Od Pitagorine do Fermatove jednadžbe

Župarić-Iljić, Jelena

Master's thesis / Diplomski rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Science / Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:217:377563

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2025-02-28**

Repository / Repozitorij:

Repository of the Faculty of Science - University of Zagreb

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Jelena Županić-Iljić

OD PITAGORINE DO FERMATOVE JEDNADŽBE

Diplomski rad

Voditelj rada:
prof. dr. sc. Andrej Dujella

Zagreb, rujan, 2022.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Mojim roditeljima, za bezuvjetnu podršku i ljubav.
Hvala vam na vrijednim savjetima, toploj brizi, svim molitvama (što sa zemlje, što s neba), te na svakoj žrtvi koju ste podnijeli kako bih danas bila tu gdje jesam.
Posebna zahvala braći i njihovim obiteljima za stipendiranje tijekom izazovnih studentskih dana i veliku vjeru u "malu seku". Hvala strpljivom Dinku za svako ispitivanje, ohrabrenje, potporu i brigu tijekom stresnih ispitnih perioda, te Ivi i Kikici za bodrenje pred ispite, a utjehu i/ili slavlje nakon njih. Hvala vam što ste često imali više vjere u mene nego što sam je sama imala i što ste svaki moj pad i uspjeh doživljavali kao svoj vlastiti. Veliko hvala i kolegama i prijateljima s faksa, osobito Mateji, na nesebičnoj pomoći pri učenju, podijeljenim materijalima i divnim uspomenama.
Također, zahvaljujem mentoru na susretljivosti i pomoći pri pisanju rada.
Naposljetku, hvala Onome čija me milost vodila i zaštita čuvala na putu ostvarenja ciljeva i Onome koji je mi dao snage da ovo nezaboravno putovanje privedem kraju.

Sadržaj

Uvod

Teorija brojeva je grana matematike koja proučava svojstva i međusobne odnose različitih vrsta brojeva. Njeni začeci potječu iz vremena Pitogorejaca, a važan doprinos su joj dali neki od najvećih matematičara svih vremena poput Euklida, Eulera, Lagrangea i Gaussa. Iako na prvu možda odaje dojam jedne od najjednostavnijih grana matematike, ona sadrži mnoštvo jednostavno oblikovanih, ali teško dokazivih problema koji ostaju nerazriješeni godinama, pa čak i stoljećima nakon svog izricanja. Primjer ovakvog problema je Posljednji Fermatov teorem ili Veliki Fermatov teorem koji će biti jedan od osnovnih tema ovoga rada.

Cilj rada je iznijeti povijesno-matematički pregled konstruiranja i dokazivanja Posljednjeg Fermatovog teorema počevši od njegovih korijena u vidu Pitagorina teorema.

U prvom se poglavlju mogu naći najbitnije definicije i zaključci iz teorije brojeva bitni za razumijevanje teorije u ostatku rada. Literatura za ovo poglavlje je [5].

Proučavanje pravokutnih trokuta s prirodnim stranicama, nazvanih Pitagorinim trokutima, usko je povezano s rješavanjem jednadžbe $x^2 + y^2 = z^2$, koja se javlja u iskazu Pitagorina teorema. Neka svojstva Pitagorinog teorema bila su poznata već u staroj antici, dok su druga otkrivena mnogo kasnije. U drugom poglavlju dan je iskaz Pitagorina teorema, definicija Pitagorinih trojki, te prikaz najranijih verzija Pitagorina teorema nađenih u drevnim babilonskim, kineskim i indijskim zapisima. Literatura za ovaj dio može se naći u [2], [4] i [12]. Zatim slijedi par riječi o Pitagori i njegovim sljedbenicima Pitagorejcima, te Eulerov dokaz ovog teorema. Literatura za ovaj dio poglavlja je [6], [10] i [15].

U sljedećem, trećem poglavlju promatrat će se algoritam za određivanje Pitagorinih trojki, te analitičko-geometrijska interpretacija Pitagorinih trojki. Potom slijedi par primjera vezanih za Pitagorine trojke i spomenuti algoritam. Literatura za treće poglavlje je [5], [7], [14] i [18].

Četvrto poglavlje donosi iskaz Posljednjeg Fermatovog teorema, opisuje Fermatovu metodu beskonačnog spusta, te daje dokaz Posljednjeg Fermatovog teorema u slučaju eksponenta jednakog četiri. Literatura korištena za četvrto poglavlje je [3], [5], [6], [9], [16] i [18].

Nakon toga se, u petom poglavlju, teorem analizira i za ostale eksponente, odnosno skupine eksponenata, te naposljetku slijedi opis uspješnog zaključka ovog, više od 350

godina starog, problema kojeg 1994. godine donosi Andrew Wiles uz pomoć mnoštva drugih matematičara čiji ćemo doprinos spomenuti. Literatura za ovaj dio rada je [1], [6], [9], [13], [14], [16], [17] i [19].

Posljednje poglavlje bavi se promatranjem Posljednjeg Fermatovog teorema u prstenu polinoma s kompleksnim koeficijentima. Poseban će naglasak biti stavljen na slučaj Fermatove jednadžbe prvog stupnja, čija inačica u polju cijelih brojeva, takozvana *abc slutnja*, povlači istinitost Fermatove tvrdnje za dovoljno velike cijele brojeve. U ovom se poglavlju od literature koriste [7], [8] i [16].

Diplomski rad napravljen je u sklopu aktivnosti Projekta KK.01.1.1.01.0004 - Znanstveni centar izvrsnosti za kvantne i kompleksne sustave, te reprezentacije Liejevih algebri.

Poglavlje 1

Osnovni pojmovi iz teorije brojeva

Kako bi imali sve potrebne alate za izgradnju teorije, te razumijevanje Posljednjeg Fermatovog teorema i svega što njemu prethodi, u ovom će poglavlju biti navedene osnovne definicije, teoremi, korolari i zaključci iz teorije brojeva bitni za razumijevanje ostatka rada. Dokazi naznačenih teorema, korolara i propozicija mogu se pronaći u [5].

1.1 Djeljivost

Definicija 1.1.1. *Neka su $a \neq 0$ i b cijeli brojevi. Kažemo da je b* djeljiv *s a, odnosno da a* dijeli *b, ukoliko postoji cijeli broj x takav da vrijedi $b = ax$. Pri tome koristimo oznaku $a \mid b$. Ako b nije djeljiv s a, onda pišemo $a \nmid b$.*

Ako $a \mid b$ onda još kažemo da je a djelitelj *od b, a da je b* višekratnik *od a.*

Definicija 1.1.2. *Neka su b i c cijeli brojevi. Cijeli broj a zovemo* zajednički djelitelj *od b i c ako vrijedi $a \mid b$ i $a \mid c$.*

Ako je barem jedan od brojeva b i c različit od nule, onda postoji samo konačno mnogo zajedničkih djelitelja od b i c. Najveći među njima zove se najveći zajednički djelitelj *od b i c i označava s (b, c).*

Slično se definira najveći zajednički djelitelj brojeva $b_1, b_2, \ldots, b_n$ koji nisu svi jednaki nuli, te se označava s $(b_1, b_2, \ldots, b_n)$.

Uočimo da uvijek vrijedi $(b, c) \geq 1$.

Definicija 1.1.3. *Reći ćemo da su cijeli brojevi a i b* relativno prosti *ako je $(a, b) = 1$. Za cijele brojeve $a_1, a_2, \ldots, a_n$ reći ćemo da su* relativno prosti *ako je $(a_1, a_2, \ldots, a_n) = 1$, a da su* u parovima relativno prosti *ako je $(a_i, b_j) = 1$ za sve $1 \leq i, j \leq n$, $i \neq j$.*

Definicija 1.1.4. *Kažemo da je prirodan broj* $p > 1$ prost *ukoliko* p *nema niti jednog djelitelja* d *takvog da je* $1 < d < p$. *Ako prirodan broj* $a > 1$ *nije prost, onda kažemo da je* složen.

Teorem 1.1.5. *Svaki prirodan broj* $n > 1$ *može se prikazati kao produkt prostih brojeva (s jednim ili više faktora), odnosno u obliku*

$$n = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdots {p_r}^{\alpha_r}$$

pri čemu su $p_1, \ldots, p_r$ *različiti prosti brojevi, a* $\alpha_1, \ldots, \alpha_r$ *prirodni brojevi. Ovakav prikaz broja* n *zovemo* kanonski rastav *broja* n *na proste faktore.*

Definicija 1.1.6. *Reći ćemo da je prirodan broj* a *(potpun) kvadrat ako se može zapisati u obliku* n^2, $n \in \mathbb{N}$.

Korolar 1.1.7. *Broj* a *je potpun kvadrat ako i samo ako su svi eksponenti faktora u rastavu tog broja na proste faktore parni.*

Korolar 1.1.8. *Neka su* a *i* b *relativno prosti prirodni brojevi, te neka je* ab *potpuni kvadrat. Tada su i* a *i* b *potpuni kvadrati.*

1.2 Kongruencije

Definicija 1.2.1. *Ako cijeli broj* $m \neq 0$ *dijeli razliku* $a-b$, *onda kažemo da je* a kongruentan b *modulo* m *i pišemo* $a \equiv b \pmod{m}$. *U protivnom kažemo da* a *nije kongruentan* b *modulo* m *i pišemo* $a \not\equiv b \pmod{m}$.

Neka jednostavna svojstva kongruencije dana su sljedećom propozicijom:

Propozicija 1.2.2. *Neka su* a, b, c *i* d *cijeli brojevi. Ako je* $a \equiv b \pmod{m}$ *i* $c \equiv d \pmod{m}$, *onda je* $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$ *i* $ac \equiv bd \pmod{m}$.

Sljedeća Propozicija vezana za djeljivost kvadrata prirodnog broja s 4 bit će nam kasnije bitna kod dokaza vezanih za Pitagorine trojke:

Propozicija 1.2.3. *Potpuni kvadrat broja je kongruentan ili* 0 *ili* 1 *modulo* 4. *Drugim riječima, za* $n \in \mathbb{N}$ *vrijedi* $n^2 \equiv 0 \pmod{4}$ *ili* $n^2 \equiv 1 \pmod{4}$.

Dokaz. Razlikujemo dva slučaja ovisno o parnosti broja $n \in \mathbb{N}$:

- Ukoliko je n paran, možemo ga zapisati u obliku $2k$, $k \in \mathbb{N}$. Tada je:

$$n^2 = 4k^2 \equiv 0 \pmod{4}.$$

- Za neparan n oblika $2k + 1$, $k \in \mathbb{N}$, vrijedi:

$$n^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1 \equiv 1 \pmod 4.$$

Budući da prirodan broj mora biti ili paran ili neparan, ovo su jedina dva slučaja i vidimo da tvrdnja Propozicije vrijedi. □

Prethodnom propozicijom smo dokazali i da je kvadrat (ne)parnog broja također (ne)paran broj.

Poglavlje 2

Pitagorin teorem

To this day, the theorem of Pythagoras remains the most important single theorem in the whole of mathematics.

Jacob Bronowski, The Ascent of Man

Pitagorin teorem predstavlja jedan od temeljnih teorema elementarne geometrije, no svoje primjene nalazi u gotovo svim znanstvenim područjima, što teorijskim, što praktičnim. Više od 400 verzija dokaza ovog teorema ujedinilo je matematičare poput Euklida, Alberta Einsteina i Leonarda da Vincija sa samoukim misliocima poput slijepe curice E. A. Coolidge, 16-godišnje učenice Ann Condit, te američkog predsjednika Jamesa Garfielda. Korištenje različitih grana matematike i fizike poput analitike, geometrije ili vektorskih polja iznjedrilo je najviše dokaza istog teorema u povijesti, od kojih su neki toliko složeni da zadaju muke i velikim znalcima, dok su drugi zadivljujuće jednostavni i jasni čak i osnovnoškolcima.

U ovom ćemo poglavlju proučiti najranije varijante Pitagorina teorema, reći nešto o Pitagori, Pitagorejcima i pozadini nastanka ovoga teorema, dati njegov iskaz i dokaz, te definirati Pitagorine trojke.

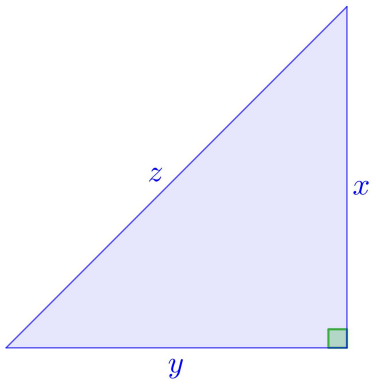
2.1 Iskaz Pitagorina teorema i definicija Pitagorinih trojki

Pitagorin teorem ili Pitagorin poučak, rezultat prvi put službeno zapisan kao *Propozicija 47* u prvoj knjizi Euklidovih *Elemenata*, najuspješnijem udžbeniku u povijesti matematike koji u trinaest knjiga obuhvaća dotadašnja matematička otkrića, objavljen je oko 300. godine prije Krista i glasi ovako:

Teorem 2.1.1 (Pitagorin teorem)**.** *Površina kvadrata nad hipotenuzom pravokutnog trokuta jednaka je zbroju površina kvadrata nad katetama, odnosno vrijedi*

$$x^2 + y^2 = z^2, \tag{2.1}$$

pri čemu su x i y duljine kateta pravokutnog trokuta, a z duljina hipotenuze (slika 2.1).



Slika 2.1: Pravokutni trokut

Euklidov dokaz Pitagorina teorema bit će prikazan u Potpoglavlju 2.4.

Uočimo da je Pitagorin teorem dvosmjeran što znači da je trokut čije stranice zadovoljavaju jednakost (2.1) pravokutan. Dakle, bilo koja trojka prirodnih brojeva (x, y, z) za koje je navedena jednakost istinita, određuje skup omjera $x : y : z$ takav da je trokut čije su stranice u tom omjeru zapravo pravokutan trokut. Time problem traženja kvadrata koji se može zapisati kao suma drugih dvaju kvadrata postaje geometrijski problem traženja Pitagorinih trojki, koje definiramo na sljedeći način:

Definicija 2.1.2. *Uređenu trojku prirodnih brojeva* (x, y, z) *zovemo* Pitagorina trojka *ukoliko su x i y katete, a z hipotenuza nekog pravokutnog trokuta, odnosno ukoliko zadovoljavaju jednadžbu* $x^2 + y^2 = z^2$.

Primijetimo da je dovoljno promatrati slučaj kada su x, y i z relativno prosti prirodni brojevi. U suprotnom, kada bi imali zajednički djelitelj $d > 1$, jednadžbu (2.1) bismo mogli podijeliti s d^2. To jest, ukoliko znamo da je (a, b, c) jedno rješenje dane jednadžbe, onda možemo generirati beskonačno mnogo drugih rješenja $(d \cdot a, d \cdot b, d \cdot c)$ jer vrijedi:

$$(da)^2 + (db)^2 = d^2(a^2 + b^2) = d^2c^2 = (dc)^2$$

Zbog ovoga, bez smanjenja općenitosti, u nastavku promatramo samo trojke relativno prostih brojeva i uvodimo sljedeću definiciju:

Definicija 2.1.3. *Kažemo da je* (x, y, z) primitivna Pitagorina trojka *ukoliko su* x, y *i* z *relativno prosti brojevi koji zadovoljavaju jednadžbu* $x^2+y^2 = z^2$. *U tom slučaju promatrani trokut nazivamo* (primitivnim) Pitagorinim trokutom.

Primjer 2.1.4. *Trojka* $(3, 4, 5)$ *je najpoznatiji i najjednostavniji primjer primitivne Pitagorine trojke. Ukoliko primitivne Pitagorine trojke poredamo uzlazno po duljini katete, sljedeća po redu je trojka* $(5, 12, 13)$.

Također, uočimo da je trojka $(6, 8, 10) = (2 \cdot 3, 2 \cdot 4, 2 \cdot 5)$ *generirana trojkom* $(3, 4, 5)$, *pa nije primitivna. Na sličan način, iz navedenih trojki možemo doći do Pitagorinih trojki* $(9, 12, 15)$ *i* $(10, 24, 26)$ *koje nisu primitivne.*

2.2 Pitagorin teorem u drevnim zapisima

Babilonske ploče

Teorem koji na jednostavan način povezuje duljine stranica pravokutnog trokuta bio je poznat tisućama godina prije Pitagorina rođenja. Njegovi se korijeni mogu naći već u babilonskoj kulturi brončanog doba (3300. godina prije Krista - 1200. godina prije Krista) iznikloj na području Mezopotamije, odnosno području današnjeg Iraka. Stari su Babilonci iza sebe ostavili trag o vrlo razvijenoj kulturi urezan u glinene ploče, od kojih velik dio još nije dekodiran.

Problem određivanja duljine stranice pravokutnika, ukoliko je poznata duljina druge stranice i duljina dijagonale, nađen na jednoj babilonskoj ploči i naveden u [4] glasi ovako:

4 je duljina i 5 dijagonala.
Kolika je širina?
Nije poznata.
4 puta 4 je 16.
5 puta 5 je 25.
Oduzmeš 16 od 25 i ostaje 9.
Što da uzmem da dobijem 9?
3 puta 3 je 9.
3 je širina.

YBC 7289

Babilonci su koristili brojevni sustav koji je primarno bio seksagezimalni, odnosno sustav s bazom 60, a sekundarno decimalni, odnosno s bazom 10. Zanimljivo je da seksagezimalni

sustav koristimo i danas, primjerice pri mjerenju vremena, računanju kutova u stupnjevima, te određivanju zemljopisnih koordinata. Jedna od značajki babilonskog brojevnog sustava je nedostatak znamenke nule, što je možebitan uzrok nerazlikovanja određenih brojeva u slučajevima kada nije poznat njihov kontekst. Ostale znamenke raspoznajemo na temelju klinova, pri čemu horizontalni klin (u obliku simbola <) označava desetice, a vertikalni klin (u obliku slova Y) jedinice u sekstagezimalnom zapisu broja. Prednost ovog brojevnog sustava je što njegova baza, 60, ima više djelitelja nego bilo koji manji prirodan broj, stoga sekstagezimalni sustav sadrži veći broj razlomaka koji imaju konačan zapis u odnosu na dekadski sustav.

