Универзитет у Београду
Математички факултет

Мастер рад

ГАУСОВИ ЦЕЛИ И ПРИМЕНЕ

Студент:
Сања Селенић

Ментор:
Зоран Петровић

Београд, 2014.

Садржај

1 Увод

• За елемент a прстена K кажемо да је у том прстену леви, односно десни делитељ нуле, ако за бар једно $b \neq 0$ важи

$$ab = 0, \text{ односно } ba = 0.$$

Комутативни прстени који немају правих делитеља нуле називају се *областима целих* или *доменима*.

• Елемент a прстена K је *инверзибилан*, односно *регуларан*, ако једначине

$$\begin{aligned} a \cdot x &= 1, \\ x \cdot a &= 1 \end{aligned}$$

имају тачно једно заједничко решење у K. То решење се назива инверзом од a у прстену K, и обележава се a^{-1}.

• Елементи a и b прстена K су *придружени*, у запису $a \sim b$, ако је $a = \alpha b$ за неку јединицу α прстена K.

• За два елемента $a, b \in K$ важи да $b \neq 0$ дели a ($b \mid a$) ако постоји $q \in K$ такво да је $a = bq$.

• За елемент p прстена K кажемо да је *атом (нерастављив)* ако није 0 или инверзибилан и ако за сваки a, $b \in K$ важи

$$p = ab \;\Rightarrow\; a \in K^* \text{ или } b \in K^*.$$

• Елемент p прстена K је *прост* ако није 0 или инверзибилан и ако за сваки a, $b \in K$ важи

$$p \mid ab \;\Rightarrow\; p \mid a \text{ или } p \mid b.$$

• Broj c је заједнички делилац за a и b ($c \mid a, b$) ако $c \mid a$ и $c \mid b$. Број d је највећи заједнички делилац за a и b ако за сваки $c \in K$ важи

$$c \mid a, b \;\Leftrightarrow\; c \mid d.$$

Уколико два елемента имају више највећих заједничких делиоца, они морају бити придружени. За два елемента прстена K кажемо да су *узајамно прости* ако имају једино јединице за заједничке делиоце.

• Комутативан домен K је *атомичан* ако је у њему сваки елемент производ коначно много атома, односно ако има бар једну факторизацију

$$a = a_1 a_2 \dots a_n$$

при чему је сваки a_i атом у K, $i = 1, 2, \dots, n$.

• Комутативан домен K је са *једнозначном факторизацијом*, ако је атомичан и ако су атомичне факторизације његових елемената једнозначне.

• Област целих K је са једнозначном факторизацијом ако и само ако је атомичан и ако се у њему прости и нерастављиви елементи подударају.

Лема 1.
Сваки прост елемент p датог комутативног домена K је прост и у прстену полинома $K[X]$.

Лема 2.
Ако је $\mathbb{K}$ поље разломака над комутативним доменом K са једнозначном факторизацијом, примитиван полином u је атом у прстену $K[X]$, ако и само ако је то и у прстену $\mathbb{K}[X]$.

Теорема 1.
Ако је K домен са једнозначном факторизацијом, онда је то и прстен полинома $K[X]$.

Доказ.
Најпре ћемо показати да је прстен $K[X]$ атомичан. Нека је $\mathbb{K}$ поље разломака над K, и нека је f полином из $K[X]$. Тада он има факторизацију $f = cq_1q_2 \cdots q_n$, при чему је c из $\mathbb{K}$, а полиноми q_1, q_2, $\cdots$, q_i су примитивни полиноми над K, који су атоми у $\mathbb{K}[X]$. По Леми 2 следи да су они атоми и у $K[X]$. Из примитивности полинома, мора бити $c \in K$. На основу Леме 1, следи да је прстен $K[X]$ атомичан.

Сада ћемо показати да је у прстену $K[X]$ сваки атом прост. Нека је f атом из $K[X]$. Претпоставимо да дели производ gh. Ако је f у K, он је прост, па је прост и у $K[X]$. Уколико f није у K, он је примитиван полином који је атом у $\mathbb{K}[X]$. Самим тим, он је и прост у $\mathbb{K}[X]$, тако да f дели g или f дели h у $\mathbb{K}[X]$.

Претпоставимо да f дели g. Тада постоји полином q из $\mathbb{K}[X]$, такав да је $g = fq$. Како је g из $K[X]$, важи да је $g = cq_1 f$, при чему је c из K, а q_1 примитиван полином над K. Према томе, f дели g у $K[X]$, па је f прост.

□

• Главноидеалски домени

Комутативни домени у којима су сви идеали главни називају се *главним* или *главноидеалским доменима.*

Теорема 2.
Сваки главни домен K је са једнозначном факторизацијом.

Доказ.
Нека је a произвољан елемент из K који није инверзибилан или нула. Потребно је проверити да ли он може да се запише као производ атома. Уколико a није атом, постоји права факторизација $a = p_1 a_1$. Даље, уколико a_1 није атом, постоји факторизација $a_1 = p_2 a_2$, и тако даље... За главне идеале прстена K важиће:

$$aK \subset a_1 K \subset a_2 K \subset ... \subset a_n K \subset ...$$

Нека је I унија ових идеала. Како је K главноидеалски, постоји елемент p из K, такав да је $I = pK$. Како је I унија идеала, p мора бити елемент неког од њих. Нека p припада идеалу $a_n K$. Тада важи:

$$pK \subset a_n K \subset I = pK$$

односно, следи да је $a_n K = pK$. Према томе, $a_n K$ је последњи члан ланца. Заиста, уколико би постојало a_{n+1}, такво да је $a_n = p_{n+1} a_{n+1}$, односно ако је $a_n K \subset a_{n+1} K \subset pK$, следило би да $a_n K = a_{n+1} K$. Тада би a_n и a_{n+1} били придружени елементи, односно факторизација $a_n = p_{n+1} a_{n+1}$ не би била права.

Показали смо да је сваки ненула неинверзибилан елемент из K дељив атомом. Сада ћемо показати да a има атомичну факторизацију. Нека је $a = p_1 a_1$, за неки атом p_1. Ако је a_1 атом, процес је готов, у супротном $a_1 = p_2 a_2$, за неки атом p_2.

Овај процес се мора завршити, тако да a може да се представи као производ атома из K.

Потребно је још показати да су у домену K сви атоми прости. Нека је q атом, такав да дели ab. Тада он или дели a или је $(q,a)=1$. У другом случају, постоје x и y такви да је $qx+ay=1$. Множењем једначине са b добија се $qxb+ayb=b$. Како q дели леву страну једначине, оно мора делити и десну, односно q дели b. Према томе, q је прост.

□

- Еуклидски домени

Комутативан прстен K је *еуклидски* ако је област целих и ако постоји бар једна функција $\sigma : K \longrightarrow \mathbf{N}_0$ која задовољава следећа два услова:

1° $ab \neq 0 \Rightarrow \sigma(ab) \geq \sigma(a)$

2° за свако $a, b \in K$, $b \neq 0$, постоје $q, r \in K$ за које је $a = bq+r$, $\sigma(r) < \sigma(b)$

Из првог услова следи да за свако $b \neq 0$ важи $\sigma(b) \geq \sigma(1)$, јер је $\sigma(b) = \sigma(b \cdot 1) \geq \sigma(1)$. Из другог услова, за $a = 0$ и $b = 1$, следи да мора бити $r = 0$, па је тада

$$\sigma(0) < \sigma(1) \leq \sigma(a),$$

за свако $a \neq 0$ из K. Подразумеваћемо да је $\sigma(0) = 0$ и $\sigma(1) = 1$. За свако $a \in K$, важи да је

$$\sigma(a) = 1 \Leftrightarrow a \in K^*.$$

Уколико је $a \in K^*$, тада је $1 = aa^{-1}$. У том случају важи да је $\sigma(1) = \sigma(aa^{-1}) \geq \sigma(a)$. Дакле, мора важити да је $\sigma(a) = 1$. Обрнуто, уколико је $\sigma(a) = 1$, постоје q и r такви да је $1 = aq+r$, $\sigma(r) < 1$. Тада је $r = 0$, па је $a \in K^*$.

Елементи q и r за које је $a = bq + r$, $\sigma(r) < \sigma(b)$, називају се еуклидским количником и остатком при еуклидском дељењу елемента a са b. Остатак може да се обележи као $r = \rho(a, b)$.

