Математичка гимназија

МАТУРСКИ РАД

- из математике -

Гаусови и Ајзенштајнови цели бројеви

Ученик:
Александар Гађански, IVa

Ментор:
др Лука Милићевић

Београд, јун 2022.

Садржај

0 Увод

У овом матурском раду биће речи о проширењима целих бројева $\mathbb{Z}[i]$ и $\mathbb{Z}[\omega]$. Најпре ћемо теоријски увести ове прстене и показати неке занимљиве особине. Овај рад ће такође покрити неке облике простих бројева попут x^2+y^2 и x^2-xy+y^2 и како ти облици имају везе са квадратним остацима, али у посебном поглављу разматраћемо и случај када се прост број може представити као $x^2 + 27y^2$, где изненађујућу улогу има кубни реципроцитет. Представићемо како се помоћу Гаусових целих бројева може наћи број целобројних тачака на кругу полупречника N са центром у $(0, 0)$ и како се Ајзенштајнови цели бројеви могу користити у решавању специјаланог случаја последње Фермаове теореме када $3 \mid n$. Након разматрања оба прстена обрадићемо задатке који су се јављали на такмичењима, а чија решења имају директне везе са овим радом.

Такође, желео бих да се захвалим свом ментору др Луки Милићевићу на саветима што се тиче самог садржаја овог рада, као и доказа неких теорема.

1 Гаусови цели бројеви

У овом поглављу бавићемо се особинама Гаусових целих бројева. Важно је напоменути да ће у даљем делу рада Гаусови цели бројеви бити означени малим грчким словима, док су мала латинична слова резервисана за целе бројеве уколико то није другачије наглашено.

1.1 Дефиниција и основни појмови

Скуп Гаусових целих бројева $\mathbb{Z}[i]$ представља раширење, нама познатог, скупа целих бројева.

Дефиниција 1. Гаусов цео број *је сваки комплексан број код кога су имагинаран и реалан део целобројни.*

Теорема 1. *Скуп Гаусових целих бројева са стандардним операцијама сабирања и множења образује комутативни прстен са јединицом.*

Доказ. Лако се проверавају све аксиоме комутативног прстена. □

Дефиниција 2. *Кажемо да Гаусов цео број* α **дели** *број* β *уколико постоји* γ *такво да је* $\beta = \gamma\alpha$*. Ово математички записујемо као* $\alpha \mid \beta$*.*

Пример 1. *Сваки број дели* 0*. Заиста,* $0 = 0 \cdot \alpha$ *за свако* α*, па чак и нулу. Видимо да и* $0 \mid 0$*. Ово нам указује да* γ *из дефиниције не мора бити јединствено.*

Дељивост у прстену Гаусових целих бројева испуњава све особине на које смо навикли приликом рада са целим бројевима, али и неке друге.

Став 1. *Нека су* α*,* β*,* γ *и* δ *Гаусови цели бројеви и нека су* m*,* a *и* b *целобројни, тада важи:*

- $\alpha \mid \alpha$,
- $\alpha \mid \beta \wedge \beta \mid \gamma \Rightarrow \alpha \mid \gamma$,
- $\delta \mid \alpha \wedge \delta \mid \beta \Rightarrow \delta \mid \alpha + \beta$,
- $\big(\forall \kappa \in \mathbb{Z}[i]\big)\delta \mid \alpha \Rightarrow \delta \mid \kappa\alpha$,
- $\alpha \mid \gamma \wedge \beta \mid \delta \Rightarrow \alpha\beta \mid \gamma\delta$,
- $\alpha\beta \mid \alpha\gamma \wedge \alpha \neq 0 \Rightarrow \beta \mid \gamma$,
- $\alpha \mid \beta \Rightarrow \overline{\alpha} \mid \overline{\beta}$.
- $m \mid a + bi \Rightarrow m \mid a \wedge m \mid b$.

Доказ. Лако се проверава из дефиниције. □

Када делимо два броја, дељеник није нужно дељив делиоцем и зато нам је значајно да уведемо дељење са остатком. Остатак је неки Гаусов цео број који желимо да има особине сличне остатку при дељењу целим бројевима, односно да он буде мањи од делиоца. Како не постоји поредак међу Гаусовим целим бројевима, користићемо норму[1].

Дефиниција 3. *За $\alpha = a + bi$, ненегативан цео број $N(\alpha) = a^2 + b^2$ представља* **норму** *Гаусовог целог броја α.*

Норма броја α се такође може записати као $N(\alpha) = \alpha\overline{\alpha}$, што ће нам бити корисно касније.

Став 2. *За Гаусове целе бројеве α и β важи $N(\alpha\beta) = N(\alpha)N(\beta)$.*

Доказ. Како су $\alpha, \beta \in \mathbb{C}$, и важи да је $N(\gamma) = |\gamma|^2$, тада је $N(\alpha)N(\beta) = |\alpha|^2|\beta|^2 = |\alpha\beta|^2 = N(\alpha\beta)$. □

А сада, и коначно да уведемо дељење са остатком.

Теорема 2. *За бројеве α и $\beta \neq 0$ постоје Гаусови цели бројеви υ и ρ такви да је $\alpha = \upsilon\beta + \rho$ и где је $N(\rho) \leq \frac{1}{2}N(\beta)$.*

Доказ. Знамо да је $\dfrac{\alpha}{\beta} = \dfrac{\alpha\overline{\beta}}{\beta\overline{\beta}} = \dfrac{\alpha\overline{\beta}}{N(\beta)} = \dfrac{m + ni}{N(\beta)}$, за неке целе бројеве m и n.
Сада, поделимо m и n бројем $N(\beta)$ у $\mathbb{Z}$. Односно, на основу дељења са остатком у $\mathbb{Z}$, знамо да постоје цели бројеви q_1, q_2, r_1, r_2, за које важи $m = q_1N(\beta) + r_1$, $n = q_2N(\beta) + r_2$ и $|r_1|, |r_2| \leq \frac{1}{2}N(\beta)$. Нека је $\upsilon = q_1 + q_2i$. Приметимо да је $\dfrac{\alpha}{\beta} = \upsilon + \dfrac{r_1 + r_2i}{N(\beta)}$, тј. $\alpha = \upsilon\beta + \dfrac{r_1 + r_2i}{\overline{\beta}}$, односно $\alpha - \upsilon\beta = \dfrac{r_1 + r_2i}{\overline{\beta}}$. Покажимо сада да је $N(\alpha - \upsilon\beta) \leq \frac{1}{2}N(\beta)$. Како је $N(\alpha - \upsilon\beta) = \dfrac{r_1^2 + r_2^2}{N(\beta)} \leq \dfrac{\frac{1}{4}N(\beta)^2 + \frac{1}{4}N(\beta)^2}{N(\beta)} = \frac{1}{2}N(\beta)$, за наше ρ узећемо $\alpha - \upsilon\beta$. □

Важно је напоменути да као и код целих, али за разлику од природних бројева, υ и ρ не морају бити јединствени. Могуће је постићи јединственост уколико бисмо бирали υ са најмањом нормом, односно аргументом у случају једнакости норми, али је то непотребно компликовање.

Дефиниција 4. *Гаусов цео број је* **јединични** *уколико он дели 1.*

Став 3. *Јединични бројеви имају норму једнаку 1, и има их 4 ($\pm 1, \pm i$).*

Доказ. Нека је $\omega = a + bi$ јединични елемент. Пошто $\omega \mid 1$, тада мора постојати α такав да је $\omega\alpha = 1$, из чега следи да је $N(\omega\alpha) = 1$, а применом Става 2, добијамо да је $N(\omega)N(\alpha) = 1$. Како је норма Гаусовог целог броја заправо ненегативан цео број, одатле следи да је $N(\alpha) = N(\omega) = 1$. Из дефиниције норме, знамо да је $a = 0, b = \pm 1$ или $a = \pm 1, b = 0$, одакле добијамо четири могућности за вредност броја ω (± 1 и $\pm i$). □

Дефиниција 5. *Кажемо да су Гаусови цели бројеви α и β* **еквивалентни**, *уколико постоји јединичан елемент ω такав да је $\alpha = \omega\beta$. За еквивалентне α и β пишемо $\alpha \sim \beta$.*

Дефиниција 6. *Кажемо да је δ* **заједнички делилац** *бројева α и β уколико $\delta \mid \alpha$ и $\delta \mid \beta$.*

[1] Функција која обезбеђује потребан поредак се назива еуклидска функција, слично као што се прстени са особином дељења са остатком зову еуклидски домени. Еуклидска функција не мора нужно бити норма, али се испоставља да у прстену Гаусових целих бројева она задовољава потребне услове. У апстрактнијим прстенима норма се на другачији начин дефинише, а постоје и прстени са неправилним понашањем такви да уопште ни не поседују норму.

Дефиниција 7. Највећи заједнички делиоци *бројева α и β су њихови заједнички делиоци за које важи да су дељиви свим њиховим заједничким делиоцима. Скуп највећих заједничких делиоца бројева α и β записиваћемо као $D_{\alpha,\beta}$.*

Дефиниција 8. *За бројеве α и β кажемо да су* **узајамно прости** *ако је 1 њихов највећи заједнички делилац.*

Теорема 3. *За свака два броја α и β постоји њихов највећи заједнички делилац, и он се може представити као линеарна комбинација $\kappa\alpha + \lambda\beta$, за неке Гаусове целе бројеве κ и λ.*

Доказ. Уколико је $\alpha = \beta = 0$, тада је $D_{\alpha,\beta} = \{0\}$, који је очигледно њихова линеарна комбинација. Иначе, нека је η број облика $\kappa\alpha + \lambda\beta$ са најмањом позитивном нормом. Претпоставимо да η није заједнички делилац бројева α и β. Без умањења општости нека $\eta \nmid \alpha$. Сада, пошто α није дељив са $\eta \neq 0$, постоје υ и ρ такви да је $\alpha = \upsilon\eta + \rho$ и $N(\eta) > N(\rho) > 0$. Можемо изразити ρ као $\alpha - \upsilon\eta$, што је једнако са $\alpha(1 - \upsilon\kappa) - \lambda\beta$, па је и ρ линеарна комбинација α и β, а притом ρ има строго мању норму од η што је у контрадикцији са нашом претпоставком, стога следи да је η заједнички делилац α и β. Нека је δ заједнички делилац бројева α и β, како $\delta \mid \alpha$ и $\delta \mid \beta$, из става 1, $\delta \mid \eta$ као њихову линеарну комбинацију, па је $\eta \in D_{\alpha,\beta}$. □

Став 4. *Постоје тачно четири највећа заједничка делиоца, свих са истом нормом.*

Доказ. Нека су δ_1 и δ_2 највећи заједнички делиоци за бројеве α и β. Из дефиниције највећег заједничког делиоца $\delta_1 \mid \delta_2$ и $\delta_2 \mid \delta_1$ односно постоје неки κ_1 и κ_2 такви да је $\delta_1 = \kappa_2\delta_2$ и $\delta_2 = \kappa_1\delta_1$, из чега се добије да је $\delta_1 = \kappa_1\kappa_2\delta_1$, тј. $N(\kappa_1) = N(\kappa_2) = 1$, па су κ_1 и κ_2 јединични елементи, па је $\delta_1 = \pm\delta_2$ или $\delta_1 = \pm i\delta_2$. Лако се провери да све ове вредности δ_1 одговарају по особинама највећем заједничком делиоцу за бројеве α и β. □

Став 5. *Нека за α и β не важи $\alpha = \beta = 0$. Од свих заједничких делилаца бројева α и β највећу норму имају бројеви из $D_{\alpha,\beta}$.*

Доказ. Нека је δ произвољни заједнички делилац за бројеве α и β, и нека је $\sigma \in D_{\alpha,\beta}$ ($N(\sigma) > 0$). Из дефиниције $\delta \mid \sigma$, тј. $\sigma = \kappa\delta$, за неки $\kappa \in \mathbb{Z}[i]$, из чега следи да је $N(\sigma) = N(\kappa)N(\delta) \Rightarrow N(\sigma) \geq N(\delta)$. Једнакост се достиже искључиво када је κ јединичан, односно $\delta \sim \sigma$, тј. $\delta \in D_{\alpha,\beta}$. Како је $D_{\alpha,\beta} = \{\pm\sigma, \pm i\sigma\}$, сви највећи заједнички делиоци имају једнаку највећу норму. □

Теорема 4. *Нека су α и β узајамно прости Гаусови цели бројеви. Тада за сваки $\chi \in \mathbb{Z}[i]$ важи $1 \in D_{\alpha\beta,\chi} \iff 1 \in D_{\alpha,\chi} \wedge 1 \in D_{\beta,\chi}$.*

Доказ. ($\Rightarrow$) Претпоставимо супротно. Без умањења општости, нека α није узајамно прост са χ, и нека је $\vartheta \in D_{\alpha,\chi}$ неки нејединични највећи заједнички делилац бројева α и χ. Како $\vartheta \mid \alpha$, следи да $\vartheta \mid \alpha\beta$, а притом $\vartheta \mid \chi$, тако имамо да је ϑ заједнички делилац бројева $\alpha\beta$ и χ који није јединичан, па одатле $\alpha\beta$ и χ никако не могу бити узајамно прости.