Primjer ploče na kojoj je korišten babilonski brojevni sustav vidimo na slici 2.2a. Slika prikazuje ploču broj 7289 u zbirci sveučilišta Yale, *YBC 7289*, koja datira između 1800. i 1600. godine prije Krista. Prvi prikazani broj, <<<, smješten u gornjem lijevom kutu ploče, označava duljinu stranice utisnutog kvadrata jednaku 30. Iznad horizontalne dijagonale kvadrata nalaze se brojevi 1, 24, 51 i 10 čiji je prijevod u decimalni sustav sljedeći:

$$1 + \frac{24}{60} + \frac{51}{60^2} + \frac{10}{60^3} = 1.41421\overline{296} \approx \sqrt{2}$$

Na sličan način, pomoću brojeva 42, 25 i 35 smještenih ispod horizontalne dijagonale kvadrata dobijemo:

$$42 + \frac{25}{60} + \frac{35}{60^2} = 42.4263\dot{8} \approx 30\sqrt{2}$$

Ovaj zapis sugerira da su narodi stare Mezopotamije bili svjesni veze između duljine dijagonale kvadrata, d, i duljine stranice kvadrata, a, opisane jednadžbom $d = a\sqrt{2}$. Ostaje pitanje zašto su za duljinu stranice kvadrata koristili broj 30. Budući da je baza njihovog sustava bio broj 60, pretpostavlja se da je korištena upravo ova duljina zbog pojednostavljivanja računa. Zapis također ukazuje na to da su pri određivanju vrijednosti broja $\sqrt{2}$ došli do zapanjujuće točnosti. Važnost ovog broja leži u tome što predstavlja duljinu dijagonale jediničnog kvadrata koja se dobije korištenjem Pitagorina poučka. Štoviše, $\sqrt{2}$ otkriva novu vrstu brojeva, iracionalnih, koji se ne mogu zapisati kao omjer dvaju cijelih brojeva.

(a) YBC 7289 (b) Plimpton 322

Slika 2.2: Prikaz babilonskih ploča

Plimpton 322

Slika 2.2b prikazuje 322. babilonsku ploču iz zbirke G. A. Plimptona sa sveučilišta Kolumbija, koja vuče porijeklo iz vremena oko 1800. godine prije Krista. Na ploči *Plimpton 322* klinastim je pismom urezana tablica sačinjena od petnaest numeričkih redaka iz kojih iščitavamo petnaest Pitagorinih trojki. Zadivljujuće je što se na njoj nalaze trojke velikih brojeva, poput $(4601, 4800, 6649)$, što ukazuje na to da su Babilonci poznavali osnove teorije brojeva i osnovne principe algoritma za nalaženje Pitagorinih trojki, koji će se gotovo 1500 godina kasnije formalizirati u Euklidovim *Elementima*. Analizu ovog algoritma donosimo u Potpoglavlju 3.1.

Ploča *Plimpton 322* sadrži četiri naslovljena stupca, no prvi stupac zbog oštećenja nije vidljiv u potpunosti. Zahvaljujući znanstvenim istraživanjima, dio koji nedostaje djelomično je obnovljen, pa sada možemo s relativnom lakoćom iščitati ploču. Drugi i treći stupci tablice redom nose nazive *širina*, odnosno *dijagonala*, dok zadnji stupac sadrži numeraciju redaka brojevima od 1 do 15. Budući da su Babilonci pravokutni trokut tumačili kao polovicu pravokutnika, dobivenu podjelom pravokutnika na dva jednaka dijela putem jedne od dijagonala, širinu pravokutnika iz drugog stupca poistovjećujemo s kraćom stranicom pravokutnog trokuta u oznaci b, dok dijagonalu pravokutnika iz trećeg stupca poistovjećujemo s hipotenuzom pravokutnog trokuta u oznaci c. Tablica 2.1 donosi prikaz sadržaja ploče nakon prijevoda u dekadski sustav.

$\frac{b^2}{c^2-b^2}$ ili $[\frac{c^2}{c^2-b^2}]$	b (širina)	c (dijagonala)	redni broj
[1].9834028	119	169	1
[1].9491586	3367	4825	2
[1].9188021	4601	6649	3
[1].8862479	12709	18541	4
[1].8150077	65	97	5
[1].7851929	319	481	6
[1].7199837	2291	3541	7
[1].6927094	799	1249	8
[1].6426694	481	769	9
[1].5861226	4961	8161	10
[1].5625	45	75	11
[1].4894168	1679	2929	12
[1].4500174	161	289	13
[1].4302388	1771	3229	14
[1].3871605	56	106	15

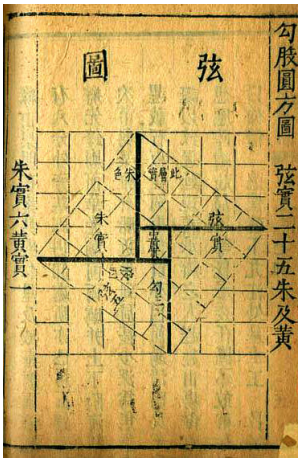
Tablica 2.1: Sadržaj ploče *Plimpton 322* zapisan u dekadskom sustavu

Može se pokazati da za dane brojeve b i c postoji jedinstveni kvadrat broja a za kojeg je istinita jednakost $a^2 + b^2 = c^2$, odnosno vrijedi Pitagorina jednadžba (2.1). Budući da oštećenja na ploči skrivaju vodeću znamenku brojeva u prvom stupcu, ne možemo sa sigurnošću tvrditi prikazuju li brojevi omjer $\frac{c^2}{c^2-b^2} = \frac{c^2}{a^2}$ ili $\frac{b^2}{c^2-b^2} = \frac{b^2}{a^2}$. U prvom slučaju vodeća znamenka je 1, a u drugom 0. Međutim, koji god slučaj uzmemo u obzir, vidimo da iz jednog omjera lako slijedi drugi. Zaista, dijeljenjem jednadžbe $a^2 + b^2 = c^2$ s a^2 dobijemo jednadžbu $1 + \frac{b^2}{a^2} = \frac{c^2}{a^2}$. Stoga, dodavanjem ili oduzimanjem jedinice vidimo da iz jednog omjera proizlazi drugi omjer. Unatoč manjim autorovim pogreškama nastalim u računu ili prilikom prepisivanja brojeva, *Plimpton 322* daje naslutiti da Babilonci nisu bili upoznati samo s Pitagorinim teoremom, već su poznavali temelje teorije brojeva. Štoviše, posjedovali su računske vještine kojima su teoriju provodili u realizaciju, što je vrlo značajno za civilizaciju koja je živjela tisuću godina prije pojave prvih velikih grčkih matematičara.

Kineska inačica Pitagorina teorema

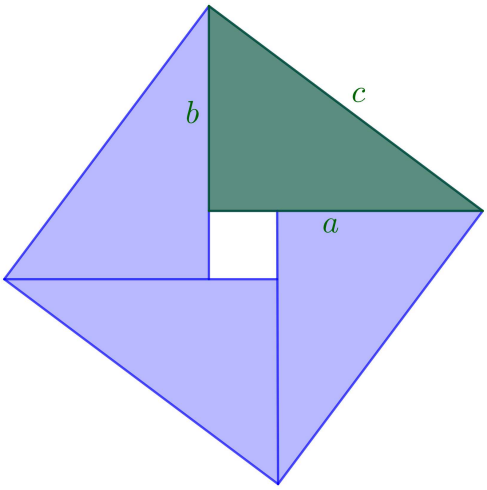
Drevni matematički tekst *Chou Pei Suan Ching*, napisan u periodu između 500. i 200. godine prije Krista, pokazatelj je da su Kinezi davno prije Pitagore bili svjesni veze opisane Pitagorinim teoremom. Slika 2.3 iz ovog teksta prikazuje *Hsuan-thu dijagram* koji predstavlja slikovitu primjenu Pitagorina teorema u slučaju trokuta s duljinama stranica 3, 4 i 5

i iz kojeg se na jednostavan način može dokazati istinitost Pitagorine tvrdnje. U kineskoj literaturi Pitagorin teorem poznat je kao Gougu teorem (na kineskom *gou* znači baza ili dulji krak, dok *gu* označava kraći krak).



Slika 2.3: *Hsuan-thu dijagram* iz teksta *Chou Pei Suan Ching*

Kako bi pojasnili dani dijagram, promotrimo njegovu uvećanu i modificiranu verziju prikazanu slikom 2.4.



Slika 2.4: Modificirani *Hsuan-thu* dijagram

Nađimo površinu koju zauzima veliki kvadrat na dva različita načina. Uočimo da je dani kvadrat podijeljen na četiri jednaka pravokutna trokuta i promotrimo istaknuti pravokutni trokut sa stranicama duljina a, b i c. Budući da je površina ovog trokuta jednaka $\frac{a \cdot b}{2}$,

ukupna površina koju zauzimaju sva četiri trokuta iznosi $2ab$. Lako se vidi da je duljina stranice kvadrata u sredini jednaka $a - b$, stoga mu je površina dana s $(a - b)^2$. Kako bi dobili ukupnu površinu velikog kvadrata moramo zbrojiti površinu malog kvadrata i ukupnu površinu koju zauzimaju četiri trokuta, te dobijemo da površina velikog kvadrata jednaka $2ab + (a - b)^2$.

S druge strane, duljina stranice velikog kvadrata je c, stoga mu površina iznosi c^2. Kako obje površine moraju biti jednake, izjednačimo izraze za površinu kvadrata dobivene na dva različita načina:

$$\begin{aligned} 2ab + (a - b)^2 &= c^2 \\ \cancel{2ab} + a^2 - \cancel{2ab} + b^2 &= c^2 \\ a^2 + b^2 &= c^2 \end{aligned}$$

Primijetimo da smo došli do jednadžbe Pitagorina poučka (2.1).

Sulvasutra, Indija

U *Sulvasutri*, jednoj od najstarijih zbirki hinduističkih tekstova napisanih između 800. i 500. godine prije Krista, mogu se naći razne varijante Pitagorina teorema i primjeri njegove primjene. Jedna od tih inačica, koja se odnosi na tvrdnju Pitagorinog poučka u slučaju jednakokračnog trokuta, glasi ovako:

Uže rastegnuto preko dijagonale kvadrata tvori površinu jednaku dvostrukoj površini početnog kvadrata.

Drugim riječima, kvadrat hipotenuze jednak je zbroju kvadrata stranica. U kasnijim tekstovima pojavljuje se i generalizirani oblik teorema:

Uže rastegnuto preko dijagonale pravokutnika tvori površinu koju zajedno čine vodoravna i okomita stranica.

Pri čemu se pod pojmom *površina nastala dužinom* implicira na površinu kvadrata kojem je dana dužina stranica.

Unatoč svemu navedenom, jedan od najpoznatijih teorema u matematičkoj povijesti nazvan je po grčkom filozofu Pitagori, rođenom na otoku Samosu oko 580. godine prije Krista. Iako su poznavanje principa Pitagorina teorema, te njegova uspješna primjena neosporni među narodima koji su živjeli prije Pitagorina vremena, teorem nosi navedeni naziv jer je prvi poznati cjeloviti dokaz teorema zabilježen u krugovima njegovih učenika, Pitagorejaca. Shodno tome, sljedeće Potpoglavlje posvećujemo njemu i njegovoj školi kako bi objasnili okolnosti u kojima je ovaj veliki teorem dobio ime.

2.3 Pitagora i utjecaj Pitagorejaca na oblikovanje matematičke povijesti

No other proposition of geometry has exerted so much influence on so many branches of mathematics as has the simple quadratic formula known as the Pythagorean Theorem.

Tobias Dantzig, 1955.

Pitagora je iznimno važna figura u razvoju matematike, ali se o njegovim matematičkim postignućima zna poprilično malo. Načelo tajanstvenosti kojim su se vodili brojni mislioci okupljeni oko njega dovelo je do toga da danas ne znamo previše toga o Pitagorinom životu. Za razliku od kasnijih grčkih matematičara, koji su iza sebe ostavili mnoštvo knjiga, danas nemamo sačuvano niti jedno njegovo pisano djelo. Jedan od razloga pomanjkanja matematičkih zapisa je taj što se u njegovo doba znanje većinom prenosilo usmenom predajom, djelomično zbog nedostatka materijala za pisanje. Većina onoga što nam je o Pitagori poznato dolazi od kasnijih generacija pisaca koji su se često nadmetali u veličanju svoga učitelja. Prva poznata poveznica Pitagore i Pitagorinog teorema nastala je više od pet stoljeća nakon njegove smrti, u Ciceronovim[1] i Plutarhovim[2] spisima. Iz poštovanja, mnogi su Pitagorejci svoja otkrića pripisivali upravo Pitagori, pa nam danas nije lako odvojiti njegov izvorni rad od rada ostatka zajednice. Upravo bismo zbog ovih razloga mogli pomisliti da je Pitagorin teorem filozofa Pitagoru iz Samosa možda neopravdano učinio besmrtnim.

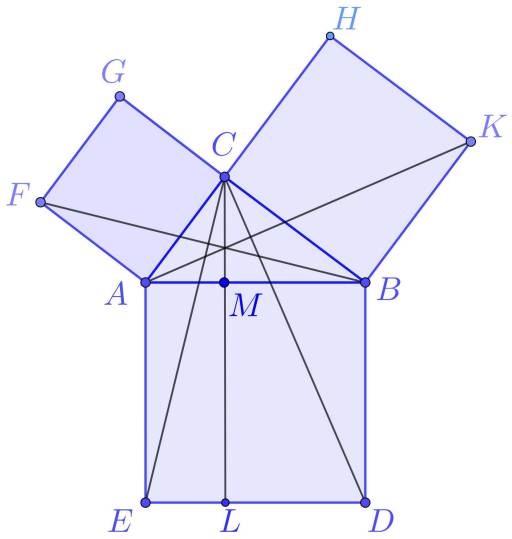
Iako danas ne možemo biti sigurni u Pitagorine stvarne doprinose, sasvim je jasno da je njegova škola dala izvanredan doprinos razvoju matematike. Pitagorejci nisu istraživali matematiku načinom kojeg mi danas primjenjujemo u obrazovnim ustanovama niti su kreirali matematičke izjave kako to rade današnji matematičari. Njih su zanimali temeljni koncepti matematike - pojam broja, matematički likovi poput kruga i trokuta, te apstraktna ideja dokaza. Zanimale su ih tvrdnje koje mi danas smatramo toliko jednostavnim da se o njima nema što promišljati. Brojna zapažanja u matematici, glazbi i astronomiji dovela su ih do vjerovanja da se sve oko nas, čitav svemir, svi odnosi i relacije mogu opisati brojevima ili svesti na manipulacije brojevima. Matematičko se razmišljanje nakon Pitagorina doba uvelike promijenilo. Umjesto samog uspostavljanja odnosa između matematičkih pojmova i objekata, naglasak se premjestio na dokazivanje tog odnosa logički dosljednim argumentima. Ova promjena označila je prijelaz teorijske matematike predgrčkih matematičara na deduktivnu disciplinu kakva je ona i danas.

[1] Marko Tulije Ciceron, 106. god. pr. Kr. - 43. god. pr. Kr., rimski govornik, filozofski pisac i državnik

[2] Plutarh, 46. - oko 120. god., grčki povjesničar, biograf i filozof

2.4 Euklidov dokaz

Slijedi pregled Euklidova dokaza, jednog od najpoznatijih dokaza Pitagorina teorema.



Slika 2.5: Skica uz Euklidov dokaz Pitagorina teorema

Dokaz. Neka je $\triangle ABC$ pravokutan trokut uz oznake kao na skici 2.5. Želimo dokazati istinitost jednakosti

$$\left|\overline{AC}\right|^2 + \left|\overline{CB}\right|^2 = \left|\overline{AB}\right|^2.$$

Kvadrati $AEDB$, $ACGF$ i $CBKH$ konstruirani su nad stranicama $\triangle ABC$. Uočimo da vrijedi $\left|\overline{BK}\right| = \left|\overline{CB}\right|$ jer je $CBKH$ kvadrat, te $\left|\overline{AB}\right| = \left|\overline{BD}\right|$ jer je $AEDB$ kvadrat. Provucimo kroz točku C dužinu paralelnu s $\overline{BD}$ i označimo sjecišta sa stranicama kvadrata slovima M i L. Također, nacrtajmo dužine $\overline{FB}$ i $\overline{AK}$. Uočimo da je $m\angle ABK = m\angle ABC + 90° = m\angle CBA + m\angle ABD = m\angle CBD$, pa su kutovi $\angle ABK$ i $\angle CBD$ po definiciji sukladni. Budući da vrijedi

$$\begin{aligned}\left|\overline{BK}\right| &= \left|\overline{CB}\right|,\\ \left|\overline{AB}\right| &= \left|\overline{BD}\right|,\\ \angle ABK &\cong \angle CBD,\end{aligned}$$

prema S-K-S teoremu o sukladnosti trokuta slijedi da je $\triangle ABK \cong \triangle CBD$.
Nadalje, budući da je $\overline{MD}$ dijagonala pravokutnika $MLDB$, površina $\triangle MDB$ je upola manja od površine pravokutnika $MLDB$. S druge strane, površina $\triangle CBD$ je jednaka površini

$\triangle MDB$ budući da imaju jednaku duljinu osnovice, $\left|\overline{BD}\right|$, i visine, $\left|\overline{MB}\right|$. Iz ovoga slijedi da je površina $\triangle CBD$ upola manja od površine pravokutnika $MLDB$. Analogno tome, vrijedi da je površina $\triangle ABK$ upola manja od površine pravokutnika $CBKH$. Koristeći sukladnost trokuta $\triangle ABK$ i $\triangle CBD$, imamo:

$$P(CBKH) = 2 \cdot P(ABK) = 2 \cdot P(CBD) = P(MLDB)$$

Budući da je duljina stranice kvadrata $CBKH$ jednaka $\left|\overline{CB}\right|$, slijedi $P(CBKH) = \left|\overline{CB}\right|^2$, dok je s druge strane $P(MLDB) = \left|\overline{MB}\right| \cdot \left|\overline{BD}\right|$.
Slično, pokazujemo da je $\left|\overline{AC}\right|^2 = P(ACGF) = P(AELM) = \left|\overline{AE}\right| \cdot \left|\overline{AM}\right|$. Sada imamo:

$$\begin{aligned}\left|\overline{AC}\right|^2 + \left|\overline{CB}\right|^2 &= \left|\overline{AM}\right| \cdot \left|\overline{AE}\right| + \left|\overline{MB}\right| \cdot \left|\overline{BD}\right| = \left|\overline{AM}\right| \cdot \left|\overline{BD}\right| + \left|\overline{MB}\right| \cdot \left|\overline{BD}\right| \\ &= \left|\overline{BD}\right| \cdot \left(\left|\overline{AM}\right| + \left|\overline{MB}\right|\right) = \left|\overline{BD}\right| \cdot \left|\overline{AB}\right| = \left|\overline{AB}\right| \cdot \left|\overline{AB}\right| = \left|\overline{AB}\right|^2\end{aligned}$$

□

Uočimo da Euklidov dokaz ne tumači Pitagorin teorem kao metrički odnos između stranica pravokutnog trokuta, već kao svojstvo kvadrata konstruiranih nad stranicama pravokutnog trokuta. Razlog tomu je što su Grci aritmetičke operacije tumačili u geometrijskom smislu, te je bilo prirodno Pitagorin teorem smatrati relacijom među površinama.