Теорема 3.
Нека је K еуклидски домен. За свако a и $b \neq 0$ из K постоји систем $(a, b) = [a_0, a_1, \ldots, a_k]$ елемената из K, у коме је $a_0 = a$, $a_1 = b$,

$$a_r = \rho(a_{r-2}, a_{r-1}) \ (2 \leq r \leq k)$$

као и $\rho(a_{k-1}, a_k) = 0$. Свако a_r је облика $pa + qb$, и a_k је управо највећи заједнички делилац од a и b.

У еуклидским доменима атоми и прости елементи се подударају. То се доказује на исти начин, као на крају Теореме 2.

Теорема 4.
Сваки еуклидски прстен је са јединственом факторизацијом.

Доказ.
Нека је прстен K еуклидски, и нека је a произвољан елемент из K. Ако је a атом, он је са јединственом факторизацијом. Ако a није атом, онда може да се запише и облику $a = a_1 b_1$. Уколико су a_1 и b_1 атоми, доказ је завршен. У супротном, уколико неки од њих није атом, на пример b_1, он може да се запише у облику $b_1 = a_2 b_2$. Тада је $a = a_1 a_2 b_2$. Овај поступак се наставља све док се не добије атомична факторизација елемента a. Овај процес мора да се заврши. То ће следити из особине функције σ:

$$\sigma(ab) = \sigma(a) \ \Leftrightarrow \ b \text{ инвертибилан.}$$

Нека је факторизација елемента $a = a_1 a_2 \ldots a_n$. Обележимо са $b = a_2 \ldots a_n$. Како b није инверз (није атом), важиће:

$$\sigma(a) = \sigma(a_1 a_2 \ldots a_n) > \sigma(a_2 \ldots a_n) > \sigma(a_3 \ldots a_n) > \ldots > \sigma(a_n)$$

Процес се мора завршити, па је a производ атома. Дакле, еуклидски прстен K је атомичан, а како се у њему прости и атоми подударају, следи да је он са јединственом факторизацијом. □

Да је сваки еуклидски прстен са јединственом факторизацијом, може да се докаже и на други начин, преко главноидеалских домена. Показаћемо да је сваки еуклидски прстен главни, па

ће на основу Теореме 2 следити да је он и са једнозначном факторизацијом.

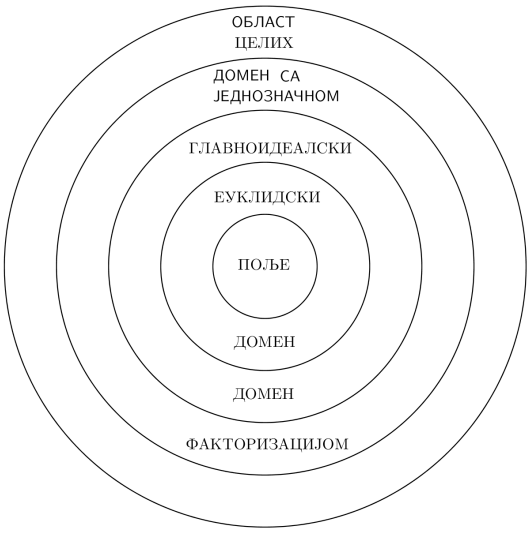
Нека је I произвољан идеал прстена K. Скуп који је облика $\{\sigma(a) : a \in I, a \neq 0\}$ је непразан подскуп скупа природних бројева $\mathbf{N}$. Према томе, он има најмањи елемент , на пример $\sigma(b) = m$, где је $b \neq 0$ из I. Како је b из I, јасно је да је $bK \subset I$.

Нека је $a \in I$. Тада, постоје q, r такви да је

$$a = bq + r, \;\; \sigma(r) < \sigma(b) = m.$$

Како су a и b из I, тада је и $r = a - bq$ из I. Из $\sigma(r) < \sigma(b) = m.$, следи да мора бити $r = 0$. Према томе $a = bq$, одакле се види да је $I \subset bK$. Према томе, идеал $I = bK$ је главни.

• У еуклидским доменима, уколико прост број дели производ ab, он мора делити или a или b.



Слика 1: Венов дијаграм домена

2 Прстен $\mathbf{Z}[\sqrt{n}]$

Прстен целих бројева $\mathbf{Z}$ је прстен са једнозначном факторизацијом. На основу Теореме 1 важи да ће такав бити и прстен полинома $\mathbf{Z}[x]$. Прстен целих бројева $\mathbf{Z}$ је и главноидеалски. Међутим, у $\mathbf{Z}[x]$ постоји идеал који није главни, тако да прстен полинома $\mathbf{Z}[x]$ није главноидеалски. Такав је, на пример идеал $I = \langle 2, X \rangle$.

Нас ће занимати шта се дешава са конструкцијама облика $\mathbf{Z}[x]/P$, где је P идеал прстена $\mathbf{Z}[x]$. Уколико је P прост, тада је прстен $\mathbf{Z}[x]/P$ област целих.

Нека је $K = \mathbf{Z}[x]$, прстен полинома са коефицијентима из $\mathbf{Z}$ и $P = \langle x^2 - n \rangle = \{(x^2 - n)q : q \in \mathbf{Z}[x]\}$. Уколико n није квадрат неког броја, полином $x^2 - n$ је нерастављив над $\mathbf{Z}$.

Елементи прстена $\mathbf{Z}[x]/\langle x^2 - n \rangle$ су облика $p(x) + \langle x^2 - n \rangle$, где је степен од $p(x)$ мањи од степена $x^2 - n$. Дакле, елементи прстена $\mathbf{Z}[x]/\langle x^2 - n \rangle$ су облика $ax + b + \langle x^2 - n \rangle$ што може да се запише као:

$$(a + \langle x^2 - n \rangle) \cdot (x + \langle x^2 - n \rangle) + (b + \langle x^2 - n \rangle).$$

Ради лакшег записа, користићемо ознаке:

$$\begin{aligned} \bar{a} &= a + \langle x^2 - n \rangle \\ \bar{b} &= b + \langle x^2 - n \rangle \\ \alpha &= x + \langle x^2 - n \rangle. \end{aligned}$$

На тај начин је одређен прстен $\mathbf{Z}[\alpha] = \{a\alpha + b : a, b \in \mathbf{Z}\}$.

Специјално, уколико је $\alpha^2 = n + \langle x^2 - n \rangle$, где n није квадрат неког целог броја, тада је $\alpha = \sqrt{n} + \langle x^2 - n \rangle$. У том случају, прстен $\mathbf{Z}[\alpha]$ облика

$$\mathbf{Z}[\sqrt{n}] = \{a\sqrt{n} + b : a, b \in \mathbf{Z}\}.$$

Прстен $\mathbf{Z}[\sqrt{n}]$ је потпрстен прстена $\mathbf{C}$. Прстен $\mathbf{Z}[\sqrt{n}]$ садржи 0 и 1:

$$0 = 0 + 0\sqrt{n}$$
$$1 = 1 + 0\sqrt{n},$$

и затворен је за сабирање и множење

$$\begin{aligned}(a + b\sqrt{n}) + (x + y\sqrt{n}) &= (a + x) + (b + y)\sqrt{n},\\ (a + b\sqrt{n})(x + y\sqrt{n}) &= (ax + nby) + (ay + bx)\sqrt{n}.\end{aligned}$$

Како су a, b, x и y цели бројеви, тада је и вредност израза у заградама целобројна. Дакле, прстен $\mathbf{Z}[\sqrt{n}]$ је потпрстен поља, па је он интегрални домен.

Прстен $\mathbf{Z}[\sqrt{n}]$ не мора бити са једнозначном факторизацијом. У наредном делу ћемо видети да прстен $\mathbf{Z}[\sqrt{-5}]$ није са јединственом факторизацијом, док прстен Гаусових целих $\mathbf{Z}[\sqrt{i}]$ јесте.

