{193}{65} - \frac{211}{65}i.$$

DijelećI s ostatkom u prstenu $\mathbb{Z}$ dobivamo:

$$\frac{193}{65} = 2 + \frac{63}{65},$$
$$-\frac{211}{65} = -4 + \frac{49}{65}.$$

Iz ovih jednakosti vidimo da je prirodan kandidat za naš količnik $\gamma = 2 - 4i$.
Dalje trebamo izračunati ostatak. Kako je $\alpha = \beta\gamma + \delta$, slijedi da je $\delta = \alpha - \beta\gamma$.
Imamo:

$$\delta = \alpha - \beta\gamma = (27 - 23i) - (8 + i)(2 - 4i) = 7 + 7i.$$

Sada možemo uočiti da je:

$$\mathcal{N}(\delta) > \mathcal{N}(\beta) = 65.$$

Izbor ovakvih γ, δ nije dobar zato što želimo da nam bude $\mathcal{N}(\beta) > \mathcal{N}(\delta)$.
Promijenit ćemo pristup odabiru γ. Zamijenit ćemo $193 : 65 \approx 2.969$ i $-211 : 65 \approx -3.246$ najbližim cijelim brojem. Uočimo da je količnik u prvom slučaju tada 3, a u drugom slučaju je -3. Sada imamo $\gamma = 3 - 3i$.
Uvrstimo $\gamma = 3 - 3i$ u izraz $\delta = \alpha - \beta\gamma$ i dobivamo $\delta = -2i$.
Sada imamo:$\mathcal{N}(\delta) = 4 < \mathcal{N}(\beta) = 65$.

U standardnom teoremu o dijeljenju s ostatkom u prstenu $\mathbb{Z}$ ostatak bi nam uvijek bio nenegativan broj. Postupak kojim smo riješili prethodni primjer dopustio nam je da ostatak bude negativan cijeli broj. Taj postupak u vezi je s modificiranim teoremom o dijeljenju s ostatkom koji ćemo precizno iskazati i dokazati.
Ostatak dobiven modificiranim teoremom o dijeljenju s ostatkom, po apsolutnoj vrijednosti manji je ili jednak ostatku koji bismo dobili kada bismo radili standardnim postupkom.

Teorem 3.2.3. ***(Modificirani teorem o dijeljenju s ostatkom u*** $\mathbb{Z}$***).***
Neka je $a \in \mathbb{Z}$ *i* $b \in \mathbb{N}$. *Tada postoje cijeli brojevi* q *i* r *takvi da vrijedi*

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

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

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

Definiramo $r = a - bq$. Sada slijedi $a = bq + r$ i

$$|r| = |a - bq| = \left|\left(\frac{a}{b} - q\right)b\right| = \left|\frac{a}{b} - q\right|b = \left|q - \frac{a}{b}\right|b \leq \frac{1}{2}b.$$

□

Sada se možemo vratiti na početak i dokazati teorem 3.2.1.

Dokaz. (Teorem 3.2.1.)
Neka su $\alpha,\ \beta \in \mathbb{Z}[i],\ \beta \neq 0$. Želimo konstruirati $\gamma,\ \delta \in \mathbb{Z}[i]$ takve da je $\alpha = \beta\gamma + \delta$, $\mathcal{N}(\delta) \leq \frac{1}{2}\mathcal{N}(\beta)$.
Neka je

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\beta\overline{\beta}} = \frac{a + bi}{\mathcal{N}(\beta)},\ \alpha\overline{\beta} = a + bi.$$

Koristeći modificirani teorem o dijeljenju s ostatkom u $\mathbb{Z}$, podijelimo a i b s $\mathcal{N}(\beta)$. Dobivamo

$$a = \mathcal{N}(\beta)q_1 + r_1,\ q_1 \in \mathbb{Z},\ 0 \leq |r_1| \leq \frac{1}{2}\mathcal{N}(\beta),$$

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

Tako dobivene $a,\ b$ vratimo u izraz $\frac{\alpha}{\beta}$:

$$\frac{\alpha}{\beta} = \frac{\mathcal{N}(\beta)q_1 + r_1 + (\mathcal{N}(\beta)q_2 + r_2)i}{\mathcal{N}(\beta)} = q_1 + q_2 i + \frac{r_1 + r_2 i}{\mathcal{N}(\beta)}$$

Kako je $\mathcal{N}(\beta) = \beta\overline{\beta}$, stavljanjem da je $\gamma = q_1 + q_2 i$ slijedi da je

$$\frac{\alpha}{\beta} = \gamma + \frac{r_1 + r_2 i}{\beta\overline{\beta}}.$$

Množenjem ove jednakosti s β dobivamo:

$$\alpha = \gamma\beta + \frac{r_1 + r_2 i}{\overline{\beta}}.$$

iz čega slijedi da je

$$\alpha - \gamma\beta = \frac{r_1 + r_2 i}{\overline{\beta}}.$$

Kako su $\alpha,\ \beta,\ \gamma \in \mathbb{Z}[i]$, tada je i $\frac{r_1+r_2 i}{\overline{\beta}} \in \mathbb{Z}[i]$. Označimo $\delta = \alpha - \gamma\beta = \frac{r_1+r_2 i}{\overline{\beta}}$.
Još trebamo pokazati da je $\mathcal{N}(\delta) \leq \frac{1}{2}\mathcal{N}(\beta)$.
Kako je

$$\alpha - \gamma\beta = \frac{r_1 + r_2 i}{\overline{\beta}},$$

zaključujemo da je

$$\mathcal{N}(\alpha - \gamma\beta) = \mathcal{N}\Big(\frac{r_1 + r_2 i}{\overline{\beta}}\Big).$$

Znamo da je $\mathcal{N}(\beta) = \mathcal{N}(\overline{\beta})$ pa imamo:

$$\mathcal{N}(\alpha - \gamma\beta) = \Big(\frac{r_1^2 + r_2^2}{\mathcal{N}(\beta)}\Big).$$

Budući da je

$$0 \leq |r_k| \leq \frac{1}{2}\mathcal{N}(\beta),\ k = 1, 2,$$

slijedi da je

$$\mathcal{N}(\alpha - \gamma\beta) \leq \frac{\frac{1}{4}\mathcal{N}(\beta)^2 + \frac{1}{4}\mathcal{N}(\beta)^2}{\mathcal{N}(\beta)} = \frac{1}{2}\mathcal{N}(\beta).$$

□

Primjer 3.2.4. *Neka je* $\alpha = 41 + 24i$ *i* $\beta = 11 - 2i$. *Trebamo pronaći* $\gamma,\ \delta \in \mathbb{Z}[i]$ *takve da je* $\alpha = \beta\gamma + \delta$.
Slijedi da je:

$$\frac{\alpha}{\beta} = \frac{41 + 24i}{11 - 2i} \cdot \frac{11 + 2i}{11 + 2i} = \frac{403 + 346i}{125}.$$

Uočavamo da je

$$403 : 125 \approx 3.224,\ 346 : 125 \approx 2.768.$$

Zaključujemo da je $\gamma = 3 + 3i,$ *a ostatak* $\delta = (41 + 24i) - (11 - 2i)(3 + 3i) = 2 - 3i$.
Uočimo da vrijedi $\mathcal{N}(\delta) = 13 < \frac{1}{2}\mathcal{N}(\beta) = \frac{125}{2}$.

Zanimljiva razlika između teorema o dijeljenju s ostatkom u $\mathbb{Z}[i]$ i (uobičajenog) teorema o dijeljenju s ostatkom u $\mathbb{Z}$ je ta da kvocijent i ostatak nisu jedinstveni u $\mathbb{Z}[i]$. Pogledajmo sljedeći primjer.

Primjer 3.2.5. *Neka je $\alpha = 1 + 8i$ i $\beta = 2 - 4i$.*
Tada je

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\mathcal{N}(\beta)} = \frac{-30 + 20i}{20} = -\frac{3}{2} + i.$$

Uočavamo da je $-3 : 2 = -1.5$ što leži na sredini između brojeva -2 i -1. Imamo dvije mogućnosti za kvocijent: $\gamma_1 = -1 + i$ i $\gamma_2 = -2 + i$.
U prvom slučaju dobivamo

$$\delta_1 = 1 + 8i - (2 - 4i)(-1 + i) = -1 + 2i.$$

Vidimo da vrijedi: $\mathcal{N}(\delta_1) = 5 < \frac{1}{2}\mathcal{N}(\beta) = 10$.
U drugom slučaju dobivamo

$$\delta_2 = 1 + 8i - (2 - 4i)(-2 + i) = 1 - 2i.$$

Vidimo da vrijedi: $\mathcal{N}(\delta_2) = 5 < \frac{1}{2}\mathcal{N}(\beta) = 10$.

Nedostatak jedinstvenosti kvocijenta i ostatka u dijeljenju u $\mathbb{Z}[i]$ ne utječe na korisnost dijeljenja. Štoviše, ako gledamo $\mathbb{Z}$, jedinstvenost kvocijenta i ostatka u uobičajenom teoremu o dijeljenju je nevažna kod primjene npr. u Euklidovom[1] algoritmu. U sljedećem poglavlju riječ će biti upravo o Euklidovom algoritmu.

3.3 Euklidov algoritam

Na početku navodimo definicije koje su nužne za razumijevanje ovog poglavlja.

Definicija 3.3.1. *Neka su $\alpha, \beta \in \mathbb{Z}[i]$. Zajednički djelitelj Gaussovih cijelih brojeva α i β je svaki $\gamma \in \mathbb{Z}[i]$ sa svojstvom da $\gamma \mid \alpha$ i $\gamma \mid \beta$.*

Definicija 3.3.2. *Najveći zajednički djelitelj brojeva $\alpha, \beta \in \mathbb{Z}[i]$ zajednički je djelitelj od α i β s najvećom normom.*

[1] Euklid (4.-3.st.pr.Kr.) - starogrčki matematičar

Definicija 3.3.3. *Kažemo da su $\alpha,\ \beta \in \mathbb{Z}[i]$ relativno prosti ako su im jedini zajednički djelitelji invertibilni elementi.*

Odgovor na pitanje kako odrediti najveći zajednički djelitelj dvaju Gaussovih cijelih brojeva, dat će Euklidov algoritam. U nastavku navodi se iskaz i dokaz Euklidovog algoritma.