U knjizi *The Pythagorean Proposition* [11] profesora matematike E. S. Loomisa[3], objavljenoj 1927. godine, može se pronaći još zanimljivih dokaza Pitagorina teorema. Loomis je proveo cijeli život prikupljajući sve poznate dokaze Pitagorinog teorema, te 371 dokaz objedinio u svojoj knjizi podijelivši ih na dvije skupine, algebarske i geometrijske. Primio je još stotine novih dokaza nakon što je njegova knjiga objavljena, no nije ih stigao pregledati i uvrstiti u svoj zbornik prije smrti. S obzirom na njihov velik broj, nametnula se podjela dokaza na četiri skupine ovisno o korištenoj metode dokazivanja. Stoga, danas razlikujemo dokaze zasnovane na izjednačavanju površina, mozaičke dokaze u kojima se likovi raščlanjuju na više manjih, aritmetičke dokaze bazirane na računanju i dokaze koji koriste sličnost geometrijskih likova.

[3]Elisha Scott Loomis, 1852. - 1940., američki učitelj, matematičar, genealog, pisac i inženjer

Poglavlje 3

Pitagorine trojke

Nakon proučavanja Pitagorina teorema, posvetimo se ranije spomenutim Pitagorinim trojkama. Starogrčki matematičar Diofant iz Aleksandrije je već u 3. stoljeću razmatrao ove trojke prirodnih brojeva u svom djelu *Aritmetika*, sastavljenom od trinaest knjiga iz područja algebre i jednadžbi, od kojih je nažalost samo šest ostalo sačuvano.

3.1 Algoritam za određivanje Pitagorinih trojki

Promatranje Pitagorinih trokuta usko je povezano s promatranjem Pitagorinih trojki. Zanima nas kako možemo odrediti sve moguće Pitagorine trokute, odnosno Pitagorine trojke. Da bismo pronašli općeniti zapis Pitagorinih trojki, prvo ćemo opisati sve primitivne Pitagorine trojke dane Definicijom 2.1.3.

Uočimo da u svakoj primitivnoj Pitagorinoj trojki definiranoj jednadžbom $x^2 + y^2 = z^2$ točno jedan od brojeva x, y mora biti neparan. U suprotnom bi vrijedio jedan od sljedećih slučajeva:

- x i y su oba parni, pa je broj 2 njihov zajednički djelitelj. Prema Definiciji 2.1.3, trojka (x, y, z) ne može biti primitivna.

- x i y su oba neparni, pa su i x^2 i y^2 oba neparni. Iz Propozicije 1.2.3 u slučaju neparnog broja i Propozicije 1.2.2 slijedi $z^2 = x^2 + y^2 \equiv 1 + 1 \pmod 4 \equiv 2 \pmod 4$. Međutim, ovime smo dobili kontradikciju s Propozicijom 1.2.3 jer kvadrat prirodnog broja mora ili biti djeljiv s 4 ili pri dijeljenju s 4 dati ostatak 1.

Napomena 3.1.1. *U ostatku rada ćemo bez smanjenja općenitosti pretpostaviti da je y paran (ukoliko je potrebno, jednostavno zamijenimo parnosti od x i y). Prema prethodnom razmatranju odmah slijedi da x mora biti neparan. Štoviše, budući da je z^2 zbroj parnog i neparnog broja slijedi da je neparan, pa je onda neparan i z.*

Teorem 3.1.2. *Ako su m i n relativno prosti brojevi različite parnosti takvi da vrijedi $m > n$, onda je formulama*

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2, \tag{3.1}$$

dana primitivna Pitagorina trojka.

Dokaz. Lako se provjeri da trojka (x, y, z) definirana formulama (3.1) zadovoljava jednadžbu (2.1). Zaista,

$$x^2+y^2 = \left(m^2 - n^2\right)^2+(2mn)^2 = m^4-2m^2n^2+n^4+4m^2n^2 = m^4+2m^2n^2+n^4 = \left(m^2 + n^2\right)^2 = z^2$$

Provjerimo vrijedi li tvrdnja da su x, y i z relativno prosti. Pretpostavimo da nisu, odnosno da je $(x, z) = d > 1$. Kako su x i z oba neparni, onda i d mora biti neparan. Iz Propozicije 1.2.2 slijedi

$$d \mid \left(m^2 + n^2\right) + \left(m^2 - n^2\right) = 2m^2,$$
$$d \mid \left(m^2 + n^2\right) - \left(m^2 - n^2\right) = 2n^2.$$

Međutim, dane relacije su u kontradikciji s pretpostavkom da su m i n, pa onda i m^2 i n^2, relativno prosti brojevi. □

Teorem 3.1.3. *Sve primitivne Pitagorine trojke (x, y, z) u kojima je y paran dane su formulama*

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2,$$

pri čemu su m i n relativno prosti prirodni brojevi različite parnosti i vrijedi $m > n$.

Dokaz. Jednadžbu (2.1) možemo zapisati u obliku

$$y^2 = z^2 - x^2 = (z - x)(z + x) \tag{3.2}$$

Koristeći pretpostavku o parnosti, y možemo zapisati u obliku $y = 2c$, za $c \in \mathbb{N}$. Nadalje, prema Napomeni 3.1.1 znamo da su z i x neparni brojevi. Kako su $z - x$ i $z + x$ zbroj i razlika dva različita neparna broja, oni moraju biti parni, pa postoje prirodni brojevi a i b takvi da vrijedi

$$z + x = 2a \quad \text{i} \quad z - x = 2b. \tag{3.3}$$

Zbrajanjem, odnosno oduzimanjem, prethodnih jednadžbi, te sređivanjem dobijemo

$$z = a + b, \quad x = a - b. \tag{3.4}$$

Uočimo da a i b moraju biti relativno prosti, odnosno mora vrijediti $(a, b) = 1$. U suprotnom bi postojao zajednički faktor $d > 1$, pa bi iz jednakosti (3.4) slijedilo da je d zajednički faktor od z i x. Stoga, trojka (x, y, z) ne bi mogla biti primitivna.

Uvrštavanjem $y = 2c$ i (3.3) u jednadžbu (3.2), te sređivanjem dobijemo

$$c^2 = ab. \tag{3.5}$$

Iz Korolara 1.1.8 slijedi da postoje relativno prosti prirodni brojevi m i n takvi da vrijedi $a = m^2$ i $b = n^2$. Uvrštavanjem u jednakost (3.4) dobijemo raspis od z i x, dok raspis od y slijedi uvrštavanjem u jednadžbu (3.5) i korištenjem jednadžbe $y = 2c$:

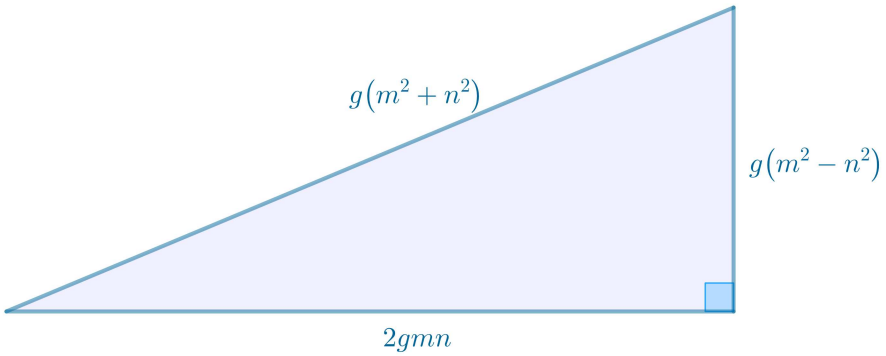
$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2.$$

Kako bi osigurali da su x, y i z relativno prosti, mora vrijediti $(m, n) = 1$ i zbroj $m + n$ mora biti neparan. Doista, budući da $x = (m - n)(m + n)$ ne smije biti paran, jer bi u protivnom x i y imali zajednički faktor, slijedi da nijedan od faktora ne smije biti paran. Kako (ne)parnost jednog faktora povlači (ne)parnost drugog, bez smanjenja općenitosti možemo pretpostaviti da $m + n$ mora biti neparan. Naposljetku, iz neparnosti od $m + n$ slijedi da su m i n različite parnosti. □

Iz Teorema 3.1.3 slijedi da su sve Pitagorine trojke dane sa

$$x = g\left(m^2 - n^2\right), \quad y = 2gmn, \quad z = g\left(m^2 + n^2\right), \tag{3.6}$$

pri čemu su m, n i g prirodni brojevi takvi da su m i n relativno prosti, različite parnosti i vrijedi $m > n$.



Slika 3.1: Pravokutni trokut čije duljine stranica tvore Pitagorinu trojku

3.2 Analitičko - geometrijska interpretacija

Promotrimo sada analitičko - geometrijsku interpretaciju dokaza Teorema 3.1.3 čija se verzija može pronaći u [14]. Prije toga navedimo i dokažimo Propoziciju koja povezuje cjelobrojna rješenja Pitagorine jednadžbe (2.1) s racionalnim rješenjima jednadžbe $u^2 + v^2 = 1$.

Propozicija 3.2.1. *Cjelobrojna rješenja jednadžbe $x^2 + y^2 = z^2$, pri čemu vrijedi da su x, y i z relativno prosti brojevi i $z > 0$, su u $1-1$ korespondenciji s racionalnim rješenjima u, v jednadžbe $u^2 + v^2 = 1$.*

Dokaz. Pretpostavimo da vrijedi jednakost $x^2 + y^2 = z^2$, pri čemu je $z > 0$ i x, y i z su relativno prosti brojevi. Drugim riječima, promatramo primitivnu Pitagorinu trojku (x, y, z). Danu jednakost podijelimo sa $z^2 > 0$ i dobijemo

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

Uvođenjem zamjena $u = \frac{x}{z}$ i $v = \frac{y}{z}$ dolazimo do jednadžbe $u^2 + v^2 = 1$. Budući da su u i v omjeri cijelih brojeva, po definiciji predstavljaju racionalna rješenja dobivene jednadžbe. Drugim riječima, $(u, v) = \left(\frac{x}{z}, \frac{y}{z}\right)$ su racionalne točke na jediničnoj kružnici danoj jednadžbom

$$u^2 + v^2 = 1. \tag{3.7}$$

Suprotno, pretpostavimo da postoje brojevi u, $v \in \mathbb{Q}$ za koje vrijedi $u^2 + v^2 = 1$. Zapišimo ih kao omjer cijelih brojeva $u = \frac{a}{b}$ i $v = \frac{c}{d}$, uz uvjet da je $bd \neq 0$. Iz ovoga slijedi

$$1 = u^2 + v^2 = \left(\frac{a}{b}\right)^2 + \left(\frac{c}{d}\right)^2.$$

Množenjem s b^2d^2 dobijemo jednakost

$$b^2d^2 = a^2d^2 + c^2b^2,$$

odnosno netrivijalnu Pitagorinu trojku (ad, cb, bd). Uočimo da se dijeljenjem s najvećim zajedničkim djeliteljem lako dobije primitivna Pitagorina trojka koja predstavlja cjelobrojna rješenja jednadžbe $x^2 + y^2 = z^2$. Time smo pokazali da svako racionalno rješenje (u, v) jednadžbe (3.7) svođenjem na zajednički nazivnik $u = \frac{x}{z}$, $v = \frac{y}{z}$ daje cjelobrojnu trojku (x, y, z), pa time i beskonačno mnogo novih rješenja (tx, ty, tz), $t \in \mathbb{Z}$. □

Dakle, uspostavljena je $1-1$ korespondencija između primitivnih Pitagorinih trokuta i racionalnih točaka koje leže na jediničnoj kružnici u prvom kvadrantu.

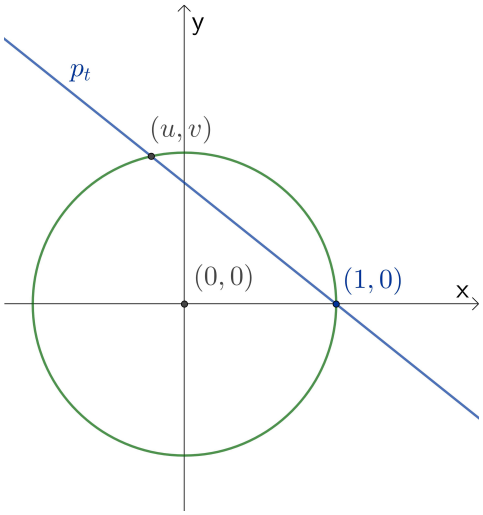
Racionalna parametrizacija jedinične kružnice

Neka je jedinična kružnica dana jednadžbom $x^2 + y^2 = 1$ i neka je $P = (x_P, y_P)$ proizvoljna točka na toj kružnici. Uzmimo bilo koju drugu racionalnu točku na kružnici i označimo je s $R = (u, v)$. Tada postoji jedinstveni pravac p koji prolazi točkama P i R i čija je jednadžba

$$p \ldots \quad y - y_P = \frac{y_P - v}{x_P - u}(x - x_P), \tag{3.8}$$

pri čemu su koeficijenti, kao i koeficijent smjera pravca $\frac{y_P - v}{x_P - u}$, racionalni brojevi.

Primjer 3.2.2. *Kako bi pojednostavili situaciju, neka je točka* $P = (1, 0)$ *i promotrimo pravac* p_t *koji prolazi točkama* $(1, 0)$ *i* (u, v)*, prikazan na slici 3.2. Uočimo da ukoliko pravac na kojem leži točka* $(1, 0)$ *nije vertikalan, sjeći će jediničnu kružnicu u točno jednoj točki različitoj od* $(1, 0)$*, označenoj s* (u, v) *za* $u < 1$.



Slika 3.2: Sjecišta kružnice $x^2 + y^2 = 1$ i pravca p_t

Ukoliko dani pravac ima koeficijent smjera jednak t, tada uvrštavanjem koordinata točaka (u, v) *i* $(1, 0)$ *u formulu za koeficijent smjera dobijemo* $t = \frac{v}{u-1}$*. Dakle, t je racionalan broj ukoliko su u i v racionalni brojevi.*

Uvrštavanjem koeficijenta smjera i koordinata točke $(1, 0)$ *u jednadžbu pravca kroz jednu točku* (3.8) *dobijemo da je dani pravac opisan jednadžbom* $y = t(x - 1)$*. Sjecišta s kružnicom proizlaze rješavanjem sustava*

$$\begin{cases} x^2 + y^2 = 1 \\ y = t(x - 1) \end{cases}$$

odnosno rješavanjem jednadžbe $1 - x^2 = y^2 = t^2(x-1)^2$. *Shodno tome, mora vrijediti ili* $x = 1$ *i* $y = 0$ *ili* $1 + x = t^2(1-x)$. *Iz drugog slučaja slijedi:*

$$\begin{aligned} 1 + x &= t^2 - t^2 x \\ x(1 + t^2) &= t^2 - 1 \\ x &= \frac{t^2 - 1}{t^2 + 1} \end{aligned}$$

Uvrštavanjem nađenog izraza u jednadžbu pravca $y = t(x-1)$ *dobijemo* $y = \frac{-2t}{t^2+1}$, *čime smo odredili koordinate sjecišta* (u, v)*:*

$$u = \frac{t^2 - 1}{t^2 + 1}, \quad v = \frac{-2t}{t^2 + 1} \tag{3.9}$$

Uvrštavanjem se lako vidi da su u *i* v *rješenja jednadžbe* $x^2 + y^2 = 1$. *Uočimo još da su koordinate racionalne ukoliko je i* t *racionalan broj. Štoviše, vrijedi i jača tvrdnja koja kaže da su* $u, v \in \mathbb{Q}$ *ako i samo ako je* $t \in \mathbb{Q}$. *Zaista, ako je* (x_0, y_0) *racionalno rješenje jednadžbe* $x^2 + y^2 = 1$, *a* T_0 *odgovarajuća točka na kružnici, onda je koeficijent smjera pravca kroz točku* $(1, 0)$ *i* T_0 *jednak* $t = \frac{y_0}{x_0 - 1}$ *i očito je racionalan broj. Prema tome, pokazali smo da pravac s koeficijentom smjera* t *kroz točku* $(1, 0)$ *presijeca jediničnu kružnicu u drugoj racionalnoj točki ako i samo ako je* t *racionalan i možemo okarakterizirati sva sjecišta u terminima broja* t.