2.1 Особине прстена $\mathbf{Z}[\sqrt{n}]$

Нека је α произвољан елемент прстена $\mathbf{Z}[\sqrt{n}]$. Тада он може да се запише у облику $\alpha = a + b\sqrt{n}$, при чему су a и b из $\mathbf{Z}$. Конјугат броја α је $\bar{\alpha} = a - b\sqrt{n}$. Норма броја α је функција $N\colon \mathbf{Z}[\sqrt{n}] \to \mathbf{Z}$, дефинисана са:

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

Теорема 5.
Норма је мултипликативна, за произвољне α и β из $\mathbf{Z}[\sqrt{n}]$, важи

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

Доказ.
Нека су $\alpha = a + b\sqrt{n}$ и $\beta = c + d\sqrt{n}$ произвољни елементи прстена $\mathbf{Z}[\sqrt{n}]$. Тада је њихов производ облика

$$\alpha\beta = (a + b\sqrt{n})(c + d\sqrt{n}) = (ac + nbd) + \sqrt{n}(ad + bc).$$

Нормирањем и сређивањем израза, добија се

$$\begin{aligned} N(\alpha\beta) &= (ac+nbd)^2 - n(ad+bc)^2 \\ &= a^2c^2 + 2abcdn + n^2b^2d^2 - na^2d^2 - 2abcdn - nb^2c^2 \\ &= a^2c^2 + n^2b^2d^2 - na^2d^2 - nb^2c^2 \\ &= c^2(a^2-nb^2) - nd^2(a^2-nb^2) \\ &= (a^2-nb^2)(c^2-nd^2) \\ &= N(\alpha)N(\beta). \end{aligned}$$

□

Јединице прстена $\mathbf{Z}[\sqrt{n}]$ су елементи чија је норма једнака 1, односно они елементи $a+b\sqrt{n}$, за које важи

$$a^2 - nb^2 = 1.$$

Пример 1.
Одредити све јединице прстена $\mathbf{Z}[\sqrt{-5}]$.

Решење:
Нека је $\alpha = a + b\sqrt{-5}$ произвољан елемент прстена $\mathbf{Z}[\sqrt{-5}]$. Његова норма је $N(\alpha) = a^2 + 5b^2$. Да би α била јединица прстена $\mathbf{Z}[\sqrt{-5}]$, мора бити $N(\alpha) = 1$, односно $a^2 + 5b^2 = 1$. То је испуњено за $a = \pm 1$, $b = 0$. Дакле, јединице прстена $\mathbf{Z}[\sqrt{-5}]$ су ± 1. Како су 1 и -1 једине јединице, придружени елементи елементу α прстена $\mathbf{Z}[\sqrt{-5}]$ су α и $-\alpha$.

△

Уколико је функција норме N еуклидска функција, тада је прстен $\mathbf{Z}[\sqrt{n}]$ еуклидски. Прстен $\mathbf{Z}[\sqrt{n}]$ је еуклидски за одређене вредности од n. Пре него што одредимо те вредности, увешћемо неке нове термине.

Нека су $a+b\sqrt{n}$ и $c+d\sqrt{n}$ два произвољна елемента прстена $\mathbf{Z}[\sqrt{n}]$. Количник та два броја ће бити:

$$\frac{a+b\sqrt{n}}{c+d\sqrt{n}} = \frac{(a+b\sqrt{n})(c-d\sqrt{n})}{(c+d\sqrt{n})(c-d\sqrt{n})} = \frac{ac-nbd}{c^2-nd^2} + \frac{bc-ad}{c^2-nd^2}\sqrt{n}$$

Обележимо ова два разломка са α и β. Видимо да је количник два елемента из $\mathbf{Z}[\sqrt{n}]$ облика $\alpha+\beta\sqrt{n}$, при чему су α, $\beta \in \mathbf{Q}$,

односно припада $\mathbf{Q}[\sqrt{n}] = \{a + b\sqrt{n} : a, b \in \mathbf{Q}\}$.

Прстен $\mathbf{Q}[\sqrt{n}]$ је количнички прстен $\mathbf{Q}[x]/\langle x^2 - n\rangle$, при чему n није квадрат неког броја из $\mathbf{Q}$. Како је полином $x^2 - n$ нерастављив над $\mathbf{Q}[x]$, прстен $\mathbf{Q}[x]/\langle x^2 - n\rangle$ је заправо поље.

Норма броја $a + b\sqrt{n} \in \mathbf{Q}[\sqrt{n}]$ је функција $N : \mathbf{Q}[\sqrt{n}] \longrightarrow \mathbf{Q}$, дефинисана са $N(a + b\sqrt{n}) = a^2 - nb^2$. Као и у случају $\mathbf{Z}[\sqrt{n}]$, норма је мултипликативна. То ћемо користити да покажемо једно својство норме, које ћемо касније користити.

Нека су α и β произвољни елементи из $\mathbf{Q}[\sqrt{n}]$. Тада је:

$$N\left(\frac{\alpha}{\beta}\right) = \frac{N(\alpha)}{N(\beta)}.$$

Како је $\mathbf{Q}[\sqrt{n}]$ је поље, сваки елемент има инверз. Према томе, за произвољан еленемт β из $\mathbf{Q}[\sqrt{n}]$ важиће $\beta\beta^{-1} = 1$. Нормирањем израза, добија се:

$$N\left(\frac{1}{\beta}\right) = \frac{1}{N(\beta)}$$

Тада је:

$$N\left(\frac{\alpha}{\beta}\right) = N\left(\alpha\frac{1}{\beta}\right) = N(\alpha)N\left(\frac{1}{\beta}\right) = N(\alpha)\frac{1}{N(\beta)} = \frac{N(\alpha)}{N(\beta)}.$$

Сада ћемо видети за које вредности броја n је прстен $\mathbf{Z}[\sqrt{n}]$ еуклидски. Уколико је прстен $\mathbf{Z}[\sqrt{n}]$ еуклидски, тада за сваки $a + b\sqrt{n}$ и $c + d\sqrt{n}$ из $\mathbf{Z}[\sqrt{n}]$, постоје $p + q\sqrt{n}$ и $r + s\sqrt{n}$ такви да је

$$a+b\sqrt{n} = (c+d\sqrt{n})(p+q\sqrt{n})+r+s\sqrt{n}, \quad N(r+s\sqrt{n}) < N(c+d\sqrt{n}).$$

Из ове једначине следи да је количник два елемента облика $a + b\sqrt{n}$ и $c + d\sqrt{n}$

$$\frac{a + b\sqrt{n}}{c + d\sqrt{n}} = p + q\sqrt{n} + \frac{r + s\sqrt{n}}{c + d\sqrt{n}}.$$

Овај количник може да се запише као

$$\alpha + \beta\sqrt{n} = (p + q\sqrt{n}) + \gamma + \delta\sqrt{n},$$

при чему су $\alpha + \beta\sqrt{n}$ и $\gamma + \delta\sqrt{n}$ елементи из $\mathbf{Q}[\sqrt{n}]$.

Како је $\alpha + \beta\sqrt{n}$ количник два дата елемета, он је познат. Потребно је одредити остале бројеве.

За норму елемента $\gamma + \delta\sqrt{n}$ важи:

$$N(\gamma + \delta\sqrt{n}) = N\left(\frac{r + s\sqrt{n}}{c + d\sqrt{n}}\right) = \frac{N(r + s\sqrt{n})}{N(c + d\sqrt{n})} < 1$$

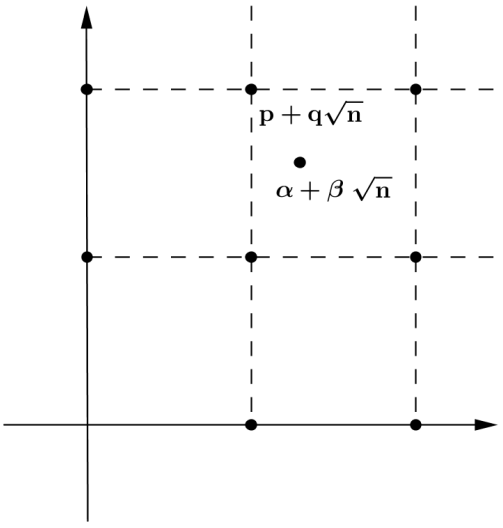
С друге стране, како је $\gamma + \delta\sqrt{n} = (\alpha + \beta\sqrt{n}) - (p + q\sqrt{n})$, следи да је

$$N(\gamma + \delta\sqrt{n}) = N\big((\alpha + \beta\sqrt{n}) - (p + q\sqrt{n})\big) < 1.$$

$$N\big((\alpha - p) + (\beta - q)\sqrt{n})\big) < 1$$

Нормирањем претходног израза, добија се неједнакост

$$(\alpha - p)^2 - n(\beta - q)^2 < 1$$



Рекли смо већ да су нам α и β познати. Потребно је одредити целе бројеве p и q који задовољавају претходну неједнакост. Како се сваки рационалан број налази између два цела, могу се одредити p и q, тако да важи

$$|\alpha - p| \leq \frac{1}{2}$$

$$|\beta - q| \leq \frac{1}{2}.$$

Уколико обележимо $(\alpha - p)^2 = x$ и $(\beta - q)^2 = y$, остаје да одредимо када је $|x - ny| < 1$. При том, $0 \leq x \leq \frac{1}{4}$ и $0 \leq y \leq \frac{1}{4}$. За које све вредности од n нам је ово испуњено?

