Univerzitet u Beogradu
Matematički fakultet

Master rad

Euklidov algoritam u prstenu Gausovih celih

Mentor:
prof. dr Goran Đanković

Student:
Sanda Baljošević 1026/2019

Beograd, 2021.

Mami i tati

Sadržaj

1 Uvod

Pored prstena celih brojeva $\mathbb{Z}$, prstena polinoma nad poljem i prstena ostataka $\mathbb{Z}/n\mathbb{Z}$, učenici nemaju prilike da se upoznaju ni sa jednim drugim prstenom. Jedan od značajnih i interesantnih primera je i prsten Gausovih celih, koji može poslužiti kao motivacija za uvođenje i bavljenje različitim algebarskim pojmovima.

U ovom radu čitaoci će biti upoznati sa osnovnim osobinama prstena Gausovih celih, pojmom norme na njemu i odgovarajućim Euklidovim algoritmom. Potom će biti reči o jedinstvenosti faktorizacije na proste faktore, kao i o zanimljivim posledicama koje se mogu primeniti na rešavanje Diofantovih jednačina.

U drugoj glavi ovog rada biće opisan prsten Gausovih celih i operacije nad njima, uz adekvatne geometrijske interpretacije. Zanimljivo je da se u određenim situacijama Gausovi celi mogu poistovetiti sa kompleksnim brojevima, o čemu će više reči biti u nastavku.

U trećoj glavi obrađen je jedan od najznačajnijih pojmova, a to je norma u prstenu Gausovih celih, uz nekoliko važnih osobina.

Četvrta glava odnosi se na pojam deljivosti u prstenu Gausovih celih. Najpre će biti data definicija deljivosti, a potom i nekoliko teorema potkrepljenih adekvatnim primerima.

Peta glava sadrži Euklidov algoritam i dokaze nekoliko važnih tvrđenja i bogata je primerima.

Šesta glava posvećena je jedinstvenosti faktorizacije na proste faktore. Takođe, biće definisan prost i složen Gausov ceo i njihove osobine.

Sedma glava sadrži nekoliko tvrđenja koja se odnose na proste elemente prstena Gausovih celih.

Osma glava sadrži nekoliko najznačajnijih primena osobina prstena Gausovih celih na aritmetiku u $\mathbb{Z}$, a to su: jedinstvenost načina na koji se prost broj koji je suma dva kvadrata može prikazati u tom obliku, klasifikacija rešenja jednačine $a^2 + b^2 = c^3$, određivanje jedinog celobrojnog rešenja jednačine $y^2 = x^3 - 1$ i sistematično određivanje celih brojeva koji su suma dva kvadrata na više načina.

Na kraju je i pregled korišćene literature.

2 Prsten Gausovih celih i operacije u njemu

Pored grupa, prsteni su algebarske strukture sa kojima se učenici, pa i studenti, prvo sreću u svom matematičkom obrazovanju.

Definicija 1. *Algebarska struktura $R = (R, +, \cdot)$ sa binarnim operacijama $+$ i $\cdot$ je prsten ako i samo ako su ispunjeni sledeći uslovi:*

1. *$(R, +)$ je Abelova grupa;*
2. *$(R, \cdot)$ je polugrupa;*
3. *operacija $\cdot$ je i levo i desno distributivna u odnosu na operaciju $+$, tj.*

$$a \cdot (b + c) = a \cdot b + a \cdot c,$$

$$(b + c) \cdot a = b \cdot a + c \cdot a.$$

Prsten R je komutativan ako i samo ako je $(R, \cdot)$ komutativna polugrupa.

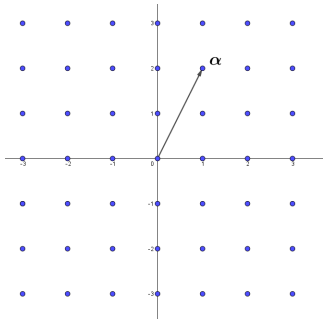
Jedan od algebarskih prstena sa kojima učenici tokom svog školovanja nemaju priliku da se upoznaju, a može biti vrlo koristan u aritmetičkim operacijama u skupu $\mathbb{Z}$ je prsten Gausovih celih.

Definicija 2. *Algebarska struktura $(\mathbb{Z}[i], +, \cdot)$, gde je $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$ naziva se prsten Gausovih celih.*

Primer 1. *Primeri Gausovih celih su: $\alpha = 1 + 8i, \beta = -5 + 11i, \gamma = 4 + 2i$ i tako dalje.*

Geometrijski, Gausovi celi mogu se predstaviti kao kompleksni brojevi sa celobrojnim realnim i imaginarnim delom.

Primer 2. *Geometrijski prikaz Gausovog celog $\alpha = 1 + 2i$ dat je na slici 1.*



Slika 1: Geometrijski prikaz Gausovog celog $\alpha = 1 + 2i$

2.1 Sabiranje i množenje Gausovih celih i njihova geometrijska interpretacija

Sabiranje i množenje Gausovih celih sprovode se na isti način kao kod kompleksnih brojeva. Oduzimanje se svodi na sabiranje, a o deljenju će više reči biti u nastavku.

Definicija 3. *Neka su $\alpha = a + bi$ i $\beta = c + di$ dva elementa prstena Gausovih celih. Njihov zbir se definiše na sledeći način:*

$$(a + bi) + (c + di) := (a + c) + (b + d)i.$$

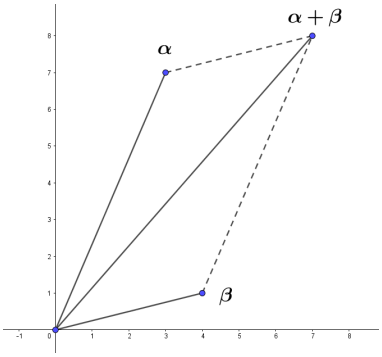
Definicija 4. *Neka su $\alpha = a + bi$ i $\beta = c + di$ dva elementa prstena Gausovih celih. Njihov proizvod se definiše na sledeći način:*

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

Primer 3. *Dati su Gausovi celi $\alpha = 3 + 7i$ i $\beta = 4 + i$. Odredimo njihov zbir:*

$$\alpha + \beta = (3 + 7i) + (4 + i) = (3 + 4) + (7 + 1)i = 7 + 8i.$$

Geometrijska interpretacija sabiranja ekvivalentna je sabiranju vektora pravilom paralelograma. Prikaz sprovedene operacije dat je na slici 2.

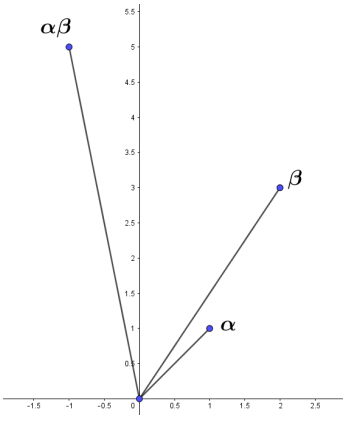


Slika 2: Zbir Gausovih celih $\alpha = 3 + 7i$ i $\beta = 4 + i$

Primer 4. *Dati su Gausovi celi $\alpha = 1 + i$ i $\beta = 2 + 3i$. Odredimo njihov proizvod:*

$$\alpha\beta = (1 + i)(2 + 3i) = (2 - 3) + (2 + 3)i = -1 + 5i.$$

Geometrijska interpretacija množenja Gausovih celih naročito je interesantna. Proizvod Gausovog celog α i Gausovog celog β ekvivalentan je rotaciji α za ugao koji β obrazuje sa pozitivnim delom $x-$ose, pa potom skaliranju sa kvadratnim korenom iz kvadrata modula odgovarajućeg kompleksnog broja β. Prikaz sprovedene operacije dat je na slici 3.



Slika 3: Proizvod Gausovih celih $\alpha = 1 + i$ i $\beta = 2 + 3i$

3 Norma u prstenu Gausovih celih

Pre nego što definišemo normu u prstenu Gausovih celih, treba reći da je konjugat Gausovog celog definisan na isti način kao i konjugat kompleksnog broja, iz čega proističe jednakost njihovih modula. Dakle, konjugat Gausovog celog $\alpha = a + bi$, je $\overline{\alpha} = a - bi, a, b \in \mathbb{Z}$.

Definicija 5. *Za proizvoljan element $\alpha = a + bi \in \mathbb{Z}[i]$, norma se definiše na sledeći način:*

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

Primera radi, ukoliko posmatramo Gausov ceo $3 + 2i$, njegovu normu po definiciji računamo na sledeći način:

$$N(3 + 2i) = 3^2 + 2^2 = 9 + 4 = 13.$$

Za svako $x \in \mathbb{Z}, N(x) = x^2$. Takođe, $N(1) = 1$.

