VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
MATEMATIKOS INSTITUTAS
TIKIMYBIŲ TEORIJOS IR SKAIČIŲ TEORIJOS KATEDRA

Žygimantas Baronėnas

Algebrinių skaičių multiplikatyvusis priklausomumas

Multiplicative Dependence of Algebraic Numbers

Magistro baigiamasis darbas

Leidžiu ginti .....
Darbo vadovas **prof. dr. Paulius Drungilas**

Vilnius 2020

Turinys

Įvadas

1 apibrėžimas. Skaičiai $z_1, z_2 \in \mathbb{C}^* = \mathbb{C} \setminus \{0\}$ vadinami *multiplikatyviai priklausomais*, jei egzistuoja tokie $a, b \in \mathbb{Z}$, iš kurių bent vienas nenulinis, kad būtų teisinga lygybė

$$z_1^a z_2^b = 1,$$

priešingu atveju, skaičiai z_1, z_2 vadinami *multiplikatyviai nepriklausomais*.

Akivaizdu, kad skaičiai z_1, z_2 yra multiplikatyviai prikausomi tada ir tik tada, kai su bet kokiomis šaknimis iš vieneto ζ, ζ', skaičiai $\zeta z_1, \zeta' z_2$ yra multiplikatyviai priklausomi. Taip pat, skaičiai z_1, z_2 yra multiplikatyviai priklausomi, jei bent vienas iš jų yra šaknis iš vieneto. Nesunku įsitikinti, kad du natūralieji skaičiai $A > B > 1$ yra multiplikatyviai priklausomi tada ir tik tada, kai egzistuoja tokie natūralieji skaičiai $a < b$ ir $g > 1$, kad $A = g^b$ ir $B = g^a$.

Tegul $\zeta_k := e^{\frac{2\pi i}{k}}$ – primityvioji k-tojo laipsnio šaknis iš vieneto. Madritsch ir Ziegler [1], [2] straipsniuose iškėlė hipotezę:

2 hipotezė ([1, 1.4 klausimas], [2, 2.8 hipotezė])**.** *Skaičiai $m-\zeta_k, n-\zeta_k$ yra multiplikatyviai nepriklausomi su kiekvienu $k \geqslant 3$ ir kiekvienu $m > n \in \mathbb{N}$, išskyrus atvejį $(n, k) = (1, 6)$.*

Nesunku pastebėti, kad jei $(n, k) = (1, 6)$, tai skaičius $n - \zeta_k = 1 - \zeta_6 = \zeta_6^{-1}$ yra šaknis iš vieneto, todėl skaičiai $m - \zeta_6, 1 - \zeta_6$ yra multiplikatyviai priklausomi su kiekvienu $m \in \mathbb{C}$.

Įtaką šios hipotezės atsiradimui padarė [3] straipsnis, kuriame Hansel ir Safer, naudodami $-m + \zeta_k$ formos bazes iš žiedo $\mathbb{Z}[\zeta_k]$, įrodė atskirą hipotezės atvejį, kai $k = 4$.

Buvo išnagrinėta ir daugiau atskirų atvejų. Pavyzdžiui, [1] straipsnyje hipotezė įrodyta, kai k yra kokio nors nedidelio pirminio skaičiaus laipsnis.

Taip pat [1], [2] straipsniuose Madritsch ir Ziegler hipotezė buvo įrodyta visiems $0 < m - n < 10^6$ ir $m > n > C(k)$, kur $C(k) > 0$ – konstanta, priklausanti tik nuo k. Ši konstanta pasirodo Schinzel ir Tijdeman straipsnyje [4], tačiau yra tokia didelė, kad panašu, jog sekant tomis pačiomis idėjomis, hipotezės nepavyktų įrodyti net mažoms k reikšmėms.

Šio magistro darbo pagrindinis tikslas yra apžvelgti P.Drungilo ir A.Dubicko [5] straipsnį apie dviejų sveikųjų skaičių, pastumtų per šaknį iš vieneto, multiplikatyvųjį priklausomumą bei gauti naujų rezultatų nagrinėjant dviejų algebrinių skaičių multiplikatyviojo priklausomumo klausimą.

Pavyko įrodyti, kad jei α – realusis algebrinis skaičius, kuris nėra sveikasis algebrinis skaičius ir $2\alpha \notin \mathbb{Z}$, tuomet su bet kuriais $m, n \in \mathbb{Z}$, $m \neq n$, skaičiai $m-\alpha, n-\alpha$ yra multiplikatyviai nepriklausomi. Taip pat ištyrėme ir tuos atvejus, kai $2\alpha \in \mathbb{Z}$.

Toliau nagrinėjome skaičių $m-\alpha$ ir $n-\alpha$ multiplikatyvųjį priklausomumą, kur $m, n \in \mathbb{Z}$, $m \neq n$, ir α – sveikasis algebrinis skaičius. Tyrėme atvejį, kai $\alpha = \sqrt{k}$, kur $k \in \mathbb{N}$, $\sqrt{k} \notin \mathbb{N}$ ir parodėme, kad skaičiai $k - \sqrt{k^2 \pm 1}, -k - \sqrt{k^2 \pm 1}$ yra multiplikatyviai priklausomi su visais $k \in \mathbb{N}$ bei suformulavome hipotezę apie kitus sveikuosius algebrinius skaičius iš šios klasės. Taip pat radome be galo daug sveikųjų algebrinių skaičių $\gamma := \pm\sqrt{\alpha} \pm \sqrt{\beta}$, kur $\alpha > \beta \in \mathbb{N}$ – bekvadračiai ir be galo daug natūraliųjų $m > n > \sqrt{\alpha} + \sqrt{\beta}$ reikšmių, su kuriomis skaičiai $m-\gamma, n-\gamma$ yra multiplikatyviai nepriklausomi.