Неједнакост $|x - ny| < 1$ има највећу вредност $\frac{|n|}{4}$ и најмању $\frac{|n-1|}{4}$. Према томе, мора бити $-3 < n < 4$, односно вредности које n узима су -2, -1, 2, 3. Дакле, доказали смо следећу теорему:

Теорема 6. *Прстени облика* $\mathbf{Z}[\sqrt{n}]$ *који су еуклидски су* $\mathbf{Z}[\sqrt{-2}]$, $\mathbf{Z}[\sqrt{-1}]$, $\mathbf{Z}[\sqrt{2}]$ *и* $\mathbf{Z}[\sqrt{3}]$

Лема 3.
Ако је 2 *нерастављив у* $\mathbf{Z}[\sqrt{n}]$, *тада он није са једнозначном факторизацијом.*

Доказ.
Нека је α из $\mathbf{Z}[\sqrt{n}]$ облика $n+\sqrt{n}$. Посматрајмо следећи производ

$$(n + \sqrt{n})(n - \sqrt{n}) = n^2 - n = n(n - 1).$$

Он је паран, према томе важи да 2 дели $(n + \sqrt{n})(n - \sqrt{n})$. Међутим, да ли су $n + \sqrt{n}$ и $n - \sqrt{n}$ дељиви са 2? Уколико 2 дели $n + \sqrt{n}$, тада постоји елемент $a + b\sqrt{n} \in \mathbf{Z}[\sqrt{n}]$ такав да је $n + \sqrt{n} = 2(a + b\sqrt{n})$. У том случају, мора бити $n = 2a$ и $1 = 2b$, односно $a = \frac{n}{2}$ и $b = \frac{1}{2}$ што је немогуће. Према томе, 2 није прост у $\mathbf{Z}[\sqrt{n}]$.

□

Лема 4.
За $n \leq -3$ *и* $n = 1(mod\ 4)$, $\mathbf{Z}[\sqrt{n}]$ *није са једнозначном факторизацијом.*

Доказ.
Претпоставимо да је 2 растављив у $\mathbf{Z}[\sqrt{n}]$. Тада постоји факторизација $2 = \alpha\beta$, при чему α и β нису инверзибилни у $\mathbf{Z}[\sqrt{n}]$. Нормирањем претходног израза, добија се $4 = N(\alpha)N(\beta)$. Како α и β нису инверзибилни, мора бити $|N(\alpha)| = |N(\beta)| = 2$. Нека је $\alpha = a + b\sqrt{n}$, тада је $a^2 - nb^2 = \pm 2$.

Уколико је $n < 0$, тада је $a^2 - nb^2 = a^2 + |n|b^2 \geq |n|$. Како b није нула, у овом случају је $|n| \geq 3$, па једначина $a^2 - nb^2 = \pm 2$ нема решење.

Уколико је $n = 1 (\mathrm{mod}\ 4)$, тада се једначина своди на $a^2 - b^2 = 2 (\mathrm{mod}\ 4)$. Квадрати по модулу 4 су 0 и 1, дакле њихова разлика никада не може бити 2. Према томе, за ове вредности броја n једначина $a^2 - nb^2 = \pm 2$ нема решење.

□

Пример 2.
Постоје домени који су главни, али нису еуклидски. Такав је прстен $\mathbf{Z}[(1 + \sqrt{-19})/2]$.

Лема 5.
Цео број x дели $a + b\sqrt{n} \in \mathbf{Z}[\sqrt{n}]$ ако и само ако x дели a и x дели b.

Доказ.
Уколико x дели $a + b\sqrt{n}$, тада постоји елемент $c + d\sqrt{n}$ из $\mathbf{Z}[\sqrt{n}]$, такав да је

$$a + b\sqrt{n} = x(c + d\sqrt{n}) = xc + xd\sqrt{n}.$$

Видимо да мора бити $a = xc$ и $b = xd$, одакле следи да x дели a и x дели b.

□

2.2 Прстен Гаусових целих $\mathbf{Z}[i]$

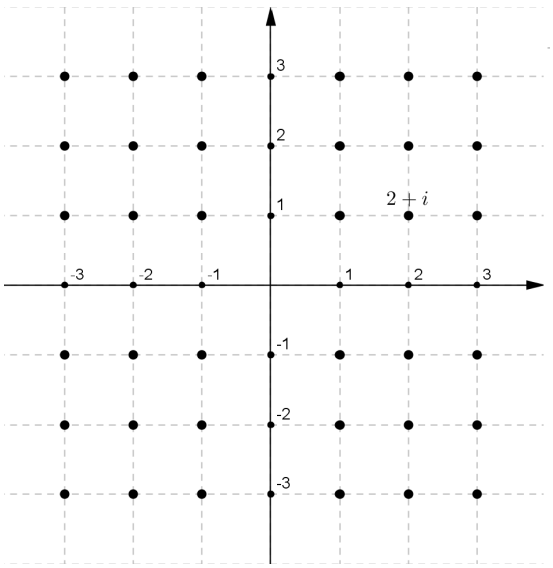
Ради лакшег решавања квадратних реципроцитета, Johann Carl Friedrich Gaus[1] је у својој другој монографији увео нове

[1] Johann Carl Friedrich Gaus (1777 ˘ 1855) немачки математичар и научник

бројеве, који су по њему названи *Гаусови цели бројеви*. То је било велико достигнуће, јер у Гаусово време комплексни бројеви нису били добро схваћени. Он је открио да је проучавање питања о квадратним остацима једноставније уколико уместо целих бројева посматрамо "целе комплексне бројеве", мада се она не односе на комплексне бројеве.

За $n = -1$, добија се прстен $\mathbf{Z}[i]$, који се назива прстен Гаусових целих. Он је облика

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



Слика 2: Гаусови цели бројеви

Прстен Гаусових целих је еуклидски прстен, у односу на функцију норме $N(a + bi) = a^2 + b^2$. Доказ тога смо видели у претходном делу. Како је прстен $\mathbf{Z}[i]$ еуклидски, он је и главноидеалски а самим тим и са једнозначном факторизацијом.

Лема 6.
Једини елементи који су инвертибилни у $\mathbf{Z}[i]$ *су* 1, -1, i *и* $-i$.

Доказ.
Претпоставимо да постоји елемент $\alpha = a + bi$ из $\mathbf{Z}[i]$, који је инвертибилан. Тада постоји $\beta = c + di$ из $\mathbf{Z}[i]$, такав да је

$$\alpha\beta = 1.$$

Нормирањем претходног израза, добија се

$$N(\alpha\beta) = N(\alpha)N(\beta) = 1,$$

одакле следи да је $N(\alpha) = 1$ и $N(\beta) = 1$. Из прве једначине, добијамо да је $a^2 + b^2 = 1$. То важи једино ако је $a^2 = 1$, $b^2 = 0$ или $a^2 = 0$, $b^2 = 1$, односно $a = \pm 1$, $b = 0$ или $a = 0$, $b = \pm 1$. Према томе, инвертибилни елементи у прстену Гаусових целих су 1, -1, i, $-i$.

□

Инвертибилне елементе у прстену Гаусових целих називамо јединицама. Како прстен $\mathbf{Z}[i]$ има четири јединице, сваком елементу $\alpha \in \mathbf{Z}[i]$ је придружено четири елемента:

$$\alpha,\ -\alpha,\ \alpha i \text{ и } -\alpha i.$$

• Дељивост у прстену $\mathbf{Z}[i]$

У прстену $\mathbf{Z}[i]$ дељивост се дефинише као и у сваком другом прстену. Међутим, не морају свака два Гаусова цела броја да буду дељива. Уколико резултат дељења два Гаусова броја није Гаусов број, тада за њих кажемо да нису дељиви у прстену $\mathbf{Z}[i]$.

Пример 3.

(1) Да ли у прстену Гаусових целих елемент $2 - 3i$ *дели* $17 - 7i$*?*

(2) Показати да $2 - 3i$ *дели* $17 + 7i$ *у прстену Гаусових целих.*

Решење.
(1) Уколико $2-3i$ дели $17-7i$, тада постоји елемент $x+yi \in \mathbf{Z}[i]$, такав да је $17-7i = (2-3i)(x+yi)$. Сређивањем израза, добија се

$$17 - 7i = (2x + 3y) + (2y - 3x)i.$$

Изједначавањем реалног и имагинарног дела, добија се да је $x = 55/13$, и $y = 37/13$. Како x и y нису цели бројеви, следи да $2 - 3i$ не дели $17 + 7i$ у прстену $\mathbf{Z}[i]$.

