Tartu Ülikool
Matemaatika-informaatikateaduskond
Matemaatika instituut
Matemaatika eriala

Galina Brokan

Gaussi täisarvud

Bakalaureusetöö (6 EAP)

Juhendaja: Valdis Laan

Tartu 2014

Gaussi täisarvud

Bakalaureusetöö
Galina Brokan

Lühikokkuvõte. Käesolevas bakalaureusetöös on vaadeldud Gaussi täisarve ja nende omadusi. On toodud Gaussi täisarvude, Gaussi täisarvude normi ja Gaussi algarvude definitsioonid. On uuritud pööratavaid Gaussi täisarve ja nende seoseid Gaussi täisarvude normiga. On ära toodud jäägiga jagamise teoreem Gaussi täisarvude jaoks ning on näidatud, et Gaussi täisarvude ring on faktoriaalne ring. Töös on näidatud, et Eukleidese algoritmi abil saab leida Gaussi täisarvude suurima ühisteguri. Töö lõpus on uuritud Gaussi algarve ja nende omadusi. Jõuame järeldusele, et Gaussi algarve on kahte liiki ja kumbagi liiki Gaussi algarve on lõpmata palju. Tööle on lisatud ka joonised, kus on näidatud kuidas Gaussi täisarvud ja Gaussi algarvud asetsevad komplekstasandil.

Märksõnad. Gaussi täisarv, jaguvus, Gaussi algarv, Gaussi täisarvu norm, suurim ühistegur.

Gaussian integers

Bachelor's thesis
Galina Brokan

Abstract. The subject of this Bachelor's thesis is Gaussian integers and their properties. In this thesis Gaussian integers, the norm of a Gaussian integer and Gaussian primes are defined. Invertible Gaussian integers and their relation to the norm of Gaussian integers are studied. The theorem about division with a remainder is formulated and the ring of Gaussian integers is shown to be a factorial ring. In this thesis it is shown that using the Euclidean algorithm the greatest common divisor of Gaussian integers can be found. At the end of the thesis Gaussian primes and their properties are studied. We arrive at a conclusion that there are two types of Gaussian primes and there are infinitely many Gaussian primes of both types. Figures have been added to the thesis illustrating how Gaussian integers and Gaussian primes are situated on the complex plane.

Key words. Gaussian integer, divisibility, Gaussian prime, the norm of a Gaussian integer, greatest common divisor.

Sisukord

Sissejuhatus

Käesoleva bakalaureusetöö üldiseks valdkonnaks on arvuteooria. Bakalaurusetöö eesmärgiks on uurida kompleksarve, mille reaalosa ja imaginaarosa kordaja on täisarvud. Niimoodi defineeritud arve nimetatakse Gaussi täisarvudeks. Need arvud on saanud oma nime teadlase jargi, kes esimesena uuris nende omadusi. Gaussi täisarvudel on väga palju ühiseid omadusi täisarvudega. Kuna Gaussi täisarvud on samal ajal ka kompleksarvud, siis ka paljud kompleksarvude omadused kehtivad Gaussi täisarvude jaoks.

Antud bakalaureusetöö on referatiivne ning selle kirjutamisel olid aluseks raamatud [5] ja [6], kus on täpsemalt uuritud Gaussi täisarvude omadusi. Lisaks kasutasime ka raamatuid [1], [4], [3] ja loengukonspekti [2]. Töö koosneb viiest peatükist.

Esimene peatükk on sissejuhatav. Selles peatükis on toodud Gaussi täisarvude definitsioon. On näidatud, et Gaussi täisarvude ring on kommutatiivne nulliteguriteta ring. On toodud joonis, kus on näidatud, kuidas Gaussi täisarvud asuvad komlekstasandil.

Teine peatükk on pühendatud Gaussi täisarvude normile. Ära on toodud Gaussi täisarvude normi definitsioon ja sellega seotud laused. On näidatud millal Gaussi täisarv on pööratav ja tõestatud sellega seotud tulemused. Selles peatükis saame teada, et Gaussi täisarve saab jäägiga jagada. Peatüki lõpuks on näidatud, et Gaussi täisarvude ring on faktoriaalne ring.

Kolmadas peatükis uurime Gaussi täisarvude suurima ühisteguri leidmist. On näidatud, et Gaussi täisarvude suurimat ühistegurit saab leida Eukleidese algoritmi kasutades. Peatüki lõpus on toodud näide selle kohta.

Neljas peatükk on Gaussi algarvude kohta. On antud Gaussi algarvude definitsioon. On lisatud ka joonis, kus on näidatud Gaussi algarvude paiknemine komlekstasandil. On uuritud Gaussi algarvude omadusi. Selles peatükis jõuame järeldusele, et Gaussi algarve on kahte liiki ja mõlemat liiki Gaussi algarve on lõpmata palju.

Viimane ehk viies peatükk on Gaussi täisarvude rakendustest. Selles peatükis me näitame, kuidas saab lahendada täisarvude kohta käivad ülesandeid kasutades Gaussi täisarvude omadusi.

1. Põhimõisted ja -omadused

Oma monograafias „Biruutjääkide teooria“ (1828, 1832) arutles Carl Friedrich Gauss muuhulgas ka ruutvastavusseaduse võimalike üldistuste üle. Ta jõudis järeldusele, et on võimalik ja vajalik laiendada täisarvu mõistet ([3], lk. 694). Nimelt tuleks vaadelda kompleksarvude hulgas arve $a+bi$, kus a ja b on täisarvud ([3], lk. 697). Ta näitas, et sellised arvud moodustavad ringi, kus pööratavaid elemente on neli: $1, -1, i, -i$. Ta uuris taandumatuid elemente selles ringis ja tõestas, et iga elemendi saab teatud mõttes üheselt esitada taandumatute elementide korrutisena. Käesolevas töös anname ülevaate nendest teemadest ja näitame ka, kuidas Gaussi täisarvude omadusi saab rakendada täisarvude jaoks sõnastatud probleemide lahendamisel.

Joonis 1: Carl Friedrich Gauss

Definitsioon. *Gaussi täisarvud* on kompleksarvud, mille reaalosa ja imaginaarosa kordaja on täisarvud. Gaussi täisarvude hulka tähistame $\mathbb{Z}[i]$. Seega

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

Definitsioon. Olgu R ring. Nullist erinevat elementi $a \in R$, mille korral leidub kas nullist erinev $b \in R$ või nullist erinev element $c \in R$ nii, et kas $ab = 0$ või $ca = 0$, nimetatakse *nulliteguriks*.

Lause 1.1 ([1], lause 3.2.21)**.** *Korpuses ei leidu nullitegureid.*

Lause 1.2. *Ring $\mathbb{Z}[i]$ on kommutatiivne nulliteguriteta ring.*

TÕESTUS. Näitame, et $\mathbb{Z}[i]$ on korpuse $\mathbb{C}$ alamring.

