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

Liudvikas Čiapas

Natūraliojo skaičiaus reiškimas tiksliųjų kvadratų suma

Representation of a Positive Integer by a Sum of Perfect Squares

Bakalauro baigiamasis darbas

Leidžiu ginti .....

Darbo vadovas dr. Aivaras Novikas

Vilnius 2020

Turinys

Įvadas 2

1 Skaičiai, išreiškiami dviejų kvadratų suma **5**

1.1 Pirminio skaičiaus reiškimas dviejų tiksliųjų kvadratų suma 5

1.2 Natūraliojo skaičiaus reiškimas dviejų tiksliųjų kvadratų suma 10

1.3 Skirtingos dviejų tiksliųjų kvadratų sumos išraiškos 11

2 Kiekvieno natūraliojo skaičiaus trumpiausia išraiška tiksliųjų kvadratų suma **13**

2.1 Trijų tiksliųjų kvadratų suma 13

2.2 Keturių tiksliųjų kvadratų suma 14

Summary 17

Literatūra 18

Įvadas

Varingo (Edward Waring) uždavinys yra viena klasikinių skaičių teorijos temų. Jis klausia, ar kiekvienam natūraliajam skaičiui $k \geq 2$ egzistuoja toks natūralusis skaičius s, kad kiekvienas teigiamas skaičius n yra s neneigiamų sveikųjų dėmenų, pakeltų laipsniu k, suma:

$$n = a_1^k + a_2^k + \cdots + a_s^k$$

Mažiausias toks s, tenkinantis šią sąlygą, dažnai apibrėžiamas funkcija $g(k)$, pabrėžiant, kad ši funkcija priklauso tik nuo laipsnio rodiklio. 1770 metais Lagranžas (Joseph-Louis Lagrange) išsprendė uždavinį atveju $k = 2$, pateikdamas išvadą, jog kiekvieną natūralųjį skaičių galima išreikšti keturių tiksliųjų kvadratų suma, tai yra $g(2) = 4$.

Šiais laikais Varingo uždavinys yra išspręstas bendruoju atveju. Įrodyta, kad toks s egzistuoja kiekvienam laipsniui k. Pavyzdžiui, $g(3) = 9$, o $g(4) = 19$. Tačiau ilgą laiką jis buvo vienas žinomiausių neišsprendžiamų klausimų skaičių teorijoje. Panašų statusą vis dar turi Goldbacho (Christian Goldbach) hipotezė, teigianti, jog kiekvieną lyginį skaičių, didesnį nei 2, galima išreikšti dviejų pirminių skaičių suma. Ši prielaida šiais laikais yra patikrinta ir patvirtinta teisinga skaičiams iki $4 \cdot 10^{18}$, tačiau vis dar nėra įrodyta.

Varingo-Goldbacho uždavinys, siejantis Varingo uždavinį ir Goldbacho hipotezę, klausia, ar kiekvienam k egzistuoja toks skaičius s, kad kiekvienas pakankamai didelis n gali būti išreikštas daugiausia s pirminių skaičių, pakeltų laipsniu k, suma:

$$n = p_1^k + p_2^k + \cdots + p_s^k$$

Šiame darbe nagrinėjamas Varingo uždavinio atvejis, kai $k = 2$. Apibrėžkime tokią aibę S, kuriai priklauso visi natūralieji skaičiai, kuriuos įmanoma užrašyti kaip dviejų kvadratų sumą. Pavyzdžiui, $250 = 9^2 + 13^2$ arba $3362 = 31^2 + 49^2$.

Skaičius 30 tokios išraiškos neturi, tačiau jį įmanoma užrašyti trijų kvadratų suma: $30 = 1^2 + 2^2 + 5^2$. Skaičiaus 60 neįmanoma išreikšti nei dviem, nei trimis kvadratais, tačiau tai galime padaryti keturiais kvadratais: $60 = 2^2 + 2^2 + 4^2 + 6^2$.

Šis Varingo uždavinio atvejis nagrinėjamas jau nuo senovės graikų laikų. Dar II amžiuje Diofantas (Diophantus) veikale „Aritmetika“ padaro išvadą, kad ne visus skaičius galima užrašyti trijų kvadratų suma. 1798 metais Ležandras (Adrien-Marie Legendre) pateikia įrodymą, jog tik skaičiai formos $4^n(8k+7)$ negali būti išreiškiami trijų sveikųjų skaičių kvadratų suma (čia n ir k – sveikieji neneigiami skaičiai).

Ir šioje reiškimo kvadratų suma temoje taip pat yra neišspręstų teoremų. Viena iš jų - ar egzistuoja be galo daug tokių pirminių skaičių, kurie gali būti išreikšti trijų iš eilės einančių natūraliųjų skaičių kvadratų suma, pavyzdžiui $149 = 6^2 + 7^2 + 8^2$.

Taigi šio darbo tikslas yra išnagrinėti skaičių teorijos metodus, naudojamus minėtiems teiginiams įrodyti. Pirmasis skyrius skirtas dviejų kvadratų sumos išraiškai. Pirmiausia nagrinėjama, kodėl tam tikri pirminiai skaičiai turi ar neturi tokios išraiškos. Tada pereinama prie bendresnio atvejo visiems natūraliesiems skaičiams. Taip pat nagrinėjamos skirtingos skaičiaus dviejų tiksliųjų kvadratų išraiškos. Antrasis skyrius skirtas trijų ir keturių kvadratų sumų atvejui. Jame įrodoma Lagranžo teorema $g(2) = 4$.

Jei kitaip nenurodyta, bus laikoma, kad raidėmis pažymėti skaičiai priklauso sveikųjų skaičių aibei.

