VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
MATEMATIKOS MAGISTRANTŪROS STUDIJŲ PROGRAMA

Lagražo keturių kvadratų teorema

Lagrange's four-square theorem

Baigiamasis magistro darbas

Atliko: Gabrielė Stankevičiūtė

VU el. p.: gabriele.stankeviciute@mif.stud.vu.lt

Vadovas: Paulius Drungilas

Vilnius
2022

Turinys

Įvadas

Lagranžo keturių kvadratų teorema teigia, kad kiekvieną natūralųjį skaičių galima išreikšti keturių sveikųjų skaičių kvadratų suma. Pavyzdžiui, $3 = 1^2 + 1^2 + 1^2 + 0^2$, $15 = 3^2 + 2^2 + 1^2 + 1^2$.

Šios teoremos įrodymai dažniausiai remiasi tuo, kad jei du skaičiai išreiškiami keturių sveikųjų skaičių kvadratų suma, tai jų sandauga taip pat išreiškiama keturių sveikųjų skaičių kvadratų suma (žr. (2.1) tapatybę). Tai vadinamoji multiplikatyvumo savybė. Iš jos išplaukia, kad Lagranžo teoremą pakanka įrodyti pirminiams skaičiams.

Klasikinis Lagranžo teoremos įrodymas pirminiam skaičiui p sudarytas iš tokių dalių:

1) įrodoma, kad egzistuoja tokie sveikieji skaičiai x, y ir m, jog $1 + x^2 + y^2 = mp$;

2) iš 1) išplaukia, kad egzistuoja tokie sveikieji skaičiai m, x_1, x_2, x_3 ir x_4, jog $x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp$;

3) įrodoma, kad 2) dalies išraiškoje mažiausia įmanoma teigiama m reikšmė yra $m = 1$.

Antras plačiai paplitęs įrodymo būdas yra naudojant kvaternijonus – pavidalo

$$\alpha = a_0 + a_1 i + a_2 j + a_3 k \tag{1}$$

skaičius, kur a_0, a_1, a_2 ir a_3 yra realieji skaičiai, dar vadinami kvaternijono α koordinatėmis, o elementai i, j, k yra susieti lygybėmis $i^2 = j^2 = k^2 = ijk = -1$. Skaičius $a_0^2 + a_1^2 + a_2^2 + a_3^2$ vadinamas (1) kvaternijono norma ir žymimas $N(\alpha)$.

Dar vienas Lagranžo teoremos įrodymas pagrįstas Hurvico skaičiais – (1) kvaternijonais, kurių visos koordinatės a_t yra sveikieji skaičiai arba visos koordinatės priklauso aibei $\mathbb{Z}+\frac{1}{2}$.

Šiame darbe taip pat yra pateikta ir keletas Lagranžo keturių kvadratų teoremos apibendrinimų, paminėta viena hipotezė ir keletas pavyzdžių. Be to, suformuluota teorema apie natūraliojo skaičiaus išraiškų keturių sveikųjų skaičių kvadratų suma skaičių.

skyrius 1

Pagalbiniai rezultatai

1 Apibrėžimas. *([1]) Sveikasis skaičius d vadinamas sveikųjų skaičių a_1, a_2, ..., a_n didžiausiu bendruoju dalikliu (dbd), jei*

1) $d \mid a_1$, $d \mid a_2$, ..., $d \mid a_n$;

2) jei $d^* \mid a_1$, $d^* \mid a_2$, ..., $d^* \mid a_n$, *tai* $d^* \mid d$.

2 Teorema (Dalybos su liekana formulė)**.** *([1]) Bet kuriems* a_1, $a_2 \in \mathbb{Z}$, $a_2 > 0$, *egzistuoja tokie vieninteliai skaičiai* x, $y \in \mathbb{Z}$, $0 \leq y < a_2$, *kad* $a_1 = a_2 x + y$.

Įrodymas. Kadangi $a_2 > 0$, tai egzistuoja toks $x \in \mathbb{Z}$, kad

$$a_2 x \leq a_1 < a_2 (x + 1).$$

Pažymėkime $y =: a_1 - a_2 x$. Akivaizdu, kad $0 \leq y < a_2$ ir $a_1 = a_2 x + y$. Jei egzistuotų kitokia tokia skaičių pora x^*, $y^* \in \mathbb{Z}$, kad $a_1 = a_2 x^* + y^*$, tai gautume lygybę

$$a_2 x^* + y^* = a_2 x + y.$$

Pertvarkę šią lygybę, gautume: $a_2 (x^* - x) = y^* - y$. Vadinasi būtų teisinga lygybė $a_2 |x^2 - x| = |y^* - y|$. Bet $0 \leq |y^* - y| < a_2$. Taigi $x^* = x$, $y^* = y$. □

3 Teiginys (Euklido algoritmas)**.** ([1]) Tarkime, a_1, a_2 - sveikieji skaičiai, $a_2 > 0$. Keletą kartų pasinaudoję dalybos su liekana formule (2 teorema), gauname:

$$\begin{aligned}
a_1 &= a_2x_2 + a_3, & 0 \le a_3 < a_2,\\
a_2 &= a_3x_3 + a_4, & 0 \le a_4 < a_3,\\
&\vdots & \vdots\\
a_{k-3} &= a_{k-2}x_{k-2} + a_{k-1}, & 0 \le a_{k-1} < a_{k-2},\\
a_{k-2} &= a_{k-1}x_{k-1} + a_k, & 0 \le a_k < a_{k-1},\\
a_{k-1} &= a_kx_k + 0.
\end{aligned}$$

Šių lygybių seka ir sudaro *Euklido algoritmo* esmę.