Teorem 3.3.4. *(**Euklidov algoritam**) Neka su $\alpha,\ \beta \in \mathbb{Z}[i],\ \alpha,\ \beta \neq 0$. Rekurzivnom primjenom teorema o dijeljenju s ostatkom na α i β pa na djelitelj i ostatak sve dok ostatak nije nula, dobivamo sljedeći niz jednakosti:*

$$\alpha = \beta\gamma_1 + \delta_1,\ \ \mathcal{N}(\delta_1) < \mathcal{N}(\beta), \tag{1}$$

$$\beta = \delta_1\gamma_2 + \delta_2,\ \ \mathcal{N}(\delta_2) < \mathcal{N}(\delta_1), \tag{2}$$

$$\delta_1 = \delta_2\gamma_3 + \delta_3,\ \ \mathcal{N}(\delta_3) < \mathcal{N}(\delta_2), \tag{3}$$

$$\vdots$$

$$\delta_{n-2} = \delta_{n-1}\gamma_n + \delta_n,\ \ \mathcal{N}(\delta_n) < \mathcal{N}(\delta_{n-1}), \tag{4}$$

$$\delta_{n-1} = \delta_n\gamma_{n+1} + 0. \tag{5}$$

Zadnji ostatak različit od nule je najveći zajednički djelitelj brojeva α i β.

Dokaz. Dokaz je identičan uobičajenom dokazu Euklidovog algoritma u prstenu $\mathbb{Z}$ pa će se zato prikazati nešto kraća argumentacija.
Iz (1) možemo zaključiti da svaki zajednički djelitelj od α i β dijeli δ_1. Isti zaključak primijenimo na (2) pa možemo zaključiti da svaki zajednički djelitelj od α i β dijeli δ_2. Analognim zaključivanjem iz preostalog niza jednakosti, zaključujemo da svaki zajednički djelitelj brojeva α i β dijeli svaki $\delta_k,\ k = 1, ..., n$. Posebno, svaki zajednički djelitelj brojeva α i β dijeli δ_n.
S druge strane, iz zadnje jednakosti (5) slijedi da δ_n dijeli δ_{n-1} pa sada iz (4) slijedi da δ_n dijeli δ_{n-2}. Analognim zaključivanjem kroz cijeli niz jednakosti, možemo zaključiti da je δ_n zajednički djelitelj brojeva α i β. Kako je on zajednički djelitelj koji je djeljiv sa svakim drugim zajedničkim djeliteljem brojeva α i β, tada slijedi da je on maksimalne norme. □

Primjer 3.3.5. *Odredimo najveći zajednički djelitelj brojeva $\alpha = 32 + 9i$ i $\beta = 4 + 11i$. Primjenom Euklidovog algoritma dobivamo*

$$32 + 9i = (4 + 11i)(2 - 2i) + 2 - 5i$$

$$4 + 11i = (2 - 5i)(-2 + i) + 3 - i$$

$$2 - 5i = (3 - i)(1 - i) - i$$

$$3 - i = (-i)(1 - 3i) + 0.$$

Uočavamo da je najveći zajednički djelitelj brojeva α i β jednak $-i$. Prema definiciji 3.3.3. zaključujemo da su α i β relativno prosti.

Pogledajmo primjer u kojem najveći zajednički djelitelj nije jedan od invertibilnih elemenata u $\mathbb{Z}[i]$.

Primjer 3.3.6. *Odredimo najveći zajednički djelitelj brojeva $\alpha = 11 + 3i$ i $\beta = 1 + 8i$. Primjenom Euklidovog algoritma dobivamo*

$$11 + 3i = (1 + 8i)(1 - i) + 2 - 4i$$

$$1 + 8i = (2 - 4i)(-1 + i) - 1 + 2i$$

$$2 - 4i = (-1 + 2i)(-2) + 0.$$

Uočavamo da je najveći zajednički djelitelj brojeva α i β jednak $-1 + 2i$.
No, najveći zajednički djelitelj danih brojeva je i $1 - 2i$ zato što je:

$$11 + 3i = (1 + 8i)(1 - i) + 2 - 4i$$

$$1 + 8i = (2 - 4i)(-2 + i) + 1 - 2i$$

$$2 - 4i = (1 - 2i)(2) + 0.$$

Dobili smo dva različita najveća zajednička djelitelja brojeva α i β. Međutim, pogledamo li bolje. uočavamo da je $-1 + 2i = (-1)(1 - 2i)$.

Napomena 3.3.7. *U daljnjem tekstu, najveći zajednički djelitelj brojeva a i b u prstenu cijelih brojeva $\mathbb{Z}$, označavat ćemo s (a, b).*

Uočimo sljedeće. Ako je γ najveći zajednički djelitelj Gaussovih cijelih brojeva α i β, onda $N(\gamma) \mid N(\alpha)$ i $N(\gamma) \mid N(\beta)$. Odnosno $N(\gamma)$ dijeli $(N(\alpha), N(\beta))$. Međutim, može se dogoditi da je $N(\gamma) < (N(\alpha), N(\beta))$. Pogledajmo primjer.

Primjer 3.3.8. *Neka su* $\alpha = 11 + 3i$ *i* $\beta = 1 + 8i$.
Vidimo da je $\mathcal{N}(\alpha) = 130$ *i* $\mathcal{N}(\beta) = 65$. *Slijedi da je*

$$(\mathcal{N}(\alpha), \mathcal{N}(\beta)) = (130, 65) = 65.$$

Najveći zajednički djelitelj danih Gaussovih cijelih brojeva je $\gamma = -1+2i$, *a njegova norma je* $\mathcal{N}(\gamma) = 5$. *Očito je da je:*

$$\mathcal{N}(\gamma) = 5 < 65 = (\mathcal{N}(\alpha), \mathcal{N}(\beta)).$$

Napomena 3.3.9. *Pretpostavimo da za Gaussove cijele brojeve* α *i* β *vrijedi da su njihove norme relativno proste u prstenu* $\mathbb{Z}$, *tj. vrijedi* $(\mathcal{N}(\alpha), \mathcal{N}(\beta)) = 1$. *Također,* γ *je najveći zajednički djelitelj od* α *i* β. *Tada* $\gamma \mid \alpha$ *i* $\gamma \mid \beta$, *iz čega slijedi da* $\mathcal{N}(\gamma) \mid \mathcal{N}(\alpha)$ *i* $\mathcal{N}(\gamma) \mid \mathcal{N}(\beta)$. *Zaključujemo da je* $\mathcal{N}(\gamma) = 1$, *odnosno* $\gamma = \lambda,\ \lambda \in \{\pm 1, \pm i\}$.

Primjer 3.3.10. *Neka je* $\alpha = 24 - 9i$ *i* $\beta = 5 + 7i$. *Vidimo da je:*

$$\mathcal{N}(\alpha) = 657,\ \mathcal{N}(\beta) = 74.$$

Uočavamo da je $(657, 74) = 1$ *pa prema prethodno navedenoj napomeni slijedi da je najveći zajednički djelitelj brojeva* α *i* β *upravo* $\lambda,\ \lambda \in \{\pm 1, \pm i\}$.

Za kraj, navodimo korolar koji govori da je najveći zajednički djelitelj dvaju Gaussovih cijelih brojeva jedinstven do na množenje invertibilnim elementom. Prisjetimo se, jedini invertibilni elementi u prstenu $\mathbb{Z}[i]$ su ± 1 i $\pm i$.

Korolar 3.3.11. *Neka su* $\alpha,\ \beta \in \mathbb{Z}[i],\ \alpha,\ \beta \neq 0$ *te neka je* γ *najveći zajednički djelitelj brojeva* α *i* β *dobiven Euklidovim algoritmom. Tada je bilo koji najveći zajednički djelitelj* δ *od* α *i* β *oblika* $\delta = \lambda\gamma,\ \lambda \in \{\pm 1, \pm i.\}$

Dokaz. Neka je γ najveći zajednički djelitelj Gaussovih cijelih brojeva α i β koji je dobiven Euklidovim algoritmom. Neka je δ najveći zajednički djelitelj brojeva α i β. Iz dokaza Euklidova algoritma (teorem 3.3.4.) znamo da $\delta \mid \gamma$, odnosno postoji Gaussov cijeli broj ϵ takav da je $\gamma = \delta\epsilon$ što nam implicira da je $\mathcal{N}(\gamma) = \mathcal{N}(\delta)\mathcal{N}(\epsilon)$. Kako je $\mathcal{N}(\gamma) = \mathcal{N}(\delta)$, to nam govori da je $\mathcal{N}(\epsilon) = 1$, odnosno da je $\epsilon = \lambda,\ \lambda \in \{\pm 1, \pm i\}$. □

3.4 Bezoutov teorem

Na početku ovog dijela iskazuje se i dokazuje Bezoutov[2] teorem. Dalje se spominju posljedice ovog teorema i primjena u konkretnim primjerima.

Teorem 3.4.1. ***(Bezoutov teorem)***
Neka je δ najveći zajednički djelitelj brojeva $\alpha,\ \beta \in \mathbb{Z}[i],\ \alpha,\ \beta \neq 0$. Tada postoje $x,\ y \in \mathbb{Z}[i]$ takvi da je $\delta = \alpha x + \beta y$.