Ukoliko $a+bi$ posmatramo kao kompleksan broj sa celobrojnim realnim i imaginarnim delom, primetićemo da je njegova norma jednaka kvadratu njegovog modula:

$$|a + bi| = \sqrt{a^2 + b^2}, N(a + bi) = a^2 + b^2 = |a + bi|^2.$$

Razlog zbog kog biramo rad sa normom u $\mathbb{Z}[i]$, umesto sa modulom, jeste taj što je norma ceo (prirodan) broj. To će nam omogućiti da lakše zaključimo koje osobine ima deljivost u prstenu Gausovih celih.

Teorema 1. *Norma je multiplikativna: za $\alpha, \beta \in \mathbb{Z}[i]$ važi*

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

▲ Neka je $\alpha = a + bi$ i $\beta = c + di$. Tada je

$$\alpha\beta = (ac - bd) + (ad + bc)i.$$

Izračunajmo sada $N(\alpha)N(\beta)$ i $N(\alpha\beta)$:

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

$N(\alpha\beta) = (ac-bd)^2+(ad+bc)^2 = (ac)^2-2abcd+(bd)^2+(ad)^2+2abcd+(bc)^2 = (ac)^2+(ad)^2+(bc)^2+(bd)^2$

Dakle,

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

Lema 1. *Jedini Gausovi celi koji su invertibilni u $\mathbb{Z}[i]$ su ± 1 i $\pm i$.*

▲ Nije teško primetiti da ± 1 i $\pm i$ imaju inverze u $\mathbb{Z}[i]$: 1 i -1 su sami sebi inverzi, a i i $-i$ su jedan drugom inverzi. Da bismo dokazali suprotan smer, pretpostavićemo da je $\alpha \in \mathbb{Z}[i]$ invertibilan, i da važi $\alpha\beta = 1$, za neko $\beta \in \mathbb{Z}[i]$. Želimo da dokažemo da $\alpha \in \{\pm 1, \pm i\}$. Ukoliko primenimo normu na obe strane jednakosti $\alpha\beta = 1$, dobijamo da važi $N(\alpha)N(\beta) = N(1) = 1$. Ovo je jednačina u skupu celih brojeva, pa možemo da zaključimo da je $N(\alpha) = \pm 1$. Kako norma ne uzima negativne vrednosti, biće $N(\alpha) = 1$. Ukoliko pretpostavimo da je $\alpha = a + bi$, sledi da je $a^2 + b^2 = 1$, a to je moguće samo ukoliko $\alpha \in \{\pm 1, \pm i\}$. ■

Invertibilni elementi se nazivaju jedinice. Jedinice u skupu $\mathbb{Z}$ su ± 1. Jedinice u skupu $\mathbb{Z}[i]$ su ± 1 i $\pm i$.

Norma svakog Gausovog celog je nenegativan ceo broj. Međutim, ne može svaki nenegativan ceo broj biti norma nekog Gausovog celog. Norma je uvek suma dva kvadrata, to jest ima oblik $a^2 + b^2$. Stoga, zaključujemo da brojevi kao što su $3, 7, 11, 15, 19, 21$ i tako dalje ne mogu biti norma nekog Gausovog celog.

4 Deljivost u prstenu Gausovih celih

Definicija 6. *Neka su $\alpha, \beta \in \mathbb{Z}[i]$. Kažemo da β deli α (u oznaci $\beta|\alpha$) ako postoji $\gamma \in \mathbb{Z}[i]$ tako da je $\alpha = \beta\gamma$. Tada kažemo da je β delilac ili faktor elementa α.*

Primer 5. *S obzirom na to da je $14 - 3i = (4 + 5i)(1 - 2i)$, $4 + 5i$ deli $14 - 3i$.*

Primer 6. *Da li je $4 + 5i$ delilac elementa $14 + 3i$? Možemo ih podeliti kako bismo proverili:*

$$\frac{14 + 3i}{4 + 5i} = \frac{(14 + 3i)(4 - 5i)}{(4 + 5i)(4 - 5i)} = \frac{71 - 58i}{41} = \frac{71}{41} - \frac{58}{41}i.$$

Dobijeni rezultat nije element skupa $\mathbb{Z}[i]$, pa zaključujemo da $4 + 5i$ ne deli $14 + 3i$ u $\mathbb{Z}[i]$.

Teorema 2. *Element prstena Gausovih celih $\alpha = a + bi$ je deljiv celim brojem c ako i samo ako $c|a$ i $c|b$.*

▲ Ukoliko $c|(a+bi)$ u $\mathbb{Z}[i]$, to znači da je $a+bi = c(m+ni)$, za neke $m, n \in \mathbb{Z}$, što je ekvivalentno činjenici da je $a = cm$ i $b = cn$, to jest $c|a$ i $c|b$. ■

Teorema 3. *Za $\alpha, \beta \in \mathbb{Z}[i]$, ukoliko $\beta|\alpha$ u $\mathbb{Z}[i]$, onda $N(\beta)|N(\alpha)$ u $\mathbb{Z}$.*

▲ Kako $\beta|\alpha$, važi da je $\alpha = \beta\gamma$ za neko $\gamma \in \mathbb{Z}[i]$. Odatle sledi da je i $N(\alpha) = N(\beta)N(\gamma)$. Ovo je jednakost u skupu $\mathbb{Z}$, što znači da $N(\beta)|N(\alpha)$. ■

Teorema 4. *Element prstena Gausovih celih ima parnu normu ako i samo ako je on umnožak elementa $1+i$.*

▲ Pošto je $N(1+i) = 2$, jasno je da svaki umnožak elementa $1+i$ ima parnu normu. Dokažimo i suprotan smer. Pretpostavimo da $m + ni$ ima parnu normu. To znači da je $m^2 + n^2 \equiv_2 0$. U tom slučaju, m i n su ili oba parna, ili oba neparna. Dakle, $m \equiv_2 n$.
Naš cilj je da $m + ni$ predstavimo kao $m + ni = (1 + i)(u + iv)$, za neke $u, v \in \mathbb{Z}$. Odatle sledi

$$m + ni = (u - v) + (u + v)i.$$

To je moguće ukoliko je $u = \frac{n+m}{2}, v = \frac{n-m}{2}$. Pošto su m i n iste parnosti, u i v su celi brojevi.
Dakle, $(1+i)|(m+ni)$. ■

Primer 7. *Norma elementa* $1+3i$ *je* 10, *i* $1+3i = (1+i)(2+i)$.

Primer 8. *Kako* $1-i$ *ima normu* 2, *sledi da* $1-i$ *mora biti umnožak elementa* $1+i$. *Zaista,* $1-i = -i(1+i)$.

Teorema 3 je veoma korisna kada treba da dokažemo da jedan element prstena Gausovih celih ne deli drugi. Na primer, ukoliko važi $(3+7i)|(10+3i)$ u $\mathbb{Z}[i]$, moralo bi važiti i da $N(3+7i)|N(10+3i)$, tj. $58|109$ u $\mathbb{Z}$, što naravno nije tačno. Prema tome, $3+7i$ ne deli $10+3i$ u $\mathbb{Z}[i]$. Na ovaj način, problem deljivosti u $\mathbb{Z}[i]$ sveli smo na problem deljivosti u $\mathbb{Z}$, što je za rad svakako jednostavnije.

Međutim, sa ovom teoremom treba biti obazriv. Ona nam garantuje da iz deljivosti u $\mathbb{Z}[i]$ proističe deljivost normi u $\mathbb{Z}$, dok obrnuto ne mora da važi. Razmotrićemo $\alpha = 14+3i$ i $\beta = 4+5i$. Primetimo da je $N(\beta) = 41$ i $N(\alpha) = 205 = 5 \cdot 41$, pa $N(\beta)|N(\alpha)$. Uprkos tome, u primeru 6 videli smo da $4+5i$ ne deli $14+3i$ u $\mathbb{Z}[i]$.

U skupu $\mathbb{Z}$, ukoliko je $|m| = |n|$, onda je $m = \pm n$. Odgovorajuće tvrđenje u skupu $\mathbb{Z}[i]$ nije tačno: ako je $N(\alpha) = N(\beta)$, ne možemo zaključiti da su α i β jedan drugom jedinični umnošci. Razmotrimo $4+5i$ i $4-5i$. Njihove norme su 41, ali jedinični umnošci elementa $4+5i$ su

$$4+5i, -4-5i, -5+4i, 5-4i.$$

Vidimo da među njima nema elementa $4-5i$, pa oni nisu jedan drugom jedinični umnošci.