Įrodysime, kad paskutinė nelygi nuliui liekana a_k yra skaičių a_1 ir a_2 didžiausias bendras daliklis. Tam reikia įrodyti, kad

1) $a_k \mid a_1$, $a_k \mid a_2$;

2) jei $d^* \mid a_1$, $d^* \mid a_2$, tai $d^* \mid a_k$.

Iš paskutinės Euklido algoritmo lygybės matome, kad $a_k \mid a_{k-1}$, iš priešpaskutinės $a_k \mid a_{k-2}$ ir t.t. Taigi $a_k \mid a_1$, $a_k \mid a_2$.

Lieka įsitikinti, kad a_k tenkina ir antrąją didžiausio bendrojo daliklio apibrėžimo savybę. Sakykime, $d^* \mid a_1$, $d^* \mid a_2$. Iš pirmosios Euklido algoritmo lygybės matome, kad $d^* \mid a_3$, ir antrosios $d^* \mid a_4$ ir t.t. Taigi galų gale gauname $d^* \mid a_k$.

4 Teorema. *([1]) Jei d yra skaičių a_1 ir a_2 didžiausias bendras daliklis, tai egzistuoja tokie skaičiai u ir v, kad*

$$d = a_1u + a_2v.$$

Įrodymas. Pritaikę skaičiams a_1 ir a_2 Euklido algoritmą (3 teiginys), tarkime, gauname $d = a_k$. Remdamiesi anksčiau parašytomis lygybėmis, gauname:

$$d = a_k = a_{k-2} - a_{k-1}x_{k-1} = a_{k-2} - (a_{k-3} - a_{k-2}x_{k-2})\,x_{k-1} =$$

$$= -a_{k-3}x_{k-1} + a_{k_2}\left(1 + x_{k-1}x_{k-2}\right) = \ldots = a_1 u + a_2 v.$$

□

5 Teorema. *([2]) Tarkime p yra nelyginis pirminis skaičius. Egzistuoja tokie sveikieji skaičiai x, y ir m, kad*

$$1 + x^2 + y^2 = mp$$

ir $0 < m < p$.

Įrodymas. Skaičiai

$$x^2 \ \left(0 \leq x \leq \frac{1}{2}\left(p-1\right)\right), \tag{1.1}$$

kurių iš viso yra $\frac{1}{2}\left(p+1\right)$, nelygsta tarpusavyje moduliu p (t.y. dalybos iš p liekana visiems šiems skaičiams skiriasi), kaip ir skaičiai

$$-1 - y^2 \ \left(0 \leq y \leq \frac{1}{2}\left(p-1\right)\right), \tag{1.2}$$

kurių taip pat iš viso yra $\frac{1}{2}\left(p+1\right)$. Tačiau iš viso yra $p+1$ skaičių x^2 ir $-1-y^2$, bet tik p galimų dalybos iš p liekanų. Vadinasi, kažkuris skaičius iš (1.1) turi lygsti kažkuriam skaičiui iš (1.2) moduliu p, t. y. abiejų liekana bus ta pati. Vadinasi egzistuoja tokie skaičiai x ir y, abu mažesni už $\frac{1}{2}p$, kad

$$x^2 \equiv -1 - y^2 \pmod{p}.$$

Iš čia gauname, kad egzistuoja toks natūralusis skaičius m, kad $1 + x^2 + y^2 = mp$. Be to,

$$0 < 1 + x^2 + y^2 < 1 + 2\left(\frac{1}{2}p\right)^2 < p^2,$$

todėl $m < p$. □

skyrius 2

Lagranžo keturių kvadratų teorema

Lagranžo keturių kvadratų teorema teigia, kad kiekvienas teigiamas sveikasis skaičius yra sudarytas iš keturių kvadratų, t.y. bet kokiam teigiamam sveikam skaičiui y yra teisinga lygybė

$$y = x_1^2 + x_2^2 + x_3^2 + x_4^2,$$

kur x_i, $i = 1, 2, 3, 4$, yra sveikieji skaičiai.

2.1 Klasikinis įrodymas pagal G. H. Hardy ir E. M. Wright knygą

Bet kuriems skaičiams x_1, x_2, x_3 ir x_4 teisinga lygybė (žr. [2]):

$$\begin{aligned}\left(x_1^2 + x_2^2 + x_3^2 + x_4^2\right)\left(y_1^2 + y_2^2 + y_3^2 + y_4^2\right) &= \left(x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4\right)^2 \\ &+ \left(x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3\right)^2 \\ &+ \left(x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4\right)^2 \\ &+ \left(x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2\right)^2.\end{aligned} \tag{2.1}$$

Tegul $\mathcal{N}$ – aibė natūraliųjų skaičių, kuriuos galima išreikšti keturių sveikųjų skaičių kvadratų suma. Pavyzdžiui, kadangi $1 = 1^2 + 0^2 + 0^2 + 0^2$ ir $2 = 1^2 + 1^2 + 0^2 + 0^2$, tai $1 \in \mathcal{N}$ ir $2 \in \mathcal{N}$. Iš (2.1) tapatybės išplaukia, kad aibė $\mathcal{N}$ yra multiplikatyvi, t. y. jei $a, b \in \mathcal{N}$,

tai ir $a \cdot b \in \mathcal{N}$. Lagranžo keturių kvadratų teorema tvirtina, kad aibė $\mathcal{N}$ sutampa su visų natūraliųjų skaičių aibe $\mathbb{N}$. Remiantis pagrindine aritmetikos teorema, kiekvieną natūralųjį skaičių, didesnį už 1, galima išreikšti pirminių skaičių sandauga. Vadinasi, norint įrodyti Lagranžo keturių kvadratų teoremą, užtenka parodyti, kad visi pirminiai skaičiai priklauso aibei $\mathcal{N}$. Kadangi $2 \in \mathcal{N}$ $(2 = 1^2 + 1^2 + 0^2 + 0^2)$, tai užtenka nagrinėti nelyginius pirminius skaičius.