1 skyrius

Skaičiai, išreiškiami dviejų kvadratų suma

Įvade jau apibrėžėme aibę S, kurią sudaro visi natūralieji skaičiai, išreiškiami dviejų tiksliųjų kvadratų suma. Akivaizdu, jog ši aibė yra begalinė. Pagrindinis šio skyriaus uždavinys – išsiaiškinti, kokie skaičiai priklauso šiai aibei

1.1 Pirminio skaičiaus reiškimas dviejų tiksliųjų kvadratų suma

1 teiginys. *Jei n=$4k+3$, tai $n \notin S$. Čia k – neneigiamas sveikasis skaičius.*

Įrodymas. Tarkime $n \in S$. Tuomet egzistuoja tokie sveikieji skaičiai x ir y, kad $n = x^2 + y^2$. Dalybos iš 2 atveju x ir y turi liekaną 0 arba 1. Išplaukia, jog $x^2 + y^2$ dalybos iš 4 atveju turi liekanas 0, 1 arba 2. Tačiau pagal teiginio sąlygą $x^2 + y^2 = 4k + 3$, todėl gavome prieštarą. □

Pagal šį teiginį jau galime šiek tiek apibūdinti aibę S. Tačiau pagrindinis uždavinys lieka neišspręstas. Kad galėtume parodyti, kokie natūralieji skaičiai priklauso šiai aibei, pirmiausia reikia rasti visus pirminius $p \in S$. Tai suteiks galimybę išspręsti uždavinį visiems natūraliesiems skaičiams.

Šiam tikslui apibrėšime pirminių skaičių aibes P_1 ir P_2:

1. $p \in P_1$, jei jį galima užrašyti forma $p = 4k + 3$, $k \in \mathbb{Z}$;
2. $p \in P_2$, jei jį galima užrašyti forma $p = 4k + 1$, $k \in \mathbb{Z}$.

Visų pirminių skaičių aibė lygi $P_1 \cup P_2 \cup \{2\}$ ir $P_1 \cap P_2 = \emptyset$.

Pagal 1 teiginį, kuris įrodo bendresnį atvejį, jau įsitikinome, kad visi aibės P_1 elementai neturi lygties $p = x^2 + y^2$ sprendinių. Taip pat turime atskirą atvejį, kuomet $p = 2$. Šis pirminis priklauso aibei S, nes $2 = 1^2 + 1^2$. Vadinasi, be $p = 2$, aibei S gali priklausyti tik tokie pirminiai skaičiai, kurie priklauso aibei P_2.

2 išvada. *Jei nelyginis pirminis skaičius $p \in S$, tai $p \in P_2$.*

Įrodymas. Išplaukia iš 1 teiginio. □

3 apibrėžimas. Pirminio skaičiaus p kvadratinių liekanų aibę sudaro skaičiai x tenkinantys lyginį $n^2 \equiv x \pmod{p}$, kai $1 \leq x \leq p-1$. Čia n – bet koks sveikasis skaičius.

Rasime skaičiaus 7 kvadratinių liekanų aibę.

$$1^2 \equiv 1 \pmod{7}$$

$$2^2 \equiv 4 \pmod{7}$$

$$3^2 \equiv 2 \pmod{7}$$

$$4^2 \equiv 2 \pmod{7}$$

$$5^2 \equiv 4 \pmod{7}$$

$$6^2 \equiv 1 \pmod{7}$$

$$7^2 \equiv 0 \pmod{7}$$

Tęsdami procesą matysime, kad liekanos kartojasi, nes $8^2 = (7+1)^2 \equiv 1^2 \pmod{7}$, $9^2 = (7+2)^2 \equiv 2^2 \pmod{7}$ ir taip toliau. Taigi, pagal apibrėžimą, skaičiaus 7 kvadratinių liekanų aibė yra $\{1,\ 2,\ 4\}$. Pagal 2 išvadą, jei pirminis skaičius p priklauso aibei S, tai $p = 4k + 1$. Iš tiesų tai visi tokie pirminiai skaičiai priklauso aibei S. Šiam teiginiui patvirtinti pirmiausia parodysime, kad -1 yra pirminio skaičiaus $p \in P_2$ kvadratinė liekana.

4 teorema (Vilsono)**.** *Natūralusis skaičius p yra pirminis tada ir tik tada, jei*

$$(p-1)! \equiv -1 \pmod{p}.$$

Įrodymas. Teorema akivaizdi skaičiams 2 ir 3, taigi nagrinėsime tik pirminius $p > 3$.

Tegul R - skaičiaus p liekanų aibė, $R = \{r_i \in \mathbb{Z},\, r_i = i,\ 1 \leq i \leq p-1\}$. Jei p būtų sudėtinis, tuomet vienas jo daliklių būtų iš šios aibės. Tuomet tas daliklis dalytų $(p-1)!$, tačiau jis, o tuo pačiu ir p, nedalytų $(p-1)!+1$. Išplaukia $(p-1)! \not\equiv -1 \pmod{p}$.

Iš kitos pusės, jei p pirminis, tuomet kiekvienas skaičius iš šios aibės yra tarpusavyje pirminis su p. Tarkime, kad kiekvienam $r_a \in R$ egzistuoja toks atvirkštinis skaičius $r_b \in R$, kad $r_a r_b \equiv 1 \pmod{p}$. Tai iš tiesų teisinga, nes jei kažkuris $r_a \in R$ neturėtų tokio atvirkštinio, tuomet egzistuotų tokie $r_c \in R$ ir $r_d \in R$, kad $r_a r_c \equiv r_a r_d \pmod{p}$. Tai yra, p dalytų skaičių $r_a(r_c - r_d)$, tačiau p nedalija nei r_a, nei $r_c - r_d$. Gavome prieštarą.