Teorema 5. *(Teorema o deljivosti) Za* $\alpha, \beta \in \mathbb{Z}[i], \beta \neq 0$, *postoje* $\gamma, \rho \in \mathbb{Z}[i]$ *takvi da je* $\alpha = \beta\gamma + \rho$ *i* $N(\rho) < N(\beta)$. *Preciznije, možemo izabrati* ρ *tako da je* $N(\rho) \leq \frac{1}{2}N(\beta)$. *Brojevi* γ *i* ρ *su količnik i ostatak, redom.*

Pre dokaza ove teoreme razmotrićemo jedan primer. Neka je $\alpha = 27-23i$ i $\beta = 8+i$. Tada je $N(\beta) = 65$. Želimo da zapišemo α u sledećem obliku: $\alpha = \beta\gamma + \rho$, gde su γ i ρ, redom, količnik i ostatak pri deljenju α sa β i važi da je $N(\rho) < 65$. Razmotrimo sledeći količnik:

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

Kako je $\frac{193}{65} = 2,969...$ i $-\frac{211}{65} = -3,246...$, zamenićemo svaki od ovih razlomaka njegovim celim delom. Dakle, uzećemo da je $\gamma = 2-4i$. U tom slučaju, dobijamo da važi

$$\alpha - \beta(2-4i) = 7+7i,$$

ali norma ostatka je $N(7+7i) = 98 > 95 = N(\beta)$. Dakle, ovakav izbor količnika bio je loša ideja.

Da bismo popravili naš izbor, potrebno je da pažljivije razmotrimo čime ćemo zameniti $\frac{193}{65}$ i $-\frac{211}{65}$. Pokušajmo, umesto celim delom, da ih zamenimo najbližim celim brojem. Tada ćemo dobiti $\gamma = 3-3i$. U tom slučaju, važiće

$$\alpha - \beta(3-3i) = -2i,$$

i $N(-2i) < N(\beta)$. Dakle, koristićemo $\gamma = 3 - 3i$ i $\rho = -2i$.

Sličan izbor mogli bismo da napravimo i u $\mathbb{Z}$. Na primer, $\frac{34}{9} = 3,77...$, što je bliže broju 4 nego broju 3. Dakle, radije ćemo zapisati

$$34 = 9 \cdot 4 - 2$$

nego

$$34 = 9 \cdot 3 + 7.$$

Iako je ostatak u prvoj jednakosti negativan, on je po apsolutnoj vrednosti manji.

Prethodni primer predstavlja modifikovanu teoremu o deljivosti u $\mathbb{Z}$. Uobičajeno, za cele brojeve a i b takve da je $b \neq 0$ teorema o deljivosti u $\mathbb{Z}$ nalaže sledeće: izaberimo bq kao umnožak b koji je najbliži broju a sa leve strane: $bq \leq a < b(q+1)$. Onda definišemo $r = a - bq$, odakle je $r \geq 0$ jer je $bq \leq a$ i $r < |b|$ jer su brojevi bq i $b(q+1)$ na rastojanju $|b|$ i a će biti bliže bq nego $b(q+1)$. U modifikovanoj teoremi o deljivosti treba uzeti bq kao umnožak broja b koji je najbliži broju a, umesto samo posmatrati broj najbliži broju a sa leve strane. Broj q u modifikovanoj teoremi o deljivosti je najbliži ceo broj broju $\frac{a}{b}$ i kao takav može se nalaziti sa desne strane broja $\frac{a}{b}$ umesto sa leve. Ceo broj r je najviše za $\frac{1}{2}|b|$ udaljen od umnoška broja b u bilo koju stranu, pa $|a - bq| \leq \frac{1}{2}|b|$. Odavde zapišimo $r = a - bq$ odakle sledi da je $a = bq + r$, pri čemu $|r| \leq \frac{1}{2}|b|$. U običnoj teoremi o deljivosti ostatak je nenegativan i ograničen odozgo sa $|b|$. Opisanim postupkom smo smanjili gornju granicu na $\frac{1}{2}|b|$ pri čemu smo dozvolili da ostatak pri deljenju bude negativan. Ponekad broj a može da leži tačno na sredini između dva umnoška broja b. U tom slučaju količnik i ostatak nisu jedinstveni. Na primer, ako je $a = 27$ i $b = 6$, tada je a tačno na sredini između $4b$ i $5b$, to jest 27 možemo predstaviti kao

$$27 = 6 \cdot 4 + 3$$

ili

$$27 = 6 \cdot 5 - 3.$$

Odavde dobijamo dva moguća izbora za r, $r = 3$ ili $r = -3$. Uobičajena teorema o deljivosti ima jedinstven količnik i ostatak ali modifikovana verzija odustaje od jedinstvenosti. Ovo možda izgleda kao problem ali to je upravo ono što nam treba da bismo dokazali teoremu o deljivosti u $\mathbb{Z}[i]$.

▲ Neka su $\alpha, \beta \in \mathbb{Z}[i], \beta \neq 0$. Želimo da konstruišemo $\gamma, \rho \in \mathbb{Z}[i]$ tako da je $\alpha = \beta\gamma + \rho$, pri čemu je $N(\rho) \leq \frac{1}{2}N(\beta)$.
Zapišimo

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\beta\overline{\beta}} = \frac{\alpha\overline{\beta}}{N(\beta)} = \frac{m + ni}{N(\beta)},$$

gde je $\alpha\overline{\beta} = m + ni$. Podelićemo m i n normom elementa β:

$$m = N(\beta)q_1 + r_1,$$

$$n = N(\beta)q_2 + r_2,$$

gde su q_1 i q_2 elementi skupa $\mathbb{Z}$ i $0 \leq |r_1|, |r_2| \leq \frac{1}{2}N(\beta)$. Tada je

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

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

Neka je $\gamma = q_1 + q_2 i$ (to će biti željeni količnik). Tada je

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

Pokažimo još da je $N(\alpha - \beta\gamma) \leq \frac{1}{2}N(\beta)$.
Primenjujući normu na poslednju jednakost, dobijamo

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

Kako je $0 \leq |r_1|, |r_2| \leq \frac{1}{2}N(\beta)$, dobijamo

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

Primer 9. *Neka je $\alpha = 11 + 10i$ i $\beta = 4 + i$. Tada je $N(\beta) = 17$. Posle kratkog računa dobićemo*

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{N(\beta)} = \frac{54 + 29i}{17}.$$

Kako je $\frac{54}{17} = 3,17...$ i $\frac{29}{17} = 1,70...$, uzećemo $\gamma = 3 + 2i$. Tada je $\alpha - \beta\gamma = 1 - i$, pa je $\rho = 1 - i$. Primetimo i da je $N(\rho) = 2 \leq \frac{1}{2}N(\beta)$.

Primer 10. *Neka je $\alpha = 37 + 2i$ i $\beta = 11 + 2i$. Tada je $N(\beta) = 125$. Primenjujući prethodno opisan algoritam deljenja u $\mathbb{Z}[i]$, dobićemo:*

$$\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\beta\overline{\beta}} = \frac{\alpha\overline{\beta}}{N(\beta)} = \frac{(37 + 2i)(11 - 2i)}{125} = \frac{411 - 52i}{125}.$$

Izborom količnika 3 dobijamo

$$\alpha = \beta \cdot 3 + (4 - 4i).$$

Međutim, tačno je i da je

$$\alpha = \beta(3 - i) + (2 + 7i).$$

Ostatak u oba slučaja ima normu manju od $N(\beta)$ (preciznije, od $\frac{1}{2}N(\beta)$).

Primer 11. *Uzmimo da je $\alpha = 1 + 8i$ i $\beta = 2 - 4i$. Tada je*

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

Kako je $-\frac{3}{2}$ aritmetička sredina brojeva -2 i -1, možemo koristiti $\gamma = -1 + i$ ili $\gamma = -2 + i$. U prvom slučaju, rezultat će biti

$$\alpha = \beta(-1 + i) - 1 + 2i,$$

a u drugom

$$\alpha = \beta(-2 + i) + 1 - 2i.$$

Nejedinstvenost količnika i ostatka pri deljenju u $\mathbb{Z}[i]$ ne umanjuje značaj deljenja. Štaviše, jedinstvenost koja postoji u skupu $\mathbb{Z}$ potpuno je irelevantna za brojne važne primene (poput Euklidovog algoritma). Sve te primene koristićemo i u $\mathbb{Z}[i]$, sa suštinski istim dokazima.

5 Euklidov algoritam

Pre opisa samog Euklidovog algoritma, definisaćemo najveći zajednički delilac u $\mathbb{Z}[i]$.

Definicija 7. *Za $\alpha, \beta \in \mathbb{Z}[i], \alpha, \beta \neq 0$ najveći zajednički delilac jeste njihov zajednički delilac sa najvećom normom.*

Ako je δ najveći zajednički delilac elemenata α i β, onda su to barem još i njegovi jedinični umnošci: $-\delta, i\delta, -i\delta$.

Definicija 8. *Ukoliko α i β nemaju zajedničkih delilaca osim jedinica, kažemo da su oni uzajamno prosti.*

Teorema 6. *(Euklidov algoritam) Neka su $\alpha, \beta \in \mathbb{Z}[i], \alpha, \beta \neq 0$. Rekurzivno primenjujemo teoremu o deljivosti, počevši od ovog para, tako što delilac i ostatak u jednoj jednakosti proglasimo deljenikom i deliocem u narednoj, sve dok je ostatak različit od nule. Kako se veći od dva polazna broja na ovaj način smanjuje, ponavljanjem postupka dobijaće se sve manji brojevi, dok se jedan od njih ne svede na nulu.*

$$\alpha = \beta\gamma_1 + \rho_1, N(\rho_1) < N(\beta)$$

$$\beta = \rho_1\gamma_2 + \rho_2, N(\rho_2) < N(\rho_1)$$

$$\rho_1 = \rho_2\gamma_3 + \rho_3, N(\rho_3) < N(\rho_2)$$

$$\vdots$$

Poslednji ostatak različit od nule deljiv je svim zajedničkim deliocima α i β, a i sam je zajednički delilac, pa je on najveći zajednički delilac α i β.