2 skyrius

Apžvalga

Naują požiūrį į Madritsch ir Ziegler iškeltą problemą pasiūlė P. Drungilas ir A. Dubickas, kurie savo straipsnyje [5] pilnai įrodė 2 hipotezę. Apžvelgsime pagrindinius įrodymo žingsnius ir idėjas.

3 apibrėžimas. Algebrinį skaičių $\alpha \neq 0$ vadinsime *sangrąžiniu*, jei $1/\alpha$ yra skaičiaus α algebrinis jungtinis virš $\mathbb{Q}$.

Naudinga pastebėti, kad kiekvieno sangrąžinio algebrinio skaičiaus $\alpha \neq \pm 1$ laipsnis $d := deg(\alpha)$ virš $\mathbb{Q}$ yra lyginis, o skaičiaus $\beta := \alpha + 1/\alpha$ laipsnis yra $d/2$.

Raktu į 2 hipotezės įrodymą tapo toks rezultatas:

4 teorema ([5, 1.1 teorema])**.** *Tegul α – sangrąžinis algebrinis skaičius, $deg(\alpha) \geqslant 4$ ir skaičius $\beta := \alpha + 1/\alpha$ turi bent du algebrinius jungtinius intervale $(-\infty, 2]$. Tuomet skaičiai $m - \alpha, n - \alpha$ yra multiplikatyviai nepriklausomi su visais natūraliaisiais $m > n > 0$.*

Teoremos įrodymas remiasi elementariomis idėjomis iš algebrinės skaičių teorijos. Kitame skyriuje jas pritaikysime naujiems rezultatams gauti.

5 teorema ([5, 1.2 teorema])**.** *Skaičiai $m - \zeta_k, n - \zeta_k$ yra multiplikatyviai nepriklausomi su kiekvienu $k \geqslant 3$ ir kiekvienu $m > n \in \mathbb{N}$, išskyrus atvejį $(n, k) = (1, 6)$.*

Pirmiausia pastebime, kad kiekvienam $k \geqslant 7$ ir $k = 5$ turime

$$deg(\zeta_k) = \phi(k) \geqslant 4,$$

kur ϕ – Oilerio funkcija. Su kiekviena iš minėtų k reikšmių, skaičius $\alpha = \zeta_k$ yra sangrąžinis algebrinis skaičius, kurio laipsnis yra $\phi(k) \geqslant 4$ ir

$$\beta := \zeta_k + 1/\zeta_k = 2cos(2\pi/k)$$

turi $\phi(k)/2 \geqslant 2$ algebrinius jungtinius intervale $(-2, 2)$. Todėl pagal 4 teoremą, skaičiai $m - \zeta_k, n - \zeta_k$ yra multiplikatyviai nepriklausomi su

visais $m > n > 0$. Likę atvejai, kai $k = 3, 4, 6$, išnagrinėjami atskirai, remiantis gerai žinomų Diofantinių lygčių teorija. Tam, kad būtų aiški idėja, atvejį $k = 3$ išnagrinėsime detaliai.

Tarkime priešingai, kad skaičiai $m-\zeta_3, n-\zeta_3$ yra multiplikatyviai priklausomi. Tuomet egzistuoja tokie $a, b \in \mathbb{Z}$, kur $a \neq 0$ arba $b \neq 0$, kad

$$(m-\zeta_3)^a = (n-\zeta_3)^b. \tag{2.1}$$

Nemažindami bendrumo galime laikyti, kad $a \in \mathbb{N}$ ir $b \in \mathbb{Z}$. Imkime skaičių kūno $K = \mathbb{Q}(\zeta_3)$ $\mathbb{Q}$-homomorfizmą f, kuris elementą ζ_3 atvaizduoja į $1/\zeta_3$, t.y. $f(\zeta_3) = 1/\zeta_3$. Tuomet šiuo atvaizdžiu paveikę abi 2.1 lygybės puses gausime

$$(m-1/\zeta_3)^a = (n-1/\zeta_3)^b. \tag{2.2}$$

Sadauginę 2.1 ir 2.2 lygybes turėsime

$$(m^2+1-m\beta)^a = (n^2+1-n\beta)^b, \tag{2.3}$$

kur $\beta := \zeta_3 + 1/\zeta_3 = 2cos(2\pi/3) = -1$. Iš (2.3) lygybės gauname, kad du natūralieji skaičiai m^2+m+1 ir n^2+n+1 yra multiplikatyviai priklausomi. Vadinasi, egzistuoja tokie natūralieji skaičiai $g > 1$ ir $b' > a' \geqslant 1$, kad

$$m^2+m+1 = g^{b'} \text{ ir } n^2+n+1 = g^{a'}.$$

Nagell [6] staipsnyje parodė, kad $18^2+18+1 = 7^3$ yra vienintelis Diofantinės lygties