Kiekvienas r turi vienintelį atvirkštinį, ir kiekvienas r yra savo atvirkštinio atvirkštinis. Jei kažkuris daliklis yra pats sau atvirkštinis, tuomet $r^2 \equiv 1 \pmod{p}$. Tada p dalija $r^2 - 1 = (r-1)(r+1)$, o kadangi p pirminis, tai arba $r-1$ arba $r+1$ dalijasi iš p. Tai teisinga tik tuomet, kai $r = 1$ ir $r = p-1$.

Taigi galime aibės R elementus suskirstyti į tokias poras $\{r_i, r_j\}$, kad $r_i r_j \equiv 1 \pmod{p}$. Iš čia turime, kad $2 \cdot 3 \ldots (p-2) \equiv 1 (\mathrm{mod}\ p)$. Padauginę lyginį iš $(p-1)$, gausime teoremos įrodymą. □

5 teorema. -1 *yra pirminio skaičiaus* $p \equiv 1 \pmod{4}$ *kvadratinė liekana.*

Įrodymas. Pagal apibrėžimą, kad įrodytume, jog -1 yra pirminio skaičiaus p kvadratinė liekana, mums reikia parodyti, kad kažkokis sveikasis skaičius x tenkina lyginį $x^2 \equiv -1 \pmod{p}$.

Nagrinėsime skaičių $(p-1)!$. Jį išskaidę galime pastebėti, jog visi daugikliai nuo $\frac{p+1}{2}$ iki $p-1$ dalybos iš p atveju turi atitinkamą liekaną, kaip ir daugikliai nuo 1 iki $\frac{p-1}{2}$, tik su priešingu ženklu. Tai yra:

$$(p-1)! = 1 \cdot 2 \cdot 3 \ldots \left(\frac{p-1}{2}\right) \cdot \left(\frac{p+1}{2}\right) \ldots (p-2) \cdot (p-1) \equiv$$

$$1 \cdot 2 \cdot 3 \ldots \left(\frac{p-1}{2}\right) \cdot \left(-\frac{p-1}{2}\right) \ldots (-2) \cdot (-1) \equiv$$

$$(-1)^{\frac{p-1}{2}} \left(\left(\frac{p-1}{2}\right)!\right)^2 (\mathrm{mod}\ p)$$

Šiuo atveju nagrinėjame tik pirminius skaičius $p = 4k+1$, taigi įrašę gauname

$$(-1)^{\frac{p-1}{2}} \left(\left(\frac{p-1}{2}\right)!\right)^2 = ((2k)!)^2$$

Vilsono teorema teigia, kad $(p-1)! \equiv -1 \pmod{p}$. Taigi savo ruožtu ir $((2k)!)^2 \equiv -1 \pmod{p}$, o tai reiškia, kad -1 yra skaičiaus $p \equiv 1 \pmod 4$ kvadratinė liekana $\square$

6 apibrėžimas. $\left(\frac{a}{p}\right)$ vadiname Ležandro simboliu, jei p – nelyginis pirminis skaičius, $\mathrm{DBD}(a,p) = 1$ ir

$$\left(\frac{a}{b}\right) = \begin{cases} 1, \text{kai } a \text{ yra skaičiaus } p \text{ kvadratinė liekana;} \\ -1, \text{kai } a \text{ nėra skaičiaus } p \text{ kvadratinė liekana;} \\ 0, \text{kai } a \equiv 0 \ (\mathrm{mod} p). \end{cases}$$

Pavyzdžiui, $\left(\frac{15}{17}\right) = 1$, nes $7^2 = 49 \equiv 15 \pmod{17}$, o $\left(\frac{3}{7}\right) = -1$, kadangi, kaip jau įsitikinome, 3 nėra skaičiaus 7 kvadratinė liekana. Taigi 5 teoremą galėtume suformuluoti ir taip: $\left(\frac{-1}{p}\right) = 1$, kai $p \equiv 1 \pmod 4$.

Dabar, pasinaudodami Mažąja Ferma (Fermat's little) teorema, kurios įrodymą galima rasti [6], išvesime bendresnę formulę visiems pirminiams skaičiams.

7 teorema (Mažoji Ferma)**.** *Jei pirminis skaičius p ir natūralusis skaičius n tarpusavyje pirminiai, tuomet $n^{p-1} \equiv 1 \pmod p$.*

8 teiginys. *Jei a ir b tarpusavyje pirminiai, tai kiekvienas $a^2 + b^2$ pirminis daliklis $p \in P_2$.*

Įrodymas. Tarkime, kad p dalija $a^2 + b^2$ kažkokiems a ir b, kai $\mathrm{DBD}(a,b) = 1$. Jei p dalija a, tai dalija ir a^2. Tuomet išplauktų, jog p dalija ir b^2 ir patį b. Prieštara, nes $\mathrm{DBD}(a,\ b) = 1$.

Taigi a, b ir p yra poromis tarpusavyje pirminiai. Kadangi p dalija $a^2 + b^2$, tai $-a^2 \equiv b^2 \pmod p$. Pakėlę abi lygties puses laipsniu $(p-1)/2$, gauname $(-1)^{(p-1)/2} a^{p-1} \equiv b^{p-1} \pmod p$. Pagal Mažąją Ferma teoremą $a^{p-1} \equiv b^{p-1} \equiv 1 \pmod p$, taigi $(-1)^{(p-1)/2} \equiv 1 \pmod p$. Išplaukia $p = 4k+1$. $\square$

Pagal 8 teiginį, jei kažkoks sveikasis skaičius $x^2 \equiv -1 \pmod p$, tai yra $x^2 + 1^2 = kp$, $k \in \mathbb{Z}$, tuomet $p \in P_2$. Tai reiškia, kad -1 nėra skaičiaus $p = 4k+3$ kvadratinė liekana, ir formulė $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ galioja visiems nelyginiams pirminiams p.