($\Leftarrow$) Имамо да постоје неки $\kappa, \lambda, \sigma, \varsigma \in \mathbb{Z}[i]$ такви да је $\kappa\alpha + \lambda\chi = 1$ и $\sigma\beta + \varsigma\chi = 1$. Множењем ове две једначине добијамо да је $\alpha\beta\kappa\sigma + \chi(\alpha\kappa\varsigma + \lambda\beta\sigma + \lambda\chi\varsigma) = 1$, односно да је 1 линеарна комбинација бројева $\alpha\beta$ и χ, из чега следи да су они узајамно прости. □

1.1.1 Еуклидов алгоритам

Слично као и у скупу целих бројева, и у $\mathbb{Z}[i]$ постоји Еуклидов алгоритам за налажење једног највећег заједничког делиоца нека два Гаусова цела броја.

Нека су дати $\alpha, \beta \in \mathbb{Z}[i]$. Уколико је $\beta = 0$, тада је наш највећи заједнички делилац α и ту стајемо. У супротном, можемо поделити ове бројеве, односо постоје $\upsilon, \rho \in \mathbb{Z}[i]$ за које важи $\alpha = \upsilon\beta + \rho$ и $N(\rho) \leq \frac{1}{2}N(\beta)$. Како сваки заједнички делилац бројева α и β дели ρ, тако и $\sigma \in D_{\alpha,\beta}$ дели ρ. Сада, највећи заједнички делилац за α и β је уједно и највећи заједнички делилац за β и ρ.

У суштини, понављамо следећи поступак док неки остатак не буде нула:

$$\begin{aligned} \alpha &= \upsilon_1\beta + \rho_1, \quad N(\rho_1) < N(\beta) \\ \beta &= \upsilon_2\rho_1 + \rho_2, \quad N(\rho_2) < N(\rho_1) \\ \rho_1 &= \upsilon_3\rho_2 + \rho_3, \quad N(\rho_3) < N(\rho_2) \\ &\vdots \end{aligned}$$

Тада је претпоследњи остатак заправо један највећи заједнички делилац бројева α и β. Остале добијамо множећи га бројевима -1, i и $-i$.

1.2 Гаусови прости бројеви

Дефиниција 9. *Неједиличан Гаусов цео број $\alpha \neq 0$ је* **нерастављив**, *уколико за било које Гаусове целе бројеве β и γ, за које важи $\alpha = \beta\gamma$, следи да је β или γ јединичан. У супротном кажемо да је* **растављив**.

Став 6. *Сваки Гаусов цео број са нормом која је прост број је нерастављив.*

Доказ. Нека је $\pi = \alpha\beta$ и нека је $N(\pi) = p$, где је p прост број. Тада је $N(\alpha\beta) = N(\alpha)N(\beta) = p$, па је $N(\alpha) = 1 \vee N(\beta) = 1$. □

Дефиниција 10. *Неједиличан Гаусов цео број $\pi \neq 0$ је* **прост** *уколико важи $\pi \mid \alpha\beta \implies \pi \mid \alpha$ или $\pi \mid \beta$. У супротном кажемо да је* **сложен**.

Теорема 5. *π је прост $\iff$ π је нерастављив.*

Доказ. ($\Rightarrow$) Нека је број π прост такав да је $\pi = \alpha\beta$. Без умањења општости, нека $\pi \mid \alpha$, тада је $\alpha = \pi\gamma$, за неко γ, одакле добијамо $\pi = \pi\beta\gamma$, па је $\beta\gamma = 1$, тј. $N(\beta) = 1$.

($\Leftarrow$) Претпоставимо да је π нерастављив и нека $\pi \mid \alpha\beta$. Нека је $\delta \in D_{\pi,\alpha}$, тада је $\delta = \kappa\pi + \lambda\alpha$. Знамо да δ дели и α и π. Како је π нерастављив, δ мора бити јединичан елемент или производ јединичног елемента и π. Сада, разликујемо два случаја:

1. δ је јединични елемент. Тада $\delta\beta = \kappa\pi\beta + \lambda\alpha\beta$, што је дељиво са π, $\Rightarrow \pi \mid \delta\beta$, а како је δ јединични елемент, π мора да дели β.
2. δ је производ јединичног елемента и π. Тада очигледно $\pi \mid \delta \mid \alpha$.

□

Последица 1. *Уколико број π има норму која је прост број, тада је π прост.*

Став 7. *Ако је π прост, тада је и његов конјугат, као и сваки његов умножак јединичним елементом, такође прост.*

Доказ. Нека је π прост, и $\overline{\pi}$ његов комплексни конјугат. Претпоставимо да $\overline{\pi}$ није прост. То значи да постоје α и β нејединични елементи такви да је $\overline{\pi} = \alpha\beta$. Одатле имамо да је $\pi = \overline{\alpha} \cdot \overline{\beta}$, али како ни α ни β нису јединични елементи, тако нису ни њихови конјугати, што је противречно са тим да је π прост.
Нека је ω јединични елемент. Такође, нека је $\pi^* = \omega\pi$. Претпоставимо сада да π^* није прост. То значи да постоје неки α и β који нису јединични елементи такви да је $\pi^* = \alpha\beta$. Имамо да је $\pi = \overline{\omega}\alpha\beta$, а како ни $\overline{\omega}\alpha$ ни β нису јединични елементи, то није могуће с обзиром на то да је по претпоставци π прост. □

Лема 1. *Сваки нејединични Гаусов цео број је прост или се може записати као производ простих Гаусових целих бројева.*

Доказ. Ово тврђење доказујемо помоћу јаке индукције.
(База индукције) $N(\alpha) = 2$. Тада је $\alpha \sim 1 + i$. Како је $1 + i$ прост, по ставу 7, и α је прост.
(Индуктивна хипотеза) за свако ϑ, $N(\vartheta) \leq n$, постоји факторизација броја ϑ помоћу Гаусових простих бројева.
(Индуктивни корак) За $N(\alpha) = n + 1$, постоје две могућности:

- α је прост.
- $\alpha = \beta\gamma$, где ни β ни γ нису јединични елементи. Тада је $N(\alpha) = N(\beta)N(\gamma)$, па су норме $N(\beta)$ и $N(\gamma)$ строго мање од $n + 1 \Rightarrow$ постоји факторизација за β и γ, стога постоји и за α.

На основу принципа математичке индукције, за сваки нејединични Гаусов цео број постоји проста факторизација унутар прстена $\mathbb{Z}[i]$. □

Лема 2. *Уколико α има факторизацију унутар прстена $\mathbb{Z}[i]$, она је јединствена до на редослед чинилаца и еквивалентност између одређених чинилаца.*

Доказ. Претпоставимо супротно. Нека број α има бар две, суштински различите, факторизације унутар прстена $\mathbb{Z}[i]$. Изједначимо их, и скратимо заједничке Гаусове просте бројеве унутар обе факторизације. Преостаје нам $\pi_1\pi_2 \dots \pi_n = \omega\psi_1\psi_2 \dots \psi_m$, где је сваки прост број π_i различит од сваког простог броја ψ_j за свака два природна броја $1 \leq i \leq n$ и $1 \leq j \leq m$, и ω је јединични елемент. Сада, π_i мора да дели неки ψ_j, па су они еквивалентни, из чега следи да су факторизације исте до на редослед и еквивалентност између чиниоца. □

Теорема 6 (Основна теорема аритметике у $\mathbb{Z}[i]$)**.** *За сваки Гаусов цео број, постоји јединствена факторизација до на редослед чинилаца и еквивалентност између одговарајућих простих бројева унутар прстена $\mathbb{Z}[i]$.*

Доказ. Постојање директно следи из леме 1, а јединственост из леме 2. □

Теорема 7. *Нека је α прост који није еквивалентан целом броју. Цео број m је дељив са α акко $N(\alpha) \mid m$ у $\mathbb{Z}$.*

Доказ. Уколико је $\alpha \sim 1 + i$, тада $\alpha \mid 2 \mid 2 \cdot \left\lfloor \frac{m}{2} \right\rfloor$. Знамо да је $\alpha \mid m$ еквивалентно са $\alpha \mid m - 2 \cdot \left\lfloor \frac{m}{2} \right\rfloor$. Ова вредност је или 1 или 0, у зависности од парности m, па следи да $N(\alpha) = 2$ дели m ако и само ако $\alpha \mid m$, јер $\alpha \nmid 1$.

Уколико је $N(\alpha) > 2$, тада су α и $\overline{\alpha}$ узајамно прости. Нека је k изложилац броја α у факторизацији броја m. Тада $\alpha^k \mid m$, па и $\overline{\alpha}^k \mid m$, али не важи $\overline{\alpha}^{k+1} \mid m$, одакле следи да је изложилац броја $\overline{\alpha}$ у факторизацији броја m такође k, па је $N(\alpha) = \alpha\overline{\alpha} \mid m$. □

Теорема 8. *Сваки природан прост број p облика $4k+1$ се може записати као збир два квадрата природних бројева.*

Доказ. Пошто је $p = 4k+1$, знамо да је[2] $\left(\frac{-1}{p}\right) = 1$, па самим тим постоји цео број m такав да $p \mid m^2+1$. Како p не дели ни $m-i$ ни $m+i$ (јер би у супротном $m \pm i$ могло да се запише као $px + pyi$, за неке целе x и y, што свакако није могуће), p није прост у Гаусовим целим бројевима, па постоје нека два нејединична броја α и β такви да је $p = \alpha\beta$. Норма броја p је $N(p) = p^2 \Rightarrow N(\alpha) = N(\beta) = p$. Нека је $\alpha = a + bi$, $N(\alpha) = a^2 + b^2$, односно $p = a^2 + b^2$, па је тврђење доказано. Овако се још и добија да је $\beta = a - bi$, односно $\beta = \overline{\alpha}$. □

Последица 2. *Сваки прост број облика $4k+1$ се може записати као производ простог Гаусовог целог броја и његовог конјугата.*

Став 8. *Ако је p прост цео број облика $4k+3$, онда је он и Гаусов прост број.*

Доказ. Претпоставимо супротно, постоје нејединични бројеви α и β такви да је $p = \alpha\beta$. Норма броја p једнака је $N(p) = p^2$, па следи да су норме бројева α и β једнаке p. Ово није могуће с обзиром на то да Диофантова једначина $x^2 + y^2 = p$ нема решења у скупу целих бројева. □

Лема 3. *Ако је p прост број облика $4k+3$ такав да $p \mid a^2+b^2$, онда и $p^2 \mid a^2+b^2$, и такође $p \mid a, b$.*

Доказ. Како $p \mid a^2 + b^2$, следи да $p \mid (a+bi)(a-bi)$, али пошто је p прост број и у прстену $\mathbb{Z}[i]$, он мора да дели и неки од ова два броја. Без умањења општости, нека $p \mid a + bi$. На основу става 1, $\overline{p} \mid \overline{a+bi}$, односно $p \mid a - bi$, па самим тим $p^2 \mid a^2 + b^2$. Како $p \mid a + bi$, то значи да је $a + bi = p(x + yi) = px + pyi \Rightarrow p \mid a, b$. □

Последица 3. *Нека је v_p потенција простог броја p. Имамо да је $2 \mid v_p\big(N(\alpha)\big)$ за прост број p облика $4k+3$.*

Теорема 9. *Гаусов цео број α је прост $\iff$ α задовољава једну од следећих својстава:*

- *$N(\alpha)$ је прост природан број;*
- *$\alpha \sim p$, где је $p \in \mathbb{N}$ прост број облика $4k+3$.*

Доказ. ($\Leftarrow$) Доказ директно следи из става 8 и последице 1.

