Reinhard Laubenbacher
David Pengelley

Paskutinė Fermat teorema

Mūsų autoriai – New Mexico universiteto (JAV) profesoriai, parašę straipsnių ir knygų apie matematikos istoriją ir jos dėstymą universitetuose. Matematikos istorijos kursas, kurį jie skaito savo universitete, vadinasi „Didžiosios teoremos: matematikos menas“. Nuo kitų matematikos istorijos kursų jis skiriasi tuo, kad studentai skaito ir nagrinėja originalius įvairių epochų matematikų darbus. Tai suteikia galimybę pajausti, koks sudėtingas ir painus yra matematinių ieškojimų kelias, ir moko vertinti mūsų akimis žiūrint paprastas, tačiau nelengvai sukurtas sąvokas ir idėjas. Žurnale spausdinamas tekstas – tai skyrius iš autorių knygos;[1] išvertėme jį ir skelbiame autoriams ir leidyklai maloniai sutikus.

1993 metų birželio 24 dienos laikraščio *New York Times* pirmajame puslapyje buvo išspausdintas straipsnis antrašte „Senos matematinės paslapties tyrinėtojai pagaliau sušuko: Eureka!“ Legendinis šūksnis prieš vieną dieną nuskambėjo Anglijoje, Kembridžo universiteto miestelyje. Prinstono matematikas Andrew Wiles, baigdamas paskaitų ciklą nedidelėje konferencijoje mįslingu pavadinimu „p-adžiosios Galois reprezentacijos, Iwasawa teorija ir Tamagawa skaičiai“, lyg tarp kitko paminėjo, kad iš jo išdėstytų rezultatų išplaukia, jog paskutinė Fermat teorema teisinga. Beveik akimirksniu telefonu ir elektroniniu paštu ši žinia, kurią dauguma matematikų linkę laikyti labiausiai jaudinančiu XX amžiaus matematikos įvykiu, apskriejo Žemės rutulį. Straipsnio pabaigoje mes dar grįšime prie jo.

Paskutinė Fermat teorema, šio jaudulio židinys, formuluojama paprastai. Ji tvirtina, kad lygtis

$$x^n + y^n = z^n$$

neturi sprendinių sveikais skaičiais $x, y, z, xyz \neq 0$, jeigu tik rodiklis n yra didesnis už du natūralusis skaičius. Iki tos 1993 metų birželio dienos šį teiginį būtų buvę teisingiau vadinti hipoteze, nes, nepaisant geriausių pasaulio matematikų pastangų, per 300 metų nuo to momento, kai pirmojoje XVII amžiaus pusėje Pierre de Fermat ją paskelbė, niekam nepavyko jos įrodyti.

Kas buvo Fermat ir kas jį paskatino suformuluoti tokį keistą teiginį? Prancūzas Pierre de Fermat (1601–1665) buvo vienas iš didžiųjų matematikos istorijos veikėjų. Savo darbais jis darė esminę įtaką perėjimui nuo klasikinės graikų

[1] R. Laubenbacher, D. Pengelley, *Mathematical Expeditions: Chronicles by the Explorers*, Springer Verlag, 1998.

tradicijos prie visiškai naujo požiūrio į matematiką, kuris įsivyravo Europoje XVII amžiuje. Šešioliktajame amžiuje ir septynioliktojo amžiaus pradžioje daugiausia pastangų buvo skirta klasikinės Graikijos matematinių tekstų – Euklido, Apolonijaus, Papo, Ptolemėjaus ir Diofanto iš Aleksandrijos veikalų – vertimui į lotynų kalbą, jų atkūrimui bei papildymui. Pats Fermat irgi ėmėsi keleto tokių atkuriamųjų darbų. Vienas iš jų – Apolonijaus veikalas „Plokštumos vietos" (*Plane loci*). Net XVII amžiaus pradžioje tokie veikalai buvo laikomi matematinės kūrybos viršūnėmis.

Septynioliktojo amžiaus matematikų bendruomenė visiškai skyrėsi nuo dabartinės. Matematiko profesijos su tam tikrais standartais ir nusistovėjusia darbų publikavimo bei tarpusavio bendravimo sistema nebuvo. Maža to, matematika nebuvo aiškiai suvokiama kaip atskira disciplina, nebuvo jokio susitarimo, ką reiktų laikyti matematika. Vargu ar kas galėjo pragyventi vien iš matematinių tyrinėjimų, tad žmonės matematika užsiiminėjo dėl įvairių priežasčių. Universitetuose buvo dėstomi matematikos pagrindai, reikalingi teisės, medicinos ir teologijos laipsniams įgyti. Pasakojant apie Fermat gyvenimą, paprastai pabrėžiama, kad jis buvo „mėgėjas", todėl jo nuveikti darbai atrodo dar įspūdingesni. Tačiau akivaizdu, kad šio termino dabartinė reikšmė negali būti siejama su jo gyvenimo laikotarpiu.

Fermat teisės mokslų laipsnį gavo 1631 metais Orleano universitete, Prancūzijoje, ir po to persikėlė į Tulūzą, kur praleido likusį savo gyvenimą, reguliariai išvykdamas į kitus miestus. Jis užsiėmė teise ir greitai tapo Parlamento – Tulūzos provincijos aukštesniojo teismo – patarėju. Šiame poste išliko iki pat mirties. Taigi savo matematinius tyrinėjimus jis galėjo vykdyti tik laisvalaikiu; buvo ilgų laikotarpių, kai profesinės pareigos neleido jam grįžti prie matematikos. Daugelis požymių rodo, kad Fermat domėjosi matematika iš dalies norėdamas atitrūkti nuo profesinių pareigų, savo malonumui. Nors jis džiaugėsi daugelio to laikotarpio matematikų dėmesiu ir pagarba, bet niekada nesistengė savo rezultatų publikuoti. Jis niekada nekeliavo į matematinės veiklos centrus, nevyko net į Paryžių, pasitenkindamas ta bendravimo su mokslo visuomene galimybe, kurią suteikė laiškai. Ypač daug jam padėjo teologas Marin Mersenne (1588–1648), kuris, gyvendamas Paryžiuje, buvo tarsi visos Europos mokslinės korespondencijos paskirstymo punktas.

Didžiausią įtaką matematiniam Fermat gyvenimui darė François Viète (1540–1603) ir jo mokykla Bordo mieste. Su Viète mokiniais jis susipažino 1620 metų pabaigoje ilgai viešėdamas Bordo. 1591 metais Viète išspausdino savo „Analizės meno įvadą" – pirmąjį iš keleto traktatų, kuriuose išplėtojo naują simbolinės algebros sistemą, žadančią didelę matematinių atradimų galimybę. Įvade jis rašė:

> Yra tam tikras matematinių tiesų ieškojimo metodas, kurį, kaip yra sakoma, pirmasis atrado Platonas. Theonas vadino jį analize, apibrėždamas jį kaip tyrinėjimą, prasidedantį nuo prielaidos, kad tai, ko ieškoma, jau yra duota, ir kurio metu daromos išvados, kol gaunama tai, kas tikrai yra visų žinoma. Šis būdas yra priešingas sintezei, kuri yra tyrinėjimas, prasidedantis nuo tikrai žinomų dalykų ir kurio metu

gaunama bei suvokiama, tai kas yra ieškoma.