9 teorema. *Jei $p \in P_2$, tai $p \in S$.*

Įrodymas. Tegul $p = 4k+1$. Pagal 5 teoremą, jau įrodėme, kad -1 yra šio pirminio skaičiaus kvadratinė liekana, tai yra $n^2 \equiv -1 \pmod p$ teisinga kažkokiam sveikajam skaičiui n. Kadangi $(-n)^2 = n^2$ ir kiekvienas $(p-1)^2, (p-2)^2, \ldots, \left(\frac{p+1}{2}\right)^2$ yra lygus atitinkamai $1^2, 2^2, \ \ldots\ , \left(\frac{p-1}{2}\right)^2$ moduliu p, tai užtenka nagrinėti tik $1 \le n < p/2$.

Kadangi -1 yra p kvadratinė liekana, tai egzistuoja toks a, kuriam teisinga lygybė $ap = n^2 + 1$ ir $ap \in S$.

Kadangi

$$0 < ap = n^2 + 1 < \frac{p^2}{4} + 1 < \frac{p^2}{4} + \frac{3p^2}{4} = p^2$$

Tai $a < p$. Tarkime skaičius b yra toks mažiausias natūralusis skaičius, kuriam teisinga $bp \in S$ ir $b \leq a$. Pažymėkime $bp = x^2 + y^2$.

Tarkime, kad $b > 1$. Tada dalydami skaičius x ir y iš b, gausime liekanas atitinkamai s_1 ir s_2. Pažymėkime $x = r_1 b + s_1$ ir $y = r_2 b + s_2$. Laikysime, kad

$$-\frac{b}{2} < s_1 \leq \frac{b}{2}\ ,\ -\frac{b}{2} < s_2 \leq \frac{b}{2}$$

Tada turime:

$$bp = x^2 + y^2 = (r_1 b + s_1)^2 + (r_2 b + s_2)^2 =$$

$$\left(r_1^2 b^2 + 2b r_1 s_1 + s_1^2\right) + \left(r_2^2 b^2 + 2b r_2 s_2 + s_2^2\right)$$

Atlikę ekvivalenčius pertvarkymus gauname:

$$bp = b(r_1^2 b + 2r_1 s_1) + s_1^2 + b(r_2^2 b + 2r_2 s_2) + s_2^2$$

$$bp - b\left(\left(r_1^2 b + 2r_1 s_1\right) + \left(r_2^2 b + 2r_2 s_2\right)\right) = s_1^2 + s_2^2$$

$$b\left(p - \left(r_1^2 b + 2r_1 s_1\right) - \left(r_2^2 b + 2r_2 s_2\right)\right) = s_1^2 + s_2^2$$

Pažymėkime

$$c = p - r_1^2 b - 2r_1 s_1 - r_2^2 b - 2r_2 s_2 \tag{1.1}$$

Tada:

$$bc = s_1^2 + s_2^2 \leq \left(\frac{b}{2}\right)^2 + \left(\frac{b}{2}\right)^2 = \frac{b^2}{2} < b^2$$

Išplaukia, kad $0 \leq c < b$. Jei $c = 0$, tai $s_1 = s_2 = 0$, o $x = r_1 b$ ir $y = r_2 b$. Iš čia išplauktų, kad $bp = x^2 + y^2 = b^2(r_1^2 + r_2^2)$. Gauname prieštarą, nes p pirminis ir todėl $p \neq b(r_1^2 + r_2^2)$. Taigi $1 \leq c < b$.

Iš lygties (1.1) turime $p = b(r_1^2 + r_2^2) + 2(r_1 s_1 + r_2 s_2) + c$. Tada $cp = bc(r_1^2 + r_2^2) + 2c(r_1 s_1 + r_2 s_2) + c^2 = (c + r_1 s_1 + r_2 s_2)^2 + (r_1 s_2 - s_1 r_2)^2$. Išplauktų, kad $cp \in S$. Tačiau tai prieštarautų prielaidai, jog b yra mažiausias nenulinis sveikasis skaičius, kuriam $bp \in S$. Taigi, $b = 1$ ir $p \in S$. □

Tokiu būdu išsprendėme uždavinį $p = x^2 + y^2$ parodydami, kad visi pirminiai $p \equiv 3 \pmod 4$ nepriklauso aibei S ir visi $p \equiv 1 \pmod 4$ priklauso. Kitame skyriuje pereisime prie bendresnio atvejo, nagrinėjančio ne tik pirminius, bet apskritai visus natūraliuosius skaičius.

1.2 Natūraliojo skaičiaus reiškimas dviejų tikslių- jų kvadratų suma

10 apibrėžimas. Gauso sveikųjų skaičių aibe vadiname aibę $\mathbb{Z}[i] = \{a + bi \mid a,\ b \in \mathbb{Z}\}$.