$$X^2+X+1 = Y^c,$$

kur $X, Y, c > 1$, sprendinys. Tuo pasinaudodami gauname, kad $(m, g, b') = (18, 7, 3)$ ir kadangi $b' > a' \geqslant 1$, tai išsprendę porą kvadratinių lygčių

$$\begin{cases} n^2+n+1 = 7^2, & n_{1,2} = -1/2 \pm \sqrt{193}/2, \\ n^2+n+1 = 7^1, & n_{1,2} = -3, 2 \end{cases}$$

randame, kad $(n, a') = (2, 1)$. Vadinasi, nagrinėjame tiksliai tokią lygybę

$$(18-\zeta_3)^a = (2-\zeta_3)^b, \tag{2.4}$$

kur $a \in \mathbb{N}$ ir $b \in \mathbb{Z}$. Iš 2.2 žinome, kad

$$(18-1/\zeta_3)^a = (2-1/\zeta_3)^b. \tag{2.5}$$

Kadangi $\zeta_3 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ ir $1/\zeta_3 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$, tai sudauginę 2.4 ir 2.5 lygybes gausime

$$343^a = 7^b \implies b = 3a.$$

Nagrinėkime santykį

$$\frac{18-\zeta_3}{(2-\zeta_3)^3}=\frac{(18-\zeta_3)(2-1/\zeta_3)^3}{(2-\zeta_3)^3(2-1/\zeta_3)^3}=\frac{(37-\sqrt{3}i)(10+9\sqrt{3}i)}{2\cdot 7^3}=\frac{397+323\sqrt{3}i}{686}.$$

Nesunku patikrinti, kad gautas skaičius yra polinomo

$$p(x)=x^2-\frac{397}{343}x+1$$

šaknis. Negana to, tai yra minimalusis šio skaičiaus polinomas. Mūsų nagrinėtas santykis turėtų būti šaknis iš vieneto, tačiau gauname, kad

$$\frac{397+323\sqrt{3}i}{686}$$

nėra sveikasis algebrinis skaičius. Vadinasi, šis skaičius nėra ir šaknis iš vieneto. Čia gauname prieštarą tam, kad skaičiai $18-\zeta_3$ ir $2-\zeta_3$ yra multiplikatyviai priklausomi. Taigi, detaliai išnagrinėjome atvejį, kai $k=3$. Likę atvejai ($k=4,6$) įrodomi labai panašiai.

6 apibrėžimas. Skaičiai $z_1,z_2,\ldots,z_k\in\mathbb{C}^*=\mathbb{C}\setminus\{0\}$ vadinami *multiplikatyviai priklausomais*, jei egzistuoja tokie $a_1,a_2,\ldots,a_k\in\mathbb{Z}$, iš kurių bent vienas nenulinis, kad būtų teisinga lygybė

$$z_1^{a_1}z_2^{a_2}\ldots z_k^{a_k}=1,$$

priešingu atveju, skaičiai $z_1,z_2,\ldots,z_k$ vadinami *multiplikatyviai nepriklausomais*.

P.Drungilas ir A. Dubickas apibendrino 4 teoremą tuo atveju, kai nagrinėjame ne dviejų, o k skaičių multiplikatyvųjį priklausomumą:

7 teorema ([5, 3.1 teorema])**.** *Tegul α – sangrąžinis algebrinis skaičius, $deg(\alpha)\geqslant 6$ ir skaičius $\beta:=\alpha+1/\alpha$ turi bent $t\geqslant 3$ algebrinius jungtinius intervale $(-\infty,2]$. Tuomet skaičiai*

$$m_1-\alpha,m_2-\alpha,\ldots,m_{t-1}-\alpha$$

yra multiplikatyviai nepriklausomi su visais natūraliaisiais $m_1>m_2>\ldots m_{t-1}>0$.

Pastebima, kad atveju $t=3$, šis rezultatas yra šiek tiek silpnesnis negu 4 teorema.

Taip pat verta paminėti, kad ankstesniame P. Drungilo ir A. Dubicko straipsnyje [7], buvo gautas įdomus rezultatas:

Jeigu α – algebrinis skaičius, kuris nėra sveikasis algebrinis skaičius ir

$$(m_1-\alpha)^{a_1}(m_2-\alpha)^{a_2}\ldots(m_k-\alpha)^{a_k}=1,$$

kur $a_1,a_2,\ldots,a_k\in\mathbb{Z}$, tai $a_1+a_2+\cdots+a_k=0$.

3 skyrius

Rezultatai

Toliau pateiksime rezultatus, kuriuos pavyko gauti tiriant dviejų sveikųjų skaičių, pastumtų per algebrinį skaičių, multiplikatyvųjį priklausomumą.

8 teiginys. *Tegul α – algebrinis skaičius, kuris nėra sveikasis algebrinis skaičius. Tarkime, jog egzistuoja tokie skaičiai $m, n \in \mathbb{Z}$, $m \neq n$, ir $a, b \in \mathbb{Z}$, kur $a \neq 0$ arba $b \neq 0$, kad būtų teisinga lygybė*

$$(m - \alpha)^a = (n - \alpha)^b.$$

Tuomet $a = b$ ir

$$\alpha = \frac{m - \zeta_a n}{1 - \zeta_a},$$

kur ζ_a yra a-tojo laipsnio šaknis iš vieneto ir $\zeta_a \neq 1$.