Napomena 3.2.3. *Da bi geometrijska interpretacija dane situacije bila jasnija, promotrimo sljedeći limes:*

$$\lim_{t \to \pm\infty} (u, v) = \lim_{t \to \pm\infty} \left(\frac{t^2 - 1}{t^2 + 1}, \frac{-2t}{t^2 + 1} \right) = (1, 0)$$

Uočimo da kada koeficijent smjera pravca, t, *teži k* $\pm\infty$, *drugo sjecište pravca s kružnicom u oznaci* (u, v), *teži k točki* $(1, 0)$. *Stoga dani pravac, odnosno sekanta kružnice, teži tangenti provučenoj kroz točku* $(1, 0)$ *koja je paralelna s y-osi.*

Vratimo se sada našem primjeru i zapišimo koeficijent smjera pravca u obliku razlomka $t = -\frac{r}{s}$, *pri čemu je* $(r, s) = 1$. *Tada zapisi po koordinatama* (3.9) *postaju*

$$u = \frac{r^2 - s^2}{r^2 + s^2} \quad i \quad v = \frac{2rs}{r^2 + s^2}.$$

Množenjem s $r^2 + s^2$ *dobijemo familiju cjelobrojnih rješenja*

$$(r^2 - s^2, 2rs, r^2 + s^2).$$

Prema Teoremu 3.1.3 slijedi da dobivena rješenja predstavljaju primitivne Pitagorine trojke.

3.3 Primjeri

Za kraj ovog poglavlja, promotrimo par primjera vezanih za Pitagorine trojke i primjenu opisanog algoritma za traženje Pitagorinih trojki.

Primjer 3.3.1. *Nađimo sve pravokutne trokute s racionalnim duljinama stranica čija je površina jednaka opsegu. Nadalje, pokažimo da su trojke* $(5, 12, 13)$ *i* $(6, 8, 10)$ *jedina cjelobrojna rješenja ovog problema.*

Rješenje: Neka su $a, b, c \in \mathbb{Q}$ stranice promatranog trokuta s površinom P i opsegom O, odnosno vrijedi

$$P = \frac{1}{2}ab,$$
$$O = a + b + c.$$

Pretpostavimo da su a, b i c relativno prosti (u suprotnom ih podijelimo sa zajedničkim djeliteljem). Budući da su ovo stranice pravokutnog trokuta, znamo da zadovoljavaju jednakost $a^2 + b^2 = c^2$. Uz pretpostavku da je b paran, a a i c neparni, prema Teoremu 3.1.3 znamo da postoje relativno prosti brojevi različite parnosti m i n takvi da je $m > n$ i vrijedi

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2.$$

Korištenjem danog uvjeta o jednakosti površine i opsega, dolazimo do jednadžbe $\frac{1}{2}ab = a + b + c$, odnosno

$$\frac{1}{2}\left(m^2 - n^2\right)2mn = m^2 \cancel{- n^2} + 2mn + m^2 \cancel{+ n^2}$$
$$(m - n)(m + n)mn = 2m(m + n)$$
$$m = \frac{n^2 + 2}{n}$$

Iz prethodne jednakosti slijedi da su stranice traženog trokuta određene sa

$$a = 4 + \frac{4}{n^2}, \quad b = 2n^2 + 4, \quad c = 2n^2 + 4 + \frac{4}{n^2}.$$

Kako bi dobili cjelobrojna rješenja, uočimo da su zbog razlomka $\frac{4}{n^2}$ jedine dvije mogućnosti za vrijednost n^2 jednake 1 i 4. Za $n^2 = 1$ dobijemo vrijednosti $a = 8$, $b = 6$, $c = 10$, dok za $n^2 = 4$ duljine stranica trokuta iznose $a = 5$, $b = 12$, $c = 13$. Dakle, jedini Pitagorini trokuti sa svojstvom da im je površina jednaka opsegu su dani trojkama $(6, 8, 10)$ i $(5, 12, 13)$. □

Primjer 3.3.2. *Dokažimo da je u svakoj primitivnoj Pitagorinoj trojki razlika između hipotenuze i svake od kateta ili kvadrat ili dvostruki kvadrat.*

Rješenje: Neka je (a, b, c) primitivna Pitagorina trojka. Tada po Teoremu 3.1.3 vrijedi

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2,$$

za m, n relativno proste brojeve različite parnosti i takve da vrijedi $m > n$. Promotrimo sljedeće razlike:

$$c - a = \cancel{m^2} + n^2 \cancel{- m^2} + n^2 = 2n^2$$
$$c - b = m^2 + n^2 - 2mn = (m - n)^2$$

Stoga je tvrdnja, da je u primitivnom Pitagorinom trokutu razlika između hipotenuze i svake od kateta ili kvadrat ili dvostruki kvadrat, dokazana. □

Primjer 3.3.3. *Nađimo sva rješenja jednadžbe $x^2 + 5y^2 = z^2$ pri čemu su x, y i z relativno prosti brojevi.*

Rješenje: Dana jednadžba se može zapisati u obliku

$$5y^2 = z^2 - x^2 = (z - x)(z + x). \tag{3.10}$$

Razlikujemo sljedeće slučajeve s obzirom na parnost od y:

- Pretpostavimo prvo da je y paran, iz čega slijedi da su x i z neparni. Dijeljenjem obje strane jednadžbe (3.10) s 4 dobijemo:

  $$5 \cdot \left(\frac{y}{2}\right)^2 = \frac{z - x}{2} \cdot \frac{z + x}{2}$$

  Budući da su brojevi x i z relativno prosti, tada su i $\frac{z-x}{2}$ i $\frac{z+x}{2}$ relativno prosti brojevi. Kako vrijedi da 5 dijeli lijevu stranu jednakosti, mora dijeliti i desnu. Stoga, postoje prirodni brojevi m, n takvi da

  $$\frac{z \pm x}{2} = 5m^2, \quad \frac{z \mp x}{2} = n^2, \quad \frac{y}{2} = mn.$$

  Zbrajanjem i oduzimanjem prvih dvaju jednakosti i sređivanjem, dobijemo rješenja $x = \pm(5m^2 - n^2)$, $y = 2mn$, $z = 5m^2 + n^2$.

- Pretpostavimo sada da je y neparan. Tada je x paran, a z neparan. Iz (3.10) slijedi da postoje prirodni brojevi a, b takvi da je

  $$z \pm x = 5a^2, \quad z \mp x = b^2, \quad y = ab.$$

  Brojevi a i b su neparni, pa je njihova razlika parna i možemo staviti $b - a = 2c$, $c \in \mathbb{Z}$. Ponovno, zbrajanjem i oduzimanjem prvih dvaju jednakosti i uvrštavanjem $b = 2c + a$, dobijemo rješenja

  $$x = \pm(2c^2 + 2ac - 2a^2), \quad y = a^2 + 2ac, \quad z = 3a^2 + 2ac + 2c^2.$$

□

Primjer 3.3.4. *Odredimo, ukoliko je to moguće, sve primitivne Pitagorine trojke u kojima je hipotenuza*

- *za jedan veća od katete.*
- *za dva veća od katete.*
- *za tri veća od katete.*

Rješenje: Promotrimo prvi slučaj:

Neka je (a, b, c) primitivna Pitagorina trojka i pretpostavimo da je b paran. Budući da su a i c neparni, mora vrijediti $c = b + 1$. Kako je (a, b, c) Pitagorina trojka, ispunjena je jednakost

$$a^2 + b^2 = (b + 1)^2,$$

koja nakon sređivanja glasi ovako

$$a^2 = 2b + 1.$$

Kako je a neparan zapišimo ga kao $a = 2k + 1$, za $k \in \mathbb{N}$. Uvrštavanjem smo došli do sljedeće parametrizacije:

$$\{(2k + 1, 2k(k + 1), 2k(k + 1) + 1) : k \in \mathbb{N}\}.$$

Promotrimo sada drugi slučaj u kojem je hipotenuza za dva veća od katete:

Neka je (a, b, c) primitivna Pitagorina trojka i pretpostavimo da je b paran. Tada su a i c neparni i vrijedi da je $c = a + 2$. Ispunjena je jednakost

$$a^2 + b^2 = (a + 2)^2,$$

koja je nakon jednostavnog sređivanja jednaka

$$b^2 = 4(a + 1).$$

Kako je b paran, zapišimo ga kao $b = 2k$, za $k \in \mathbb{N}$. Uvrštavanjem dobijemo traženu parametrizaciju

$$\left\{\left(k^2 - 1, 2k, k^2 + 1\right) : k > 1, k \in \mathbb{N}\right\}.$$

Ostao nam je još treći slučaj:

Neka je ponovno (a, b, c) primitivna Pitagorina trojka, b paran, te a i c neparni. Vrijedi da je $c = b + 3$ i

$$a^2 + b^2 = (b + 3)^2,$$

odnosno

$$a^2 = 3(2b + 3).$$

Po Teoremu 3.1.3 znamo da postoje relativno prosti prirodni brojevi različite parnosti m i n takvi da je $m > n$ i vrijedi

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2.$$

Iz prethodnih jednakosti i korištenjem jednadžbe $c = b + 3$ slijedi:

$$m^2 + n^2 = 2mn + 3$$
$$(m - n)^2 = 3$$

Uočimo da dana jednadžba nema rješenja u skupu prirodnih brojeva, stoga, ne postoji primitivna Pitagorina trojka čija je hipotenuza za tri veća od katete. □

Poglavlje 4

Posljednji Fermatov teorem

4.1 Iskaz Posljednjeg Fermatovog teorema

Pierre de Fermat[1] je u 17. stoljeću postavio temelj za izgradnju moderne teorije brojeva svojim proučavanjem i tumačenjem starogrčkih matematičkih tekstova, te nizanjem velikih rezultata, od kojih su neki, poput Posljednjeg Fermatovog teorema, zadavali muke velikim matematičarima čak desetljećima nakon njegove smrti. Danas ga smatramo jednim od najpoznatijih teoretičara brojeva, što je doduše iznenađujuće budući da je po struci bio odvjetnik, a u polju matematike je djelovao kao amater. Iznenađujuća je i činjenica da je u životu objavio samo jedan matematički rad, i to anonimni, napisan kao dodatak knjizi jednog kolege. Budući da Fermat tijekom života nije dozvoljavao objavljivanje svojih rasprava, njegovi poklonici bojali su se da će njegova matematička dostignuća propasti ukoliko se ne prikupe i ne objave posthumno. U strahu od padanja u zaborav, njegov sin Samuel preuzeo je zadatak prikupljanja očevih pisama i u njima zapisanih rasprava, matematičkih radova, komentara i rezultata napisanih u raznim knjigama kako bi povezao i na koncu objavio očeve matematičke ideje. Samuel je skupljajući materijale, na margini pored Problema 8 u očevom primjerku 2. knjige Diofantove *Aritmetike*, pronašao bilješku koja će Fermatovu slutnju učiniti jednim od najzagonetnijih problema posljednjih stoljeća. Bilješka napisana oko 1637. godine na izvornom latinskom jeziku glasi ovako:

"Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere. Cuius rei demonstrationem mirabilem sane detexi hanc marginis exiguitas non caperet."

Što u prijevodu znači:

[1] Pierre de Fermat, 1601. - 1665., francuski matematičar i pravnik

Nemoguće je razdvojiti kub na dva kuba, bikvadrat na dva bikvadrata ili, općenito, bilo koju potenciju veću od druge, na dvije potencije istog stupnja. Otkrio sam zaista nevjerojatan dokaz ovog teorema, ali je margina preuska da on na nju stane.

Opći iskaz dane tvrdnje zapisane matematičkim rječnikom danas poznajemo pod nazivom *Posljednji Fermatov teorem* ili *Veliki Fermatov teorem*.

Teorem 4.1.1 (Posljednji Fermatov teorem)**.** *Neka je $n \geq 3$ prirodan broj. Tada jednadžba*

$$x^n + y^n = z^n \tag{4.1}$$

nema rješenja u prirodnim brojevima x, y i z.

Iako ovo nije bio posljednji teorem kojeg je Fermat izrekao, nosi ovakav naziv jer je posljednji koji je ostao nedokazan. Svi drugi Fermatovi teoremi su dokazani ili pomoću dokaza koje je on sam pružio, ili su dokazi pronađeni kasnije. Ovo je posljednji teorem kojeg je trebalo dokazati i smatra se matematičkom slutnjom koja je isprovocirala najveći broj netočnih matematičkih dokaza. Nijedan cjelovit i ispravan dokaz nije predložen sljedećih 357 godina, dok konačno 1994. godine teorem nije dokazao Andrew Wiles koristeći iznimno napredne matematičke tehnike iz područja teorije brojeva i algebarske geometrije, te radove i rezultate mnogih drugih matematičara.

Napomena 4.1.2. *Budući da se Diofant u svojoj* Aritmetici *bavio racionalnim brojevima, podrazumijeva se da je i Fermat svoju tvrdnju izrekao za sve racionalne brojeve x, y i z, pri čemu je $n > 2$. Međutim, uočimo da se tvrdnja s prirodnih brojeva lako proširi na racionalne brojeve.*

Pretpostavimo da imamo rješenje x, y i z jednadžbe (4.1) *u prirodnim brojevima i neka je d najmanji zajednički višekratnik brojeva x, y i z. Tada iz jednakosti*

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

dobijemo racionalno rješenje $\frac{x}{d}$, $\frac{y}{d}$, $\frac{z}{d}$ jednadžbe $x^n + y^n = z^n$.

Također, valja primijetiti da ukoliko tvrdnju proširimo na iracionalne brojeve, tada je moguće za svaki par brojeva x i y pronaći rješenje oblika $z = \sqrt[n]{x^n + y^n}$, pa tvrdnja Posljednjeg Fermatovog teorema očito ne vrijedi.

4.2 Fermatova metoda beskonačnog spusta

U ovom Potpoglavlju razmatrat ćemo metodu beskonačnog spusta koju je Fermat koristio za dokazivanje Posljednjeg Fermatovog teorema u slučaju $n = 4$.

Spomenuta se metoda koristi kako bi pokazali da neko svojstvo ili tvrdnja ne vrijede za nenegativne cijele brojeve. Pod pretpostavkom da su određeno svojstvo ili tvrdnja istiniti za proizvoljan prirodan broj, ideja je da pokažemo da oni također vrijede i za neki strogo manji prirodni broj. Onda, analognim zaključivanjem, slijedi da će vrijediti i za još manje brojeve, i tako dalje *ad infinitum*[2]. Međutim, takvo što je nemoguće jer ne postoji beskonačan strogo padajući niz prirodnih brojeva (odnosno "beskonačan spust"). Stoga slijedi da promatrano svojstvo ili tvrdnja ne mogu vrijediti niti za jedan prirodni broj. Drugim riječima, ako pretpostavka da postoji prirodni broj koji ima dani skup svojstava, povlači da postoji strogo manji prirodni broj s istim skupom svojstava, onda prirodni broj s tim skupom svojstava ne može postojati.

Prije iznošenja dokaza Posljednjeg Fermatovog teorema u slučaju $n = 4$ pomoću metode beskonačnog spusta, promotrimo sljedeća dva primjera kako bismo bolje upoznali ovu metodu. Prvi primjer je preuzet iz [3], a drugi iz [6].

Primjer 4.2.1. *Pokažimo da jednadžba*

$$x^3 + 2y^3 = 4z^3 \tag{4.2}$$

nema netrivijalnih rješenja u skupu nenegativnih cijelih brojeva.

Rješenje: Pokažimo da je trivijalno rješenje $(0, 0, 0)$ ove jednadžbe i jedino rješenje. Pretpostavimo suprotno, odnosno postoji netrivijalno nenegativno cjelobrojno rješenje (x_1, y_1, z_1) koje zadovoljava jednadžbu (4.2), to jest vrijedi

$$x_1{}^3 + 2y_1{}^3 = 4z_1{}^3. \tag{4.3}$$

Budući da je $x_1{}^3 = 2(2z_1{}^3 - y_1{}^3)$ slijedi da $2 \mid x_1$, pa uvodimo oznaku $x_1 = 2x_2$ pri čemu je $x_2 \in \mathbb{N}$. Koristeći danu zamjenu dolazimo do jednadžbe $8x_2{}^3 + 2y_1{}^3 = 4z_1{}^3$ odnosno $4x_2{}^3 + y_1{}^3 = 2z_1{}^3$. Na sličan način uvodimo oznake $y_1 = 2y_2$, $y_2 \in \mathbb{N}$ i $z_1 = 2z_2$, $z_2 \in \mathbb{N}$, te uvrštavanjem u $4x_2{}^3 + y_1{}^3 = 2z_1{}^3$ i sređivanjem dobijemo jednadžbu

$$x_2{}^3 + 2y_2{}^3 = 4z_2{}^3.$$

Dakle, dobili smo novo rješenje (x_2, y_2, z_2) jednadžbe (4.3) takvo da je $x_1 > x_2$, $y_1 > y_2$, $z_1 > z_2$.