Taip pat Gauso skaičiams apibrėžkime funkciją $\mathrm{N}(a + bi) = |a + bi|^2 = a^2 + b^2$. Ši funkcija yra multiplikatyvi:

$$|a + bi|\,|c + di| = |(a + bi)(c + di)| \ \Rightarrow$$

$$|a + bi|^2 |c + di|^2 = |(a + bi)(c + di)|^2 \ \Rightarrow$$

$$\mathrm{N}(a + bi)\,\mathrm{N}(c + di) = \mathrm{N}((a + bi)(c + di))$$

Pavyzdžiui, $\mathrm{N}(1 + 2i)\,\mathrm{N}(3 + 4i) = \mathrm{N}((1 + 2i)(3 + 4i)) = \mathrm{N}(-5 + 10i) = (-5)^2 + 10^2 = 125$. Imkime du bet kokius Gauso skaicius $a + bi$ ir $c + di$. Tada

$$\mathrm{N}(a + bi)\,\mathrm{N}(c + di) = \mathrm{N}((a + bi)(c + di)) = \mathrm{N}((ac - bd) + (ad + bc)\,i)$$

Įrašę funkcijos reikšmes, gauname formulę:

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 \tag{1.2}$$

Šią lygybę 1202 metais Fibonačis (Fibonacci) aprašė knygoje „Liber abaci“ (liet. „Skaičiavimų knyga“). 1749 metais, Oileris (Leonhard Euler) panaudojo šią lygybę sekančio teiginio įrodymui.

11 teiginys. *Jei $n \in S$ ir $m \in S$, tai $nm \in S$.*

Įrodymas. Imkime tokius sveikuosius skaičius a, b, c ir d, kad $n = a^2 + b^2$ ir $m = c^2 + d^2$. Iš (1.2) lygybės turime $nm = (a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$. Taigi $mn \in S$ □

Pasinaudodami jau įrodytais teiginiais, galiausiai galime apibrėžti, kuriuos natūraliuosius skaičius galime išreikšti dviejų kvadratų suma.

Pagal pagrindinę aritmetikos teoremą, kiekvieną natūralųjį skaičių n vieninteliu būdų galima užrašyti pavidalu $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}$, kuris yra vadinamas skaičiaus n kanonine išraiška. Čia $p_1 < p_2 < \dots < p_k$ – skirtingi pirminiai skaičiai, $\alpha_i \geq 1,\ i = 1,\ 2,\ \dots,\ k.$. Pavyzdžiui, $540 = 2^2 \cdot 3^3 \cdot 5$.

12 teorema. *Skaičius $n \in S$ tada ir tik tada, jei skaičiaus n kanoninėje išraiškoje kiekvienas pirminis skaičius $p \in P_1$ pakeltas lyginiu laipsniu.*

Įrodymas. Tarkime, kad visi pirminiai formos $p = 4k+3$ turi lyginį laipsnį skaičiaus n kanoninėje išraiškoje. Pagal 9 teoremą, kiekvieną pirminį $p = 4k + 1$ galime išreikšti dviejų kvadratų suma. Taip pat $p = 2 = 1^2 + 1^2$. Pirminius $p^2 = (4k + 3)^2$ galime užrašyti kaip $p^2 = p^2 + 0^2$. Tuomet skaičiaus n kanoninę išraišką galime pakeisti tiksliųjų kvadratų sumų sandauga:

$$n = (m_1^2 + m_2^2) \cdot (m_3^2 + m_4^2) \ldots, m_i \in Z, i = 1, 2, 3, \ldots$$

Pagal 10 teiginį, ši sandauga lygi dviejų kvadratų sumai, tai yra $n \in S$.

Lieka įrodyti, kad jokie kiti skaičiai nepriklauso aibei S. Tarkime, kad skaičius $n = a^2 + b^2$ ir turi pirminį daliklį p.

Tarkime, kad p nedalija bent vieno iš skaičių a ir b. Jei p dalija a, tai dalija ir a^2. Tuomet išplauktų, jog p dalija ir b^2 ir patį b. Gauname prieštarą.

Taigi, p dalija ir a, ir b, arba a, b ir p yra poromis tarpusavyje pirminiai. Antruoju atveju, pagal 8 teiginio įrodymą, $p \equiv 1 \pmod 4$. Jei p dalija abu skaičius a ir b, tai yra $a \equiv b \equiv 0 \pmod p$, pažymėkime $a = x_1 p$, $b = y_1 p$. Gauname

$$n = p^2(x_1^2 + y_1^2)$$

Jei p dalija $x_1^2 + y_1^2$, tuomet analogiškai $n = p^4(x_2^2 + y_2^2)$. Tęsdami procesą t kartų galutinėje išraiškoje turėsime $n = p^2 t(x_t^2 + y_t^2)$. Išplaukia, jei $p \equiv 3 \pmod 4$, kanoninėje išraiškoje jis turi lyginį laipsnį. □

1.3 Skirtingos dviejų tiksliųjų kvadratų sumos išraiškos

Nagrinėdami skaičius iš aibės S galime pastebėti, kad kai kurie skaičiai turi daugiau nei vieną išraišką dviejų kvadratų suma. Pavyzdžiui, $65 = 1^2 + 8^2 = 4^2 + 7^2$. O skaičių 17 taip išreikšti galime vieninteliu būdu – $17 = 1^2 + 4^2$.

