Kenneth A. Ribet
Brian Hayes

Paskutinė Fermat teorema ir modernioji aritmetika

Kenneth A. Ribet yra Kalifornijos universiteto Berklyje matematikos profesorius. Pirmuosius mokslinius laipsnius jis gavo 1969 metais Browno universitete, 1973 metais Harvardo universitetas suteikė jam filosofijos daktaro (Ph.D.) laipsnį. K. A. Ribet tyrinėjo įvairius skaičių teorijos ir aritmetinės algebrinės geometrijos klausimus; geriausiai žinomas jo rezultatas – įrodymas, kad iš Taniyama-Shimura hipotezės išplaukia didžioji Fermat teorema. 1989 metais jis kartu su Abbas Bahri gavo pirmąją Fermat premiją.
Brian Hayes yra mokslo populiarinimo straipsnių autorius, redagavęs *American Scientist* žurnalą. Šis straipsnis pasirodė *American Scientist* žurnalo 1994 metų (kovo–balandžio mėn.) numeryje; išverstas ir spausdinamas mūsų leidinyje autoriams sutikus.

Pierre de Fermat hipotezė pagaliau įrodyta. Tai tarsi istorijos ironija: teorema yra lyg pastaba kur kas reikšmingesnio darbo paraštėje.

Eric Temple Bell, matematikas ir matematikų biografas, tikėjo, kad žmonijai susinaikinus branduoliniame kare didžioji Fermat teorema liks vienas iš taip ir neišspręstų klausimų. Šią pranašystę Bell pareiškė prieš pat savo mirtį 1960 metais. Jeigu jis būtų gyvenęs dar kelis dešimtmečius, įdomu, kas jį labiau stebintų: kad žmonija dar nesusinaikino, ar kad 1993 metų birželio 23 dieną buvo paskelbta, jog didžioji Fermat teorema yra įrodyta.

Pačią teoremą lengva suformuluoti. Pierre de Fermat teigė, kad jei a, b, c yra teigiami sveikieji skaičiai, o n didesnis už 2, tai lygtis

$$a^n + b^n = c^n$$

negali turėti sprendinių. Šis paprastumas yra apgaulingas: teiginio nepavyko įrodyti daugiau nei 350 metų. O Prinstono universiteto matematikas Andrew Wiles įrodymui naudoja nepaprastai sudėtingą matematikos priemonių ir metodų arsenalą. Wileso įrodymas išdėstytas storame ir sunkiai skaitomame rankraštyje, kurio nuorodos apima ne mažiau kaip per 30 metų atliktus matematinius darbus.[1]

Svarbu suvokti tikrąją paskutinės Fermat teoremos vietą šiuolaikinėje matematikoje: tai greičiau didžiulė mįslė, nei pagrindinė ar svarbi problema. Suradus įrodymą, visas įdomumas išnyksta. Kita vertus, beieškant įrodymo daug buvo nuveikta plėtojant kur kas svarbesnes matematikos sritis. Pats Wiles, norėdamas įrodyti paskutinę Fermat teoremą, įrodinėjo kitą teiginį – vadinamąją Taniyama–Shimura hipotezę, iš kurios paskutinė Fermat teorema išplaukia kaip išvada.

Taniyama–Shimura hipotezė yra gilesnis ir potencialiai reikšmingesnis teiginys negu paskutinė Fermat teorema. Ji priklauso matematikos sričiai, kuri buvo intensyviai plėtojama per pastaruosius tris dešimtmečius, bet už matematikų profesinės bendruomenės ribų liko mažai žinoma. Ši sritis vadinama *aritmetine algebrine geometrija*, arba *moderniąja aritmetika*. Ji išsirutuliojo iš pastangų pritaikyti šiuolaikinius matematikos metodus uždaviniams, kurie vadinami diofantinėmis problemomis. Sprendžiant šiuos uždavinius, ieškoma lygčių sistemos visų sprendinių sveikaisiais skaičiais. Modernioji aritmetika yra turtingos vidinės struktūros sritis, vienaip ar kitaip susijusi su kone kiekviena kita matematikos kryptimi. Tikrai įspūdinga, kad abstrakčios šios srities konstrukcijos sudarė galimybę naujai pažvelgti į svarbiausiąją iš visų diofantinių problemų – paskutinę Fermat teoremą.

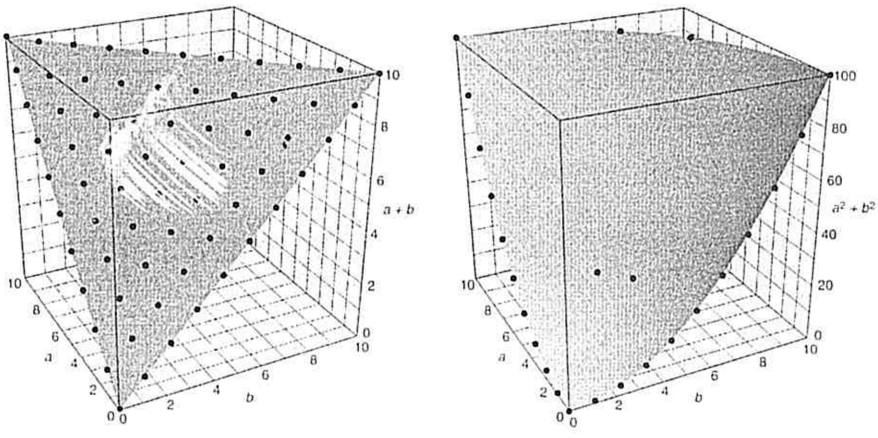
Marginalijos

Istorija apie tai, kaip Fermat suformulavo savo „paskutinę teoremą“, buvo jau daug kartų pasakota, tačiau tai yra pernelyg gera istorija, kad praleistume progą dar kartą ją papasakoti. Pierre de Fermat gimė 1601 metais Prancūzijos pietuose ir didesniąją savo gyvenimo dalį praleido Tulūzoje, kur jis buvo žymus Louis XIV administracijos teisininkas. Jis buvo matematikas mėgėjas, tačiau palaikė plačius ryšius: susirašinėjo su René Descartes, Blaise Pascaliu ir kitomis to laikotarpio įžymybėmis. Iš tikrųjų svarbiausios informacijos apie Fermat matematinius darbus teikia jo korespondencija ir pastabos knygų paraštėse.

Apie 1630 metus Fermat skaitė Diofanto iš Aleksandrijos „Aritmetiką“ – veikalą, parašytą tikriausiai I amžiuje po Kr. Jame nagrinėjami įvairūs lygčių sprendimo sveikaisiais arba racionaliaisiais skaičiais (sveikųjų skaičių santykiais) uždaviniai. Savo šios knygos egzemplioriuje Fermat padarė daugybę pastabų; ypač įdomi pastaba po 2 knygos 8 uždaviniu, kurį Diofantas formuluoja taip: „Nurodytąjį skaičių, kuris yra kito skaičiaus kvadratas, užrašykite dviejų kitų kvadratų suma“. Fermat pastaba, išversta iš lotynų kalbos skamba taip: „Neįmanoma jokio kubo išskaidyti į du kubus ar ketvirtojo laipsnio į du ketvirtuosius laipsnius, ir apskritai jokio laipsnio didesnio už du į du tuos pačius

[1] Kai šis straipsnis dar buvo rašomas, Wileso įrodymo padėtis dar buvo neaiški. Tikrinant pastebėti keli trūkumai, kurie greitai buvo pašalinti, išskyrus vieną, kuris atrodė rimtesnis. Wiles pareiškė tikįs, kad spragą galima užpildyti. Iš tikrųjų taip ir buvo padaryta; žr. R. Laubenbacher, D. Pengelley straipsnį šiame žurnalo numeryje.

laipsnius. Aš suradau tikrai nuostabų įrodymą, bet paraštės yra per siauros jam užrašyti.“ Ši viltis žadinanti užuomina apie kažkada žinotą bet prarastą įrodymą, be abejonės, prisidėjo prie legendos apie paskutinę Fermat teoremą susikūrimo. Pats Fermat neturi nieko bendra su epitetu „paskutinė“. Ši teorema toli gražu nebuvo paskutinė Fermat suformuluota teorema; jis gyveno iki 1665 metų ir dar daug nuveikė matematikoje. Būdvardis „paskutinė“ atsirado XVIII ar XIX šimtmetyje ir turbūt reiškė, jog ši teorema yra paskutinis Fermat teiginys, kuris liko nei įrodytas, nei paneigtas.



1 brėžinys

Paskutinę Fermat teoremą, teigiančią, kad lygtis $a^n + b^n = c^n$ neturi sveikųjų nenulinių sprendinių, kai $n > 2$, galima interpretuoti geometriškai. Su bet kokiu natūraliuoju n funkcija $f(a, b) = a^n + b^n$ nusako trimatės erdvės paviršių. Kai $n = 1$, šis paviršius yra plokštuma (pavaizduota kairėje), ji eina per be galo daug taškų su nenulinėmis sveikosiomis koordinatėmis. Kai $n = 2$, paviršius yra paraboloidas. Vieninteliai paraboloido taškai su sveikosiomis nenulinėmis koordinatėmis gaunami iš Pitagoro trejetų. Jų yra taip pat be galo daug. Paskutinė Fermat teorema tvirtina, kad funkcija $f(a, b) = a^n + b^n$ apibrėžiamas paviršius tokių taškų neturi, kai $n > 2$.

Ar Fermat tikrai žinojo įrodymą, kurį būtų užrašęs, jeigu paraštės būtų buvę platesnės? Labai tikėtina, kad būtent šis klausimas ir liks neatsakytas. Tikėtina, kad Fermat manė, jog rado įrodymą, bet vėliau suprato apsirikęs. Savo kolegoms rašytuose laiškuose jis mini įrodymus, kai $n = 3$ ir $n = 4$, bet nė karto nemini bendrojo atvejo įrodymo.

Ankstyvieji bandymai

Visiškai nesunku rasti lygties $a^n + b^n = c^n$ sprendinius sveikaisiais skaičiais, kai $n = 1$, nes tada lygtis virsta paprasta lygybe $a + b = c$. Dviejų svaikųjų skaičių suma visada yra sveikasis skaičius, taigi kiekvienai skaičių a, b porai visada atsiras atitinkamas c. Kai n lygus 2 (šį atvejį nagrinėjo Diofantas) uždavinys yra truputį sudėtingesnis. Lygtis $a^2 + b^2 = c^2$ nusako, žinoma, stačiojo trikampio įžambinės ir statinių ilgių ryšį; ji turi be galo daug sprendinių, pirmasis iš jų gerai žinomas sprendinys $3^2 + 4^2 = 5^2$. Euklidas, gyvenęs keliais šimtmečiais anksčiau už Diofantą, nurodė metodą, kaip gauti visus šiuos sprendinius, dar vadinamus Pitagoro trejetais.

