Hamletas Markšaitis

Neapibrėžtinės lygtys: algebrinės skaičių teorijos užuomazga

Seniausieji rasti matematiniai tekstai (molinėse lentelėse, papirusuose) rodo, kad jau apie XX a. pr. Kr. Senovės Rytuose matematika buvo pakankamai išvystyta. Palyginus su kaimynais, ypač daug buvo pasiekę babiloniečiai. Tuo metu jie aritmetiką buvo išrutulioję į algebrą, žinojo vadinamosios Pitagoro teoremos bendrąjį atvejį, mokėjo spręsti kvadratines, netgi kai kurias kubines bei bikvadratines lygtis ir taip toliau. Lygčių koeficientai būdavo parenkami taip, kad lygtys būtų išsprendžiamos natūraliaisiais arba teigiamais racionaliaisiais skaičiais. VI–III a. pr. Kr. babiloniečiai nepaprastai ištobulino astronomijos mokslo reikmėms būtiną skaičiavimo meną. Nors su skaičiais jie operavo apie 1500 metų, bet, pasirodo, nesuformulavo jokių bendrų skaičių dalumo ar kitokių savybių. Senovės Rytų matematikoje apskritai neaptikta jokių įrodymų. Uždaviniai būdavo sprendžiami žingsnis po žingsnio, kiekvienas jų būdavo atliekamas pagal tam tikrą taisyklę. Matematikos istorikams kol kas nepasisekė išaiškinti, kaip babiloniečiai įgijo matematinių žinių.

Euklido „Elementuose"(Stoicheia, III a. pr.Kr.) randamos ir pirmosios skaičių teorijos užuomazgos. Maždaug VI–III a. pr. Kr. graikai suformavo aksiomos sąvoką, įrodymo sampratą bei sukūrė gana darnų plokštumos ir erdvės geometrijos mokslą.

Visi šie laimėjimai susumuoti Euklido „Elementuose", kuriuos sudaro 13 knygų. Labai gerai žinoma, kokį poveikį Euklido „Elementai" padarė visai tolesnei matematikos raidai. Euklido „Elementų" VII–IX knygos skirtos skaičių teorijai. Jose dėstomi natūraliųjų skaičių dalumo klausimai. Panaudojus „Euklido algoritmą", VII knygoje įrodyta, kad egzistuoja bet kokių dviejų (ir daugiau) natūraliųjų skaičių bendrasis didžiausias daliklis (b.d.d.), taip pat ir bendrasis mažiausias kartotinis (b.m.k.).

Šiam faktui ekvivalentiškas geometrinis teiginys skamba taip: atkarpos, kurių ilgiai reiškiami natūraliaisiais skaičiais, yra bendramatės. Euklido algoritmu grindžiama ir daugelis kitų „Elementuose" išdėstytų tyrimų. Juose nurodytos kai kurios pirminių skaičių savybės, įrodyta, jog pirminių skaičių yra be galo daug ir t.t. Matyt, dėl netobulų to laiko žymenų ir sudėtingos terminologijos teorema apie natūraliųjų skaičių išskaidymą pirminiais skaičiais nebuvo suformuluota bei įrodyta. Ši teorema, paprastai vadinama pagrindine aritmetikos teorema, yra mokslo apie natūraliuosius, sveikuosius ir racionalinius skaičius pagrindas.

• • • $\alpha + \omega$ • • •

Euklido algoritmas

Euklido algoritmas pagrįstas dalybos su liekana formule. Tarkime, a_1, a_2 – sveikieji skaičiai, $a_2 > 0$. Tuomet egzistuoja sveikieji skaičiai b_2 ir a_3 tokie, kad

$$a_1 = a_2 b_2 + a_3, \qquad 0 \leq a_3 < a_2.$$

Pasinaudoję šia formule keletą kartų, galime parašyti:

$$\begin{aligned}
a_1 &= a_2 b_2 + a_3, && 0 \leq a_3 < a_2,\\
a_2 &= a_3 b_3 + a_4, && 0 \leq a_4 < a_3,\\
&\ldots\ldots\ldots\ldots\\
a_{k-2} &= a_{k-1} b_{k-1} + a_k, && 0 \leq a_k < a_{k-1},\\
a_{k-1} &= a_k b_k + 0.
\end{aligned}$$

Šių lygybių seka ir sudaro Euklido algoritmo esmę.

Jei skaičius d dalija skaičių a, sutarsime rašyti $d|a$, jei nedalija, – $d \nmid a$.