▲ Dokaz je identičan dokazu Euklidovog algoritma u $\mathbb{Z}$. Posmatrajući postupak od prve jednačine prema poslednjoj, vidimo da zajednički delilac α i β deli poslednji nenula ostatak. Suprotno, posmatrajući postupak od poslednje jednačine prema prvoj, vidimo da je poslednji nenula ostatak zajednički delilac α i β. Odatle zaključujemo da je poslednji nenula ostatak zajednički delilac koji je deljiv svim ostalim zajedničkim deliocima α i β. Prema tome, on mora da ima najveću normu u poređenju sa ostalim deliocima, pa je on najveći zajednički delilac.■

Primer 12. *Odredimo najveći zajednički delilac za $\alpha = 32 + 9i$ i $\beta = 4 + 11i$. Primetimo da je $N(\beta) = 137$.*

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

$$N(2 - 5i) = 29 < N(\beta),$$

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

$$N(3 - i) = 10 < N(2 - 5i),$$

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

$$N(-i) = 1 < N(3-i),$$
$$3 - i = -i(1+3i) + 0.$$

Poslednji nenula ostatak je $-i$, pa α i β imaju zajedničke samo jedinice. Prema tome, oni su uzajamno prosti.

Primer 13. *Pokažimo da su $4+5i$ i $4-5i$ uzajamno prosti u $\mathbb{Z}[i]$:*

$$4 + 5i = (4-5i)i - (1-i),$$
$$N(-1+i) = 2 < N(4-5i),$$
$$4 - 5i = -(1-i)(-4) - i,$$
$$N(-i) = 1 < N(-1+i),$$
$$-(1-i) = -i(1+i) + 0.$$

Kako je poslednji nenula ostatak jedinica u $\mathbb{Z}[i]$, dokaz je završen.

Primer 14. *Pogledajmo i jedan primer gde najveći zajednički delilac nije jedinica. Uzmimo da je $\alpha = 11+3i$ i $\beta = 1+8i$. Primenimo Euklidov algoritam:*

$$11 + 3i = (1+8i)(1-i) + 2 - 4i,$$
$$N(2-4i) = 20 < N(1+8i),$$
$$1 + 8i = (2-4i)(-1+i) - 1 + 2i,$$
$$N(-1+2i) = 5 < N(2-4i),$$
$$2 - 4i = (-1+2i)(-2) + 0,$$

pa je najveći zajednički delilac $-1+2i$.
U drugoj jednakosti mogli smo da postupimo i na drugačiji način:

$$11 + 3i = (1+8i)(1-i) + 2 - 4i,$$
$$1 + 8i = (2-4i)(-2+i) + 1 - 2i,$$
$$2 - 4i = (1-2i) \cdot 2 + 0.$$

Dakle, i $1-2i$ je takođe najveći zajednički delilac. Međutim, primetimo da je $1-2i = -1 \cdot (-1+2i)$. Dakle, najveći zajednički delilac je jedinstveno određen do na množenje jedinicom.

Ukoliko je δ najveći zajednički delilac za α i β, onda $N(\delta)$ deli $N(\alpha)$ i $N(\beta)$, pa $N(\delta)$ deli i $(N(\alpha), N(\beta))$. Međutim, može se desiti da je $N(\delta) < (N(\alpha), N(\beta))$. U primeru 13 α i β su uzajamno prosti, pa njihov najveći zajednički delilac ima normu 1, dok je $N(\alpha) = N(\beta) = 41$.

U primeru 14 $N(\alpha) = 130$ i $N(\beta) = 65$. Znamo da je $(130, 65) = 65$, a njihov najveći zajednički delilac je $-1+2i$, čija je norma 5.

Pretpostavimo da je $(N(\alpha), N(\beta)) = 1$. Tada svi zajednički delioci α i β imaju normu koja deli 1. Prema tome, i te norme moraju biti jednake 1, što znači da su zajednički delioci jedinice. Vidimo da Gausovi celi čije su norme uzajamno prosti brojevi moraju i sami biti uzajamno prosti.

Lema 2. *Za nenula $\alpha, \beta \in \mathbb{Z}[i]$, neka je δ njihov najveći zajednički delilac dobijen Euklidovim algoritmom. Bilo koji drugi najveći zajednički delilac α i β mora biti jedinični umnožak delioca δ.*

▲ Neka je δ_1 najveći zajednički delilac α i β. Iz dokaza teoreme 6 znamo da $\delta_1|\delta$. Neka je $\delta = \delta_1\gamma$, pa je

$$N(\delta) = N(\delta_1)N(\gamma) \geq N(\delta_1).$$

Pošto je δ_1 najveći zajednički delilac, njegova norma mora biti najveća u poređenju sa normama ostalih zajedničkih delilaca, pa mora važiti $N(\delta) = N(\delta_1)$. Odatle sledi da je $N(\gamma) = 1$, pa je $\gamma = \pm 1$ ili $\gamma = \pm i$. To znači da su δ i δ_1 jedan drugom jedinični umnošci. ■

Teorema 7. *(Bezuova teorema) Neka je δ bilo koji najveći zajednički delilac Gausovih celih α i β, $\alpha, \beta \neq 0$. Tada je $\delta = \alpha x + \beta y$, za neke $x, y \in \mathbb{Z}[i]$.*

▲ Mogućnost zapisivanja δ kao $\mathbb{Z}[i]$-kombinacije α i β se neće promeniti ako zamenimo δ jediničnim umnoškom. Na primer, ako možemo da uradimo ovo za $i\delta$, onda množimo sa $-i$ da bismo to uradili za δ. Odatle, prema lemi 2 potrebno je da dokažemo da je δ najveći zajednički delilac što proističe iz Euklidovog algoritma. Za takvo δ zamena unazad u Euklidovom algoritmu pokazuje da je δ $\mathbb{Z}[i]$-kombinacija α i β. Ostali detalji su identični kao u slučaju celih brojeva. ■

Lema 3. *Dva nenula Gausova cela α i β su uzajamno prosta ako i samo ako je*

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

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

▲ Ako su α i β uzajamno prosti, onda je 1 najveći zajednički delilac za α i β. Prema Bezuovoj teoremi, $1 = \alpha x + \beta y$ za neke $x, y \in \mathbb{Z}[i]$. Obrnuto, ako je $1 = \alpha x + \beta y$ za neke $x, y \in \mathbb{Z}[i]$, onda svaki zajednički delilac α i β mora da deli 1, pa mora biti jedinica. Dakle, α i β su uzajamno prosti.■

Primer 15. *U primeru 12 videli smo da su $\alpha = 32+9i$ i $\beta = 4+11i$ uzajamno prosti, jer je poslednji nenula ostatak u Euklidovom algoritmu $-i$. Izrazimo sada $-i$ kao $\mathbb{Z}[i]-$kombinaciju α i β:*

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

Primer 16. *U primeru* 13 *pokazali smo da su* $4+5i$ *i* $4-5i$ *uzajamno prosti. Izrazimo* $-i$ *kao njihovu* $\mathbb{Z}[i]-$*kombinaciju:*

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

Množenjem poslednje jednakosti sa i *dobijamo*

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

Primer 17. *U primeru* 14 *videli smo da je* $-1+2i$ *najveći zajednički delilac za* $\alpha=11+3i$ *i* $\beta=1+8i$. *Možemo zapisati:*

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

Primer 18. *Uzmimo da je* $\alpha=10+91i$ *i* $\beta=7+3i$. *Primenom Euklidovog algoritma dobijamo:*

$$\begin{aligned} \alpha &= \beta(6+11i)+1-4i, \\ \beta &= (1-4i)(2i)+(-1+i), \\ 1-4i &= (-1+i)(-3+i)-1, \\ -1+i &= -1(1-i)+0. \end{aligned}$$

Poslednji nenula ostatak je -1, *pa su* α *i* β *uzajamno prosti. Predstavimo sada* -1 *kao njihovu* $\mathbb{Z}[i]-$*kombinaciju:*

$$\begin{aligned} -1 &= 1-4i-(-1+i)(-3+i) \\ &= 1-4i-(\beta-(1-4i)(2i))(-3+i) \\ &= (1-4i)(1+(2i)(-3+i))-\beta(-3+i) \\ &= (1-4i)(-1-6i)+\beta(3-i) \\ &= (\alpha-\beta(6+11i))(-1-6i)+\beta(3-i) \\ &= \alpha(-1-6i)+\beta(-(6+11i)(-1-6i)+3-i) \\ &= \alpha(-1-6i)+\beta(-57+46i). \end{aligned}$$

Množenjem poslednje jednakosti sa -1 dobijamo

$$1 = \alpha(1+6i) + \beta(57-46i).$$

U ovom primeru videli smo da su $10+91i$ i $7+3i$ uzajamno prosti u $\mathbb{Z}[i]$. Međutim, primetimo da njihove norme

$$N(10+91i) = 8381 = 17^2 \cdot 29,$$
$$N(7+3i) = 58 = 2 \cdot 29,$$

imaju zajednički faktor u $\mathbb{Z}$. To proističe iz njihove faktorizacije. Ne ulazeći u postupak faktorisanja, uporedićemo faktorizacije α i β:

$$10+91i = (1-4i)(4+i)(5+2i),$$
$$7+3i = (1+i)(5-2i).$$

Faktori $5+2i$ i $5-2i$ imaju jednake norme ($N(5+2i) = N(5-2i) = 29$), ali su uzajamno prosti u $\mathbb{Z}[i]$.