Dokaz. Po korolaru 3.3.11. bez smanjenja općenitosti možemo pretpostaviti da je δ dobiven Euklidovim algoritmom. Pogledajmo teorem 3.3.4. (Euklidov algoritam). Iz jednakosti (1) slijedi da je:

$$\delta_1 = \alpha - \beta\gamma_1.$$

Ovu jednakost uvrstimo u (2) i dobivamo:

$$\delta_2 = \beta - (\alpha - \beta\gamma_1)\gamma_2 = \beta(1 + \gamma_1\gamma_2) - \alpha\gamma_2.$$

Uočimo da smo ostatak δ_1 i ostatak δ_2 prikazali kao linearnu kombinaciju brojeva α i β. Postupak možemo analogno provesti dalje i dobivamo da je svaki δ_k linearna kombinacija brojeva α i β. Posebno, najveći zajednički djelitelj brojeva α i β je linearna kombinacija od α i β. □

Korolar 3.4.2. *Neka su $\alpha,\ \beta \in \mathbb{Z}[i],\ \alpha,\ \beta \neq 0$. α i β su relativno prosti akko je*

$$\alpha x + \beta y = 1,$$

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

Dokaz. Neka su α i $\beta \in \mathbb{Z}[i]$ relativno prosti. Tada prema Bezoutovom teoremu slijedi da postoje $x,\ y \in \mathbb{Z}[i]$ takvi da je $\alpha x + \beta y = 1$.
Obratno, ako je $\alpha x + \beta y = 1,\ x,\ y \in \mathbb{Z}[i]$, tada bilo koji zajednički djelitelj od α i β dijeli 1. Jedini elementi koji dijele 1 su invertibilni elementi pa nam iz toga slijedi da su brojevi α i β relativno prosti. □

[2]Etienne Bezout (1730-1783.) - francuski matematičar

Primjer 3.4.3. *U odjeljku Euklidov algoritam (primjer 3.3.6.) pokazali smo da je najveći zajednički djelitelj Gaussovih cijelih brojeva $\alpha = 11 + 3i$ i $\beta = 1 + 8i$ jednak $-1 + 2i$. Sada želimo prikazati $-1+2i$ kao linearnu kombinaciju brojeva α i β. Koristeći raspis Euklidova algoritma iz primjera 3.3.6., imamo*

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

Primjer 3.4.4. *U odjeljku Euklidov algoritam (primjer 3.3.5.) pokazali smo da je najveći zajednički djelitelj Gaussovih cijelih brojeva $\alpha = 32 + 9i$ i $\beta = 4 + 11i$ jednak $-i$. Sada želimo prikazati $-i$ kao linearnu kombinaciju brojeva α i β. Koristeći raspis Euklidova algoritma iz primjera 3.3.5., imamo*

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

Dobili smo da je

$$-i = \alpha(3i) - \beta(7 + 5i).$$

Ako taj izraz pomnožimo s i dobit ćemo

$$1 = \alpha(-3) + \beta(5 - 7i).$$

Primjer 3.4.5. *Neka je $\alpha = 4 + 5i$ i $\beta = 4 - 5i$. Prikažimo najveći zajednički djelitelj brojeva α i β kao njihovu linearnu kombinaciju.*
Prvo ćemo pomoću Euklidovog algoritma odrediti najveći zajednički djelitelj.

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

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

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

Iz Euklidovog algoritma možemo vidjeti da je najveći zajednički djelitelj brojeva α *i* β *jednak* $-i$. *Uočavamo da su brojevi* α *i* β *relativno prosti. Sada prikazujemo* $-i$ *kao linearnu kombinaciju brojeva* α *i* β.

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

Množenjem izraza s i dobivamo:

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

to jest

$$1 = 4\alpha + (1 - 4i)\beta.$$

Napomena 3.4.6. *Uočimo da je u posljednjem primjeru* $\mathcal{N}(\alpha) = \mathcal{N}(\beta) = 41$ *i norme nisu relativno proste u* $\mathbb{Z}$, *dok su Gaussovi cijeli brojevi* α *i* β *relativno prosti u* $\mathbb{Z}[i]$.

Korolar 3.4.7. *Neka su* $\alpha,\ \beta,\ \gamma \in \mathbb{Z}[i]$ *i neka su* α *i* β *relativno prosti.*
Ako $\alpha \mid \beta\gamma$, *onda* $\alpha \mid \gamma$.

Dokaz. Neka $\alpha \mid \beta\gamma$. Tada postoji Gaussov cijeli broj δ takav da je $\beta\gamma = \alpha\delta$. Prema pretpostavci su α i β relativno prosti. Prema Bezoutovom teoremu slijedi da postoje $x,\ y \in \mathbb{Z}[i]$ takvi da je

$$\alpha x + \beta y = 1.$$

Množenjem ove jednakosti s γ dobivamo:

$$\alpha\gamma x + \beta\gamma y = \gamma.$$

Kako je

$$\beta\gamma = \alpha\delta,$$

slijedi da je

$$\alpha\gamma x + \alpha\delta y = \gamma,$$

odnosno

$$\alpha(\gamma x + \delta y) = \gamma.$$

Sada lako uočavamo da $\alpha \mid \gamma$, a to smo trebali pokazati. □

Korolar 3.4.8. *Neka su* $\alpha, \beta \in \mathbb{Z}[i]$, α *i* β *relativno prosti.*
Ako $\alpha \mid \gamma$ *i* $\beta \mid \gamma$ *u* $\mathbb{Z}[i]$, *onda i* $\alpha\beta \mid \gamma$.

Dokaz. Znamo da $\alpha \mid \gamma$ pa postoji $\delta_1 \in \mathbb{Z}[i]$ tako da je $\gamma = \alpha\delta_1$. Isto tako $\beta \mid \gamma$ pa postoji $\delta_2 \in \mathbb{Z}[i]$ tako da je $\gamma = \beta\delta_2$. Kako su α i β relativno prosti, postoje $x,\ y \in \mathbb{Z}[i]$ takvi da je

$$\alpha x + \beta y = 1.$$

Množenjem ove jednakosti s γ dobivamo

$$\alpha\gamma x + \beta\gamma y = \gamma,$$

pa imamo

$$\alpha\beta\delta_2 x + \beta\alpha\delta_1 y = \gamma,$$

odnosno

$$\alpha\beta(\delta_2 x + \delta_1 y) = \gamma.$$

Iz ovoga slijedi da $\alpha\beta \mid \gamma$, a to smo trebali pokazati. □

Korolar 3.4.9. *Neka su* $\alpha,\ \beta,\ \gamma \in \mathbb{Z}[i]$, $\alpha,\ \beta,\ \gamma \neq 0$. *Ako su* α *i* γ *relativno prosti te* β *i* γ *relativno prosti, onda su i* $\alpha\beta$ *i* γ *relativno prosti.*

Dokaz. Kako su α i γ relativno prosti, prema Bezoutovom teoremu slijedi da postoje Gaussovi cijeli brojevi x_1 i y_1 takvi da je

$$\alpha x_1 + \gamma y_1 = 1.$$

Analogno, za relativno proste Gaussove cijele brojeve β i γ postoje x_2 i $y_2 \in \mathbb{Z}[i]$ takvi da je

$$\beta x_2 + \gamma y_2 = 1.$$

Međusobno pomnožimo ove dvije jednakosti:

$$\alpha\beta x_1 x_2 + \alpha\gamma x_1 y_2 + \gamma\beta y_1 x_2 + \gamma^2 y_1 y_2 = 1.$$

Sređivanjem izraza dobivamo

$$\alpha\beta(x_1 x_2) + \gamma(\alpha x_1 y_2 + \beta y_1 x_2 + \gamma y_1 y_2) = 1.$$

Konačno, po korolaru 3.4.2. zaključujemo da su $\alpha\beta$ i γ relativno prosti. □

Poglavlje 4

Faktorizacija

4.1 Prosti Gaussovi cijeli brojevi

U ovome odjeljku definirat ćemo proste i složene Gaussove cijele brojeve. To će nam ujedno biti uvodni dio za sljedeći odjeljak - jedinstvenost faktorizacije.

Lema 4.1.1. *Neka je* $\alpha \in \mathbb{Z}[i],\ \alpha \neq 0$. *Bilo koji djelitelj od* α, *čija je norma* 1 *ili* $\mathcal{N}(\alpha)$, *je invertibilni element ili invertibilni element pomnožen s* α.

Dokaz. Neka je β bilo koji djelitelj od α. Ako $\beta \mid \alpha$, onda $\mathcal{N}(\beta) \mid \mathcal{N}(\alpha)$. U slučaju da je $\mathcal{N}(\beta) = 1$, tada je $\beta = \pm 1$ ili $\beta = \pm i$. Ako $\beta \mid \alpha$ i $\mathcal{N}(\alpha) = \mathcal{N}(\beta)$, onda je $\alpha = \beta\gamma$, za neki $\gamma \in \mathbb{Z}[i]$. Tada je $\mathcal{N}(\alpha) = \mathcal{N}(\beta)\mathcal{N}(\gamma)$, iz čega slijedi da je $\mathcal{N}(\gamma) = 1$. Sada možemo zaključiti da je $\gamma = \pm 1$ ili $\gamma = \pm i$, a tada je $\beta = \pm\alpha$ ili $\beta = \pm i\alpha$. □

Uočimo da lema 4.1.1. ne govori da su jedini Gaussovi cijeli brojevi čija je norma $\mathcal{N}(\alpha)$, $\pm\ \alpha$ i $\pm\ i\alpha$. Primjera radi, pogledajmo Gaussove cijele brojeve $\alpha = 1 + 7i$ i $\beta = 5 + 5i$. Oba ta broja imaju normu 50 i nijedan ne možemo dobiti od drugoga množenjem s nekim invertibilnim elementom. Ono što nam lema 4.1.1. govori je da su jedini Gaussovi cijeli brojevi koji dijele $\alpha \in \mathbb{Z}[i]$ i čija je norma jednaka $\mathcal{N}(\alpha)$, $\pm\alpha$ i $\pm\ i\alpha$.
Ako je $\mathcal{N}(\alpha) > 1$, tada uvijek ima barem osam djelitelja od α. To su: ± 1, $\pm i$, $\pm\alpha$ i $\pm i\alpha$. Te djelitelje zovemo *trivijalni djelitelji* ili *trivijalni faktori*. Možemo uočiti da su ti trivijalni faktori analogoni trivijalnim faktorima u prstenu $\mathbb{Z} : \pm 1$ i $\pm\ n$, gdje je n cijeli broj takav da je $|n| > 1$. Faktore koji nisu trivijalni zvat ćemo *netrivijalnim faktorima.* Po lemi 4.1.1. vrijedi da je njihova norma strogo između 1 i $\mathcal{N}(\alpha)$.

Definicija 4.1.2. *Neka je $\alpha \in \mathbb{Z}[i]$ i $\mathcal{N}(\alpha) > 1$. Broj α zovemo složenim Gaussovim cijelim brojem ako ima barem jedan netrivijalan fakor. Ako ima samo trivijalne faktore, tada kažemo da je α prost Gaussov cijeli broj.*

Primijetimo da su prosti Gaussovi cijeli brojevi točno ireducibilni elementi u prstenu $\mathbb{Z}[i]$ (vidi definiciju 1.0.6.). Štoviše, u Korolaru 4.2.4. dokazat ćemo da je $\mathbb{Z}[i]$ faktorijalan prsten pa su po propoziciji 1.0.10., kao što naziv sugerira, prosti Gaussovi cijeli brojevi točno prosti elementi u prstenu $\mathbb{Z}[i]$.