Įrodysime, kad paskutinė nelygi nuliui liekana a_k yra skaičių a_1, a_2 didžiausias bendrasis daliklis (d.b.d.). Dažnai skaičių a_1, a_2 didžiausias bendrasis daliklis apibrėžiamas kaip didžiausias natūralusis skaičius d, dalijantis ir a_1, ir a_2. Mums bus parankiau naudotis kitu d.b.d. apibrėžimu.

Apibrėžimas. *Skaičių d vadinsime skaičių $a_1, a_2, \ldots, a_n$ didžiausiu bendruoju dalikliu, jei jis turi šias savybes:*

1) $d|a_1, d|a_2, \ldots, d|a_n$;
2) *jei* $d'|a_1, d'|a_2, \ldots, d'|a_n$, *tai* $d'|d$.

Dabar nesunku įsitikinti, kad paskutinė nelygi nuliui liekana a_k yra skaičių a_1, a_2 d.b.d. Pirmiausia įsitikinsime, kad a_k turi pirmąją d.b.d. apibrėžimo savybę. Iš paskutinės Euklido algoritmo lygybės matome, kad $a_k|a_{k-1}$, iš priešpaskutinės – $a_k|a_{k-2}$ ir t. t. Taigi $a_k|a_2$ ir $a_k|a_1$.

Lieka įsitikinti, kad a_k turi ir antrąją d.b.d. savybę. Tarkime, $d'|a_1, d'|a_2$. Tuomet iš Euklido algoritmo pirmosios lygybės matome, kad $d'|a_3$, iš antrosios – $d'|a_4$ ir t.t. Tęsdami toliau gausime, $d'|a_k$.

Išvada. *Jei d yra skaičių a_1, a_2 d.b.d., tai egzistuoja tokie sveikieji skaičiai u_1, u_2, kad*

$$d = u_1 a_1 + u_2 a_2.$$

Pritaikę skaičiams a_1, a_2 Euklido algoritmą, tarkime, $d = a_k$. Iš anksčiau parašytų lygybių gauname:

$$\begin{aligned}
d = a_k &= a_{k-2} - a_{k-1} b_{k-1} = a_{k-2} - (a_{k-3} - a_{k-2} b_{k-2}) b_{k-1}\\
&= -a_{k-3} b_{k-1} + a_{k-2}(1 + b_{k-1} b_{k-2}) = \ldots = a_1 u_1 + a_2 u_2.
\end{aligned}$$

• • • $\alpha + \omega$ • • •

Pagrindinė aritmetikos teorema

Formuluojant uždavinius bei pateikiant atsakymus, patogu remtis pagrindine aritmetikos teorema. Tad šiame skyrelyje ją suformuluosime ir įrodysime.

Apibrėžimas. *Natūralųjį skaičių $p > 1$ vadinsime pirminiu, jei p dalijasi tik iš* 1 *ir p.*

Įrodysime svarbią pirminių skaičių savybę.

Teorema. *Jei pirminis p dalija natūraliųjų skaičių a ir b sandaugą ab, tai p dalija bent vieną iš skaičių a, b.*

Įrodymas. Jei $p|a$, įrodymas baigtas. Jei $p \nmid a$, tai p ir a d.b.d. lygus 1. Pasirėmę ankstesnio skyrelio išvada, gauname, jog egzistuoja tokie u_1, u_2, kad

$$1 = au_1 + pu_2.$$

Padauginę šią lygybę iš b, gausime

$$b = abu_1 + pbu_2.$$

Kadangi p dalija abu šios lygybės dešinės pusės dėmenis, tai dalija ir jų sumą b.

Pagrindinė aritmetikos teorema. *Kiekvieną natūralųjį skaičių a galime vieninteliu būdu užrašyti pirminių skaičių sandauga*

$$a = p_1 p_2 \cdot \ldots \cdot p_r, \qquad p_1 \leq p_2 \leq \ldots \leq p_r.$$

Pastabos.

1. Į skaičiaus $a = 1$ skaidinį neįeina nė vienas pirminis skaičius.
2. Vienas ir tas pats pirminis skaičius p skaičiaus a skaidinyje gali pasikartoti. Skaičiaus p pasikartojimų skaičių a skaidinyje vadinsime skaičiaus p kartotinumu. Tada galime parašyti
$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s};$$
čia: $p_1, p_2, \ldots, p_s$ – skirtingi pirminiai skaičiai, $\alpha_1 > 0, \alpha_2 > 0, \ldots, \alpha_s > 0$ – jų kartotinumai. Šis vienintelis a skaidinys vadinamas <u>*kanoniniu*</u>. Analogiškai kiekvieną sveiką skaičių $a \neq 0$ galime vieninteliu būdu užrašyti taip:
$$a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}.$$
3. Jeigu $a \neq 0$ yra racionalusis skaičius, tai jis vieninteliu būdu užrašomas taip:
$$a = \pm \frac{p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}}{q_1^{\beta_1} q_2^{\beta_2} \cdot \ldots \cdot q_r^{\beta_r}};$$