($\Rightarrow$) Број 2 није прост у $\mathbb{Z}[i]$ јер је $2 = (1+i)(1-i)$. Уколико је α еквивалентан сложеном природном броју, очигледно је сложен у прстену $\mathbb{Z}[i]$. На основу последице 2, прост број облика $4k+1$ не може бити прост у $\mathbb{Z}[i]$. Једино нам преостаје да покажемо да Гаусов цео број са сложеном нормом нееквивалентан природном броју не може бити уједно и прост у Гаусовим целим бројевима. Сада, нека је α такав да му је норма сложен број. Нека су p и q различити прости бројеви такви да $p, q \mid N(\alpha) = \alpha\overline{\alpha}$. Ако је p или q облика $4k+3$ (без умањења општости, нека је то p), на основу леме 3 $p \mid \alpha, \overline{\alpha}$ и тада је $\beta = \dfrac{\alpha}{p} \in \mathbb{Z}[i]$, а пошто α није еквивалентан природном броју, тада β није јединични елемент, па је α сложен. Уколико ни p ни q нису облика $4k+3$, они се могу представити као $p = \eta\overline{\eta}$ и $q = \vartheta\overline{\vartheta}$, где су η и ϑ Гаусови прости такви да бар један од бројева $\eta\vartheta, \overline{\eta}\vartheta$ дели α. Како Гаусов сложен број дели α, тада је и α сложен.

□

[2] Ово се једноставно показује Ојлеровим критеријумом

Теорема 10. *Природан број n се може представити као збир два квадрата целих бројева акко је у његовој канонској факторизацији изложилац сваког простог броја облика $4k+3$ паран.*

Доказ. ($\Rightarrow$) Доказ директно следи из последице 3.

($\Leftarrow$) На основу теореме 8, ако прост број p_i облика $4k+1$ дели n, тада се p_i може представити као $\alpha_i\overline{\alpha}_i$. Нека q_j представља сваки прост број облика $4k+3$, и нека је његов изложилац једнак $2t_j$, и коначно, нека 2^m тачно дели n. Можемо формирати Гаусов цео број $\beta = (1+i)^m \prod_{p_i|n, q_j|n} q_j^{t_j}\alpha_i$ са особином да је $n = \beta\overline{\beta}$. Ако β представимо као $a+bi$, тада је $n = a^2+b^2$ што је и требало показати.

□

1.3 Број начина да се природан број представи као збир квадрата два цела броја

У овом делу ћемо се бавити бројем решења једначине $n = x^2+y^2$ у скупу $\mathbb{Z}$, у зависности од природног броја n.

Најпре, позабавићемо се једноставнијим случајем, односно, претпоставимо да n има искључиво просте делиоце облика $4k+1$. Факторизација n у природним бројевима је тада $\prod_{i=1}^{k} p_i^{t_i}$.
Приметимо да је једначина $n = x^2+y^2$ еквивалентна једначини $n = (x+yi)(x-yi)$, односно $n = (x+yi)\overline{(x+yi)}$. Како смо показали да прост број p конгруентан 1 при дељењу са 4 може да се запише као производ два Гаусова проста броја $\pi\overline{\pi}$, факторизација у прстену $\mathbb{Z}[i]$ броја n изгледа овако:

$$n = \prod_{i=1}^{k} \pi_i^{t_i} \cdot \overline{\pi_i}^{t_i},$$

где су π_i Гаусови прости бројеви. Нека је $n = \alpha\overline{\alpha}$. Приметимо да је број различитих α које задовољавају ову једначину једнак броју решења почетне једначине. Како су α и $\overline{\alpha}$ комплексно конјуговани, уколико је експонент простог броја ψ у факторизацији броја α једнак t, тада је експонент $\overline{\psi}$ у $\overline{\alpha}$ такође t. Сада, за сваки p_i^t, можемо изабрати колико се π_i, а колико $\overline{\pi}_i$ налази у α. Тај број је $t+1$, па добијамо да је укупан број различитих α једнак

$$\prod_{i=1}^{k}(t_i+1).$$

Овде није крај, с обзиром на то да је факторизација броја p јединствена у $\mathbb{Z}[i]$ само до на еквивалентност простих чинилаца, односно ако је $p = \pi\overline{\pi}$, постоји и $p = i\pi\cdot(-i)\overline{\pi}$, али макроскопски гледано, све те факторизације множе α јединичним бројем. Како јединичних бројева има 4, сазнајемо да је коначан број решења заправо

$$4\prod_{i=1}^{k}(t_i+1).$$

Покушајмо сада да пронађемо број решења када је n произвољан непаран број.
Овде ћемо се концентрисати на просте бројеве q облика $4k+3$ јер су нам они новина. На основу леме 3, изложиоци таквих простих бројева у канонској факторизацији броја n морају бити парни да би једначина уопште имала решење. Како знамо да сада $q = 4k+3$ мора да испуњава особину да $q^{2m} \parallel n$, наше првобитне α и $\overline{\alpha}$ можемо помножити

са q^m, и добити нови број. Уколико овај поступак применимо на сваки прост број тог облика, добијамо наше нове α и $\overline{\alpha}$. Број њих овим додатком остаје непромењен јер постоји јединствен распоред простих бројева облика $4k+3$.

Последње на шта треба да обратимо пажњу су степени двојке који деле n. Шта би се десило уколико наше n помножимо са 2. Приметимо да је $2=(1+i)(1-i)$. На први поглед, делује нам као да двојка утиче на исти начин као што утичу и прости бројеви облика $4k+1$, али то заправо није баш тако. Имајући у виду да су $1+i$ и $1-i$ комплексно конјуговани, и да је $1+i=i(1-i)$, њихова размена бројеве α и $\overline{\alpha}$ заправо множи са i, односно $-i$, што смо већ урачунали. Дакле, степени броја 2 не утичу на коначан број различитих α, па самим тим, за број

$$n=2^a\prod_{i=1}^{k}p_i^{b_i}\cdot\prod_{j=1}^{l}q_j^{c_j},$$

једначина има $4\prod_{i=1}^{k}(b_i+1)$ решења када је $\prod_{i=1}^{l}(c_i+1)$ непаран, а 0 у супротном, где су бројеви p_i облика $4k+1$, а бројеви q_i облика $4k+3$.

1.4 Конгруенције у прстену Гаусових целих бројева

Видели смо да у прстену $\mathbb{Z}[i]$ имамо просте и сложене бројеве, дељивост и факторизацију, дељење са остатком и највећи заједнички делилац. Логичан следећи корак би био увести конгруенције и операције над њима.

Дефиниција 11. *Два Гаусова цела броја α и β су* **конгруентни по модулу** *μ ако μ дели њихову разлику. Тада пишемо $\alpha\equiv\beta \pmod{\mu}$.*

Као и код целих бројева, конгруенција по модулу је релација еквиваленције, и целе бројеве је могуће распоредити по тим класама, тако да се сви бројеви који су међусобно конгруентни распореде унутар исте класе. Сличан појам уводимо и овде.

Став 9. *Релација конгруенције по модулу μ у прстену $\mathbb{Z}[i]$ је релација еквиваленције.*

Доказ. Лако се показују особине рефлексивности, симетричности и транзитивности. □

Теорема 11. *Ако је $a+bi\equiv c+di \pmod{m}$, за неки цео број m, тада је $a\equiv c \pmod{m}$ $\wedge$ $b\equiv d \pmod{m}$.*

Доказ. $a+bi\equiv c+di \pmod{m}$ је из дефиниције еквивалентно са $m\mid(a-c)+(b-d)i$, а из последње тврдње става 1, следи да $m\mid a-c$ и $m\mid b-d$, односно $a\equiv c \pmod{m}\wedge b\equiv d \pmod{m}$. □

Став 10. *За целе бројеве a, b и m важи $a\equiv b \pmod{m}$ у $\mathbb{Z}[i]\iff a\equiv b \pmod{m}$ у $\mathbb{Z}$.*

Доказ. Доказ се лако показује у оба смера користећи став 1. □

И, коначно, да уведемо класе еквиваленције.

Дефиниција 12. Класа остатака *Гаусовог целог броја α по модулу μ је скуп бројева $\underline{\alpha_\mu}=\{\beta\in\mathbb{Z}[i]\mid\alpha\equiv\beta \pmod{\mu}\}$ такав да свака два конгруентна броја по модулу μ буду у истој класи. Скуп свих класа остатака по модулу μ означавамо $(\mathbb{Z}[i]/\mu)$.*

Битно је рећи да код једначина са конгруенцијом по неком модулу μ јединственост решења подразумева да за нека два решења χ_1 и χ_2 важи $\chi_1\equiv\chi_2 \pmod{\mu}$. Тада су χ_1 и χ_2 еквивалентна решења те једначине.

Теорема 12. *За Гаусове целе бројеве α, γ и $\beta \neq 0$, такви да су α и β узајамно прости, једначина $\alpha\chi \equiv \gamma \pmod{\beta}$ има јединствено решење.*

Доказ. Једначина $\alpha\chi \equiv 1 \pmod{\beta}$ је еквивалентна једначини $\chi\alpha + \upsilon\beta = 1$, што је еквивалентно са тим да су α и β узајмно прости. Докажимо да је решење јединствено. Нека су χ_1 и χ_2 решења. Како $\beta \mid \alpha\chi_1 - 1$ и $\beta \mid \alpha\chi_2 - 1$, тада $\beta \mid \alpha(\chi_1 - \chi_2)$, а пошто су α и β узајамно прости, $\beta \mid \chi_1 - \chi_2$, па они морају бити конгруентни. □

Лема 4. *Нека су $\alpha_1, \alpha_2, \ldots, \alpha_n$ Гаусови цели бројеви такви да су свака два узајамно прости. Уколико за свако $i \in \{1, 2, \ldots, n\}$ важи $\alpha_i \mid \beta$ за неки $\beta \in \mathbb{Z}[i]$, тада $\alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_n \mid \beta$.*

Доказ. Доказаћемо тврђење индукцијом.
(База индукције) За $n = 2$, имамо да су α_1 и α_2 узајамно прости, па постоје κ и λ такви да је $\kappa\alpha_1 + \lambda\alpha_2 = 1$. Сада, нека је $\beta = \beta_1\alpha_1 = \beta_2\alpha_2$. Множећи обе стране једначине са β добијамо да је

$$\beta = \beta\kappa\alpha_1 + \beta\lambda\alpha_2 = \beta_2\kappa\alpha_1\alpha_2 + \beta_1\lambda\alpha_1\alpha_2 = \alpha_1\alpha_2(\beta_2\kappa + \beta_1\lambda),$$

одакле закључујемо да $\alpha_1\alpha_2 \mid \beta$.
(Индуктивна хипотеза) Претпоставимо да за неко $n \geq 2$ важи тврђење.
(Индуктивни корак) Нека су $\alpha_1, \alpha_2, \ldots, \alpha_n, \alpha_{n+1} \in \mathbb{Z}[i]$ по паровима узајамно прости такви да за свако $i \in \{1, 2, \ldots, n+1\}$ важи $\alpha_i \mid \beta$. На основу индуктивне хипотезе знамо да $\alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_n \mid \beta$. Применом теореме 4, α_{n+1} је узајамно просто са $\alpha_1\alpha_2$. Ако поновимо овај процес, α_{n+1} је узајамно просто са $\alpha_1\alpha_2\alpha_3$, итд., α_{n+1} је узајамно просто са $\alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_n$. Сада применом базе индукције, за узајамно просте бројеве α_{n+1} и $\alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_n$ који деле β, знамо да и њихов производ такође дели β чиме смо доказали лему. □

Теорема 13 (Кинеска теорема о остацима). *Нека су дати по паровима узајамно прости бројеви $\alpha_1, \alpha_2, \ldots, \alpha_n$. Тада систем једначина*

$$\chi \equiv \beta_1 \pmod{\alpha_1} \tag{1.1}$$
$$\chi \equiv \beta_2 \pmod{\alpha_2} \tag{1.2}$$
$$\vdots \tag{1.3}$$
$$\chi \equiv \beta_n \pmod{\alpha_n} \tag{1.4}$$
$$\tag{1.5}$$

има јединствено решење при модулу $\alpha_1\alpha_2 \ldots \alpha_n$.

Доказ. Нека је $\mu = \alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_n$, и нека је $\gamma_i = \dfrac{\mu}{\alpha_i}$. Применом теореме 4 лако се провери да је γ_i узајамно просто са α_i. На основу теореме 12, знамо да постоје Гаусови цели бројеви γ_i^{-1} који задовољавају $\gamma_i\gamma_i^{-1} \equiv 1 \pmod{\alpha_i}$. Приметимо да

$$\chi = \sum_i^n \beta_i\gamma_i\gamma_i^{-1}$$

задовољава цео систем. Преостаје да покажемо јединственост. Ако ζ задовољава i-ту једначину, тада је $\chi - \zeta$ дељиво са α_i, па је, на основу леме 4, $\zeta \equiv \chi \pmod{\mu}$. □

Дефиниција 13. *Кажемо за Гаусов цео број α да је* **инвертибилан** *мод μ уколико једначина $\alpha\chi \equiv 1 \pmod{\mu}$ има решење.*

Показали смо у теореми 12 да је α инвертибилан мод β акко су α и β узајамно прости.