(2) Као и у претходном примеру, потребно је наћи $x + yi \in \mathbf{Z}[i]$, такав да је $17 + 7i = (2 - 3i)(x + yi)$. Сређивањем израза и изједначавањем реалног и имагинарног дела, следи да је $x = 1$ и $y = 5$. Дакле, како је

$$17 + 7i = (1 + 5i)(2 - 3i),$$

важи да $2 - 3i$ дели $17 + 7i$ у прстену $\mathbf{Z}[i]$.

△

Теорема 7.
Нека су α и β два произвољна елемента пратена $\mathbf{Z}[i]$. Тада важи да ако β дели α у $\mathbf{Z}[i]$ тада $N(\beta)$ дели $N(\alpha)$ у $\mathbf{Z}$.

Доказ.
Уколико β дели α у прстену $\mathbf{Z}[i]$, тада постоји $\gamma \in \mathbf{Z}[i]$, такав да је $\alpha = \beta\gamma$. Нормирањем претходне једначине, и користећи мултипликативност норме, добија се

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

Ова једначина је из $\mathbf{Z}$, а како је $N(\alpha) = N(\beta)N(\gamma)$, следи да $N(\beta)|N(\alpha)$ у $\mathbf{Z}$.

□

Ова теорема омогућава и да се на брз начин провери која два Гаусова цела броја нису дељива. На пример, уколико $(7 + 2i)$ дели $(5 + 11i)$ у прстену $\mathbf{Z}[i]$, тада $N(7 + 2i)$ дели $N(5 + 11i)$ у $\mathbf{Z}$, односно 53 дели 146, што није тачно. Дакле, уколико норме елемената нису дељиве у $\mathbf{Z}$, тада елементи нису дељиви

у прстену $\mathbf{Z}[i]$.
Обрат теореме не важи: уколико $N(\beta)$ дели $N(\alpha)$ у $\mathbf{Z}$, не мора да важи да β дели α у $\mathbf{Z}[i]$.

Пример 4.
Показати да $5+3i$ *не дели* $13+i$ *у* $\mathbf{Z}[i]$.

Решење:
Норма броја $5+3i$ је 34, а норма броја $13+i$ је 170. Видимо да 34 дели 170 у $\mathbf{Z}$. Међутим, да ли $5+3i$ дели $13+i$ у $\mathbf{Z}[i]$? Уколико то важи, мора постојати елемент $x+yi$ из $\mathbf{Z}[i]$, такав да је $13+i=(5+3i)(x+yi)$. Сређивањем израза добија се

$$13+i=5x-3y+(3x+5y)i.$$

Изједначавањем реалног и имагинарног дела, добија се

$$\begin{aligned} 13 &= 5x-3y \\ 1 &= 3x+5y. \end{aligned}$$

Решавањем система, следи да је $x=24/17$ и $y=-11/17$, што нису цели бројеви, па $x+yi$ није елемент прстена $\mathbf{Z}[i]$. Дакле $5+3i$ не дели $13+i$ у $\mathbf{Z}[i]$.

$\triangle$

Теорема 8.
Уколико је α *елемент прстена* $\mathbf{Z}[i]$ *чији је фактор* $1+i$*, тада ће његова норма бити парна у* $\mathbf{Z}$

Доказ.
Уколико је $1+i$ фактор од α, тада α може да се запише у облику $\alpha=(1+i)\beta$, за неко $\beta\in\mathbf{Z}[\mathbf{i}]$. Нормирањем овог израза, добија се

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

Дакле, норма елемента α је парна.

$\square$

• Еуклидов алгоритам у $\mathbf{Z}[i]$

Како је прстен $\mathbf{Z}[i]$ еуклидски, у њему је дефинисан еуклидов алгоритам, за одређивање највећег заједничког делиоца два еле−мента. Показаћемо на неколико једноставних примера, како еуклидов алгоритам изгледа у прстену $\mathbf{Z}[i]$.

Пример 5.

(1) Показати да су $\alpha = 30+7i$ и $\beta = 3+10i$ релативно прости у prstenu $\mathbf{Z}[i]$.

(2) Одредити највећи заједнички делилац за $\alpha = 15-10i$ и $\beta = 6-7i$.

Решење.

(1) Применом еуклидовог алгоритма на бројеве α и β добијамо:

$$\begin{aligned} 30+7i &= (3+10i)(1-3i)-3+6i \\ 3+10i &= (-3+6i)(1-i)+i \\ -3+6i &= i(6+3i)+0 \end{aligned}$$

Како је последњи не-нула остатак јединица, закључујемо да су $\alpha = 30+7i$ и $\beta = 3+10i$ релативно прости у $\mathbf{Z}[i]$.

(2)

$$\begin{aligned} 15-10i &= (6-7i)(2+i)-4-2i \\ 6-7i &= (-4-2i)(-1+2i)-2-i \\ -4-2i &= (-2-i)(2)+0. \end{aligned}$$

Последњи остатак различит од нуле је $-2-i$, тако да је он највећи заједнички делилац за α и β.

$\triangle$

Највећи заједнички делилац d за два елемента α, $\beta \in \mathbf{Z}[i]$, одређен преко еуклидовог алгоритма, може да се представи као њихова линеарна комбинација. То се добија враћањем уназад кроз кораке еуклидовог алгоритма. Применићемо тај поступак на претходни пример.

Пример 6.

(1) $\alpha = 30 + 7i$ и $\beta = 3 + 10i$ су релативно прости, јер им је последњи не-нула остатак у Еуклидовом алгоритму једнак i. То i се може изразити као $\mathbf{Z}[i]-$ комбинација од α и β, кретањем уназад кроз кораке Еуклидовог алгоритма:

$$\begin{aligned} i &= 3 + 10i - (-3 + 6i)(1 - i) = \\ &= 3 + 10i - (30 + 7i - (3 + 10i)(1 - 3i))(1 - i) = \\ &= \beta - (\alpha - (\beta)(1 - 3i))(1 - i) = \\ &= (-1 + i)\alpha + (-1 - 4i)\beta. \end{aligned}$$

Према томе, како је i највећи заједнички делилац за α и β важи

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

(2) Видели смо да је $-2 - i$ највећи заједнички делилац за $\alpha = 15 - 10i$ и $\beta = 6 - 7i$. Крећући се уназад кроз кораке Еуклидовог алгоритма, добијамо:

$$\begin{aligned} -2 - i &= 6 - 7i - (-4 - 2i)(-1 + 2i) = \\ &= 6 - 7i - (15 - 10i - (6 - 7i)(2 + i))(-1 + 2i) = \\ &= (15 - 10i)(1 - 2i) + (6 - 7i)(1 + (2 + i)(-1 + 2i)) = \\ &= (15 - 10i)(1 - 2i) + (6 - 7i)(-3 + 3i) = \\ &= \alpha(1 - 2i) + \beta(-3 + 3i). \end{aligned}$$

Дакле, највећи заједнички делилац за α и β може да се запише у облику:

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

2.3 Прости елементи у $\mathbf{Z}[i]$

Како је прстен $\mathbf{Z}[i]$ еуклидски, у њему се прости елементи и атоми подударају. У претходном делу смо видели да прстен $\mathbf{Z}[i]$ има четири јединице. Користећи ту чињеницу, можемо одредити који су прости бројеви у $\mathbf{Z}[i]$.

Теорема 9.
Број $\alpha \in \mathbf{Z}[i]$ је Гаусов прост број уколико су му једини фактори:

$$1,\ -1,\ i,\ -i,\ \alpha,\ -\alpha,\ i\alpha \text{ и } -i\alpha.$$

Доказ.
Како је α прост, а самим тим и атом, следи да ако је он облика $\alpha = \beta\gamma$, или β или γ морају бити инверзибилни. Нека је β инверзибилан, тада је он или ± 1 или $\pm i$. У том случају, γ мора бити $\pm\alpha$ или $\pm i\alpha$. Дакле, фактори од α су ± 1, $\pm i$, $\pm\alpha$ и $\pm i\alpha$. □

Ови фактори се називају *тривијални* фактори елемента α. Уколико је a цео број који није прост, тада он неће бити ни Гаусов прост број. Међутим, да ли је сваки цео прост број уједно и Гаусов прост број? У овом делу ћемо видети да то не мора да важи.

Гаусов прост број се може дефинисати и као Гаусов цео број који није производ Гаусових целих са мањом нормом. Следећа лема нам даје једну везу између целих простих бројева и Гаусових простих бројева.

Лема 7.
Ако је норма Гаусовог целог броја проста у $\mathbf{Z}$, тада је он прост у $\mathbf{Z}[i]$.