• • • $\alpha + \omega$ • • •

čia: $p_1, \ldots, p_s, q_1, q_2, \ldots, q_r$ – skirtingi pirminiai skaičiai, $\alpha_1, \ldots, \alpha_s$, $\beta_1, \ldots, \beta_r$ – natūralieji. Tarę, jog sveikieji skaičiai $\alpha_1 \neq 0, \alpha_2 \neq 0, \ldots, \alpha_t \neq 0$ gali būti tiek teigiami, tiek neigiami, racionaliojo skaičiaus $a \neq 0$ skaidinį galima taip užrašyti:

$$a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_t}.$$

Pagrindinės aritmetikos teoremos įrodymas. Pirmiausia įrodysime, kad kiekvieną natūralųjį skaičių galima išskaidyti į pirminių skaičių sandaugą, o po to – skaidinio vienatį. Į skaičiaus $b = 1$ skaidinį neįeina nė vienas pirminis skaičius, o skaičius $b = 2$ yra pats pirminis. Taigi pagrindinė aritmetikos teorema yra teisinga, kai $b = 1, 2$. Tarsime, kad ji teisinga visiems $b < a$ ir įrodysime, kad tada ji taip pat teisinga ir natūraliajam a.

Galimi du atvejai:

1) skaičius a yra pirminis;
2) skaičius a nėra pirminis.

Pirmuoju atveju skaičius jau išskaidytas į pirminių sandaugą. Antruoju atveju egzistuoja skaičiai $a' < a, a'' < a$, kad $a = a'a''$. Pagal prielaidą skaičių a', a'' skaidiniai pirminiais egzistuoja. Tada iš jų galime sudaryti ir skaičiaus a skaidinį.

Dabar įrodysime, kad skaidinys yra vienintelis, t. y., jei

$$a = p_1 p_2 \cdot \ldots \cdot p_s = q_1 q_2 \cdot \ldots \cdot q_r \tag{1}$$

yra du skaidiniai pirminiais skaičiais ir daugikliai išdėstyti nemažėjančia tvarka, tai $s = r$ ir $p_i = q_i$ kiekvienam i. Tarkime $p_1 < q_1$, tada

$$p_1 | q_1 q_2 \cdot \ldots \cdot q_r,$$

bet $p_1 \nmid q_i, i = 1, \ldots r$. Iš anksčiau įrodytos teoremos išplaukia, jog taip negali būti. Tada $p_1 \geq q_1$. Analogiškai įsitikinsime, kad nelygybė $p_1 > q_1$ taip pat negalima. Tada $p_1 = q_1$, ir suprastinę lygybę (1) iš p_1, gausime

$$p_2 \cdot \ldots \cdot p_s = q_2 \cdot \ldots \cdot q_r.$$

Pakartoję ankstesnius samprotavimus, gausime $p_2 = q_2$ ir lygybę galėsime vėl suprastinti. Jeigu būtų $s \neq r$, tai po baigtinio skaičiaus prastinimų gautume lygybę, kurios vienoje pusėje būtų vienetas, o kitoje – keleto pirminių skaičių sandauga. Kadangi tokia lygybė negali galioti, tai $s = r$.

Teorema įrodyta.

Šiuolaikinė skaičių teorija buvo pradėta kurti tik XIX a. po Kr. ir intensyviai plėtojama XIX–XX a. Jos atsiradimą skatino algebrinių lygčių (arba tokių lygčių sistemų), kurių koeficientai yra sveikieji skaičiai ir kurių sprendiniai – taip pat sveikieji skaičiai, tyrimas. Lygtys (lygčių sistemos), jeigu jose nežinomųjų yra daugiau negu lygčių, dažnai vadinamos neapibrėžtinėmis lygtimis. Apžvelgsime kai kurių neapibrėžtinių lygčių pavyzdžius. Formuluodami uždavinius arba uždavinių atsakymus, remsimės pagrindine aritmetikos teorema.

• • • $\alpha + \omega$ • • •

Pitagoro trejetai

Neapibrėžtinę lygtį

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

babiloniečiai žinojo jau XX–XV a. pr. Kr. Jų sudarytose šios lygties sprendinių lentelėse nurodytas sprendinys (4961, 6480, 8161). Vargu ar įmanoma atspėti tokį sprendinį, nežinant šios lygties sprendinių sudarymo taisyklės.