Kontrollime alamringi definitsiooni tingimusi:

(i) Olgu $\alpha = a + bi \in \mathbb{Z}[i]$ ja $\beta = c + di \in \mathbb{Z}[i]$, kus $a, b, c, d \in \mathbb{Z}$. Siis $\alpha + \beta = (a + c) + i(b + d) \in \mathbb{Z}[i]$, sest $a + c, b + d \in \mathbb{Z}$.

(ii) Olgu $\alpha = a + bi$. Kuna $a, b \in \mathbb{Z}$, siis ka $-a, -b \in \mathbb{Z}$. Seega $-\alpha = -(a + bi) = (-a) + (-b)i \in \mathbb{Z}[i]$.

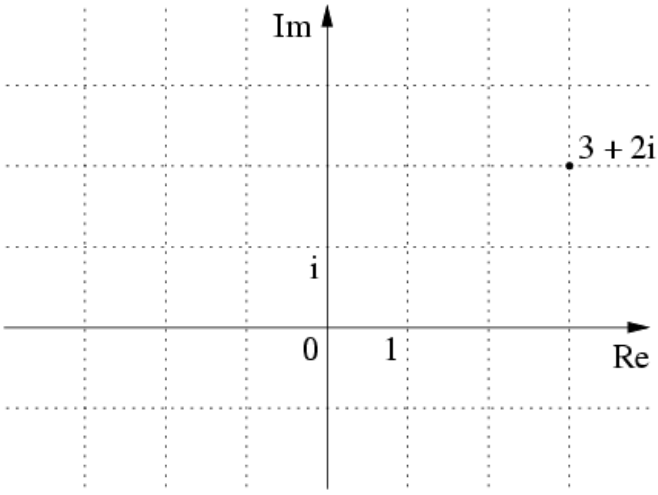
(iii) Olgu $\alpha = a + bi$ ja $\beta = c + di$. Siis $\alpha \cdot \beta = (ac + bd) + (ad + bc)i \in \mathbb{Z}[i]$, sest $ac + bd, ad + bc \in \mathbb{Z}$.

(iv) Korpuse $\mathbb{C}$ ühikelement 1 kuulub ka hulka $\mathbb{Z}[i]$, sest $1 = 1 + 0i$.

Näitasime, et $\mathbb{Z}[i]$ on korpuse $\mathbb{C}$ alamring, seega on ta ise ka ring.

Ring $\mathbb{Z}[i]$ on kommutatiivne, kuna ta on korpuse $\mathbb{C}$ alamring, mis on aga kommutatiivne.

Kasutades eelmist lauset võime öelda, et $\mathbb{Z}[i]$ on nulliteguriteta, kuna $\mathbb{C}$ on korpus. □



Joonis 2: Gaussi täisarvud komplekstasandil

Definitsioon. Olgu R kommutatiivne nulliteguriteta ring ja $a, b \in R$. Öeldakse, et element a *jagab* elementi b (ja tähistatakse $a|b$), kui leidub selline element $c \in R$, et $ac = b$.

Definitsioon. Kompleksarvu $\alpha = a+bi$ *kaaskompleksarvuks* nimetatakse kompleksarvu $\bar{\alpha} = a - bi$.

On selge, et kui $\alpha \in \mathbb{Z}[i]$ siis ka $\bar{\alpha} \in \mathbb{Z}[i]$.

Lause 1.3 ([1], lk. 185–186)**.** *Kui* $\alpha, \beta \in \mathbb{C}$*, siis* $\overline{\alpha\beta} = \bar{\alpha}\bar{\beta}$ *ja* $\overline{\alpha+\beta} = \bar{\alpha} + \bar{\beta}$.

Lause 1.4. *Kui arv* β *jagab arvu* α *ringis* $\mathbb{Z}[i]$*, siis ka arv* $\bar{\beta}$ *jagab arvu* $\bar{\alpha}$ *ringis* $\mathbb{Z}[i]$.

TÕESTUS. Kui β jagab arvu α, siis leidub selline $\gamma \in \mathbb{Z}[i]$, et $\beta\gamma = \alpha$. Järelikult $\bar{\beta}\bar{\gamma} = \overline{\beta\gamma} = \bar{\alpha}$, mis tähendab, et $\bar{\beta}$ jagab arvu $\bar{\alpha}$. □

Järeldus 1.5. *Kui Gaussi täisarv* α *jagab täisarvu* a *ringis* $\mathbb{Z}[i]$*, siis ka* α *kaaskompleksarv jagab täisarvu* a.

TÕESTUS. Tõestuseks kasutame eelmist lauset. Kui $\alpha|a$, siis $\bar{\alpha}|\bar{a}$, kus $\bar{a} = a$. □

2. Gaussi täisarvude norm

Kuna Gaussi täisarvud on kompleksarvud, siis võib vaadelda nende moodulit. Defineerime mooduli abil Gaussi täisarvude jaoks normi ja uurime, millised omadused sellel normil on.

Definitsioon. Gaussi täisarvu $\alpha = a + bi$ *normiks* nimetatakse tema mooduli ruutu, st mittenegatiivset täisarvu $a^2 + b^2$. Tavaliselt arvu α normi tähistatakse $N(\alpha)$. Seega $N(\alpha) = a^2 + b^2$.

Lause 2.6. *Gaussi täisarv α jagab oma normi ringis $\mathbb{Z}[i]$.*

TÕESTUS. Kuna

$$\alpha \cdot \bar{\alpha} = (a + bi) \cdot (a - bi) = a^2 - abi + abi + b^2 = a^2 + b^2 = N(\alpha),$$

kus $\bar{\alpha}$ on ka Gaussi täisarv, siis $\alpha | N(\alpha)$ ringis $\mathbb{Z}[i]$. □

Lause 2.7. *Täisarvu norm on võrdne tema ruuduga.*

TÕESTUS. Kui $a \in \mathbb{Z}$, siis $N(a) = a^2 + 0 = a^2$. □

Lause 2.8. *Kahe Gaussi täisarvu korrutise norm võrdub nende arvude normide korrutisega, ehk $N(\alpha\beta) = N(\alpha)N(\beta)$ mistahes $\alpha, \beta \in \mathbb{Z}[i]$ korral.*

TÕESTUS. Teame, et selline omadus kehtib kompleksarvude mooduli kohta ($|\alpha\beta| = |\alpha| \cdot |\beta|$). Kasutades seda omadust saame, et mistahes $\alpha\beta \in \mathbb{Z}[i]$ korral

$$N(\alpha\beta) = |\alpha\beta|^2 = |\alpha\beta||\alpha\beta| = |\alpha||\beta||\alpha||\beta| = |\alpha|^2|\beta|^2 = N(\alpha)N(\beta).$$

□

Järeldus 2.9. *Kui $\alpha, \beta \in \mathbb{Z}[i]$ ja $\beta \neq 0$, siis $N(\alpha\beta) \geqslant N(\alpha)$.*

TÕESTUS. Kui $\beta \neq 0$, siis $N(\beta) \geqslant 1$. Seega $N(\alpha\beta) = N(\alpha)N(\beta) \geqslant N(\alpha)$. □

Toome ühe näite sellest, kuidas Gaussi täisarvude normi saab rakendada.