Nors senieji meistrai pateikia tik dvi analizės rūšis – zetetiką ir poristiką – kurioms Theono apibrėžimas geriausiai tinka, aš pridėjau dar ir trečiąją, kurią būtų galima vadinti rhetika, arba egzegetika. Žinomųjų dydžių ir ieškomojo dydžio lygtis ar proporcija sudaroma naudojantis zetetika. Poristika naudojamasi tikrinant teoremos teisingumą lygtimi ar proporcija. Nežinomo dydžio reikšmė iš žinomos lygties ar proporcijos randama remiantis egzegetika. Taigi visas analizės menas, turint galvoje tris jo dalis, gali būti pavadintas teisingų matematinių atradimų mokslu ([21], 11–12).

Viète veikalas yra svarbi perėjimo nuo senosios prie moderniosios matematikos gairė, nors jis ir neturėjo labai didelės įtakos to meto mokslinei bendruomenei, o jo simbolinė algebra liko Renè Descartes (1596–1650) darbų šešėlyje. (Detaliau apie Viète veikalą rašoma [6] ir [10]. Viète įtaka Fermat darbams išsamiau aptariama [11].) Fermat pripažino Viète simbolinę algebrą ir liko jai ištikimas visuose darbuose. Viète lygčių teorija tapo Fermat skaičių teorijos ir analizės darbų pagrindu.

Nors Fermat labai daug pasidarbavo plėtojant diferencialinį ir integralinį skaičiavimą bei analizinę geometriją, tačiau sveikųjų skaičių savybių tyrimas buvo viso jo gyvenimo aistra. Dabar šią sritį mes vadiname skaičių teorija. Čia Fermat įtaka vėlesnių amžių matematikos raidai yra pati svariausia. Jo skaičių teorijos tyrinėjimai sukasi apie saujelę temų, kurių ištakos siekia klasikinę graikų tradiciją, susijusią su dalumo klausimais ir pirminiais skaičiais.

Visų pirma Fermat sutelkė pastangas *tobulųjų skaičių*, t.y. skaičių, kurie yra savo tikrinių daliklių suma, problemai. Pavyzdžiui, skaičius 6 yra tobulas: $6 = 1 + 2 + 3$. Šia problema domėjosi jau pitagoriečiai. Svarbiausias klasikinis graikų laimėjimas formuluojamas Euklido „Elementų“ IX knygos 36 teiginyje:

Jeigu skaičius, pradedant vienetu, dauginsime iš 2 ir sumuosime, kol suma pasidarys lygi pirminiam skaičiui, tai šios sumos ir paskutinio dėmens sandauga bus tobulas skaičius.

Naudojantis moderniais žymenimis, šį teiginį galime suformuluoti taip:
jei kuriam nors $n \geqslant 1$ *skaičius* $2^{n+1}-1$ *yra pirminis, tai sandauga* $2^n(2^{n+1}-1)$ *yra tobulasis skaičius.*

Tačiau problema toli gražu neišspręsta, nes lieka neaišku, ar nėra kitokių tobulųjų skaičių. Dar svarbiau yra tai, kad norint šiuo teiginiu naudotis tobuliesiems skaičiams rasti, reikia efektyvaus tikrinimo, ar nurodytas skaičius yra pirminis, būdo. Spręsdamas pastarąjį klausimą, Fermat toli pažengė, tačiau tik XVIII šimtmetyje Euler įrodė, kad visi lyginiai tobulieji skaičiai yra Euklido teiginyje nurodytos formos. Ar yra nelyginių tobulųjų skaičių – dar ir šiandien yra viena iš svarbiausių neišspręstų skaičių teorijos problemų. Žinoma, kad nėra nelyginio tobulojo skaičiaus, mažesnio už 10^{160} ([8], p. 167). Istorinė tobulųjų skaičių tyrinėjimo apžvalga pateikiama [5], [13] knygose.

Iš Euklido teiginio išplaukia, kad kiekvienas sekos

$$2^2-1,\ 2^3-1,\ 2^4-1,\ \ldots,\ 2^n-1,\ \ldots$$

• • • $\alpha + \omega$ • • •

pirminis skaičius atitinka tobuląjį skaičių. Šie pirminiai skaičiai vadinami *Mersenne pirminiais*. Pagrindinis Fermat įrankis, kurį jis naudojo tikrindamas, ar tokie skaičiai yra pirminiai dabar vadinamas *Fermat teorema* (kartais *mažąja Fermat teorema*). Jo žodžiais tariant:

> Be jokios išimties kiekvienas pirminis skaičius matuoja vieną iš bet kurios progresijos narių minus 1, o šio nario rodiklis yra turimojo pirminio skaičiaus minus 1 daliklis. Taigi suradus pirmąjį rodiklį, kuris turi šią savybę, visi nariai, kurių rodikliai yra šio pirmojo nario rodiklio kartotiniai, taip pat turės šią savybę.

Ši teorema dabar formuluojama taip.

Fermat teorema. *Jei p yra pirminis skaičius, nedalijantis skaičiaus a, tai dalijant a^{p-1} iš p, gaunama liekana lygi 1 . Egzistuoja toks mažiausias sveikasis teigiamas skaičius n, kad a^n dalijant iš p gaunama liekana lygi 1, n dalija $p-1$ ir su visais sveikaisiais teigiamais k skaičius a^{kn} dalijant iš p taip pat gaunama liekana 1.*

Kaip šiuo teiginiu galima pasinaudoti? Visų pirma pastebėkime: jei 2^n-1 yra pirminis, tai ir pats n yra pirminis (žr. uždavinių skyrelį, 3 užd.). Iš savo teoremos Fermat padarė tokią išvadą (4 uždavinys), leidžiančią labai sumažinti 2^n-1 potencialių daliklių, kuriuos reikia tikrinti, skaičių.

Išvada. *Tegu p yra nelyginis pirminis skaičius, q – taip pat pirminis skaičius. Jei q dalija 2^p-1, tai egzistuoja tam tikras sveikasis k, kad $q=2kp+1$.*

Dideliems pirminiams p šia išvada pagrįstas metodas yra dar gana lėtas, tačiau gali būti išplėtoti greitesni metodai ([8]).