Nastavljajući ovaj postupak konstruira se niz pozitivnih cjelobrojnih rješenja (x_n, y_n, z_n), $n \geq 1$ za kojeg vrijedi $x_1 > x_2 > x_3 > \ldots$. Time dolazimo do kontradikcije s činjenicom da ne postoji beskonačni strogo padajući niz prirodnih, odnosno pozitivnih cijelih brojeva. □

[2] *hrv.* do beskonačnosti

Primjer 4.2.2. *U drugom primjeru razmotrit ćemo dokaz Korolara 1.1.8 pomoću Fermatove metode beskonačnog spusta. Kako je metoda beskonačnog spusta metoda za opovrgavanje tvrdnji, trebamo osporiti tvrdnju da postoje prirodni brojevi a i b koji su relativno prosti i takvi da je ab kvadrat, a pritom a i b nisu oba kvadrati.*

Dokaz. Pretpostavimo da postoje relativno prosti prirodni brojevi a i b za koje vrijedi $ab = u^2$, $u \in \mathbb{N}$ i bez smanjenja općenitosti uzmimo slučaj u kojem a nije kvadrat (ukoliko je potrebno, zamijenimo a i b i promatramo slučaj u kojem b nije kvadrat). Prema Teoremu 1.1.5 postoji barem jedan prosti broj $d_0 \in \mathbb{N}$ koji dijeli a. Stoga, a možemo zapisati u obliku $a = d_0 \cdot k$, $k \in \mathbb{N}$. Također, d_0 dijeli ab odnosno $d_0 \mid (u \cdot u)$, iz čega slijedi da $d_0 \mid u$, pa možemo staviti $u = d_0 \cdot v$, $v \in \mathbb{N}$. Uočimo da vrijedi

$$(d_0 \cdot k)b = ab = u^2 = d_0^2 v^2,$$

iz čega slijedi jednakost

$$kb = d_0 v^2. \tag{4.4}$$

Kako d_0 dijeli desnu stranu dane jednakosti, mora dijeliti i lijevu. Shodno tome, d_0 dijeli ili k ili b. Međutim, d_0 ne može dijeliti b jer su a i b relativno prosti. Dakle, d_0 dijeli k, pa uvodimo oznaku $k = d_0 \cdot d_1$, $d_1 \in \mathbb{N}$. Uvrštavanjem ove oznake u jednadžbu (4.4) i sređivanjem dobijemo jednadžbu

$$d_1 b = v^2.$$

S obzirom da vrijedi $a = d_0 \cdot k = d_0 \cdot d_0 \cdot d_1$, zaključujemo da je bilo koji djelitelj od d_1 ujedno i djelitelj od a. Budući da su a i b relativno prosti, d_1 i b nemaju zajedničkog djelitelja većeg od 1. Štoviše, d_1 nije kvadrat jer bi u suprotnom $a = {d_0}^2 d_1$ također bio kvadrat, što bi uzrokovalo kontradikciju s pretpostavkom.

Prema tome, brojevi d_1 i b su relativno prosti, $d_1 b = v^2$ je kvadrat, a d_1 i b nisu oba kvadrati. Uz to, vrijedi da je $d_1 < a$. Koristeći ponovno istovjetan argument može se pokazati da postoji prirodni broj $d_2 < d_1$ takav da d_2 i b imaju sva tri opisana svojstva. Uzastopno ponavljanje ovog argumenta daje beskonačni strogo padajući niz prirodnih brojeva $a > d_1 > d_2 > d_3 > \ldots$. Budući da ovakva situacija nije moguća, zaključujemo da ne postoje brojevi a i b s opisanim svojstvima, odnosno a i b moraju oba biti kvadrati. □

Za dokazivanje sljedećih teorema koji prethode Posljednjem Fermatovom teoremu u slučaju $n = 4$, dovoljno je kombinirati Fermatovu metodu beskonačnog spusta i metodu konstruiranja Pitagorinih trojki opisanu u prethodnom Poglavlju 3. Dokazi su preuzeti iz [5] i modificirani.

Teorem 4.2.3. *Jednadžba*

$$x^4 + y^4 = z^2$$

nema rješenja u prirodnim brojevima. Drugim riječima, ne postoji pravokutni trokut kojem su duljine kateta kvadrati prirodnih brojeva.

Dokaz. Pretpostavimo da takav trokut postoji i izaberimo među svim takvim trokutima onaj s najmanjom hipotenuzom z. Kako je $x^4+y^4 = \left(x^2\right)^2+\left(y^2\right)^2 = z^2$, dobijemo Pitagorinu trojku (x^2, y^2, z).

Pokažimo da su x i y relativno prosti. U protivnom bi imali zajedničkog djelitelja $d > 1$ i vrijedilo bi $x = a\cdot d$, $y = b\cdot d$ za $a, b, d \in \mathbb{N}$. Tada bi iz $z^2 = d^4(a^4+b^4)$ slijedilo da postoji $c \in \mathbb{N}$ takav da je $z = d^2\cdot c$. Time bi dobili jednakost $c^2 = a^4 + b^4$ odnosno Pitagorinu trojku (a^2, b^2, c) s hipotenuzom c manjom od z, što je kontradikcija s pretpostavkom o minimalnosti od z.

Budući da su x i y relativno prosti, onda su i x^2 i y^2 relativno prosti, pa je (x^2, y^2, z) primitivna Pitagorina trojka. Uz pretpostavku da je y paran (inače međusobno zamijenimo x i y), po Teoremu 3.1.3 postoje relativno prosti prirodni brojevi različite parnosti m i n takvi da je $m > n$ i vrijedi

$$x^2 = m^2 - n^2, \quad y^2 = 2mn, \quad z = m^2 + n^2.$$

Bez smanjenja općenitosti možemo pretpostaviti da je n paran, odnosno m neparan broj, te uvesti oznaku $n = 2k$ za $k \in \mathbb{N}$. Kako je y paran, zapišimo ga kao $y = 2t$ za $t \in \mathbb{N}$, pa iz jednadžbe $y^2 = 2mn$ dobijemo

$$t^2 = mk.$$

Prema Korolaru 1.1.8 postoje prirodni brojevi r i s takvi da je $m = r^2$ i $k = s^2$. Kako su x i y relativno prosti, trojka (x, n, m) je primitivna Pitagorina trojka, pa po Teoremu 3.1.3 postoje relativno prosti prirodni brojevi različite parnosti u i v takvi da je $n = 2uv$ i $m = u^2 + v^2$. Sada iz $n = 2k = 2s^2$ slijedi da je

$$s^2 = uv.$$

Ponovno, prema Korolaru 1.1.8 znamo da postoje $a, b \in \mathbb{N}$ takvi da je $u = a^2$, $v = b^2$. Prema tome, vrijedi

$$r^2 = m = u^2 + v^2 = \left(a^2\right)^2 + \left(b^2\right)^2,$$

čime smo dobili Pitagorinu trojku (a^2, b^2, r) za čiju hipotenuzu vrijedi

$$r < r^2 = m < m^2 + n^2 = z,$$

što je u suprotnosti s minimalnosti od z. □

Teorem 4.2.4. *Jednadžba*

$$x^4 + y^2 = z^4 \tag{4.5}$$

nema rješenja u prirodnim brojevima. Drugim riječima, ne postoji Pitagorin trokut u kome su hipotenuza i jedna kateta kvadrati prirodnih brojeva.

Dokaz. Pretpostavimo suprotno, odnosno da trokut s opisanim svojstvom postoji i promatrajmo onaj s najmanjom hipotenuzom. Dakle, neka je (x^2, y, z^2) Pitagorina trojka s najmanjom hipotenuzom z^2. Uočimo da je dana trojka primitivna. Zaista, ukoliko postoji zajednički djelitelj $d > 1$ brojeva x i z, tada možemo staviti $x = a \cdot d$ i $z = b \cdot d$ za prirodne brojeve a, b i d. Iz jednakosti $y^2 = z^4 - x^4 = (b^4 - a^4)d^4$ slijedi da postoji prirodan broj c takav da vrijedi $y = d^2 \cdot c$. Uvrštavanjem u (4.5) i dijeljenjem obje strane jednadžbe s d^4 dobijemo

$$\left(a^2\right)^2 + c^2 = \left(b^2\right)^2.$$

Ovom je jednakošću definirana Pitagorina trojka (a^2, c, b^2) s hipotenuzom b^2 manjom od z^2, što je kontradikcija s minimalnosti od z^2. Stoga mora vrijediti da je (x^2, y, z^2) primitivna Pitagorina trojka.

Iz jednadžbe (4.5) uočimo da vrijedi

$$\left(x^2\right)^2 + y^2 = \left(z^2\right)^2.$$

Ukoliko je y paran, onda prema Teoremu 3.1.3 postoje relativno prosti prirodni brojevi m, n različite parnosti takvi da je $m > n$ za koje vrijedi

$$x^2 = m^2 - n^2, \quad y = 2mn \quad \text{i} \quad z^2 = m^2 + n^2.$$

Množenjem prve i zadnje jednakosti dobijemo $(xz)^2 = m^4 - n^4$, odnosno $\left(n^2\right)^2 + (xz)^2 = \left(m^2\right)^2$. Uočimo da je u Pitagorinoj trojki (n^2, xz, m^2) hipotenuza $m^2 < z^2$ što je proturječno s pretpostavkom o minimalnosti od z^2.

Prema tome, y mora biti neparan, što znači da je x^2, pa onda i x paran. Budući da vrijedi $y^2 = z^4 - x^4 = (z^2 - x^2)(z^2 + x^2)$ možemo primijeniti Korolar 1.1.8, pa postoje prirodni brojevi r, s za koje vrijedi

$$z^2 - x^2 = r^2 \quad \text{i} \quad z^2 + x^2 = s^2.$$

$$\frac{s \pm r}{2} = {m_1}^2 - {n_1}^2, \quad \frac{s \mp r}{2} = 2m_1 n_1 \quad \text{i} \quad z = {m_1}^2 + {n_1}^2.$$

Također, vrijedi $2x^2 = s^2 - r^2 = (s - r)(s + r) = 2(2m_1 n_1)2\left({m_1}^2 - {n_1}^2\right) = 8m_1 n_1(m_1 - n_1)(m_1 + n_1)$. Kako su m_1 i n_1 relativno prosti brojevi različite parnosti, slijedi da su brojevi m_1, n_1, $m_1 - n_1$ i $m_1 + n_1$ u parovima relativno prosti. Stoga, prema Korolaru 1.1.8 postoje k, l, p i $q \in \mathbb{N}$ takvi da je

$$m_1 = k^2, \quad n_1 = l^2, \quad m_1 - n_1 = p^2, \quad m_1 + n_1 = q^2.$$

Odavde je $k^4 - l^4 = \left({m_1}^2 - {n_1}^2\right) = (m_1 - n_1)(m_1 + n_1) = (pq)^2$, odnosno $\left(l^2\right)^2 + (pq)^2 = \left(k^2\right)^2$. Danom jednakosti je formirana Pitagorina trojka $\left(l^2, pq, k^2\right)$ s hipotenuzom $k^2 = m_1 < m_1^2 + n_1^2 = z < z^2$ čime je stvorena kontradikcija s minimalnosti od z^2. □

4.3 Posljednji Fermatov teorem u slučaju n=4

Teorem 4.3.1 (Posljednji Fermatov teorem u slučaju $n = 4$)**.** *Ne postoje rješenja jednadžbe*

$$x^4 + y^4 = z^4 \tag{4.6}$$

u skupu prirodnih brojeva. Drugim riječima, ne postoji Pitagorin trokut u kome su sve tri stranice kvadrati prirodnih brojeva.

Dokaz. Pretpostavimo suprotno, odnosno da postoje prirodni brojevi x, y i z koji zadovoljavaju jednadžbu (4.6). Kako je $z^4 = \left(z^2\right)^2$ vrijedi da je uređena trojka prirodnih brojeva (x, y, z^2) rješenje jednadžbe $x^4 + y^4 = z^2$. Međutim, time smo dobili kontradikciju s tvrdnjom Teorema 4.2.3, pa se može zaključiti da pretpostavka nije bila valjana. □

Napomena 4.3.2. *Teorem 4.3.1 se na sličan način može dokazati korištenjem Teorema 4.2.4, ukoliko y^4 zapišemo kao $\left(y^2\right)^2$.*

Slijedi Korolar koji, kao posljedica Posljednjeg Fermatovog teorema u slučaju $n = 4$, daje karakterizaciju Pitagorina trokuta preko njegove površine.

Korolar 4.3.3. *Ne postoji Pitagorin trokut čija je površina potpun kvadrat.*

Dokaz. Pretpostavimo suprotno, odnosno da takav trokut sa stranicama x, y i z postoji. Stoga mora vrijediti

$$x^2 + y^2 = z^2 \quad \text{i} \quad P(\triangle) = \frac{xy}{2}.$$

Prema pretpostavci, postoji prirodan broj u takav da je $P(\triangle) = u^2$. Iz ovoga slijedi jednadžba $2xy = (2u)^2$. Dodavanjem i oduzimanjem $2xy$ u prvoj jednadžbi i uvrštavanjem prethodne jednadžbe, dobijemo

$$(x + y)^2 = z^2 + (2u)^2, \quad (x - y)^2 = z^2 - (2u)^2.$$

Kombinacijom prethodnih dvaju jednakosti dolazimo do $\left(x^2 - y^2\right)^2 = z^4 - (2u)^4$, odnosno

$$\left(x^2 - y^2\right)^2 + (2u)^4 = z^4.$$

Dakle, dobili smo Pitagorin trokut čija je hipotenuza z^2, a jedna kateta $(2u)^2$, što je u suprotnosti s Teoremom 4.2.4. Shodno tome, zaključujemo da površina Pitagorinog trokuta ne može biti potpun kvadrat. □

Napomena 4.3.4. *Iz prethodnog korolara slijedi da ne postoji Pitagorin trokut s racionalnim stranicama čija je površina jednaka* 1. *Zaista, ukoliko pretpostavimo da takav trokut postoji i označimo njegove stranice s* $\frac{a}{d}$, $\frac{b}{d}$ *i* $\frac{c}{d}$ *pri čemu su a, b, c i d pozitivni cijeli brojevi, vrijedi jednakost*

$$\left(\frac{a}{d}\right)^2 + \left(\frac{b}{d}\right)^2 = \left(\frac{c}{d}\right)^2,$$

odnosno nakon sređivanja

$$a^2 + b^2 = c^2.$$

Uočimo da je jednadžbom definiran Pitagorin trokut s cjelobrojnim stranicama a, b i c. Kako za površinu početnog trokuta vrijedi $\frac{1}{2} \cdot \frac{a}{d} \cdot \frac{b}{d} = 1$*, lako slijedi jednadžba*

$$\frac{ab}{2} = d^2.$$

Dakle, dobili smo da je površina Pitagorina trokuta s cjelobrojnim stranicama a, b, c potpun kvadrat, što se protivi tvrdnji Korolara 4.3.3.

Primjer 4.3.5. *Pokažimo da ne postoje cjelobrojna rješenja jednadžbe* $x^4 + 4y^4 = z^2$.

Rješenje: Pretpostavimo suprotno i zapišimo danu jednadžbu u obliku

$$\left(x^2\right)^2 + \left(2y^2\right)^2 = z^2,$$

iz čega slijedi da je $\left(x^2, 2y^2, z\right)$ Pitagorina trojka. Pitagorin trokut čije su stranice dane s x^2, $2y^2$ i z ima površinu

$$P(\triangle) = \frac{1}{\cancel{2}} \cdot x^2 \cdot \cancel{2}y^2 = (xy)^2.$$

Budući da je površina promatranog trokuta potpun kvadrat, dobili smo kontradikciju s Korolarom 4.3.3. Stoga zaključujemo da dana jednadžba nema cjelobrojnih rješenja. □

Slučaj $n = 4$ Posljednjeg Fermatovog teorema jedini je slučaj kod kojeg je poznat relativno jednostavan elementarni dokaz. Već za slučaj $n = 3$ potrebno je promatrati kompleksne brojeve oblika $a + b\sqrt{-3}$, pri čemu su $a, b \in \mathbb{Z}$. Stoga u sljedećem Poglavlju donosimo sažetak dokazivanja teorema za ostale eksponente.

Poglavlje 5

Opis dokazivanja Posljednjeg Fermatovog teorema za eksponente različite od četiri

Fermat je uočio da ukoliko rješenje postoji za bilo koju potenciju n, tada će rješenje postojati i za bilo koji višekratnik potencije n. Stoga je dovoljno promatrati samo potencije koje su prosti brojevi. Uistinu, za prirodan broj m vidimo da jednadžba $x^{4m} + y^{4m} = z^{4m}$ nema rješenja jer bi inače trojka (x^m, y^m, z^m) predstavljala rješenje jednadžbe (4.6) za koju smo utvrdili da ne vrijedi u skupu prirodnih brojeva. Prema tome, zaključujemo da je Posljednji Fermatov teorem istinit za sve eksponente n djeljive s 4, pa onda i s 2.

Promotrimo sada slučaj kada eksponent $n > 2$ nije djeljiv s 4. Tada znamo da n ne može biti potencija broja 2 i da mora biti djeljiv s nekim prostim brojem $p \neq 2$. Drugim riječima, postoji prirodan broj k za kojeg vrijedi $n = pk$. Zaključujemo da nam je za dokazivanje tvrdnje da jednadžba $x^n + y^n = z^n$ nema rješenja u skupu prirodnih brojeva dovoljno pokazati da

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

nema rješenja za prost broj $p \neq 2$. Dakle, jednom kada smo dokazali Posljednji Fermatov teorem za slučaj $n = 4$, dokaz općeg slučaja smo ograničili na promatranje prostih eksponenata većih od 2.

5.1 Eulerov dokaz u slučaju n = 3

Euler je računao bez vidljiva napora, onako kako čovjek diše ili kako se orao održava na vjetru.

Francois Arago

Leonhard Euler[1] jedan je od najplodonosnijih i najuspješnijih matematičara 18. stoljeća. Njegovi doprinosi prisutni su u gotovo svim područjima matematike, od primijenjene matematike do algebarske topologije i teorije brojeva. Uz izricanje novih teorema i otkrivanje novih računarskih metoda, osmislio je čitav niz udžbenika iz algebre, analitike, matematičke fizike i mnogih drugih područja, koji su postali temelj obrazovanja sljedećih generacija matematičara. Duboko je zaslužan za osmišljavanje i promicanje moderne matematičke notacije i terminologije.