13 teorema. *Neatsižvelgiant į dėmenų tvarką ir ženklus, kiekvienas pirminis skaičius $p \in P_2$ vieninteliu būdu gali būti išreikštas dviejų tiksliųjų kvadratų suma.*

Įrodymas. Tarkime $p = 4k + 1$ turi dvi skirtingas kvadratų sumos išraiškas, tai yra $p = a^2 + b^2 = c^2 + d^2$. Jau įrodėme, kad -1 yra šio pirminio skaičiaus kvadratinė liekana. Taigi lyginys $x^2 \equiv -1 \pmod p$ turi sprendinį, kurį pažymime x_{-1}. Pagal prielaidą $a^2 \equiv -b^2 \equiv x_{-1}^2 b^2 \pmod p$ ir $c^2 \equiv -d^2 \equiv x_{-1}^2 d^2 \pmod p$. Iš čia turime du atvejus:

1. $a \equiv \pm x_{-1} b \pmod{p}$ ir $c \equiv \pm x_{-1} d \pmod{p}$. Taigi $ac + bd \equiv x_{-1}^2 bd + bd \equiv 0$ ir $ad - bc \equiv \pm x_{-1}(bd - bd) \equiv 0 \pmod{p}$. Išplaukia, kad egzistuoja tokie sveikieji skaičiai m ir n, kad $ac + bd = mp$ ir $ad - bc = np$. Pagal 11 teiginį turime $p^2 = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 = (mp)^2 + (np)^2$. Iš pastarosios lygybės gauname $1 = m^2 + n^2$, tačiau tai teisinga tik tada, kai $m = 0$ arba $n = 0$, tai yra $ac + bd = 0$ arba $ad - bc = 0$. Kadangi $\mathrm{DBD}(a, b) = \mathrm{DBD}(c, d) = 1$, tai $ac + bd = 0$ ir $ad - bc = 0$ tada ir tik tada, jei $a = \pm c$ ir $b = \pm d$ arba $a = \pm d$ ir $b = \mp c$. Bet kuriuo atveju, gauname, kad abi išraiškos yra vienodos neatsižvelgiant į dėmenų tvarką ir ženklus.

2. $a \equiv \pm x_{-1} b \pmod{p}$ ir $c \equiv \mp x_{-1} d \pmod{p}$. Taigi $ac - bd \equiv -x_{-1}^2 bd - bd \equiv 0$ ir $ad + bc \equiv \pm x_{-1}(bd - bd) \equiv 0 \pmod{p}$. Imkime tokius m ir n, kad $ac - bd = mp$ ir $ad + bc = np$. Tada turime $p^2 = (a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 = (mp)^2 + (np)^2$. Toliau įrodinėjimas analogiškas ir vėl gauname, kad abi išraiškos yra vienodos neatsižvelgiant į dėmenų tvarką ir ženklus.

□

Tokiu būdu įrodėme, kad pirminius skaičius iš aibės P_2 vieninteliu būdu galime išreikšti dviejų tiksliųjų kvadratų suma.

Tarkime skaičius d – natūralaus skaičiaus n daliklis. Apibrėžkime funkciją:

$$f(d) = \begin{cases} 1, \ d \equiv 1 \pmod{4}; \\ -1, \ d \equiv 3 \pmod{4}; \\ 0, \ d \equiv 0 \pmod{2}. \end{cases}$$

Tegul $h(n)$ – skaičiaus n skirtingų dviejų tiksliųjų kvadratų sumų išraiškų skaičius, tai yra lygties $n = x^2 + y^2$ sprendinių skaičius, kai $x > 0$, $y \geq 0$, o (x, y) ir (y, x) laikomi skirtingais sprendiniais. Funkciją $h(n)$ galima apibrėžti formule, kurios įrodymą galima rasti [3]:

$$h(n) = \sum_{d|\mathrm{n}} f(d)$$

Jei nagrinėsime natūralaus skaičiaus n kanoninę išraišką $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}$, tuomet patogiau naudoti ekvivalenčią formulę:

$$h(n) = \prod_{p_i \equiv 1 (\mathrm{mod}\ 4)} (1 + \alpha_i), \ 1 \leq i \leq k \tag{1.3}$$

Pavyzdžiui, kai $n = 325 = 5^2 * 13$, tai pagal (1.3) $f(n) = 3 \cdot 2 = 6$.

2 skyrius

Kiekvieno natūraliojo skaičiaus trumpiausia išraiška tiksliųjų kvadratų suma

Pirmajame skyriuje parodėme, kad ne visi skaičiai priklauso aibei S. Šiame skyriuje įrodysime, kad platesnei skaičių, išreiškiamų keturių tiksliųjų kvadratų suma, aibei pirklauso visi natūralieji skaičiai. Taip pat aptarsime tarpinį trijų kvadratų atvejį.

2.1 Trijų tiksliųjų kvadratų suma

14 teorema (Ležandro trijų kvadratų)**.** *Sveikasis skaičius $a = 4^m(8k + 7)$ neturi trijų tiksliųjų kvadratų išraiškos. Čia m ir k – neneigiami sveikieji skaičiai.*

Įrodymas. Tarkime a gali būti išreiškiamas trimis kvadratais. Pažymėkime $a = x_1^2 + x_2^2 + x_3^2$. Dalybos iš 4 atveju x_i^2 $(i = 1, 2, 3)$ turi liekaną 0, jei x_i – lyginis, arba 1, jei nelyginis. Taigi, jei $m > 1$, $a \equiv 0 \pmod 4$ ir visi x_i – lyginiai. Tada $\frac{a}{4} = 4^{m-1}(8k + 7) = \left(\frac{x_1}{2}\right)^2 + \left(\frac{x_2}{2}\right)^2 + \left(\frac{x_3}{2}\right)^2$. Kartojame procesą, kol gauname $b = 8k + 7 = y_1^2 + y_2^2 + y_3^2$.