Visai netikėtai mažoji Fermat teorema buvo pritaikyta apie 1970 metus, konstruojant labai saugius šifrus, vadinamąsias viešojo rakto kriptosistemas. Jas imta plačiai taikyti verslo bei finansinės informacijos perdavimo procesams, taip pat ir bankų automatams. Apie šiuos ir kitus skaičių teorijos taikymus rašoma [18]. [1]

Fermat, pradėjęs nagrinėti skaičius a^n+1, čia a,n yra sveikieji skaičiai, išplėtė pirminių skaičių tyrinėjimus. Laiške Mersenne, parašytame 1640 metais per Kalėdas, Fermat tvirtina, kad tokie skaičiai gali būti pirminiai tik tuomet, kai a yra lyginis, o n – skaičiaus 2 laipsnis (5 uždavinys). Remdamasis šiais skaičiavimais, Fermat teigė, kad iš tikrųjų visi $2^{2^n}+1$ skaičiai yra pirminiai. Daugelį metų šio teiginio jam nepavyko įrodyti, tačiau 1659 metais laiške Carcavi jis teigė, kad pagaliau pasisekė surasti įrodymą ([11]). Tačiau 1732 metais Leonhard Euler parodė, kad skaičius $2^{2^5}+1$ dalijasi iš 641, taigi Fermat suklydo. Šio pavidalo pirminiai dabar vadinami *Fermat pirminiais*.

Be tobulųjų skaičių, kitas svarbus Fermat skaičių teorijos tyrimų įkvėpimo šaltinis buvo Diofanto iš Aleksandrijos, gyvenusio III šimtmetyje, veikalas „Aritmetika“. Diofantas buvo vienas iš paskutinių didžiųjų antikinės Graikijos matematikų. „Aritmetiką“ sudarė 189 uždavinių, susijusių su vieno ar daugiau

[1] Taip pat rašyta ir mūsų žurnale. Žr. J. Kubilius. Pirminiai skaičiai ir kriptografija, *Alfa+Omega*, 1996, 1, 65–70.

kintamųjų lygčių sprendimu racionaliaisiais skaičiais. Veikalas apėmė trylika knygų, iš kurių išliko tik šešios ([2]).[2]

Sprendimai pateikiami specialių skaitinių pavyzdžių pavidalu, naudojant racionaliuosius skaičius. Svarbus mūsų temai pavyzdys suformuluotas kaip II knygos 8 uždavinys, kurį, naudodami modernius žymenis, cituojame pagal [10, p. 166]:

> II-8 uždavinys. Išskaidyti nurodytą kvadratinį skaičių į du kvadratus.
>
> Tarkime, skaičių 16 reikia išskaidyti į du kvadratus. Tegu pirmasis kvadratas yra x^2. Tada kitas bus $16-x^2$. Taigi reikia, kad $16-x^2=a$ būtų kvadratas. Aš imsiu tokius kvadratus: $(ax-4)^2$, čia a yra bet koks skaičius, o 4 – šaknis iš 16. Pavyzdžiui, paėmus $2x-4$, kvadratas yra $4x^2+16-16x$. Tada $4x^2+16-16x=16-x^2$. Pridėkime prie abiejų pusių narius, kurie lygtyje neigiami, ir atimkime lygius iš lygių. Tada $5x^2=16x$ ir $x=16/5$. Todėl vienas skaičius yra 256/25, kitas – 144/25, o jų suma yra 400/25 arba 16, kiekvienas skaičius yra kvadratas.

Panaikinę vardiklius, lengvai gauname šios lygties sprendinį sveikaisiais skaičiais. Sveikųjų skaičių trejetai x, y, z, tenkinantys lygtį

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

vadinami *Pitagoro trejetais* (6 uždavinys). Pavyzdžiui, $(3,4,5)$ ir $(5,12,13)$ yra Pitagoro trejetai. Pitagoro trejetai aptinkami jau babiloniečių kultūroje. Euklidas savo „Elementuose“ visiškai išsamiai nusako, kokie trejetai (jų yra be galo daug) yra Pitagoro trejetai. Pitagoro teorema nurodo šių trejetų ryšį su stačiaisiais trikampiais, kurių visos kraštinės reiškiamos sveikaisiais skaičiais (7, 8, 9 uždaviniai).

Diofantas formuluoja skatinančius tyrinėti šio uždavinio variantus, reikalaudamas, kad sprendiniai tenkintų ypatingas sąlygas. Toks yra VI knygos 6 uždavinys, kuriame reikalaujama rasti statų trikampį (su racionaliomis kraštinėmis), kad jo ploto ir vienos kraštinės suma būtų lygi nurodytam skaičiui ([11], p. 304, taip pat [4], v. II, p. 176). Fermat labai išplėtė Diofanto vadinamąjį vienos ir dvigubos lygties metodą ir pavertė jį galingu šios rūšies uždavinių sprendimo įrankiu.

Kita Fermat tyrimų kryptis, kurią vėlesnės skaičių teorijos specialistų kartos išsamiai plėtojo, taip pat prasidėjo vienu Diofanto „Aritmetikos“ uždaviniu. Trečiosios knygos 19 uždavinys reikalauja rasti keturis skaičius, prie kurių sumos kvadrato pridėjus (arba atėmus) bet kurį iš šių skaičių, vėl būtų gaunamas kvadratas. Diofantas šį uždavinį suvedė į keturių stačiųjų trikampių su vienodomis įžambinėmis uždavinį. Jis pateikia specialų skaitinį sprendinį ([11], p. 315). „Aritmetiką“, kuria rėmėsi Fermat savo tyrinėjimuose, 1612 metais išspausdino Claude Gaspar Bachet de Méziriac. Bachet domėjimasis matematinėmis pramogomis ir mįslėmis įtraukė į skaičių teoriją. Papildęs savo komentarais, jis parengė naują „Aritmetikos“ vertimą iš graikų kalbos į lotynų kalbą, į tos epochos mokslo *lingua franca*. Bachet, ieškodamas 19 uždavinio

[2] 1972 metais R. Rashed rado dar keturias „Aritmetikos“ knygas su 101 uždaviniu Irane, Mashade, Imamo Resa kapo bibliotekoje, [14], [19].

bendrojo sprendimo, suformulavo problemą, reikalaujančią tam tikrais būdais rasti skaičius, kurie būtų dviejų kvadratų sumos. Savo komentaruose jis pateikė atskirų pavyzdžių, bet ne išsamų šio uždavinio sprendimą. Ir vėl genialus Fermat protas randa galutinį atsakymą. Kaip įprasta dabar, jis iš pradžių nagrinėja tik pirminius skaičius, o bendrąjį sprendinį gauna naudodamasis skaičiaus skaidiniu pirminiais daugikliais. Nelyginiai pirminiai gali būti suskirstyti į dvi grupes, iš kurių vieną sudaro pirminiai skaičiai, reiškiami formule $4k-1$ su sveikaisiais skaičiais $k \geqslant 1$, kitą grupę – $4k+1$ formos pirminiai skaičiai. Jis įrodo, kad pirmosios grupės pirminiai skaičiai negali būti užrašomi dviejų kvadratų suma ir bendrajam uždavinio sprendiniui jokios reikšmės neturi. Sprendimą Fermat nusako tokiais žodžiais:

> Pirminis skaičius, kuris yra didesnis už keturių kartotinį vienetu, tik vieną kartą (t. y. vieninteliu būdu) yra stataus trikampio įžambinė, jo kvadratas – du kartus, kubas – tris kartus, kvadrato kvadratas (t. y. ketvirtas laipsnis) – keturis kartus, ir taip toliau *ad infinitum*... ([11], p. 316)

Toliau jis tiria $4n+1$ formos pirminių skaičių sandaugas ir, nenurodydamas įrodymo metodo, formuluoja (teisingą) teiginį: jeigu $n = n' p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, čia p_i yra $4k+1$ formos pirminiai skaičiai, o n' sudaro tik iš $4k-1$ formos skaičiai, tai n^2 galima užrašyti dviejų kvadratų suma

$$\frac{1}{2}\left[(2a_1+1)(2a_2+1)\cdots(2a_r+1)-1\right]$$

būdų ([11], p. 318, taip pat [22], p. 71). Šiandien šie ir kiti panašūs rezultatai yra kvadratinių formų teorijos dalis. Apie kvadratų sumas galima daug sužinoti iš puikios [9] knygos.

Tuomet Fermat neatskleidė, kaip jis įrodė šį rezultatą. Tik vėliau 1659 metais laiške Christianui Huygensui (1629–1695), švytuoklinio laikrodžio išradėjui, jis pagaliau nurodė metodą, kuriuo naudojosi įrodydamas šį bei kitus įspūdingus rezultatus. Fermat vadino šį metodą „begalinio nusileidimo metodu“. Jis paaiškino Huygensui metodą pateikdamas įrodymą, kad nėra stataus trikampio, kurio plotas būtų lygus sveikojo skaičiaus kvadratui. Jeigu toks trikampis būtų, jis galėtų sukonstruoti kitą statųjį trikampį, kurio plotas taip pat būtų kvadratas, bet mažesnis už pirmojo trikampio plotą. Savo ruožtu pasinaudojęs šiuo naujuoju trikampiu, jis galėtų surasti dar vieną, kurio plotas dar mažesnis, ir taip toliau. Tačiau šis procesas, pateikiantis mums vis mažesnius ir mažesnius teigiamus sveikuosius skaičius, negali tęstis be galo, todėl neįmanoma rasti ir pirmojo trikampio, nuo kurio būtų galima pradėti. Nors atrodytų, kad šis metodas tinka tik neigimo rezultatams, t.y. kad tam tikri dalykai yra neįmanomi, įrodyti, Fermat sugebėjo jį pritaikyti ir pozityviems teiginiams pagrįsti. Vienas iš jų – anksčiau minėtas teiginys, kad bet kuris $4k+1$ formos pirminis skaičius yra kvadratų suma.

Atrodo, šiuo metodu jis įstengė įrodyti, kad joks kubas nėra kubų suma, nė ketvirtasis laipsnis nėra ketvirtųjų laipsnių suma. Anksčiau šiuos uždavinius jis buvo nusiuntęs kitiems matematikams kaip savotiškas iššūkio problemas. Kai

1670 metais Fermat sūnus Samuelis išspausdino Bachet išverstą „Aritmetiką“ su visais tėvo papildymais, 2-oji pastaba buvo suformuluota taip:

> Joks kubas negali būti išskaidytas į du kubus, nė bikvadratas į du bikvadratus, ir bendrai, joks didesnis už du laipsnis į du tuos pačius laipsnius ([22], p. 104).

Kitais žodžiais tariant, Fermat tvirtina, kad lygtis $x^n + y^n = z^n$ neturi nenulinių sprendinių, kai n yra didesnis už 2. Jis parašė, kad paraštės per siauros užrašyti tikrai nuostabų įrodymą. Tai suteikė daugeliui kankinančios vilties. Panašiai jis yra rašęs ir kitur, norėdamas paaiškinti, kodėl nėra įrodymo. Ši žymiausia užrašyta paraštėje pastaba tapo žinoma kaip „Paskutinė Fermat teorema“ ir nedavė ramybės matematikams iki šiol, kol visą darbą apvainikavo Andrew Wileso įrodymas. Žinoma, buvo daug diskutuojama, ar Fermat iš tikrųjų žinojo įrodymą, ar tik naiviai manė, kad jo begalinio nusileidimo metodas tinka visiems laipsniams. Žemiau pateikiame dviejų žymiausių XX amžiaus matematikų nuomones. Visų pirma André Weil sako:

> Kaip pastebėjome ... svarbiausios Diofanto problemos susijusios su nulinės ir pirmosios rūšies kreivėmis. Tik vienu nesėkmingai susiklosčiusiu atveju Fermat pamini aukštesnės rūšies kreivę; vargu ar galima abejoti, kad tai įvyko dėl jo paties neapsižiūrėjimo, nors dėl keistų likimo vingių jo reputacija neišmanančiųjų akyse kaip tik tuo ir remiasi. Suprantama, turime galvoje jo neatsargius žodžius *et generaliter nullam in infinitum potestatem* jo teiginyje apie „Paskutinę Fermat teoremą“, kaip nevykusiai tas teiginys buvo pavadintas... Kaip jis galėjo nujausti, kad rašo amžinybei? Mes žinome jo įrodymą bikvadratams ... jis galėjo sukonstruoti įrodymą kubams, panašų į tą, kurį Euler atrado 1753 metais ... Jis dažnai pakartodavo šiuos teiginius ... bet niekada neminėdavo bendresniojo. Gal trumpam laikotarpiui , gal būdamas jaunas ... jis galėjo manyti, kad turi bendrojo įrodymo principą; ką jis turėjo galvoje tą dieną, niekada nebus sužinota ([22], p. 104).

Atsargesnę nuomonę pareiškė L. J. Mordell ([12], p. 4):

> Matematinės studijos ir tyrimai panašūs į kopimą į kalnus. Whymper bandė septynis kartus, kol galų gale 1860 metais įkopė į Matterhorną[3] , bet ir tada keturi jo komandos nariai žuvo. Dabar kiekvienas turistas už nedidelę kainą gali būti užtemptas į viršukalnę ir tikriausiai neįvertina pirmojo įkopimo sunkumo. Taip būna ir matematikoje: gali būti nelengva suprasti, kaip sunku padaryti pirmąjį nedidelį žingsnį, kuris po to atrodo toks natūralus ir akivaizdus; įmanomas dalykas, kad toks žingsnis galėjo būti atrastas ir vėl prarastas.