Napomena 4.1.3. *Za $\alpha = \beta\gamma$, uvjet $1 < \mathcal{N}(\beta) < \mathcal{N}(\alpha)$ je ekvivalentan uvjetu $\mathcal{N}(\beta) > 1$ i $\mathcal{N}(\gamma) > 1$. Prikaz Gaussovog cijelog broja α u obliku produkta Gaussovih cijelih brojeva čija je norma strogo veća od 1, zovemo netrivijalna faktorizacija od α.*

Pogledajmo neke primjere trivijalnih i netrivijalnih faktorizacija Gaussovih cijelih brojeva.

Primjer 4.1.4. *Pogledajmo Gaussov cijeli broj $\alpha = 13 - i$. Njegova netrivijalna faktorizacija bila bi $(1 - 4i)(1 + 3i)$, dok bi trivijalna faktorizacija glasila $-1(i - 13)$.*

Primjer 4.1.5. *Pogledajmo broj 5. Jedna njegova netrivijalna faktorizacija glasi $(1 - 2i)(1 + 2i)$. Ovdje imamo zanimljivu činjenicu. Znamo da je broj 5 prost broj u prstenu $\mathbb{Z}$, dok je u prstenu $\mathbb{Z}[i]$ broj 5 složen broj. Isto tako je i broj 2 složen u $\mathbb{Z}[i]$ jer je $2 = (1 + i)(1 - i)$.*

Primjer 4.1.6. *Pogledajmo broj 3. Znamo da je 3 prost broj u $\mathbb{Z}$, ali je prost broj i u $\mathbb{Z}[i]$. Kako bismo se u to uvjerili, pretpostavimo suprotno, tj. da je 3 složen broj, i neka je njegova netrivijalna faktorizacija $3 = \alpha\beta$. Uzmimo normu obje strane i dobivamo $9 = \mathcal{N}(\alpha)\mathcal{N}(\beta)$. Kako je riječ o netrivijalnoj faktorizaciji, znamo da vrijedi $\mathcal{N}(\alpha),\ \mathcal{N}(\beta) > 1$. Slijedi da je $\mathcal{N}(\alpha) = 3$ tj. za $\alpha = a + bi \in \mathbb{Z}[i]$ vrijedi $a^2 + b^2 = 3$. Ovdje dolazimo do kontradikcije zato što ne postoje takvi $a,\ b \in \mathbb{Z}$. Dakle, broj 3 ima samo trivijalne faktore u $\mathbb{Z}[i]$ pa je zato prost Gaussov cijeli broj.*

Teorem 4.1.7. *Ako je norma Gaussovog cijelog broja prost broj u $\mathbb{Z}$, tada je taj Gaussov cijeli broj prost u $\mathbb{Z}[i]$.*

Dokaz. Neka je norma Gaussovog cijelog broja α prost broj. Označimo ju sa $p = \mathcal{N}(\alpha)$. Trebamo pokazati da α ima jedino trivijalne faktore, tj. da faktori imaju normu 1 ili $\mathcal{N}(\alpha)$. Neka je $\alpha = \beta\gamma$ bilo koja faktorizacija od α u $\mathbb{Z}[i]$. Uzmemo norme sa obje strane i dobivamo da je $\mathcal{N}(\alpha) = p = \mathcal{N}(\beta)\mathcal{N}(\gamma)$. Kako je p norma, ona mora biti pozitivna pa je zato

$p \in \mathbb{Z}^+$. Iz ovoga slijedi da mora biti $\mathcal{N}(\beta) = 1$ ili $\mathcal{N}(\gamma) = 1$. Tako je ili β ili γ invertibilan element, pa slijedi da α nema netrivijalnih faktora. Zaključujemo da je α prost broj u $\mathbb{Z}[i]$. □

Napomena 4.1.8. *Uočimo da obrat teorema 4.1.7. ne vrijedi, odnosno, prost Gaussov cijeli broj ne mora imati normu koja je također prost broj. Kao kontraprimjer uzmemo broj 3. U primjeru 4.1.6. pokazali smo da je 3 prost broj u $\mathbb{Z}[i]$, međutim njegova norma je 9, a znamo da 9 nije prost broj u $\mathbb{Z}$.*

Teorem 4.1.9. *Svaki $\alpha \in \mathbb{Z}[i]$ s normom strogo većom od 1 produkt je prostih Gaussovih cijelih brojeva.*

Dokaz. Neka je $\alpha \in \mathbb{Z}[i]$ i $\mathcal{N}(\alpha) > 1$. Dokaz provodimo metodom matematičke indukcije po $\mathcal{N}(\alpha)$. Pretpostavimo da je $\mathcal{N}(\alpha) = 2$. Drugačije rečeno, tada je $\alpha = 1 \pm i$ ili $\alpha = -1 \pm i$. Prema teoremu 4.1.7. slijedi da je α prost Gaussov cijeli broj. Pretpostavimo sada da je $n \geq 3$ te da je svaki Gaussov cijeli broj α, norme veće ili jednake 3 i strogo manje od n, produkt prostih Gaussovih cijelih brojeva. Želimo pokazati da je svaki $\alpha \in \mathbb{Z}[i]$ norme n produkt prostih Gaussovih cijelih brojeva. Najprije uočimo, ako ne postoji $\alpha \in \mathbb{Z}[i]$ takav da je $\mathcal{N}(\alpha) = n$, tada nemamo što dokazati. Zato pretpostavimo da postoji $\alpha \in \mathbb{Z}[i]$, $\mathcal{N}(\alpha) = n$, gdje je α složen Gaussov cijeli broj, i neka je $\alpha = \beta\gamma$ netrivijalna faktorizacija od α. Vrijedi da su $\mathcal{N}(\beta)$, $\mathcal{N}(\gamma) < \mathcal{N}(\alpha) = n$. Prema pretpostavci indukcije, β i γ su produkti prostih Gaussovih cijelih brojeva. Zaključno, njihov produkt α je produkt prostih brojeva u $\mathbb{Z}[i]$. □

4.2 Jedinstvenost faktorizacije

Prije samog iskaza i dokaza teorema o jedinstvenosti faktorizacije Gaussovih cijelih brojeva, dokazujemo lemu koja će nam pomoći u njegovu dokazivanju.

Lema 4.2.1. *Neka je p prost Gaussov cijeli broj i neka su α_1, ..., $\alpha_k \in \mathbb{Z}[i]$. Ako $p \mid \alpha_1 \cdots \alpha_k$, tada $p \mid \alpha_i$ za neki $i \in \{1, \ldots, k\}$.*

Dokaz. Dokaz provodimo metodom matematičke indukcije po k. Za $k = 2$, neka $p \mid \alpha_1\alpha_2$. Pretpostavimo da p ne dijeli α_1. To znači da su p i α_1 relativno prosti pa prema korolaru 3.4.7 slijedi da $p \mid \alpha_2$. Pretpostavimo sad da tvrdnja leme vrijedi za neki $k \in \mathbb{N}$. Trebamo pokazati da, ako vrijedi da

$$p \mid \alpha_1 \cdots \alpha_{k+1},$$

onda $p \mid \alpha_i$ za neki $i \in \{1, \ldots, k+1\}$. Označimo $\beta = \alpha_1 \cdots \alpha_k$, tada

$$p \mid \beta\alpha_{k+1}.$$

Ako $p \nmid \beta$, onda slijedi da su oni relativno prosti pa mora $p \mid \alpha_{k+1}$. U suprotnome, $p \mid \beta$ pa po pretpostavci indukcije slijedi da $p \mid \alpha_i$ za neki $i \in \{1, \ldots, k\}$. □

Primjer 4.2.2. *Primijetimo da je*

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

Uočimo da su svi faktori na desnoj strani prosti u $\mathbb{Z}[i]$ zato što su njihove norme proste u $\mathbb{Z}$. Isto tako uočavamo da ove dvije faktorizacije nisu jednake, ali ako dopustimo množenje s jedinicom, lako vidimo da vrijedi:

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

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

Ovaj primjer nam objašnjava ulogu invertibilnih elemenata kod množenja faktora u jedinstvenoj faktorizaciji.

Teorem 4.2.3. *(Jedinstvenost prikaza Gaussovih cijelih brojeva u obliku produkta prostih Gaussovih cijelih brojeva)*
Neka je $\alpha \in \mathbb{Z}[i], \mathcal{N}(\alpha) > 1$. Ako je

$$\alpha = \alpha_1 \cdots \alpha_r = \alpha'_1 \cdots \alpha'_s,$$

gdje su $\alpha_j,\ j \in \{1, ..., r\}$ i $\alpha'_k,\ k \in \{1, ..., s\}$ prosti Gaussovi cijeli brojevi, tada je $r = s$ te postoji permutacija $\sigma \in S_r$ i elementi $\lambda_1, \ldots, \lambda_r \in \{\pm 1, \pm i\}$ takvi da je $\alpha_j = \lambda_j \alpha'_{\sigma(j)}$.