Tegul p – nelyginis pirminis skaičius. Remiantis 5 teorema, egzistuoja tokie sveikieji skaičiai x, y ir m, kad

$$1 + x^2 + y^2 = mp$$

ir $0 < m < p$. Taigi skaičiaus p kartotinį mp galima išreikšti keturių kvadratų suma:

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2,$$

kur x_1, x_2, x_3 ir x_4 yra sveikieji skaičiai iš kurių bent vienas nesidalija iš p (jei visi dalintųsi iš p, tuomet skaičius mp dalintųsi iš p^2 ir tuomet m dalintųsi iš p; tačiau $0 < m < p$). Įrodysime, kad mažiausias toks kartotinis mp yra pats p.

Tarkime, kad $m_0 p$ yra mažiausiais kartotinis, kuriam teisinga

$$m_0 p = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

Jei $m_0 = 1$, tai įrodymas tuo ir baigiasi. Tarkime $m_0 > 1$. Remiantis 5 teorema, $m_0 < p$.

Jei m_0 yra lyginis skaičius, tuomet suma $x_1^2 + x_2^2 + x_3^2 + x_4^2$ irgi bus lyginis skaičius, ir turime tris galimus atvejus:

1) x_1, x_2, x_3, x_4 visi yra lyginiai skaičiai, arba

2) x_1, x_2, x_3, x_4 visi yra nelyginiai skaičiai, arba

3) du iš šių skaičių yra lyginiai, ir du skaičiai yra nelyginiai.

Neprarandant bendrumo tarkime, kad trečiame variante x_1 ir x_2 yra lyginiai bei x_3 ir x_4 yra nelyginiai skaičiai. Tada visais trimis atvejais skaičiai

$$x_1 + x_2,\ x_1 - x_2,\ x_3 + x_4,\ x_3 - x_4$$

bus lyginiai ir iš tapatybės

$$\frac{1}{2}m_0 p = \left(\frac{x_1+x_2}{2}\right)^2 + \left(\frac{x_1-x_2}{2}\right)^2 + \left(\frac{x_3+x_4}{2}\right)^2 + \left(\frac{x_3-x_4}{2}\right)^2$$

išplaukia, kad skaičiaus p kartotinis $\frac{m_0}{2}p$ yra išreiškiamas keturių sveikų skaičių kvadratų suma. Tačiau $\frac{m_0}{2} < m_0$, o tai prieštarauja skaičiaus m_0 parinkimui. Vadinasi, skaičius m_0 yra nelyginis.

Skaičiai x_1, x_2, x_3 ir x_4 nėra visi dalūs iš m_0, nes priešingu atveju gautume, kad $m_0^2 \mid m_0 p$ ir $m_0 \mid p$, kas prieštarauja m_0 parinkimui ($1 < m_0 < p$; p – pirminis). Kadangi m_0 yra nelyginis ir $m_0 > 1$, tai $m_0 \geq 3$.

Parenkame tokius sveikuosius skaičius b_1, b_2, b_3 ir b_4, kad

$$y_i = x_i - b_i m_0 \text{ ir } |y_i| < \frac{1}{2}m_0 \quad (i = 1, 2, 3, 4).$$

Tada

$$0 < y_1^2 + y_2^2 + y_3^2 + y_4^2 < 4\left(\frac{1}{2}m_0\right)^2 = m_0^2$$

ir

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \pmod{m_0}.$$

Iš to seka, kad

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = m_0 p \ (m_0 < p),$$
$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = m_0 m_1 \ (0 < m_0 < m_1).$$

Šiems skaičiams pritaikę (2.1) tapatybę, gauname

$$m_0^2 m_1 p = z_1^2 + z_2^2 + z_3^2 + z_4^2. \tag{2.2}$$

Kita vertus,

$$z_1 = \sum_{i=1}^{4} x_i y_i = \sum_{i=1}^{4} x_i (x_i - b_i m_0) \equiv \sum_{i=1}^{4} x_i^2 \equiv 0 \pmod{m_0}.$$

Panašiai gaunama, kad skaičiai z_2, z_3 ir z_4 taip pat dalijasi iš m_0. Pažymėję

$$z_i = m_0 t_i, \ t_i \in \mathbb{Z}, (i = 1, 2, 3, 4)$$

ir šias išraiškas įstatę į (2.2) lygybę, gauname

$$m_1 p = t_1^2 + t_2^2 + t_3^2 + t_4^2.$$

Tačiau $m_1 < m_0$, o tai prieštarauja skaičiaus m_0 parinkimui. Iš to išplaukia, kad $m_0 = 1$.