Žinome, kad $b \equiv 7 \pmod 8$ ir b – nelyginis, todėl vienas iš y_i $(i = 1, 2, 3)$ nelyginis arba visi trys nelyginiai. Skaičiaus 8 kvadratinių liekanų aibę sudaro $\{0, 1, 4\}$. Taigi jei visi y_i – nelyginiai, tai $y_1^2 + y_2^2 + y_3^2 \equiv 3 \pmod 8$ – prieštara. Neprarasdami bendrumo, tarkime y_1 yra nelyginis, o y_2 ir y_3 – lyginiai. Tada $y_2^2 \equiv 0$ arba $y_2^2 \equiv 4 \pmod 8$ (analogiškai y_3). Todėl $b \equiv 1$ arba $b \equiv 5 \pmod 8$ – vėl prieštara. Išplaukia,

kad a neišreiškiamas trimis kvadratais. $\square$

1798 metais Ležandras pateikia įrodymą, kad visi skaičiai, neišreiškiami trijų tiksliųjų kvadratų suma, yra būtent tokios formos.

2.2 Keturių tiksliųjų kvadratų suma

Jei z_1, z_2, z_3, z_4 Gauso skaičiai, tai

$$\begin{pmatrix} z_1 & -\overline{z_2} \\ z_2 & \overline{z_1} \end{pmatrix} \begin{pmatrix} z_3 & -\overline{z_4} \\ z_4 & \overline{z_3} \end{pmatrix} = \begin{pmatrix} z_1 z_3 - \overline{z_2} z_4 & -\overline{(z_2 z_3 + \overline{z_1} z_4)} \\ z_2 z_3 + \overline{z_1} z_4 & \overline{z_1 z_3 - \overline{z_2} z_4} \end{pmatrix}$$

Skaičiuodami abiejų lygybės pusių determinantus gauname

$$(\mathrm{N}(z_1) + \mathrm{N}(z_2))(\mathrm{N}(z_3) + \mathrm{N}(z_4)) = \mathrm{N}(z_1 z_3 - \overline{z_2} z_4) + \mathrm{N}(z_2 z_3 + \overline{z_1} z_4)$$

Imkime $z_1 = a_1 - a_2 i$, $z_2 = -a_3 - a_4 i$, $z_3 = b_1 + b_2 i$ ir $z_4 = b_3 + b_4 i$. Tada gauname Oilerio keturių kvadratų sumų sandaugos tapatybę:

$$\left(a_1^2 + a_2^2 + a_3^2 + a_4^2\right)\left(b_1^2 + b_2^2 + b_3^2 + b_4^2\right) =$$

$$(a_1 b_1 + a_2 b_2 + a_3 b_3 + a_4 b_4)^2 + (a_1 b_2 - a_2 b_1 + a_3 b_4 - a_4 b_3)^2 +$$

$$(a_1 b_3 - a_2 b_4 - a_3 b_1 + a_4 b_2)^2 + (a_1 b_4 + a_2 b_3 - a_3 b_2 - a_4 b_1)^2$$

15 lema. *Jei p – pirminis, $x^2 + y^2 + 1 \equiv 0 \pmod{p}$ turi sprendinį, kai x, y – sveikieji skaičiai.*

Įrodymas. Kai $p = 2$ teorema teisinga, taigi nagrinėsime tik nelyginius pirminius p.

Tegul aibę A sudaro skaičiai $0 \le a \le p-1$, kurie tenkina lyginį $x^2 \equiv a \pmod{p}$, o aibę B skaičiai $0 \le b \le p-1$, tenkinantys lyginį $-1 - y^2 \equiv b \pmod{p}$, kai x ir y – bet kokie sveikieji skaičiai. Įrodysime, kad kiekviena iš šių aibių turi $(p+1)/2$ elementų.

Skaičiaus p kvadratinės liekanos yra poromis lygios: $(p-1)^2 \equiv 1^2$, $(p-2)^2 \equiv 2^2$,..., $\left(\frac{p+1}{2}\right)^2 \equiv \left(\frac{p-1}{2}\right)^2 \pmod{\mathrm{p}}$. Taip pat $x^2 = (-x)^2$. Taigi nagrinėsime tik $1 \le x \le (p-1)/2$.

Tarkime egzistuoja tokie x_1 ir x_2, kad $x_1^2 \equiv a$ ir $x_2^2 \equiv a \pmod{p}$. Tada $x_1^2 \equiv x_2^2 \pmod{\mathrm{p}}$. Tai reiškia p dalija $x_1^2 - x_2^2 = (x_1 + x_2)(x_1 - x_2)$. Tuomet p dalytų $(x_1 + x_2)$ arba $(x_1 - x_2)$. Kadangi $2 \le (x_1 + x_2) \le p-1$, tai p nėra $(x_1 + x_2)$ daliklis,

tai yra p dalija $(x_1 - x_2)$. Kadangi $0 \leq |x_1 - x_2| \leq (p-1)/2$, tai šis teiginys teisingas tik tada, kai $x_1 = x_2$.

Įrodėme, kad kiekvienam $0 \leq x \leq (p-1)/2$ galime priskirti unikalų a, tenkinantį lyginį $x^2 \equiv a \pmod{p}$. Todėl aibė A turi lygiai $(p+1)/2$ elementų. Analogiškai, aibei B priklauso priklauso $(p+1)/2$ skaičių, tenkinančių lyginį $-1-y^2 \equiv b \pmod{p}$.