Dokaz. Pokazali smo da se svaki Gaussov cijeli broj može prikazati kao produkt prostih Gaussovih cijelih brojeva. Ako je α prost Gaussov cijeli broj, tada je tvrdnja teorema očita. Zato pretpostavljamo da je α složen Gaussov cijeli broj. Dokaz radimo metodom matematičke indukcije po $\mathcal{N}(\alpha)$. Za bazu indukcije uzimamo slučaj $\mathcal{N}(\alpha) = 2$. Ovaj slučaj smo već razmatrali u dokazu teorema 4.1.9. i vidjeli da ne postoje složeni Gaussovi cijeli brojevi α norme 2, pa je tvrdnja trivijalno zadovoljena. Neka je $n \in \mathbb{N},\ n \geq 3$, i pretpostavimo da za svaki $\alpha \in \mathbb{Z}[i],\ 1 < \mathcal{N}(\alpha) < n$, vrijedi dana tvrdnja. Želimo pokazati da $\alpha \in \mathbb{Z}[i],\ \mathcal{N}(\alpha) = n$ ima jedinstvenu faktorizaciju. Pretpostavimo da postoje dvije faktorizacije od α, tj.

$$\alpha = \alpha_1 \cdots \alpha_r = \alpha'_1 \cdots \alpha'_s.$$

Kako $\alpha_1 \mid \alpha$, slijedi da $\alpha_1 \mid \alpha'_1 \cdots \alpha'_s$. Prema lemi 4.2.1. slijedi da $\alpha_1 \mid \alpha'_j$ za neki $j = 1, ..., s$. Bez smanjenja općenitosti možemo pretpostaviti da je $j = 1$, tj. da $\alpha_1 \mid \alpha'_1$. Kako su α_1 i α'_1 prosti, vrijedi da nemaju netrivijalnih faktora. Slijedi da je $\alpha_1 = \lambda_1 \alpha'_1$, za neki $\lambda_1 \in \{\pm 1, \pm i\}$. Sada faktorizaciju broja α možemo zapisati kao

$$\alpha = \lambda_1 \alpha'_1 \alpha_2 \cdots \alpha_r = \alpha'_1 \cdots \alpha'_s.$$

Dijeljenjem izraza s α'_1 dobivamo:

$$\frac{\alpha}{\alpha'_1} = \beta = \lambda_1\alpha_2 \cdots \alpha_r = \alpha'_2 \cdots \alpha'_s.$$

Očito je da je $\mathcal{N}(\beta) = \frac{\mathcal{N}(\alpha)}{\mathcal{N}(\alpha'_1)} < \mathcal{N}(\alpha)$. Kako je λ_1 jedinica, slijedi da je $\lambda_1\alpha_2$ prost Gaussov cijeli broj. Sada imamo dvije faktorizacije broja β sa $r-1$ i $s-1$ prostih faktora. Kako je $\mathcal{N}(\beta) < n$, prema pretpostavci slijedi da je $r-1 = s-1$ iz čega slijedi da je $r = s$. Drugi dio pretpostavke povlači da postoji permutacija $\sigma \in S_r$ i elementi $\lambda_2, \ldots, \lambda_r \in \{\pm 1, \pm i\}$ takvi da je $\sigma(1) = 1$ i $\alpha_j = \lambda_j\alpha'_{\sigma(j)}$ za sve $j \in \{1, \ldots, r\}$. □

Uočimo da nam prethodni teorem govori da je faktorizacija Gaussovog cijelog broja, čija je norma strogo veća od 1, jedinstvena do na poredak i množenje invertibilnim elementima (jedinicama). Iz teorema 4.1.9. i 4.2.3. lako slijedi (vidi definiciju 1.0.9.):

Korolar 4.2.4. *Prsten $\mathbb{Z}[i]$ je faktorijalan prsten.*

Primjer 4.2.5. *Prikažimo Gaussov cijeli broj $\alpha = 7+11i$ kao produkt prostih faktora. Prvo trebamo odrediti normu. Vrijedi da je $\mathcal{N}(\alpha) = 7^2 + 11^2 = 170$. Dalje ćemo faktorizirati broj 170 u skupu prirodnih brojeva. Imamo:*

$$170 = 2 \cdot 5 \cdot 17.$$

Sada želimo pronaći Gaussove cijele brojeve koji imaju norme 2, 5 i 17. Vrijedi da je:

$$\mathcal{N}(1+i) = 2 = \mathcal{N}(1-i),$$

$$\mathcal{N}(1+2i) = 5 = \mathcal{N}(1-2i),$$

$$\mathcal{N}(4+i) = 17 = \mathcal{N}(4-i).$$

Lako se vidi da ovi Gaussovi cijeli brojevi pomnoženi jedinicama u $\mathbb{Z}[i]$ daju sve Gaussove cijele brojeve norme 2, 5 i 17.
Prema teoremu 4.1.7. slijedi da su ti Gaussovi cijeli brojevi prosti jer su njihove norme prosti brojevi u $\mathbb{Z}$. Izaberemo po jedan faktor norme 2, 5 odnosno 17 i pomnožimo ih. Jedna od konačno mnogo mogućih kombinacija dat će jedinstveni rastav zadanog broja na proste faktore.
U ovom primjeru faktori $(1-i)(1-2i)(4-i) = -7-11i$ daju $-\alpha$ pa zato jedinstveni rastav na proste fakore glasi:

$$7 + 11i = -(1-i)(1-2i)(4-i).$$

Poglavlje 5

Primjena $\mathbb{Z}[i]$ na aritmetiku u $\mathbb{Z}$

U ovom, posljednjem poglavlju navest ćemo neke od primjena $\mathbb{Z}[i]$ na aritmetiku u $\mathbb{Z}$. Promatrat ćemo proste brojeve u $\mathbb{Z}$ te iskoristiti Gaussove cijele brojeve za dokazivanje tvrdnje da se prost broj u $\mathbb{Z}$ može zapisati kao suma dvaju kvadrata najviše na jedan način. Govorit će se i o primjeni $\mathbb{Z}[i]$ na klasifikaciju primitivnih Pitagorinih[1] trojki te na određivanje cjelobrojnih rješenja jednadžbi $a^2 + b^2 = c^3$ i $y^2 + 1 = x^3$.

5.1 Prosti brojevi

Na početku ovog odjeljka navodimo Wilsonov teorem koji ćemo koristiti u dokazivanju tvrdnji.

Teorem 5.1.1. *Ako je p prost broj, onda je* $(p-1)! \equiv -1 \pmod{p}$.

Dokaz. Dokaz Wilsonovog teorema možete pogledati u [2] ili [4]. □

Lema 5.1.2. *Neka je* $p = 4n+1$, $n \in \mathbb{N}$ *prost broj. Tada* $p \mid m^2 + 1$ *za neki* $m \in \mathbb{Z}$.

Dokaz. Primijenimo Wilsonov teorem na prost broj $p = 4n+1$ te dobivamo

$$\begin{aligned}
-1 &\equiv 1 \cdot 2 \cdot 3 \cdots 4n \pmod{\text{p}} \\
&\equiv (1 \cdot 2 \cdots 2n) \cdot ((2n+1) \cdots (4n-1) \cdot (4n)) \pmod{\text{p}} \\
&\equiv (1 \cdot 2 \cdots 2n) \cdot ((-2n) \cdots (-2)(-1)) \pmod{\text{p}} \text{ jer je } p - k \equiv -k \pmod{\text{p}} \\
&= (1 \cdot 2 \cdots 2n)^2 (-1)^{2n} \pmod{\text{p}} \\
&= (1 \cdot 2 \cdots 2n)^2 \pmod{\text{p}}.
\end{aligned}$$

Stavimo da je $m = (2n)!$ pa imamo da je $m^2 \equiv -1 \pmod{\text{p}}$. Time smo dobili da $p \mid m^2+1$. □

[1] Pitagora (6. - 5. st. pr. Kr.) - starogrčki matematičar; prvi "pravi" matematičar

Propozicija 5.1.3. *Neka je p prost broj koji se može zapisati u obliku sume dvaju kvadrata, tj. $p = a^2 + b^2,\ a,\ b \in \mathbb{Z}$. Tada su a i b jedinstveni do na predznak i poredak.*

Dokaz. Neka je zadan prost broj p, $p = a^2 + b^2,\ a,\ b \in \mathbb{Z}$. Broj p možemo faktorizirati u prstenu $\mathbb{Z}[i]$ kao

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

gdje su faktori $a \pm bi$ prosti Gaussovi cijeli brojevi (vidi teorem 4.1.9.).
Pretpostavimo da postoji još jedan zapis broja p kao sume dvaju kvadrata.
Neka su $c,\ d \in \mathbb{Z}[i]$. Tada je

$$p = (c + di)(c - di),$$

gdje su $c \pm di$ prosti Gaussovi cijeli brojevi.
Prema teoremu o jedinstvenoj faktorizaciji u prstenu $\mathbb{Z}[i]$ (teorem 4.2.3.) slijedi da je

$$a + bi = \lambda(c + di) \text{ ili } a + bi = \lambda(c - di),$$

za neki $\lambda \in \{\pm 1, \pm i\}$. Dovoljno nam je promatrati samo jedan od ova dva slučaja zato što je razlika u predznaku, a nama je cilj pokazati da se brojevi a i b podudaraju s brojevima c i d do na predznak i poredak.
Dalje promatramo slučaj kada je

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

Za $\lambda = 1$ slijedi da je $c = a$ i $d = b$. Za $\lambda = -1$ slijedi da je $c = -a$ i $d = -b$. Ako je $\lambda = i$, tada je $c = b$ i $d = -a$. Ako je $\lambda = -i$, tada je $c = -b$ i $d = a$.
Ovime smo pokazali da su brojevi c i d jednaki brojevima a i b do na predznak i poredak. □

Primjer 5.1.4. *Pogledajmo neke proste brojeve kao sume dvaju kvadrata:*

$$2 = 1^2 + 1^2,\ \ 5 = 1^2 + 2^2,\ \ 13 = 2^2 + 3^2,\ \ 17 = 1^2 + 4^2$$

Sada navodimo propoziciju koju ćemo koristiti u dokazu Fermatovog teorema o dva kvadrata, a dokaz propozicije nalazi se u [6, Poglavlje 6.3]

Propozicija 5.1.5. *Neka je p prost broj u $\mathbb{Z}$. Tada je p prost Gaussov cijeli broj ako i samo ako p nije suma dvaju kvadrata.*

Teorem 5.1.6. ***(Fermatov teorem o dva kvadrata)***
Svaki prost broj oblika $p = 4n + 1$ može se prikazati u obliku sume dvaju kvadrata, tj. $p = a^2 + b^2,\ a,\ b \in \mathbb{Z}[i]$.

Dokaz. Neka je zadan prost broj p oblika $p = 4n + 1$, i neka je $m \in \mathbb{Z}$ takav da $p \mid m^2 + 1$ (kao što je bio slučaj u prethodnoj lemi). Pogledajmo broj $m^2 + 1$. Njegova faktorizacija u prstenu $\mathbb{Z}[i]$ glasi

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

$p \mid m^2 + 1$, ali $p \nmid m - i$ i $p \nmid m + i$ zato što $\frac{m}{p} - \frac{i}{p}$ i $\frac{m}{p} + \frac{i}{p}$ nisu Gaussovi cijeli brojevi. Prema lemi 4.2.1. slijedi da p nije prost Gaussov cijeli broj. Sad prethodna lema povlači tvrdnju. □

Nadalje, uz oznake i pretpostavke teorema 5.1.6., slijedi da je

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

faktorizacija u produkt prostih Gaussovih cijelih brojeva, a već smo dokazali da je ona jedinstvena do na poredak i množenje invertibilnim elementima. Slijedi iskaz snažnije tvrdnje Fermatovog teorema o dva kvadrata:
Svaki prost broj oblika $p = 4n + 1$ je suma dvaju kvadrata, tj. $p = a^2 + b^2$, gdje su a i b jedinstveni par prirodnih brojeva.