Įrodymas. Tarkime priešingai, kad lygybė

$$(m - \alpha)^a = (n - \alpha)^b \tag{3.1}$$

teisinga su skaičiais $a, b \in \mathbb{Z}$, $a \neq b$. Nemažindami bendrumo galime laikyti, kad $a > b$ ir $a \geqslant 0$.

Jei $a = 0$, tai $b < 0$ ir iš (3.1) lygybės gauname $(n - \alpha)^{-b} = 1$. Vadinasi, α yra polinomo

$$(n - x)^{-b} - 1$$

šaknis. Taigi, α yra sveikasis algebrinis skaičius – prieštara. Dabar turime, jog $a > b$ ir $a > 0$.

Jei $b \leqslant 0$, tai iš (3.1) lygybės gauname, kad α yra polinomo

$$(m - x)^a (n - x)^{-b} - 1$$

šaknis. Tai reiškia, kad α yra sveikasis algebrinis skaičius – prieštara.

Jei $b > 0$, tai iš (3.1) lygybės gauname, kad α yra polinomo

$$(m - x)^a - (n - x)^b$$

šaknis. Vėlgi, gauname prieštarą tam, kad α nėra sveikasis algebrinis skaičius. Taigi turime, kad (3.1) lygybėje $a = b > 0$. Tuomet

$$\left(\frac{m-\alpha}{n-\alpha}\right)^a = 1 \implies \frac{m-\alpha}{n-\alpha} = \zeta_a,$$

kur ζ_a yra a-tojo laipsnio šaknis iš vieneto. Be to, $\zeta_a \neq 1$, nes priešingu atveju gautume $m = n$. Iš čia turime, kad

$$\alpha = \frac{m - \zeta_a n}{1 - \zeta_a}.$$

□

9 išvada. *Tarkime, kad α – realusis algebrinis skaičius, kuris nėra sveikasis algebrinis skaičius ir $2\alpha \notin \mathbb{Z}$. Tuomet su bet kuriais $m, n \in \mathbb{Z}$, $m \neq n$, skaičiai $m - \alpha$ ir $n - \alpha$ yra multiplikatyviai nepriklausomi.*

Įrodymas. Tarkime, kad skaičiai $m - \alpha$ ir $n - \alpha$ yra multiplikatyviai priklausomi, t.y. egzistuoja tokie sveikieji skaičiai $a, b \in \mathbb{Z}$, iš kurių bent vienas nenulinis, kad yra teisinga lygybė $(m - \alpha)^a = (n - \alpha)^b$. Tuomet, remiantis 8 teiginiu, egzistuoja tokia a-tojo laipsnio šaknis iš vieneto $\zeta_a \neq 1$, kad

$$\alpha = \frac{m - \zeta_a n}{1 - \zeta_a} = n + \frac{m - n}{1 - \zeta_a}.$$

Kadangi $\alpha \in \mathbb{R}$, tai ir $\zeta_a \in \mathbb{R}$. Vadinasi, $\zeta_a = -1$. Tuomet $\alpha = n + \frac{m-n}{2}$ ir $2\alpha = m + n \in \mathbb{Z}$. Prieštara. Todėl skaičiai $m - \alpha$ ir $n - \alpha$ nėra multiplikatyviai priklausomi. □

Jei α – realusis algebrinis skaičius, kuris nėra sveikasis algebrinis skaičius ir $2\alpha \in \mathbb{Z}$, tai $\alpha = \frac{2k+1}{2}$, kur $k \in \mathbb{Z}$. Galime išnagrinėti ir šį atvejį.

10 pastaba. *Tegul $\alpha = \frac{2k+1}{2}$, kur $k \in \mathbb{Z}$. Skaičiai $m - \alpha$ ir $n - \alpha$, kur $m, n \in \mathbb{Z}$, $m \neq n$, yra multiplikatyviai priklausomi tada ir tik tada, kai $m + n = 2\alpha$.*

Įrodymas. Pirmiausia parodysime, kad lygybė $(m - \alpha)^a = (n - \alpha)^b$ gali būti teisinga tik tuomet, kai $a = b$. Tikrai,

$$\left(m - \frac{2k+1}{2}\right)^a = \left(n - \frac{2k+1}{2}\right)^b \iff (2m - 2k - 1)^a = 2^{a-b} \cdot (2n - 2k - 1)^b.$$

Pastebėkime, kad kairėje paskutiniosios lygybės pusėje visada turėsime nelyginį skaičių, tačiau dešinėje nelyginį skaičių gausime tik tuo-

met, kai $a = b$. Vadinasi,

$$(m-\alpha)^a = (n-\alpha)^a \iff m-\alpha = |n-\alpha|$$

Iš čia gauname, kad

$$m-\alpha = -(n-\alpha) \implies m = 2\alpha - n \text{ arba } n = 2\alpha - m.$$

□

Kitaip tariant, su bet kokiais $k, m \in \mathbb{Z}$ skaičiai $m - \frac{2k+1}{2}$ ir $\frac{2k+1}{2} - m$ yra multiplikatyviai priklausomi.