Kai $n = 1$ arba $n = 2$, sprendinių yra be galo daug, tad atrodo keista, kad su $n \geqslant 3$ sprendinių nėra, bet tai kaip tik ir tvirtina Fermat teorema. Ją galima interpretuoti geometriškai. Su kiekviena n reikšme lygtis $a^n + b^n = c^n$ trimatėje erdvėje apibrėžia glodų paviršių. Reikšmes $n = 1$ ir $n = 2$ atitinkantys paviršiai eina per be galo daug taškų su visomis trimis sveikosiomis koordinatėmis, bet paviršiai, atitinkantys didesnes n reikšmes, neina per tokius taškus (išskyrus taškus su $a = 0$ arba $b = 0$).

Pats Fermat įrodė teoremą, kai $n = 4$ (ir šįkart jis užrašė įrodymą kitoje knygos paraštėje). Iš tikrųjų Fermat įrodė truputį bendresnį teiginį – kad lygtis $a^4 + b^4 = c^2$ neturi sprendinių sveikaisiais skaičiais; kadangi sveikojo skaičiaus ketvirtasis laipsnis yra ir sveikojo skaičiaus kvadratas, tai iš Fermat įrodyto teiginio išplaukia ir jo teorema kai $n = 4$. Samprotaudamas kitaip, Fermat įrodė, kad nėra Pitagoro trejetų $a^2 + b^2 = c^2$, jog a ir b būtų sveikųjų skaičių kvadratai. Įrodymas rėmėsi Fermat sukurtu vadinamuoju begalinio nusileidimo metodu. Fermat surado algoritmą, kuriuo iš kiekvieno sprendinio galima gauti kitą sprendinį su mažesniais skaičiais. Iš šio sprendinio gaunamas dar vienas sprendinys su dar mažesniais skaičiais. Procesą galima tęsti neribotai, šitaip gaunant begalinę vis mažesnių sprendinių seką. Tačiau negali būti begalinės mažėjančių sveikųjų teigiamų skaičių sekos, nes mažiausias toks skaičius yra 1. Prieštaros galima išvengti tik atmetus pradinę prielaidą, kad bent vienas sprendinys sveikaisiais skaičiais egzistuoja.

Atveju $n = 3$ teoremą įrodė Leonhard Euler – didysis XVIII amžiaus šveicarų matematikas. Jo įrodymas taip pat remiasi begalinio nusileidimo metodu, tačiau yra sudėtingesnis negu su $n = 4$. Vėlesniais metais buvo įrodyti dar keli atskiri Fermat teoremos atvejai. 1820 metais prancūzų matematikas Adrien Marie Legendre ir vokiečių matematikas P. G. Lejeune Dirichlet sukūrė įrodymą, kai $n = 5$. Dirichlet bandė įrodyti teoremą, kai $n = 7$, tačiau sugebėjo sukurti įrodymą tik, kai $n = 14$; atvejo $n = 7$ įrodymą iš esmės pateikė prancūzas Gabrielis Lamé. Labai arti bendrojo atvejo 1847 metais pavyko pasistūmėti vokiečių matematikui Ernstui E. Kummeriui. Iš Kummerio darbų išplaukia, kad paskutinė Fermat teorema teisinga su be galo daug n reikšmių, būtent su visais n, kurie dalijasi iš „reguliariųjų" pirminių skaičių, sudarančių tam tikrą pirminių skaičių aibės poaibį. Vieninteliai nereguliarieji pirminiai skaičiai, mažesni už 100, yra $37, 59$ ir 67; Kummer vėliau sugebėjo įrodyti teoremą ir šiems pirminiams skaičiams. Taigi paskutinė Fermat teorema buvo įrodyta visiems $n < 100$.

Pastaraisiais metais naudojantis kompiuteriais buvo nustatyta, kad teorema gali būti neteisinga tik su labai dideliais laipsnio rodikliais. 1993 metų liepos mėnesį buvo paskelbta (Buhler, Crandall, Ernvall ir Metsänkylä), kad paskutinė Fermat teorema teisinga su visais n, mažesniais už 4 milijonus. Taigi galimas lygties $a^n + b^n = c^n$ sprendinys būtų sudarytas iš astronominių skaičių (mažiausia c^n reikšmė būtų užrašoma daugiau nei 26 mln. dešimtainių skaitmenų). Tačiau kad ir didelė rodiklių, kuriems teorema teisinga, aibė, ji yra tik baigtinė. Yra be galo daug Kummerio nereguliariųjų pirminių skaičių, todėl paskutinės Fermat teoremos įrodymo negalima užbaigti tiesiog nagrinėjant vieną atvejį po kito.

Ką reikia įrodyti

Moderniųjų laikų požiūris į paskutinę Fermat teoremą yra netiesioginis. Užuot tiesiogiai nagrinėjus Fermat lygtį, analizuojama kitos rūšies lygtis, kurioje skaičiai a^n ir b^n vaidina svarbų vaidmenį.

Kalbant labai bendrai, argumentus galima apibūdinti taip.

Tarkime Fermat lygčiai egzistuoja kontrapavyzdys, arba, kitais žodžiais tariant, egzistuoja skaičių pora a^n ir b^n, kad jų suma yra n-asis natūraliojo skaičiaus laipsnis. Tada turi egzistuoti tam tikras matematinis objektas, vadinamoji elipsinė kreivė, kurią apibrėžia lygtis su koeficientais, nusakomais a^n ir b^n. Pavadinkime šią kreivę tiesiog E. Vienas iš mūsų (Ribet) 1986 metais įrodė, kad ši kreivė negali turėti tam tikros savybės, vadinamos modalumu. Tai, ką Wiles pareiškė birželio mėnesį, trumpai galima suformuluoti taip: klasės, kuriai priklauso ir E, kreivės turi modalumo savybę. Iš šios prieštaros išplaukia, kad E neegzistuoja, todėl neįmanoma rasti kontrapavyzdžio paskutinei Fermat teoremai.

Šiame straipsnyje pateikiame keletą šio samprotavimo detalių. Atskirai paaiškinsime, kas yra elipsinė kreivė ir ką reiškia modalumo savybė. Tikslus įrodymo išdėstymas pareikalautų daug pastangų, taigi apsiribosime pagrindinių momentų paaiškinimu.

Iš pradžių geriausiai būtų patikslinti, ką iš tikrųjų reikia įrodyti. Gali būti suformuluoti specialūs apribojimai lygties $a^n + b^n = c^n$ skaičiams a, b, c ir laipsnio rodikliui n. Visų pirma galime apsiriboti atveju, kai n yra nelyginis pirminis skaičius. Pakanka nagrinėti tik pirminius rodiklius, nes iš bet kurio teoremos kontrapavyzdžio su sudėtiniu n gaunamas kontrapavyzdys su mažesniu pirminiu rodikliu. Kitais žodžiais tariant, jei $a^{pq} + b^{pq} = c^{pq}$ turi sprendinį sveikaisiais skaičiais, tai $a^p + b^p = c^p$ ir $a^q + b^q = c^q$ taip pat turi sprendinius. Vieninteliai sudėtiniai rodikliai, kuriems šis samprotavimas netinka, yra didesni už 2 dvejeto laipsniai, nes jie nesidalija iš nelyginių pirminių skaičių. Tačiau jie dalijasi iš 4 ir paties Fermat įrodymas tinka šiam atvejui. Tiesą sakant, nereikia rūpintis visais skaičių $3, 4, 5, 7$ ir apskritai jokių pirminių ne didesnių už 4 mln. kartotiniais, tačiau konstruojant bendrą įrodymą šie žinomi rezultatai nesuteikia jokių pranašumų. Wileso įrodymas tinka visiems pirminiams n, ne mažesniems už 5.

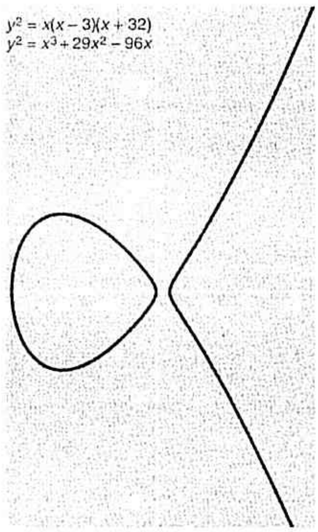
Panašiai gaunama, kad pakanka nagrinėti tik tarpusavyje pirminių a, b ir c atvejį, t.y. kai jie neturi bendrų pirminių daliklių. Analogiškai, jeigu žinomas kontrapavyzdys, kai a, b ir c turi bendrą daugiklį, tai padalijus abi lygybės puses iš atitinkamo daugiklio, gaunamas mažesnis lygties sprendinys.

Suformuluosime dar du teiginius apie skaičių a^n, b^n ir c^n reikšmes, neaiškindami jų detaliau. Tik vienas iš skaičių a, b ir c turi būti lyginis; tarsime, kad tai yra b. Kadangi n yra ne mažesnis už 5, tai b^n dalijasi ne tik iš 2, bet ir iš 2^5, t. y. iš 32. Iš likusių dviejų nelyginių skaičių vienas turi lygti 1 moduliu 4 (dalijant iš 4 gaunama liekaną lygi 1), kitas – lygti 3 moduliu 4.

Nuo šio momento mes iš esmės galime nustumti Fermat lygtį į antrą planą ir naudotis kintamaisiais A, B ir C, atitinkančius a^n, b^n ir c^n. Naujieji kintamieji turi tenkinti nustatytas sąlygas:

$$A + B = C, \quad ABC \neq 0;$$
$$A, B, C \text{ yra tarpusavyje pirminiai;}$$
$$B \text{ dalijasi iš } 32; \quad A = 3 \text{ moduliu } 4; \quad C = 1 \text{ moduliu } 4.$$

Tačiau negalima pamiršti ir paskutinės A, B ir C savybės: A, B ir C tik tada bus Fermat teoremos kontrapavyzdys, kai jie bus n-ieji natūraliųjų skaičių laipsniai, $n \geqslant 5$. Kadangi $a^n b^n c^n = (abc)^n$, tai ir ABC turi būti n-asis laipsnis.