Primjer 5.1.7. *Pogledajmo peti Fermatov broj $2^{2^5} + 1$. Taj broj je suma dvaju kvadrata*

$$2^{2^5} + 1 = (2^{16})^2 + 1.$$

Fermat je pretpostavljao da je taj broj prost broj, a Euler ga je zapisao na drugi način kao sumu dvaju kvadrata:

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

Prema propoziciji 5.1.3. možemo zaključiti kako peti Fermatov broj nije prost broj.

Dalje navodimo korolar koji će nam biti od koristi u daljnjem dokazivanju tvrdnji za proste brojeve oblika $p = 4n + 1$.

Korolar 5.1.8. *Ako je p prost broj u $\mathbb{Z}^+$ koji zadovoljava izraz $p \equiv 3 \pmod 4$, tada se p ne može prikazati u obliku sume dvaju kvadrata u $\mathbb{Z}$ te ostaje prost u $\mathbb{Z}[i]$.*

Dokaz. Pretpostavimo suprotno, da se neki prost broj $p \equiv 3 \pmod 4$ može zapisati u obliku $p = a^2 + b^2$ za neke $a, b \in \mathbb{Z}$. Kako je p neparan, slijedi da je točno jedan od brojeva a i b neparan; bez smanjenja općenitosti pretpostavimo da je a neparan, dakle $a = 2m + 1$ za neki $m \in \mathbb{Z}$, dok je b paran, dakle $b = 2n$ za neki $n \in \mathbb{Z}$. Sad imamo

$$p = a^2+b^2 = (2m+1)^2+(2n)^2 = 4m^2+4m+1+4n^2 = 4(m^2+m+n^2)+1 \equiv 1 \not\equiv 3 \pmod 4$$

Došli smo do kontradikcije. Dakle, za p prost broj u $\mathbb{Z}^+$, $p \equiv 3 \pmod 4$ vrijedi da se p ne može prikazati u obliku sume dvaju kvadrata u $\mathbb{Z}$. □

Teorem 5.1.9. *Kongruencija $x^2 \equiv -1 \pmod p$, gdje je p neparan prost broj, ima rješenje ako i samo ako je p oblika $p = 4n + 1$.*

Dokaz. Lema 5.1.2. za $p = 4n + 1$ daje x takav da je $x^2 \equiv -1 \pmod p$. Želimo pokazati da dana kongruencija nema rješenja kad je p oblika $p = 4n + 3$. Da bismo to dokazali, pretpostavimo suprotno. Ako je

$$x^2 \equiv -1 \pmod{p = 4n + 3},$$

tada potenciranjem obiju strana s $2n + 1$ dobivamo:

$$(x^2)^{2n+1} \equiv (-1)^{2n+1} \equiv -1 \pmod{p = 4n + 3}.$$

Dalje uočimo da je $2(2n + 1) = 4n + 2 = (4n + 1) + 1 = p - 1$. Iz toga slijedi:

$$x^{p-1} \equiv -1 \pmod p.$$

Sada smo došli do kontradikcije s Fermatovim malim teoremom: *Neka je $a \in \mathbb{Z}$ i p prost broj, $p \nmid a$. Tada je $a^{p-1} \equiv 1 \pmod p$.* Dokaz ovog teorema može se pogledati u [2].
Konačno, $x^2 \equiv -1 \pmod p$ nema rješenja za $p = 4n + 3$ pa iz toga slijedi da je p prost broj oblika $p = 4n + 1$. □

Za kraj pokazat ćemo da ima beskonačno mnogo prostih brojeva oblika $4n + 1$.

Teorem 5.1.10. *Prostih brojeva p oblika $p = 4n + 1$ ima beskonačno mnogo.*

Dokaz. Zbog prethodnog teorema, dovoljno je pokazati da postoji beskonačno mnogo prostih brojeva koji dijele vrijednosti izraza $x^2 + 1$, $x \in \mathbb{Z}$. Pretpostavimo suprotno, tj. da postoji konačno mnogo prostih brojeva koji dijele te vrijednosti i označimo ih s $p_1, p_2, ..., p_k$.
Promatramo polinom

$$g(y) = (p_1 p_2 \cdots p_k y)^2 + 1.$$

Svaki prost broj koji dijeli vrijednost polinoma $g(y),\ y \in \mathbb{Z}$, dijelit će i vrijednost od $x^2 + 1$, jer je $x = p_1 p_2 \cdots p_k y$. Uočimo da niti jedan od $p_1, p_2, ..., p_k$ ne dijeli $g(y)$ jer uvijek ostaje ostatak 1. Zaključujemo da nema prostog broja koji dijeli $g(y),\ y \in \mathbb{Z}$ pa su jedine mogućnosti za $g(y)$ ± 1, tj.

$$(p_1 p_2 \cdots p_k y)^2 + 1 = \pm 1,\ \forall y \in \mathbb{Z}.$$

Sada smo došli do kontradikcije jer svaka od ovih kvadratnih jednadžbi ima najviše dva rješenja y. Zaključno, $x^2 + 1$ je djeljiv sa beskonačno mnogo prostih brojeva, odnosno, postoji beskonačno mnogo prostih brojeva oblika $p = 4n + 1$. □

5.2 Primitivne Pitagorine trojke

U ovom odjeljku definirat ćemo pojam (primitivnih) Pitagorinih trojki te ih klasificirati uz pomoć Gaussovih cijelih brojeva.

Definicija 5.2.1. *Uređenu trojku prirodnih brojeva (x, y, z) zovemo Pitagorina trojka ako su x i y katete, a z hipotenuza nekog pravokutnog trokuta, odnosno 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. Takav trokut zovemo (primitivni) Pitagorin trokut.

Napomena 5.2.2. *Uočimo da je u primitivnoj Pitagorinoj trojki točno jedan od brojeva x, y paran i točno jedan neparan. Ako bi oba bila parna, trojka očito ne bi bila primitivna. Ako bi oba bila neparna, a znamo da je kvadrat neparnog broja $\equiv 1$ (mod 4), imali bi $x^2 + y^2 \equiv 2$ (mod 4). Kako je paran kvadrat $\equiv 0$ (mod 4), slijedi da je $z^2 \equiv 0$ (mod 4). Sada smo došli do kontradikcije.*
Dakle, u primitivnoj Pitagorinoj trojki (x, y, z) jedan od x, y je paran, drugi neparan i z je neparan.

Primjer 5.2.3. *Neki primjeri primitivnih Pitagorinih trojki su:*

$$(3, 4, 5),\ (5, 12, 13),\ (9, 40, 41),\ (20, 21, 29),\ (65, 72, 97)$$

Ako imamo

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

tada možemo pisati

$$(x - yi)(x + yi) = z^2.$$

Faktori neparnog kvadrata z^2 su $x - yi$ i $x + yi$, koji su Gaussovi cijeli brojevi.

Sada ćemo iskazati i dokazati tri leme koje će nam trebati u dokazivanju teorema koji ćemo kasnije iskazati.

Lema 5.2.4. *Neka je (x, y, z) primitivna Pitagorina trojka. Tada su $x - yi$ i $x + yi$ relativno prosti u $\mathbb{Z}[i]$.*

Dokaz. Ako je $(x, y) = 1$ u prstenu $\mathbb{Z}$, tada je i $(x, y) = 1$ u prstenu $\mathbb{Z}[i]$. Zajednički djelitelj brojeva $x - yi$ i $x + yi$ dijeli i njihovu sumu $(x - yi) + (x + yi) = 2x$ te njihovu razliku $(x - yi) - (x + yi) = -2yi$. Kako je $(x, y) = 1$, slijedi da su svi zajednički prosti djelitelji brojeva $x - yi$ i $x + yi$ sadržani među prostim Gaussovim cijelim brojevima koji dijele 2 pa su oblika $\pm 1 \pm i$. Imamo faktorizaciju

$$(x - yi)(x + yi) = z^2,$$

gdje je z^2 neparan. Slijedi da niti jedan Gaussov cijeli broj oblika $\pm 1 \pm i$ ne dijeli z^2 pa su stoga $x - yi$ i $x + yi$ relativno prosti. □

Lema 5.2.5. *Neka su $x - yi$ i $x + yi$ relativno prosti Gaussovi cijeli brojevi takvi da vrijedi*

$$(x - yi)(x + yi) = z^2,$$

za neki $z \in \mathbb{Z}[i]$. Tada postoje $\alpha,\ \beta,\ \lambda_1,\ \lambda_2 \in \mathbb{Z}[i],\ \lambda_1,\ \lambda_2$ invertibilni elementi, takvi da je $x - yi = \lambda_1\alpha^2$ i $x + yi = \lambda_2\beta^2$.

Dokaz. Brojevi $x - yi$ i $x + yi$ nemaju zajedničkih prostih faktora, a svaki faktor od z^2 se pojavljuje s parnom potencijom. Slijedi da se svaki prosti faktor od $x - yi$ i $x + yi$ mora također pojavljivati s parnom potencijom. Sada je očito da je produkt prostih brojeva od kojih se svaki pojavljuje s parnom potencijom, kvadrat. Zaključujemo da se svaki od brojeva $x-yi$ i $x+yi$ može prikazati kao produkt invertibilnih elemenata i potpunih kvadrata (preostali mogući faktori koji nisu prosti, mogu biti samo invertibilni elementi) □

Neka je (x, y, z) primitivna Pitagorina trojka. Pokazali smo da je $x-yi$ produkt invertibilnog elementa i kvadrata pa ima jedan od sljedećih prikaza:

$$(a - bi)^2,$$

$$-(a - bi)^2,$$

$$i(a - bi)^2,$$

$$-i(a - bi)^2,$$

gdje su a i $b \in \mathbb{Z}$. Raspisivanjem ovih izraza vidimo da $x - yi$ ima jedan od oblika:

$$(a^2 - b^2) - 2abi,$$

$$(b^2 - a^2) + 2abi,$$

$$2ab + (a^2 - b^2)i,$$

$$-2ab + (b^2 - a^2)i.$$

U svakom od navedenih slučajeva, izjednačavamo realni i imaginarni dio pa dobivamo da je x ili y oblika $u^2 - v^2,\ u > v$, dok je drugi od njih oblika $2uv$, gdje su $u,\ v \in \mathbb{N}$. Također, mora vrijediti da je $(u, v) = 1$ zato što je svaki prosti zajednički djelitelj brojeva u i v zajednički djelitelj od $u^2 - v^2$ i $2uv$ (dakle od x i y) pa su u i v međusobno relativno prosti i različite parnosti. Ako bi bili iste parnosti, onda bi x i y bili parni. Bez smanjenja općenitosti možemo pretpostaviti da je x neparan, a y paran.