Sve posledice Bezuove teoreme u $\mathbb{Z}$ imaju analogna tvrđenja u $\mathbb{Z}[i]$. U nastavku će biti reči o nekima od njih.

Lema 4. *Neka $\alpha|\beta\gamma$ u $\mathbb{Z}[i]$, gde su α i β uzajamno prosti. Tada $\alpha|\gamma$.*

▲ Dokaz tvrđenja je identičan kao u slučaju celih brojeva. Neka je $\beta\gamma = \alpha\kappa$ za neko $\kappa \in \mathbb{Z}[i]$. Pošto su α i β uzajamno prosti, postoje $x, y \in \mathbb{Z}[i]$ takvi da je

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

Množenjem obe strane prethodne jednakosti sa γ dobijamo

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

Dakle, $\alpha|\gamma$. ■

Lema 5. *Ako $\alpha|\gamma$ i $\beta|\gamma$ u $\mathbb{Z}[i]$, pri čemu su α i β uzajamno prosti, onda $\alpha\beta|\gamma$.*

▲ Iz uslova $\alpha|\gamma$ i $\beta|\gamma$ u $\mathbb{Z}[i]$ sledi da postoje $a, b \in \mathbb{Z}[i]$ tako da je $\gamma = \alpha \cdot a$ i $\gamma = \beta \cdot b$. Međutim, kako je $(\alpha, \beta) = 1$, sledi da postoji $c \in \mathbb{Z}[i]$ tako da je $a = \beta \cdot c$. To znači da je $\gamma = \alpha\beta c$, odnosno važi $\alpha\beta|\gamma$. ■

Lema 6. *Ako su α, β i γ nenula elementi skupa $\mathbb{Z}[i]$, α i β su uzajamno prosti sa γ ako i samo ako je $\alpha\beta$ uzajamno prost sa γ.*

▲ Dokaz je identičan kao u slučaju celih brojeva. Ukoliko α i β nemaju zajedničke faktore sa γ, onda ni njihov proizvod neće imati zajedničke faktore sa γ. Obrnuto, ukoliko proizvod elemenata α i β nema zajedničke faktore sa γ, onda ne mogu imati ni oni ponaosob. ■

Kroz mnoštvo izloženih definicija, teorema, posledica i primera videli smo da se najveći zajednički delilac u $\mathbb{Z}[i]$ može okarakterisati na više načina, kao što je to bio slučaj i u $\mathbb{Z}$. Najveći zajednički delilac brojeva $a, b \in \mathbb{Z}, a, b \neq 0$ može se opisati kao:

- највећи од свих заједничких делилаца бројева a и b (по дефиницији)
- позитиван заједнички делилац који је дељив свим преосталим заједничким деличима
- најмања позитивна вредност израза $ax + by, (x, y \in \mathbb{Z})$
- позитивна вредности израза $ax + by, (x, y \in \mathbb{Z})$ која дели све остале вредности израза $ax + by, (x, y \in \mathbb{Z})$.

Аналогно случају целих бројева, највећи заједнички делилац α и β, $\alpha, \beta \in \mathbb{Z}[i], \alpha, \beta \neq 0$ је:

- заједнички делилац α и β чија је норма највећа у поређењу са осталим заједничким деличима (по дефиницији)
- заједнички делилац који је дељив свим преосталим заједничким деличима
- ненула вредност израза $\alpha x + \beta y$ $(x, y \in \mathbb{Z}[i])$ са најмањом могућом нормом
- ненула вредност израза $\alpha x + \beta y$ $(x, y \in \mathbb{Z}[i])$ која дели све остале вредности израза $\alpha x + \beta y (x, y \in \mathbb{Z}[i])$.

6 Jedinstvenost faktorizacije

U ovom poglavlju definisaćemo proste i složene Gausove cele, a potom i dokazati jedinstvenost faktorizacije.

Lema 7. *Za $\alpha \neq 0$, bilo koji delilac čija je norma jednaka 1 ili $N(\alpha)$ je ili jedinica, ili jedinični umnožak elementa α.*

▲ Ako $\beta|\alpha$ i $N(\beta) = 1$, onda je $\beta = \pm 1$ ili $\beta = \pm i$. Ako $\beta|\alpha$ i $N(\beta) = N(\alpha)$, razmotrimo i delilac γ, takav da je

$$\alpha = \beta\gamma.$$

Primenjujući normu na obe strane prethodne jednakosti dobijamo

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

Kako je $N(\alpha) = N(\beta)$, sledi da je $N(\gamma) = 1$. Dakle, $\gamma = \pm 1$ ili $\gamma = \pm i$, pa je $\beta = \pm\alpha$ ili $\beta = \pm i\alpha$.■

Treba primetiti da lema 7 ne tvrdi i to da su jedini Gausovi celi čija je norma jednaka $N(\alpha)$ zapravo $\pm\alpha$ i $\pm i\alpha$. Primera radi, norme elemenata $1 + 8i$ i $4 + 7i$ su 65, ali oni nisu jedan drugom jedinični umnošci.

Kada je $N(\alpha) > 1$, uvek postoji sledećih 8 očiglednih faktora elementa α: $\pm 1, \pm i, \pm\alpha, \pm i\alpha$. Njih nazivamo trivijalnim faktorima elementa α. Njima analogni bili bi trivijalni faktori ± 1 i $\pm n$ u slučaju celog broja n takvog da je $|n| > 1$. Svi ostali faktori elementa α se nazivaju netrivijalni. Imajući u vidu prethodnu lemu, norme netrivijalnih faktora su brojevi između 1 i $N(\alpha)$ (ne uključujući 1 i $N(\alpha)$).

Definicija 9. *Neka je $\alpha \in \mathbb{Z}[i]$ takav da je $N(\alpha) > 1$. Kažemo da je α složen ukoliko ima bar jedan netrivijalni faktor. Ako α ima samo trivijalne faktore, onda je on prost.*

Ukoliko je $\alpha = \beta\gamma$, uslov $1 < N(\beta) < N(\alpha)$ ekivalentan je uslovima: $N(\beta) > 1$ i $N(\gamma) > 1$. Dakle, α je predstavljen kao proizvod dva Gausova cela čije su norme veće od 1, što je netrivijalna faktorizacija elementa α. Prema tome, složen element prstena Gausovih celih je onaj element koji dopušta netrivijalnu faktorizaciju.

Na primer, trivijalna faktorizacija elementa $7 + i$ bila bi $i(1 - 7i)$. Netrivijalna je $(1 - 2i)(1 + 3i)$. Netrivijalna faktorizacija elementa 5 je $(1 + 2i)(1 - 2i)$. Interesantno je to da je 5 prost u $\mathbb{Z}$, ali je složen u $\mathbb{Z}[i]$. Čak i 2 je složen u prstenu Gausovih celih: $2 = (1 + i)(1 - i)$. Međutim, 3 je prost i u $\mathbb{Z}[i]$. Prema tome, pojedini prosti elementi skupa $\mathbb{Z}$ prosti su i u $\mathbb{Z}[i]$, dok drugi nisu.

Da bismo dokazali da je 3 prost i u $\mathbb{Z}[i]$, pretpostavićemo suprotno. Neka je 3 složen i neka je njegova netrivijalna faktorizacija

$$3 = \alpha\beta.$$

Ukoliko primenimo normu na obe strane prethodne jednakosti, dobijamo

$$9 = N(\alpha)N(\beta).$$

Pošto smo pretpostavili da je faktorizacija netrivijalna, mora važiti da je $N(\alpha) > 1$ i $N(\beta) > 1$. Dakle, $N(\alpha) = 3$. Ako je $\alpha = a + bi$, to bi značilo da je $a^2 + b^2 = 3$. Međutim, ne postoje celi brojevi a i b koji zadovoljavaju ovu jednakost, što je kontradikcija sa polaznom pretpostavkom. Dakle, 3 je prost i u $\mathbb{Z}[i]$.