Godine 1770. Euler je predložio dokaz Posljednjeg Fermatovog teorema za slučaj $n = 3$, ali je dokaz bio nepotpun. Teorem u ovom slučaju govori da ne postoje cjelobrojna rješenja jednadžbe

$$x^3 + y^3 = z^3. \tag{5.1}$$

Osnovna ideja dokaza bilo je korištenje Fermatove metode beskonačnog spusta opisane u 4.2. Analiza Eulerovog dokaza otkrila je važan segment koji mu je nedostajao, a odnosio se na svojstvo djeljivosti cijelih brojeva oblika $p^2 + 3q^2$. Dokaz polazi od pretpostavke da su x, y i z u parovima relativno prosti brojevi, z je paran, a x i y neparni. Kako su $x + y$ i $x - y$ parni, zapišemo ih redom kao $2p$ i $2q$, za $p, q \in \mathbb{Z}$. Iz ovoga proizlazi da je $x = p + q$ i $y = p - q$, pa se iz jednadžbe (5.1) dobiva

$$2p\left(p^2 + 3q^2\right) = z^3, \quad pq \neq 0.$$

Euler je nakon toga izraz $p^2 + 3q^2$ htio zapisati kao savršeni kub, pa je ustanovio da je dovoljno pronaći $a, b \in \mathbb{Z}$ takve da vrijedi

$$p = a^3 - 9ab^2 \quad \text{i} \quad q = 3a^2b - 3b^3. \tag{5.2}$$

Tada je

$$p^2 + 3q^2 = \left(a^2 + 3b^2\right)^3. \tag{5.3}$$

Zatim je pokušao pokazati da i obrnuti postupak također funkcionira, odnosno da, ukoliko je $p^2 + 3q^2$ savršen kub, postoje cijeli brojevi a i b koji zadovoljavaju relaciju 5.3. Pri dokazivanju je koristio raspis

$$p^2 + 3q^2 = (p - q\sqrt{-3})(p + q\sqrt{-3}),$$

[1] Leonhard Euler, 1707. - 1783., švicarski matematičar, fizičar i astronom

no napravio je propust zbog nedovoljnog poznavanja računa u prstenu kompleksnih brojeva. Vjerovao je da brojevi oblika $p + q\sqrt{-3}$ posjeduju ista svojstva kao i cijeli brojevi. Preciznije, koristeći aritmetiku cijelih brojeva pretpostavio je da prsten

$$\mathbb{Z}\left[\sqrt{-3}\right] = \left\{x + \sqrt{-3}y : x, y \in \mathbb{Z}\right\}$$

karakterizira jedinstvena faktorizacija, no iskorišteno svojstvo nije dokazao. Međutim, drugi rezultati koje je Euler kasnije objavio ponudili su alternativni dokaz za slučaj $n = 3$, bez logičkih praznina, što je opravdalo pridavanje punih zasluga Euleru za ovaj slučaj.

Naknadno je njemački matematičar Gauss[2] prilagodio Eulerov dokaz teorema za kubove u prstenu $\mathbb{Z}\left[\sqrt{-3}\right]$ i on se može pronaći u [14]. Gaussovi rezultati iz teorije brojeva, objavljeni 1801. godine u knjizi *Disquisitiones Arithmeticae*[3], bili su od velike važnosti u kasnijim pokušajima dokazivanja Posljednjeg Fermatovog teorema. Gauss je dao značajan doprinos razvoju grane matematike poznate kao kompleksna analiza, području koje se bavi primjenom Eulerovih kompleksnih brojeva u vidu kompleksnih funkcija kompleksne varijable. Proučavanje ponašanja funkcija u kompleksnoj ravnini, takozvanih analitičkih funkcija, opisivanje njihovih svojstava, te analiza posebnog oblika analitičkih funkcija pod nazivom modularne forme bit će ključni u promjeni pogleda na dokazivanje Posljednjeg Fermatovog teorema.

5.2 Sophie Germain i slučajevi n = 5, 7

Približno dvije stotine godina nakon što je Fermat napisao svoju poznatu bilješku na marginama Diofantove *Aritmetike*, teorem je bio dokazan samo za eksponente 3, 4 i njihove višekratnike. Međutim, budući da je teorem trebalo dokazati za bilo koji proizvoljan eksponent, ostao je još dug put do pronalaženja općeg dokaza koji bi vrijedio za sve eksponente, ma koliko veliki oni bili. Činilo se da matematičari traže naizgled nedostižan dokaz, dok početkom 19. stoljeća nije ostvaren pomak zahvaljujući francuskoj matematičarki Sophie Germain[4].

Teorem Sophie Germain

Godine 1804. Gauss je primio pismo potpisano s *Monsieur Antoine - Auguste Le Blanc* koje je sadržavalo inovativne rezultate vezane za dokazivanje Posljednjeg Fermatovog teorema. Kroz kontinuiranu komunikaciju s Le Blancom, stekao je poštovanje prema njegovom radu. Prošlo je mnogo vremena prije nego što je saznao da je pravi autor pisama

[2] Karl Friedrich Gauss, 1777. - 1855., njemački matematičar, fizičar, geodet i astronom

[3] hrv. *Istraživanja u aritmetici*

[4] Sophie Germain, 1776. - 1831., francuska matematičarka

zapravo francuskinja Sophie Germain. Jedna od rijetkih žena u području matematike u to doba preuzela je muški identitet kako bi izbjegla sve predrasude tog vremena prema ženama i privukla pažnju jednog od najvećih tadašnjih matematičkih autoriteta. Germain je predložila podjelu problema dokazivanja Posljednjeg Fermatovog teorema na dva slučaja:

I. Jednadžba $x^p + y^p = z^p$ nema cjelobrojnih rješenja, pri čemu su x, y i z nisu djeljivi s p.

II. Jednadžba $x^p + y^p = z^p$ nema cjelobrojnih rješenja, pri čemu su x, y i z djeljivi s p.

1823. godine dokazala je prvi slučaj koristeći sljedeću tvrdnju koju danas poznajemo kao Teorem Sophie Germain:

Teorem 5.2.1 (Teorem Sophie Germain)**.** *Neka su n i p različiti neparni prosti brojevi koji zadovoljavaju sljedeće uvjete:*

1. *Ukoliko su x, y i z cijeli brojevi takvi da je*

$$x^n + y^n + z^n \equiv 0 \pmod{p},$$

onda vrijedi $p \mid xyz$, odnosno p dijeli x, y ili z.

2. *Kongruencija $x^n \equiv n \pmod{p}$ nema rješenja za nijedan cijeli broj x.*

Tada je prvi slučaj Posljednjeg Fermatovog teorema istinit za eksponent p.

Često se Teorem 5.2.1 iznosi u sljedećem obliku, čiji se dokaz može pronaći u [14]:

Teorem 5.2.2. *Ukoliko je $p > 2$ neparan prost broj za kojeg je $q = 2p + 1$ također prost, onda p mora dijeliti jedan od brojeva x, y ili z koji zadovoljavaju jednakost $x^p + y^p = z^p$. Drugim riječima, jednadžba*

$$x^p + y^p + z^p = 0$$

nema cjelobrojnih rješenja takvih da vrijedi $p \nmid xyz$.

Napomena 5.2.3. *Prost broj p za kojeg je $2p + 1$ također prost nazivamo* Sophie Germainovim prostim.

U kojoj god varijanti predočen, Teorem Sophie Germain smatra se prvom općenitom propozicijom Posljednjeg Fermatovog teorema, za razliku od svih dotadašnjih rezultata koji su se bazirali samo na pojedinačnim eksponentima. Iz njega direktno proizlazi da za sve Sophie Germainove proste brojeve $p = 3, 5, 11, 23, \ldots$ Fermatova jednadžba nema rješenja takvih da $p \nmid xyz$. Ovaj rezultat je bio veliki iskorak naprijed, usprkos tome što je

teorem bio dokazan samo za dio eksponenata i jedan od dvaju slučajeva. Naknadno su Germain i Legendre[5] zajedno pokazali da svi neparni prosti eksponenti $p \leq 197$ zadovoljavaju **I.** slučaj Posljednjeg Fermatovog teorema.

Pozornost se potom usmjerila na **II.** slučaj. Dokaz za $p = 5$ objavio je 1828. godine Dirichlet[6], no kako u njemu nije uzeo u obzir sve moguće slučajeve, dokaz nije bio potpun. Legendre je popunio nedostatke dvije godine kasnije, čime je slučaj $p = 5$ bio dokazan. Dirichlet je nastavio raditi na slučaju $p = 7$, no putem je shvatio da su njegove metode prikladnije za blisko povezani slučaj $p = 14$ kojeg je argumentirao 1832. godine. Slučaj $p = 7$ konačno je 1839. godine dokazao Lamé[7], a Lebesgue[8] je 1840. pronašao jednostavniji dokaz. Dokazi teorema za $p = 5$ i $p = 7$ mogu se pronaći u [16].

5.3 Nastavak dokazivanja teorema u 19. i 20. stoljeću

Fourierovi redovi

Sljedeća osoba na putu dokazivanja Posljednjeg Fermatovog teorema je Joseph Fourier[9], koji je istražujući provođenje topline u pustinji razvio teoriju periodičnih funkcija. Red takvih funkcija, korištenih na određeni način za procjenu druge funkcije, danas se naziva *Fourierov red*. Fourier je otkrio da se većina funkcija može procijeniti sumom sinus i kosinus funkcija, do na određeni stupanj točnosti. Premda je njegov glavni cilj bila primjena ovih funkcija za opisivanje raznih pojava u prirodi, Fourierovi redovi su pronašli korisne primjene i u čistoj matematici, polju koje nikada nije bilo jedno od Fourierovih glavnih interesa. U dvadesetom će se stoljeću Fourierovi redovi implementirati u teoriji brojeva u djelu Goroa Shimure[10], za transformaciju matematičkih elemenata iz jednog područja u drugo, a dokaz Shimurinog zaključka činit će samu srž dokazivanja Posljednjeg Fermatovog teorema. Daljnje proširenje periodičnih Fourierovih funkcija na kompleksnu ravninu dovest će do otkrića automorfnih funkcija i modularnih formi, koje će također imati presudnu ulogu u dokazivanju teorema kroz rad drugog francuskog matematičara s početka dvadesetog stoljeća, Henrija Poincaréa[11]. Više o Shimuri i Poincaréu slijedi u nastavku poglavlja.

[5] Adrien-Marie Legendre, 1752. - 1833., francuski matematičar i astronom
[6] Peter Gustav Lejeune Dirichlet, 1805. - 1859., njemački matematičar
[7] Gabriel Léon Jean Baptiste Lamé, 1795. — 1870., francuski matematičar i inženjer
[8] Henri Léon Lebesgue, 1875. - 1941., francuski matematičar
[9] Joseph Fourier, 1768. - 1830., francuski matematičar i fizičar
[10] Goro Shimura, 1930. - 2019., japanski matematičar
[11] Jules Henri Poincaré, 1854. – 1912., francuski matematičar i teorijski fizičar

Jedinstvenost faktorizacije i Kummerovi idealni brojevi

Ohrabren uspjehom u slučaju $p = 7$, Lamé je nastavio svoj rad na dokazivanju Posljednjeg Fermatovog teorema, te je 1847. godine uzbuđeno objavio da je pronašao općeniti dokaz. Metoda koju je upotrijebio svodila se na faktoriziranje lijeve strane jednadžbe (4.1) na linearne faktore, koristeći kompleksne brojeve. Drugim riječima, koristio je raspis

$$x^n + y^n = (x + y)(x + \zeta y) \cdots (x + \zeta^{n-1} y),$$

pri čemu je $\zeta = e^{\frac{2\pi i}{n}}$ za neparan prost broj n. Lamé je skromno priznao da je ideju dobio od Liouvillea[12], pridavši mu sve zasluge, no Liouville je uočio da rješenje zapravo nije valjano. Naime, primijetio je da ovakav raspis u prstenu cijelih ciklotomskih[13] brojeva ovisi o jedinstvenosti faktorizacije. Bio je to otmjen pokušaj, ali nažalost još jedan od mnogih koji nije urodio plodom.

Ideja o faktorizaciji ponovno će zaživjeti u Kummerovom[14] radu. On se više nego itko drugi u svoje vrijeme približio općem rješenju Fermatovog problema. Štoviše, osmislio je cijelu teoriju u matematici u pokušaju da dokaže Posljednji Fermatov teorem. Budući da jedinstvenost navedene faktorizacije nije bila iskoristiva, Kummer je uveo novu vrstu brojeva koji su sadržavali sva tražena svojstva - idealne brojeve. Iako nije uspio dokazati teorem, ostvario je izniman uspjeh u svojim pokušajima. Njegov rad na idealnim brojevima omogućio mu je da 1847. godine dokaže teorem za vrlo opsežnu klasu, štoviše beskonačnu, prostih eksponenata koji su dio klase *regularnih*[15] prostih brojeva. Dakle, Kummerov dokaz je preusmjerio naglasak sa sve kompliciranijih metoda dokazivanja teorema korištenih u slučaju malih eksponenata, na općenitiji dokaz za širok raspon eksponenata. Činjenica da je osmišljavanje potpuno nove matematičke teorije bilo inspirirano pokušajima rješavanja Posljednjeg Fermatovog teorema pokazuje kako se briljantne teorije mogu razviti samo pokušajima rješavanja određenih problema. Kummerova teorija idealnih brojeva dovela je do onoga što je danas poznato kao *ideali*, koji će kasnije imati utjecaj na rad mnogih matematičara vezan za Posljednji Fermatov teorem.

Wolfskehlova nagrada

Krajem 19. i početkom 20. stoljeća dokazi posebnih slučajeva postajali su sve složeniji, zahtijevajući visoku angažiranost matematičkih stručnjaka. Nešto značajniji pomak u do-

[12] Joseph Liouville, 1809. - 1882., francuski matematičar i inženjer

[13] *Ciklotomski brojevi* su brojevi oblika $a_0 + a_1\zeta + a_2\zeta^2 + \ldots + a_{n-1}\zeta^{n-1}$, pri čemu su $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$ i $\zeta = e^{\frac{2\pi i}{n}}$ za prost broj n. Ciklotomski cijeli brojevi tvore prsten $\mathbb{Z}[\zeta_n]$.

[14] Ernst Eduard Kummer, 1810. – 1893., njemački matematičar

[15] Prost broj p je *regularan* ukoliko ne dijeli broj klasa ciklotomskog polja generiranog s $e^{\frac{2\pi i}{p}}$, u oznaci $\mathbb{Q}[\zeta_p]$. U suprotnom, kažemo da je *neregularan*. Pritom je broj klasa pozitivan cijeli broj koji označava broj klasa ideala polja $\mathbb{Q}[\zeta_p]$. Jedini neregularni prosti brojevi manji od 100 su 37, 59 i 67.

kazivanju teorema ostvario je "matematičar iz hobija", Wolfskehl[16], kojeg je ispravljanje greške u Kummerovom radu spriječilo od nauma da si oduzme život. Premda zapravo nije bio ništa bliže rješenju teorema, postao je toliko očaran nedokazanim teoremom, da je većinu svog bogatstva posmrtno ostavio zakladi koja bi ga dodijelila prvoj osobi koja ili dokaže teorem ili pronađe protuprimjer. Nagrada je bila velike vrijednosti, stoga ne čudi da je u prvoj godini od objavljivanja pristigao čak 621 neuspjeli pokušaj. Kako je 20. stoljeće odmicalo, količina se pokušaja smanjivala, no i dalje pomalo pristižući sa svih strana svijeta. Unatoč velikom broju pokušaja, stvarni napredak početkom 20. stoljeća bio je podosta oskudan i većinom tehnički.

Galoisova teorija i Abelova grupa

Na području apstraktne algebre razvijene u devetnaestom stoljeću istaknuo se Évariste Galois[17], genij neusporedivih sposobnosti koji je već kao tinejdžer upijao čitave teorije algebre, razumljive samo vrsnim matematičarima, i razvijao vlastiti sustav, danas poznat kao *Galoisova teorija*. Nažalost, u svom tragično kratkom životu nije uspio objaviti novouvedenu teoriju niti je za nju doživio ikakvo priznanje. Nadajući se da će mu pomoći pri objavljivanju, svoju je dokumentaciju poslao cijenjenim matematičarima Cauchyju[18] i Poissonu[19], no nadareni Parižanin bio je puno ispred svog vremena, pa njegov izvanredan rad nije bio prepoznat. Mladenačka ga je zaljubljenost na kraju koštala svega, pa je zbog ljubavnog sukoba preminuo u dobi od dvadeset i jedne godine. Njegov očajnički pokušaj da zapiše još neobjavljenu matematičku teoriju noć prije sukoba, ispunjen je krikovima "*Nemam vremena, nemam vremena*" između redaka formula, te žustro precrtanima riječima "*jedna žena*". Liouville je naknadno uredio i 1846. godine objavio Galoisov rukopis, te će se njegova teorija stoljeće i pol kasnije koristiti kao jedan od ključnih koraka u metodi primijenjenoj za dokazivanje Posljednjeg Fermatovog teorema.

Sljedeća važna figura neizravno uključena u dokazivanje teorema mladi je matematičar Abel[20], koji, iako je riješio jedan od najslavnijih problema svoga vremena: problem rješavanja jednadžbe petog stupnja, poput svog suvremenika Galoisa ostaje u sjeni do kraja života. Najveće mu je postignuće koncept *Abelove grupe*[21], koji je uz još apstraktniji algebarski entitet pod nazivom *Abelova mnogostrukost*, vrlo važan u modernoj algebri i ključan element u tumačenju Fermatovog problema. Nažalost, život u siromaštvu i napor uzrokovan

[16] Paul Friedrich Wolfskehl, 1856. - 1906., njemački liječnik sa zanimanjem za matematiku

[17] Évariste Galois, 1811. - 1832., francuski matematičar

[18] Augustin Louis Cauchy, 1789. - 1857., francuski matematičar

[19] Siméon Denis Poisson, 1781. – 1840., francuski fizičar i matematičar

[20] Niels Henrik Abel, 1802. – 1829., norveški matematičar

[21] *Abelova grupa* je komutativna grupa, odnosno grupa u kojoj se redoslijed matematičkih operacija može obrnuti bez utjecaja na ishod.

uzdržavanjem obitelji u teškim okolnostima skrivili su njegovu preranu smrt ne dozvolivši mladom talentu da se ostvari u potpunosti.

Dedekindova teorija ideala i Poincaréove modularne forme

Jedan od najznačajnijih Gaussovih nasljednika matematičar je Dedekind[22], koji je predložio nacrt teorije razvijene za algebarske brojeve[23], te je uzvisio teoriju grupa do razine na kojoj se danas podučava i tumači. Njegov najveći doprinos modernom pristupu dokazivanja Posljednjeg Fermatovog teorema bio je razvoj teorije ideala, apstrakcije Kummerovih idealnih brojeva. Stoljeće nakon što ih je Dedekind izgradio, ideali će inspirirati Barryja Mazura[24] čije će se djelo iskoristiti u konačnom dokazu Posljednjeg Fermatovog teorema.