Näide 2.10. Esitame arvu $221 = 13 \cdot 17$ ruutude summana.

Teame, et $13 = 2^2 + 3^2$ ja $17 = 1^2 + 4^2$. Paneme tähele, et $13 = N(2 + 3i)$ ja $17 = N(1 + 4i)$. Järelikult, lause 2.8 põhjal

$$\begin{aligned} 221 &= 13 \cdot 17 = N(2 + 3i) \cdot N(1 + 4i) = N[(2 + 3i)(1 + 4i)] \\ &= N(-10 + 11i) = 10^2 + 11^2. \end{aligned}$$

Teise võimaliku lahendusena:

$$221 = N(2 - 3i)N(1 + 4i) = N(14 + 5i) = 14^2 + 5^2.$$

Lause 2.11. *Kui $\beta|\alpha$ ringis $\mathbb{Z}[i]$, siis $N(\beta)|N(\alpha)$ ringis $\mathbb{Z}$.*

TÕESTUS. Kui $\beta|\alpha$, siis jaguvuse definitsiooni tõttu $\alpha = \beta\gamma$, kus γ on ka Gaussi täisarv. Kasutades lauset 2.8 saame võrduse $N(\alpha) = N(\beta)N(\gamma)$, mis tähendab, et $N(\beta)|N(\alpha)$ ringis $\mathbb{Z}$. □

Vastupidises suunas väide ei kehti. Norm $N(\beta)$ võib jagada normi $N(\alpha)$ ka siis, kui arv β ei jaga arvu α. Näiteks arv $\beta = 1 - 2i$ ei jaga arvu $\alpha = 1 + 2i$, aga $N(\beta) = 5$ jagab arvu $N(\alpha) = 5$. Oletame vastuväiteliselt, et $\beta|\alpha$. Siis leidub $\gamma = e + fi$ nii, et $\beta\gamma = \alpha$, $\gamma \in \mathbb{Z}[i]$ ja $e, f \in \mathbb{Z}$. Järelikult

$$\begin{aligned}(1 - 2i)(e + fi) &= 1 + 2i,\\ e + fi - 2ie + 2f &= 1 + 2i,\\ (e + 2f) + i(f - 2e) &= 1 + 2i.\end{aligned}$$

Viimasest võrdusest saame võrrandisüsteemi

$$\begin{cases} e + 2f = 1 \\ f - 2e = 2 \end{cases}.$$

Avaldades esimesest võrrandist $e = 1 - 2f$ ja asendades teise võrrandisse saame, et

$$\begin{aligned}f - 2 + 4f &= 2,\\ 5f &= 4,\\ f &= \frac{4}{5}.\end{aligned}$$

Saame, et $f = 4/5$, ehk $f \notin \mathbb{Z}$, mis on vastuolus eeldusega.

Definitsioon. Ringi elementi, millel leidub pöördelement korrutamise suhtes, nimetatakse selle ringi *pööratavaks* elemendiks. Ringi R kõigi pööratavate elementide hulka tähistame $U(R)$.

Lihtne on näha, et kehtib järgmine lause.

Lause 2.12. *Kommutatiivse ringi R element a on pööratav parajasti siis, kui a jagab ringi R ühikelementi.*

TÕESTUS. Tarvilikkus. Olgu a pööratav element, siis leidub selline element $b \in R$, et $ab = 1$. Sellest järeldub, et $a|b$.

Piisavus. Oletame, et a jagab ringi R ühikelementi, ehk $a|1$. Sellest järedub, et leidub selline element $b \in R$, et $ab = 1$. Seega a ja b on teineteise pöördelemendid. □

Lause 2.13. *Gaussi täisarv on pööratav parajasti siis, kui selle arvu norm on* 1.

TÕESTUS. Tarvilikkus. Olgu antud pööratav Gaussi täisarv $\alpha = a + bi$. Lause 2.12 põhjal $\alpha|1$. Kasutades lauset 2.11 saame, et $N(\alpha)$ peab jagama arvu $N(1)$, kus $N(1) = 1$. Täisarvu 1 ainsaks mittenegatiivseks täisarvuliseks jagajaks on tema ise, ehk 1. Järelikult $N(\alpha) = 1$.

Piisavus. Olgu Gaussi täisarvu $\alpha = a + bi$ norm 1. Siis

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

Järelikult $a + bi$ on pööratav element. □

Lause 2.14. *Ainult nelja Gaussi täisarvu norm on võrdne ühega. Need arvud on* $1,i,-1$ *ja* $-i$. *Seega*

$$U(\mathbb{Z}[i]) = \{1, -1, i, -i\}.$$

TÕESTUS. Olgu $N(a + bi) = a^2 + b^2 = 1$, kus a ja b on täisarvud. On ilmne, et $a^2 \leqslant 1$, järelikult $a = 0$ või $a = \pm 1$.

Kui $a = 0$, siis $b = \pm 1$ ja $a + bi = \pm i$.

Kui $a = \pm 1$, siis $b = 0$ ja $a + bi = \pm 1$. □

Definitsioon. Elemente a ja b nulliteguriteta ringis R nimetatakse *assotsieeritud elementideks*, kui $a = bc$ ja element $c \in R$ on pööratav.

Märgime, et võrdusest $a = bc$, kus c on pööratav, järeldub võrdus $b = ac^{-1}$. See tähendab, et kui elemendid a ja b on assotsieeritud, siis on seda ka b ja a.

Definitsioon. Olgu R nulliteguriteta ring. Mittepööratavat elementi $p \in R$ nimetatakse *taandumatuks*, kui võrdusest $p = ab$, $a, b \in R$, järeldub, et kas a on pööratav või b on pööratav.

Definitsioonist järeldub, et taandumatu element on nullist erinev. Lihtne järeldus definitsioonidest on ka see, et taandumatu elemendi ja pööratava elemendi korrutis on taandumatu.

Lemma 2.15. *Olgu* a, b *kommutatiivse nulliteguriteta ringi* R *nullist erinevad elemendid. Element* a *on elemendi* b *jagaja ja element* b *on elemendi* a *jagaja parajasti siis, kui elemendid* a *ja* b *on assotsieerutud.*

TÕESTUS. Tarvilikkus. Olgu $a|b$ ja $b|a$. Siis leiduvad sellised elemendid c ja d ringis R, et $b = ac$ ja $a = bd$. Järelikult $b = bdc$. Kuna iga nullist erinev element ringist R on taandatav, siis $dc = 1$. Seega on element c pööratav ning elemendid a ja b assotsieeritud elemendid.

Piisavus. Järeldub assotsieerituse definitsioonist ja pärast seda definitsiooni tehtud märkusest. □

Lause 2.16. *On olemas ainult lõplik arv Gaussi täisarve, mille norm ei ületa antud positiivset reaalarvu.*

TÕESTUS. Olgu M positiivne reaalarv. Oletame, et $N(a+bi) \leqslant M$, kus $a+bi$ on Gaussi täisarv. See tähendab, et $a^2+b^2 \leqslant M$, kus a ja b on täisarvud. Sellest järeldub, et

$$|a| \leqslant \sqrt{M} \quad \text{ja} \quad |b| \leqslant \sqrt{M}.$$

On ainult lõplik arv täisarve, mille absoluutvärtus ei ole suurem kui $\sqrt{M}$.