2 brėžinys

Elipsinė kreivė yra geometrinė taškų, tenkinančių tam tikrą kubinę lygtį, vieta. Šios kreivės glaudžiai susiję su paskutine Fermat teorema. Jei ši teorema būtų neteisinga, egzistuotų elipsinė kreivė su ypatingomis savybėmis. Brėžinyje pavaizduota elipsinė kreivė, kurios lygtis $y^2 = x^3 + 29x^2 - 96x$ arba $y^2 = x(x-3)(x+32)$.

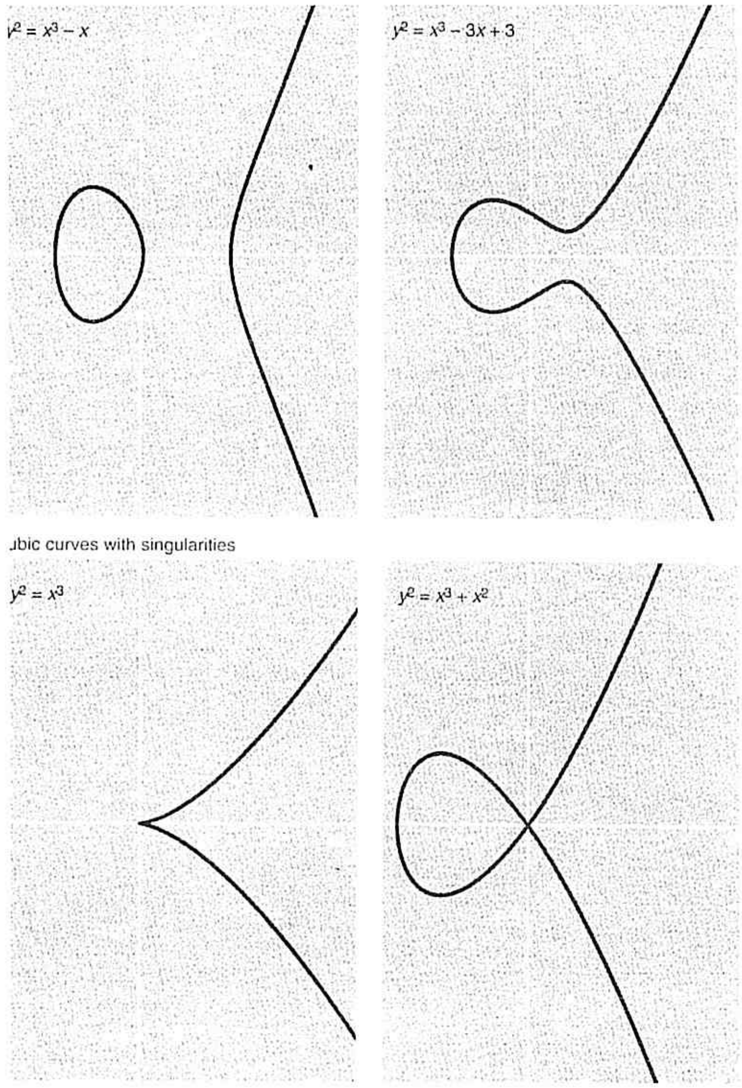
Štai šiuo momentu ir pasirodo elipsinės kreivės. Kreivė, kuri mus domina, apibrėžiama lygtimi

$$y^2 = x(x - A)(x + B);$$

čia skaičiai A, B imami iš anksčiau aptarto hipotetinio kontrapavyzdžio paskutinei Fermat teoremai. (Nors skaičius C ir nepasirodo, informacija nėra prarandama, nes C galime išreikšti suma $A+B$.) Įrodymo strategija tokia: siekiama įrodyti, kad šia lygtimi apibrėžiama kreivė nėra modulinė, tačiau kita vertus, visos elipsinės tam tikros klasės (į ją įeina ir minėtoji kreivė) kreivės, yra modulinės. Vienintelis būdas išvengti prieštaros – atmesti prielaidą, kad skaičiai A, B ir $A + B$, turintys išvardytas savybes egzistuoja.

Elipsinės kreivės

Pertrauksime įrodymo aptarimą ir įvesime įdomius matematinius objektus – vadinamąsias elipsines kreives. Iš pradžių pabrėšime, kad elipsinė kreivė *nėra* elipsė. Pavadinimas atspindi ryšį su elipsinėmis funkcijomis, kurios buvo sugalvotos norint palengvinti elipsės perimetro skaičiavimą; vėliau pasirodė, kad jas galima pritaikyti ir kitiems tikslams. Elipsinės kreivės yra plokštumos kreivės, apibrėžiamos tam tikromis kubinėmis lygtimis, jų forma nė iš tolo nepriminena elipsės.



3 brėžinys

Kubinės lygtys apibrėžia įvairios formos kreives. Tik kai kurias iš jų galime pavadinti elipsinėmis kreivėmis. Viršutiniai brėžiniai vaizduoja elipsines kreives. Pirmoji sudaryta iš dviejų nesusijusių dalių, antroji – iš vienos. Apatinės kreivės nėra elipsinės kreivės, nes jos turi singuliarumo taškų, t.y. tokių taškų, kuriuose liestinės nėra vienareikšmiškai apibrėžtos. Taškas (0,0) abiems kreivėms yra singuliarumo taškas.

• • • $\alpha + \omega$ • • •

Galime sukonstruoti specialią elipsinę kreivę parinkdami užrašytoje lygtyje skaičių A, B reikšmes. Sąlygos šiems skaičiams reikalauja, kad A dalybos iš 4 liekana būtų 3, taigi paprasčiausia reikšmė $A = 3$. Analogiškai, kadangi B turi dalytis iš 32, galima imti $B = 32$. (Suprantama, $A = 3$ ir $B = 32$ nėra paskutinės Fermat teoremos kontrapavyzdys; tai tik skaičiai, tenkinantys tam tikras sąlygas, kurias turi tenkinti ir kontrapavyzdžio skaičiai.) Su šiais skaičiais gauname lygtį

$$y^2 = x(x-3)(x+32);$$

sudauginę dešinės pusės narius gausime ekvivalenčią išraišką

$$y^2 = x^3 + 29x^2 - 96x.$$

Pabrėšime, kad gautoji lygtis yra kubinė, nes didžiausias kintamųjų laipsnis yra kubas; tačiau tai speciali lygtis, siejanti y^2 su x^3. Taip pat pabrėšime, kad lygties koeficientai yra sveikieji skaičiai. Apskritai elipsinės kreivės lygties koeficientai gali būti bet kokie skaičiai, bet čia nagrinėjamų kreivių koeficientai, jeigu nepadaryta išlyga, yra sveikieji skaičiai.

Lygtis, kurią ką tik sudarėme, apibrėžia kreivę x, y plokštumoje. Kreivė yra geometrinė vietą taškų, kurių koordinatės x, y tenkina lygtį. Pavyzdžiui, taškas $(0, 0)$ yra ant šios kreivės, nes įstatę $x = y = 0$ gauname teisingą teiginį. Kreivė, apibrėžta minėta lygtimi, pavaizduota 2 brėžinyje. Ją sudaro dvi nesikertančios dalys: uždara kilpa y ašies kairėje ir begalinė šaka dešinėje. Tiksli kreivės forma priklauso nuo koeficientų reikšmių. Kai kuriais atvejais kreivė susideda iš vienos dalies.

Ne kiekvieną kubinę lygtį atitinka elipsinė kreivė. Elipsinė kreivė yra glodi, arba nesinguliari. Šią sąvoką tiksliau paaiškinsime tarę, kad kiekviename taške kreivė privalo turėti liestinę. Kreivė negali turėti smaigalių, kuriuose liestinė neapibrėžta, arba mazgo taškų, kuriuose kreivė kerta pati save ir turi dvi ar daugiau liestinių. Dvi glodžios elipsinės kreivės ir dvi kubinės kreivės, turinčios singuliarių taškų pavaizduotos 3 brėžinyje.

Algebriniu požiūriu reikalavimas, kad kreivė būtų nesinguliari, ekvivalentus reikalavimui, kad lygtis turėtų tris skirtingas šaknis, t. y., su trimis skirtingomis x reikšmėmis reiškinys $x(x-A)(x-B)$ būtų lygus nuliui. Akivaizdu, kad viena šaknis $x = 0$, o kitos – $x = A$ ir $x = -B$. Taigi elipsines kreives atitinka lygtys su apribojimais $A \neq 0, B \neq 0$ ir $A \neq -B$. Paskutinę sąlygą galime suformuluoti taip: $A + B \neq 0$, arba $C \neq 0$, taigi bendras reikalavimas yra $ABC \neq 0$.

Kodėl matematikai tiek dėmesio skyrė šiai vienai kreivių šeimai? Juk yra be galo daug siejančių x ir y polinominių lygčių, kurias atitinka begalinė plokštumos kreivių įvairovė. Vienas iš galimų atsakymų yra toks: elipsinės kreivės sudaro pirmąją, Diofanto požiūriu, netrivialią kreivių klasę.