Ši lygtis buvo žinoma ir Antikos graikams. Pitagoras (apie 530–510 m. pr. Kr.) žinojo, kaip sudaryti šios lygties sprendinius. Apie juos taip pat rašoma ir Euklido „Elementų" X knygoje.

Ši lygtis sutinkama taip pat ir Diofanto (Diophanti, apie 250 m.) „Aritmetikoje". Išliko tik 6 šio veikalo knygos, kiek jų buvo – spėliojama. Lygtis suformuluota II knygos 8 uždavinyje. P. Ferma (Pierre de Fermat, 1601–1665) skaitydamas Diofanto „Aritmetiką" šio uždavinio paraštėje užrašė pastabą (tai antroji pastaba iš 48). Mūsų laikų žymenimis ši pastaba būtų formuluojama taip:

lygtis $x^n + y^n = z^n$, $n > 2$, *neturi sprendinių natūraliaisiais skaičiais.*

Tai garsioji Ferma problema, arba – paskutinė Ferma teorema.
Dabar aptarsime lygties $x^2 + y^2 = z^2$ sprendinius bei jų sudarymo būdus.

Lygties sprendinį (x_0, y_0, z_0), jei x_0, y_0, z_0 yra natūralieji skaičiai, kurių d.b.d. lygus 1, vadinsime **primityviuoju Pitagoro trejetu**. Jeigu (x_0, y_0, z_0) yra lygties sprendinys, o t_0 – natūralusis skaičius, tai (t_0x_0, t_0y_0, t_0z_0) taip pat yra lygties sprendinys. Šį skaičių trejetą vadinsime tiesiog **Pitagoro trejetu**. Kiekvienas Pitagoro trejetas duoda 8 lygties sprendinius sveikaisiais skaičiais, kuriuos gauname daugindami Pitagoro trejeto komponentes iš ± 1. Šitaip gaunami visi lygties $x^2 + y^2 = z^2$ sprendiniai sveikaisiais skaičiais. Belieka aptarti primityviųjų Pitagoro trejetų sudarymo metodą.

Pastebėkime, jog, jei natūralieji skaičiai x, y, z tenkina lygtį, tai bent vienas iš jų yra lyginis. Sutarkime, kad nagrinėsime tik tuos primityviuosius Pitagoro trejetus (x_0, y_0, z_0), kuriems y_0 yra lyginis. Tokių primityviųjų Pitagoro trejetų aibę nesunku apibrėžti. Ji sutampa su trejetų

$$(p^2 - q^2, 2pq, p^2 + q^2),$$

kur $p > q \geq 1$ yra skirtingo lyginumo natūralieji skaičiai, p, q d.b.d lygus 1, aibe. Sukeitę šių trejetų pirmąsias dvi komponentes vietomis, gausime kitus primityviuosius Pitagoro trejetus.

Toks yra atsakymas. Dabar panagrinėsime, kokiu būdu jis gaunamas. Vienas iš sprendinių radimo būdų – geometrinis. Kadangi trivialus sprendinys (0, 0, 0) mūsų nedomina, perrašykime mūsų lygtį šitaip:

$$\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1.$$

Taigi spręsti lygtį $x^2 + y^2 = z^2$ sveikaisiais skaičiais yra tas pats, kas spręsti lygtį

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

• • • $\alpha + \omega$ • • •

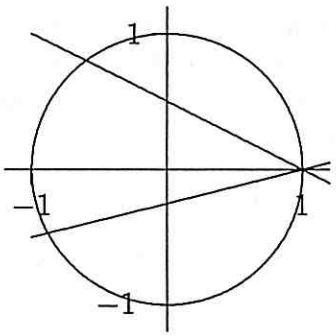
racionaliaisiais skaičiais. Pastaroji lygtis plokštumoje apibrėžia antros eilės kreivę – apskritimą. Nagrinėkime tiesių, einančių per šio apskritimo tašką $(1,0)$, pluoštą

$$\frac{x-1}{a} = \frac{y}{b}, \quad a, b \neq 0, \quad a,\ b \text{ sveiki skaičiai, } d.b.d. \text{ lygus } 1.$$

Pažymėję

$$\frac{x-1}{a} = \frac{y}{b} = t,$$

kiekvienos tiesės lygtį parašysime parametrine forma: $x = 1 + at, y = bt$. Kiekviena tiesė kerta apskritimą dviejuose taškuose: taške $(1,0)$ ir dar viename taške, žr. brėžinį.