Kuna arvude a ja b jaoks on lõplik arv võimalusi, siis ka arve $a+bi$, mille korral $N(a+bi) \leqslant M$, on lõplik arv. □

Definitsioon. Nulliteguriteta kommutatiivset ringi R nimetatakse *Eukleidese ringiks*, kui leidub kujutus

$$\delta\colon R \setminus \{0\} \to \mathbb{N} \cup \{0\},$$

mille korral:

(i) iga $a \in R, 0 \neq b \in R$, puhul $\delta(ab) \geqslant \delta(a)$;

(ii) iga $a \in R$ ja iga $0 \neq b \in R$ korral leiduvad sellised elemendid q ja r ringist R, et $a = bq + r$, kusjuures kas $r = 0$ või $\delta(r) < \delta(b)$.

Definitsioon. Nulliteguriteta ringi R nimetatakse *faktoriaalseks ringiks*, kui tema mistahes nullist erinev mittepööratav element on esitatav taandumatute elementide korrutisena ning selline esitus on ühene selles mõttes, et kui mittepööratav element $a \in R\setminus\{0\}$ on esitatav korrutisena

$$a = p_1 p_2 \cdots p_r$$

ja ka korrutisena

$$a = q_1 q_2 \cdots q_s,$$

kus $p_1, p_2, \ldots, p_r$, $q_1, q_2, \ldots, q_s$ on taandumatud elemendid, siis $r = s$ ning (pärast tegurite $q_1, q_2, \ldots, q_s$ võimalikku ümbernummerdamist) elemendid p_i ja q_i on assotsieeritud iga $i = 1, 2, \ldots, r$ korral.

Teoreem 2.17 ([1], lause 6.13.4)**.** *Eukleidese ring on faktoriaalne ring.*

Lemma 2.18. *Iga kompleksarvu $z = x + iy$ saab esitada kujul $z = v + z_1$, kus v on Gaussi täisarv ja z_1 on kompleksarv mille moodul on väiksem kui* 1.

TÕESTUS. Olgu a ja b sellised täisarvud, et $|x-a| \leqslant \frac{1}{2}$, $|y-b| \leqslant \frac{1}{2}$. Siis saame kirjutada

$$x = a + x_1, \;\; y = b + y_1,$$

kus x_1 ja y_1 on reaalarvud, mille absolutväärtus ei ületa arvu $\frac{1}{2}$. Tähistame

$$v = a + bi; \;\; z_1 = x_1 + y_1 i.$$

Lihtne on näha, et

$$z = x + iy = a + x_1 + i(b + y_1) = a + x_1 + bi + iy_1 = (a + bi) + (x_1 + y_1 i) = v + z_1$$

ja

$$|z_1| = \sqrt{x_1^2 + y_1^2} \leqslant \sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2} = \sqrt{\frac{1}{2}} < 1.$$

□

Teoreem 2.19. ***(Jäägiga jagamine)*** *Kui α ja $\beta \neq 0$, on Gaussi täisarvud, siis leiduvad sellised Gaussi täisarvud q ja r (jagatis ja jääk), et*

$$\alpha = \beta q + r,$$

ning

$$N(r) < N(\beta).$$

TÕESTUS. Lemmat 2.18 kasutades näeme, et kompleksarvu $z = \frac{\alpha}{\beta}$ võib esitada kujul

$$\frac{\alpha}{\beta} = q + z_1, \text{ kus } q \in \mathbb{Z}[i], \;\; z_1 \in \mathbb{C} \text{ ja } |z_1| < 1.$$

Seega,

$$\alpha = \beta q + r,$$

kus $r = \beta z_1$.

Kuna α, β, q on Gaussi täisarvud, siis $r = \alpha - \beta v$ peab ka olema Gaussi täisarv. Lisaks sellele $|r| = |\beta z_1| = |\beta| \cdot |z_1| < |\beta|$, kuna $|z_1| < 1$. Sellepärast saame, et $N(r) = |r|^2 < |\beta|^2 = N(\beta)$. □

Näide 2.20. Kasutades teoreemi 2.19, jagame arvu $\alpha = 17 - 3i$ jäägiga arvuga $\beta = 8 + 5i$.

Kõigepealt leiame kompleksarvu $\frac{\alpha}{\beta}$:

$$\frac{\alpha}{\beta} = \frac{17 - 3i}{8 + 5i} = \frac{(17 - 3i)(8 - 5i)}{(8 + 5i)(8 - 5i)} = \frac{(136 - 15) + i(-24 - 85)}{89} = \frac{121}{89} - \frac{109}{89} i.$$

Kõige lähem täisarv arvule $\frac{121}{89}$ on 1. Kõige lähem täisarv arvule $-\frac{109}{89}$ on -1. Seega $v = 1 - i$ ja $p = (17 - 3i) - (8 + 5i)(1 - i) = 4$, kusjuures $N(4) = 16 < 89 = N(8 + 5i)$.

Teoreem 2.21. *Gaussi täisarvude ring on faktoriaalne ring.*

TÕESTUS. Näitame, et Gaussi täisarvude ring on Eukleidese ring.

Lauses 1.2 tõestasime, et ring $\mathbb{Z}[i]$ on kommutatiivne nullteguriteta ring.

Vaatleme kujutust

$$N\colon \mathbb{Z}[i]\backslash\{0\} \longrightarrow \mathbb{N}\cup\{0\},\ \ \alpha \longmapsto N(\alpha).$$

Eukleidese ringi definitsiooni tingimus (i) on täidetud tänu järeldusele 2.9. Tingimus (ii) kehtib tänu teoreemile 2.19. Seega $\mathbb{Z}[i]$ on Eukleidese ring.

Teoreemist 2.17 teame aga, et Eukleidese ring on faktoriaalne ring, seega Gaussi täisarvude ring on ka faktoriaalne ring. □

3. Suurim ühistegur

Gaussi täisarvudest saab ka suurima ühisteguri leida. Selles peatükis näitame, kuidas seda teha Eukleidese algoritmi abil. Sõnastame ka mõned tulemused, mis on meil edaspidiseks vajalikud.

Definitsioon. Olgu R nulliteguriteta kommutatiivne ring. Elementide a ja b, $a, b \in R$, *suurimaks ühisteguriks* nimetatakse niisugust elementi $d \in R$, mis rahuldab järgmist kahte tingimust:

(i) d on nii a kui ka b jagaja, see tähendab, et $d|a$ ja $d|b$,

(ii) kui $c \in R$ on nii a kui ka b jagaja, siis c on d jagaja, see tähendab, et $c|a \wedge c|b \Longrightarrow c|d$.

Definitsioon. Olgu R nulliteguriteta kommutatiivne ring. Kui elementide $a, b \in R$ suurim ühistegur on 1, siis öeldakse, et elemendid a ja b on *ühisteguriteta*.