Na prijelazu iz devetnaestog stoljeća u dvadeseto, na scenu stupa francuski matematičar Poincaré, čije je glavno središte interesa proučavanje simetrija u teoriji kompleksnih funkcija. Analizom periodičnih funkcija u kompleksnoj ravnini, otkrio je postojanje takozvanih *automorfnih funkcija*, koje ostaju nepromijenjene kada na njih djeluje *Möbiusova transformacija* oblika

$$f(z) \longrightarrow f\left(\frac{az+b}{cz+d}\right),$$

pri čemu za kompleksne koeficijente a, b, c i d vrijedi $ad - bc \neq 0$. Štoviše, Poincaré je ovako definirane funkcije proširio na *modularne forme* koje će odigrati važnu ulogu u dokazu Fermatovog problema. Također, pružio je izrazit doprinos području koje je započeo proučavati Euler, topologiji. Smislio je način prevođenja topoloških problema u algebarski oblik tako što je klasificirao dvodimenzionalne plohe u trodimenzionalnom prostoru prema genusu[25], broju rupa u plohi nekog tijela. Iako se u početku činilo da ova ideja nema veze s Fermatovim problemom, nesvjesno je posadio sjeme koje će kasnije uroditi plodom. S vremenom je uočeno da cjelobrojno rješenje Fermatove jednadžbe (4.1) odgovara racionalnom rješenju $a = \frac{x}{z}$, $b = \frac{y}{z}$ jednadžbe

$$a^n + b^n - 1 = 0, \tag{5.4}$$

što je dokazivanje Posljednjeg Fermatovog teorema svelo na dokazivanje da dana jednadžba nema racionalnih rješenja.

[22] Julius Wilhelm Richard Dedekind, 1831. – 1916., njemački matematičar
[23] *Algebarski brojevi* su definirani kao rješenja algebarskih jednadžbi
[24] Barry Charles Mazur, 1937. - , američki matematičar
[25] Primjerice, sfera bez rupa ima genus 0, dok torus ima genus 1.

Faltingsonov dokaz Mordellove pretpostavke

1922. godine matematičar Mordell[26] dolazi do sjajne ideje da u obzir uzme ne samo racionalna rješenja jednadžbe, već i kompleksna. Koristeći Poincaréovu klasifikaciju ploha prema genusu, otkrio je potpuno neočekivanu vezu između genusa prostora rješenja jednadžbe i toga ima li jednadžba konačan ili beskonačan broj rješenja. Utvrdio je da ukoliko ploha prostora rješenja jednadžbe (5.4) ima dvije ili više rupa (odnosno, genus veći ili jednak 2), tada jednadžba ima samo konačno mnogo racionalnih rješenja. Mordell nije uspio dokazati svoje otkriće, pa je postalo poznato pod nazivom *Mordellova pretpostavka*. Budući da je genus Fermatove jednadžbe (4.1) za $n > 3$ veći ili jednak 2, dokazivanjem Mordellove pretpostavke odmah bi slijedilo da ukoliko rješenja Fermatove za $n > 3$ uopće postoje, onda ih ima najviše konačno mnogo.

Mordellova pretpostavka dokazana je 1983. godine zaslugom dvadesetsedmogodišnjaka Faltingsa[27], a ubrzo nakon toga pristigli su novi rezultati. Britanski matematičari Granville[28] i Heath-Brown[29] koriste Faltingsov rezultat kako bi 1985. godine pokazali da je Posljednji Fermatov teorem istinit za gotovo sve eksponente. Preciznije, dokazali su da se broj rješenja Fermatove jednadžbe, ukoliko uopće postoje, smanjuje s povećanjem eksponenta n. Drugim riječima, udio eksponenata za koje je teorem istinit se približava udjelu od sto posto kako n raste. Dakle, ako rješenja postoje, onda ih je malo i vrlo su udaljena.

Eliptičke krivulje

Diofantski problemi počeli su se sve više proučavati u 20. stoljeću koristeći matematičke entitete zvane *eliptičke krivulje*[30]. Promatranjem racionalnih točaka na eliptičkim krivuljama, zaključilo se da ti brojevi čine grupu, što znači da imaju lijepa svojstva. Stručnjaci za teoriju brojeva već su neko vrijeme znali da su neke od eliptičkih krivulja modularne, no nije bilo sasvim jasno iz kojih razloga. Jedna od eliptičkih krivulja je i *Fermatova krivulja stupnja n*, u oznaci $\mathcal{F}_n$, pridružena jednadžbi (5.4). Na slici 5.1 prikazane su neke od Fermatovih krivulja. Posljednji Fermatov teorem izražen u terminima Fermatovih krivulja glasi ovako:

Teorem 5.3.1 (Posljednji Fermatov teorem za Fermatove krivulje)**.** *Jedine točke s obje racionalne koordinate na krivulji $\mathcal{F}_n$ za $n > 2$ su točke presjeka s koordinatnim osima.*

[26] Louis Joel Mordell, 1888. – 1972., britanski matematičar, rođen u Americi

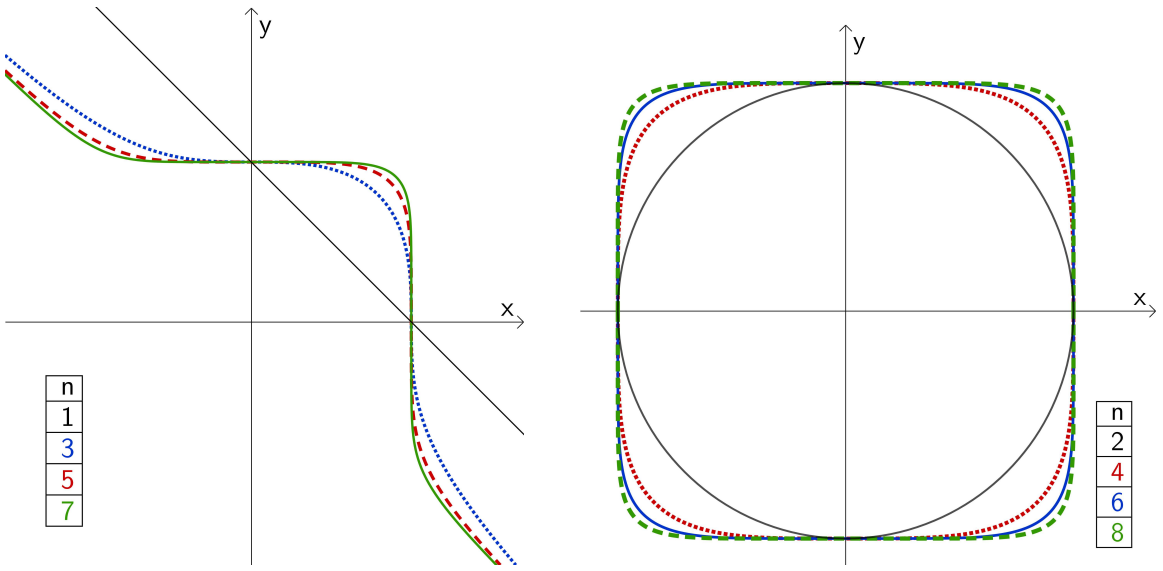
[27] Gerd Faltings, 1954. - , njemački matematičar

[28] Andrew Granville, 1962. - , britanski matematičar

[29] Roger Heath-Brown, 1952. - , britanski matematičar

[30] *Eliptička krivulja nad poljem K* je glatka, projektivna krivulja genusa 1 sa specificiranom točkom $O \in K$. Više o eliptičkim krivuljama može se pronaći u [13].

Napomena 5.3.2. *Nalik tome, Mordellova pretpostavka ekvivalentna je tvrdnji da na svakoj algebarskoj krivulji stupnja većeg od tri postoji najviše konačno mnogo racionalnih točaka.*



Slika 5.1: Primjeri Fermatovih krivulja za neparne i parne eksponente

Shimura - Taniyama pretpostavka

Sljedeće uloge u rješavanju Fermatovog problema odigrali su dvojica japanskih matematičara, Taniyama[31] i Shimura. 1955. godine pomogli su organizirati Tokyo - Nikko simpozij o teoriji algebarskih brojeva, kako bi izgradili istraživačke veze s matematičarima iz njihovog područja interesa, teorije eliptičkih krivulja. Na simpoziju je nadareni dvadesetsedmogodišnjak Taniyama iznio tvrdnje koje će kasnije revolucionirati teoriju brojeva. Naime, predložio je izjednačavanje eliptičkih krivulja s modularnim formama, odnosno poistovjetio matematičke strukture koje pripadaju sasvim različitim područjima. Štoviše, Taniyama je uspio povezati Poincaréove automorfne funkcije u kompleksnoj ravnini sa zeta funkcijama eliptičkih krivulja. Iako je imao snažno intuitivno razumijevanje matematike i vukao ga je osjećaj da su automorfne funkcije sa svojim brojnim simetrijama u kompleksnoj ravnini na neki način povezane s diofanskim jednadžbama, utjelovljena pretpostavka nije bila do kraja rasvijetljena jer mu je nedostajala sposobnost da problem formulira na matematički koherentan način. Međutim, ukoliko je njegova pretpostavka bila točna, to bi značilo da se neriješeni problemi u jednom području mogu prevesti na jezik i koncepte drugoga, pa možda čak i riješiti metodom koja je tamo dostupna. Među sudionicima simpozija

[31] Yutaka Taniyama, 1927. - 1958., japanski matematičar

bio je i André Weil[32], član Bourbaki društva[33], koji je u to vrijeme pokušavao matematičkoj zajednici usmjeriti pažnju na zeta funkcije, te mladi francuski matematičar Serre[34]. Weil je pokazao interes za danu hipotezu, no nakon razgovora s Taniyamom, sumnja u predloženu povezanost naoko nespojivih matematičkih struktura se produbila. Dana je tvrdnja bila potpuna kontroverza na tadašnjoj matematičkoj sceni i nije bila shvaćena ozbiljno, što je možebitno utjecalo na Taniyamu koji si je tri godine kasnije oduzeo život.

Međutim, njegov prijatelj Shimura nikad nije izgubio vjeru u točnost predočene ideje. U desetljeću koje je uslijedilo nakon Tokyo - Nikko konferencije, Shimura je marljivo skupljao argumente i ispravljao pogreške svog pokojnog prijatelja, te ga je vlastito istraživanje navelo da formulira hrabriju i precizniju pretpostavku. Tvrdio je da se svaka eliptička krivulja nad racionalnim brojevima može uniformizirati modularnom formom, odnosno da svaka eliptička krivulja s racionalnim koeficijentima ima par u kompleksnoj poluravnini $\{z = x + iy \mid y > 0\}$ sa svojom neeuklidskom, hiperboličkom geometrijom. Ova je tvrdnja s vremenom stjecala sve više pobornika i danas nosi naziv *Shimura - Taniyama pretpostavka*, mada to nije uvijek bilo tako. Početkom 1960. godine, Serre je iskritizirao Shimurine rezultate, a Weil je potvrdio da ni deset godina nakon Taniyamine srodne pretpostavke još uvijek ne vjeruje ni jednoj ni drugoj tezi. Međutim, nakon Weilovih objava vezanih za razgovore sa Shimurom, njegovo se ime krenulo povezivati s Shimura - Taniyama pretpostavkom premda nije smatrao da je ispravna. S desetljećima koja su prolazila, bilo je sve više razloga za vjerovanje u točnost ove tvrdnje, a kako je Weilu nezaslužena popularnost godila, pri objavama vezanim za ovu pretpostavku izostavljao je Shimurinu ključnu ulogu, pa su tako modularne eliptičke krivulje postale poznate kao *Weilove krivulje*. Pogreška se produbila kada su se matematičari u svojim radovima referirali na tuđa djela, pa je Shimura - Taniyama pretpostavka pogrešno nazivana Weil - Taniyama pretpostavka, dok je Shimurino ime potpuno zanemareno. Klopko zavrzlame napokon se rasplelo 1986. godine kada je Weil u pismu matematičaru Langu[35] porekao bilo kakvu ideju o pokušaju umanjivanja Taniyaminih i Shimurinih zasluga pri formuliranju čuvene pretpostavke.

[32] André Weil, 1906. - 1998., francuski matematičar

[33] Udruženje nadarenih matematičara osnovano između dva svjetska rata u Parizu po uzoru na Pitagorejce. Bourbaki skupina donosi novu viziju matematike, reorganizira i pojašnjava njene sastavnice koristeći osebujan stil i objavljujući knjige pod pseudonimom Nicolas Bourbaki, pazeći da se pritom važniji rezultati pripišu zaslužnim matematičarima.

[34] Jean-Pierre Serre, 1926. - , francuski matematičar

[35] Serge Lang, 1927. - 2005., francusko-američki matematičar

Freyeva pretpostavka: Shimura - Taniyama pretpostavka $\Longrightarrow$ Posljednji Fermatov teorem

Gerhard Frey[36] je 70-ih godina prošlog stoljeća, pod utjecajem Mazurovog rada, razmišljao o primjenama modularnih krivulja i Galoisovih reprezentacija na teoriju eliptičkih krivulja. Otkrio je da bi to, gotovo neizbježno, dovelo do rješenja diofantskih problema koji su usko povezani s Fermatovom jednadžbom. Godine 1984. održao je govor na konferenciji u Oberwolfachu, gdje je iznio naizgled sasvim šokantnu tvrdnju. Naime, vjerovao je da će Posljednji Fermatov teorem biti dokazan ukoliko je Shimura - Taniyama pretpostavka istinita, odnosno sugerirao je sljedeću implikaciju:

$$\text{Shimura - Taniyama pretpostavka} \implies \text{Posljednji Fermatov teorem}$$

Način na koji je Freyeva ideja funkcionirala bio je genijalan. Predložio je sljedeće:
Pretpostavimo da Posljednji Fermatov teorem nije istinit, odnosno da za neki eksponent $n > 2$ *postoji rješenje a, b, c Fermatove jednadžbe* $x^n + y^n = z^n$*, pri čemu su* $x, y, z \in \mathbb{Z}$*. Tada bi to rješenje dovelo do specifične eliptičke krivulje (danas poznate pod nazivom* Freyeva krivulja*) čija bi se jednadžba mogla zapisati u sljedećem obliku:*

$$\begin{aligned} y^2 &= x\,(x + a^n)\,(x - b^n) \\ &= x^3 + (a^n - b^n)\,x^2 - a^n b^n x \end{aligned}$$

Štoviše, Frey je uočio par doista čudnih posljedica ove tvrdnje. Među ostalim, diskriminanta $a^{2n}b^{2n}c^{2n}$ *predložene jednadžbe savršeni je kvadrat. Ovakva je krivulja toliko neobična da zapravo nikako ne bi mogla ni postojati. Zaista, eliptička krivulja koja bi proizašla u slučaju da Posljednji Fermatov teorem nije točan, ne bi bila modularna. To bi odmah značilo da je u suprotnosti s Shimura - Taniyama pretpostavkom koja tvrdi da sve eliptičke krivulje moraju biti modularne. Ovime bi slijedilo da ni rješenja Fermatove jednadžbe ne bi mogla postojati, čime bi Posljednji Fermatov teorem bio dokazan.*
Ovo je bio kompliciran slijed implikacija, ali je spretno slijedio logiku matematičkog dokaza, koristeći obrat po kontrapoziciji. Iako danu pretpostavku, neformalno nazvanu *Epsilon pretpostavka*, nije uspio u potpunosti dokazati, Frey je ponudio uvjerljive argumente koji podržavaju njenu točnost.

Ribetov dokaz Freyeve pretpostavke

Američki matematičar Ribet[37] sljedeća je ključna osoba u dokazu Fermatovog problema. Ribet na početku svoje karijere uopće nije bio zainteresiran za Fermatov problem, jer je

[36] Gerhard Frey, 1944. - , njemački matematičar
[37] Kenneth Alan Ribet, 1948. - , američki matematičar

smatrao da je to jedan od problema kojima se ne može pridodati išta od stvarne važnosti. Mnogi drugi matematičari dijelili su s njim mišljenje, budući da su problemi u teoriji brojeva obično izolirani, bez sveobuhvatne strategije ili temeljnog općeg principa rješavanja. Međutim, Posljednji Fermatov teorem je iznimno zanimljiv jer se proteže kroz cijelu matematičku povijest, od početaka civilizacije pa sve do našeg vremena. Uz to, konačno rješenje teorema obuhvaća mnoštvo matematičkih područja, uključujući primjerice teoriju brojeva, algebru, analizu, geometriju i topologiju. Ribetovo se gledište promijenilo pod utjecajem velikog stručnjaka u teoriji brojeva, Barryja Mazura. Kada je prvi put čuo za Freyjevu izjavu, Ribet je mislio da je šala, no s vremenom ga je privukao ovaj vrlo popularan problem koji se nalazio u području kojeg je dobro poznavao. Situacija je dobila novi zaplet kada je Ribet 1986. godine, uz Mazurovu pomoć, te koristeći Serreove ideje o modularnim Galoisovim grupama, dokazao Freyjevo nagađanje. Čovjek koji je samo godinu dana ranije Freyev prijedlog smatrao neostvarivim, dokazao je njegovu istinitost, te time širom otvorio vrata razumijevanju Fermatovog problema. Svijetu je još trebao netko tko će dokazati naizgled nesavladivu Shimura - Taniyama pretpostavku.

5.4 Andrew Wiles donosi sretan kraj priči staroj više od 350 godina

Osoba koja je o tome dugo maštala bio je Andrew Wiles[38]. Kako se prisjetio u novinarskom izvještaju 1997. godine:

I was a 10-year old, and one day I happened to be looking in my local public library and I found a book on math and it told a bit about the history of this problem - that someone had resolved this problem 300 years ago, but no one had ever seen the proof, no one knew if there was a proof, and people ever since have looked for the proof. And here was a problem that I, a 10-year-old, could understand, but none of the great mathematicians in the past had been able to resolve. And from that moment of course I just tried to solve it myself. It was such a challenge, such a beautiful problem.