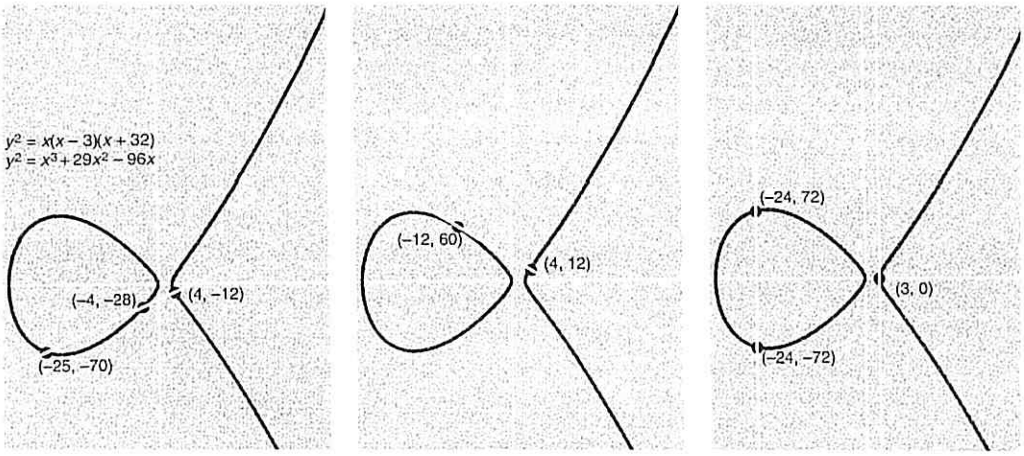
Visos plokštumos kreivės – arba jas atitinkančios lygtys – gali būti suskirstytos pagal jų *rūšį*; rūšis yra skaičius, glaudžiai susijęs su lygties laipsniu. Kalbant tiksliau, nesinguliarios kreivės, kurią apibrėžia d laipsnio polinominė lygtis, rūšis lygi $(d-1)(d-2)/2$. Tiesės ir kūgio pjūviai – elipsės, parabolės ir hiperbolės – apibrėžiami tiesinėmis ($d = 1$) arba kvadratinėmis lygtimis ($d = 2$), todėl visų jų rūšis lygi 0. Elipsinių kreivių, kurios pagal apibrėžimą yra nesinguliarios, o jas atitinkančios lygtys yra trečiojo laipsnio, rūšis lygi 1. Nesinguliarios ketvirtojo, penktojo ir aukštesniųjų eilių kreivės turi didesnes rūšis. Louis J. Mordell 1922 metais pastebėjo, kad lygties rūšis susijusi su jos racionaliųjų sprendinių skaičiumi, arba taškų su racionaliomis koordinatėmis, per kuriuos eina kreivė, skaičiumi. Jau buvo žinoma, kad nulinės rūšies kreivės arba neturi racionaliųjų sprendinių, arba jų turi be galo daug; begalinio sprendinių skaičiaus atvejus visada nesunku aprašyti. Mordell suformulavo hipotezę, kad didesnės už 2 rūšies kreivės turi daugiausiai baigtinį racionaliųjų sprendinių skaičių. 1983 metais matematinės bendruomenės nuostabai Mordello hipotezę įrodė Gerd Faltings, jaunas matematikas, tuomet dirbęs Vokietijoje, Wuppertalio universitete. Liko tarpinis 1 rūšies – elipsinių kreivių atvejis, kai nėra paprasto būdo nustatyti, ar sprendinių skaičius baigtinis, ar begalinis.

Kirstinės ir liestinės

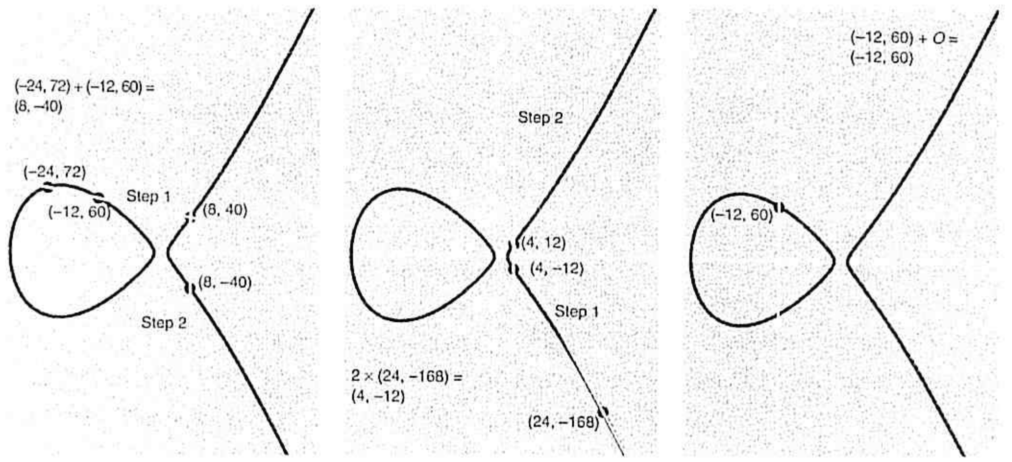
Taškų su racionaliomis koordinatėmis ant elipsinės kreivės gali būti be galo daug arba tik baigtinis skaičius. Tai priklauso nuo lygties koeficientų. Visais atvejais racionaliųjų taškų aibės struktūra yra turtinga, tai leidžia ją sistemingai tyrinėti.

Bet kuriuos du elipsinės kreivės taškus – racionaliuosius ar iracionaliuosius – sujungus atkarpa arba kirstine, ją galima pratęsti, kad ji kirstų kreivę trečiajame taške. Akivaizdžią šios taisyklės išimtį sudaro taškai, kurių x koordinatė yra ta pati. Tada kirstinė yra lygiagreti su y ašimi. Šios „vertikalios“ kirstinės gali būti pratęstos į begalybę, bet elipsinės kreivės nebekirs. Vertikalių kirstinių išimtinė padėtis gali būti panaikinta papildžius kreivę vienu begalybėje esančiu tašku, įsivaizduojant, kad visos vertikalios tiesės eina per tą tašką. Šis ypatingas taškas vadinamas pradiniu tašku, jis žymimas raide O; taigi visos vertikaliosios kirstinės eina per O. Vadinasi papildžius kreivę pradžios tašku, galima tarti, kad kiekviena kirstinė kerta elipsinę kreivę tiksliai trijuose taškuose.

Analogišką teiginį galima pasakyti apie elipsinės kreivės liestines: kiekviena liestinė, be lietimosi taško, kerta kreivę dar viename taške. Ypatingu atveju, kai liestinė yra vertikali, kitas taškas yra pradžios taškas O. Liestinę galime įsivaizduoti kaip kirstinių, einančių per du vis arčiau ir arčiau vienas kito esančius elipsinės kreivės taškus, ribinę padėtį, gaunamą, kai abu taškai galų gale sutampa. Taigi liestinę galime laikyti kirstine, einančia per tą patį tašką du kartus. Šitaip samprotaudami galime tvirtinti, kad kiekviena elipsinės kreivės kirstinė ar liestinė kerta kreivę trijuose taškuose. Kad visos elipsinės kreivės turėtų šią savybę, kubinės kreivės su singuliarumo taškais nepriskiriamos elipsinių kreivių šeimai, nes smaigalio ar kituose singuliarumo taškuose liestinės nėra vienareikšmiškai apibrėžtos.



4 brėžinys
Kirstinių ir liestinių procesas parodo racionaliųjų elipsinės kreivės taškų ryšius. Procedūra atliekama taip. Pasirinkę du racionaliuosius taškus, sujunkime juos atkarpa ir pratęskime ją į abi puses. Gautoji tiesė bus kirstinė, kertanti kreivę trečiajame racionaliajame taške (kairysis brėžinys), arba liestinė viename iš pasirinktųjų taškų (antrasis brėžinys). Liestinę galime laikyti „išsigimusia" kirstine, kuri eina per tą patį tašką du kartus. Tada ir apie liestinę galėsime sakyti, kad ji turi su kreive tris bendrus taškus. Vienintelę išimtį sudaro vertikalios liestinės (trečiasis brėžinys). Kad panaikintume šią išimtį, įvedame ypatingąjį (pradinį) tašką. Galime jį įsivaizduoti kaip be galo nutolusį tašką, per kurį eina visos tiesės lygiagrečios su Oy ašimi.



5 brėžinys
Racionalieji elipsinės kreivės taškai sudaro grupę, kurios operaciją galima apibrėžti naudojantis kirstinėmis ir liestinėmis. Vadinsime šią operaciją tiesiog sudėtimi. Kairiajame brėžinyje parodyta, kaip sudedami du skirtingi kreivės taškai. Nubrėžus kirstinę per šiuos taškus, randamas trečiasis elipsinės kreivės taškas, tada šis taškas sujungiamas su pradžios tašku (t.y. per tašką nubrėžiama lygiagreti Oy ašiai tiesė). Ši tiesė kerta elipsinę kreivę dar viename taške, būtent jis ir laikomas pasirinktųjų racionaliųjų taškų suma. Kairiajame brėžinyje pavaizduota sudėtis $(-24, 72) + (-12, 60) = (8, -40)$. Jei reikia prie taško pridėti jį patį, tai pirmajame žingsnyje brėžiama liestinė. Antrasis brėžinys vaizduoja veiksmą $(24, -168) + (24, -168) = (4, -12)$. Trečiajame brėžinyje parodyta, kad sudėjus tašką su pradžios tašku, vėl gaunamas tas pats taškas.

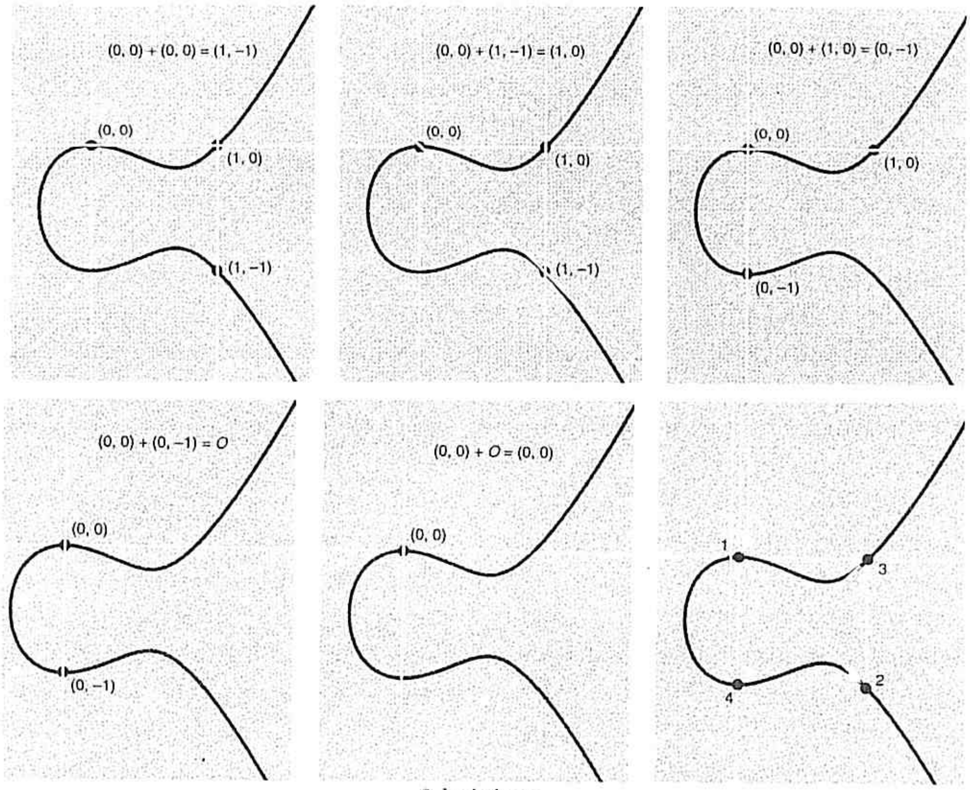
Geometrija, kuria remiasi ši elipsinių kreivių kirstinių ir liestinių konstrukcija, darosi dar įspūdingesnė, panagrinėjus racionaliuosius kreivės taškus, t.y. taškus, kurių x ir y koordinatės yra racionalieji skaičiai. Jeigu kirstinė brėžiama per du racionaliuosius taškus, trečiasis kirtimosi taškas taip pat yra racionalus (žr. 4 brėžinį). Analogiškai kitas racionaliojo taško liestinės ir kreivės susikirtimo taškas taip pat yra racionalusis. (Kad toks tvirtinimas neturėtų išimčių, pradžios taškas O taip pat laikomas racionaliuoju.) Taigi mokėdami brėžti kirstines ir liestines galime generuoti racionaliuosius taškus: turėdami vieną ar du racionaliuosius taškus, galime tiesiogiai surasti jų ir daugiau. Maža to, iš Mordello teoremos išplaukia, kad visi racionalieji kreivės taškai gali būti gauti naudojant liestinių ir kirstinių procedūrą iš tam tikros baigtinės racionaliųjų taškų aibės.