Teorema 8. *Ako je norma Gausovog celog prost broj u $\mathbb{Z}$, onda je taj Gausov ceo prost u $\mathbb{Z}[i]$.*

▲ Neka $\alpha \in \mathbb{Z}[i]$ ima normu koja je prost broj u $\mathbb{Z}$, $p = N(\alpha)$. Pokazaćemo da α ima samo trivijalne faktore u $\mathbb{Z}[i]$.

Razmotrimo bilo koju faktorizaciju elementa α u $\mathbb{Z}[i]$, na primer $\alpha = \beta\gamma$. Primenom norme, dobijamo $p = N(\beta)N(\gamma)$. Ovo je jednačina u skupu pozitivnih celih brojeva, a pošto je p prost broj, $N(\beta)$ ili $N(\gamma)$ mora biti jednako 1. Prema tome, β ili γ je jedinica, pa α nema netrivijalnu faktorizaciju. Dakle, α je prost. ■

Obrnuto ne važi: ukoliko je Gausov ceo prost, njegova norma ne mora biti prost broj. Na primer, 3 ima normu 9, a 3 je prost u $\mathbb{Z}[i]$.

Teorema 9. *Svaki element α prstena Gausovih celih, takav da je $N(\alpha) > 1$, jeste proizvod prostih elemenata $\mathbb{Z}[i]$.*

▲ Primenićemo indukciju po $N(\alpha)$. Pretpostavimo da je $N(\alpha) = 2$. Tada, po teoremi 8, α je prost. Pretpostavimo sada da je $n \geq 3$ i da je svaki Gausov ceo čija je norma veća od 1 a manja od n proizvod prostih. Želimo da dokažemo da je svaki Gausov ceo čija je norma jednaka n proizvod prostih. Ukoliko ne bi postojao Gausov ceo čija je norma jednaka n, ne bismo imali šta da dokazujemo. Stoga, pretpostavićemo da takav element postoji. Ukoliko je on prost Gausov ceo, tvrđenje je dokazano. Međutim, ako je α složen Gausov ceo čija je norma jednaka n, postoji netrivijalna faktorizacija $\alpha = \beta\gamma$, pri čemu je $N(\beta), N(\gamma) < N(\alpha) = n$. Prema induktivnoj hipotezi, β i γ su proizvodi prostih u $\mathbb{Z}[i]$. Dakle, i njihov proizvod α biće proizvod prostih u $\mathbb{Z}[i]$. Time je tvrđenje dokazano. ■

Lema 8. *Neka je π prost Gausov ceo. Za Gausove cele $\alpha_1, \alpha_2, \ldots \alpha_r$, ukoliko $\pi | \alpha_1\alpha_2 \ldots \alpha_r$, onda π deli neki α_j.*

▲ Dokažimo slučaj kada je $r = 2$. Za $r > 2$ tvrđenje se dokazuje indukcijom. Neka $\pi | \alpha_1\alpha_2$. Pretpostavimo da π ne deli α_1. To znači da su π i α_1 uzajamno prosti. Ukoliko bi π i α_1 imali najveći zajednički delilac različit od jedinice, on bi morao biti jedinični umnožak elementa π, a odatle bi sledilo da $\pi | \alpha_1$, što nije tačno.

Dakle, pošto znamo da su π i α_1 uzajamno prosti, prema lemi 4, $\pi | \alpha_2$. ■

Teorema 10. *(Jedinstvenost faktorizacije) Svaki $\alpha \in \mathbb{Z}[i]$ takav da je $N(\alpha) > 1$ ima jedinstvenu faktorizaciju na proste elemente u sledećem smislu. Ukoliko je*

$$\alpha = \pi_1\pi_2 \ldots \pi_r = \pi'_1\pi'_2 \ldots \pi'_s,$$

gde su svi π_i i π'_j prosti u $\mathbb{Z}[i]$, onda je $r = s$ i nakon pogodnog preznačavanja svaki π_i je jedinični umnožak π'_i.

▲ Ukoliko je α prost, tvrđenje očigledno važi. Primenimo indukciju po $N(\alpha)$. Ukoliko je $N(\alpha) = 2$, α je prost. Pretpostavimo da je $n \geq 3$ i da svaki Gausov ceo čija je norma veća od 1 a manja od n ima jedinstvenu faktorizaciju. Pretpostavimo da postoji složen Gausov ceo čija je norma jednaka n i dokažimo da on ima jedinstvenu faktorizaciju. Razmotrimo dve proste faktorizacije elementa α kao u iskazu teoreme:

$$\alpha = \pi_1\pi_2 \ldots \pi_r = \pi'_1\pi'_2 \ldots \pi'_s.$$

Pošto $\pi_1|\alpha$, važi i da

$$\pi_1|\pi_1'\pi_2'\dots\pi_s'.$$

Prema lemi 8, $\pi_1|\pi_j'$ za neko j. Možemo pretpostaviti da je $j=1$, tj. $\pi_1|\pi_1'$. Jedini faktori elementa π_1' različiti od jedinice su njegovi jedinični umnošci, pa je $\pi_1 = u\pi_1'$, za neko $u \in \{\pm 1, \pm i\}$.
Sada možemo zapisati

$$\alpha = u\pi_1'\pi_2\dots\pi_r = \pi_1'\pi_2'\dots\pi_s'.$$

Skraćivanjem π_1' u obe faktorizacije preostaje da je

$$u\pi_2\dots\pi_r = \pi_2'\dots\pi_s'.$$

Označimo ova dva proizvoda sa β. Dakle, $N(\beta) = N(\alpha)/N(\pi_1') < N(\alpha)$. Iako je u jedinica, proizvod $u\pi_2$ je takođe prost, pa smo dobili dve faktorizacije β, sa $r-1$ faktora na levoj i $s-1$ faktora na desnoj strani. Pošto je $N(\beta) < n$, na osnovu induktivne hipoteze znamo da β ima jedinstvenu faktorizaciju, pa je $r-1 = s-1$. Posle pogodnog preznačavanja, $u\pi_2$ i π_2' su jedinični umnošci, π_2 i π_2' su jedinični umnošci, pa je svaki π_i jedinični umnožak π_i', što dokaz čini kompletnim. ■

Iako sada znamo da postoji jedinstvena faktorizacija, nije uvek lako doći do nje. Kako bismo to ilustrovali, posmatraćemo normu da bismo mogli da iskoristimo iskustvo stečeno u $\mathbb{Z}$.

Ideja je sledeća: svaka faktorizacija u $\mathbb{Z}[i]$ povlači faktorizaciju normi.

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

Uzmimo da je $\alpha = 3+4i$. Tada je $N(\alpha) = 3^2+4^2 = 25 = 5\cdot 5$. Dakle, netrivijalni faktor $4+3i$ morao bi da ima normu 5. Znamo koji Gausovi celi imaju normu 5: do na množenje jedinicom to su $1+2i$ i $1-2i$. Isprobajmo različite mogućnosti:

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

Poslednji proizvod jednak je $-\alpha$, pa je

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

Pronađimo sada faktorizaciju elementa $2319+1694i$. Norma ovog elementa je 8247397, a

$$8247397 = 17\cdot 29\cdot 16729.$$

Sada je potrebno naći Gausove cele čije su norme 17, 29 i 16729. Primetimo da važi

$$17 = 1^2+4^2,$$
$$29 = 2^2+5^2,$$
$$16729 = 40^2+123^2.$$

Dakle, možemo zaključiti da je

$$17 = (1+4i)(1-4i),$$
$$29 = (2+5i)(2-5i),$$

$$16729 = (40 + 123i)(40 - 123i).$$

Izaberimo sada po jedan faktor iz svakog od ova 3 proizvoda i odredimo njihov proizvod. Pogodan izbor daće nam

$$(1 + 4i)(2 + 5i)(40 + 123i) = -2319 - 1694i.$$

Dakle,

$$2319 + 1694i = -(1 + 4i)(2 + 5i)(40 + 123i).$$

Svaki od 3 faktora elementa $2319 + 1694i$ je prost, jer mu je norma prost broj u $\mathbb{Z}$.

7 Prosti elementi prstena Gausovih celih

U ovom poglavlju biće razmotrene neke od osobina prostih elemenata prstena Gausovih celih.

Teorema 11. *Neka je π prost element prstena Gausovih celih. Tada za neki prost ceo broj p, važi $\pi|p$.*

▲ Kako je $N(\pi) = \pi\overline{\pi}$, važiće da $\pi|N(\pi)$ u $\mathbb{Z}$. Kako je $N(\pi) > 1$, možemo zapisati $N(\pi)$ kao proizvod pozitivnih prostih brojeva u $\mathbb{Z}$ na sledeći način:

$$N(\pi) = p_1 p_2 ... p_r.$$

Kako $\pi|N(\pi)$ u $\mathbb{Z}$, i π je prost u $\mathbb{Z}[i]$, prema lemi 8 postoji j takvo da $\pi|p_j$. ■

Prva tri prosta prirodna broja mogu se u $\mathbb{Z}[i]$ rastaviti na sledeći način:

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

$$3 = 3$$

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

Teorema 12. *Prost nenegativan ceo broj p je rastavljiv u $\mathbb{Z}[i]$ ako i samo ako je on suma dva kvadrata.*

▲ Ako je nenegativan prost ceo broj p rastavljiv u $\mathbb{Z}[i]$, neka je njegova netrivijalna faktorizacija $p = \alpha\beta$. Primenjujući normu na poslednju jednakost, dobijamo $p^2 = N(\alpha)N(\beta)$. Kako je faktorizacija netrivijalna i $p > 0$, mora biti $N(\alpha) = p$. Tada, ukoliko je $\alpha = a + bi$, sledi da je $p = a^2 + b^2$.