Доказ.
Нека је α елемент прстена $\mathbf{Z}[i]$, чија је норма $N(\alpha)$ проста у $\mathbf{Z}$. Претпоставимо да је α сложен. Тада постоје β и γ такви да је

$\alpha = \beta\gamma$. Нормирањем претходног израза, и користећи особину мултипликативности норме, добија се:

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

Како је $N(\alpha)$ прост у $\mathbf{Z}$, мора бити $N(\beta) = 1$ или $N(\gamma) = 1$. Према томе, β или γ су јединице у прстену $\mathbf{Z}[i]$, па α нема нетривијалну факторизацију.

□

Довољан услов за Гаусове целе бројеве да буду прости је да имају просту норму. Тај услов није неопходан. То ћемо видети на примеру броја 7.

Пример 7.

(1) Број $1 + i$ је Гаусов прост број. Његова норма је

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

а то је прост број у $\mathbf{Z}$. Како не постоји Гаусов цео број чија норма дели број 2, $1+i$ није производ Гаусових целих са мањом нормом.

(2) Број 2 није Гаусов прост број. У $\mathbf{Z}[i]$, он може да се запише као

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

Оба броја, $1 + i$ и $1 - i$ имају норму једнаку 2, што је мање од норме $N(2) = 4$.

(3) Да би се показало да је 7 прост у $\mathbf{Z}[i]$, послужићемо се контрадикцијом. Претпоставимо да је 7 сложен. Тада постоје α и β из $\mathbf{Z}[i]$, такви да је нетривијална факторизација

$$7 = \alpha\beta.$$

Нормирањем претходне једначине добија се $49 = N(\alpha)N(\beta)$. Како је факторизација нетривијална, $N(\alpha) > 1$ и $N(\beta) > 1$.

Према томе, мора бити $N(\alpha) = 7$ и $N(\beta) = 7$. Нека је $\alpha = a+ib$. Из $N(\alpha) = 7$, добија се $a^2 + b^2 = 7$. Не постоје цели бројеви који задовољавају дату једнакост, према томе, то је контрадикција. Дакле, 7 има једино тривијалну факторизацију у $\mathbf{Z}[i]$, па је 7 прост у $\mathbf{Z}[i]$.

Нека је p прост, позитиван, цео број. Уколико он није прост у $\mathbf{Z}[i]$, има фактор $a + bi$. Тада важи $N(a + bi)$ дели $N(p) = p^2$, односно $N(a + bi) = (a + bi)(a - bi) = a^2 + b^2 = p$. То нас доводи до следеће теореме.

Теорема 10.
Прост, позитиван, цео број p је сложен у $\mathbf{Z}[i]$ ако и само ако може да се запише као збир два квадрата.

Доказ.
$\Rightarrow$: Нека је p прост, позитиван, цео број који је сложен у $\mathbf{Z}[i]$. Тада може да се запише у облику:

$$p = (a + bi)\gamma$$

где су $a + bi$ и γ Гаусови цели чија је норма мања од норме од p. Нормирањем се добија да је

$$p^2 = (a^2 + b^2)\gamma^2.$$

Како је p прост, мора бити $p = a^2 + b^2$.

$\Leftarrow$: Нека је $p = a^2 + b^2$. Тада у $\mathbf{Z}[i]$ он може да се факторише на следећи начин:

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

одакле се види да p није прост у $\mathbf{Z}[i]$.

□

Први прости бројеви у $\mathbf{Z}$ који су збир два квадрата су 2, 5, 13, 17 и 29. Они могу да се запишу на следећи начин:

$$\begin{aligned} 2 &= 1^2 + 1^2, \\ 5 &= 1^2 + 2^2, \\ 13 &= 2^2 + 3^2, \\ 17 &= 1^2 + 4^2, \\ 29 &= 2^2 + 5^2. \end{aligned}$$

Сваки од њих је сложен у $\mathbf{Z}[i]$, јер могу да се представе као производ конјугата, чије су норме једнаке тим простим бројевима.

$$\begin{aligned} 2 &= (1+i)(1-i) \\ 5 &= (1+2i)(1-2i) \\ 13 &= (2+3i)(2-3i) \\ 17 &= (1+4i)(1-4i) \\ 29 &= (2+5i)(2-5i) \end{aligned}$$

Лема 8.
Цели прости бројеви облика $p = 3 \ (mod\ 4)$ су нерастављиви у $\mathbf{Z}[i]$, па су и прости.

Доказ.
Претпоставимо супротно, нека је прост цео број $p = 3 \pmod 4$ сложен у $\mathbf{Z}[i]$. Тада он може да се факторише на следећи начин:

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

где су $a + bi$ и $c + di \in \mathbf{Z}[i]$. Нормирањем претходне једнакости, добија се:

$$p^2 = (a^2 + b^2)(c^2 + d^2).$$

Како је p прост, мора бити:

$$\begin{aligned} a^2 + b^2 &= p \\ c^2 + d^2 &= p. \end{aligned}$$

Међутим, како збир два квадрата може бити једнак 0, 1 или 2 (mod 4), а p је број облике 3 (mod 4), следи да једначине немају решења. Према томе, p мора бити прост у $\mathbf{Z}[i]$.

□

Лема 9.
Нека је $p = a^2 + b^2 = 1$ (mod 4) прост позитиван цео број. Тада су $a + bi$ и $a - bi$ прости у $\mathbf{Z}[i]$.

Доказ.
Уколико је $p = a^2 + b^2 = 1$ (mod 4) прост позитиван цео број, тада је

$$p = a^2 + b^2 = (a + bi)(a - bi).$$

Нормирањем се добија да је $N(a+bi) = p$ и $N(a-bi) = p$. Како је њихова норма проста, онда и они морају бити прости.

Уколико су $a+bi$ и $a-bi$ придружени, тада је $a-bi = u(a+bi)$, где је u нека јединица. Размотрићемо све случајеве. Уколико је $u = 1$, тада је $a - bi = a + bi$, односно $p = a^2$. Уколико је $u = -1$, тада је $a - bi = -a - bi$, односно $p = b^2$. И, уколико је $u = \pm i$, тада је $a - bi = \pm i(a + bi)$, односно $p = 2b^2$. Како је прост позитиван цео број, ове могућности отпадају. Према томе, $a + bi$ и $a - bi$ нису придружени.

□

На основу претходних лема, можемо формулисати теорему, која нам показује који су све Гаусови прости бројеви.

Теорема 11.
Прости Гаусови цели бројеви су (до на придруженост):

- *прости цели бројеви конгруентни са* 3 (*mod* 4)
- $1 + i$
- $x + yi$ *и* $x - yi$ *где је* $p = x^2 + y^2 = 1$ (*mod* 4) *прост позитиван цео број*

Лема 10.
За сваки прост број $\alpha \in \mathbf{Z}[i]$, постоји позитиван прост број $a \in \mathbf{Z}$ такав да α дели a.

Доказ.
Нека је α прост елемент прстена $\mathbf{Z}[i]$. Како је његова норма једнака $N(\alpha) = \alpha \cdot \bar{\alpha}$, увек важи да α дели $N(\alpha)$. Уколико је његова норма $N(\alpha)$ проста у $\mathbf{Z}$, тада је $a = N(\alpha)$.

Уколико је норма сложена, она може да се факторише у $\mathbf{Z}$ на следећи начин:

$$N(\alpha) = a_1 a_2 \cdots a_n,$$

при чему су a_j, $j = 1, 2, ..., n$ прости у $\mathbf{Z}$. Како α дели $N(\alpha)$, а α је прост, мора постојати a_j такав да α дели a_j.

□

Коришћењем факторизације норме у $\mathbf{Z}$, може се одредити који су фактори Гаусових целих бројева. То следи из својства мултипликативности норме.

Пример 8.
Која је проста факторизација броја $1845 + 1006i$ у $\mathbf{Z}[\mathbf{i}]$?

Решење.
Норма броја $1845 + 1006i$ је 4416061, а проста факторизација броја 4416061 у $\mathbf{Z}$ је $13 \cdot 37 \cdot 9181$.
Да би се добила факторизација од $1845 + 1006i$ у $\mathbf{Z}[i]$,најпре се морају одредити који Гаусови цели имају норме 13, 37, 9181, а затим се међусобно множе док се не добије тражени број. Гаусови фактори од 13, 37 и 9181 могу се одредити на основу представљања сваког броја као збир два квадрата:

$$\begin{aligned} 2^2 + 3^2 &= 13 \\ 1^2 + 6^2 &= 37 \\ 30^2 + 91^2 &= 9181. \end{aligned}$$

На основу овога се може одредити њихова факторизација у $\mathbf{Z}[i]$:

$$\begin{aligned} 13 &= (2 + 3i)(2 - 3i) \\ 37 &= (1 + 6i)(1 - 6i) \\ 9181 &= (30 + 91i)(30 - 91i) \end{aligned}$$

Изаберимо један фактор из сваког производа и помножимо их. Када помножимо вредности заграда у којима је сабирање, добијамо

$$(2+3i)(1+6i)(30+91i) = -1845 - 1006i.$$

Према томе, проста факторизација од $1845 + 1006i$ је

$$1845 + 1006i = -(2+3i)(1+6i)(30+91i).$$

Сваки фактор са десне стране једначине је прост у $\mathbf{Z}[i]$, зато што је њихова норма проста у $\mathbf{Z}[i]$.