Teoreem 3.22. *Kui* $a, b \in \mathbb{Z}$ *ja* $\text{SÜT}(a, b) = 1$ *ringis* $\mathbb{Z}$, *siis* $\text{SÜT}(a, b) = 1$ *ringis* $\mathbb{Z}[i]$.

Tõestus. Olgu a ja b ühisteguriteta täisarvud. Siis saab leida sellised täisarvud x ja y, et

$$ax + by = 1.$$

Sellest võrdusest järeldub, et a ja b iga ühistegur, mis on Gaussi täisarv, peab olema arvu 1 jagaja ringis $\mathbb{Z}[i]$. □

Nagu teada (vt. [1], lk. 196) saab Eukleidese ringis suurimat ühistegurit leida Eukleidese algoritmi abil. Vaatame, kuidas see algoritm töötab Gaussi täisarvude ringi korral.

Olgu α ja β Gaussi täisarvud, ning $\beta \neq 0$.

Jagame jäägiga arvu α arvuga β. Kui jääk ei ole null, siis jagame β saadud jäägiga. Jätkame jagamist kuni seda on võimalik teha. Saame järgmised võrdused ja võrratused:

$$\begin{aligned}
\alpha &= \beta\sigma_1 + p_1, \text{ kus } N(p_1) < N(\beta),\\
\beta &= p_1\sigma_2 + p_2, \text{ kus } N(p_2) < N(p_1),\\
p_1 &= p_2\sigma_3 + p_3, \text{ kus } N(p_3) < N(p_2),\\
&\dots\\
p_{k-2} &= p_{k-1}\sigma_k + p_k, \text{ kus } N(p_k) < N(p_{k-1}),\\
p_{k-1} &= p_k\sigma_{k+1}
\end{aligned}$$

Jagamine ei saa jätkuda lõpmatuseni, sest jääkide $p_1, p_2, p_3, \ldots$ normid moodustavad mittenegatiivsete täisarvude kahaneva jada. Järelikult peab järjestikuste jagamiste protsess lõppema, aga ta saab lõppeda ainult siis, kui jääk on null.

Ülal kirjeldatud skeemis me eeldame, et ilma jäägita jagamine toimub $(k+1)$-sel skeemi sammul.

Nagu teame, on viimane nullist erinev jääk p_k arvude α ja β suurim ühistegur.

Näide 3.23. Leiame Gaussi täisarvude $\alpha = 96 - 38i$ ja $\beta = 31 + 77i$, suurima ühisteguri. Kasutame selleks Eukleidse algoritmi:

$$\begin{aligned}
&\frac{\alpha}{\beta} = \frac{96-38i}{31+77i} = \frac{5}{689} - \frac{857}{689}i; \;\; \sigma_1 = 0 + (-1)i = -i \\
&p_1 = \alpha - \sigma_1\beta = 96 - 38i + i(31+77i) = 19 - 7i \\
&\frac{\beta}{p_1} = \frac{31+77i}{19-7i} = \frac{5}{41} + \frac{166}{41}i; \;\; \sigma_2 = 0 + 4i = 4i \\
&p_2 = \beta - \sigma_2 p_1 = 31 + 77i - (19-7i)4i = 3 + i \\
&\frac{p_1}{p_2} = \frac{19-7i}{3+i} = 5 - 4i \text{ on Gaussi täisarv.}
\end{aligned}$$

Järelikult, $3 + i$ on arvude α ja β suurim ühistegur.

Lihtne on veenduda, et kehtivad jargmised tulemused.

Lause 3.24. *Kui R on faktoriaalne ring ja $a, b, c \in R$, siis* $\text{SÜT}(ca, cb) = c \cdot \text{SÜT}(a, b)$.

Lause 3.25. *Kui R on nulliteguriteta kommutatiivne ring, $a, b, u \in R$ ja u on pööratav, siis* $\text{SÜT}(a, bu) = \text{SÜT}(a, b)$.

Lause 3.26. *Olgu R faktoriaalne ring, $a, b \in R$, olgu $d = \text{SÜT}(a, b)$ ning olgu $a = da'$ ja $b = db'$, kus $a', b' \in R$. Siis* $\text{SÜT}(a', b') = 1$.

Neid lauseid on meil edaspidi vaja.

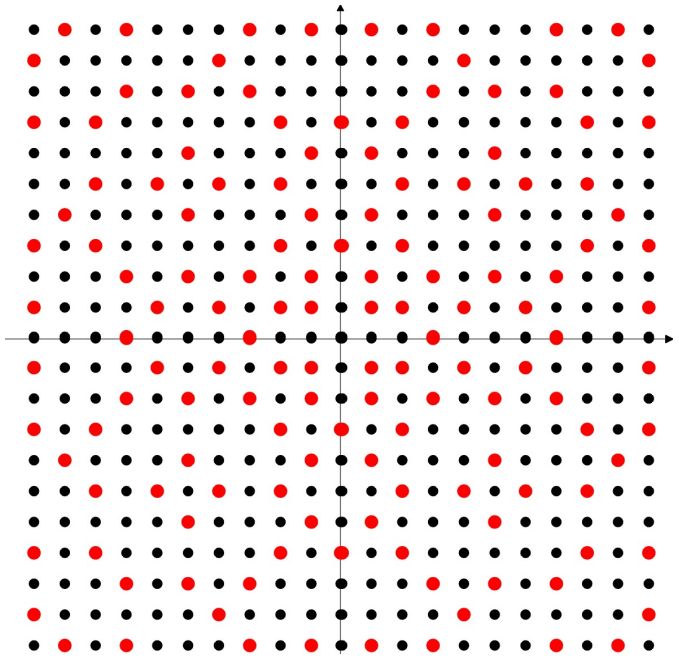
4. Gaussi algarvud

Selles peatükis me proovime aru saada, millised arvud on Gaussi algarvud. Näitame, et Gaussi algarvud jagunevad kahte tüüpi.

Definitsioon. *Algarv* on naturaalarv $p > 1$, mille ainsad naturaalarvulised jagajad on 1 ja p.

Naturaalarvu, mis on suurem kui 1 ja mis pole algarv, nimetatakse *kordarvuks*.

Definitsioon. Ringi $\mathbb{Z}[i]$ taandumatuid elemente nimetatakse *Gaussi algarvudeks*.



Joonis 3: Gaussi algarvud (punasega märgitud) komplekstasandil.

Definitsioonist järeldub, et nullist erinev mittepööratav Gaussi täisarv α on Gaussi algarv siis ja ainult siis, kui teda jagavad ainult temaga assotsieeritud Gaussi täisarvud ja pööratavad Gaussi täisarvud. Seega Gaussi täisarv π on Gaussi algarv parajasti siis, kui

1) $\pi \notin \{0, 1, -1, i, -i\}$,

2) kui $\pi = \alpha\beta$, kus $\alpha,\ \beta \in \mathbb{Z}[i]$, siis kas $\alpha \in \{1, -1, i, -i\}$ või $\beta \in \{1, -1, i, -i\}$.