Žvelgiant plačiau, Fermat buvo vienas iš didžiųjų matematikos pionierių, kuris, remdamasis klasikinės Graikijos laimėjimais, sukūrė skaičių teorijai visiškai naują paradigmą ir padėjo pagrindą matematinei teorijai, vėliau pavadintai „matematikos karaliene“. Tačiau, kaip atsitinka daugeliui mokslo pionierių, per visą gyvenimą jis veltui bandė atkreipti mokslo visuomenės dėmesį į savo skaičių teorijos tyrinėjimus. Nepavykus sudominti tokių žymių matematikų kaip John

[3] Alpių viršukalnė ant Italijos ir Šveicarijos sienos.

Wallis (1616–1703), labai įtakingo Newtono pirmtako Anglijoje, ir Blaiso Pascalio (1623–1662) Paryžiuje, Fermat anksčiau minėtame laiške paskutinį kartą pabandė laimėti Huygenso dėmesį. Savo laišką jis baigia taip:

> Santraukoje pateikiu savo mintis apie skaičius. Aš rašau tai todėl, kad bijau, jog neturėsiu laiko išplėsti ir detaliai išdėstyti visų šių įrodymų ir metodų. Bet kuriuo atveju šie užrašai padės mokytiems žmonėms patiems surasti tai, ko aš neišplėtojau, ypač jei vonai de Carcavi ir Frènicle pasidalys žiniomis apie tam tikrų negatyvių teiginių įrodymus begalinio nusileidimo metodu, kuriuos aš jiems pasiunčiau. Galbūt ateities kartos bus man dėkingos, kad parodžiau, jog senieji meistrai ne viską žinojo, ir tai persmelks protus tų, kurie ateis po manęs „nešti fakelo ateities kartoms", kaip pasakė didysis Anglijos kancleris. Sekdamas jo jausmu ir mintimi aš pridurčiau: „Daugelis eis ir nueis, o žinios kaupsis" ([11], p. 351).

Nežinia, kodėl Fermat nepavyko suvilioti didžiųjų amžininkų sekti juo. Gal būt kaltas Fermat slėpiningumas, nes jis gautus rezultatus skelbdavo kaip uždavinius ir nepateikdavo įrodymų, o gal jo tyrimų krypčiai dar nebuvo tinkamas laikas. Praėjo net šimtas metų, kol kitas Fermat rango matematikas pratęsė jo darbą.

Leonhard Euler (1707–1783), be abejonės buvo vienas didžiausių visų laikų matematikų. Gimęs Šveicarijoje, Euler savo gyvenimą praleido Sankt Peterburgo ir Berlyno akademijose. Jo matematiniai interesai buvo labai platūs, apėmė taip pat ir skaičių teoriją, kuri, jo žodžiais tariant, buvo kaip pramoga po pagrindinių jo tyrimo sričių. Eulerio dėmesį į Fermat darbus atkreipė Christian Goldbach (1690–1764) jų susirašinėjimo, kurį 1729 metais pradėjo Euler, pradžioje. Atsakydamas į laišką, Goldbach pridėjo prierašą: „Ar jums žinoma Fermat pastaba, kad visi skaičiai $2^{2^n}+1$ yra pirminiai? Jis sakė, kad negalėjo to įrodyti; kiek žinau, niekas negalėjo to padaryti " ([22], p.172). Jų susirašinėjimas tęsėsi daugiau kaip trisdešimt metų iki Goldbacho mirties. Goldbach buvo daug keliavęs ir gerai išsilavinęs žmogus, jo pagrindiniai intelektualiniai interesai buvo kalbos ir matematika. Jis pažinojo daugelį žymių to meto matematikų, taip pat ir Nicolas (1687–1759) bei Daniel (1700–1782) Bernoulli, kurie jo rūpesčiu gavo Sankt Peterburgo akademijoje vietas. Pastarieji, savo ruožtu, pasirūpino, kad akademijoje atsirastų vieta jaunajam Euleriui.

Didelė Eulerio skaičių teorijos darbų dalis atlikta sistemingai bandant įrodyti visus Fermat teiginius, taip pat ir paskutinę Fermat teoremą ([22], p.170). Jis pateikė pirmą įrodymą trečiojo laipsnio atveju, kuris yra daug sudėtingesnis už ketvirtojo laipsnio atvejį. Kitas originalus Eulerio rezultatas šioje srityje – jo paties įrodymas ketvirtojo laipsnio lygčiai.

Antroje XVIII amžiaus pusėje tik nedaugelis mokslininkų domėjosi grynąja matematika. Laimei, vienas iš jų pasišventė skaičių teorijos tyrimams. Skaičių teorija 1768 metais susidomėjo Joseph Louis Lagrange (1736–1813). Per dešimtmetį jis parašė seriją šios srities darbų, iš kurių daugelį – įkvėptas Eulerio tyrimų. Šiose publikacijose nebuvo naujų rezultatų apie paskutinę Fermat teoremą, bet jis išlaikė skaičių teorijos tradiciją, kurią vėliau perėmė kiti tyrinėtojai. Lagrange tapo Eulerio įpėdiniu Berlyno mokslų akademijoje ir po jo

mirties paveldėjo žymiausio Europos matematiko vardą. 1786 metais Lagrange išvyko į Paryžių, kur gyveno iki pat mirties.

Vienas iš Lagrange bendradarbių Paryžiuje buvo Adrien-Marie Legendre (1752–1833), kuris atkreipė Lagrange dėmesį prieš ketverius metus, atsiuntęs laimėjusį premiją darbą iš balistikos srities ([22], p. 324). 1785 metais Legendre pateikė Paryžiaus akademijai darbą, pavadintą „Neapibrėžtosios analizės tyrimai". Tai buvo jo pirmas skaičių teorijos darbas, tiesiogiai įkvėptas Eulerio ir Lagrange raštų. Tuo metu Euler buvo jau miręs, o Lagrange šioje srityje jau nebedirbo. Legendre ėmėsi vykdyti plačią skaičių teorijos tyrimų programą, kurios rezultatas – išsamus skaičių teorijos traktatas „Esė apie skaičių teoriją", išspausdintas 1798 metais. Buvo išleisti keli jo leidimai, paskutinis pasirodė 1830 metais pavadinimu „Skaičių teorija". Pirmame ir antrame leidimuose, Legendre pakartojo paskutinės Fermat teoremos Eulerio įrodymus trečiojo ir ketvirtojo laipsnių lygtims. Po to 1825 metų priede antrajam leidimui jis pridėjo savo rezultatų, vienas iš jų – įrodymas penktojo laipsnio atveju. Čia Legendre indėlis – iš dalies užbaigtas jauno vokiečių matematiko Lejeune Dirichlet (1805–1859) tais pačiais metais sukurtas įrodymas.