$\triangle$

3 Примена Гаусових целих на аритметику од Z

Прстен Гаусових целих може бити од велике користи приликом доказивања математичких теорема које се односе на обичне целе бројеве.
У овом делу ће бити разматрано следеће:

- прости бројеви као збир два квадрата
- Питагорине тројке
- Једначине облика $x^2 + y^2 = z^3$
- Једначине облика $y^2 = x^n - 1$

3.1 Прости бројеви као збир два квадрата

У овом делу ћемо видети који све бројеви могу да се запишу као збир два квадрата. Том приликом ћемо користити Вилсонову теорему, која гласи:

Нека је p прост број. Тада је

$$(p-1)! = -1 (\text{mod } p).$$

Теорема 12.
Нека је p позитиван, прост, цео број. Тада је $p = a^2 + b^2$ ако и само ако је $p = 1$ $(mod\ 4)$.

Решење.
$\Rightarrow$: Нека је p збир два квадрата. Тада је $p = 0$, 1 или 2 (mod 4). Како је p прост, први случај је немогућ, а трећи је могућ једино за $p = 2$. Према томе, $p = 1$ (mod 4).

$\Leftarrow$: Нека је $p \equiv 1$ (mod 4), и претпоставимо да је прост у $\mathbf{Z}[i]$. На основу Вилсонове теореме, важи да је:

$$
\begin{aligned}
-1(\mod p) &= (p-1)! = (4k+1-1)! = (4k)! = \\
&= (1)(2)\dots(2k)(2k+1)(2k+2)\dots(4k) = \\
&= (2k)!(2k+1)(2k+)\dots(4k) = \\
&= (2k)!(4k+1-2k)(4k+1-(2k-1))\dots(4k+1-1) = \\
&= (2k)!(-2k)(-(2k-1))\dots(-1) = \\
&= (2k)!(-1)^{2k}(2k)(2k-1)\dots(1) = \\
&= ((2k)!)^2
\end{aligned}
$$

Нека је $x = (2k)!$. На основу претходног извођења важи да је $x^2 = -1 \pmod p$, односно p дели $x^2 + 1$. У $\mathbf{Z}[i]$, $x^2 + 1$ може да се факторише као

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

Како је p прост и дели $x^2 + 1$, следи да p дели $x - i$ или $x + i$. Нека p дели $x + i$. То значи да постоји елемент $a + bi$ из $\mathbf{Z}[i]$ такав да је

$$p(a + bi) = (x + i).$$

Изједначавањем реалног и имагинарног дела, добија се $pa = x$ и $pb = 1$. То је контрадикција, према томе p је сложен у $\mathbf{Z}[i]$, па може да се запише као збир два квадрата. △

Прости бројеви на јединствен начин могу да се запишу као збир два квадрата. Међутим, сложени бројеви могу да буду збирови два квадрата на више од једног начина.

Пример 9.
Написати број 130 *као збир два квадрата.*

Решење.
У $\mathbf{Z}$, број 130 може да се запише као производ бројева 10 и 13. У $\mathbf{Z}[i]$, они могу да се факторишу на следећи начин:

$$
\begin{aligned}
10 &= (1 + 3i)(1 - 3i) \\
13 &= (2 + 3i)(2 - 3i)
\end{aligned}
$$

Ове факторе можемо да комбинујемо на два начина:

$10{\cdot}13 = ((1{+}3i)(2{+}3i))((1{-}3i)(2{-}3i)) = ((1{+}3i)(2{-}3i))((1{-}3i)(2{+}3i))$.

Наког рачунања добија се да је

$$130 = (-7+9i)(-7-9i) = (11+3i)(11-3i).$$

Дакле, 130 може да се запише као производ два квадрата, на два начина:

$$130 = 7^2 + 9^2 = 11^2 + 3^2.$$

△

Сваки позитиван цео број може да се запише као производ 4 квадрата. Постоје и бројеви који могу да се запишу као збир четири квадрата на више од једног начина. На пример, за број 157 важи факторизација $157 = 6^2 + 7^2 + 4^2 + 8^2$, као и факторизација $157 = 2^2 + 6^2 + 6^2 + 9^2$.

3.2 Питагорине тројке

Питагорина тројка (a, b, c) је решење једначине

$$a^2 + b^2 = c^2.$$

Тројка је примитивна, уколико a, b и c немају заједничке факторе. Квадрат непарног броја је једнак 1 (mod 4), а квадрат парног 0 (mod 4). Да би и њихов збир био квадрат, један мора да буде непаран, а један паран број. Према томе, и њихов збир ће бити непаран број.

Теорема 13.
Питагорина тројка (a, b, c) може да се запише у облику:

$$\begin{aligned} a &= x^2 - y^2 \\ b &= 2xy \\ c &= x^2 + y^2 \end{aligned}$$

при чему је $x > y > 0$, $(x, y) = 1$ и $x \neq y$ mod 2.

Доказ.

Како је (a, b, c) Питагорина тројка, из једначине $a^2 + b^2 = c^2$ следи факторизација у прстену $\mathbf{Z}[i]$

$$c^2 = (a + bi)(a - bi) = a^2 + b^2.$$

Да ли су $a+bi$ и $a-bi$ нису међусобно прости у прстену $\mathbf{Z}[i]$? Уколико нису, постоји δ који дели и $a + bi$ и $a - bi$. Тада ће δ делити и њихов збир и разлику, односно $\delta \mid 2a$ и $\delta \mid 2bi$ у $\mathbf{Z}[i]$. Тада $N(\delta) \mid 4a^2$ и $N(\delta) \mid 4b^2$. Како су a и b узајамно прости, следи да је $N(\delta) = 1$, односно $\delta = \pm 1$ или $\pm i$.

Дакле, $a+bi$ и $a-bi$ су узајамно прости, а њихов производ је једнак квадрату. То је могуће једино уколико су и они квадрати, или квадрати помножени јединицом. Према томе,

$$a + bi = (x + yi)^2$$

или

$$(a + bi) = i(x + yi)^2,$$

за неко $x + yi \in \mathbf{Z}[i]$.Сређивањем израза добија се

$$a + bi = (x^2 - y^2) + (2xy)i$$

или

$$a + bi = (-2xy) + (x^2 - y^2)i.$$

Како је у првој a непаран, а у другој паран број, једначина која задовољава услове теореме је прва. Из ње следи да је $a = x^2 - y^2$ и $b = 2xy$. Заменом a и b у почетну једначину, добија се c:

$$\begin{aligned} c^2 &= a^2 + b^2 = (x^2 - y^2)^2 + 4x^2y^2 = \\ &= x^4 + 2x^2y^2 + y^4 = (x^2 + y^2)^2. \end{aligned}$$

Како је $c > 0$, важи $c = x^2 + y^2$. Чињеница да је тројка (a, b, c) примитивна, повлачи да су и x и y међусобно прости бројеви.

□

Пример 10.
Ако је $(m, n) = (3, 2)$ тада је примитивна Питагорина тројка облика (5, 12, 13).

3.3 Једначина облика $a^2 + b^2 = c^3$

Теорема 14.
За решења једначине $a^2 + b^2 = c^3$, уз услов $(a, b) = 1$ важи да је:

$$\begin{aligned} a &= m^3 - 3mn^2 \\ b &= 3m^2n - n^3 \\ c &= m^2 + n^2 \end{aligned}$$

при чему је $(m, n) = 1$ и $m \neq n \pmod 2$.

Доказ.
Из услова $(a, b) = 1$ следи да a и b нису оба парна. Они морају бити или оба непарна, или један паран а други непаран. У првом случају би морало бити $c^3 = 1 + 1 = 2 \pmod 4$, а како 2 није куб (mod 4) први случај је немогућ. Према томе, и c мора бити непаран.