Järeldus 4.27. *Kui α on Gaussi algarv, siis $N(\alpha) > 1$.*

TÕESTUS. Gaussi täisarvu α normi jaoks on kolm võimalust:

1) $N(\alpha) = 0$,

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

3) $N(\alpha) > 1$.

Paneme tähele, et kui α on Gaussi algarv, siis ei kehti võrdused 1) ja 2). Kuna võrdusest $N(\alpha) = 0$ järeldub, et $\alpha = 0$, siis ei saa kehtida võrdus 1) .

Kui $N(\alpha) = 1$, siis sellest järeldub, et $\alpha \in \{\pm 1, \pm i\}$. Saime, et α on pööratav element, seega α ei ole taandumatu. □

Teoreem 4.28. *Kui $\pi \in \mathbb{Z}[i]$ ja $N(\pi)$ on algarv, siis π on Gaussi algarv.*

TÕESTUS. Olgu $N(\pi)$ algarv. Siis $\pi \neq 0$. Samuti π on mittepööratav, sest pööratava elemendi norm on 1. Seega kui π ei ole Gaussi algarv, siis leiduvad $\alpha, \beta \in \mathbb{Z}[i]$ nii, et $\pi = \alpha\beta$ ja α, β ei ole pööratavad. Siis $N(\pi) = N(\alpha)N(\beta)$, kus $N(\alpha) \neq 1$ ja $N(\beta) \neq 1$. Kuna $N(\alpha) \neq 0$ ja $N(\beta) \neq 0$, siis $N(\alpha) > 1$ ja $N(\beta) > 1$, mis on vastuolus sellega, et $N(\pi)$ on algarv. Seega π on Gaussi algarv. □

Näide 4.29. Gaussi täisarvud $1 + i, 1 - i, -1 + i$ ja $-1 - i$ on Gaussi algarvud, sest nende kõigi norm on algarv 2.

Teoreemist 2.21 ja raamatu [1] teoreemist 6.12.5 järeldub vahetult järgmine tulemus.

Lause 4.30. *Kui π on Gaussi algarv, α, β Gaussi täisarvud ja $\pi|\alpha\beta$, siis $\pi|\alpha$ või $\pi|\beta$.*

Teoreem 4.31. *Iga Gaussi algarv on täpselt ühe algarvu jagaja.*

TÕESTUS. Lause 2.6 põhjal teame, et iga nullist erinev Gaussi täisarv on mingi naturaalarvu jagaja, näiteks oma normi jagaja. See kehtib ka Gaussi algarvude kohta.

Olgu Gaussi algarv π naturaalarvu a jagaja. Siis $a > 1$, sest $\pi \notin \{0, 1, -1, i, -i\}$.

Lahutame naturaalarvu a algteguriteks: $a = p_1 p_2 \cdots p_k$.

Tegurite $p_1, p_2, \ldots, p_k$ hulgas võib olla võrdseid. Kuna $\pi|p_1 p_2 \cdots p_k$, siis lause 4.30 põhjal leidub $i \in \{1, \ldots, k\}$ nii, et $\pi|p_i$.

Olgu p, q erinevad algarvud, mille korral $\pi|p$ ja $\pi|q$. Siis π jagab $\text{SÜT}(p, q)$ ringis $\mathbb{Z}[i]$. Teoreemi 3.22 põhjal $\text{SÜT}(p, q) = 1$ ringis $\mathbb{Z}[i]$. Seega $\pi|1$, ehk π on pööratav. Saime vastuolu. □

Teoreem 4.32. *Gaussi algarvu norm on algarv või algarvu ruut.*

TÕESTUS. Olgu π Gaussi algarv. Teoreemi 4.31 põhjal leidub algarv p nii, et $\pi|p$:

$$p = \pi\alpha,$$

kus $\alpha \in \mathbb{Z}[i]$. Siis saame normide jaoks võrduse:

$$N(p) = N(\pi)N(\alpha).$$

Näeme, et $N(\pi)$ on arvu $N(p) = p^2$ jagaja ringis $\mathbb{Z}$. Järelikult $N(\pi)$, mis on positiivne täisarv ja ei ole 1, võib olla ainult p või p^2.

Paneme tähele, et $N(\pi)$ saab olla p^2 ainult siis, kui võrduses $p = \pi\alpha$ arv α on üks pööratarvatest Gaussi täisarvudest, st. kui π on assotsieeritud naturaalarvuga p.

Kui $N(\pi) = p$, siis $p = \pi\bar{\pi}$, kus $\bar{\pi}$ on arvu π kaaskompleksarv. Ka arv $\bar{\pi}$ on Gaussi algarv, kuna $N(\bar{\pi}) = N(\pi) = p$ ja me saame kasutada teoreemi 4.28. □

Definitsioon. Gaussi algarve, mille norm on algarv, nimetatakse *esimest liiki* Gaussi algarvudeks. Gaussi algarve, mille norm on algarvu ruut, nimetatakse *teist liiki* Gaussi algarvudeks.

Olgu $\alpha = a + bi$ esimest liiki Gaussi algarv. Siis

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

Järelikult, algarv p, mis on esimest liiki Gaussi algarvu norm, on esitatud kahe täisarvu ruutude summana. Kehtib ka vastupidine: kui algarv p on esitatud kahe täisarvu ruutude summana, siis teda saab lahutada kaheks algteguriks. Tõepoolest, kui

$$p = a^2 + b^2,$$

kus $a, b \in \mathbb{Z}[i]$, siis

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

ning arvud $a + bi$ ja $a - bi$ Gaussi algarvud, kuna nende kummagi norm võrdub algarvuga p.

Definitsioon. Olgu $a, b \in \mathbb{Z}$ ja $n \in \mathbb{N}$. Öeldakse, et a ja b on *kongruentsed* mooduli n järgi (ja kirjutatakse $a \equiv b \pmod{n}$), kui $n|b - a$, s.t. kui leidub selline $k \in \mathbb{Z}$, et $b = a + (-k)n$.

Lause 4.33. *Iga algarv kujul $4n+3$, kus $n \in \mathbb{N} \cup \{0\}$, on teist liiki Gaussi algarv.*

TÕESTUS. Vaatleme algarvu $p = 4k + 3$, kus $k \in \mathbb{N} \cup \{0\}$. Kuna ring $\mathbb{Z}[i]$ on faktoriaalne, siis p esitub taandumatute elementide korrutisena: $p = \pi_1 \cdots \pi_s$, kus $\pi_1, \ldots, \pi_s$ on taandumatud. Võrdusest $p^2 = N(\pi_1) \cdots N(\pi_s)$ järeldub, et on kaks võimalust.

1) $s = 1$ ja $N(\pi_1) = p^2$. Sellisel juhul p on teist liiki Gaussi algarv.

2) $s = 2$, $N(\pi_1) = p$ ja $N(\pi_2) = p$. Siis π_1 ja π_2 on esimest liiki Gaussi algarvud.

Eespooltõestatu põhjal

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

kus $a, b \in \mathbb{Z}$.