Kai 1808 metai pasirodė antrasis „Skaičių teorijos" leidimas, jis atrodė senamadiškas, palyginti su nepaprastu jauno vokiečių matematiko Carlo Friedricho Gausso (1777–1855) veikalu „Disquisitiones Arithmetique" (Aritmetiniai tyrinėjimai), išspausdintu 1801 metais ir padėjusiu pagrindus šiuolaikinei skaičių teorijai. Jame pateikiama daug įrodymų, tarp jų ir *kvadratinio dualumo teoremos* – vieno iš fundamentalių teiginių apie pirminius skaičius. Ją kaip prielaidą suformulavo Euler, o Lagrange pateikė neteisingą jo įrodymą. Savo veikale Gaussas išplėtojo lyginių aritmetikos teoriją, kuri ir šiandien yra svarbi. „Disquisitiones" pagaliau pavertė skaičių teoriją matematine teorija su darnia rezultatų ir metodų sistema. Tolydžio kai kurie didžiausi XIX amžiaus matematiniai protai buvo pavilioti naujos srities apžavų. Ši sritis suklestėjo, kai antroje XIX amžiaus pusėje ir XX amžiuje ėmė gausiai rastis naujų rezultatų ir metodų.

Gausso pažiūros apie paskutinę Fermat teoremą išdėstytos 1816 metų kovo 21 dienos laiške jo kolegai W. Olbersui:

> Kaip atskiras rezultatas paskutinė Fermat teorema man didelės reikšmės neturi, nes nesunku suformuluoti daugybę teoremų, kurių niekas negalėtų nei įrodyti, nei paneigti. Vis dėlto ji paskatino mane grįžti prie tam tikrų senų minčių apie aukštesnės aritmetikos išplėtimą. Žinoma, ši teorija yra viena iš tų, kur neįmanoma nuspėti, kiek įmanoma priartėti prie tolumoje stūksančių tikslų. Tam reikia ir laimingos žvaigždės. Mano padėtis ir daug pastangų reikalaujanti veikla neleidžia atsidėti tiems svarstymams, kaip buvo laimingais 1796–1798 metais, kai aš sukūriau pagrindines „Disquisitiones Arithmeticae" dalis.
>
> Deja, aš esu įsitikinęs, kad jeigu laimė man lems daugiau, negu galiu tikėtis, ir man pavyks šioje teorijoje žengti pagrindinius žingsnius, tai Fermat teorema pasirodys joje kaip viena iš mažiausiai įdomių išvadų ([17], p. 629).

Bet tuo metu laimė Gaussui nenusišypsojo ir jis nebesugrįžo prie rimtų skaičių teorijos tyrimų. Vis dėlto, „Disquisitiones" ir jų lyginių aritmetika įkvėpė

naujai paskutinės Fermat teoremos bendrojo atvejo atakai. Paryžiuje jaunoji Sophie Germain (1776–1831), jau išstudijavusi Legendre „Esė“, godžiai skaitė Gausso knygą. Ji iš karto įžvelgė galimybę panaudoti lyginių metodą bendrajam paskutinės Fermat teoremos įrodymui ir didelę savo gyvenimo dalį paskyrė, deja, bevaisėms pastangoms. Tačiau jai pavyko įrodyti pirmąjį bendrą rezultatą apie paskutinę Fermat teoremą ir jos požiūris buvo sėkmingai taikytas daugelio tyrinėtojų netgi iki 1980 metų.

Dar vienas svarbus šios istorijos etapas – rezultatas, kurį įprasta priskirti Sophie Germain ir vadinti Sophie Germain teorema. Germain nepublikavo jokių darbų apie paskutinę Fermat teoremą. Vienintelė skelbta nuoroda apie jos darbą yra pastaba jau minėto paskutinei Fermat teoremai skirto Legendre „Esė“ antrojo leidimo priedo paraštėje. Čia aptariami Germain rezultatai užrašyti rankraščiuose, kurie saugomi Paryžiaus Nacionalinėje bibliotekoje bei minimi neskelbtoje jos ir Gausso korespondencijoje.

Jau Fermat pastebėjo, kad teoremą pakanka įrodyti ketvirtajam laipsniui ir nelyginiams pirminiams p (10 uždavinys). Germain įrodė: jei tokiam p atsirastų nenuliniai sveikieji skaičiai x, y, z, kad

$$x^p + y^p = z^p,$$

ir tam tikras pagalbinis pirminis q, tenkinantis tam tikras sąlygas, tai p^2 dalytų vieną iš skaičių x, y, z. Šiems pagalbiniams pirminiams skaičiams rasti ji sukūrė algoritmą ir sėkmingai panaudojo visiems nedidesniems už 100 pirminiams. Jos pagalbinių pirminių radimo metodas gali būti sėkmingai taikomas ir aukštesniems pirminių laipsniams. Tai padarė Legendre. Jis surado juos visiems p iki 197. Taigi visiems pirminiams iki 197 į Fermat lygties sprendinį būtinai turi įeiti skaičius, kuris dalijasi iš laipsnio rodiklio. Šiuo rezultatu pagrįstas Fermat lygties sprendinių skirstymas į du atvejus. Jei sprendinio skaičių sandauga xyz nesidalija iš laipsnio rodiklio, sakoma, kad x, y, z yra pirmojo atvejo sprendinys, jei dalijasi – x, y, z yra antrojo atvejo sprendinys.

Nors ir prieš Germain buvo moterų, pavyzdžiui, klasikinės Graikijos matematikė Hypatia arba Renesanso laikais Maria Gaetana Agnesi, turėjusių įtakos matematikos raidai, Sophie Germain buvo pirmoji istorijoje moteris, gavusi naujų ir reikšmingų matematinių rezultų tiek skaičių teorijos, tiek matematinės fizikos srityje. Germain biografija puikiai išdėstyta [23] knygoje.

Devynioliktojo amžiaus viduryje paskutinei Fermat teoremai įrodyti buvo taikomi sudėtingi metodai. Vokiečių skaičių teorijos specialisto Ernsto Kummerio (1810–1893) 1847 metų gegužės mėnesį rašytame į Paryžių laiške Josephui Liouville kalbama apie nesėkmę, sveikųjų skaičių skaidymo pirminiais daugikliais vienaties dėsnį taikant tam tikriems kompleksiniams skaičiams. Kai kuriuose pateiktuose paskutinės Fermat teoremos įrodymo bandymuose buvo daroma prielaida, kad tokio skaidymo vienaties dėsnis galioja bendriausiu atveju, bet Kummer gavo rezultatų, liudijančių, kad šis dėsnis ne visada teisingas. Kummer problemą pradėjo tyrinėti visai naujais metodais. Tai buvo radikalus posūkis nuo pirmtakų darbų, tapęs algebrinės skaičių teorijos pradžia. Jis pats prie

paskutinės Fermat teoremos įrodymo prisidėjo tuo, kad nustatė, jog Fermat tvirtinimas teisingas tam tikriems pirminiams, kuriuos imta vadinti *reguliariaisiais*. Pavyzdžiui, visi pirminiai skaičiai, neviršijantys 100, išskyrus 37, 59, 67, yra reguliarūs.