Surasime pastarąjį tašką. Tam tereikia išspręsti lygčių su trimis nežinomaisiais sistemą:

$$\begin{cases} x^2 + y^2 = 1, \\ x = 1 + at, \\ y = bt. \end{cases}$$

Išsprendę gausime dvi parametro t reikšmes: $t = 0$ ir $t = -2a/(a^2 + b^2)$. Jas atitinka bendrieji tiesės ir apskritimo taškai:

$$(0,1), \quad \Big(\frac{b^2 - a^2}{a^2 + b^2}, -\frac{2ab}{a^2 + b^2}\Big).$$

Iš antrojo taško gauname šiuos lygties $x^2 + y^2 = z^2$ sprendinius:

$$(a^2 - b^2, -2ab, a^2 + b^2), \quad (a^2 - b^2, 2ab, a^2 + b^2).$$

Kitas lygties sprendimo būdas yra analizinis. Jis yra kur kas ilgesnis. Tačiau aukštesnio laipsnio neapibrėžtines lygtis galima išspręsti tik šiuo būdu.

Kvadratų sumos ir kiti uždaviniai

Kokie natūralieji skaičiai gali būti užrašomi dviejų natūraliųjų skaičių kvadratų suma, arba

kokiems natūraliesiems n lygtis $n = x^2 + y^2$ išsprendžiama natūraliaisiais skaičiais?

Apie atskirus šio uždavinio atvejus rašoma Diofanto „Aritmetikoje". Atsakymą bendru atveju suformulavo A. Žiraras (Albert Girard, 1595–1632) ir keletu metų vėliau P. Ferma, matyt, nepriklausomai nuo A. Žiraro. P. Ferma tvirtino žinąs ir įrodymą, bet jo įrodymas nebuvo rastas. A. Žiraro ir P. Ferma atsakymas toks:

duotasis skaičius n yra dviejų natūraliųjų skaičių kvadratų suma tada ir tik tada, kai n yra arba kvadratas, arba $4k + 1$ pavidalo pirminis skaičius, arba skaičius 2, arba tokių skaičių sandauga.

Pasirėmę pagrindine aritmetikos teorema, galime pasakyti trumpiau:

natūralusis skaičius n yra dviejų natūraliųjų skaičių kvadratų suma tada ir tik tada, kai į jo kanoninį skaidinį pirminiai $4k + 3$ pavidalo skaičiai įeina lyginiu laipsniu.

Šią gražią teoremą pirmas įrodė L. Oileris (Leonhard Euler, 1707–1783) 1747 m. Šios teoremos įrodyme L. Oileris nesinaudoja jokia sudėtinga teorija. Šia prasme įrodymas yra elementarus, tačiau nėra paprastas.

Išskirkime vieną šios teoremos atvejį. Kiekvienas nelyginis pirminis skaičius pakliūna į vieną iš progresijų

$$5, 9, \ldots, 4k + 1, \ldots$$
$$3, 7, \ldots, 4k + 3, \ldots$$

Iš Oilerio teoremos išplaukia, jog tie ir tik tie nelyginiai pirminiai skaičiai, kurie priklauso progresijai $4k+1, k = 1, 2, \ldots$, yra dviejų natūraliųjų skaičių kvadratų sumos, gi nė vienas pirminis skaičius iš progresijos $4k + 3$, $k = 0, 1, 2, \ldots$, negali būti tokiu būdu užrašytas. Šis įdomus ir intriguojantis faktas yra nepaprastai gražios ir gilios – klasių kūnų teorijos fragmentas. Ši teorija – algebrinės skaičių teorijos viršūnė.

Dabar galime suformuluoti be galo daug uždavinių, panašių į ką tik nagrinėtąjį.

Tegu d yra natūralusis skaičius, nesidalijantis iš jokio natūraliojo skaičiaus $m > 1$ kvadrato. Kokiems n lygtis $n = x^2 + dy^2$ išsprendžiama natūraliaisiais skaičiais?

Šį uždavinį nagrinėjo P. Ferma. Pasirodo, net skaičiams $d = 2, 3$ reikėjo individualių šio uždavinio sprendimo metodų. Ypač sunkus atvejis $d = 5$. P. Ferma ir šiuo atveju teisingai suformulavo atsakymą, nors jis labai sudėtingas. Tik algebrinės skaičių teorijos požiūriu galima paaiškinti, kodėl taip yra. Vien tik šioms d reikšmėms $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$ nagrinėjamojo uždavinio sprendimo būdai yra palyginti paprasti, o atsakymai panašūs į suformuluotą Oilerio teoremą.