Įvedus tam tikrus patobulinimus, elipsinės kreivės racionaliųjų taškų aibė įgyja matematinės grupės struktūrą. Grupę sudaro elementų aibė ir tam tikras kompozicijos dėsnis – būdas iš dviejų elementų gauti kitą grupės elementą. Klasikinis grupės pavyzdys – sveikųjų skaičių aibė, kurioje apibrėžta sudėties operacija. Sudedant du sveikuosius skaičius, visada gaunamas sveikasis skaičius. Grupė turi turėti vienetinį elementą, kurio vaidmenį skaičių sudėties atveju atlieka nulis; kiekvienam sveikajam n, $n + 0 = n$. Kiekvienas elementas n turi turėti atvirkštinį, kurį sudėję su n, gauname vienetinį elementą; sveikųjų skaičių sudėties atveju skaičiaus n atvirkštinis yra $-n$.

Elipsinės kreivės racionalieji taškai sudaro grupę su šiek tiek sudėtingesniu negu aukščiau išdėstytas kirstinių ir liestinių procesas kompozicijos dėsniu. Kaip veikia kompozicijos procedūra parodyta 5 brėžinyje. Norėdami „sudėti" taškus p ir q, pratęskime kirstinę, einančią per juos. Raskime trečiąjį kirtimosi tašką, kurį pažymėkime r. Dabar išveskime kirstinę per pradžios tašką O ir r, o ją pratęsę gausime kitą tašką r'. Šis naujasis taškas r' ir yra taškų p ir q „suma". Taško O įvedimo priežastis yra kaip tik ta, kad jis atlieka vienetinio elemento vaidmenį. Su bet kokiu tašku p teisinga lygybė $p + O = p$. Taigi grupės kompozicijos dėsnis apibrėžia racionaliųjų elipsinės kreivės taškų aritmetiką.

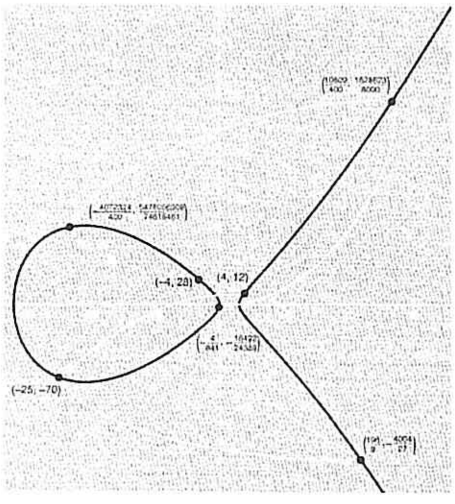
Ypač svarbi aritmetinė operacija, kai taškas sudedamas su pačiu savimi. Geometriškai šis procesas atliekamas naudojantis ne kirstine, bet liestine. Aritmetikos požiūriu tai daugybos iš sveikojo skaičiaus analogas. Suma $P + P$ yra ekvivalenti sandaugai $2P$. Dar kartą prie gauto rezultato pridėjus P, gauname $3P$, ir pan. Su kai kuriais taškais šis procesas gali būti neribotai tęsiamas niekada nesugrįžtant į ankstesnius taškus: sakoma, kad tokių taškų eilė yra begalinė. Kitus, baigtinės eilės taškus sudėjus su jais pačiais baigtinį skaičių kartų, gaunamas O, pridėjus P dar kartą pagal apibrėžimą vėl gaunamas P ir baigtinė taškų seka kartojasi. Baigtinės ir begalinės eilės taškų pavyzdžiai parodyti 6 ir 7 brėžiniuose.

Ką bendro elipsinių kreivių aritmetika turi su paskutine Fermat teorema? Ryšys atsiranda per modulinių kreivių sąvoką, arba susijusią modulinę formą. Kaip tik tai dabar ir aptarsime.



6 brėžinys

Kartodami sudėtį nustatome taško eilę. Brėžiniuose parodyta elipsinė kreivė, kurios lygtis $y^2 + y = x^3 + x^2$. Taškas $(0,0)$ sudedamas su pačiu savimi, po to prie sumos vėl pridedamas $(0,0)$ ir t.t. Pirmas brėžinys vaizduoja sudėtį $(0,0)+(0,0) = (1,-1)$, antrasis – $3\times(0,0) = (1,-1)+(0,0) = (1,0)$. Trečiajame brėžinyje matome, kad $4\times(0,0) = (1,0)+(0,0) = (0,-1)$, ketvirtajame – $5\times(0,0) = (0,-1)+(0,0) = O$. Penktasis brėžinys rodo, kad dar viena sudėtis grąžina atgal: $O+(0,0) = (0,0)$. Taigi taškas $(0,0)$ yra penktos eilės. Paskutiniame brėžinyje parodyta viso proceso eiga.



7 brėžinys

Kai kurie elipsinės kreivės taškai gali būti begalinės eilės. Juos sudedant niekada nepasiekiamas pradinis taškas. Visi racionalieji elipsinės kreivės $y^2 = x(x-3)(x+32)$, išskyrus $(0,-32), (0,0)$ ir $(0,3)$ yra begalinės eilės. Brėžinyje parodytas sudėties procesas, prasidedantis taško $(-4,28)$ sudėtimi su savimi pačiu. Procesas gali būti tęsiamas ir tęsiamas, bet pradžios taško nepasieksime.

Ką reiškia būti moduline kreive

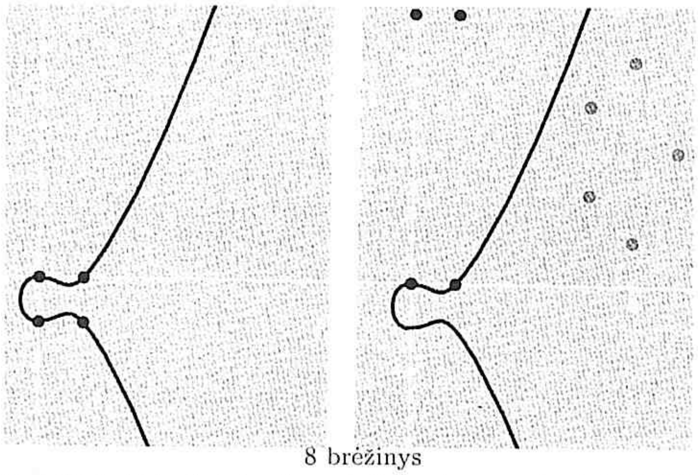
Elipsinių kreivių tyrimo užuomazgų galime rasti Fermat ir netgi Diofanto darbuose, modulinės formos atsirado XIX šimtmetyje, tačiau abi sritys buvo glaudžiai susietos tik 1955 metais. Tais metais Yutaka Taniyama, jaunas japonų matematikas, iškėlė drąsią hipotezę, kuri iš pradžių buvo suformuluota konferencijos metu kaip tam tikrų uždavinių seka. Tikslesnę formą hipotezei suteikė Goro Shimura iš Princetono universiteto, dabar ji vadinama Taniyama–Shimura hipoteze. Ji tvirtina, kad visos elipsinės kreivės su racionaliaisiais koeficientais yra modulinės. Iš pradžių į šį tvirtinimą buvo žiūrima skeptiškai, bet laikui bėgant juo vis labiau buvo linkstama tikėti. Dar prieš tai, kai Wiles pradėjo ieškoti Taniyama–Shimura hipotezės įrodymo, daugelis matematikų manė, kad ji tikriausiai teisinga.

Viena iš priežasčių, kad iš pirmo žvilgsnio Taniyama–Shimura hipotezė atrodo tokia neįtikėtina, yra ta, kad elipsinės kreivės ir modulinės formos yra labai skirtingi objektai. Norėdami suprasti, kaip jie susiję, vėl nagrinėkime elipsinės kreivės racionaliuosius taškus. Apie šiuos nagrinėjamos kreivės taškus galima suformuluoti daug klausimų. Kiek jų yra? Jeigu jų aibė baigtinė, ar yra būdas juos suskaičiuoti? Ar yra dėsniai, pagal kuriuos šie taškai išsidėsto ant kreivės? Ar taškus galima klasifikuoti?

Bandant atsakyti į tokius klausimus į elipsinę kreivę apibrėžiančią lygtį naudinga pažvelgti ne kaip į lygtį, bet kaip į lyginį tam tikru pirminiu moduliu p. Kitais žodžiais tariant, lygtis „redukuojama" visas x ir y reikšmes dalijant iš p ir paliekant tik liekanas. Šį procesą galima pailiustruoti elipsinės kreivės, kurią apibrėžia lygtis $y^2 + y = x^3 - x^2$, pavyzdžiu. Kreivė turi tik penkis racionaliuosius taškus: $(0,0)$, $(0,-1)$, $(1,0)$, $(1,-1)$ ir pradžios tašką. Visi šie taškai lieka lygties sprendiniais ir moduliu 7. Tačiau kai lygtis redukuojama moduliu 7, sprendiniais tampa kai kurie papildomi, nepriklausantys kreivei taškai. Pavyzdžiui, taškas $(5,1)$ tampa sprendiniu, nes 1^2+1 moduliu 7 lygsta 5^3-5^2 moduliu 7 (abu skaičiai turi tą pačią, lygią 2, dalybos iš 7 liekaną). Redukuojant moduliu 5, gaunama kitokia sprendinių taškų aibė, redukuojant moduliu 13 vėl kitokia.