Сада нас интересује колико заправо различитих остатака имамо при дељењу неким бројем. То је мало теже формулисати тако, али срећом увели смо класе остатака које нам помажу са тим.

Дефиниција 14. *За Гаусов цео број $\mu \neq 0$ уводимо позитиван природан број $n(\mu)$ као* **број различитих класа остатака по модулу** *μ.*

Најпре, битно је да покажемо да тај број заправо постоји, тј. да нема бесконачно остатака по модулу.

Став 11. *За свако $\alpha \in \mathbb{Z}[i] \setminus \{0\}$, $n(\alpha) < \infty$.*

Доказ. Због дељења са остатком, свака класа остатака има елемент мање норме од $N(\alpha)$. Односно, знамо да за неки конкретан број ϑ постоје υ и ρ за које важи $N(\rho) \leq \frac{1}{2}N(\alpha)$ и $\vartheta - \rho = \alpha\upsilon$, тј $\alpha \mid \vartheta - \rho$ што је еквивалентно са $\vartheta \equiv \rho \pmod{\alpha}$, па је $\rho \in \underline{\vartheta_\alpha}$. Како бројева чија је норма мања или једнака половини $N(\alpha)$ има коначан број, тврђење става директно следи. □

Прво ћемо тачну вредност броја $n(\alpha)$ одредити за целе бројеве, јер су ту ствари једноставније.

Лема 5. *За цео број $m \neq 0$ број различитих класа остатака при дељењу са m има m^2.*

Доказ. За бројеве $\alpha = a + bi$ и $\xi = x + yi$ конгруенција $\alpha \equiv \xi \pmod{m}$ је еквивалентна са $a \equiv x \pmod{m}$ у $\mathbb{Z} \wedge b \equiv y \pmod{m}$ у $\mathbb{Z}$. Како a и b могу узети сваки по m вредности, укупан број различитих вредности за α је $m \cdot m$, односно m^2. □

Лема 6. *За Гаусов цео број $\alpha \neq 0$ важи $n(\alpha) = n(\overline{\alpha})$.*

Доказ. Из става 1 имамо да је $\alpha \mid \xi - \zeta$ еквивалентно са $\overline{\alpha} \mid \overline{\xi} - \overline{\zeta}$, односно постоји бијекција која слика сваку класу остатака $\underline{\xi_\alpha}$ у $\underline{\overline{\xi}_{\overline{\alpha}}}$, па је $n(\alpha) = n(\overline{\alpha})$. □

Лема 7. *За Гаусове целе бројеве α и β ($\alpha, \beta \neq 0$) важи $n(\alpha\beta) = n(\alpha)n(\beta)$.*

Доказ. Нека је $n(\alpha) = m$ и $n(\beta) = n$, и нека су $\xi_1, \xi_2, \ldots \xi_m$ и $\zeta_1, \zeta_2, \ldots \zeta_n$ представници свих класа при дељењу са α и β редом. Нека је $\chi \in \mathbb{Z}[i]$, и нека је $\chi \equiv \xi_i \pmod{\alpha}$, односно $\chi - \xi_i = \alpha\vartheta$ за неко $\vartheta \in \mathbb{Z}[i]$ и нека је $\vartheta \equiv \zeta_j \pmod{\beta}$, па је $\vartheta = \zeta_j + \beta\omega$ за неки Гаусов цео број ω. Тада је $\chi = \xi_i + \alpha\zeta_j + \alpha\beta\omega$, тј. $\chi \equiv \xi_i + \alpha\zeta_j \pmod{\alpha\beta}$, па смо показали да је $n(\alpha\beta) \leq mn$.

Остаје нам да покажемо да нема понављања међу ових mn бројева, односно претпоставимо да важи:

$$\xi_i + \alpha\zeta_j \equiv \xi_{i'} + \alpha\zeta_{j'} \pmod{\alpha\beta},$$

докажимо $(i, j) = (i', j')$.

Из претпоставке добијамо да је $\xi_i \equiv \xi_{i'} \pmod{\alpha}$, али, по начину на који смо их бирали, мора следити да је $i = i'$, па нам преостаје $\alpha\zeta_j \equiv \alpha\zeta_{j'} \pmod{\alpha\beta}$, односно $\zeta_j \equiv \zeta_{j'} \pmod{\beta}$, али из истог разлога следи да је $j = j'$, па је тврђење доказано. □

Сад смо довољно припремљени да израчунамо конкретну вредност n функције.

Теорема 14. *За Гаусов цео број $\alpha \neq 0$ важи релација $n(\alpha) = N(\alpha)$.*

Доказ. Како је, на основу леме 5, $n(N(\alpha)) = N(\alpha)^2$, односно $n(\alpha\overline{\alpha}) = N(\alpha)^2$, а применом леме 6 и леме 7 добијамо да је $n(\alpha)^2 = N(\alpha)^2$, али како су $n(\alpha)$ и $N(\alpha)$ позитивни цели бројеви, једноставним коренованјем обе стране, добијамо да је $n(\alpha) = N(\alpha)$. □

1.4.1 Мала Фермаова теорема

Када би неко покушао наивно да „преведе" малу Фермаову теорему у $\mathbb{Z}[i]$ вероватно би рекао нешто попут $\alpha^{\pi-1} \equiv 1 \pmod{\pi}$. Првенствено, $\alpha^{\pi-1}$ не значи ништа (осим у комплексној анализи, али чак и тада то не би био елемент прстена Гаусових целих бројева), а друго, $p-1$ у једначини $a^{p-1} \equiv 1 \pmod{p}$ означава нешто друго - број ненула елемената у $\mathbb{Z}_p$. Свакако, постоји лепо проширење мале Фермаове теореме на $\mathbb{Z}[i]$.

Теорема 15 (Мала Фермаова теорема). *Нека је π прост Гаусов цео број, и нека је α недељив бројем π, тада важи $\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}$.*

Доказ. Како знамо да је $N(\pi) = n(\pi)$, нека су $\nu_1, \nu_2, \ldots, \nu_{N(\pi)}$ различити представници класа остатака при дељењу са π, при чему је $\nu_{N(\pi)} = 0$. Пошто $\pi \nmid \alpha$, они су узајамно прости, па (због теореме 10) $\alpha\nu_1, \alpha\nu_2, \ldots, \alpha\nu_{N(\pi-1)}$ заправо представља пермутацију низа $\nu_1, \nu_2, \ldots, \nu_{N(\pi)} \pmod{\pi}$. Када измножимо обе пермутације и изједначимо их $\alpha^{N(\pi)-1}\nu_1\nu_2 \ldots \nu_{N(\pi)} \equiv \nu_1\nu_2 \ldots \nu_{N(\pi)} \pmod{\pi}$. Пошто је сваки ν_j узајамно прост са π, можемо га скратити, одакле директно доказујемо теорему. □

Уколико се присетимо доказа мале Фермаове теореме у $\mathbb{Z}$, који је малтене исти у $\mathbb{Z}[i]$, што нам указује колико су заправо Гаусови цели бројеви слични са целима.

Пример 2. *Увидимо на примеру $\pi = 7$, $\alpha = i$, „неправилна теорема" $\alpha^{\pi-1} \equiv 1 \pmod{\pi}$ не ради чак ни када је изложилац цео број. Наиме, -1 није конгруентно са 1 при модулу 7, иако је 7 прост у $\mathbb{Z}[i]$.*

1.4.2 Ојлерова фи функција

Као што знамо, мала Фермаова теорема је само специјалан случај Ојлерове теореме која не захтева да модул буде прост број. Уколико се присетимо како гласи Ојлерова теорема, приметићемо да постоји $\varphi(n)$, функција која броји колико има бројева мањих од n узајамно простих са n. Тешко је директно одатле дефинисати аналогију са Гаусовим целим бројевима, али можемо је увести на следећи начин.

Дефиниција 15 (Ојлерова фи функција). *За Гаусов цео број $\alpha \neq 0$ функција $\phi(\alpha)$ даје број класа остатака при дељењу са α чији су представници инвертибилни по модулу α.*

Пре него што кренемо да рачунамо неке вредности ϕ функције, показаћемо да важи Ојлерова теорема и у $\mathbb{Z}[i]$.

Теорема 16 (Ојлерова теорема). *За узајамно просте Гаусове целе бројеве μ и α, важи $\alpha^{\phi(\mu)} \equiv 1 \pmod{\mu}$.*

Доказ. Нека је $n = \phi(\mu)$, и нека су $\nu_1, \nu_2, \ldots \nu_n$ инвертибилни представници различитих класа остатака при дељењу са μ. Пошто је α узајамно прост са μ, због инвертибилности α и представника класа, низ $\alpha\nu_1, \alpha\nu_2, \ldots, \alpha\nu_n$ је пермутација низа $\nu_1, \nu_2, \ldots \nu_n \pmod{\mu}$. Множећи елементе обе пермутације и изједначавајући их добијамо $\alpha^{\phi(\mu)}\nu_1\nu_2 \ldots \nu_n \equiv \nu_1\nu_2 \ldots \nu_n \pmod{\mu}$, а како су сви ν_j узајамно прости са μ, можемо их скратити и тако директно доказати тврђење теореме. □

Као и код мале Фермаове теореме, доказ је скоро па идентичан као и код целих бројева. Чак се и да приметити да је $\phi(\pi) = N(\pi) - 1$, што је добра увертира за следећи део.

Теорема 17. *За Гаусов прост број π вредност функције $\phi(\pi^t)$ је једнака $N(\pi)^{t-1}(N(\pi)-1)$.*

Доказ. Како смо показали да различитих класа остатака при дељењу са π^t има тачно $N(\pi^t)$, од тога треба одузети број оних који су дељиви са π да бисмо добили $\phi(\pi^t)$. Избројмо сада колико има дељивих са π. Тада ти остаци морају бити облика $\pi\alpha$. Како важи да је $\pi\alpha \equiv \pi\beta \pmod{\pi^t} \iff \alpha \equiv \beta \pmod{\pi^{t-1}}$, имамо бијекцију између тих остатака и свих остатака при дељењу са π^{t-1}, а како знамо да таквих има $N(\pi)^{t-1}$, добијамо да је $\phi(\pi^t) = N(\pi)^{t-1}(N(\pi)-1)$. □

Да се наслутити да је ϕ функција мултипликативна, попут њеног аналогона, φ функције у $\mathbb{Z}$.

Теорема 18. *Уколико су α и β узајамно прости Гаусови цели бројеви, тада важи релација $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta)$.*

Доказ. Приметимо најпре да је доказ теореме еквивалентан доказивању да постоји бијекција између $(\mathbb{Z}[i]/\alpha\beta)$ и $(\mathbb{Z}[i]/\alpha) \times (\mathbb{Z}[i]/\beta)$. Доказ те тврдње следи директно из кинеске теореме о остацима, односно да постоји јединствено решење по модулу $\alpha\beta$ система

$$\zeta \equiv \xi \pmod{\alpha}, \tag{1.6}$$
$$\zeta \equiv \upsilon \pmod{\beta}. \tag{1.7}$$

Одавде, сликајући број ζ у (ξ, υ) остварујемо поменуту бијекцију чиме је доказ завршен. □

Последица 4. *Како смо израчунали вредност ϕ функције за степене простих бројева, и доказали мултипликативност, сада је могуће израчунати њену вредност за било који Гаусов цео број.*

$$\phi(\alpha) = N(\alpha) \prod_{\pi_i \mid \alpha} \left(1 - \frac{1}{N(\pi_i)}\right),$$

где за свако различито i и j, $\pi_i \not\sim \pi_j$.

1.4.3 Вилсонова теорема

Као и код мале Фермаове теореме, лако се може погрешно закључити аналогија Вилсонове теореме у целим бројевима. $(\pi-1)! \equiv -1 \pmod{\pi}$, за прост број π нема смисла јер факторијел није дефинисан за комплексне бројеве (осим ако не посматрамо гама функцију, али тек тада постаје бесмислено). Простом заменом броја $\pi-1$ његовом нормом ($(N(\pi)-1)!$ уместо $(\pi-1)!$) се добија тражена конгруенција, али најпре морамо видети шта се крије иза тога.

Главна ствар је опет посматрати суштину теореме на мало другачији начин. Шта нам представља $(p-1)!$ у целим? То је заправо производ свих ненула елемената у $\mathbb{Z}_p$, односно производ представника свих инвертибилних класа остатака при дељењу са p. Исту ствар ћемо урадити и у $\mathbb{Z}[i]$, помножићемо све ненула остатке при дељењу са π, и посматрати шта се ту дешава.