Kongruentieji ir kitokie skaičiai

Ferma paskutinės teoremos įrodymo matematikai ieškojo daugiau nei 300 metų. Tik visiškai neseniai ją pagaliau pavyko įrodyti. Dabar suformuluosime uždavinį, kuris nėra toks populiarus kaip paskutinė Ferma teorema, nors jam jau daugiau nei 2000 metų.

Apibrėžimas. *Skaičių a vadinsime kongruenčiuoju, jei jis lygus stačiojo trikampio, kurio kraštinės reiškiamos racionaliaisiais skaičiais, plotui.*

• • • $\alpha + \omega$ • • •

Tarkime, x, y, z yra stačiojo trikampio kraštinių ilgiai. Tuomet $x^2 + y^2 = z^2$ (Pitagoro teorema), o trikampio plotas lygus $xy/2$. Vadinasi, racionalusis skaičius a yra kongruentusis skaičius, jei sistema

$$\begin{cases} \dfrac{xy}{2} = a, \\ x^2 + y^2 = z^2 \end{cases}$$

išsprendžiama racionaliaisiais skaičiais.

Jeigu kongruentųjį skaičių a atitinkančio stačiojo trikampio kraštinių ilgiai yra x, y, z, tai pasirėmę pagrindine aritmetikos teorema bei kiek pagalvoję, galėsime tvirtinti, kad atsiras toks racionalusis skaičius t, kad stačiojo trikampio su kraštinėmis tx, ty, tz plotas bus sveikas skaičius

$$n = p_1 p_2 \dots p_s;$$

čia $p_1, p_2, \dots, p_s$ skirtingi pirminiai skaičiai. Apsiribokime tik tokio pavidalo kongruenčiaisiais skaičiais ir uždavinį formuluokime taip:

nurodyti algoritmą, kuriuo būtų galima nustatyti, ar skaičius $n = p_1 p_2 \dots p_s$, *čia* $p_1, \dots, p_s$ *skirtingi pirminiai skaičiai, yra kongruentusis ar ne.*

Iš pirmo žvilsnio šis uždavinys atrodo keistokai. Juk lygtį $x^2 + y^2 = z^2$ mokame spręsti tiek sveikaisiais, tiek racionaliaisiais skaičiais. Galime nurodyti algoritmą, kuris įgalintų nuosekliai rašyti lygties $x^2 + y^2 = z^2$ sveikuosius sprendinius. Juos radę, apskaičiuotume skaičius $xy/2$, o išskyrę, jei reikalinga, kvadratą, surastume ir norimo pavidalo kongruenčiuosius skaičius. Pateiksime tokių skaičiavimų pavyzdžių.

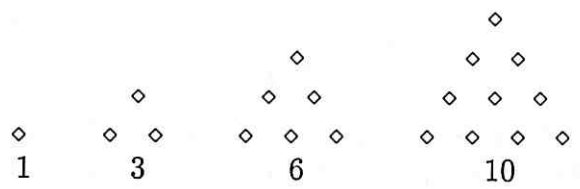
p	q	x	y	z	$xy/2$	n
2	1	3	4	5	6	6
3	2	5	12	13	30	30
4	1	15	8	17	60	15
4	3	7	24	25	84	21
5	2	21	20	29	210	210
5	4	9	40	33	180	5
6	1	35	12	37	210	210
6	5	11	60	71	330	330
7	2	45	28	53	630	70
7	4	33	56	65	924	231
7	6	13	84	85	546	546

Lentelėje $x = p^2 - q^2, y = 2pq, z = p^2 + q^2, xy/2 = pq(p^2 - q^2)$, o paskutiniame stulpelyje užrašytas skaičius, gautas iš $xy/2$, išskyrus kvadratą. Taigi paskutiniame stulpelyje gauname kongruenčius skaičius, nesidalijančius iš kvadratų. Pavyzdžiui, jei norėtume nustatyti, ar $n = 17$ yra kongruentinis skaičius, tektų skaičiuoti ir kantriai laukti, kol šis skaičius pasirodys paskutiniame stulpelyje. Tačiau jis gali visai nepasirodyti arba pasirodyti tik atlikus labai daug skaičiavimų!

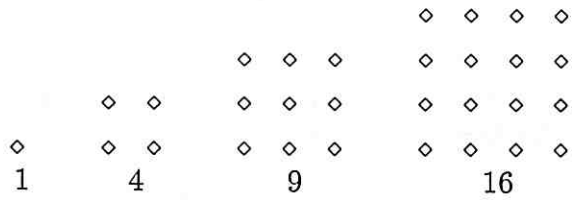
• • • $\alpha + \omega$ • • •

1983 metais J. Tunelis (J. Tunnell) įrodė, jog kongruentieji skaičiai, nesidalijantys iš kvadratų, tenkina tam tikrą sąlygą, kurią galima skaičiuojant patikrinti. Tačiau nežinoma, ar ši sąlyga yra pakankama, kad ją tenkinantis skaičius būtų kongruentus. Tai priklauso nuo elipsinių kreivių $y^2 = x^3 + ax + 6$ kol kas dar nežinomų savybių.