Kuna p on paaritu arv, siis a ja b peavad olema erineva paarsusega. Näiteks a on paaris ja b on paaritu arv. Siis

$$a^2 \equiv 0 \pmod 4, \;\; b^2 \equiv 1 \pmod 4$$

ning järelikult

$$p = a^2 + b^2 \equiv 1 \pmod 4,$$

see tähendab, et p on kujul $4n + 1$, mis on vastuolus eeldusega. □

Lause 4.34 (Vt. [1], lause 7.1.9)**.** *n-nda astme polünoomil üle kommutatiivse korpuse K ei saa (kordsust arvestades) olla rohkem kui n juurt korpuses K.*

Lause 4.35. *Kongruentsil*

$$x^2 + 1 \equiv 0 \pmod p$$

algarvulise mooduliga p leidub lahend, kui $p = 4n + 1$.

TÕESTUS. Olgu $p = 4n + 1$.

Siis $x^{p-1} - 1 = x^{4n} - 1$ jagub polünoomiga $x^4 - 1$ ja, järelikult, ka polünoomiga $x^2 + 1$. Seega $(x^2 + 1)g(x) = x^{p-1} - 1$, kus $g(x)$ on polünoom astmega $p - 3$.

Kongruents $x^{p-1} - 1 \equiv 0 \pmod p$ omab $p - 1$ lahendit, nimelt $x = 1, 2, 3, \ldots, p - 1$.

Järelikult, lause 4.34 tõttu, kongruentsil $x^2+1 \equiv 0 (\mathrm{mod}\, p)$ on kaks lahendit. □

Teoreem 4.36. *Iga algarvu kujul $4n + 1$, kus $n \in \mathbb{N}$ saab lahutada kahe esimest liiki Gaussi algarvu korrutiseks.*

TÕESTUS. Olgu $p = 4k + 1$ algarv. Kongurentsil

$$x^2 + 1 \equiv 0 \pmod{p}$$

leidub lahend tänu lausele 4.35.

Olgu $a \in \mathbb{Z}$ selle kongurentsi lahend. Siis p jagab arvu $(a + i)(a - i) = a^2 + 1$. Sellest järeldub, et Gaussi täisarvud $a + i$ ja $a - i$ ei saa olla samaaegselt ühisteguriteta arvuga p, kuna muidu nende korrutis $a^2 + 1$, mis jagub arvuga p, oleks ühisteguriteta arvuga p.

Olgu näiteks $\text{SÜT}(a + i, p) \neq 1$ ja tähistame $\pi = \text{SÜT}(a + i, p)$. On lihtne näha, et arvude $a - i$ ja p suurimaks ühisteguriks on siis arv $\bar{\pi}$, mis on arvu π kaaskompleksarv. Arvud π ja $\bar{\pi}$ ei ole pööratavad arvud ja nad on ühistegurita. Vastasel juhul oleks nad ühisteguriga α, mis ei ole pööratav, siis α jagaks arve $a + i$, $a - i$ ja p ning järelikult, oleks ta siis arvude p ning $(a + i) - (a - i) = 2i$ ühisteguriks, mis pole võimalik, kuna arvud p ja $2i$ ühisteguriteta. Sellest järeldub, et p, mis jagub arvudega π ja $\bar{\pi}$, jagub nende korrutisega:

$$p = \pi\bar{\pi}\lambda = N(\pi) \cdot \lambda,$$

kus $\lambda \in \mathbb{Z}[i]$. Võrdusest $p = N(\pi) \cdot \lambda$ järeldub, et $\lambda \in \mathbb{N}$.

Kuna $N(\pi)$ on naturaalarv, mis ei ole 1, saab see olla ainult $N(\pi) = p$ ja $\lambda = 1$. Sellest järeldame, et π ja $\bar{\pi}$ on esimest liiki Gaussi algarvud, kuna neist kummagi norm võrdub algarvuga p. □

Teoreem 4.37. *Arv 2 jagub ainult ühe esimest liiki Gaussi algarvuga. Nimelt* $2 = -i(1 + i)^2$.

TÕESTUS. Võrdust $2 = -i(1 + i)^2$ kontrollime järgmiselt:

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

Arv $1 + i$ on esimest liiki algarv, tänu teoreemile 4.28 kuna

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

Väide, et Gaussi algarvud, mis ei ole kujul $1 + i$, ei jaga arvu 2, järeldub algteguriteks lahutamise ühesusest (teoreem 2.21). □

Võtame lõpuks kokku tähtsamad faktid Gaussi algarvude kohta.

1. Iga Gaussi algarv on naturaalarvu jagaja.
2. Algarvud kujul $4n + 3$ on Gaussi algarvud.

3. Algarvud kujul $4n+1$ saab lahutada kahe esimest liiki Gaussi algarvu korrutiseks.

4. Arv 2 on assotsieeritud esimest liiki Gaussi algarvu $1+i$ ruuduga.

Tuletame meelde mõned tulemused harilike algarvude kohta.

Lause 4.38 ([2], teoreem 2.4)**.** *Algarve kujul* $4n+3$*, kus* $n \in \mathbb{N} \cup \{0\}$*, on lõpmata palju.*

Lause 4.39 ([2], lause 9.9)**.** *Algarve kujul* $4n+1$*, kus* $n \in \mathbb{N}$*, on lõpmata palju.*

Järeldus 4.40. *Teist liiki Gaussi algarve on lõpmata palju.*

TÕESTUS. Järeldub lausest 4.33 ja lausest 4.38. □

Järeldus 4.41. *Eseimest liiki Gaussi algarve on lõpmata palju.*

TÕESTUS. Järeldub teoreemist 4.36 ja lausest 4.39. □

5. Rakendused

Toome mõned näited selle kohta, kuidas Gaussi täisarvude abil saab leida täisarvuliste kordajatega võrrandite täisarvulisi lahendeid.

Näide 5.42. Leiame Pythagorase võrrandi $x^2+y^2=z^2$ kõik täisarvulised lahendid (x,y,z), kus $\text{SÜT}(x,y)=1$.

LAHENDUS. Olgu (x,y,z) võrrandi $x^2+y^2=z^2$ lahend ja $\text{SÜT}(x,y)=1$. Siis üks arvudest x,y peab olema paariasrv, teine paaritu arv ja z ka paaritu arv.

Arvud x,y,z rahuldavad võrdust $(x+yi)(x-yi)=z^2$. Näitame, et $\text{SÜT}(x+yi,x-yi)=1$. Selleks oletame, et leidub mittepööratav element $c\in\mathbb{Z}[i]$ nii, et $c|x+yi$ ja $c|x-yi$. Siis

$$c|(x+yi)-(x-yi)=2yi,$$
$$c|(x+yi)+(x-yi)=2x.$$

Kui $c\nmid 2$, siis lause 4.30 tõttu $c|x$ ja $c|y$. Teoreemi 3.22 põhjal $\text{SÜT}(x,y)=1$ ringis $\mathbb{Z}[i]$. Seega $c|1$ ringis $\mathbb{Z}[i]$ ehk c on pööratav, saime vastuolu. Järelikult $c|2$. Siis aga $N(c)|N(2)=4$, s.t. $N(c)=2$ või $N(c)=4$. Võrdusest $(x+yi)(x-yi)=z^2$ järeldub, et $c^2|z^2$ ja seega $N(c^2)|N(z^2)$. Kuna aga $N(z^2)$ on paaritu arv ja $N(c^2)$ on paaris, siis oleme saanud vastuolu.