Најпре, треба да докажемо пар лема ради лакшег доказивања Вилсонове теореме.

Лема 8 (Безуов став)**.** *Нека је дат прстен F, и нека је $P(x)$ полином у $F[x]$. Тада је $P(x)$ дељиво линеарним мономом $x-a$ ($a \in F$) акко је $P(a) = 0$.*

Доказ. Доказ је идентичан доказу у пољу реалних бројева. □

Лема 9. *Нека је дат комутативан прстен F који је интегрални домен, и нека је $P(x)$ полином у $F[x]$ степена n. Постоји највише n различитих решења једначине $P(x) = 0$ у F.*

Доказ. Показаћемо индукцијом. За $n = 1$ видимо полином $x - t$ има јединствено решење $x = t$, и да нити један други елемент у F није решење. Сада, претпоставимо да за $n-1$ важи тврђење леме. На основу Безуовог става закључујемо да уколико је a решење једначине $P(x) = 0$ у F, тада постоји полином $Q(x)$ степена $n - 1$ такав да је $P(x) = (x - a)Q(x)$. Уколико је $c \neq a$ такође решење једначине $P(x) = 0$, тада је c такође и решење једначине $Q(x) = 0$ (зато што је F интегрални домен) јер у супротном ни $c - a$ ни $Q(c)$ не би били 0, чиме смо и показали тврђење. □

Подразумеваћемо дефиниције поретка и примитивног корена у комутативним прстенима, али ћемо увести исте у Гаусовим целим бројевима, такође у даљем делу рада, подразумеваћемо да су сви прстени комутативни.

Дефиниција 16. Поредак *Гаусовог целог броја α по модулу μ је најмањи природан број n такав да је $\alpha^n \equiv 1 \pmod{\mu}$.*

Дефиниција 17. *Гаусов цео број α је* **примитивни корен** *по модулу μ уколико важи да су α и μ узајамно прости и да је поредак броја α по модулу μ једанк $\phi(\mu)$.*

Примитивни корен нам игра значајну улогу јер се у низу $\gamma, \gamma^2, \gamma^3, \ldots, \gamma^{\phi(\mu)}$ јављају представници свих инвертибилних класа остатака по модулу μ.

Лема 10. *Нека је M највећи поредак елемената F, коначног поља са јединицом. Тада сви остали пореци деле M.*

Доказ. Претпоставимо супротно. Нека $u \in F$ има поредак M, и нека постоји $w \in F$ које има поредак k такво да k не дели M. То значи да постоји прост број p такав да $p^f || M$ и $p^e || k$, где је $e > f$. Бројеви u^{p^f} и $w^{\frac{k}{p^e}}$ имају поретке $\frac{M}{p^f}$ и p^e редом, а како су ти пореци узајамно прости, поредак броја $u^{p^f} \cdot w^{\frac{k}{p^e}}$ је Mp^{e-f} што је веће од M, што је немогуће. □

Став 12. *Скуп $(\mathbb{Z}[i]/\pi)$ за Гаусов прост број π са операцијама множења и сабирања по модулу је коначно поље.*

Доказ. Лако се показују све особине поља. □

Сада ћемо показати постојање примитивног корена у овом скупу.

Лема 11. *Нека је дат Гаусов прост број π. Тада постоји примитивни корен γ по модулу π.*

Доказ. Нека је M максимални поредак по модулу π. Како сви остали пореци морају да деле M, тада једначина $\chi^M \equiv 1 \pmod{\pi}$ има $N(\pi) - 1$ решења, па је M барем $N(\pi) - 1$, а на основу мале Фермаове теореме, знамо да је M највише $N(\pi) - 1$, па стога елемент са највећим поретком јесте примитивни корен. □

Како смо показали постојање примитивног корена, доказивање Вилсонове теореме нам неће бити проблем.

Теорема 19 (Вилсонова теорема). *Производ представника свих инвертибилних класа остатака при дељењу са простим модулом π у $\mathbb{Z}[i]$ је конгруентан са -1 по модулу π.*

Доказ. Пошто је π прост, постоји примитивни корен γ, па се онда производ свих представника класа остатака може представити као

$$P = \gamma\gamma^2\gamma^3 \ldots \gamma^{t-1},$$

где је $t = N(\pi)$. Како је $P \equiv \gamma^{\frac{t(t-1)}{2}} \pmod{\pi}$, разликујемо два случаја.
Ако је t паран, тада је $\pi \sim 1+i$, па P даје остатак 1, али како је $1 \equiv -1 \pmod{1+i}$, тако је и $P \equiv -1 \pmod{\pi}$.
Ако је t непаран, тада имамо да је $\frac{t(t-1)}{2} \equiv \frac{t-1}{2} \pmod{t-1}$, па је $P^2 \equiv 1 \pmod{\pi}$, али како P никад није конгруентно са 1 при дељењу са π, следи да је $P \equiv -1 \pmod{\pi}$. □

1.5 Примене на такмичењима

Пошто смо видели да постоји велики број теорема које се могу применити на Гаусове целе бројеве, у овом делу ћемо неке од њих и искористити за решавање два задатка који су се јавили на такмичењима.

Задатак 1 (Изборно за ИМО 2021.). Дат је прост број p. Колико има уређених четворки (a, b, c, d) природних бројева који нису дељиви са p и задовољавају следеће једначине

$$ac + bd = p(a + c) \quad \text{и} \quad bc - ad = p(b - d)?$$

Решење. Дефинишимо α и β као $\alpha = a+bi$ и $\beta = c-di$ у $\mathbb{Z}[i]$. Приметимо да је дати систем једначина еквивалентан једначини $\alpha\beta = p(\alpha + \beta)$. Ову једначину можемо такође записати као и $(\alpha - p)(\beta - p) = p^2$. Разликујемо три случаја:

1) Ако је p облика $4k + 3$, тада је p такође прост и у $\mathbb{Z}[i]$, па он мора да дели бар један од бројева α и β што имплицира да $p \mid a, b$ или $p \mid c, d$, а то је у контрадикцији са условом задатка.

2) Ако је $p = 2$, тада је $p = (1 + i)(1 - i) = i(1 + i)^2$, односно $p^2 = -(1 + i)^4$, па је бар један од бројева α и β дељив бројем $(1+i)^2 = 2i$, па 2 дели бар један од бројева α и β, одакле следи да $2 \mid a, b$ или $2 \mid c, d$, што је исто у контрадикцији са условом задатка.

3) У случају $p = 4k + 1$, имамо да се p може представити као производ $\pi\overline{\pi}$, где је π Гаусов прост број облика $x + yi$, $x, y \in \mathbb{N}$. Из истог разлога као у претходна два случаја p не сме да дели ни α ни β, одакле добијамо да $\alpha - p$ и $\beta - p$ морају бити неки од $\pm\pi^2, \pm\overline{\pi}^2, \pm i\pi^2$ или $\pm i\overline{\pi}^2$. С обзиром да a, b, c и d морају бити природни, укупно имамо 4 решења.

□

Задатак 2 (ИМО 2016.). Дат је конвексан многоугао $P = A_1A_2 \dots A_k$ у равни. Темена $A_1, A_2, \dots, A_k$ имају целобројне координате и леже на истој кружници. Нека је S површина многоугла P. Непаран природан број n је такав да су квадрати дужина свих страница многоугла P природни бројеви дељиви са n. Доказати да је $2S$ цео број дељив са n.

Решење. Посматрајмо задатак у $\mathbb{Z}[i]$, и нека тачки A_i одговара Гаусов цео број $\zeta_i = x_i + iy_i$. Најпре ћемо показати да тврђење директно следи уколико покажемо да је n облика p^e за неки прост број $p \geq 3$.
Уколико је p облика $4t + 3$, имамо да $p^e \mid N(\zeta_{i+1} - \zeta_i)$, одакле следи да $p^f \mid \zeta_{i+1} - \zeta_i$, где је $f = \left\lceil \frac{e}{2} \right\rceil$, па су сви ζ_i међусобно конгруентни по модулу p^f. Сада, како површина остаје инваријантна након транслације за одређен вектор,„померићемо" целу раван за $-\zeta_1$, и тако добити k Гаусових целих бројева где су сви дељиви бројем p^f. Сада, имамо да је $2S = \sum(x_iy_{i+1} - x_{i+1}y_i) = \operatorname{Im}\left(\sum(\overline{\zeta}_i\zeta_{i+1})\right)$, где је сваки члан ове суме дељив бројем p^{2f}, што имплицира да је двострука површина дељива бројем n.

Ако је p облика $4t+1$, имамо да p може да се представи као $\pi\overline{\pi}$, где је π Гаусов прост број. Нека су $v_\pi(\chi)$ и $v_{\overline{\pi}}(\chi)$ редом изложиоци бројева π и $\overline{\pi}$ редом у канонској факторизацији броја χ. Како $p^e \mid N(\zeta_{i+1}-\zeta_i)$, имамо да је $v_\pi(\zeta_{i+1}-\zeta_i)+v_{\overline{\pi}}(\zeta_{i+1}-\zeta_i)\geq e$.
Сада тврдимо следеће: *Постоји тријангулација многоугла таква да за сваки троугао постоји* $0\leq s\leq e$ *за који* $\pi^s\overline{\pi}^{e-s}$ *дели све векторе страница.*
Ову тврдњу ћемо показати индукцијом по e. За $e=1$, сваки вектор странице је умножак броја π или $\overline{\pi}$. Ако постоје два узастопна вектора страница дељива са π можемо исећи троугао формиран од те две странице (то јест те три тачке) и остаће нам мањи многоугао чије су све странице дељиве или са π или са $\overline{\pi}$, па на основу индукције по броју страница добијамо да постоји таква тријангулација. Аналогно за две узастопне странице дељиве са $\overline{\pi}$.
Сада, уколико не постоје две узастопне странице дељиве са π или $\overline{\pi}$, то значи да се наизменично мењају умношци бројева π и $\overline{\pi}$, и да број страница мора бити паран. Зато, нека је $k=2l$ и без умањења општости нека $q\mid\zeta_1-\zeta_2$. Због концикличности тачака знамо да

$$\frac{(\zeta_1-\zeta_2)(\zeta_3-\zeta_4)\cdots(\zeta_{2l-1}-\zeta_{2l})}{(\zeta_2-\zeta_3)(\zeta_4-\zeta_5)\cdots(\zeta_{2l}-\zeta_1)}$$

мора бити реалан број, односно он је једнак свом коњугату, одакле имамо да је

$$(\zeta_1-\zeta_2)\cdots(\zeta_{2l-1}-\zeta_{2l})(\overline{\zeta}_2-\overline{\zeta}_3)\cdots(\overline{\zeta}_{2l}-\overline{\zeta}_1)=(\overline{\zeta}_1-\overline{\zeta}_2)\cdots(\overline{\zeta}_{2l-1}-\overline{\zeta}_{2l})(\zeta_2-\zeta_3)\cdots(\zeta_{2l}-\zeta_1).$$

Лева страна је дељива бројем π^{2l}, док десна страна није уопште дељива бројем π, одакле следи контрадикција.

Ако је $e\geq 2$, претпоставимо да тврђење важи за $e-1$. Користећи индуктивну хипотезу директно за $e-1$ видимо да постоји тријангулација таква да су све странице умношци броја $\pi^s\overline{\pi}^{e-1-s}$. Претпоставимо да је s другачије за два различита троугла. Можемо претпоставити да та два троугла деле страницу јер постоји „пут" троуглова од једног до другог. Сада, нека су странице једног троугла умношци броја $\pi^{s_1}\overline{\pi}^{e-1-s_1}$, а другог $\pi^{s_2}\overline{\pi}^{e-1-s_2}$, где је $s_1<s_2$. Заједничка ивица мора бити умножак броја $\pi^{s_2}\overline{\pi}^{e-1-s_1}$, односно њен квадрат мора бити дељив бројем $p^{e-1-s_1+s_2}$, што је дељиво бројем p^e. Ова страница мора бити дијагонала па можемо поделити многоугао том дијагоналом на два мања за које важи индуктивна претпоставка.