Kadangi skaičiaus p liekanų aibė $\{0,\ 1,\ 2,\ \ldots,\ p-1\}$ turi p elementų, o $A \cup B$ turi $\frac{p+1}{2} + \frac{p+1}{2} = p+1$ elementų, tai aibės A ir B kertasi. Tai yra, egzistuoja lyginio $x^2 \equiv -y^2 - 1 \pmod{p}$ sprendinys. □

16 išvada. *Egzistuoja toks sveikasis skaičius a, kad $ap = x^2 + y^2 + 1$ ir $a < p$. a, x, y – sveikieji skaičiai, p – pirminis.*

Įrodymas. Pagal 15 lemą, egzistuoja tokie x ir y tenkinantys lyginį $x^2 + y^2 + 1 \equiv 0 \pmod{p}$. Kai $p = 2$, tai išvada teisinga. Taigi, neprarasdami bendrumo, laikysime, kad p nelyginis ir $0 \leq x \leq \left(\frac{p-1}{2}\right)$, $0 \leq y \leq \left(\frac{p-1}{2}\right)$. Tuomet egzistuoja toks sveikasis skaičius a, kad $ap = x^2 + y^2 + 1^2 + 0^2$. Kadangi

$$ap = x^2 + y^2 + 1^2 \leq \left(\frac{p-1}{2}\right)^2 + \left(\frac{p-1}{2}\right)^2 + 1 < \left(\frac{p}{2}\right)^2 + \left(\frac{p}{2}\right)^2 + 1 = \frac{p^2}{2} + 1 < p^2$$

tai $a < p$. □

17 teorema (Lagranžo)**.** *Kiekvieną neneigiamą sveikąjį skaičių galime išreikšti keturių sveikųjų skaičių kvadratų suma.*

Įrodymas. Pagal 16 išvadą, egzistuoja toks natūralusis skaičius $a < p$, kad $ap = x^2 + y^2 + 1^2 + 0^2$, čia p – pirminis ir x, y – sveikieji skaičiai.

Tarkime skaičius b yra toks mažiausias natūralusis skaičius, kad $b \leq a$ ir bp gali būti išreiškiamas keturių kvadratų suma.

Tarkime $b > 1$. Pažymėkime $bp = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Tegul y_i – skaičiaus x_i dalybos iš b liekana, $i = 1, 2, 3, 4$. Pažymėkime $x_i = r_i b + y_i$. Laikysime, kad $-b/2 < y_i \leq b/2$. Tada

$$bp = x_1^2 + x_2^2 + x_3^2 + x_4^2 =$$

$$(r_1 b + y_1)^2 + (r_2 b + y_2)^2 + (r_3 b + y_3)^2 + (r_4 b + y_4)^2 \equiv$$

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

Egzistuoja toks $c \geq 0$, kad $bc = y_1^2 + y_2^2 + y_3^2 + y_4^2$. Tada $bc \leq \left(\frac{b}{2}\right)^2 + \left(\frac{b}{2}\right)^2 + \left(\frac{b}{2}\right)^2 + \left(\frac{b}{2}\right)^2 = b^2$. Taigi $c \leq b$. Jei $c = 0$, tai $y_i = 0$ ir $x_i = r_i b$. Išplauktų

$p = b(r_1^2 + r_2^2 + r_3^2 + r_4^2)$ – prieštara, nes p – pirminis. Jei $c = b$, tada $y_i = b/2$. Pagal lyginį $x_i \equiv y_i \pmod{b}$ gautume:

$$bp = x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv \frac{b^2}{4} + \frac{b^2}{4} + \frac{b^2}{4} + \frac{b^2}{4} = b^2 \equiv 0 \pmod{b^2}$$

arba kitaip tariant b dalija p – prieštara. Todėl $0 < c < b$. Sudauginę lygtis $bp = x_1^2 + x_2^2 + x_3^2 + x_4^2$ ir $bc = y_1^2 + y_2^2 + y_3^2 + y_4^2$ bei pasinaudodami Oilerio keturių kvadratų sumų sandaugos tapatybe gauname:

$$b^2cp = (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 +$$

$$(x_1y_3 - x_2y_4 - x_3y_1 + x_4y_2)^2 + (x_1y_4 + x_2y_3 - x_3y_2 - x_4y_1)^2$$

Kadangi $x_i \equiv y_i \pmod{b}$, tai visi keturi dešinės pusės kvadratai dalijasi iš b^2. Suprastinę gauname, kad cp išreiškiamas keturių kvadratų suma. Tačiau tai prieštarautų prielaidai, jog b yra mažiausias natūralusis skaičius, kuriam bp gali būti išreiškiamas keturių tiksliųjų kvadratų suma. Taigi, $b = 1$ ir $p = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Tokiu būdu kiekvieną pirminį skaičių p galime išreikšti keturių tiksliųjų kvadratų suma. Pagal Oilerio tapatybę, tokių sumų sandauga yra keturių naujų tiksliųjų kvadratų suma. Taigi teorema įrodyta ne tik pirminiams, bet ir sudėtiniams skaičiams. □

Representation of a Positive Integer by a Sum of Perfect Squares

Summary

Waring's problem is one of the classical problems in number theory. Throughout history it's variations interest mathematicians and to this day it continues to be one of the most famous question in classical mathematics.

The aims of this work are to present the problem of positive integer representations by a sum of perfect squares and analyse various number theory methods, specifically used for proofs of Fermat's two square, Legendre's three square and Lagrange's four square theorems.

Literatūra

[1] R. Dedekind *Theory of Algebraic Integers,* Cambridge University Press (1996), 21-24

[2] Gauss, C. Friedrich *Disquisitiones Arithmeticae,* Yale University Press (1965), section 293

[3] K. Ireland, M. Rosen *A Classical Introduction to Modern Number Theory,* 2nd ed., Springer (1990), 278-286

[4] T. Murphy *Introduction to Number Theory,* lecture notes, Trinity College Dublin (2016), chapter 9, 1-12

[5] J. Suomalainen *Waring's Problem,* University of Helsinki (2016)

[6] J.J. Tattersall, *Elementary Number Theory in Nine Chapters,* 1st. ed., Cambridge University Press (1999), 182-197, 239-253