Apskritai redukcija nėra įmanoma pagal bet kuriuos pirminius. Po redukcijos lygtis turi apibrėžti nesinguliarią kreivę. Vadinasi, trys jos šaknys moduliu p turi būti skirtingos. Lygčiai $y^2 = x(x-A)(x+B)$, čia A ir B tenkina visus aukščiau suformuluotus reikalavimus, ši sąlyga teisinga visiems p, kurie nedalija sandaugos $AB(A+B)$, arba ABC. Specialiai kreivei $y^2 = x(x-3)(x+32)$ šie leistinieji pirminiai skaičiai yra tie, kurie nedalija $3 \times 32 \times 35 = 3360$. Taigi kreivės negalima redukuoti pirminių $p = 2, 3, 5, 7$ atžvilgiu, nes jie dalija 3360. Pirminių skaičių, kurie dalija ABC, sandaugą – šiuo atveju $2 \times 3 \times 5 \times 7 = 210$ – vadinama elipsinės kreivės *konduktoriumi*; jis nurodo pirminių skaičių, kurių atžvilgiu redukcija yra „bloga", aibę.

Kas gi laimima redukuojant elipsinę kreivę moduliu p? Vienu požiūriu nauda akivaizdi: redukuotos kreivės racionaliųjų taškų aibė yra baigtinė. Nagrinėti baigtinį objektą dažnai yra paprasčiau negu begalinį. Be viso to, galima turėti vilties, kad šie „lokalieji" sprendiniai, susiję su tam tikru pirminiu, gali atskleisti ką nors ir apie pradinės lygties „globaliuosius" sprendinius. Atskiru atveju elipsinę kreivę galima tirti skaičiuojant sprendinius moduliu p daugeliui pirminių p (nenagrinėjant tų, kurie dalija ABC).



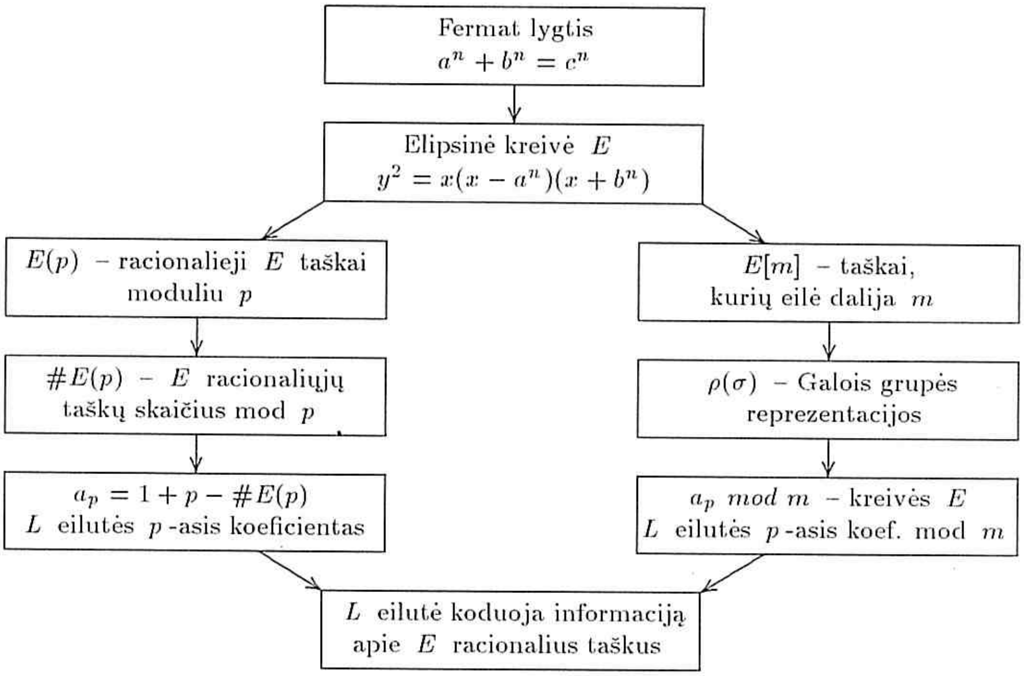
8 brėžinys

Redukuodami elipsinės kreivės lygtį moduliu p (p yra pirminis skaičius), gauname naują taškų, kuriuos galima laikyti lygties sprendiniais, aibę. Lygtis $y^2 + y = x^3 + x^2$ turi tik penkis racionaliuosius sprendinius: $(0,0),(1,0),(0,-1),(1,-1)$ ir pradžios tašką O. Redukavus lygtį moduliu 7 prisideda dar penki taškai (dešinysis brėžinys). Pradiniai taškai irgi išlieka sprendiniais, tik $(0,-1),(1,-1)$ redukavus užrašomi kaip $(0,6),(1,6)$.

Taškų skaičiaus didėjimo, didėjant p, tyrimas atskleidžia informaciją apie kreivę ir, atskiru atveju, apie racionaliųjų taškų grupės dėsnį. Ši informacija koduojama matematiniu objektu – vadinamąja L eilute, sudaroma naudojant tam tikrus skaičius a_p, nurodančius, kiek taškų moduliu p atitinka pirminius skaičius p. Tikslus L eilutės ir racionaliųjų taškų grupės ryšis formuluojamas dar neįrodytoje hipotezėje; pagrindinę idėją galima paaiškinti taip: kreivė, turinti daug racionaliųjų taškų, turėtų jų turėti daug ir moduliu p su įvairiais p. Atvirkštinis teiginys taip pat turėtų būti teisingas.

Visa L eilutė reiškiama begaline sandauga, kurioje slypi informacija, susijusi su be galo daug pirminių skaičių, tačiau kiekvienai specialiai elipsinei kreivei norimu tikslumu baigtinė aproksimacija gali būti sudaryta, tiesiogiai skaičiuojant racionaliuosius taškus daugelio pirminių skaičių moduliais. Šis procesas reikalauja daug pastangų, o L eilutės forma, gaunama šiuo būdu, yra sunkiai panaudojama kitiems skaičiavimams. Modulinės formos labai supaprastina padėtį – bent jau kai kurių, o gal būt ir visų elipsinių kreivių atveju.

Modulinės formos atsirado visiškai kitoje matematikos karalystėje: jos yra analizinės funkcijos, apibrėžtos kompleksiniams skaičiams. (Kompleksiniai skaičiai sudaryti iš realiosios ir menamosios dalies; menamoji dalis yra realiojo skaičiaus ir i sandauga; i yra skaičius, kurio kvadratas lygus -1.) Realieji skaičiai gali būti išdėstyti ant tolydžios tiesės, analogiškai kompleksinius skaičius galima išdėstyti plokštumoje, taškus su koordinatėmis x, y atitinka kompleksiniai skaičiai $x + iy$. Modulinės formos apibrėžtos viršutinėje kompleksinių skaičių plokštumos pusplokštumėje, kurią sudaro taškai su $y > 0$. Kitais žodžiais tariant, modulinė forma yra funkcija, kuri kiekvienam kompleksiniam skaičiui iš viršutinės pusplokštumės priskiria kitą kompleksinį skaičių (galbūt tą patį).



9 brėžinys
L eilutės yra matematinis objektas, vaidinantis labai svarbų vaidmenį Fermat teoremos įrodyme. Šias eilutes galima sudaryti dviem būdais. Einant vienu keliu (diagramos kairėje) elipsinė kreivė E redukuojama moduliu p su daugeliu pirminių p. Tam tikra formulė susieja L eilutės koeficientus su redukuotų kreivių racionaliųjų taškų skaičiais. Einant kitu keliu (dešinėje), nagrinėjamos taškų, kurių eilės dalija įvairius skaičius m, aibės $E[m]$. Transformacijų grupė, veikianti šioje aibėje suteikia informacijos apie L eilutės koeficientus.

Reikšmingas bruožas, išskiriantis modulines formas iš kitų kompleksinės analizės funkcijų, yra tas, kad jos yra invariantiškos (t.y. nesikeičia) atliekant tam tikras viršutinės pusplokštumės transformacijas. Šios transformacijos, nusakomos kvadratinėmis sveikųjų skaičių matricomis, vadinamos trupmeniniais tiesiniais atvaizdžiais. Pavyzdžiui, kiekviena modulinė forma f nesikeičia atliekant sveikaskaičius postūmius: reikšmė $f(z)$ su visais kompleksiniais skaičiais z yra lygi reikšmei $f(z+1)$. Kitais atvejais modulinės formos nėra griežtai invariantiškos, bet naujoji reikšmė gaunama iš senos, dauginant iš to paties paprasto daugiklio. Modulinės formos f „lygis" yra tam tikras teigiamas skaičius, apibrėžiantis trupmeninių tiesinių transformacijų, nepakeičiančių f, aibę. Kalbant ne visiškai tiksliai, N lygio modulinių formų erdvė didėja, didėjant N. Pavyzdžiui, dvylikto ar mažesnio už dešimt lygio modulinių formų nėra, tačiau yra vienuolikto lygio modulinė forma; ji yra vienintelė tokia prasme: kitos to paties lygio modulinės formos gaunamos dauginant pradinę iš skaičiaus.

Svarbi modulinių formų savybė, siejanti jas su paskutine Fermat teorema ir Taniyama–Shimura hipoteze, yra ta, kad pagal modulines formas sudaromos L eilutės, analogiškos L eilutėms, atsirandančioms iš elipsinių kreivių. Kadangi tiek modulinės formos, tiek L eilutės yra kompleksinės analizės objektai, L

eilutės, susijusios su elipsine kreive tyrimas tampa paprastesnis, kai nustatoma, kad ta pati L eilutė taip pat susijusi ir su moduline forma. Taniyama–Shimura hipotezė kaip tik ir tvirtina, kad kiekvienai elipsinei kreivei egzistuoja tokia modulinė forma, kad ta pati L eilutė atitinka tiek elipsinę kreivę, tiek modulinę formą.