Ако све странице имају исто s, цео многоугао мора бити дељив бројем $\pi^s\overline{\pi}^{e-1-s}$, па га можемо хомотетисати (поделити га са $\pi^s\overline{\pi}_{e-1-s}$) и добити многоугао чији су квадрати страница умношци броја p. Сада, можемо применити случај $e=1$ на хомотетисани многоугао и видети да и он може бити тријангулиран. Множећи назад све са $\pi^s\overline{\pi}^{e-1-s}$, добијамо тијангулацију почетног полигона таквог да је свака страница сваког троугла умножак $\pi^s\overline{\pi}^{e-s_1}$ или $\pi^{s+1}\overline{\pi}^{e-1-s_1}$, па је и овај случај покривен.
Овиме смо доказали нашу тврдњу, сада преостаје да се вратимо на почетак проблема и уочимо да је многоугао подељен у троуглове чије су странице умношци броја $\pi^s\overline{\pi}^{e-s}$ за неко s. Двострука површина сваког троугла мора бити дељива бројем $N(\pi^s\overline{\pi}^{e-s})=p^e$, па је и читава двострука површина дељива бројем $p^e=n$. □

2 Ајзенштајнови цели бројеви

Поред Гаусових целих бројева постоје и Ајзенштајнови цели бројеви који су такође раширење скупа целих бројева. Као и у претходном делу рада, уколико то није другачије наглашено, грчка слова (осим ω) означавају Ајзенштајнове целе бројеве, док су бројеви из скупа $\mathbb{Z}$ означени словима енглеске латинице.
Пошто су теореме, ставови и леме малтене идентични као и у $\mathbb{Z}[i]$, доказе ћемо наводити искључиво ако се суштински разликују од оних у претходном поглављу.

2.1 Дефиниција и основни појмови

Уместо четвртог корена броја 1 (број i), Ајзенштајнови цели бројеви се баве трећим кореном јединице.

Дефиниција 18. Ајзенштајнов цео број *је сваки комплексан број облика* $a + b\omega$, *где су* a *и* b *цели, док је* $\omega = \dfrac{-1 + i\sqrt{3}}{2}$. *Скуп Ајзенштајнових целих бројева означаваћемо са* $\mathbb{Z}[\omega]$.

Теорема 20. *Скуп* $\mathbb{Z}[\omega]$ *са стандардним операцијама сабирања и множења образује комутативни прстен са јединицом.*

Доказ. Лако се проверавају све аксиоме комутативног прстена. □

Дефиниција 19. *Кажемо да број* α **дели** *број* β *уколико постоји* γ *такво да је* $\beta = \gamma\alpha$. *Ово математички записујемо као* $\alpha \mid \beta$.

Став 13. *Нека су* α, β *и* γ *Ајзенштајнови цели бројеви, тада важи:*

- $\alpha \mid \alpha$,
- $\alpha \mid \beta \wedge \beta \mid \gamma \Rightarrow \alpha \mid \gamma$,
- $\delta \mid \alpha \wedge \delta \mid \beta \Rightarrow \delta \mid \alpha + \beta$,
- $\big(\forall \kappa \in \mathbb{Z}[\omega]\big)\delta \mid \alpha \Rightarrow \delta \mid \kappa\alpha$,
- $\alpha \mid \gamma \wedge \beta \mid \delta \Rightarrow \alpha\beta \mid \gamma\delta$,
- $\alpha\beta \mid \alpha\gamma \wedge \alpha \neq 0 \Rightarrow \beta \mid \gamma$,
- $\alpha \mid \beta \Rightarrow \overline{\alpha} \mid \overline{\beta}$.
- $m \mid a + bi \Rightarrow m \mid a \wedge m \mid b$.

Доказ. Лако се проверава из дефиниције. □

Норму Ајзенштајновог целог броја такође дефинишемо као квадрат модула комплексног броја.

Дефиниција 20. *За $\alpha = a + b\omega$, ненегативан цео број $N(\alpha) = a^2 - ab + b^2$ представља* **норму** *Ајзенштајновог целог броја α. Норма броја α се такође може записати као $N(\alpha) = \alpha\overline{\alpha}$.*

Став 14. *За Ајзенштајнове целе бројеве α и β важи $N(\alpha\beta) = N(\alpha)N(\beta)$.*

Став 15. *За Гаусове целе бројеве α и β важи $N(\alpha\beta) = N(\alpha)N(\beta)$.*

Доказ. Како су $\alpha, \beta \in \mathbb{C}$, и важи да је $N(\gamma) = |\gamma|^2$, тада је $N(\alpha)N(\beta) = |\alpha|^2|\beta|^2 = |\alpha\beta|^2 = N(\alpha\beta)$. □

Да бисмо показали да је $\mathbb{Z}[\omega]$ еуклидски домен, потребно нам је дељење са остатком.

Теорема 21. *За бројеве α и $\beta \neq 0$ постоје Ајзенштајнови цели бројеви υ и ρ такви да је $\alpha = \upsilon\beta + \rho$ и где је $N(\rho) \leq \frac{\sqrt{3}}{2}N(\beta)$.*

За разлику од Гаусових целих, овде ћемо показати геометријски доказ.

Доказ. Комплексан број $z = \dfrac{\alpha}{\beta}$ се налази у комплексној равни. Приметимо да мрежа Ајзенштајнових целих бројева формира поплочавање јединичним једнакостраничним троугловима, и да се z мора налазити у бар једном од њих. Свака тачка у јединичном троуглу је удаљена највише $\dfrac{\sqrt{3}}{2}$ од најближег темена. Нека је то најближе теме број υ, а нека је $\rho = \alpha - \upsilon\beta$. Лако се проверава да ови бројеви задовољавају услове из теореме. □

Дефиниција 21. *Ајзенштајнов цео број је* **јединични** *уколико он дели 1.*

Став 16. *Јединични бројеви имају норму једнаку 1, и има их 6 ($\pm 1, \pm\omega, \pm\omega^2$).*

Дефиниција 22. *Кажемо да су Ајзенштајнови цели бројеви α и β* **еквивалентни** *уколико постоји јединични елемент θ, такав да је $\alpha = \theta\beta$.*

Како смо показали да је $\mathbb{Z}[\omega]$ еуклидски домен (да постоји дељење са остатком) сви докази за највећи заједнички делилац, просту факторизацију, Еуклидов алгоритам, Ајзенштајнове просте бројеве итд. су идентични, па ћемо их само навести без икаквог доказивања.

Дефиниција 23. Највећи заједнички делиоци *бројева α и β су њихови заједнички делиоци за које важи да су дељиви свим њиховим заједничким делиоцима. Скуп највећих заједничких делиоца бројева α и β записиваћемо као $D_{\alpha,\beta}$.*

Дефиниција 24. *Ајзенштајнови цели бројеви α и β су* **узајамно прости** *уколико је 1 њихов највећи заједнички делилац.*

Дефиниција 25. *За свака два Ајзенштајнова цела броја α и β постоји њихов највећи заједнички делилац, и он се може представити као линеарна комбинација $\kappa\alpha + \lambda\beta$, за неке $\kappa\lambda \in \mathbb{Z}[\omega]$.*

Став 17. *За $\alpha, \beta \in \mathbb{Z}[\omega]$ где бар један није нула, постоји тачно шест највећих заједничких делилаца, свих 6 са истом нормом.*

Став 18. *За $\alpha, \beta \in \mathbb{Z}[\omega]$ где бар један није нула, њихови највећи заједнички делиоци имају највећу норму међу свим заједничким делиоцима.*

Теорема 22. *За два Ајзенштајнова цела броја α и β постоји Еуклидов алгоритам којим се одређује један њихов највећи заједнички делилац.*
Алгоритам је исти као и у $\mathbb{Z}[i]$.

$$\begin{aligned} \alpha &= \upsilon_1\beta + \rho_1, \quad N(\rho_1) < N(\beta) \\ \beta &= \upsilon_2\rho_1 + \rho_2, \quad N(\rho_2) < N(\rho_1) \\ \rho_1 &= \upsilon_3\rho_2 + \rho_3, \quad N(\rho_3) < N(\rho_2) \\ &\vdots \end{aligned}$$

Претпоследњи остатак представља један највећи заједнички делилац бројева α и β.

2.2 Ајзенштајнови прости бројеви

Аналогно као и код Гаусових целих бројева, уводе се и Ајзенштајнови прости бројеви.

Дефиниција 26. *Нејединични Ајзенштајнов цео број $\alpha \neq 0$ је* **нерастављив**, *уколико за било које Ајзенштајнове целе бројеве β и γ, за које важи $\alpha = \beta\gamma$, следи да је β или γ јединичан. У супротном кажемо да је* **растављив**.

Став 19. *Сваки Ајзенштајнов цео број са нормом која је прост број је нерастављив.*

Дефиниција 27. *Нејединични Ајзенштајнов цео број $\pi \neq 0$ је* **прост** *уколико важи $\pi \mid \alpha\beta \implies \pi \mid \alpha$ или $\pi \mid \beta$. У супротном кажемо да је* **сложен**.

Теорема 23. *π је прост $\iff$ π је нерастављив.*

Последица 5. *Уколико број π има норму која је прост број, тада је π прост.*

Став 20. *Ако је π прост, тада је и његов коњугат, као и сваки његов умножак јединичним елементом, такође прост.*

Теорема 24 (Основна теорема аритметике у $\mathbb{Z}[\omega]$)**.** *За сваки Ајзенштајнов цео број, постоји јединствена факторизација до на редослед чинилаца и еквивалентност између одговарајућих простих бројева унутар престена $\mathbb{Z}[\omega]$.*

Теорема 25. *Нека је $p \in \mathbb{Z}$ прост цео број. Тада важи:*

- *ако је $p = 3$, тада је $1 - \omega$ прост у $\mathbb{Z}[\omega]$ и $3 = -\omega^2(1-\omega)^2$;*
- *ако је $p \equiv 1 \pmod 3$, тада постоје π и $\overline{\pi}$, нееквивалентни прости у $\mathbb{Z}[\omega]$, такви да је $p = \pi\overline{\pi}$;*
- *ако је $p \equiv 2 \pmod 3$, тада је p прост у $\mathbb{Z}[\omega]$.*

Доказ. $N(1-\omega) = 3$, што је прост цео број, па је $1-\omega$ нерастављив, а самим тим и прост у $\mathbb{Z}[\omega]$.
Доказ другог тврђења ћемо показати у следећој теореми.
Претпоставимо да прост број q облика $3k+2$ није прост у $\mathbb{Z}[\omega]$, тада постоје α и β, неједнични Ајзенштајнови цели бројеви такви да је $q = \alpha\beta$, односно $N(q) = q^2 = N(\alpha\beta)$, одакле следи да је $N(\alpha) = N(\beta) = q$, што је немогуће, зато што $x^2 - xy + y^2 \not\equiv 2 \pmod 3$. □

Теорема 26. *Уколико је прост број p облика $3k+1$, он се може записати као $x^2 - xy + y^2$, за неке целе x и y.*

Доказ. Како је $p \equiv 1 \pmod 3$, знамо да је $\left(\frac{p}{3}\right) = 1$, па је

$$1 = \left(\frac{p}{3}\right)(-1)^{p-1} = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}}.$$

Из закона реципроцитета имамо да је $1 = (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right) = \left(\frac{-3}{p}\right)$, одакле сазнајемо да је -3 квадратни остатак по модулу p. Како је то испуњено, постоји непарно[1] n такво да $p \mid n^2+3$, сада узмимо да је $n = 2m-1$, добијамо да је $p \mid 4m^2-4m+4$, тј. $p \mid m^2-m+1$ јер је 4 узајамно просто са p, односно $p \mid (m+\omega)(m+\omega^2)$. Како p не дели нити један од $m+\omega$ и $m+\omega^2$, следи да p није прост у $\mathbb{Z}[\omega]$, па постоје α и β, нејединични чији је производ једнак p. Како је $N(\alpha)N(\beta) = N(p) = p^2$, знамо да је $N(\alpha) = N(\beta) = p$, па су α и β прости, комплексно конјуговани, са нормом p. Сада, нека је $\alpha = x+\omega y$, изједначавањем $p = N(\alpha) = x^2 - xy + y^2$ доказујемо теорему. □

2.3 Конгруенције у прстену Ајзенштајнових целих бројева

Да бисмо показали најзанимљивије теореме везане за $\mathbb{Z}[\omega]$, неопходно је да уведемо и конгруенције. Пошто смо и ову област прешли у претходном поглављу, доказе нећемо наводити уколико су они аналогни.