2.2 Klasikinis įrodymas pagal K. Ireland ir M. Rosen knygą

Pateiksime dar vieną klasikinį įrodymą pagal Kenneth Ireland ir Michael Rosen knygą [3]. Lagranžo keturių kvadratų teorema išplaukia iš 5 teoremos ir tokios teoremos:

6 Teorema. *([3]) Tarkime, kad pirminiam skaičiui p egzistuoja toks natūralusis skaičius m, $1 < m < p$, kad skaičių mp galima išreikšti keturių sveikųjų skaičių kvadratų suma. Tada egzistuoja toks natūralusis skaičius $r < m$, kad skaičių rp galima išreikšti keturių sveikųjų skaičių kvadratų suma.*

Įrodymas. Egzistuoja toks natūralusis skaičius m, $1 < m < p$, ir tokie sveikieji skaičiai x_1, x_2, x_3 ir x_4, kad

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2. \tag{2.3}$$

Parenkame tokius sveikuosius skaičius y_1, y_2, y_3 ir y_4, kad $x_i \equiv y_i \pmod{m}$, $i = 1, 2, 3, 4$, ir $-\frac{m}{2} \leq y_i \leq \frac{m}{2}$. Tada

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \pmod{m},$$

ir egzistuoja toks sveikasis skaičius $r \geq 0$, kad

$$mr = y_1^2 + y_2^2 + y_3^2 + y_4^2. \tag{2.4}$$

Be to,

$$mr \leq \frac{m^2}{4} + \frac{m^2}{4} + \frac{m^2}{4} + \frac{m^2}{4} = m^2.$$

Todėl $r \leq m$.

Matome, kad $r \neq 0$, nes priešingu atveju $y_i = 0$, $i = 1, 2, 3, 4$, ir iš (2.3) išplauktų, kad $m \mid p$, o tai prieštarauja sąlygai $1 < m < p$. Kita vertus, $r \neq m$, nes priešingu atveju gautume $y_i = \frac{m}{2}$, $x_i^2 \equiv \frac{m^2}{4} \pmod{m^2}$ ir iš (2.3) išplauktų, kad $mp = m^2 \pmod{m^2}$, t. y. $m \mid p$, o tai prieštarauja sąlygai $1 < m < p$.

(2.3) ir (2.4) skaičiams pritaikę (2.1) tapatybę, gauname

$$\begin{aligned} m^2 rp = {} & (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\ & + (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2 . \end{aligned} \tag{2.5}$$

Be to, iš sąlygų $x_i \equiv y_i \pmod{m}$, $i = 1, 2, 3, 4$, gauname, kad kiekvienas (2.5) dešinės pusės kvadratas dalijasi iš m^2. Padaliję abi (2.5) puses iš m^2, gauname, kad skaičių rp $(0 < r < m)$ galima išreikšti keturių sveikųjų skaičių kvadratų suma. □

2.3 Įrodymas naudojant kvaternijonus

Lagranžo keturių kvadratų teoremą galima lengvai įrodyti naudojant kvaternijonų teoriją (žr. [2]). Šiame skyriuje paliesime šios teorijos paviršių, susipažinsime su keliomis pagrindinėmis kvaternijonų teorijos sąvokomis ir bendra įrodymo idėja, o sekančiame skyriuje išsiaiškinsime daugiau detalių.

Kvaternijonai yra hyper-kompleksinės sistemos (kompleksinių skaičių aibės praplėtimo) skaičiai, pateikiami forma

$$\alpha = a_0 + a_1 i + a_2 j + a_3 k,$$

kur skaičiai a_0, a_1, a_2, a_3 yra realieji skaičiai, dar vadinami kvaternijono α koordinatėmis, o kompleksiniai skaičiai i, j, k yra šios praplėstios hyper-kompleksinės sistemos charakteristiniai elementai. Du kvaternijonai yra vadinami vienas kitam lygiais, kai jų atitinkamos koordinatės sutampa.

Kvaternijojų sudėtis tenkina tas pačias taisykles kaip ir paprastų realiųjų skaičių sudėtis, tačiau sandauga šiek tiek skiriasi:

$$i^2 = j^2 = k^2 = -1,$$

$$ij = k = -ji,$$

$$jk = i = -kj,$$

$$ki = j = -ik.$$

Dviejų kvaternijonų sandauga $\alpha\overline{\alpha} = \overline{\alpha}\alpha$, kur $\overline{\alpha} = a_0 - a_1 i - a_2 j - a_3 k$ yra kvaternijono α jungtinis skaičius, yra vadinama kvaternijono α norma bei žymima $N(\alpha) = a_0^2 + a_1^2 + a_2^2 + a_3^2$. Taip pat $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$.

Kvaternijoną α vadinsime sveikjuoju, jeigu jo koordinatės a_0, a_1, a_2, a_3

1) visos yra sveikieji skaičiai, arba

2) visos yra nelyginiai sveikieji skaičiai padalinti iš 2.

Kvaternijono α atvirkštiniu skaičiumi vadinamas kvaternijonas

$$\alpha^{-1} = \frac{\overline{\alpha}}{N(\alpha)}, \qquad \alpha\alpha^{-1} = \alpha^{-1}\alpha = 1.$$

Jeigu abu kvaternijonai α ir α^{-1} yra sveikieji, kvanterijonas α yra vadinamas vienetiniu bei žymimas $\alpha = \epsilon$.

Tarkime ϵ yra bet koks koks vienetinis kvaternijonas. Tuomet skaičiai $\epsilon\alpha$ ir $\alpha\epsilon$ yra vadinami kvaternijono α asocijuotais skaičiais, kurie turi tokią pačią normą. Sveikojo kvaternijono asocijuoti skaičiai taip pat yra sveikieji kvaternijonai.