Pusantro šimto metų po Kummerio rezultatų skaičių teorijos pasaulyje vyko lėtas įrodymo užbaigimo darbas. Apie tai parašyta gerų apžvalginių straipsnių, (pav., [7], [15]). Įrodyta daug pagalbinių rezultatų. Pavyzdžiui, 1909 metais A. Wiefericho įrodytas teiginys:

jeigu laipsnio rodikliui p egzistuoja pirmojo atvejo sprendinys, tai skaičius p turi tenkintį sąlygą

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

1976 metais buvo įrodyta, kad paskutinė Fermat teorema teisinga visiems ne didesniems už 125 000 laipsnio rodikliams. 1992 metais šio rezultato galiojimo sritis buvo išplėsta iki 4 000 000. Įvykiai ėmė klostytis jaudinančiai po 1983 metų, kai vokiečių matematikas Gerd Faltings įrodė vadinamąją Mordello hipotezę – algebrinės geometrijos rezultatą, tvirtinantį, kad su $n \geqslant 4$ lygtis $x^n + y^n = z^n$ gali turėti tik baigtinį skaičių poromis tarpusavyje pirminių (t.y. neturinčių bendrų pirminių daliklių) sprendinių skaičių. Algebrinėje geometrijoje nagrinėjamos polinominių lygčių sistemų, pavyzdžiui,

$$\begin{aligned} y - x^2 &= 0, \\ y - x^3 &= 0, \end{aligned}$$

sprendinių aibės. Suprantama, sprendinių aibė priklauso, nuo to, kokie skaičiai, pavyzdžiui, racionalieji ar realieji, yra nagrinėjami. Šių skaičių atveju dalijant iš z laipsnio, Fermat lygtį galima suvesti į lygtį $x^p + y^p = 1$. Turėdami racionalųjį šios lygties sprendinį ir panaikinę vardiklius, gautume Fermat lygties sprendinį sveikaisiais skaičiais. Plokštumoje lygties $x^p + y^p = 1$ sprendinių aibė apibrėžia kreivę. Paskutinė Fermat teorema ekvivalenti teiginiui, kad ši kreivė neina per taškus su abiem racionaliosiomis koordinatėmis. Taigi žvelgiant į paskutinę Fermat teoremą kaip į algebrinės geometrijos problemą, galima taikyti ne tik skaičių teorijos bet ir šios srities metodus. Mordello hipotezė teigė, kad kai kurios kreivės, pavyzdžiui, $x^n + y^n = 1$, kai $n \geqslant 5$, turi tik baigtinį skaičių racionaliųjų taškų. Taigi atskiru atveju Fermat lygtis turi tik baigtinį skaičių poromis tarpusavyje pirminių sveikaskaičių sprendinių.

Žinoma, nuo Faltingso rezultato iki paskutinės Fermat teoremos dar toli. Bet tai leido 1985 metais A. Granville ir D. Heath-Brownui įrodyti, kad paskutinė Fermat teorema teisinga „daugumai" rodiklių n, t.y., kad kuo n didesnis, tuo artimesnė nuliui tikimybė, kad Fermat tvirtinimas rodikliui n neteisingas. Rezultatų vis gausėjo. Buvo suformuluota daugiau skaičių teorijos hipotezių, iš kurių turėtų išplaukti paskutinė Fermat teorema. Viena iš jų – vadinamoji Taniyama–Shimura hipotezė, susijusi su elipsinėmis kreivėmis, kurių koeficientai racionalūs. Šios kreivės užrašomos lygtimis

$$y^2 = ax^3 + bx^2 + cx + d;$$

• • • $\alpha + \omega$ • • •

čia a, b, c, d yra racionalieji skaičiai, $a \neq 0$; be to, visos dešiniosios pusės polinomo šaknys yra skirtingos. Hipotezė tvirtina, kad visos tokios kreivės yra *modulinės*. (Čia šios sąvokos negalime aptarti detaliau. Išsamesnės medžiagos skaitytojas gali rasti puikiame straipsnyje [3], taip pat [16], [20].) Atsakymas, kodėl iš šios hipotezės išplaukia paskutinė Fermat teorema, glūdi 1980 metų pradžioje vokiečių matematiko Gerhardo Frey įrodytame teiginyje. Jis nurodė, kad naudojantis netrivialiu Fermat lygties sprendiniu galima sukonstruoti tam tikrą elipsinę kreivę, kuri, kaip jis galvojo, nebūtų modulinė. Šios kreivės, dabar vadinamos Frey kreivėmis, konstruojamos taip. Frey kreivės, atitinkančios netrivialų sprendinį $a^p + b^p = c^p$, su $p \geqslant 5$, lygtis yra

$$y^2 = x(x - a^p)(x + b^p).$$

1986 metais Ken Ribet iš Berkeley žengė paskutinį žingsnį, patvirtindamas Frey nuojautą. Taigi Taniyama–Shimura hipotezės įrodymas reikštų, kad paskutinė Fermat teorema taip pat teisinga.

1993 metų birželio mėnesį Prinstono matematikas Andrew Wiles skaitė Kembridže, Newtono institute, Anglijoje, tris paskaitas, kurių metu išdėstė Taniyama–Shimura hipotezės įrodymo kontūrus tam tikrai elipsinių kreivių klasei, kuriai priklauso ir Frey kreivės. Taigi atrodė, kad daugiau kaip po 300 metų paskutinės Fermat teoremos įrodymas pagaliau baigtas. Wiles parengė ilgą rankraštį, kuriame išdėstė savo ypač sudėtingų ir sunkių samprotavimų detales. Šį tekstą jis pateikė keliems šios srities specialistams patikrinti. Tikrintojų komitetas ilgai tylėjo, po to matematikų bendruomenėje ėmė sklisti nerimą keliantys gandai, kad prieš kelis metus nuskambėjęs triumfas yra netikras, nes įrodyme yra spraga. Iš tikrųjų tapo aišku, kad Wileso įrodyme spraga tikrai yra. Laimei 1994 metų rugsėjo mėnesį Wiles ir Kembridžo (UK) matematikas Richard Taylor sugebėjo išvengti šios spragos ir sukurti išsamų įrodymą, kuris buvo labai kruopščiai patikrintas ir pripažintas teisingu.