Pitagoriečiai sugalvojo „trikampius“, „keturkampius“ ir kitokius skaičius, susiejančius geometriją su aritmetika.



„Trikampiai“ skaičiai



„Keturkampiai“ skaičiai

Tegu $a_1^{(n)}, a_2^{(n)}, \ldots, a_j^{(n)}, \ldots$ yra „n-kampių“ skaičių seka. Nesunku įsitikinti, kad

$$a_j^{(n)} = j + (n-2)\frac{j(j-1)}{2}, \qquad j = 1, 2, \ldots.$$

P. Ferma suformulavo labai įdomų teiginį: kiekvieną natūralųjį skaičių N galima užrašyti ne daugiau kaip n „n-kampių“ skaičių suma.

Atveju $n = 3$ teiginį įrodė K. Gausas (Carl Friedrich Gauß, 1777–1855). Atveju $n = 4$ įrodymą pateikė J. Lagranžas (Joseph Louis Lagrange, 1736–1813.) Bendruoju atveju uždavinį išsprendė A. Koši (Augustin Cauchy, 1789–1857).

Taigi kiekvieną natūralųjį skaičių galima užrašyti ne daugiau kaip 4 natūraliųjų skaičių kvadratų suma.

Vietoje plokštumos figūrų galima nagrinėti erdvinius taisyklingus kūnus ir apibrėžti „erdvinius“ skaičius.

Dar apie neapibrėžtines lygtis

Tegu natūralusis skaičius d nesidalija iš jokio didesnio už 1 natūraliojo skaičiaus kvadrato. Nagrinėkime lygtį

$$x^2 - dy^2 = 1.$$

Šią lygtį galima spręsti tiek sveikaisiais, tiek racionaliaisiais skaičiais. Įsitikinsime, kad tai iš tiesų yra du iš esmės skirtingi uždaviniai. Tai labai gerai žinojo P. Ferma.

• • • $\alpha + \omega$ • • •

Išpręsime lygtį racionaliaisiais skaičiais, pasinaudoję kaip anksčiau geometriniu metodu. Plokštumoje lygtis apibrėžia antros eilės kreivę, kuriai priklauso taškas (1, 0). Nagrinėsime tiesių, einančių per šį tašką, pluoštą:

$$\frac{x-1}{a} = \frac{y}{b}, \quad a, b \neq 0, \quad a,\ b \text{ sveiki skaičiai, } d.b.d. \text{ lygus 1.}$$

Pažymėję

$$\frac{x-1}{a} = \frac{y}{b} = t,$$

kiekvienos tiesės lygtį parašysime parametrine forma: $x = 1 + at, y = bt$ ir ieškosimė šios tiesės bei kreivės susikirtimo taškų. Tai darysime spręsdami sistemą t atžvilgiu:

$$\begin{cases} x^2 - dy^2 = 1, \\ x = 1 + at, \\ y = bt. \end{cases}$$

Išsprendę gausime dvi parametro t reikšmes: $t = 0$ ir $t = 2a/(db^2 - a^2)$. Juos atitinka bendrieji tiesės ir antros eilės kreivės taškai:

$$(0, 1), \quad \left(\frac{db^2 + a^2}{db^2 - a^2}, \frac{2ab}{db^2 - a^2}\right).$$

Jei a, b yra sveikieji (racionalieji) skaičiai, tai antrasis taškas yra lygties $x^2 - dy^2 = 1$ sprendinys.

Jei sveikuosius a, b pavyktų parinkti taip, kad $db^2 - a^2 = \pm 1$, tai gautume lygties sprendinį sveikaisiais skaičiais. Tačiau tokių a, b parinkimas yra ekvivalentus pradinės lygties sprendimui sveikaisiais skaičiais. Tai gali būti itin nelengva. Pavyzdžiui, lygties

$$x^2 - 61y^2 = 1$$

sprendinys mažiausiais natūraliaisiais skaičiais yra toks: (1766319049, 226153980). Įspūdingi skaičiai! Patikrinkite!