Kadangi elipsinės kreivės yra algebros objektai, Taniyama–Shimura hipotezė atspindi glaudų algebros ir kompleksinės analizės ryšį. Hipotezė iš pradžių atrodė mažai tikėtina, tačiau dabar jos naudai byloja daug skaitinių duomenų bei filosofinių argumentų. Wileso pateiktas hipotezės įrodymas didelei elipsinių kreivių klasei dar labiau paremia nuomonę, kad šis įspūdingas sąryšis tikrai teisingas.

Įrodymas, kad E nėra modulinė

Įvykių grandinę, kurią vainikavo Wileso pareiškimas tą įsimintiną vasarą, išjudino 1985 metais Gerhardo Frey iš Saarlando universiteto Vokietijoje hipotezė. Būtent Frey atkreipė dėmesį į lygtis $y^2 = x(x - A)(x + B)$, sudarytas su A, B iš tariamojo Fermat paskutinės teoremos kontrapavyzdžio. Atitinkama elipsinė kreivė dabar dažnai vadinama Frey kreive. Frey suprato, kad dėl sąlygų, kurias turi tenkinti A ir B, elipsinė kreivė $y^2 = x(x - A)(x + B)$ negali būti modulinė. Jis negalėjo pateikti griežto įrodymo, tačiau Jean-Pierre Serre iš Colège de France greitai tiksliai suformulavo, ką reikia padaryti, kad Frey įžvalga būtų įrodyta: jis suformulavo tikslią hipotezę apie modulines formas, kurią įrodžius iš karto būtų gauta, kad Frey hipotezė yra teisinga. Po metų Ribet pateikė įrodymą. Šis rezultatas nustatė tiesioginį ryšį tarp elipsinių kreivių ir paskutinės Fermat teoremos, nes Taniyama–Shimura hipotezė tvirtina, kad **visos** elipsinės kreivės yra modulinės.

Kaip galima įrodyti, kad elipsinė kreivė yra arba nėra modulinė? Specialiai lygčiai su žinomais, skaitiniais koeficientais yra skaitiniai metodai, leidžiantys atsakyti į šį klausimą; metodai reikalauja daug darbo, tačiau yra patikimi. Tačiau šiuo atveju skaitinių metodų negalima pritaikyti, nes kreivės egzistavimas yra tariamas. Mes galime užrašyti Frey lygtį $y^2 = x(x - A)(x + B)$, bet nežinodami paskutinės Fermat teoremos kontrapavyzdžio, negalime įstatyti skaitinių A ir B reikšmių; kita vertus, jei teorema teisinga, tokių reikšmių iš viso nėra. Kadangi skaičiavimų negalime atlikti neužrašę kreivės lygties aiškia forma, tenka ieškoti kitos, netiesioginės strategijos.

Pirmąjį šio proceso žingsnį sudaro specialaus elipsinių kreivių taškų pogrupio tyrimas. Kreivei E ir pasirinktajam sveikajam skaičiui m šį pogrupį pažymėsime $E[m]$. Jį sudaro taškai, kurių eilė dalo m. Tokie taškai vadinami m dalybos taškais. Priminsime, kad taško eilė yra skaičius, nurodantis, kiek kartų prie taško reikia reikia pridėti jį patį, kad gautume pradžios tašką O. Taigi grupę $E[m]$ sudaro tie taškai, kurių m-asis kartotinis (arba suma iš m vienodų, lygių tam pačiam taškui dėmenų) lygus pradžios taškui. Naudinga patyrinėti šią keistą taškų seką. Jeigu elipsinė kreivė E yra modulinė, $E[m]$ tyrinėjimas atskleidžia informaciją apie su E susijusią modulinę formą. Negana to, yra tam tikra būdas apibrėžti $E[m]$ modalumą; įrodžius kad be galo daugeliui m $E[m]$ yra modulinės grupės, galima įrodyti, kad pati kreivė E

yra modulinė. Ir atvirkščiai, įrodžius, kad $E[m]$ nėra modulinė tam tikroms m reikšmėms, galima teigti, kad ir E negali būti modulinė.

Tenka padaryti dvi pastabas. Visų pirma, kai kurios elipsinės kreivės turi begalinės eilės taškų, nepriklausančių jokiai aibei $E[m]$. Kita vertus, $E[m]$ taškų koordinatės nebūtinai sveikieji ar net racionalieji skaičiai. Daugiausia, ką galima pasakyti, – koordinatės yra algebriniai skaičiai, t.y. algebrinės lygties su racionaliaisiais koeficientais sprendiniai.

Kaip galima įrodyti, kad tam tikriems m $E[m]$ nėra modulinė? Svarbiausia reikšmė $m = n$, čia n yra Fermat paskutinės teoremos lygties laipsnis. Kaip minėta anksčiau, jei A, B, C yra kontrapavyzdžio skaičiai, tai ABC yra tikslus n-asis sveikojo skaičiaus laipsnis. Tačiau, kai ABC yra n-asis laipsnis, grupė $E[n]$ turi tam tikrų neįprastų savybių, panašių į elipsinės kreivės su konduktorium, lygiu 2, n-dalybos taškų savybes. Tačiau jau yra žinoma, kad elipsinių kreivių su konduktorium 2 nėra; mažiausias įmanomas konduktorius lygus 11. Labai panašu, kad spėjamas ryšys su konduktoriaus, lygaus 2, kreivėmis gali padėti rasti prieštarą, kuri leistų paskutinę Fermat teoremą įrodyti tiesiogiai, nesinaudojant Taniyama–Shimura hipoteze. Deja, niekam dar nepavyko šių užuominų paversti griežtu įrodymu. Įrodymas, kad $E[n]$ nėra modulinė, gautas aplinkiniu keliu. Padarius prielaidą, kad $E[n]$ yra modulinė, reikia ją susieti su minimalaus lygio moduline forma. Esminė įrodymo dalis – įrodyti, kad šis lygis lygus 2, tačiau tai yra neįmanoma, nes lygio 2 modulinių formų nėra.

Prie tokios išvados vedantis samprotavimas yra sudėtingas, kelias vingiuoja per dar didesnę moderniosios aritmetikos tankmę. Išeities taškas – transformacijų grupės, vadinamosios Galois grupės, veikimo aibėse $E[m]$ kiekvienai m reikšmei tyrimas. Galois grupės čia neapibrėšime, pakaks pasakyti, kad kiekvienas šios grupės elementas „sumaišo“ $E[m]$ taškus, tačiau išlaiko sudėties dėsnį. Tarkime, kad σ yra Galois grupės elementas, o P yra $E[m]$ taškas. Jei $mP = O$, tai ir $m(\sigma P) = O$.

Keitiniai, indukuoti Galois grupės elementų, gali būti vaizduojami 2×2 matricomis, kurių elementai yra sveikieji skaičiai moduliu m. Transformacijos, kurią generuoja elementas σ, matricą pažymėkime $\rho(\sigma)$. Sakoma, kad matricos sudaro Galois grupės reprezentaciją. Verta pažymėti, kad reprezentacija išlaiko Galois grupės kompozicijos dėsnį; jeigu σ ir τ yra grupės elementai, kurių kombinacija yra transformacija ν, tai matrica $\rho(\nu)$ lygi matricų $\rho(\sigma)$ ir $\rho(\tau)$ sandaugai.

Stabtelėkime ir apžvelkime nueitą kelią. Mes pradėjome nuo elipsinės kreivės E, kurią apibrėžia lygtis su skaičiais A, B iš tariamo paskutinės Fermat teoremos kontrapavyzdžio. Po to perėjome prie diskrečios taškų aibės $E[m]$, į kurią įeina taškai, kurių eilė dalija sveikąjį skaičių m. Mes ištyrėme, kaip tam tikra Galois grupė veikia aibėje $E[m]$, ir atskiru atveju nagrinėjome šios grupės reprezentaciją 2×2 matricomis. Dabar jau galime nustatyti ryšį su moduliškumu. Pasirodo, kad transformacijų grupė, prie kurios priartėjome su šiais sudėtingais argumentais, suteikia informacijos apie kreivės E L eilutę. Egzistuoja formulė šioms eilutėms generuoti. Ja naudojantis ja gali būti apibrėžiamas moduliškumas.

Galois grupės ir L eilučių ryšys atsiranda šitaip. Kaip jau buvo minėta,

L eilutės koeficientai skaičiuojami redukuojant kreivę E įvairiais pirminiais moduliais p. Kiekvienas p duoda vieną eilutės narį; kalbant tiksliau, L eilutės koeficientas a_p lygus $1 + p$ ir E, redukuotos moduliu p, racionaliųjų taškų skaičiaus skirtumui. Tačiau m dalumo taškų aibė $E[m]$ pateikia kitą koeficientų a_p interpretacijos būdą, bent jau daugeliui pirminių p. Kiekvienam p yra tam tikras Galois grupės elementas σ_p, kurio atitinkama matrica $\rho(\sigma_p)$ priklauso nuo m ir p. Dviejų šios matricos įstrižainės elementų suma moduliu m kongruenti su skaičiumi a_p.

Ribet įrodymo, kad Frey elipsinė kreivė negali būti modulinė, išeities tašką sudaro galimybė koeficientus moduliu p atkurti iš Galois teorijos. Jeigu tarsime, kad E iš tikrųjų yra modulinė kreivė, tai anksčiau minėtos neįprastos $E[n]$ savybės leidžia surasti nenulinę antrojo lygio modulinę formą, kuri moduliu n yra susieta su kreivės E forma. Tačiau antrojo lygio formos negali būti. Tai ir yra prieštara pradinei prielaidai, kad E yra modulinė. Taigi svarstydami prieiname paskutinę išvadą: jeigu yra paskutinės Fermat teoremos kontrapavyzdys, tai turi būti nors viena elipsinė kreivė, kuri nėra modulinė, kam prieštarauja Taniyama–Shimura hipotezė.

Įrodymas, kad E yra modulinė

Wiles sakė, kad Taniyama–Shimura hipotezės įrodymo jis pradėjo ieškoti, kai tik sužinojo, kad tuo keliu galima gauti paskutinės Fermat teoremos įrodymą. Jo pastangos truko septynerius metus.