Kuna kahe ühisteguriteta arvu $x+yi$ ja $x-yi$ korrutis on täisruut, siis algteguriteks lahutamise ühesusest järeldub, et nii arvu $x+yi$ kui $x-yi$ algteguriteks lahutuses peavad algtegurid esinema paarisarvulises astmes. Muuhulgas

$$x+yi=\varepsilon\pi_1^2\pi_2^2\cdots\pi_k^2=\varepsilon\alpha^2,$$

kus $\varepsilon\in U(\mathbb{Z}[i])$ ja $\alpha=\pi_1\pi_2\cdots\pi_k$ on mingi Gaussi täisarv. Arvu ε jaoks on neli võimalust:

$$\varepsilon=1;\ \ \varepsilon=-1;\ \ \varepsilon=i;\ \ \varepsilon=-i.$$

Kuid piisab vaadata nendest ainult kahte: $\varepsilon=1$ ja $\varepsilon=i$, kuna

$$-\alpha^2=(\alpha i)^2,\ \ -i\alpha^2=i(\alpha i)^2.$$

Need võimalused arvu $x+yi$ jaoks on järgmised:

$$x+yi=(a+bi)^2 \text{ ja } x+yi=i(a+bi)^2,$$

kus a,b on mingid täisarvud ja $\alpha=a+bi$.

Avame sulud ja võrdleme reaal- ja imaginaarosasid, saame arvude x ja y jaoks avaldise:

$$x=a^2-b^2;\ \ y=2ab \quad \text{või} \quad x=-2ab;\ y=a^2-b^2.$$

Saab näidata, et kui valida a ja b nii, et nad on ühistegurita ja erineva paarsusega, siis nende valemite abil defineeritud x ja y on ka ühistegurita.

Näide 5.43. Leiame kõik võrrandi

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

täisarvulised lahendid (x, y, z), kus $\text{SÜT}(x, y) = 1$.

LAHENDUS. Kõigepealt märgime, et võrrandi igas lahendis peavad x ja y olema paaritud, sest kui x ja y on erineva paarsusega, siis $x^2 + y^2$ on paaritu ja ei saa võduda $2z^2$-ga, kui aga x ja y on mõlemad paarisarvud, siis $\text{SÜT}(x, y) \geqslant 2$.

Esitame võrrandi kujul

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

Paneme tähele, et $2 \nmid x + yi$. Kui $2|x + yi$ siis $2(a + bi) = x + yi$, kus $a, b \in \mathbb{Z}$. Võrdus kehtib ainult siis, kui $2a = x$ ja $2b = y$. Saime vastuolu, sest x ja y on paaritud.

Näitame, et $1 + i = \text{SÜT}(x + yi, x - yi)$.

i) Kuna x ja y on paaritud, siis

$$\frac{x + yi}{1 + i} = \frac{x + y}{2} + \frac{y - x}{2} i \in \mathbb{Z}[i],$$
$$\frac{x - yi}{1 + i} = \frac{x - y}{2} + \frac{-x - y}{2} i \in \mathbb{Z}[i].$$

Seega $1 + i|x + yi$ ja $1 + i|x - yi$ ringis $\mathbb{Z}[i]$.

ii) Oletame, et $\delta|x + yi$ ja $\delta|x - yi$. Siis $\delta|2x$ ja $\delta|2yi$, kust $\delta|2y$. Järelikult, kasutades lauset 3.24 saame, et $\delta|\text{SÜT}(2x, 2y) = 2 \cdot \text{SÜT}(x, y) = 2$. Arvu 2 jagajad assotsieerituse täpsuseni on $1, 1 + i$ ja 2. Ei ole võimalik, et $\delta = 2$, sest $2 \nmid x + yi$. Seega $\delta = 1$ või $\delta = 1 + i$. Mõlemal juhul $\delta|1 + i$.

Kuna $1 + i = \text{SÜT}(x + yi, x - yi)$, siis

$$\text{SÜT}\left(\frac{x + yi}{1 + i}, \frac{x - yi}{1 + i}\right) = 1$$

lause 3.26 põhjal.

Paneme tähele, et

$$\frac{x - yi}{1 + i} = \frac{(-y - xi)i}{(1 - i)i} = \frac{-y - xi}{1 - i} = \frac{x - yi}{1 - i} \cdot (-i),$$

kus $-i$ on pööratav. Järelikult lause 3.25 põhjal

$$1 = \text{SÜT}\left(\frac{x+yi}{1+i}, \frac{x-yi}{1-i} \cdot (-i)\right) = \text{SÜT}\left(\frac{x+yi}{1+i}, \frac{x-yi}{1-i}\right).$$

Kuna

$$\frac{x+yi}{1+i} \cdot \frac{x-yi}{1-i} = z^2,$$

siis faktoriaalsuse tõttu saame võrduse

$$x + yi = \varepsilon(1+i)(a+bi)^2,$$

kus $a + bi \in \mathbb{Z}[i]$.

Jälle ε uurimisel piisab vaadata kahte võimalust:

$$\varepsilon = 1 \text{ ja } \varepsilon = i.$$

Need võimalused määravad lahendid:

$$\begin{cases} x = a^2 - 2ab - b^2 \\ y = a^2 + 2ab - b^2 \end{cases}$$

ja

$$\begin{cases} x = -a^2 - 2ab + b^2 \\ y = a^2 - 2ab - b^2 \end{cases}.$$

Kirjandus

[1] M. Kilp, *Algebra I*, Eesti Matemaatika Selts, Tartu, 2005.

[2] V. Laan, *Arvuteooria loengukonspekt*, Tartu Ülikool, 2012, http://math.ut.ee/pmi/kursused/arvuteooria/kon.pdf (viimati vaadatud 21.05.2014).

[3] К. Ф. Гаусс, *Труды по теории чисел*, Издательство Академии Наук СССР, Москва, 1959.

[4] А. Н. Колмогоров, А. П. Ющкевич (ред.), *Математика XIX века. Математическая логика, алгебра, теория чисел, теория вероятностей*, Наука, Москва, 1978.

[5] Р. О. Кузьмин, Д. К. Фаддеев, *Алгебра и арифметика комлексных чисел. Пособие для учителей*, Учпедгиз, Москва, 1939.

[6] Л. Я. Окунев, *Целые комлексные числа*, Государственное учебно-педагогическое издательство Наркомпроса РСФСР, Москва, 1941.

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Galina Brokan (sünnikuupäev 05.03.1992),

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose "Gaussi täisarvud", mille juhendaja on Valdis Laan,

   1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace'is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

   1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace'i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartus, **04.06.2014**