Једначина $a^2 + b^2 = c^3$ може да се факторише прстену $\mathbf{Z}[i]$ на следећи начин:

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

Да ли су $a + bi$ и $a - bi$ релативно прости? Уколико нису, постоји заједнички делилац δ. Како он дели и $a + bi$ и $a - bi$, тада он дели и њихов збир и разлику, односно дели $2a$, $2bi$ у $\mathbf{Z}[i]$. Нормирањем се види са $N(\delta)|4a^2$ и $N(\delta)|4b^2$. Како је $(a, b) = 1$ следи да је $N(\delta) = 1$, односно $\delta = \pm 1$ или $\pm i$. Према томе, $a+bi$ и $a - bi$ релативно прости.

Дакле, $a + bi$ и $a - bi$ релативно прости а њихов производ је куб. То је могуће једино ако су и они кубови, или кубови помножени јединицом. Како свака јединица може да се запише као куб

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

може се подразумевати да су $a+bi$ и $a-bi$ кубови. Нека је $a+bi=(m+ni)^3$, $m,\, n \in \mathbf{Z}$. Сређивањем израза, добија се

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

Заменом вредности за a и b у почетну једначину, добија се

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

па је $c = m^2 + n^2$.

Из чињенице да је $(a,b) = 1$ следи да је $(m,n) = 1$. Уколико би било $m = n \pmod 2$, тада би $a = -2m^3 = 0 \pmod 2$ и $b = 2m^3 = 0 \pmod 2$, па би a и b били оба парна, а то је немогуће. Дакле, $m \neq n \pmod 2$.

□

Пример 11.
Једино решење једначине $y^2 + 1 = x^3$ у Z је $(x,y) = (1,0)$.

Решење:
Једначина $y^2 + 1 = x^3$ може да се факторише у $\mathbf{Z}[i]$ на следећи начин:

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

Како су $y+i$ и $y-i$ прости у прстену $\mathbf{Z}[i]$, по јединственој факторизацији у $\mathbf{Z}[i]$ следи да сваки фактор мора бути куб, до на придруженост. Према томе:

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

за неке $m,n \in \mathbf{Z}$. Изједначавањем реалних и имагинарних делова, добија се:

$$\begin{aligned} y &= m^3 - 3mn^2 = m(m^2 - 3n^2) \\ 1 &= 3m^2n - n^3 = n(3m^2 - n^2). \end{aligned}$$

Из друге једначине следи да је $n = \pm 1$. Уколико је $n = 1$, тада је $1 = 3m^2 - 1$, па је $3m^2 = 2$, а то нема целобројних решења. Ако је $n = -1$, тада је $1 = -(3m^2 - 1)$, па је $m = 0$. Дакле, $y = 0$, па је $x^3 = y^2 + 1 = 1$, $x = 1$.

△

Пример 12.
Једина решења једначине

$$x^2 + 4 = y^3$$

јесу $(x, y) = (\pm 2, 2)$ *и* $(x, y) = (\pm 11, 5)$.

Решење:
Једначина $x^2 + 4 = y^3$ може да се факторише у $\mathbf{Z}[i]$ на следећи начин:

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

Уколико је δ највећи заједнички делилац за $x - 2i$ и $x + 2i$, тада он дели и њихов збир и њихову разлику. Дакле, δ дели $2x$ и $4i$. Како δ дели $4i$, он мора бити степен од $1+i$, до на придруженост.

Уколико је x непаран, највећи заједнички делилац је 1, па су $x - 2i$ и $x + 2i$ релативно прости.

Уколико је x паран, највећи заједнички делилац за $x - 2i$ и $x + 2i$ је $(1 + i)^3$. Заиста, како је x паран, постоји неки број z такав да је $x = 2z$. Тада почетка једначина изгледа

$$y^3 = x^2 + 4 = 4z^2 + 4 = 4(z^2 + 1).$$

Како 4 дели y^3, да би постојао куб броја, мора 2 да дели z^2+1. У $\mathbf{Z}[i]$, $z^2 + 1$ може да се факторише као $z^2 + 1 = (z + i)(z - i)$. Како $1 + i^2$ дели 4, и $1 + i$ дели $z + i$ и $z - i$, следи да је $(1 + i)^3$ највећи заједнички делилац за $x - 2i$ и $x + 2i$.

Закључујемо да $x - 2i$ и $x + 2i$ могу да се запишу као куб неког броја у $\mathbf{Z}[i]$.

$$x + 2i = (a + bi)^3 = (a^3 - 3ab^2) + (3a^2b - b^3)i$$

Изједначавањем реалног и имагинарног дела, добија се да су једине могућности $(a, b) = (\pm 1, 1)$ или $(\pm 1, -2)$, одакле се види да је $x = \pm 2$ или ± 11 . Дакле, једина решења једначине $x^2 + 4 = y^3$ у $\mathbf{Z}$ јесу $(x, y) = (\pm 2, 2)$ и $(x, y) = (\pm 11, 5)$.

$\triangle$

3.4 Једначина облика $y^2 = x^n - 1$

Једначина $y^2 = x^n - 1$, где је $n \geq 2$, нема решења за целе бројеве x и y различите од нуле.

Пример 13.
Одредити решења једначине $y^5 = x^2 + 1$.

Решење.
Једначина $y^5 = x^2 + 1$ може да се факторише у $\mathbf{Z}[i]$ на следећи начин:

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

Најпре је потребно одредити да ли је y парно или непарно. Потребно је посматрати y^5 и $x^2+1 \pmod 4$. Уколико је y паран број, $y^5 \pmod 4$ је 0. Међутим, за сваку вредност броја x, важи да је $x^2+1 \pmod 4$ је различито од 0. Према томе, y је непаран број.

Да ли су $x + i$ и $x - i$ релативно прости? Претпоставимо да нису. Нека је δ заједнички делилац за $x+i$ и $x-i$. Тада он дели и њихов збир и разлику, односно $\delta \mid 2x$ и $\delta \mid 2i$. Тада за норму важи да $N(\delta) \mid 4$ у $\mathbf{Z}$. Такође, како је δ заједнички делилац за $x + i$ и $x - i$, важи да

$$N(\delta) \mid N(x + i) = x^2 + 1 = y^5.$$

Како је y непаран, мора бити $N(\delta) = 1$, односно δ је јединица у $\mathbf{Z}[i]$.

Како су $x + i$ и $x - i$ релативно прости, а њихов производ је пети степен, онда морају и они бити пети степен неког елемента из $\mathbf{Z}[i]$, до на придруженост. Како свака јединица у $\mathbf{Z}[i]$ може да се запише као пети степен јединице ($1 = 1^5$, $-1 = (-1)^5$, $i = i^5$, $-i = (-i)^5$), постоји $\alpha \in \mathbf{Z}[i]$ такав да је

$$x + i = \alpha^5.$$

Уколико је $\alpha = a + bi$, применом биномне формуле добија се:

$$\begin{aligned} x + i = (a + bi)^5 &= a^5 + 5a^4bi - 10a^3b^2 - 10a^2b^3i + 5ab^4 + ib^5 = \\ &= (a^5 - 10a^3b^2 + 5ab^4) + (5a^4b - 10a^2b^3 + b^5)i. \end{aligned}$$

Из претходне једнакости следи да је

$$\begin{aligned} x &= a^5 - 10a^3b^2 + 5ab^4 = a(a^4 - 10a^2b^2 + 5b^4) \\ 1 &= 5a^4b - 10a^2b^3 + b^5 = b(5a^4 - 10a^2b^2 + b^4). \end{aligned}$$

Из последње једначине се види да постоје две могућности:

$$\begin{aligned} b &= 1 \\ 5a^4 - 10a^2 + 1 &= 1 \end{aligned}$$

или

$$\begin{aligned} b &= -1 \\ 5a^4 - 10a^2 + 1 &= -1 \end{aligned}$$

Уколико је $b = 1$, следи да је $5a^2(a^2 - 2) = 0$, одакле се види да је $a = 0$ или $a^2 = 2$. Како је $a^2 = 2$ немогуће у $\mathbf{Z}$, следи да је у овом случају $a = 0$.

Уколико је $b = -1$, следи да је $5a^4 - 10a^2 = -2$, односно $5(a^4 - 2a^2) = -2$, што је немогуће.
Дакле, једино решење једначине $y^5 = x^2 + 1$ је $(x, y) = (0, 1)$.

$\triangle$

Литература

[1] Калајџић Г., *Алгебра*, Математички факултет, Београд 2008

[2] Stillwell, J., *Elements of Number Theory*, Springer, 2003

[3] Conrad K., *The Gaussian integers*

[4] Mutafian C., *Le défi algébrique*, t. 2, Vuibert, 1976