Korolar 5.2.6. *Neka je (x,y,z) primitivna Pitagorina trojka u kojoj je x neparan broj. Tada je $x + yi$ potpun kvadrat u $\mathbb{Z}[i]$.*

Dokaz. Prema lemi 5.2.5. znamo da je $x+yi$ jednak produktu nekog invertibilnog elementa i kvadrata. Dakle, $x + yi$ jednak je jednom od ovih izraza:

$$(a + bi)^2,$$

$$-(a + bi)^2,$$

$$i(a + bi)^2,$$

$$-i(a + bi)^2,$$

za neke $a, b \in \mathbb{Z}$.
Raspisivanjem dobivamo:

$$(a^2 - b^2) + 2abi,$$

$$(b^2 - a^2) - 2abi,$$

$$-2ab + (a^2 - b^2)i,$$

$$2ab + (b^2 - a^2)i.$$

Iz pretpostavke znamo da je x neparan što znači da je oblika $u^2 - v^2,\ u > v$. Tada slijedi da je y paran i da je oblika $2uv$. Sada vidimo da je jedino moguće rješenje $x + yi = (a + bi)^2$ ili $x + yi = -(a + bi)^2 = (i(a + bi))^2$ pa je $x + yi$ potpuni kvadrat u prstenu $\mathbb{Z}[i]$. □

Primjer 5.2.7. *Pokažimo da je* $5 + 12i$ *potpuni kvadrat u prstenu* $\mathbb{Z}[i]$.
Rješenje:
Kako je $(5, 12, 13)$ *primitivna Pitagorina trojka, prema prethodnom korolaru znamo da je* $5 + 12i = (a + bi)^2$*, za neke* $a, b \in \mathbb{Z}$*. Slijedi da je* $5 = a^2 - b^2,\ 12 = 2ab$*. Sada imamo:*

$$a^2 - b^2 = 5$$

$$6 = ab.$$

Kvadriramo drugu jednakost i u nju uvrstimo $b^2 = a^2 - 5$ *pa dobivamo:*

$$a^4 - 5a^2 - 36 = 0.$$

Uvođenjem supstitucije $t = a^2$ *izraz pojednostavljujemo na*

$$t^2 - 5t - 36 = 0.$$

Rješenja ove kvadratne jednadžbe su: $t_1 = 9$ *i* $t_2 = -4$*. Kako tražimo cijele brojeve, promatramo samo* t_1*. Vraćanjem u supstituciju dobivamo da je jedno rješenje* $a = 3$ *te* $b = 2$.
Dakle, $5 + 12i = (3 + 2i)^2$.

Teorem 5.2.8. *Ako je* $x^2 + y^2 = z^2$*, za relativno proste prirodne brojeve x i y, tada je jedan od brojeva x ili y oblika* $u^2 - v^2$*, a drugi je oblika* $2uv$*, gdje su u i v relativno prosti prirodni brojevi. U oba slučaja je* $z = u^2 + v^2$ *jer je*

$$(u^2 - v^2)^2 + (2uv)^2 = u^4 + 2u^2v^2 + v^4 = (u^2 + v^2)^2,$$

tj. z je suma dva kvadrata.

Dokaz. Bez smanjenja općenitosti pretpostavimo da je x neparan broj. Tada po korolaru 5.2.6. postoje $u, v \in \mathbb{Z}$ takvi da je $x + yi = (u + vi)^2$, dakle imamo

$$x + yi = u^2 - v^2 + 2uvi,$$

tj.

$$x = u^2 - v^2,\ y = 2uv.$$

Ovo dokazuje tvrdnju. □

Lema 5.2.9. *Jednadžba $x^4+y^4 = z^2$ nema rješenja u skupu prirodnih brojeva, tj. ne postoji pravokutni trokut kojem su duljine kateta kvadrati prirodnih brojeva.*

Dokaz. Pretpostavimo suprotno, tj. da postoji takav trokut i izaberemo među svim takvim trokutima onaj trokut koji ima najmanju hipotenuzu. Sada imamo Pitagorinu trojku (x^2, y^2, z). Prvo pokažemo da su x i y relativno prosti. U protivnom bi bilo $x = a \cdot d$, $y = b \cdot d$, za neki prirodan broj $d > 1$. Tada bi iz $z^2 = d^4(a^4 + b^4)$ slijedilo da postoji neki $c \in \mathbb{N}$ takav da je $z = d^2 \cdot c$ pa bismo dobili Pitagorinu trojku (a^2, b^2, c) s hipotenuzom koja je manja od z, a to bi bila kontradikcija s odabirom z. Dakle, (x^2, y^2, z) je primitivna Pitagorina trojka. Prema teoremu 5.2.8., ako uzmemo da je y paran, postoje relativno prosti prirodni brojevi u i v, različite parnosti, takvi da vrijedi:

$$x^2 = u^2 - v^2,\ y^2 = 2uv,\ z = u^2 + v^2.$$

Iz prve jednakosti slijedi da je $x^2 + v^2 = u^2$ pa je v paran, a u neparan. Dalje stavimo: $v = 2k,\ y = 2l$ pa imamo $l^2 = uk$. Odavde, s obzirom da su u i k relativno prosti, slijedi da postoje prirodni brojevi m i n takvi da je $u = m^2$ i $k = n^2$. Kako je (x, v, u) primitivna Pitagorina trojka, prema teoremu 5.2.8. slijedi da postoje e i f, $(e, f) = 1,\ v = 2ef$, $u = e^2 + f^2$. Sada iz $v = 2n^2$ imamo da je $n^2 = ef$, pa postoje $a,\ b \in \mathbb{N}$ takvi da je $e = a^2$ i $f = b^2$. Prema tome, $a^4 + b^4 = m^2$. Sada je (a^2, b^2, m) Pitagorina trojka za čiju hipotenuzu vrijedi: $m < m^2 = u < u^2 + v^2 = z$, a to je u kontradikciji s izborom z. □

5.3 Cjelobrojna rješenja

U ovom odjeljku promatrat ćemo jednadžbe oblika $a^2 + b^2 = c^3$ i $y^2 + 1 = x^3$ te iskoristiti prsten $\mathbb{Z}[i]$ za dokazivanje nekih njihovih karakteristika.

Teorem 5.3.1. *Neka je zadana jednadžba $a^2 + b^2 = c^3$. Cjelobrojna rješenja (a, b, c) ove jednadžbe sa svojstvom $(a, b) = 1$ dana su sa*

$$a = m^3 - 3mn^2,\ b = 3m^2n - n^3,\ c = m^2 + n^2,$$

gdje je $(m, n) = 1$ i $m \not\equiv n \pmod 2$.

Dokaz. Iz činjenice da je $(a, b) = 1$ slijedi da a i b nisu oba parna. Ako bi oba bila neparna, tada bi imali $c^3 \equiv 1+1 \equiv 2 \pmod 8$ što očito ne vrijedi ni za koji cijeli broj c. Zaključujemo da je jedan od brojeva a ili b paran, a drugi je neparan, $a \not\equiv b \pmod 2$ i c je neparan.
Zadanu jednadžbu možemo faktorizirati u $\mathbb{Z}[i]$ kao

$$(a + bi)(a - bi) = c^3.$$

Prvo treba pokazati da su $a + bi$ i $a - bi$ relativno prosti. To se dokaže kao u dokazu leme 5.2.4. Nadalje, produkt faktora $a + bi$ i $a - bi$ je savršeni kub u $\mathbb{Z}[i]$ te znamo da su faktori relativno prosti pa prema jedinstvenoj faktorizaciji u $\mathbb{Z}[i]$ slijedi da su $a + bi$ i $a - bi$ oba kubovi do na umnožak invertibilnim elementom. Stoga, neka je $a + bi = \lambda\alpha^3$ gdje je $\lambda \in \{\pm 1, \pm i\}$. Uočimo da je svaki invertibilni element sam po sebi kub:

$$1 = 1^3,\ -1 = (-1)^3,\ i = (-i)^3,\ -i = i^3$$

pa zato možemo reći da je $a + bi$ savršen kub.
Dalje zapisujemo $a + bi = (m + ni)^3$, gdje su $m,\ n \in \mathbb{Z}$. Desnu stranu jednakosti kubiramo, a potom izjednačimo realni i imaginarni dio s lijeve i desne strane. Sređivanjem izraza dobivamo:

$$a = m^3 - 3mn^2,\ b = 3m^2n - n^3.$$

Kako su a i b relativno prosti, slijedi da su i m i n relativno prosti, tj. $(m, n) = 1$.
Ako bi bilo $m \equiv n \pmod 2$, tada bi imali $a \equiv -2m^3 \equiv 0 \pmod 2$ i $b \equiv 2m^3 \equiv 0 \pmod 2$, a to bi značilo da su i a i b parni što znamo da nije istina. Dakle, $m \not\equiv n \pmod 2$.
Nadalje, $c^3 = (a + bi)(a - bi) = (m + ni)^3(m - ni)^3 = (m^2 + n^2)^3$. Dakle, $c = m^2 + n^2$.
Obratno, ako je $(m, n) = 1$ i $m \not\equiv n \pmod 2$, tada a i b (definirani kao gore) i $c = m^2 + n^2$ zadovoljavaju $a^2 + b^2 = c^3$ i $a + bi = (m + ni)^3$. Još treba pokazati da je $(a, b) = 1$, a to se lako pokaže koristeći činjenicu $(m, n) = 1$.
Izbor ovakvih m i n je jedinstven, a to proizlazi iz $a + bi = (m + ni)^3$. Ako bi imali m' i n' takve da zadovoljavaju jednakosti za $a,\ b$ i c, tada bi bilo $(m + ni)^3 = (m' + n'i)^3$. Iz ovoga slijedi $m + ni = m' + n'i$ te konačno, $m = m'$ i $n = n'$. □

Primjer 5.3.2. *Pogledajmo primjere nekih rješenja jednadžbe $a^2 + b^2 = c^3$ za odabrane m i n.*
Za $m = 1,\ n = 0$ imamo:

$$a = m^3 - 2mn^2 = 1,$$
$$b = 3m^2n - n^3 = 0,$$
$$c = m^2 + n^2 = 1$$

pa slijedi $1^2 + 0^2 = 1^3$.
Za $m = 7,\ n = 2$ imamo:

$$a = m^3 - 2mn^2 = 259,$$
$$b = 3m^2n - n^3 = 286,$$
$$c = m^2 + n^2 = 53$$

pa slijedi $259^2 + 286^2 = 53^3$.