Yra žinomi metodai, kuriais galima surasti bent vieną lygties $x^2 - dy^2 = 1$ sprendinį sveikaisiais skaičiais. Žinant bent vieną sprendinį sveikaisiais (arba racionaliaisiais) skaičiais, galima tokių sprendinių sudaryti be galo daug. Jei $(x_1, y_1), (x_2, y_2)$ yra du skirtingi arba vienodi lygties $x^2 - dy^2 = 1$ sprendiniai, tai

$$(x_1x_2 - dy_1y_2, -x_1y_2 + x_2y_1)$$

yra taip pat šios lygties sprendinys. Reikia labiau įsigilinti į algebrinę skaičių teoriją, kad paaiškėtų kodėl taip yra.

K.F. Gauso „Disquisitiones Arithmeticae“

Mūsų apžvalgos pradžioje aptarėme garsiuosius Euklido „Elementus“. Dabar aptarsime 1801 metais išleistą K. F. Gauso veikalą „Disquisitiones Arithmeticae“, kuriuo buvo sukurti skaičių teorijos pagrindai.

K. F. Gauso „Disquisitiones Arithmeticae“ sudaro septynios dalys.

Pirmojoje dalyje pateikiami įvairūs apibrėžimai, dalumo iš 3, 9, 11 požymiai, lyginių natūraliojo skaičiaus moduliu apibrėžimas bei pagrindinės savybės.

Antrojoje dalyje įrodyta pagrindinė aritmetikos teorema, nagrinėjami pirmos eilės lyginiai su nežinomaisiais. Nurodyta, kaip tokius lyginius spręsti naudojantis Euklido algoritmu. Taip pat pažymima, kad spręsti galima ir su grandininių trupmenų pagalba. Nagrinėjama Oilerio funkcija $\phi(m)$, lygi natūraliųjų skaičių, mažesnių už m ir turinčių su m d.b.d, lygų 1, skaičiui.

Trečiojoje dalyje nagrinėjami lyginių laipsniai, įrodoma „mažoji“ Ferma teorema, apibrėžiama primityvioji liekanų klasė pirminio skaičiaus p moduliu, apibrėžiamas lyginių klasės indeksas ir t.t.

Ketvirtojoje dalyje įrodytas kvadratinis apverčiamumo dėsnis, paties K. Gauso pavadintas „auksine teorema“ (theorema aurea). XIX–XX a. matematikai padėjo daug pastangų aukštesnių eilių apverčiamumo dėsniams surasti.

Penktojoje ir šeštojoje dalyse išdėstyti nepaprastai įdomūs faktai apie kvadratines formas $f(x) = ax^2 + 2bxy + cy^2$.

Septintojoje dalyje tiriamas klausimas, kokiems pirminiams p apskritimą galima padalyti į p lygių dalių, naudojant tik liniuotę ir skriestuvą. Šis uždavinys su $p = 17$ buvo žinomas dar Antikos matematikams. K. Gausui pirmajam pavyko jį išspręsti. Tačiau jis išnagrinėjo ne tik šį, bet ir bendrąjį atvejį bei nustatė, koks turi būti pirminis p, kad apskritimo padalijimas būtų įmanomas. Be to, šioje dalyje užrašytas gan paslaptingas sakinys: „tą patį galima padaryti ir su lemniskate“. N. Abelis (Niels Henrik Abel, 1802–1829) labai susidomėjo šia pastaba ir išaiškino gilią jos prasmę. N. Abelis, K. Gausas ir K. Jakobis (Carl Gustav Jacobi, 1804–1851) nepriklausomai vienas nuo kito sukūrė elipsinių funkcijų teoriją (elipsinių kreivių teoriją), kuri suvaidino svarbų vaidmenį ieškant paskutinės Ferma teoremos įrodymo.

Po K.F. Gauso veikalo „Disquisitiones Arithmeticae“ pasirodymo ir kitų jo tyrimų skaičių teorijoje prasidėjo intensyvus tiriamasis darbas. Viena vertus, buvo ieškoma aukštesnės eilės apverčiamumo dėsnių, kita vertus – buvo bandoma įrodyti paskutinę Ferma teoremą. Visos šios pastangos ypač skatino algebrinės skaičių teorijos atsiradimą.

• • • $\alpha + \omega$ • • •

Apie Gauso stilių

„Gausas visada stengėsi suteikti savo tyrimams tobulo meno kūrinio formą, kitaip jis nenurimdavo. Jis nepaskelbė nė vieno savo darbo, kol tas nebuvo įgijęs trokštamos formos. Jis mėgo sakyti, kad prie baigto statyti pastato pastoliai neturi būti matomi."

S. Valtershauzenas (Sartorius von Waltershausen)

„Jis daro kaip lapė, kuri uodega užtrina savo pėdsakus smėly."

N. Abelis (Niels Henrik Abel)