Wileso įrodymas neapima visos Taniyama–Shimura hipotezės, tam tikri atvejai yra nenagrinėjami. Kai kreivė yra redukuojama moduliu p, kartais būna, kad visos trys skirtingos šaknys susilieja į vieną skaitinę reikšmę. Pavyzdžiui, lygties $y^2 = x(x-10)(x+15)$ visos trys šaknys $0, 10$ ir -15 moduliu 5 sutampa. Wileso įrodymas netinka tokioms kreivėms. Jis apsiriboja *beveik stabiliomis* elipsinėmis kreivėmis, t.y. tokiomis, kurios turi savybę: jeigu dvi šaknys moduliu p, susijungia, tai trečioji išlieka skirtinga nuo jų. Kreivė, kurios lygtis yra $y^2 = x(x-A)(x+B)$, beveik stabili būna tuomet, kai nėra pirminio skaičiaus, dalijančio ir A, ir B. Šią sąlygą, suprantama, tenkina lygtis $y^2 = x(x-3)(x+32)$. Iš tikrųjų ši sąlyga galioja kiekvienai lygčiai, gautai iš tariamo paskutinės Fermat teoremos kontrapavyzdžio. Tai išplaukia iš reikalavimų koeficientams A ir B, formuluojamų moduliu 4 ir moduliu 32. Taigi kreivė, gauta iš kontrapavyzdžio, turi būti beveik stabili.

Užsibrėžęs įrodyti, kad visos beveik stabilios elipsinės kreivės yra modulinės, Wiles dirbo tais pačiais matematiniais „įrankiais“, kurie yra naudojami ir Ribet įrodyme, ir dar daugeliu kitų – kai kurie iš jų dar nebuvo sukurti, kai 1986 metais Wiles pradėjo savo tyrimą. Kaip ir Ribet, Wiles nagrinėjo taškų P, kuriems $mP = O$, aibę $E[m]$ ir atitinkamą Galois grupės reprezentaciją. Bet Wileso tikslas vienu aspektu buvo sunkiau pasiekiamas. Ribet įrodymui pakako vienintelio kontrapavyzdžio, o Wilesas privalėjo įrodyti, kad $E[m]$ yra modulinė be galo daugeliui m.

Pagrindinę Wileso strategija – tirti aibių šeimą $E[3], E[9], E[27]$ ir t.t. Kitaip tariant – tirti šeimas $E[m^\nu]$, čia ν yra sveikieji teigiami skaičiai. Buvo svarbi priežastis pasirinkti būtent šią šeimą: apie 1980-uosius metus Robert

P. Langlands iš Aukštųjų tyrimų instituto[2] ir Jerrold B. Tunnell iš Rutgers universiteto įrodė (žr. [7], [16]), kad aibė $E[3]$ pati yra modulinė. Langlandso–Tunnellio teorema teigia, kad bet kokiai elipsinei kreivei E trečiosios eilės taškų aibė sudaro grupę, kuri turi susijusią su ja modulinę formą. Šį rezultatą reikėjo įrodyti visai aibių $E[3^{\nu}]$ šeimai.

Wilesui pavyko tai atlikti pasinaudojus Galois grupės reprezentacijomis. Tačiau atsirado kita kliūtis, nors ir mažesnė. Kad įrodymą būtų galima sudaryti, reprezentacija, kurią apibrėžia 3-dalumo E taškai, turi būti neskaidi, t.y. jos neturi būti įmanoma sudaryti iš mažesnių reprezentacijų. Wiles įveikia šią kliūtį naudodamas išradingą taktiką. Jis įrodo, kad jei E yra beveik stabili, tai arba 3-dalumo taškų generuota reprezentacija yra stabili, arba 5-dalumo E taškų reprezentacija yra stabili. Po to jis naudojasi samprotavimais, kurie leidžia jam dirbti, jei reikia, su 5-dalumo taškais, nors apie juos ir nekalbama Langlandso–Tunellio teoremoje.

Šiame Wileso įrodymo žingsnyje dalyvauja keli reprezentacijų rinkiniai. Vienos reprezentacijos atsiranda iš modulinių formų, taigi yra modulinės pagal apibrėžimą. Kitos yra atsiradusios iš elipsinės kreivės E. Reikia įrodyti, kad jos taip pat yra modulinės. Įvairius reprezentacijų rinkinius įmanoma susieti naudojant deformacijų teorijos techniką, kurią sukūrė Barry Mazur iš Harvardo universiteto. Norėdamas, kad ši schema veiktų, Wiles turėjo įrodyti, jog kiekviena reprezentacijos ρ „deformacija", kuri kaip tikėtasi yra modulinė, iš tikrųjų yra modulinė. Jo įrodymas pagrįstas skaičiavimu: jis siekė parodyti, kad deformacijų nėra daugiau negu modulinių formų. Tai pati sudėtingiausia ir techniškiausia įrodymo dalis. Jai sukurti reikėjo iš viršaus įvertinti tam tikro objekto, vadinamosios Selmerio grupės. elementų skaičių. Kaip tik šioje grandyje ir buvo rasta neišbaigta vieta.

Wiles suformulavo savo rezultatą trijų paskaitų ciklo pabaigoje Isaac Newtono matematinių mokslų institute, Kembridžo universitete. Suformulavęs savo pagrindinę teoremą – Taniyama–Shimura hipotezę beveik stabilioms elipsinėms kreivėms – jis pridūrė išvadą: jei $a^n + b^n = c^n$, tai $abc = 0$. Atrodė, kad visai natūralu, jog paskutinė Fermat teorema išniro pabaigoje lyg atsitiktinė pastaba, padaryta prabėgomis – panašiai pats Fermat suformulavo ją prieš 350 metų.

Wileso įrodymas yra teigiantis, konstruktyvus. Jeigu įrodyme būtų kalbama tik apie paskutinę Fermat teoremą, tai būtų grynai negatyvus teiginys, neigiantis tam tikrų sveikųjų skaičių (tenkinančių Fermat lygtį $a^n + b^n = c^n$) egzistavimą. Tačiau įrodydamas dalinį Taniyama–Shimura hipotezės atvejį, Wilesas nustatė, kad tam tikri objektai egzistuoja – būtent modulinės formos, susijusios su beveik stabiliomis elipsinėmis kreivėmis. Pavyzdžiui, iš Wileso įrodymo išplaukia, kad lygtis $y^2 = x(x-3)(x+32)$ turi tokią susietą formą.

Wileso įrodymas užrašytas 200 puslapių rankraštyje, kuris įteiktas žurnalui *Inventiones Mathematicae*.[3] Darbą sudaro penki skyriai, kiekvienas iš jų galėtų būti atskiras žurnalo straipsnis. Darbe cituojama dauguma svarbių aritmetinės

---

[2] Institute for Advanced Study.

[3] Paskutinės Fermat teoremos įrodymas buvo paskelbtas straipsnyje: A. Wiles, Modular Elliptic Curves and Fermat's Last Theorem, *Ann. Math.*, 141 (1995).

algebrinės geometrijos rezultatų, gautų per pastaruosius 25 metus.

Tuoj po paskaitų Kembridže darbas buvo nusiųstas šešiems recenzentams, tačiau plačiau nebuvo skelbtas. Sklido gandai apie įrodymo spragas ir Wiles pasiuntė paaiškinantį laišką elektroninėms matematinėms naujienoms (*Usenet news group sci.math*):

> Nagrinėjant įrodymą buvo atskleistas tam tikras skaičius spragų, iš kurių dauguma buvo įveiktos, išskyrus vieną. Iš esmės daugelio Taniyama–Shimura hipotezės atvejų suvedimas į Selmerio grupės skaičiavimą yra teisingas. Tačiau galutinis tikslaus Selmerio grupės rėžio skaičiavimas dar nebaigtas. Aš tikiuosi, kad artimiausioje ateityje man pavyks tai atlikti, naudojantis idėjomis, išdėstytomis Kembridžo paskaitose.

Vasario mėnesį, kai Wilesas pradėjo skaityti paskaitų ciklą Prinstone, spraga dar nebuvo užpildyta.

Kliūtis, suprantama, apmaudi, tačiau yra geras pagrindas tikėti Wileso optimizmu. Jeigu, blogiausiu atveju, kliūties ir nepavyktų įveikti, tyrinėjimo galimybės nebūtų išsemtos. Dar yra daug nepanaudotų moderniosios aritmetikos rezervų.[4]

Bibliografija

1. E. T. Bell, The last problem, Introduction and notes by Underwood Dudley, Washington, D.C.: Mathematical Association of America, 1961, 1990.
2. J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä, Irregular primes and cyclotomic invariants to four million, *Math. of Comp.*, **61**, 151–153 (1993).
3. D. A. Cox, Introduction to Fermat's last theorem, *Amer. Math. Monthly*, **101** (1), 3–14 (1994).
4. H. M. Edwards, *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*, New York, Springer (1977).
5. D. Husemöler, *Elliptic Curves*, With an appendix by Ruth Lawrence, New York, Springer (1987).
6. A. W. Knapp, *Elliptic Curves*, Princeton University Press (1992).
7. R. P. Langlands, Base Change for $GL(2)$, *Ann. of Math. Stud.*, **96**, Princeton University Press, Princeton (1980).
8. P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, New York, Springer (1979).
9. K. A. Ribet, On modular representations of $Gal(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms, *Invent. Math.*, **100**, 431–476 (1990).
10. K. A. Ribet, From the Taniyama–Shimura conjecture to Fermat's last theorem, *Ann. Fac. Sci. Toulouse*, **11**, 116–139 (1990).
11. K. A. Ribet, *Modular Elliptic Curves and Fermat's Last Theorem*, Sel. Lect. in Math., American Mathematical Society, Video Recording, Providence, R.I. (1993).
12. K.Rubin, A.Silverberg, A report on Wiles' Cambridge lectures, *Bull. Amer. Math. Soc.*
13. J. H. Silverman, *The Arithmetic of Elliptic Curves*, New York, Springer, (1986).
14. J. H. Silverman, J. H. Tate, *Rational Points on Elliptic Curves*, New York, Springer, (1992).
15. J. H. Silverman, P. Mulbregt, Elliptic curve calculator, (1992). Internete: wuarchive.wustl.edu (Mathematica programos skaičiavimams su elipsinėmis kreivėmis.)
16. J. Tunell, Artin's conjecture for representations of octaedral type, *Bull. Amer. Math. Soc.*, **5**, 173–175 (1981).

[4] Primename, kad šis straipsnis buvo išspausdintas 1994 metais. 1994 metais įrodymo spraga buvo galutinai užpildyta.