Pereikime prie Lagranžo keturių kvadratų teoremos įrodymo. Jei sakome, kad p yra realusis pirminis skaičius, tai turime, kad $p = \lambda\pi$, $N(\lambda) = N(\pi) = p$. Šis teiginys remiasi teoremomis, kurios teigia, kad

1) integralinis kvaternijonas π yra neredukuojamas tada ir tik tada, kai jo norma $N(\pi)$ yra realusis pirminis skaičius, ir

2) realusis pirminis skaičius p negali būti neredukuojamas kvaternijonas,

kurios nebus įrodytos šiame darbe. Jeigu kvaternijonas π turi koordinates a_0, a_1, a_2, a_3, kurios yra sveikieji skaičiai, tuomet

$$p = N(\pi) = a_0^2 + a_1^2 + a_2^2 + a_3^2,$$

ir tuo teorema yra įrodyta. Jeigu ne, tuomet egzistuoja kvaternijojo π asocijuotas skaičius π^*, kuris turi sveikasias koordinates (taip pat remiantis teorema, kuri nėra įrodyta šiame darbe). Kadangi $p = N(\pi) = N(\pi^*)$, teorema yra įrodyta. Ir tuomet naudodami (2.1) tapatybę bei pagrindinę algebros teoremą gauname Lagranžo keturių kvadratų teoremą teisingą bet kokiam sveikam teigiamam skaičiui.

2.4 Pavyzdys

Išreikškime skaičių 385 keturių kvadratų suma naudodami (2.1) tapatybę. Skaičių 385 galime užrašyti kaip sandaugą

$$385 = 5 \cdot 7 \cdot 11. \tag{2.6}$$

Išreiškus šiuos daugikliuss keturių kvadratų suma gauname

$$\begin{aligned} 5 &= 2^2 + 1^2 + 0^2 + 0^2, \\ 7 &= 2^2 + 1^2 + 1^2 + 1^2, \\ 11 &= 3^2 + 1^2 + 1^2 + 0^2, \end{aligned}$$

ir šias išraiškas įsistatę į (2.6) gauname

$$385 = \left(2^2 + 1^2 + 0^2 + 0^2\right) \cdot \left(2^2 + 1^2 + 1^2 + 1^2\right) \cdot \left(3^2 + 1^2 + 1^2 + 0^2\right). \tag{2.7}$$

Naudodami (2.1) tapatybę sudauginame pirmus 2 skliaustus

$$\begin{aligned} \left(2^2 + 1^2 + 0^2 + 0^2\right) \cdot \left(2^2 + 1^2 + 1^2 + 1^2\right) &= (2 \cdot 2 + 1 \cdot 1 + 0 \cdot 1 + 0 \cdot 1)^2 \\ &+ (2 \cdot 1 - 1 \cdot 2 + 0 \cdot 1 - 0 \cdot 1)^2 \\ &+ (2 \cdot 1 - 0 \cdot 2 + 0 \cdot 1 - 1 \cdot 1)^2 \\ &+ (2 \cdot 1 - 0 \cdot 2 + 1 \cdot 1 - 0 \cdot 1)^2 \\ &= 5^2 + 0^2 + 1^2 + 3^2 \end{aligned}$$

bei gautą rezultatą įsistatome į (2.7):

$$385 = \left(5^2 + 0^2 + 1^2 + 3^2\right) \cdot \left(3^2 + 1^2 + 1^2 + 0^2\right). \tag{2.8}$$

Naudodami (2.1) tapatybę sudauginame likusius skliaustus

$$\begin{aligned}\left(5^2+0^2+1^2+3^2\right)\cdot\left(3^2+1^2+1^2+0^2\right) &= (5\cdot 3+0\cdot 1+1\cdot 1+3\cdot 0)^2\\ &+(5\cdot 1-0\cdot 3+1\cdot 0-3\cdot 1)^2\\ &+(5\cdot 1-1\cdot 3+3\cdot 1-0\cdot 0)^2\\ &+(5\cdot 0-3\cdot 3+0\cdot 1-1\cdot 1)^2\\ &=16^2+2^2+5^2+(-10)^2\end{aligned}$$

ir įsistatę į (2.8) gauname, kad skaičių 385 keturių kvadratų suma galima išreikšti kaip

$$385=16^2+2^2+5^2+10^2.$$

skyrius 3

Hurvico skaičiai

3.1 Apibrėžimas

Paskutinis šiame darbe pateikiamas Lagranžo keturių kvadratų teoremos įrodymas naudoja Hurvico skaičius, kurie sudaro poaibį prieš tai buvusiame skyriuje pristatytų kvaternijonų.

7 Apibrėžimas. *([4]) Hurvico skaičiais yra vadinami kvaternijonai, priklausantys aibei*

$$\left\{a_0 + a_1 i + a_2 j + a_3 k : a_0, a_1, a_2, a_3 \in \mathbb{Z} \;\; arba \;\; a_0, a_1, a_2, a_3 \in \mathbb{Z} + \frac{1}{2}\right\}$$

Taigi kiekvieną Hurvico skaičių galima išreikšti kvaternijonų i, j, k ir $h := \frac{1+i+j+k}{2}$, padaugintų iš sveikųjų skaičių, suma. Todėl Hurvico skaičių aibė sutampa su aibe $\mathbb{Z}[h, i, j, k]$.

Hurvico skaičių aibė yra uždara sumos ir daugybos atžvilgiu (yra nekomutatyvus žiedas).

Aibė

$$\mathbb{Z}[i, j, k] = \{a_0 + a_1 i + a_2 j + a_3 k \;\; : \;\; a_0, a_1, a_2, a_3 \in \mathbb{Z}\}$$

yra Hurvico skaičių aibės poaibis.