Pretpostavimo sada da je prost nenegativan ceo broj p suma dva kvadrata, $p = a^2 + b^2$. Tada u $\mathbb{Z}[i]$ dobijamo netrivijalnu faktorizaciju

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

pa je p rastavljiv u $\mathbb{Z}[i]$. ■

Prvih 5 celih brojeva koji su suma dva kvadrata su: $2, 5, 13, 17, 29$:

$$2 = 1^2 + 1^2, 5 = 1^2 + 2^2, 13 = 2^2 + 3^2, 17 = 1^2 + 4^2, 29 = 2^2 + 5^2.$$

Svaki od njih je rastavljiv u $\mathbb{Z}[i]$. Na primer,

$$29 = (2+5i)(2-5i).$$

Faktorizacija broja 2 je posebna, jer su njegovi faktori jedan drugom jedinični umnošci:

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

Dakle,

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

8 Primene osobina prstena Gausovih celih na aritmetiku u $\mathbb{Z}$

Primene svojstava prstena Gausovih celih na aritmetiku u $\mathbb{Z}$ su brojne, a uglavnom su usko povezane sa sumom dva kvadrata. Ukoliko pogledamo jednakost

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

gde je suma dva kvadrata na levoj, a faktorizacija u $\mathbb{Z}[i]$ na desnoj strani, videćemo koliko $\mathbb{Z}[i]$ može biti koristan u rešavanju problema u vezi sa sumom dva kvadrata.

Neki od problema kojima ćemo se baviti u ovom odeljku su:

- prost broj koji je suma dva kvadrata može se tako predstaviti na jedinstven način,
- klasifikacija rešenja jednačine $a^2 + b^2 = c^3$,
- jedino celobrojno rešenje jednačine $y^2 = x^3 - 1$ je $(x, y) = (1, 0)$,
- sistematično određivanje celih brojeva koji su suma dva kvadrata na više načina,
- generisanje Pitagorinih trojki.

8.1 Prost broj koji je suma dva kvadrata

Teorema 13. *Ukoliko je prost broj p suma dva kvadrata, onda je njegovo predstavljanje na taj način jedinstveno: $p = a^2 + b^2$, gde su celi brojevi a i b jedinstveni do na redosled i znak.*

▲ Neka je $p = a^2 + b^2$, gde su $a, b \in \mathbb{Z}$. Tada možemo zaključiti da se p u $\mathbb{Z}[i]$ faktoriše na sledeći način:

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

Pošto i $a + bi$ i $a - bi$ imaju normu jednaku p, a p je prost broj u $\mathbb{Z}$, sledi da su $a + bi$ i $a - bi$ prosti u $\mathbb{Z}[i]$. Ukoliko bi postojala druga reprezentacija $p = c^2 + d^2$, tada bi bilo

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

gde je $c \pm di$ prost u $\mathbb{Z}[i]$. Iz jedinstvenosti faktorizacije sledi da je

$$a + bi = u(c + di),$$

ili

$$a + bi = u(c - di)$$

za neku jedinicu u.

Jedina razlika između $c + di$ i $c - di$ je znak koeficijenta ispred i, a mi svakako želimo da dokažemo da su a i b jedinstveno određeni do na znak i redosled, pa možemo posmatrati samo slučaj

$$a + bi = u(c + di).$$

Ukoliko je $u = 1$, onda je $c = a$ i $d = b$. Ako je $u = -1$, onda je $c = -a$ i $d = -b$. Ukoliko je $u = i$, onda je $c = b$ i $d = -a$, a ako je $u = -i$, onda je $c = -b$ i $d = a$. Dakle, a i b su jedinstveno određeni, do na znak i redosled.■

Primetimo da poslednje tvrđenje za složene brojeve ne važi. Na primer, $50 = 1^2 + 7^2 = 5^2 + 5^2$, a i $65 = 1^2 + 8^2 = 4^2 + 7^2$. Neki od prostih brojeva koji se mogu napisati kao suma dva kvadrata su

$$2 = 1^2 + 1^2, 5 = 1^2 + 2^2, 13 = 2^2 + 3^2, 17 = 1^2 + 4^2, 29 = 2^2 + 5^2.$$

8.2 Rešavanje jednačine $a^2 + b^2 = c^3$

Naredna primena kojom ćemo se baviti jeste rešavanje jednačine $a^2 + b^2 = c^3$, $a, b, c \in \mathbb{Z}$, gde važi $(a, b) = 1$.

Teorema 14. *Za trojke (a, b, c), gde važi $a, b, c \in \mathbb{Z}$ i $(a, b) = 1$, celobrojna rešenja jednačine $a^2 + b^2 = c^3$ opisana su parametarskim formulama*

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

gde važi $m, n \in \mathbb{N}$, $(m, n) = 1$ i m i n nisu iste parnosti. Različit izbor brojeva m i n daje različita rešenja (a, b, c).

▲ Kako je $(a, b) = 1$, a i b nisu oba parna. Ako bi oba bila neparna, bilo bi

$$c^3 \equiv_8 1 + 1 \equiv_8 2,$$

a 2 nije kvadrat po modulu 8. Dakle, jedan od brojeva a i b je paran, a drugi je neparan. Broj c je neparan. U $\mathbb{Z}[i]$ $a^2 + b^2 = c^3$ možemo zapisati na sledeći način:

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

Dokažimo da su $a + bi$ i $a - bi$ uzajamno prosti. Ako bi δ bio zajednički delilac, onda bi važilo $\delta | 2a, \delta | 2b, \delta | c^3$. Primenjujući normu dobijamo da je $N(\delta)$ faktor svakog od brojeva $4a^2, 4b^2$ i c^6. Pošto je c neparan, $N(\delta)$ je neparan, pa $N(\delta)$ deli a^2 i b^2. Brojevi a i b su uzajamno prosti, pa je $N(\delta) = 1$, odnosno $\delta = \pm 1$ ili $\delta = \pm i$. Prema tome, $a + bi$ i $a - bi$ su uzajamno prosti.

Pošto su $a + bi$ i $a - bi$ uzajamno prosti u $\mathbb{Z}[i]$, a njihov proizvod je potpun kub u $\mathbb{Z}[i]$, na osnovu jedinstvenosti faktorizacije sledi da su i $a + bi$ i $a - bi$ kubovi do na množenje jedinicom. Na primer,

$$a + bi = u\alpha^3,$$

gde $u \in \{\pm 1, \pm i\}$. Međutim, svaka jedinica je kub jedinice:

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

Prema tome, $a + bi$ je potpun kub. Možemo zapisati

$$a + bi = (m + ni)^3,$$

za neke cele brojeve m i n. Nakon kubiranja i izjednačavanja realnih i imaginarnih delova, dobijamo

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

Bilo koji zajednički faktor brojeva m i n bi na osnovu prethodnih formula bio zajednički faktor i za a i b, pa zaključujemo da važi $(m,n)=1$. Ukoliko bi m i n bili iste parnosti, na osnovu prethodnih formula a i b bi bili parni, što nije tačno, pa možemo zaključiti i da m i n nisu iste parnosti. Takođe,

$$c^3=(a+bi)(a-bi)=(m+ni)^3(m-ni)^3=(m^2+n^2)^3.$$

Odatle sledi da je

$$c=m^2+n^2.$$

Obrnuto, ako je $(m,n)=1$ i m i n nisu iste parnosti, onda a,b,c definisani na sledeći način

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

zadovoljavaju jednačinu $a^2+b^2=c^3$ i $a+bi=(m+ni)^3$.

Jedinstvenost izbora m i n proističe iz jednakosti $a+bi=(m+ni)^3$. ■

8.3 Rešavanje jednačine $y^2=x^3-1$

Teorema 15. *Jedini brojevi $x,y\in\mathbb{Z}[i]$ koji zadovoljavaju jednakost $y^2=x^3-1$ su $(x,y)=(1,0)$.*

▲ Očigledno je da uređeni par $(x,y)=(1,0)$ zadovoljava jednakost $y^2=x^3-1$. Dokažimo da je to jedino rešenje. Polaznu jednačinu zapisaćemo u obliku

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

što se može zapisati i kao

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

Ideja je nadalje ista kao u prethodnom dokazu. Ukoliko su faktori na desnoj strani jednakosti uzajamno prosti u $\mathbb{Z}[i]$, budući da je njihov proizvod kub, svaki od njih takođe mora biti kub, do na množenje jedinicom. Svaka jedinica je kub jedinice:

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

pa ako su $y+i$ i $y-i$ uzajamno prosti, oni su kubovi.