Teorem 5.3.3. *Jedini $x,\ y \in \mathbb{Z}$ koji zadovoljavaju jednadžbu $y^2 = x^3 - 1$ su $(x, y) = (1, 0)$.*

Dokaz. Uvrštavanjem $(x, y) = (1, 0)$ u jednadžbu dobivamo:

$$0^2 = 1^3 - 1$$
$$0 = 0$$

iz čega se vidi da $(x, y) = (1, 0)$ zadovoljava jednadžbu.Trebamo pokazati da je $(1, 0)$ jedini uređeni par (x, y) koji zadovoljava jednadžbu. Jednadžbu najprije zapišemo u obliku

$$x^3 = y^2 + 1,$$

a potom jednadžbu faktoriziramo u prstenu $\mathbb{Z}[i]$

$$x^3 = (y + i)(y - i).$$

Sada trebamo pokazati da su $y + i$ i $y - i$ relativno prosti; to se dokaže točno kao u dokazu leme 5.2.4. Kako su ta dva faktora relativno prosti u $\mathbb{Z}[i]$ i kako je njihov produkt kub, svaki faktor treba također biti kub do na umnožak nekim invertibilnim elementom. Nadalje, možemo pisati

$$y + i = (m + ni)^3,$$

za neke $m,\ n \in \mathbb{Z}$. Argumentacja je ista kao i u dokazu teorema 5.3.1. Desnu stranu jednakosti kubiramo, a potom izjednačavamo realni i imaginarni dio s lijeve i desne strane. Sređivanjem izraza dobivamo:

$$y = m^3 - 3mn^2 = m(m^2 - 3n^2),\ 1 = 3m^2n - n^3 = n(3m^2 - n^2).$$

Desna strana jednakosti povlači da je $n = \pm 1$. U slučaju kad je $n = 1$ imamo $1 = 3m^2 - 1$, tj. $3m^2 = 2$, a ta jednadžba nema cjelobrojnih rješenja. Ako je $n = -1$, tada imamo $1 = -(3m^2 - 1)$ iz čega slijedi da je $m = 0$. Dakle, $y = 0$, a $x^3 = y^2 + 1 = 0^2 + 1 = 1$. □

Napomena 5.3.4. *1850. godine je francusko-belgijski matematičar Victor-Améd'ee Lebesgue dokazao tvrdnju da jednadžba $y^2 = x^d - 1$, $d \geq 2$ nema rješenja u skupu $\mathbb{Z} \setminus 0$.*

Bibliografija

[1] Keith Conrad, *The Gaussian integers*, dostupno na https://kconrad.math.uconn.edu/blurbs/ugradnumthy/Zinotes.pdf (lipanj 2020.).

[2] Andrej Dujella, *Uvod u teoriju brojeva*, PMF-Matematički odjel, Sveučilište u Zagrebu (skripta) (2003).

[3] Hrvoje Kraljević, *Algebra*, Sveučilište Josipa Jurja Strossmayera u Osijeku (2008).

[4] Ivan Matić, *Uvod u teoriju brojeva*, Odjel za matematiku Sveučilišta JJ Strossmayera u Osijeku (2015).

[5] Boris Širola, *Algebarske strukture*, PMF-Matematički odjel, Sveučilište u Zagrebu, skripta (2014).

[6] John Stillwell, *Elements of number theory*, Springer Science & Business Media, 2002.

Sažetak

Prsten Gaussovih cijelih brojeva $\mathbb{Z}[i]$ generalizacija je prstena cijelih brojeva $\mathbb{Z}$. Kao takvi, Gaussovi cijeli brojevi zadržali su većinu svojstava cijelih brojeva. U $\mathbb{Z}[i]$ imamo faktorizaciju $x^2 + y^2 = (x + yi)(x - yi),\ i = \sqrt{-1}$.
Kroz svojstva invertibilnosti i dijeljenja iskazuje se i dokazuje modificirani teorem o dijeljenju s ostatkom u $\mathbb{Z}$ koji nam pomaže u dokazivanju teorema o dijeljenju s ostatkom u $\mathbb{Z}[i]$. Kroz primjere vidi se upotreba Euklidovog algoritma pri određivanju najvećeg zajedničkog djelitelja dvaju Gaussovih cijelih brojeva. Upotrebom Bezoutovog teorema pokazali smo da su $\alpha,\ \beta \in \mathbb{Z}[i]$ relativno prosti akko je $\alpha x + \beta y = 1$ za neke $x,\ y \in \mathbb{Z}[i]$.
Govorili smo o prostim Gaussovim cijelim brojevima. Dokazali smo koristan teorem o prepoznavanju prostih brojeva u $\mathbb{Z}[i]$, koji nam govori da ako je norma Gaussovog cijelog broja prost broj u $\mathbb{Z}$, da je tada taj Gaussov cijeli broj prost u $\mathbb{Z}[i]$. Također, pokazali smo da je prikaz Gaussovih cijelih brojeva u obliku produkta prostih Gaussovih cijelih brojeva jedinstven do na permutacije i množenje faktora invertibilnim elementima.
Za kraj, govorilo se o primjenama Gaussovih cijelih brojeva. Posebno, pomoću Gaussovih cijelih brojeva dokazali smo neke tvrdnje o prostim brojevima, opisali (primitivne) Pitagorine trojke i proučavali cjelobrojna rješenja jednadžbi $a^2 + b^2 = c^3$ i $y^2 + 1 = x^3$.

Summary

The ring of Gaussian integers $\mathbb{Z}[i]$ is a generalization of the ring $\mathbb{Z}$. As such, Gaussian integers kept most of characteristics of integers. In $\mathbb{Z}[i]$ we have factorization $x^2 + y^2 = (x + yi)(x - yi),\ i = \sqrt{-1}$.
Through the properties of invertibility and division, we proved the modified division theorem which helped us prove the division theorem in $\mathbb{Z}[i]$. Through examples we saw the use of Euclidean algorithm in finding the greatest common divisor of two Gaussian integers. With the help of Bezout's theorem we showed that $\alpha,\ \beta \in \mathbb{Z}[i]$ are relatively prime if and only if $\alpha x + \beta y = 1$ for some $x,\ y \in \mathbb{Z}[i]$.
We have talked about primes in $\mathbb{Z}[i]$. Also, we proved a theorem about recognizing primes in $\mathbb{Z}[i]$ which tells that if the norm of a Gaussian integer is prime in $\mathbb{Z}$, then this Gaussian integer is prime in $\mathbb{Z}[i]$. Moreover, we have shown the unique factorization into primes of the Gaussian integers.
At the end, we talked about applications of Gaussian integers. We used Gaussian integers to prove a few claims on primes in Z, describe the (primitive) Pythagorean triples and study the integer solutions of equations $a^2 + b^2 = c^3$ and $y^2 + 1 = x^3$.

Životopis

Osobni podaci
Ime i prezime: Iva Novak
Datum i mjesto rođenja: 26.04.1996., Čakovec
Adresa: Bana Josipa Jelačića 165, Mačkovec, 40 000 Čakovec
E-mail: ivily007@gmail.com

Obrazovanje
Osnovnu školu pohađala sam u periodu između 2003. i 2011. godine. Pohađala sam Osnovnu školu Petar Zrinski Šenkovec. 2011. godine upisala sam Gimnaziju Josipa Slavenskog Čakovec smjer Opća gimnazija. Istu sam završila 2015. godine. U srednjoj školi rodila se moja ljubav prema matematici te sam zato 2015. godine upisala Prirodoslovno-matematički fakultet u Zagrebu, smjer: nastavnički. 2018. godine završila sam preddiplomski studij te stekla titulu univ. bacc. educ. math, a iste godine upisala Diplomski studij matematika: smjer nastavnički na istom fakultetu. Trenutno završavam petu godinu i pišem diplomski rad na temu *Prsten Gaussovih cijelih brojeva i primjene*.

Radno iskustvo
U sklopu kolegija Metodika nastave matematike 3, 4. godine diplomskog studija matematika: smjer nastavnički, bila je obavezna praksa u osnovnoj školi. Praksu sam uspješno obavila u Osnovnoj školi Silvija Strahimira Kranjčevića Zagreb pod vodstvom profesorice Tanje Soucie. U sklopu prakse u osnovnoj školi imala sam priliku volontirati na večeri matematike i učenicima osnovnih škola približiti primjenu matematike u svakodnevnom životu te je tako učiniti još zanimljivijom. U sklopu kolegija Metodika nastave matematike 4, 5. godine diplomskog studija matematika: smjer nastavnički, bila je obavezna praksa u srednjoj školi. Praksu sam uspješno obavila u Tehničkoj školi Zagreb pod vodstvom profesorice Mirjane Matijević. U sklopu Tehničke škole Zagreb, smjerovi u kojima sam obavljala praksu bili su Tehnička gimnazija, Tehničar za elektrotehniku i računalstvo i Tehničar vuče – strojovođa. Volontiranjem i davanjem instrukcija učenicima osnovnih i srednjih škola, također sam stekla iskustvo rada s učenicima i uvidjela razlike u programima matematike ovisno iz koje škole učenici dolaze.

Vještine
Rad na računalu: aktivno i svakodnevno korištenje MSOffice paketa, programiranje u programskom jeziku Python, programski jezik LaTex, korištenje Interneta i izrada web stranica, izrada interaktivnih sadržaja za nastavu
Strani jezici: engleski jezik aktivno u govoru i pismu, njemački jezik pasivno u govoru i pismu

Slobodno vrijeme
Trčanje, vježbanje, instrukcije