Tegul α ir δ – Hurvico skaičiai. Skaičius δ vadinamas skaičiaus α dešiniuoju (atitinkamai kairiuoju) dalikliu, jei egzistuoja toks Hurvico skaičius γ, kad $\alpha = \gamma\delta$ (atitinkamai $\alpha = \delta\gamma$). Jei Hurvico skaičius δ yra Hurvico skaičiaus α kairysis arba dešinysis daliklis, tuomet

sakysime, kad δ yra skaičiaus α daliklis. Nesunku įsitikinti, kad Hurvico skaičius yra kairysis vieneto daliklis tada ir tik tada, kai jis yra ir dešinysis vieneto daliklis. Todėl kairieji ir dešinieji vieneto dalikliai vadinami tiesiog vieneto dalikliais. Nesunku įsitikinti, kad Hurvico skaičius yra vieneto daliklis tada ir tik tada, kai jo norma lygi 1. Iš čia nesunkiai gauname, kad Hurvico skaičių aibėje yra lygiai 24 vieneto dalikliai: 8 skaičiai ± 1, $\pm i$, $\pm j$ ir $\pm k$ priklauso aibei $\mathbb{Z}[i,j,k]$ ir dar 16 skaičių $\pm\frac{1}{2} \pm \frac{i}{2} \pm \frac{j}{2} \pm \frac{k}{2}$.

Hurvico skaičiams teisingas dalybos su liekana teiginys (žr. [4]): bet kuriems Hurvico skaičiams α ir $\beta \neq 0$ egzistuoja tokie Hurvico skaičiai q ir r, kad $\alpha = q\beta + r$ ir $N(r) < N(\beta)$.

8 Apibrėžimas. *([4]) Nenulinis Hurvico skaičius vadinamas redukuojamu, jei jį galima išreikšti dviejų Hurvico skaičių, nei vienas iš kurių nėra vieneto daliklis, sandauga. Hurvico skaičius, kuris nėra vieneto daliklis ir nėra redukuojamas, vadinamas neredukuojamu.*

9 Teiginys (Neredukuojamo Hurvico skaičiaus savybė)**.** ([4]) Jei realusis neredukuojamas Hurvico skaičius π yra Hurvico skaičių α ir β sandaugos $\alpha\beta$ daliklis, tuomet π yra α daliklis arba π yra β daliklis.

3.2 Lagranžo keturių kvadratų teoremos įrodymas naudojant Hurvico skaičius

10 Teorema (Sąlyginė keturių kvadratų teorema)**.** *([4]) Bet kuris pirminis skaičius, kuris nėra Hurvico neredukuojamas skaičius, gali būti išreikštas keturių sveikųjų skaičių kvadratų suma.*

Įrodymas. Tarkime, kad p yra pirminis skaičius, kuris nėra Hurvico neredukuojamas skaičius. Tuomet egzistuoja tokie Hurvico skaičiai $a_0 + a_1 i + a_2 j + a_3 k$ ir γ, kurie nėra vieneto dalikliai, kad

$$p = (a_0 + a_1 i + a_2 j + a_3 k)\,\gamma.$$

Imame abiejų pusių jungtinius skaičius:

$$p = \overline{p} = \overline{\gamma}\,(a_0 - a_1 i - a_2 j - a_3 k)\,.$$

Sudauginę skaičius su jų jungtiniais, gauname

$$\begin{aligned} p^2 &= (a_0 + a_1 i + a_2 j + a_3 k)\,\gamma\overline{\gamma}\,(a_0 - a_1 i - a_2 j - a_3 k) = \\ &= (a_0 + a_1 i + a_2 j + a_3 k)\,(a_0 - a_1 i - a_2 j - a_3 k)\,\gamma\overline{\gamma} = \\ &= \left(a_0^2 + a_1^2 + a_2^2 + a_3^2\right)|\gamma|^2, \end{aligned}$$

kur $(a_0^2 + a_1^2 + a_2^2 + a_3^2)$ ir $|\gamma|^2$ yra sveikieji skaičiai, didesni už 1. Remiantis pagrindine algebros teorema vienintelė įmanoma skaičiaus p^2 išraiška yra $p \cdot p$. Todėl

$$p = a_0^2 + a_1^2 + a_2^2 + a_3^2 = (a_0 + a_1 i + a_2 j + a_3 k)\,(a_0 - a_1 i - a_2 j - a_3 k).$$

Jei Hurvico skaičius $a_0 + a_1 i + a_2 j + a_3 k$ priklauso $\mathbb{Z}[i, j, k]$, tuomet p yra išreikštas keturių sveikųjų skaičių kvadratų suma.