Kyla klausimas, o kokia situacija, jeigu α – sveikasis algebrinis skaičius? Pirmiausia natūralu galvoti apie kvadratinius algebrinius skaičius, tačiau ir pačiu paprasčiausiu atveju, kai $\alpha = \sqrt{k}$, kur $k \in \mathbb{N}$ ir $\sqrt{k} \notin \mathbb{N}$, susiduriame su sunkumais. Galime išpešti tik gana trivialų rezultatą:

11 teiginys. *Skaičiai $k-\sqrt{k^2 \pm 1}$ ir $-k-\sqrt{k^2 \pm 1}$ yra multiplikatyviai priklausomi su visais $k \in \mathbb{N}$.*

Įrodymas.

$$(-k-\sqrt{k^2 \pm 1})^{-2} = \Big(\frac{1}{k+\sqrt{k^2 \pm 1}}\Big)^2 =$$

$$= \Big(\frac{k-\sqrt{k^2 \pm 1}}{(k+\sqrt{k^2 \pm 1})(k-\sqrt{k^2 \pm 1})}\Big)^2 = \Big(\frac{k-\sqrt{k^2 \pm 1}}{k^2-(k^2 \pm 1)}\Big)^2 = (k-\sqrt{k^2 \pm 1})^2.$$

□

12 hipotezė. *Tegul $\alpha = \sqrt{k}$, kur $k \in \mathbb{N} \setminus \{l^2, l^2 \pm 1 : l \in \mathbb{N}\}$. Tuomet skaičiai $m-\alpha$ ir $n-\alpha$ yra multiplikatyviai nepriklausomi su visais $m, n \in \mathbb{Z}$, $m \neq n$.*

Skaičiams m, n leidus įgyti sveikąsias reikšmes iš intervalo $[-50, 50]$ ir skaičiams a, b atitinkamai sveikąsias reikšmes iš intervalo $[-5, 5]$ kompiuterio pagalba pavyko patikrinti, kad lygybė

$$(m-\alpha)^a = (n-\alpha)^b$$

negalioja su visais $k \in [1, 500] \setminus \{l^2, l^2 \pm 1 : l \in \mathbb{N}\}$. Sekant 5 teoremos įrodymo idėjomis, bent dalinio uždavinio sprendimą galėtume suvesti į Diofantinės lygties

$$X^2 - D = Y^n,$$

kur $X, Y, n, D \in \mathbb{N}$ sprendinių paiešką. Tokios lygtys, kuomet $X, Y, n \in \mathbb{N}, DBD(X, Y) = 1, n > 2, D \in \mathbb{Z}$, mokslinėje literatūroje dar vadinamos apibendrintosiomis Lebesgue-Nagell tipo lygtimis. Šiek tiek daugiau pasistūmėta nagrinėjant atvejus, kai $D < 0$, tačiau, jei $D > 0$,

kaip ir mūsų hipotezės atveju, žinoma gerokai mažiau. Apie gautus rezultatus, sprendžiant tokio tipo lygtis, daugiau sužinoti galima [8] straipsnyje. Pavyzdžiui, iki šiol nėra žinoma, ar lygtis

$$X^2 - 2 = Y^n,$$

kur $X, Y, n \in \mathbb{N}, DBD(X, Y) = 1, n > 2$ turi bent vieną sprendinį. Todėl vargu, ar eidami šiuo keliu, įrodytume net ir atskirus mūsų hipotezės atvejus.

Toliau, pasinaudodami 4 teoremos įrodymo idėja, sukonstruosime be galo daug tokių sveikųjų algebrinių skaičių γ ir natūraliųjų skaičių m, n, su kuriais skaičiai $m-\gamma$, $n-\gamma$ būtų multiplikatyviai nepriklausomi.

13 teiginys. *Tegul $\alpha > \beta \in \mathbb{N}$ – bekvadračiai. Tuomet skaičiai $m - (\sqrt{\alpha} + \sqrt{\beta})$ ir $n - (\sqrt{\alpha} + \sqrt{\beta})$ yra multiplikatyviai nepriklausomi su visais natūraliaisiais $m > n > \sqrt{\alpha} + \sqrt{\beta}$.*

Įrodymas. Tarkime priešingai, jog egzistuoja tokie skaičiai $a, b \in \mathbb{Z}$, kur $a \neq 0$ arba $b \neq 0$ ir natūralieji skaičiai $m > n > \sqrt{\alpha} + \sqrt{\beta}$, kad

$$(m - (\sqrt{\alpha} + \sqrt{\beta}))^a = (n - (\sqrt{\alpha} + \sqrt{\beta}))^b. \tag{3.2}$$

Nemažindami bendrumo galime laikyti, kad $a \geqslant 0$. Gerai žinoma, kad skaičiaus $\sqrt{\alpha} + \sqrt{\beta}$ algebriniai jungtiniai skaičiai virš $\mathbb{Q}$ yra

$$\pm\sqrt{\alpha} \pm \sqrt{\beta}.$$

Imkime skaičių kūno $K = \mathbb{Q}(\sqrt{\alpha} + \sqrt{\beta})$ $\mathbb{Q}$-homomorfizmą f, kuris skaičių $\sqrt{\alpha} + \sqrt{\beta}$ atvaizduoja į skaičių $\sqrt{\alpha} - \sqrt{\beta}$, t.y.