1997 metų birželio 27 dieną Götingene, Vokietijoje, Andrew Wilesas gavo Wolfskehlio premiją. Ją įsteigė vokiečių matematikas Paul Wolfskehlis (1856–1906), kuris susidomėjo Fermat teorema klausydamas Ernsto Kummerio paskaitų ir skaitydamas jo straipsnius. Pirmas asmuo, teisingai įrodęs paskutinę Fermat teoremą arba pateikęs būtinas ir pakankamas sąlygas tiems laipsnio rodikliams, kuriems Fermat lygtis neturi sveikųjų teigiamų sprendinių, turėjo gauti 100 000 Vokietijos markių. (Kai premija buvo įteikta Andrew Wilesui, jos vertė buvo apie 43 000 USD.) Premija patrigubino neteisingų įrodymų srautą. (Išsamiau apie premiją rašoma [1], p. 1294–1303.)

Vienas iš didžiausių XX amžiaus matematikos laimėjimų, – Wileso ir Tayloro įrodymas – užbaigė beveik keturis šimtmečius trukusią odisėją. Kita vertus, rezultatai, pasitarnavę įrodymui, iškėlė daug jaudinančių klausimų, kurie turės įtakos matematikos raidai ateityje, taip kaip paskutinė Fermat teorema darė įtaką matematikai praeityje. Mes galime būti laimingi, kad gyvename vienu įdomiausių visos matematikos istorijos laikotarpių. Jau dabar aišku, kad ateityje skaičių teorijos laukia nauji jaudinantys atradimai.

• • • $\alpha + \omega$ • • •

Uždaviniai

1 uždavinys. Įrodykite Euklido „Elementų" teiginį apie tobuluosius skaičius. Pasinaudokite juo ir raskite kiek galite daugiau tobulųjų skaičių.

2 uždavinys. Kaip mažąją Fermat teoremą užrašytumėte dabartiniais matematiniais žymenimis?

3 uždavinys. Tegu n yra teigiamas sveikasis skaičius, $2^n - 1$ – pirminis. Įrodykite, kad tada n taip pat turi būti pirminis.

Nuoroda: Įrodykite lygybę

$$\frac{2^{ab}-1}{2^a-1} = 2^{a(b-1)} + 2^{a(b-2)} + \cdots + 1.$$

4 uždavinys. Pasinaudokite mažąja Fermat teorema ir įrodykite išvadą: jei p yra nelyginis pirminis skaičius ir pirminis skaičius q dalija $2^p - 1$, tai su tam tikru sveikuoju k teisinga lygybė $q = 2kp + 1$.

5 uždavinys. Tarkime, $a^n + 1$ yra pirminis skaičius. Įrodykite, kad a yra būtinai lyginis, o n yra dvejeto laipsnis.

Nuoroda: Įrodykite, kad su $n = 2^k m$, čia $m > 1$ yra nelyginis, teisinga lygybė

$$\frac{a^{2^k m}+1}{a^{2^k}+1} = a^{2^k(m-1)} - a^{2^k(m-2)} + a^{2^k(m-3)} - \cdots + 1.$$

6 uždavinys. Kokie Pitagoro trejetai gaunami iš Diofanto uždavinio apie kvadrato skaidymą dviejų kvadratų suma sprendimo?

7 uždavinys. Primityviuoju Pitagoro trejetu vadinamas toks trejetas, kurio skaičiai yra poromis tarpusavyje pirminiai. Įrodykite, kad, padauginus visus primityviojo Pitagoro trejeto skaičius iš to paties daugiklio, vėl gaunamas Pitagoro trejetas ir, atvirkščiai, kiekvienas Pitagoro trejetas gaunamas šiuo būdu iš tam tikro primityviojo trejeto.

8 uždavinys. Įrodykite, kad dviejų nelyginių skaičių kvadratų suma negali būti sveikojo skaičiaus kvadratas. Pasinaudoję tuo, padarykite išvadą, kad bet kurio Pitagoro trejeto vienas iš pirmųjų dviejų skaičių yra būtinai lyginis.

9 uždavinys. Kaip naudojantis Euklido dalybos su liekana algoritmu galima nustatyti, ar Pitagoro trejetas yra primityvusis, ar ne?

10 uždavinys. Įrodykite, kad paskutinė Fermat teorema yra teisinga su visais rodikliais n, jei ji teisinga, kai $n = 4$ ir kai n yra nelyginis pirminis skaičius.

• • • $\alpha + \omega$ • • •

Literatūra

1. K. Barner, Paul Wolfskehl and the Wolfskehl Prize, *Notices of the Amer. Math. Soc.*, 44, 1294–1303 (1997).
2. I. Bashmakova, *Diophantus and Diophantine Equations,* Math. Assoc. of Amer., Washington, D.C. (1997).
3. D. Cox, Introduction to Fermat's Last Theorem, *Amer. Math. Month.*, 101, 3–14 (1994).
4. L. E. Dickson, *Introduction to the Theory of Numbers,* University of Chicago Press (1929).
5. L. E. Dickson, *History of the Theory of Numbers,* Chelsea Publishing, New York (1992).
6. *Dictionary of Scientific Biography,* C. C. Gilispie and F. L. Holmes (eds.), Scribner, New York (1970).
7. H. M. Edwards, *Fermat's Last Theorem: A Genetic Introduction to Number Theory,* Springer, New York (1987).
8. P. Giblin, *Primes and Programming,* Cambridge University Press, New York (1993).
9. E. Grosswald, *Representations of Integers as Sums of Squares,* Springer, New York (1985).
10. V. Katz, *A History of Mathematics,* Harper Collins, New York (1983).
11. M. S. Mahoney, *The Mathematical Career of Pierre de Fermat,* Princeton University Press (1994).
12. L. J. Mordell, *Three Lectures on Fermat's Last Theorem,* Chelsea Publishing Co, New York (1962).
13. O. Ore, *Number Theory and its History,* Dover, New York (1988).
14. R. Rashed (ed.), *Diophantus, Lés Arithmétiques. Livres IV–VII. Zweisprachige Ausg. (Oevres de Diophante,) vol. III et IV,* Les Belles Lettres, Paris (1984).
15. P. Ribenboim, *13 Lectures on Fermat's Last Theorem,* Springer, New York (1979).
16. K. Ribet, B. Hayes, Fermat's Last Theorem and Modern Arithmetic, *Amer. Sci.*, 82, 144–156 (1994).
17. C. Schilling, J. Kramer, *Wilhelm Olbers, Sein Leben und seine Werke,* vol. I, Berlin, (1900/09).
18. M. R. Schroeder, *Number Theory in Science and Communication,* 2nd ed., Springer, New York (1990).
19. J. Sesiano (ed.), *Books IV to VII of Diophantus' Arithmetica in the Arabic Translation Attributed to Qusta Ibn Luqa,* Springer, New York (1982).
20. S. Singh, K. Ribet, Fermat's Last Stand, *Scient. Amer.*, Nov. (1997).
21. F. Viète, *The Analytic Art,* Kent State University Press, Ohio (1983).
22. A. Weil, *Number Theory: An Approach Through History; from Hammurapi to Legendre,* Birkhäuser, Boston (1983).