Дефиниција 28. *Два Ајзенштајнова цела броја α и β су* **конгруентни по модулу** *μ ако μ дели њихову разлику. Тада пишемо $\alpha \equiv \beta \pmod\mu$.*

Став 21. *Релација конгруенције по модулу μ у прстену $\mathbb{Z}[\omega]$ је релација еквиваленције.*

Дефиниција 29. Класа остатака *Ајзенштајновог целог броја α по модулу μ је скуп бројева $\underline{\alpha_\mu} = \{\beta \in \mathbb{Z}[\omega] \mid \alpha \equiv \beta \pmod\mu\}$ такав да свака два конгруентна броја по модулу μ буду у истој класи. Скуп свих класа остатака по модулу μ означавамо $(\mathbb{Z}[\omega]/\mu)$.*

Теорема 27. *За Ајзенштајнове целе бројеве α, γ и $\beta \neq 0$, такви да су α и β и γ и β узајамно прости, једначина $\alpha\chi \equiv \gamma \pmod\beta$ има јединствено решење.*

Лема 12. *Нека су $\alpha_1, \alpha_2, \ldots, \alpha_n$ Ајзенштајнови цели бројеви такви да су свака два узајамно прости. Уколико за свако $i \in \{1, 2, \ldots, n\}$ важи $\alpha_i \mid \beta$ за неки $\beta \in \mathbb{Z}[\omega]$, тада $\alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_n \mid \beta$.*

Теорема 28 (Кинеска теорема о остацима)**.** *Нека су дати по паровима узајамно прости бројеви $\alpha_1, \alpha_2, \ldots, \alpha_n$. Тада систем једначина*

$$\chi \equiv \beta_1 \pmod{\alpha_1} \tag{2.1}$$
$$\chi \equiv \beta_2 \pmod{\alpha_2} \tag{2.2}$$
$$\vdots \tag{2.3}$$
$$\chi \equiv \beta_n \pmod{\alpha_n} \tag{2.4}$$
$$\tag{2.5}$$

има јединствено решење при модулу $\alpha_1\alpha_2\ldots\alpha_n$.

Дефиниција 30. *Кажемо за Ајзенштајнов цео број α да је* **инвертибилан** *по модулу μ уколико једначина $\alpha\chi \equiv 1 \pmod\mu$ има решење.*

[1] Овде можемо узети да је n непаран број јер уколико је паран, само га саберемо са p

Дефиниција 31. *За Ајзенштајнов цео број $\mu \neq 0$ уводимо позитиван природан број $n(\mu)$ као* **број различитих класа остатака по модулу** *μ.*

Став 22. *За свако $\alpha \in \mathbb{Z}[\omega] \setminus \{0\}$, $n(\alpha) < \infty$.*

Лема 13. *За цео број $m \neq 0$ број различитих класа остатака при дељењу са m има m^2.*

Лема 14. *За Ајзенштајнов цео број $\alpha \neq 0$ важи $n(\alpha) = n(\overline{\alpha})$.*

Лема 15. *За Ајзенштајнов прост број π важи да је*

Лема 16. *За Ајзенштајнове целе бројеве α и β ($\alpha, \beta \neq 0$) важи $n(\alpha\beta) = n(\alpha)n(\beta)$.*

Теорема 29. *За Ајзенштајнов цео број $\alpha \neq 0$ важи релација $n(\alpha) = N(\alpha)$.*

Теорема 30 (Мала Фермаова теорема)**.** *Нека је π прост Ајзенштајнов цео број, и нека је α недељив бројем π, тада важи $\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}$.*

Дефиниција 32 (Ојлерова фи функција)**.** *За Ајзенштајнов цео број $\alpha \neq 0$ функција $\phi(\alpha)$ даје број класа остатака при дељењу са α чији су представници инвертибилни мод α.*

Као и у Гаусовим целим бројевима, вредност ϕ функције је

$$\phi(\alpha) = N(\alpha) \prod_{\pi_i | \alpha} \left(1 - \frac{1}{N(\pi_i)}\right),$$

чиме можемо да комплетирамо и следећу теорему.

Теорема 31 (Ојлерова теорема)**.** *За узајамно просте Ајзенштајнове целе бројеве μ и α, важи $\alpha^{\phi(\mu)} \equiv 1 \pmod{\mu}$.*

Теорема 32. *Нека је $P_n(\chi)$, полином у $\mathbb{Z}[\omega][\chi]$ за који важи да је $degP = n$. Тада једначина $P_n(\chi) \equiv 0 \pmod{\pi}$ има највише n различитих решења у $\mathbb{Z}[\omega]$ уколико важи да је π Ајзенштајнов прост.*

Теорема 33 (Вилсонова теорема)**.** *Производ представника свих инвертибилних класа остатака при дељењу са простим модулом π у $\mathbb{Z}[\omega]$ је конгруентан са -1 по модулу π.*

2.4 Последња Фермаова теорема за кубове

Након увођења конгруенција по модулу у $\mathbb{Z}[\omega]$, можемо показати доказ последње Фермаове теореме за кубове.

Знамо да је последња Фермаова теорема била неколико векова нерешен проблем, да би је на крају доказао Ендру Вајлс крајем прошлог миленијума.

У овом делу, бавићемо се специјалним случајем последње Фермаове теореме, односно када су изложиоци умношци тројке.

Теорема 34. *Једначина $\xi^3 + \upsilon^3 + \zeta^3 = 0$ нема ненула решења у $\mathbb{Z}[\omega]$.*

Најпре ћемо доказати леме које ћемо користити у доказу.

Лема 17. *Нека је $\lambda = 1 - \omega$. Тада важи:*

1) λ је Ајзенштајнов прост број.

2) Сваки број у $\mathbb{Z}[\omega]$ је или дељив са λ, или даје остатак ± 1 при дељењу са λ.

3) Ако је $\chi \equiv \pm 1 \pmod{\lambda}$, тада је и $\chi^3 \equiv \pm 1 \pmod{\lambda^4}$.

4) Ако је $\xi^3+\upsilon^3+\zeta^3=0$, тада је бар један од бројева ξ,υ или ζ дељив бројем λ.

Доказ. 1) Следи директно из чињенице да је $N(\lambda)=3$.

2) Како је $a+b\omega=a+b-b\lambda=c+3d-b\lambda$, за неке целе c и d, и $\lambda\mid 3$, следи да је $a+b\omega=c+3d-b\lambda\equiv c \pmod{\lambda}$. Како цео број $3k+l$ ($l\in\{0,\pm1\}$) даје остатак l при дељењу са λ, тако сваки Ајзенштајнов цео број даје остатак 0 или ±1 при дељењу са λ.

3) Нека је $\chi\equiv 1 \pmod{\lambda}$, тј. да постоји $\kappa\in\mathbb{Z}[\omega]$ такво да је $\chi=1+\kappa\lambda$. Примећујемо да је $\chi^3-1=(\chi-1)(\chi-\omega)(\chi-\omega^2)=\lambda^3\kappa(\kappa+1)(\kappa-\omega^2)$. Пошто је $-\omega^2=1+\omega=-1+3-\lambda\equiv -1 \pmod{\lambda}$, имамо да је $\kappa(\kappa+1)(\kappa-\omega^2)$ производ три броја са различитим остацима по модулу λ. Како постоје искључиво три различита остатка при дељењу са λ, овај производ је такође дељив бројем λ, па је $\chi^3\equiv\pm1 \pmod{\lambda^4}$.

Слично се покаже и за $\chi\equiv -1 \pmod{\lambda}$.

4) Претпоставимо да ниједан од датих бројева није дељив бројем λ. Тада је $\xi^3+\upsilon^3+\zeta^3\equiv \pm1\pm1\pm1 \equiv \pm1,\pm3 \pmod{\lambda^4}$. Како је $N(\lambda^4)=81$, а $N(\pm1)=1$ и $N(\pm3)=9$, следи да десна страна не може бити нула што је контрадикција.

□

Сада ћемо без умањења општости користити да $\lambda\mid\zeta$. Сада нам је довољно само да докажемо следеће:

Лема 18. *Нека је $n\in\mathbb{N}$, и нека је ε јединични елемент у $\mathbb{Z}[\omega]$. Претпоставимо да су $\xi,\upsilon,\chi\in\mathbb{Z}[\omega]$ ненула, по паровима узајамно проста решења једначине*

$$\xi^3+\upsilon^3+\varepsilon\lambda^{3n}\chi^3=0 \tag{2.6}$$

где λ не дели нити један од бројева ξ,υ,χ. Тада важи:

1) $n\geq 2$.

2) Три чиниоца броја $-\varepsilon\lambda^{3n}\chi^3=\xi^3+\upsilon^3=(\xi+\upsilon)(\xi+\omega\upsilon)(\xi+\omega^2\upsilon)$ су дељиви са λ, и разломци $\dfrac{\xi+\upsilon}{\lambda},\dfrac{\xi+\omega\upsilon}{\lambda},\dfrac{\xi+\omega^2\upsilon}{\lambda}$ су по паровима узајамно прости.

3) Без умањења општости, $\lambda^{3(n-1)}\mid\xi+\upsilon$. Тада

$$\xi+\upsilon=\varepsilon_1\lambda^{3n-2}\rho^3 \qquad \xi+\omega\upsilon=\varepsilon_2\lambda\sigma^3 \qquad \xi+\omega^2\upsilon=\varepsilon_3\lambda\tau^3$$

где су $\varepsilon_1,\varepsilon_2,\varepsilon_3$ јединични елементи у $\mathbb{Z}[\omega]$ и ρ,σ,τ су по паровима узајамно прости Ајзенштајнови цели бројеви који нису дељиви бројем λ. Тада постоје јединични елементи ε_4 и ε_5 такви да:

$$\sigma^3+\varepsilon_4\tau^3+\varepsilon_5\lambda^{3(n-1)}\rho^3=0$$

Додатно, $\varepsilon_4=\pm1$ има себе за трећи корен па се може урачунати у τ.

Како је $3\leq 3(n-1)<3n$, можемо закључити да једначина (2.6) нема решења.

Доказ. 1) Немогуће је да $\xi\equiv\upsilon \pmod{\lambda}$, због леме 16 знамо да је $\xi^3+\upsilon^3\equiv\pm2 \pmod{\lambda^4}$ из чега следи да $\lambda^3\nmid\xi^3+\upsilon^3$.
Како су ξ и υ различити по модулу λ, следи да су конгруентни 1 и -1 по модулу λ^4 редом. Примећујемо да је

$$-\varepsilon\lambda^{3n}\chi^3=\xi^3+\upsilon^3\equiv 0 \pmod{\lambda^4}\Longrightarrow\lambda^4\mid\lambda^3\chi^3\Longrightarrow\lambda\mid\lambda^{3n-3}\chi^3.$$

Пошто је λ прост који не дели χ, следи да $\lambda\mid\lambda^{3n-3}$, одакле сазнајемо да је $3n-3\geq 1$, тј. $n\geq 2$.

2) Како је $1 \equiv \omega \equiv \omega^2 \pmod{\lambda}$, имамо да је $\xi + \upsilon \equiv \xi + \omega\upsilon \equiv \xi + \omega^2\upsilon \pmod{\lambda}$, где су сва три члана дељива бројем λ.
Уколико би постојао заједнички делилац бројева $\frac{\xi+\upsilon}{\lambda}$ и $\frac{\xi+\omega\upsilon}{\lambda}$, он би делио $\frac{\xi+\upsilon}{\lambda} - \frac{\xi+\omega\upsilon}{\lambda} = \upsilon$ и $-\omega\frac{\xi+\upsilon}{\lambda} + \frac{\xi+\omega\upsilon}{\lambda} = \xi$, али како су они узајамно прости, сазнајемо да је тражени заједнички делилац заправо јединични елемент.

3) Како је $1+\omega+\omega^2 = 0$, имамо да је

$$\begin{aligned} 0 &= \xi + \upsilon + \omega(\xi+\omega\upsilon) + \omega^2(\xi+\omega^2\upsilon) = \varepsilon_1\lambda^{3n-2}\rho^3 + \omega\varepsilon_2\lambda\sigma^3 + \omega^2\varepsilon_3\lambda\tau^3 \\ \Longrightarrow &\sigma^3 + \varepsilon_4\tau^3 + \varepsilon_5\lambda^{3(n-1)}\rho^3 = 0 \end{aligned}$$

где је $\varepsilon_4 = \frac{\omega\varepsilon_3}{\varepsilon_2}$ и $\varepsilon_5 = \frac{\varepsilon_1}{\omega\varepsilon_2}$.
Како је $n \geq 2$, приметимо да је $\sigma^3 + \varepsilon_4\tau^3 \equiv 0 \pmod{\lambda^2}$. Због леме 16, σ^3 и τ^3 су $\pm 1 \pmod{\lambda^4}$, па самим тим и $\pm 1 \pmod{\lambda^2}$. Тако, имамо да је $\varepsilon_4 \equiv \pm 1 \pmod{\lambda^2}$. Како је $N(\lambda^2) = 9$, лако се провери да су једини јединични ε_4 за које је $\varepsilon_4 \pm 1$ дељиво бројем λ^2 заправо само $\varepsilon_4 = \pm 1$.