Tarkime, kad $\psi := a_0 + a_1 i + a_2 j + a_3 k \notin \mathbb{Z}[i, j, k]$. Tada kiekvienas koeficientas a_t, $t = 0, 1, 2, 3$, priklauso aibei $\mathbb{Z} + \frac{1}{2}$. Parinkime tokį skaičių $\omega = \frac{\pm 1 \pm i \pm j \pm k}{2}$, kad skaičiaus $\psi - \omega = a_0^* + a_1^* i + a_2^* j + a_3^* k$ koeficientai a_0^*, a_1^*, a_2^* ir a_3^* būtų lyginiai sveikieji skaičiai. Tada $\psi = \omega + a_0^* + a_1^* i + a_2^* j + a_3^* k$ ir

$$\begin{aligned} p &= (a_0 + a_1 i + a_2 j + a_3 k)(a_0 - a_1 i - a_2 j - a_3 k) = \\ &= (\omega + a_0^* + a_1^* i + a_2^* j + a_3^* k)(\overline{\omega} + a_0 * - a_1^* i - a_2^* j - a_3^* k) = \\ &= (\omega + a_0^* + a_1^* i + a_2^* j + a_3^* k)\overline{\omega} \times \omega(\overline{\omega} + a_0^* - a_1^* i - a_2^* j - a_3^* k) = \\ &= (1 + \overline{\omega} a_0^* + \overline{\omega} a_1^* i + \overline{\omega} a_2^* j + \overline{\omega} a_3^* k)(1 + \omega a_0^* - \omega a_1^* i - \omega a_2^* j - \omega a_3^* k). \end{aligned}$$

Kadangi koeficientai a_0^*, a_1^*, a_2^* ir a_3^* yra lyginiai sveikieji skaičiai, tai Hurvico skaičiaus $1 + \overline{\omega} a_0^* + \overline{\omega} a_1^* i + \overline{\omega} a_2^* j + \overline{\omega} a_3^* k$ visi koeficientai yra sveikieji skaičiai. Taigi egzistuoja tokie $A_0, A_1, A_2, A_3 \in \mathbb{Z}$, kad $1 + \overline{\omega} a_0^* + \overline{\omega} a_1^* i + \overline{\omega} a_2^* j + \overline{\omega} a_3^* k = A_0 + A_1 i + A_2 j + A_3 k$. Kadangi $N(\overline{\omega}) = 1$, tai

$$\begin{aligned} p &= N(a_0 + a_1 i + a_2 j + a_3 k) = N\left(\omega + a_0^* + a_1^* i + a_2^* j + a_3^* k\right) N(\overline{\omega}) = \\ &= N\left((\omega + a_0^* + a_1^* i + a_2^* j + a_3^* k)\overline{\omega}\right) = N\left(1 + \overline{\omega} a_0^* + \overline{\omega} a_1^* i + \overline{\omega} a_2^* j + \overline{\omega} a_3^* k\right) = \\ &= N\left(A_0 + A_1 i + A_2 j + A_3 k\right) = A_0^2 + A_1^2 + A_2^2 + A_3^2. \end{aligned}$$

□

Prisiminkime 5 teoremą, kuri teigia, kad kiekvienam nelyginiam pirminiui skaičiui p egzistuoja skaičiai x, y, ir m tokie, kad

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

t.y. egzistuoja tokie sveikieji skaičiai x ir y, kad p dalija $1 + x^2 + y^2$, bei pereikime prie pilno Lagranžo teoremos įrodymo.

11 Teorema (Keturių kvadratų teorema)**.** *([4]) Kiekvieną natūralųjį skaičių galima išreikšti keturių sveikųjų skaičių kvadratų suma.*

Įrodymas. Tegu p yra nelyginis pirminis skaičius. Tuomet remdamiesi 5 teorema galima rasti x ir y tokius, kad p dalintų $1 + x^2 + y^2$. Išskaidykime šį skaičių Hurvico skaičių sandauga:

$$1 + x^2 + y^2 = (1 + xi + yj)(1 - xi - yj).$$

Jei p būtų neredukuojamas Hurvico skaičius, tuomet, remiantis neredukuojamo Hurvico skaičiaus savybe (9 teiginys), p būtų $1 + xi + yj$ daliklis arba p būtų $1 - xi - yj$ daliklis. Tačiau nei vienas variantas nėra galimas, kadangi nei vienas iš skaičių

$$\frac{1}{p} + \frac{xi}{p} + \frac{yj}{p} \quad \text{ar} \quad \frac{1}{p} - \frac{xi}{p} - \frac{yj}{p}$$

nėra Hurvico skaičius. Iš to išplaukia, kad p yra redukuojamas Hurvico skaičius, todėl, remiantis Sąlygine keturių kvadratų teoremą (10 teorema), skaičius p išreiškiamas keturių sveikųjų skaičių kvadratų suma. Remiantis (2.1) tapatybe gauname, kad bet kokį natūralų skaičių galima išreikšti keturių sveikųjų skaičių kvadratų suma. □

skyrius 4

Lagranžo keturių kvadratų teoremos apibendrinimai

12 Teorema. *([5]) Tegul $a \in \{1, 4\}$ ir $m \in \{4, 5, 6\}$. Tada bet koks natūralusis skaičius n gali būti užrašytas išraiška*

$$n = ax_1^m + x_2^2 + x_3^2 + x_4^2,$$

kur x_1, x_2, x_3 ir x_4 yra sveikieji skaičiai.

Pavyzdžiui,

$$71 = 1^4 + 3^2 + 5^2 + 6^2,$$
$$240 = 2^5 + 0^2 + 8^2 + 12^2,$$
$$624 = 2^6 + 4^2 + 12^2 + 20^2.$$

Taip pat [5] darbe iškelta hipotezė, kad kiekvieną natūralųjį skaičių n galima išreikšti pavidalu $x_1^2 + x_2^3 + x_3^4 + 2x_4^4$ ir $x_1^5 + x_2^4 + x_3^2 + 3x_4^2$, kur x_1, x_2, x_3 ir x_4 yra sveikieji skaičiai.