Kako bismo pokazali da su $y+i$ i $y-i$ uzajamno prosti, pretpostavimo da je δ njihov zajednički delilac. Tada δ deli i njihovu razliku, pa $\delta|2i$. Kako je $2i=(1+i)^2$, na osnovu jedinstvenosti faktorizacije zaključujemo da δ može biti 1, $1+i$ ili $(1+i)^2$, do na množenje jedinicom.

Ukoliko δ nije jedinica, δ je deljivo sa $1+i$, pa $(1+i)|x^3$. Primenjujući normu, dobijamo da $2|x^6$, pa je x paran broj. Tada je $y^2+1=x^3\equiv_4 0$, pa $y^2\equiv_4 -1$. Međutim, -1 ne može biti kvadrat po modulu 4. Dakle, δ je jedinica.

Sada kada znamo da su $y+i$ i $y-i$ uzajamno prosti, možemo zapisati

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

za neke $m,n\in\mathbb{Z}$. Nakon kubiranja i izjednačavanja realnih i imaginarnih delova, dobijamo da važi

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

Iz druge jednakosti možemo zaključiti da je $n=\pm 1$. Ako je $n=1$, onda je $1=3m^2-1$, pa je $3m^2=2$, što nema celobrojna rešenja. Ako je $n=-1$, onda je $1=-(3m^2-1)$, pa je $m=0$. Dakle, $y=0$, pa je $x=1$. ■

8.4 Predstavljanje celog broja u obliku sume dva kvadrata na više načina

Na kraju ovog poglavlja vratićemo se na prvu primenu, a to je suma dva kvadrata. Videli smo da se prost broj koji je suma dva kvadrata na jedinstven način može prikazati u tom obliku, što u slučaju složenih brojeva ne važi.

Dakle, možemo iskoristiti aritmetiku u $\mathbb{Z}[i]$ kako bismo na sistematičan način konstruisali cele brojeve koji se mogu predstaviti kao suma dva kvadrata na više načina.

Primer 19. *Razmotrićemo faktorizaciju brojeva* 5 *i* 13 *u* $\mathbb{Z}[i]$*:*

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

Tada je

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

što daje jednakost

$$65 = (-4+7i)(-4-7i) = (8+i)(8-i).$$

Dakle,

$$65 = 4^2 + 7^2 = 8^2 + 1^2.$$

Primer 20. *U narednom primeru, iskoristimo sledeće jednakosti*

$$5 = (1+2i)(1-2i),$$
$$10 = (1+3i)(1-3i).$$

Kombinujući po jedan faktor broja 5 *i jedan faktor broja* 10 *formirajmo proizvode:*

$$(1+2i)(1+3i) = -5+5i,$$
$$(1+2i)(1-3i) = 7-i$$
$$(1-2i)(1+3i) = -5-5i$$
$$(1-2i)(1-3i) = 7+i.$$

Dobili smo dva para konjugovanih Gausovih celih. Primenjujući normu, dobijamo

$$N(1+2i)N(1+3i) = N(-5+5i) = 5^2 + 5^2,$$
$$N(1+2i)N(1-3i) = N(7-i) = 1^2 + 7^2$$
$$N(1-2i)N(1+3i) = N(-5-5i) = 5^2 + 5^2$$
$$N(1-2i)N(1-3i) = N(7+i) = 1^2 + 7^2.$$

Dakle,

$$50 = 5^2 + 5^2 = 1^2 + 7^2.$$

Primer 21. *Za kraj, pronađimo ceo broj koji se može zapisati kao suma kvadrata na tri različita načina. Koristićemo proste brojeve* 5, 13 *i* 17. *U* $\mathbb{Z}[i]$ *važi*

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

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

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

Razmotrimo sledeće proizvode:

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

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

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

Primenimo normu na prethodne tri jednakosti:

$$N(1+2i)N(2+3i)N(1+4i) = 5\cdot 13\cdot 17 = N(-32-9i) = 9^2+32^2,$$

$$N(1-2i)N(2+3i)N(1+4i) = 5\cdot 13\cdot 17 = N(12+31i) = 12^2+31^2,$$

$$N(1+2i)N(2-3i)N(1+4i) = 5\cdot 13\cdot 17 = N(4+33i) = 4^2+33^2.$$

Dakle, vidimo da je

$$1105 = 9^2+32^2 = 12^2+31^2 = 4^2+33^2$$

.

8.5 Generisanje Pitagorinih trojki pomoću prstena $\mathbb{Z}[i]$

U ovom odeljku biće prikazana primena jedinstvenosti faktorizacije u $\mathbb{Z}[i]$ radi generisanja Pitagorinih trojki.

Pretpostavimo da je uređena trojka (x,y,z) rešenje jednačine $x^2+y^2=z^2$, pri čemu su x i y uzajamno prosti i $x,y,z\in\mathbb{Z}$. Odatle sledi da je jedan od brojeva x i y paran, a drugi neparan. Zapišimo jednačinu $x^2+y^2=z^2$ u $\mathbb{Z}[i]$ na sledeći način:

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

Tvrdimo da su Gausovi celi $x+iy$ i $x-iy$ uzajamno prosti. Zaista, pretpostavimo da je $d\in\mathbb{Z}[i]$ nerastavljiv delilac elemenata $x+iy$ i $x-iy$. U tom slučaju moralo bi da važi: $d|2x, d|2y$. Ukoliko bi važilo da $2|d$, to bi bilo protivno pretpostavci da je z neparan. Dakle, neka važi $d|x, d|y$. Primenjujući normu zaključujemo da u tom slučaju mora važiti i $N(d)|x^2, N(d)|y^2$. Međutim, x i y su uzajamno prosti. Sledi da su $x+iy$ i $x-iy$ uzajamno prosti u $\mathbb{Z}[i]$. Dakle, $x+iy = u(a+ib)^2$, za neku jedinicu u i neke $a,b\in\mathbb{Z}$. Prema tome, $x+iy = u(a^2-b^2+2abi)$. Uzimajući $u=1$ dobijamo $x=a^2-b^2, y=2ab$, pa je $z=a^2+b^2$. Uzimajući druge jedinične vrednosti za u dobili bismo slične izraze.

Dakle, $x=a^2-b^2, y=2ab, z=a^2+b^2$ zadovoljavaju jednačinu $x^2+y^2=z^2$ za svako $a,b\in\mathbb{Z}$. Prema tome, pronašli smo sve Pitagorine trojke.

9 Zaključak

Ovaj rad ima za cilj da čitaoca upozna sa prstenom Gausovih celih i osnovnim konceptima sa njim u vezi i da pruži dobru osnovu za dalje proučavanje ove tematike.

Prsten Gausovih celih je primer prstena sa kojim se studenti matematike upoznaju na informativnom nivou, bez dubljeg zalaženja u njegove osobine, značaj i primenu. Poznavanje koncepata opisanih u ovom radu ima široku primenu, a opisani su samo neki od primera primene na aritmetiku u $\mathbb{Z}$. U ovom radu pokazano je kako se prsten Gausovih celih $\mathbb{Z}[i]$ može iskoristiti za dokazivanje činjenice da se svaki prost broj koji je suma dva kvadrata na jedinstven način može predstaviti u tom obliku. Takođe, prikazano je kako nam novo znanje može pomoći u rešavanju jednačine oblika $a^2 + b^2 = c^3$, ali i jednačine $y^2 = x^3 - 1$. Najzad, poznavanje prstena Gausovih celih može se iskoristiti za sistematično generisanje brojeva koji se mogu zapisati kao suma dva ili više kvadrata.

Radi još detaljnijeg upoznavanja sa temom i mogućnostima njenog širenja čitaocu se preporučuje proučavanje navedene literature.

Literatura

[1] Campbell Duff, *An open door to number theory*, American Mathematical Society, 2018.

[2] Conrad Keith, *The Gaussian integers*, https://kconrad.math.uconn.edu/math5230f12/handouts/Zinotes.pdf, 2017.

[3] Andreescu Titu, Andrica Dorin, Cucurezeanu Ion, *An introduction to Diophantine equations - A problem-based approach*, Birk, 2011.

[4] Grulović Milan, *Predavanja iz Algebre 4 (Teorija prstena i polja i Teorija Galoa)*, Departman za matematiku i informatiku (PMF Novi Sad), 2017.

[5] Stanić Marija, Ikodinović Nebojša, *Teorija brojeva - zbirka zadataka*, Zavod za udžbenike i nastavna sredstva Beograd, 2004.

[6] Cohen Henri, *Explicit methods for solving Diophantine equations*, Tucson, Arizona Winter School, 2006.

[7] Cohen Henri, *Number Theory, Volume I: Tools and Diophantine Equations*, Springer, 2007.