□

Како смо добили једначину $\sigma^3 + \varepsilon_4\tau^3 + \varepsilon_5\lambda^{3(n-1)}\rho^3$, на њу можемо применити поново лему 18 и поново смањити изложилац броја λ и тако доћи до тренутка када нити један члан није дељив бројем λ, али по леми 17 закључујемо да је то немогуће. Како не постоје ненула решења једначине $\xi^3 + \upsilon^3 + \zeta^3 = 0$ у $\mathbb{Z}[\omega]$, тако не постоје решења ни у $\mathbb{Z}$.

2.5 Кубни реципроцитет и прости бројеви облика x^2+27y^2

У историји нас је често занимало ког облика могу бити прости бројеви, јер смо све време трагали за функцијом која би генерисала просте бројеве. Показали смо какви морају бити прости бројеви да би се представили као x^2+y^2 или x^2-xy+y^2, али облик који ћемо обрадити у овом делу је доста захтевнији од поменута два. Овде неочекивану улогу игра кубни реципроцитет без обзира што је облик x^2+27y^2 квадратна форма.

Најпре, увешћемо Лежандров симбол за кубне остатке. Како смо сигурни да важе одређене теореме у $\mathbb{Z}[\omega]$, то и можемо учинити.

Нека је π прост број који није еквивалентан броју $\lambda = 1-\omega$. Лако се провери да $3 \mid N(\pi)-1$. Сада, нека је α Ајзенштајнов цео број који није дељив бројем π. На основу мале Фермаове теореме, знамо да је $\chi = \alpha^{\frac{N(\pi)-1}{3}}$ једно решење једначине $\chi^3 \equiv 1 \pmod{\pi}$. Како је ово једначина трећег степена и остаци при дељењу са π формирају коначно поље, она има највише три решења, а како су $1, \omega, \omega^2$ различита решења (јер $\pi \not\sim 1-\omega$), она су и једина, из чега следи да је $\alpha^{\frac{N(\pi)-1}{3}} \equiv 1, \omega, \omega^2 \pmod{\pi}$.

Дефиниција 33. *За Ајзенштајнов цео број α и прост број π ($\pi \nmid \alpha$) уводимо ознаку $\left(\frac{\alpha}{\pi}\right)_3$ које узима вредност 1, ω или ω^2, и за коју важи да је $\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{\frac{N(\pi)-1}{3}}$. Ако је $\left(\frac{\alpha}{\pi}\right)_3 = 1$, тада кажемо да је α кубни остатак по модулу π, а у осталим случајевима кажемо да α није кубни остатак (некада кажемо да је α кубни неостатак) по модулу π.*

Дефиниција 34. *Кажемо да је прост број* **примаран** *уколико је конгруентан са ± 1 при дељењу са 3.*

Као и код квадратних остатака, важе сличне особине везане за кубне остатке.

Став 23. *Нека су $\alpha, \beta, \pi \in \mathbb{Z}[\omega]$, где је π Ајзенштајнов прост број, тада важи:*

- $\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$
- $\alpha \equiv \beta \pmod{\pi} \Longrightarrow \left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$
- $\left(\frac{\alpha}{\pi}\right)_3 = 1 \Longleftrightarrow \alpha^{\frac{N(\pi)-1}{3}} \equiv 1 \pmod{\pi} \Longleftrightarrow \chi^3 \equiv \alpha \pmod{\pi}$ *има решење у* $\mathbb{Z}[\omega]$.
- $\overline{\left(\frac{\alpha}{\pi}\right)_3} = \left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_3$
- *Ако је* $\pi \sim \psi$, *онда је* $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\alpha}{\psi}\right)_3$

Доказ. Трећа тврдња се показује тако што се испоставља да је $(\mathbb{Z}[\omega]/\pi)$ коначно поље, па садржи примитиван корен, одакле се лако показује тврђење. Остале тврдње се такође лако показују. □

Теорема 35 (Кубни реципроцитет)**.** *Нека су π и ψ примарни Ајзенштајнови прости бројеви. Тада важи* $\left(\frac{\pi}{\psi}\right)_3 = \left(\frac{\psi}{\pi}\right)_3$.

Доказ. Може се наћи у [1]. □

Сада желимо да видимо како се понаша симбол за целе бројеве, односно шта представља $\left(\frac{a}{p}\right)_3$, где је p прост цео број.

Ако је $p = 3$, тада је по малој Фермаовој теореми $a^3 \equiv a \pmod{3}$, па је сваки број кубни остатак при дељењу са 3.
У случају када је p облика $3k+2$, имамо да је $x^p \equiv x \pmod{p}$, односно $x^{p-1} \equiv 1 \pmod{p}$, па је $x^{2p-1} \equiv x^{6k+3} \equiv \left(x^{2k+1}\right)^3 \equiv x \pmod{p}$, па је сваки број кубни остатак по модулу p.
Што се тиче случаја $p = 3k+1$, ту имамо да постоје Ајзенштајнови прости π и $\overline{\pi}$, такви да је $p = \pi\overline{\pi}$. Када $p \nmid a$, имамо да $x^3 \equiv a \pmod{p}$ има решење ако и само ако је $\left(\frac{a}{\pi}\right)_3 = \left(\frac{a}{\overline{\pi}}\right)_3 = 1$.

Сада смо спремни да покажемо када прост број може бити облика $x^2 + 27y^2$.

Теорема 36. *Прост број p се може записати у облику x^2+27y^2, где су x и y цели бројеви ако и само ако је $p \equiv 1 \pmod{3}$ и 2 је кубни остатак по модулу p.*

Доказ. ($\Rightarrow$) Ако је p облика $x^2 + 27y^2$, очигледно следи да је $p \equiv 1 \pmod{3}$, па нам преостаје да покажемо да је $\left(\frac{2}{p}\right)_3 = 1$. Нека је $\pi = x + 3\sqrt{3}yi$, односно $\pi\overline{\pi} = p$. Следи да је π Ајзенштајнов прост број, и додатно $\left(\frac{2}{p}\right)_3 = \left(\frac{2}{\pi}\right)_3 = \left(\frac{\pi}{2}\right)_3$, али како је $i\sqrt{3} = 1 + 2\omega, \pi = x + 3y + 6y\omega$, па је $\pi \equiv x + 3y \equiv x + y \pmod{2}$, али x и y су супротне парности јер је $p = x^2 + 27y^2$ прост, па је $\pi \equiv 1 \pmod{2}$ чиме смо доказали овај смер.

($\Leftarrow$) Претпоставимо да је $p \equiv 1 \pmod{3}$, и да је 2 кубни остатак по модулу p. Можемо записати p као $\pi\overline{\pi}$, где је π Ајзенштајнов прост број, и можемо претпоставити да је π примаран. То значи да је π облика $a + 3\omega b$ за целе a и b. Следи да је $4p = 4\pi\overline{\pi} =$

$(2a-3b)^2+27b^2$.
Ако успемо да докажемо да је b паран број, показали смо и овај смер, зато што можемо поделити обе стране бројем 4. Сада, до изражаја долази $\left(\frac{2}{p}\right)_3 = 1$. Због закона кубног реципроцитета знамо да је $\left(\frac{\pi}{2}\right)_3 = 1$, из чега следи да је $\pi \equiv 1 \pmod 2$, тј. $a+3b\omega \equiv 1 \pmod 2$, што нам говори да је a непаран, док је b паран цео број, чиме смо показали тврђење.

□

2.6 Примене на такмичењу

Овај рад завршићемо једним задатком са међународне математичке олимпијаде одржане 2001. године у Хонгконгу. Овај задатак је имао прегршт решења, од којих је једно геометријско, а ми ћемо погледати једно које се базира на прстену $\mathbb{Z}[\omega]$.

Задатак 3. *Нека су $a > b > c > d$ природни бројеви. Уколико важи*

$$ac+bd = (b+d+a-c)(b+d-a+c),$$

показати да је $ab+cd$ сложен.

Решење. Алгебарским трансформацијама добијамо следеће:

$$\begin{aligned} ac+bd &= (b+d)^2-(a-c)^2 \\ a^2-ac+c^2 &= b^2+bd+d^2 \\ (a+\omega c)\overline{(a+\omega c)} &= (b-\omega d)\overline{(b-\omega d)} \end{aligned}$$

Уведимо сада бројеве $\xi = a+\omega c$, $\overline{\xi} = \overline{a+\omega c}$, $\upsilon = b-\omega d$ и $\overline{\upsilon} = \overline{b-\omega d}$, тада је $\xi\overline{\xi} = \upsilon\overline{\upsilon}$.
Сада, нека је $n \in D_{\xi,\upsilon}$, и нека је $m = \frac{\xi}{n}, n, m \in \mathbb{Z}[\omega]$. Како $m \mid \overline{\upsilon}$, следи да $m \in D_{\xi,\overline{\upsilon}}$, па је $\xi = nm$ и $\upsilon = n\overline{m}$.
$n = p+q\omega, m = r+s\omega$, где су $p,q,r,s \in \mathbb{Z}$. Расписивањем израза добијамо да је

$$\xi = pr+qs+\omega(qr+ps-qs),$$

па је $a = pr-qs$ и $c = qr+ps-qs$.
Аналогно имамо да је $b = pr+qs-ps$ и $d = ps-qr$.

Сада, након мало расписивања, може се закључити да је

$$ab+cd = (p^2-q^2)(r^2-rs+s^2).$$

Једина могућност када би ово могао бити прост број је када је $p^2-q^2 = \pm 1$ или $r^2-rs+s^2 = \pm 1$. Ако је $p^2-q^2 = \pm 1$, онда је $\{p,q\} = \{0,\pm 1\}$, што проузрокује да је или $a = -b$ или $c = d$, али због услова задатка, то није могуће. Сада, ако је $r^2-rs+s^2 = \pm 1$, то значи да r^2-rs+s^2 мора бити 1 (јер је ова једначина увек ненегативна), одакле добијамо решења $(r,s) \in \{(0,1),(0,-1),(1,0),(-1,0),(1,1),(-1,-1)\}$, из којих следи бар једна од следећих једнакости $b = -c \vee a = b \vee a = d$, што није могуће, па је $ab+cd$ сложен. □

3 Закључак

Овај матурски рад се бави проширењима целих бројева која су такође и еуклидски домени, и самим тим деле многе особине целих бројева на које смо навикли. Ипак, иако је приметна сличност $\mathbb{Z}[i]$ и $\mathbb{Z}[\omega]$ са $\mathbb{Z}$, не треба све паралеле узимати здраво за готово. Такође, постоји још прегршт лема и теорема које се могу доказати, али овај рад нема за циљ да их наброји апсолутно све, већ да пробере најзанимљивије од њих и приближи их читаоцима. Такође још једна поента овог рада је увиђање да се и неки, наизглед тешки, проблеми врло лако доказују у $\mathbb{Z}[i]$ или $\mathbb{Z}[\omega]$. Надам се да овај рад може да послужи као увод у тему квадратних проширења целих бројева, која се заједно с повезаним темама може пронаћи у радовима који су остављени у литератури.

Литература

[1] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory, second ed.* Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990.

[2] D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, Class Field Theory and Complex Multiplication.* 1989.

[3] N. Donaldson, *Gaussian Integers and Rings of Algebraic Integers.* https://www.math.uci.edu/~ndonalds/math180b/6gaussian.pdf.

[4] D. S. Dummit, R. M. Foote, *Abstract Algebra*, third ed., 2003.

[5] D. Đukić, *Raširenja racionalnih brojeva.* https://imomath.com/srb/dodatne/rasirenja-Q_ddj.pdf.

[6] *Gaussian integer.* https://en.wikipedia.org/wiki/Gaussian_integer#cite_note-6.

[7] K. Conrad, *The Gaussian Integers.* https://kconrad.math.uconn.edu/blurbs/ugradnumthy/Zinotes.pdf.

[8] C. A. May, *Application of the Euler Phi Function in the Set of Gaussian Integers.* https://digitalcommons.northgeorgia.edu/cgi/viewcontent.cgi?article=1011&context=honors_theses.

[9] B. Lynn, *The Chinese Remainder Theorem.* https://crypto.stanford.edu/pbc/notes/numbertheory/crt.html.

[10] H. Ho, *Gaussian Integers.* http://math.uchicago.edu/~may/REU2016/REUPapers/Ho.pdf.

[11] *Math 3527 (Number Theory 1).* https://web.northeastern.edu/dummit/teaching_sp20_3527/3527_lecture_26_primitive_roots.pdf.