13 Teorema. *([2]) Jei p yra nelyginis pirminis skaičius, tuomet skaičių $4p$ galima išreikšti keturių nelyginių sveikųjų skaičių kvadratų suma.*

Pavyzdžiui turėdami $p = 3$ turėsime tokią išraišką:

$$4 \cdot 3 = 12 = 1^2 + 1^2 + 1^2 + 3^2.$$

Tačiau $4 \cdot 2 = 8$ nebus suma keturių nelyginių sveikųjų skaičių kvadratų.

14 Teorema. *([2]) Natūraliojo skaičiaus n išraiškų keturių sveikųjų skaičių kvadratų suma skaičius (išraiškos, kurios skiriasi tiktai kvadratų tvarka ar ženklu, yra laikomos skirtingomis) yra lygus skaičiaus n daliklių, kurie nėra* 4 *kartotiniai (paties* 4 *neskaitant), sumai, padaugintai iš* 8*.*

Pavyzdžiui, rasime visas skaičiaus 4 išraiškas keturių sveikųjų skaičių kvadratų suma:

$$\begin{aligned}
4 &= 1^2 + 1^2 + 1^2 + (\pm 1)^2 = \\
&= (-1)^2 + (\pm 1)^2 + 1^2 + 1^2 = \\
&= (-1)^2 + (-1)^2 + (-1)^2 + (\pm 1)^2 = \\
&= (-1)^2 + (\pm 1)^2 + 1^2 + (-1)^2 = \\
&= (-1)^2 + 1^2 + (-1)^2 + (\pm 1)^2 = \\
&= 1^2 + (-1)^2 + (\pm 1)^2 + 1^2 = \\
&= 1^2 + (-1)^2 + (\pm 1)^2 + (-1)^2 = \\
&= 1^2 + 1^2 + (-1)^2 + (\pm 1)^2 = \\
&= (\pm 2)^2 + 0^2 + 0^2 + 0^2 = \\
&= 0^2 + (\pm 2)^2 + 0^2 + 0^2 = \\
&= 0^2 + 0^2 + (\pm 2)^2 + 0^2 = \\
&= 0^2 + 0^2 + 0^2 + (\pm 2)^2 .
\end{aligned}$$

Matome, kad iš viso turime 24 įmanomas išraiškas. Naudojant 14 teoremą šį skaičių galima rasti lengviau. Skaičius 4 turi iš viso 3 daliklius: 1, 2, ir 4, ir nei vienas iš jų nėra 4 kartotinis (paties 4 neskaitant), vadinasi įmanomų išraiškų iš viso yra $3 \cdot 8 = 24$.

Kitą skaičių paimkime 26. Šis skaičius turi iš viso iš viso 8 daliklius: 1, 2, 3, 4, 6, 8, 12, ir 24. Paties 4 neskaitant tarp daliklių yra 3 skaičiai, kurie yra 4 kartotiniai - 8, 12, ir 24, tad juos atmetus dirbame su 5 dalikliais, ir pagal 14 teoremą skaičius 26 turi iš viso $5 \cdot 8 = 40$ įmanomų išraiškų keturių sveikųjų skaičių kvadratų suma.

Kita teorema duodą paprastesnį įmanomų išraiškų keturių sveikųjų skaičių kvadratų suma skaičių.

15 Teorema. *([3]) Natūraliojo skaičiaus n, $n \equiv 4 \pmod 8$, išraiškų keturių sveikųjų skaičių kvadratų suma skaičius (išraiškos, kurios skiriasi tiktai kvadratų tvarka ar ženklu, yra laikomos vienodomis) yra lygus teigiamų nelyginių skaičiaus n daliklių skaičiui.*

Paimkime skaičių 12. Šio skaičiaus galimos išraiškos keturių kvadratų suma yra:

$$\begin{aligned} 12 &= 1^2 + 1^2 + 1^2 + 3^2 \\ &= 2^2 + 2^2 + 2^2 + 0^2. \end{aligned}$$

Matome, kad iš viso turime 2 skirtingas išraiškas. Naudodami 15 teoremą turime, kad skaičiaus 12 dalikliai yra 1, 2, 3, 4, ir 6, iš kurių tik 1 ir 3 yra nelyginiai, vadinasi yra tik dvi įmanomos skaičiaus 12 išraiškos keturių sveikųjų skaičių kvadratų suma.

16 Išvada. *([3]) Natūraliojo skaičiaus n išraiškų keturių sveikųjų skaičių kvadratų suma $x_1^2 + x_2^2 + x_3^2 + x_4^2 = n$ skaičius yra lygus*

1) skaičiaus n daliklių skaičiaus sandaugai su 8, jei skaičius n yra nelyginis, arba

2) skaičiaus n nelyginių daliklių skaičiaus sandaugai su 24, jei n yra lyginis.

Summary

Lagrange's four-square theorem

Lagrange's four-square theorem states, that every positive integer can be expressed as the sum of four squares, that is for every positive integer n there exist integers x_1, x_2, x_3 and x_4 such that

$$y = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

The aim of this work is to present several proofs of this theorem, as well as show few of improvements for this theorem and ways to count the number of possible expressions in sums of four squares.

Literatūra

[1] P. Drungilas, H. Markšaitis, *Algebra*, 1 dalis, **58-59** (2013).

[2] G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, Sixth Edition, **88**, **399-403**, **407-409**, **415** (2008).

[3] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Second Edition, **281-282** (1990).

[4] J. H. Ray Ng, *Quaternions and the Four Square Theorem.* `http://www.math.uchicago.edu/~may/VIGRE/VIGRE2008/REUPapers/Ng.pdf`

[5] Z. W. Sun, *Refining Lagrange's four-square theorem*, Journal of Number Theory, No. 175, **168** (2017).