$$f(\sqrt{\alpha} + \sqrt{\beta}) = \sqrt{\alpha} - \sqrt{\beta}.$$

Šiuo $\mathbb{Q}$-homomorfizmu paveikę abi (3.2) lygybės puses gausime

$$(m - (\sqrt{\alpha} - \sqrt{\beta}))^a = (n - (\sqrt{\alpha} - \sqrt{\beta}))^b. \tag{3.3}$$

Sudauginę (3.2) ir (3.3) lygybes turėsime

$$(m^2 - 2m\sqrt{\alpha} + (\alpha - \beta))^a = (n^2 - 2n\sqrt{\alpha} + (\alpha - \beta))^b. \tag{3.4}$$

Skaičiaus $\sqrt{\alpha}$ minimalusis polinomas virš $\mathbb{Q}$ yra $p(x) = x^2 - \alpha$, todėl $\sqrt{\alpha}$ algebriniai jungtiniai skaičiai virš $\mathbb{Q}$ yra $\pm\sqrt{\alpha}$. Vadinasi, galime paimti skaičių kūno $L = \mathbb{Q}(\sqrt{\alpha})$ $\mathbb{Q}$-homomorfizmą g, kuris skaičių $\sqrt{\alpha}$

atvaizduotų į skaičių $-\sqrt{\alpha}$, t.y.

$$g(\sqrt{\alpha}) = -\sqrt{\alpha}.$$

Šiuo $\mathbb{Q}$-homomorfizmu paveikę abi (3.4) lygybės puses gausime dar vieną lygybę

$$(m^2 + 2m\sqrt{\alpha} + (\alpha - \beta))^a = (n^2 + 2n\sqrt{\alpha} + (\alpha - \beta))^b. \tag{3.5}$$

Patogumo dėlei (3.4) ir (3.5) lygybes apjunkime

$$(m^2 \pm 2m\sqrt{\alpha} + (\alpha - \beta))^a = (n^2 \pm 2n\sqrt{\alpha} + (\alpha - \beta))^b. \tag{3.6}$$

Pirmiausia įrodysime, kad $a > 0$. Tikrai, jei $a = 0$ ir $b \neq 0$, tuomet skaičiai $n^2 \pm 2n\sqrt{\alpha} + (\alpha - \beta)$ yra šaknys iš vieneto. Kadangi $n^2 \pm 2n\sqrt{\alpha} + (\alpha - \beta) \in \mathbb{R}$, tai $n^2 \pm 2n\sqrt{\alpha} + (\alpha - \beta) = \pm 1$. Tačiau tuomet

$$\sqrt{\alpha} = \frac{\pm 1 - \alpha + \beta - n^2}{\pm 2n} \in \mathbb{Q}$$

ir gauname prieštarą. Visiškai analogiškai galėtume parodyti, kad $b \neq 0$, tačiau tai įrodysime kitu būdu, kurio naudą pamatysime šiek tiek vėliau.

Taigi, jei $b = 0$ ir $a \neq 0$, tuomet skaičiai $m^2 \pm 2m\sqrt{\alpha} + (\alpha - \beta)$ yra šaknys iš vieneto. Kadangi $m^2 \pm 2m\sqrt{\alpha} + (\alpha - \beta) \in \mathbb{R}$, tai $m^2 \pm 2m\sqrt{\alpha} + (\alpha - \beta) = \pm 1$. Tačiau,

$$\begin{aligned} m^2 \pm 2m\sqrt{\alpha} + (\alpha - \beta) &\geqslant m^2 - 2m\sqrt{\alpha} + \alpha - \beta = \\ &= (m - \sqrt{\alpha})^2 - \beta \geqslant (n + 1 - \sqrt{\alpha})^2 - \beta > \\ &> (\sqrt{\alpha} + \sqrt{\beta} + 1 - \sqrt{\alpha})^2 - \beta = \\ &= (\sqrt{\beta} + 1)^2 - \beta = 2\sqrt{\beta} + 1 > 1. \end{aligned}$$

Toliau svarbu pastebėti, kad

$$m^2 - mx + (\alpha - \beta) > n^2 - nx + (\alpha - \beta) > 0,$$

su kiekvienu $x \in (-\infty, 2\sqrt{\alpha}]$. Pirmiausia įrodysime pirmąją nelygybę, iš tikrųjų

$$\begin{gathered} m^2 - mx + (\alpha - \beta) > n^2 - nx + (\alpha - \beta) \\ m^2 - mx > n^2 - nx \\ m^2 - n^2 > (m - n)x \\ m + n > x. \end{gathered}$$

Pastaroji nelygybė teisinga, nes

$$m+n > 2\sqrt{\alpha}+2\sqrt{\beta} \geqslant 2\sqrt{\alpha}+2\sqrt{2} > x.$$

Kita vertus,

$$\begin{aligned} n^2-nx+\alpha-\beta &\geqslant n^2-2\sqrt{\alpha}n+\alpha-\beta = \\ &= (n-\sqrt{\alpha})^2-\beta > (\sqrt{\alpha}+\sqrt{\beta}-\sqrt{\alpha})^2-\beta = 0. \end{aligned}$$

Taigi, kadangi $m^2-mx+(\alpha-\beta) > n^2-nx+(\alpha-\beta) > 0$, tai intervale $(-\infty, 2\sqrt{\alpha}]$ galime apibrėžti funkciją

$$f(x) := a\log(m^2-mx+(\alpha-\beta)) - b\log(n^2-nx+(\alpha-\beta)).$$

Iš (3.6) lygybės žinome, kad ši funkcija turi bent du nulius $x_1 = -2\sqrt{\alpha}$ ir $x_2 = 2\sqrt{\alpha}$. Pasinaudoję Rolio teorema gauname, kad funkcijos f išvestinė

$$f'(x) := -\frac{am}{m^2-mx+(\alpha-\beta)} + \frac{bn}{n^2-nx+(\alpha-\beta)}$$

privalo turėti realiąją šaknį $\gamma \in (-2\sqrt{\alpha}, 2\sqrt{\alpha}) \subset (-\infty, 2\sqrt{\alpha}]$. Todėl iš $f'(\gamma) = 0$ nesunkiai randame, kad

$$a(n+(\alpha-\beta)/n-\gamma) = b(m+(\alpha-\beta)/m-\gamma). \tag{3.7}$$

Pastebėkime, kad $m+(\alpha-\beta)/m-\gamma > n+(\alpha-\beta)/n-\gamma > 0$. Tikrai, pirmiausia įrodykime pirmąją nelygybe. Užsirašykime $m = n+k$, kur $k \in \mathbb{N}$ ir skaičiuokime

$$m+\frac{\alpha-\beta}{m}-\gamma > n+\frac{\alpha-\beta}{n}-\gamma \tag{3.8}$$

$$k+\frac{\alpha-\beta}{n+k} > \frac{\alpha-\beta}{n}$$

$$\frac{nk+k^2+\alpha-\beta}{n+k} > \frac{\alpha-\beta}{n}$$

$$n^2k+nk^2+\alpha n-\beta n > \alpha n+\alpha k-\beta n-\beta k$$

$$n(n+k) > \alpha-\beta.$$

Pastaroji nelygybė teisinga, nes

$$n(n+k) > n^2 \geqslant (\sqrt{\alpha}+\sqrt{\beta})^2 > \alpha+\beta > \alpha-\beta.$$

Taigi liko parodyti, kad $n + (\alpha - \beta)/n - \gamma > 0$. Ši nelygybė būtų teisinga, jei sugebėtume įrodyti, kad $n + (\alpha - \beta)/n - 2\sqrt{\alpha} > 0$. Tačiau padauginus abi šios nelygybės puses iš n gautume nelygybę, kurią jau išnagrinėjome

$$n^2 - 2\sqrt{\alpha}n + (\alpha - \beta) > 0,$$

ji teisinga su visais $n > \sqrt{\alpha} + \sqrt{\beta}$. Taigi turime, kad

$$n + (\alpha - \beta)/n - \gamma > 0$$

ir anksčiau parodėme, kad $a > 0$, todėl kairioji (3.7) lygybės pusė yra teigiama. Vadinasi, dešinioji (3.7) lygybės pusė taip pat teigiama. Jau įsitikinome, kad $m + (\alpha - \beta)/m - \gamma > 0$, todėl gauname, jog $b > 0$. Taigi, kadangi $b \geqslant 1$ ir kairioji (3.6) lygybės pusė didesnė už vienetą, t.y. $(m^2 \pm 2m\sqrt{\alpha} + (\alpha - \beta))^a > 1$, tai gauname, kad $n^2 \pm 2n\sqrt{\alpha} + (\alpha - \beta) > 1$. Galiausiai, kadangi

$$m^2 \pm 2m\sqrt{\alpha} + (\alpha - \beta) > n^2 \pm 2n\sqrt{\alpha} + (\alpha - \beta) > 1$$

ir $a, b \geqslant 1$, tai iš (3.6) lygybės išvedame, kad $a < b$. Kita vertus, iš (3.7) ir (3.8) lygybių išplaukia $a > b$. Prieštara. Vadinasi, skaičiai $m - (\sqrt{\alpha} + \sqrt{\beta})$ ir $n - (\sqrt{\alpha} + \sqrt{\beta})$ yra multiplikatyviai nepriklausomi. □

14 išvada. *Tegul $\alpha > \beta \in \mathbb{N}$ – bekvadračiai ir $\gamma = \pm\sqrt{\alpha} \pm \sqrt{\beta}$. Tuomet skaičiai $m - \gamma$ ir $n - \gamma$ yra multiplikatyviai nepriklausomi su visais natūraliaisiais $m > n > \sqrt{\alpha} + \sqrt{\beta}$.*

Įrodymas. Atvejį $\gamma = \sqrt{\alpha} + \sqrt{\beta}$ jau įrodėme 13 teiginyje, todėl laikykime, kad $\gamma \neq \sqrt{\alpha} + \sqrt{\beta}$. Tarkime priešingai, jog egzistuoja tokie skaičiai $a, b \in \mathbb{Z}$ ir $m > n > \sqrt{\alpha} + \sqrt{\beta}$, kad būtų teisinga lygybė

$$(m - \gamma)^a = (n - \gamma)^b, \tag{3.9}$$

kur $a \neq 0$ arba $b \neq 0$. Imkime skaičių kūno $K = \mathbb{Q}(\gamma)$ $\mathbb{Q}$-homomorfizmą f, kuris skaičių γ atvaizduoja į skaičių $\sqrt{\alpha} + \sqrt{\beta}$, t.y.

$$f(\gamma) = \sqrt{\alpha} + \sqrt{\beta}.$$

Šiuo $\mathbb{Q}$-homomorfizmu paveikę abi (3.9) lygybės puses gausime

$$(m - (\sqrt{\alpha} + \sqrt{\beta}))^a = (n - (\sqrt{\alpha} + \sqrt{\beta}))^b. \tag{3.10}$$

Tačiau ši lygybė prieštarauja 13 teiginio tvirtinimui. □

Summary

Definition 1. Any two nonzero numbers $z_1, z_2 \in \mathbb{C}^* = \mathbb{C} \setminus \{0\}$ are called *multiplicatively dependent* if there exist $a, b \in \mathbb{Z}$, not both zero, such that

$$z_1^a z_2^b = 1,$$

and *multiplicatively independent* otherwise.

For each $k \in \mathbb{N}$ denote by $\zeta_k := e^{\frac{2\pi i}{k}}$ the primitive kth root of unity. Madritsch and Ziegler [1], [2] raised the following conjecture:

Conjecture 2 ([1, 1.4 Question], [2, 2.8 Conjecture])**.** For any $k \geqslant 3$ and any positive integers $m > n$ the numbers $m - \zeta_k, n - \zeta_k$ are multiplicatively independent except when $(n, k) = (1, 6)$.

It is easy to check that in the exceptional case $(n, k) = (1, 6)$, the number $n - \zeta_k = 1 - \zeta_6 = \zeta_6^{-1}$ is a root of unity, so that the numbers $m - \zeta_6, 1 - \zeta_6$ are multiplicatively dependent for every $m \in \mathbb{C}$.

Hansel and Safer [3] have considered the case $k = 4$ with application to the multiplicative independence of the bases of $\mathbb{Z}[\zeta_k]$ of the form $-m + \zeta_k$. The case when k is a power of some small prime has also been settled in [1].

It is worth mentioning that in [1], [2] conjecture was settled for $0 < m - n < 10^6$ and also for any $m > n > C(k)$, where $C(k)$ is a positive constant depending on k only. The constant $C(k)$ comes from the paper of Schinzel and Tijdeman [4], but it seems to be not effective enough to help solve the conjecture.

P. Drungilas and A. Dubickas [5] proved Madritsch and Ziegler conjecture 2 using an entirely different and more straightforward approach.

The main focus of this thesis lies in the multiplicative dependence of two integers shifted by an algebraic number. A particular motivation for this topic comes from the paper of P. Drungilas and A. Dubickas [5]. We looked into the main ideas of the proof of the above-mentioned conjecture 2 and discussed some other important results. We succeeded to prove that for any algebraic number α which is not an algebraic integer and $2\alpha \notin \mathbb{Z}$, the numbers $m - \alpha$, $n - \alpha$ are multiplicatively independent for every $m, n \in \mathbb{Z}$, $m \neq n$. In particular, we also settled the case when $2\alpha \in \mathbb{Z}$.

It was natural to consider the same problem when α is an algebraic integer. We looked into the class of $\alpha = \sqrt{k}$, where $k \in \mathbb{N}$, $\sqrt{k} \notin \mathbb{N}$ and formulated a conjecture based on empirical evidence. We also showed that the numbers $k - \sqrt{k^2 \pm 1}$ and $-k - \sqrt{k^2 \pm 1}$ are multiplicatively dependent for every $k \in \mathbb{N}$. Finally, we found an infinite class of algebraic integers $\gamma := \pm\sqrt{\alpha} \pm \sqrt{\beta}$, where $\alpha > \beta \in \mathbb{N}$ - squarefree and infinitely many positive integers $m > n > \sqrt{\alpha} + \sqrt{\beta}$ such that the numbers $m - \gamma, n - \gamma$ are multiplicatively independent.

Literatūra

[1] M. G. Madritsch, V. Ziegler, *An infinite family of multiplicatively independent bases of number systems in cyclotomic number fields*, Acta Sci. Math. (Szeged) **81** (2015), no. 1-2, 33–44.

[2] M. G. Madritsch, V. Ziegler, *On multiplicatively independent bases in cyclotomic number fields*, Acta Math. Hungar. **146** (2015), no. 1, 224–239.

[3] G. Hansel, T. Safer, *Vers un théorème de Cobham pour les entiers de Gauss*, Bull. Belg. Math. Soc. Simon Stevin **10** (2003), no. suppl., 723–735.

[4] A. Schinzel, R. Tijdeman, *On the equation $y^m = P(x)$*, Acta Arith. **31** (1976), no. 2, 199–204.

[5] P. Drungilas, A. Dubickas, *Multiplicative dependence of two integers shifted by a root of unity*, Proc. Amer. Math. Soc. **147** (2019), no. 2, 505-511.

[6] T. Nagell, *Des équations indéterminées*, Nordsk. Mat. Forenings Skr. **2** (1920), 14 pp.

[7] P. Drungilas, A. Dubickas, *Multiplicative dependence of shifted algebraic numbers*, Colloq. Math. **96** (2003), no. 1, 75-81.

[8] M. Le, G. Soydan, *A brief survey on the generalized Lebesgue-Ramanujan-Nagell equation*, eprint arXiv:2001.09617 (2020).