1971. godine Wiles iz rodnog Cambridgea odlazi na sveučilište u Oxfordu studirati matematiku, te se nakon diplome vraća u Cambridge na sveučilište kako bi pisao doktorat. Želio je nastaviti s potragom za dokazom Posljednjeg Fermatovog teorema, ali na nagovor mentora Johna Coatesa[39] odustaje od dječačkog sna, svjestan činjenice da bi se istraživanje moglo pretvoriti u gubitak vremena kojeg si nije mogao priuštiti. Umjesto toga, Wiles

[38] Sir Andrew John Wiles, 1953. - , engleski matematičar i profesor na sveučilištu u Oxfordu

[39] John Henry Coates, 1945. - 2022., australski matematičar

je proučavao eliptičke krivulje i područje nazvano *Iwasawina teorija*[40]. Nakon završenog doktorata 1980. godine, postaje profesor na Princetonu. Kada je Ribet 1985. godine dokazao Freyevu pretpostavku, san kojeg se Wiles morao odreći ponovno je oživio. Potpuno se posvetio dokazivanju Shimura - Taniyama pretpostavke, radeći u strogoj tajnosti i izolaciji u uredu na tavanu, kako ne bi privukao mnogo pažnje i kako bi mogao ostati usredotočen. Njegova veličina, kako je Frey izjavio, bila je u tome što je čvrsto vjerovao u ono što je radio, i to u vrijeme kada je gotovo svaki drugi matematičar na svijetu mislio da se Shimura - Taniyama pretpostavka ne može dokazati koristeći alate dvadesetog stoljeća. No, Wilesova je glavna moć bila u tome što je na raspolaganju imao mnoštvo rezultata svojih suvremenika i prethodnika iz različitih matematičkih područja. Kako bi dokazao Shimura - Taniyama pretpostavku, znao je da mora dokazati da je svaka eliptička krivulja modularna. Činilo mu se da je najbolja ideja pokušati zasebno izbrojiti koliko ima eliptičkih krivulja, a koliko modularnih, te zatim pokazati da su ti brojevi jednaki. Shvatio je da ne mora dokazivati cijelu Shimura - Taniyama pretpostavku, već samo slučaj polustabilnih eliptičkih krivulja s racionalnim koeficijentima, te je bio svjestan činjenice da opisano brojanje neće funkcionirati jer ima posla sa skupom koji je beskonačan. Stoga je Wiles probao problem razbiti na više manjih, no to ga nažalost nije dovelo do uspjeha.

Galoisove reprezentacije i Flachova pomoć

Nakon dvije godine uzaludnog truda iskušao je novi pristup. Ideja mu je bila transformirati eliptičke krivulje u Galoisove reprezentacije, a zatim usporediti broj Galoisovih reprezentacija s brojem modularnih formi. Korištenje Galoisove teorije omogućilo bi mu da pređe s promatranja beskonačnog skupa na promatranje konačnog, što bi bilo olakšavajuće budući da je s konačnim skupom elemenata mnogo zgodnije rukovati. Koristio je svoje područje stručnosti, horizontalnu Iwasawinu teoriju, kako bi prebrojio skupove, no nakon dodatnih godinu dana rada, Wiles je ponovno naišao na poteškoću. Na konferenciji u Bostonu 1991. godine, susreće Coatesa koji ga povezuje s briljantnim mladim studentom Flachom[41], čiji je nedavni rad bio upravo ono što je Wilesu trebalo za dokaz Shimura - Taniyama pretpostavke. Wiles odmah napušta horizontalnu Iwasawinu teoriju i danonoćno proučava Flachove rezultate.

Pomoć kolega i Mazurova promjena *3-na-5*

U siječnju 1993. godine, nakon šest godina samostalnog rada, Wiles naziva kolegu s Princetona, profesora Katza[42], kako bi provjerio njegov rad. Trebao mu je stručnjak koji poz-

[40]Područje teorije brojeva izniklo iz radova japanskog matematičara Kenkichija Iwasawe u kasnim 1950-ima. Više o ovoj teoriji može se pronaći u [17].

[41]Matthias Flach, 1963. - , njemački matematičar

[42]Nicholas Michael Katz, 1943. - , američki matematičar i profesor na sveučilištu Princeton

naje danu materiju, ali i osoba od povjerenja koja bi pazila da se njegove ideje i rezultati ne šire dalje. Stoga domišljato organizira kolegij na diplomskom studiju, pod nazivom *Izračuni s eliptičkim krivuljama*, kojeg će Katz pohađati kao jedan od studenata. To im omogućuje neprestanu suradnju bez uplitanja drugih matematičara i znatiželjnih očiju javnosti. Svi studenti koji su pohađali kolegij odustali su u prvih nekoliko tjedana jer je prezentiranu teoriju bilo teško pratiti, pa je Katz ostao sam u publici. Predavanja nisu otkrila nikakvu pogrešku i činilo se da je Wiles na dobrom putu prema rješenju Fermatovog problema. Krajem proljeća 1993. godine kolegij se približavao kraju, no Wilesu je ostala još jedna prepreka. Uspio je dokazati modularnost većine klasa eliptičkih krivulja, ali mu je za nekoliko preostalih to svojstvo izmicalo. Uporan u naumu da dođe do rješenja, traži pomoć pouzdanog kolege, profesora Sarnaka[43], no čak ni uz njegovu asistenciju ne uspijeva riješiti problem.

Kako bi se odmorio od intenzivne potrage koja se činila kao da ne vodi nikuda, Wiles je krenuo razmatrati stari Mazurov rad o proširenju teorije ideala. Jedna njegova izjava posebno mu je privukla pozornost. Naime, Mazur je tvrdio da je klasu eliptičkih krivulja temeljenih na prostom broju 3 moguće transformirati tako da ih se može proučavati koristeći prosti broj 5. Budući da je za klasu eliptičkih krivulja temeljenih na broju 5 Wiles već pokazao da su modularne, a za drugu klasu nije mogao dokazati modularnost, Mazurova promjena *3-na-5* bila je posljednji trik koji je trebao iskoristiti. Još jednom, briljantna ideja drugog matematičara pomogla je Wilesu prevladati naizgled nepremostivu prepreku. Andrew Wiles sada je konačno bio gotov.

O modularnim formama, eliptičkim krivuljama i Galoisovim reprezentacijama

Umjesto da preda svoj dokaz stručnom matematičkom časopisu na recenziranje, odlučio je dokaz predstaviti u lipnju na konferenciji o Iwasawinoj teoriji u Cambridgeu. Ovakvoj odluci je u prilog išla činjenica da je Cambridge bio Wilesov rodni grad, mjesto gdje je prvi put čuo za Fermatov problem, tako da nije postojalo bolje mjesto na kojem bi ostvario dječački san i završio cijelu priču. Također, Wiles je želio izbjeći proces recenziranja jer se bojao da bi putem netko od čitača mogao odati dotad strogo čuvanu tajnu ili čak prisvojiti dokaz. Na konferenciji u Cambridgeu održao je tri predavanja pod naslovom *O modularnim formama, eliptičkim krivuljama i Galoisovim reprezentacijama*, ali s tipičnom skromnošću nije dao naslutiti kamo ona vode. Donio je preko 200 stranica formula i izvoda, izvornih misli izrečenih u obliku teorema popraćenih dugim, apstraktnim dokazima. Glasine su se širile kako je vrijeme odmicalo i s dvadesetak matematičara prisutnih na prvom predavanju, publika je do zadnjeg predavanja narasla toliko da je ispunila cijelu

[43] Peter Clive Sarnak , 1953. - , matematičar rođen u Južnoj Africi s dvojnom južnoafričkom i američkom nacionalnošću

prostoriju. Mnogi su čak, očekujući slavan završetak predavanja, nosili i kamere. Kako je Wiles na zadnjem predavanju raspisivao naizgled beskrajne formule na ploči, tako se napetost povećavala. Završavao je nekoliko zadnjih redaka dokaza zagonetne i kompliciranе Shimura - Taniyama pretpostavke za polustabilne eliptičke krivulje, kasnije nazvane *Teoremom o modularnosti*, a zatim je u posljednjoj rečenici, gotovo usputno, spomenuo da je ovime, kao izravna posljedica, dokazana višestoljetna Fermatova tvrdnja. Potom se okrenuo i sa skromnim smiješkom dodao "Mislim da ću ovdje stati."

U prostoriji je na trenutak zavladala tišina, a nakon toga ga je zapanjena publika nagradila gromoglasnim pljeskom, hvatajući kamerama trenutke koji su promijenili matematičku povijest. Za nekoliko minuta, vijest o rješavanju jednog od najslavnijih matematičkih problema proširila se cijelim svijetom, a tihi i samozatajni Andrew Wiles preko noći je postao svjetski poznato ime. Wilesov je dokaz, prema mnogima, bio najveći matematički rezultat dvadesetog stoljeća.

Povratak Iwasawinoj teoriji

Da bi priča bila dovršena, dokaz je trebalo recenzirati. Stoga je Wilesov rad poslan brojnim vodećim stručnjacima u teoriji brojeva. Jedan od njih bio je i Katz, koji je proveo dva mjeseca ne radeći ništa osim detaljnog proučavanja materijala. Nakon prijeđene polovice rada, Katz je naišao na problem u upotrebi Flachove tehnike. U dokazu nije postojao Eulerov sustav i bez njega nije bilo formule za broj klasa pomoću kojeg bi se pobrojale Galoisove reprezentacije eliptičkih krivulja u odnosu na modularne forme. Time ni Shimura - Taniyama pretpostavka ne bi vrijedila, pa ne bi bilo ni dokaza Posljednjeg Fermatovog teorema.

Shrvani i posramljeni Wiles ponovno se vratio u svoj ured na tavanu kako bi pokušao popraviti dokaz uz pomoć drugih kolega, uključujući svog bivšeg učenika Richarda Taylora[44], no čak ni nakon više od godinu dana rada, rješenje se nije naziralo. S obzirom na mnoge neuspjele dokaze Posljednjeg Fermatovog teorema koji su prethodili Wilesovoj objavi, sve su se više počele javljati sumnje u valjanost njegovog dokaza. Premda je Wiles izgubio svaku nadu i spremao se odustati od naizgled nerješivog problema, 19. rujna 1994. za svojim stolom u Princetonu, odlučio je posljednji put pogledati dokaz prije nego što sve odbaci. Ako će već odustati, želio je barem točno znati koja je tehnička činjenica dovela do propasti cijele stvari. Nakon dvadesetak minuta proučavanja papira, uočio je problem. *Bio je to najvažniji trenutak u mom cjelokupnom radnom vijeku*, kasnije je opisao. Wiles je shvatio da je pristup horizontalne Iwasawine teorije, koji je napustio tri godine ranije, upravo ono što bi popravilo grešku u Eulerovom sustavu. Sutradan je ispravio dokaz i sve je savršeno sjelo na svoje mjesto. Održao je obećanje svom prijatelju Tayloru, koji je došao kako bi mu pomogao ispraviti dokaz, te i njega u zahvalu potpisao u novom radu, bez obzira što je do

[44]Richard Lawrence Taylor, 1962. - , britanski matematičar

ideje došao nakon Taylorovog povratka kući. Wiles je ovoga puta koristio konvencionalni pristup predstavljanju matematičkih rezultata i predao rad stručnom časopisu na recenziranje. Pregledavanje je trajalo nekoliko mjeseci, ali ovog puta nisu pronađene pogreške. U svibnju 1995. godine, u časopisu *The Annals of Mathematics* objavljen je Wilesov originalni rad s Cambridgea zajedno s ispravkom Taylora i Wilesa. Andrew Wiles je konačno riješio problem koji je više od 350 godina mučio matematičare diljem svijeta.

Više pojedinosti vezanih za dokaz Posljednjeg Fermatovog teorema može se pronaći u [9] i [16].

5.5 Jednostavniji dokaz - realnost ili iluzija?

Wiles je opisao svoj dokaz kao dokaz dvadesetog stoljeća, jer je on bio postignuće velikog broja matematičara i ne bi bio ostvariv bez mnogih teorija razvijenih u prethodnim stoljećima. Fermat zasigurno ovaj dokaz nije mogao imati na umu kada je napisao svoju poznatu bilješku, no i dalje postoji mogućnost da je zamišljao neki drugi dokaz. Međutim, začuđujuća je činjenica da je živio još gotovo tri desetljeća nakon zapisivanja tvrdnje na margini Diofantove *Aritmetike* i nikada nije rekao ništa više o njoj.

Moguće je da je Fermat postao svjestan težine izrečene tvrdnje i shvatio da ne posjeduje dokaz ili je možda pogrešno mislio da se njegova metoda beskonačnog spusta, korištena u dokazivanju jednostavnog slučaja $n = 4$, može primijeniti na opće rješenje. S druge strane, možda je jednostavno zaboravio na teorem i nastavio raditi druge stvari ili je pak zapisao dokaz koji je s vremenom izgubljen. Treba razmotriti i mogućnost da je Fermat poznavao određene dijelove matematike koji su možda s vremenom izgubljeni.

Koju god mogućnost uzeli u obzir, dokazivanje teorema na način na koji je to konačno učinjeno 1990-ih, zahtijevalo je puno veću razinu znanja od one s kojom je Fermat raspolagao. Je li Fermat uistinu posjedovao dokaz teorema, onaj koji nije mogao stati na marginu knjige, zauvijek će ostati tajna.

Poglavlje 6

Posljednji Fermatov teorem u prstenu polinoma s kompleksnim koeficijentima

6.1 Fermatova jednadžba stupnja većeg od dva

Nakon što smo opisali složeni postupak dokazivanja Posljednjeg Fermatovog teorema u polju cijelih brojeva, još ćemo promotriti dokaz teorema u prstenu polinoma s kompleksnim koeficijentima, koji je već 1851. godine dokumentirao Liouville.

Želimo pokazati da za $p > 2$ ne postoji netrivijalno rješenje Fermatove jednadžbe

$$x^p + y^p = z^p, \tag{6.1}$$

pri čemu se pod terminom *netrivijalno* podrazumijeva da $(x(t), y(t), z(t))$ nije polinomni višekratnik rješenja jednadžbe (6.1) u skupu cijelih brojeva.

Propozicija 6.1.1. *Ne postoji netrivijalno rješenje $x(t)$, $y(t)$, $z(t) \in \mathbb{C}[t]$ jednadžbe*

$$(x(t))^p + (y(t))^p = (z(t))^p ,$$

pri čemu je $p \geq 3$.

Dokaz. Pretpostavimo suprotno, odnosno da za $p \geq 3$ postoji rješenje dane jednadžbe takvo da su x, y i z različiti od nul-polinoma. Možemo pretpostaviti da x, y i z nemaju zajedničkog djelitelja različitog od konstantnog polinoma 1. U suprotnom ih, bez smanjenja općenitosti, možemo podijeliti s njime. Također, pretpostavimo da su u parovima relativno prosti. Deriviranjem jednakosti (6.1) dobijemo

$$px^{p-1}x' + py^{p-1}y' = pz^{p-1}z'.$$

Nakon dijeljenja sa zajedničkim faktorom p, dolazimo do jednadžbe

$$x^{p-1}x' + y^{p-1}y' = z^{p-1}z'. \tag{6.2}$$

Ukoliko x^{p-1}, y^{p-1} i z^{p-1} promatramo kao varijable, vidimo da smo dobili dvije linearne jednadžbe (6.1) i (6.2), što nas potiče na korištenje linearne algebre za uklanjanje varijable. Najprije pomnožimo (6.1) s y' i (6.2) s y, a potom dobivene jednakosti oduzmemo i sredimo:

$$x^{p-1}(xy' - yx') + y^{p-1}\cancel{(yy' - yy')} = z^{p-1}(zy' - yz')$$
$$x^{p-1}(xy' - yx') = z^{p-1}(zy' - yz')$$

Iz zadnje jednakosti slijedi da x^{p-1} dijeli $z^{p-1}(zy' - yz')$. Međutim, budući da x i z po pretpostavci nemaju zajedničkih faktora, mora vrijediti da

$$x^{p-1} \text{ dijeli } zy' - yz'. \tag{6.3}$$

Ukoliko je $zy' - yz' = 0$, tada je $\frac{zy'-yz'}{z^2} = \left(\frac{y}{z}\right)' = 0$, što povlači da je $y = Cz$, za $C \in \mathbb{Z}$. Prema tome, y je konstantni višekratnik od z, što je kontradiktorno s pretpostavkom da su x i z relativno prosti. Dakle, mora vrijediti da je $zy' - yz' \neq 0$. Uzmimo sada stupnjeve polinoma u obzir i prisjetimo se da je stupanj derivacije polinoma jednak stupnju početnog polinoma umanjenom za jedan. Tvrdnja (6.3) stoga povlači

$$(p-1)\,\text{stupanj}(x) \leq \text{stupanj}(zy' - yz') \leq \text{stupanj}(zy') = \text{stupanj}(z) + \text{stupanj}(y) - 1.$$

Ukoliko dodamo stupanj(x) s obje strane nejednakosti, dolazimo do

$$(p-1)\,\text{stupanj}(x) + \text{stupanj}(x) \leq \text{stupanj}(x) + \text{stupanj}(y) + \text{stupanj}(z) - 1$$
$$p\,\text{stupanj}(x) < \text{stupanj}(x) + \text{stupanj}(y) + \text{stupanj}(z)$$

Desna strana gornje nejednakosti je simetrična s obzirom na x, y i z, dok je lijeva ovisna o polinomu x. Na sličan bismo način mogli doći do nejednakosti za y i z na lijevoj strani:

$$p\,\text{stupanj}(y) < \text{stupanj}(x) + \text{stupanj}(y) + \text{stupanj}(z),$$
$$p\,\text{stupanj}(z) < \text{stupanj}(x) + \text{stupanj}(y) + \text{stupanj}(z)$$

Zbrajanjem nejednakosti i dijeljenjem s izrazom (stupanj(x) + stupanj(y) + stupanj(z)), dolazimo do uvjeta

$$p < 3.$$

Došli smo do kontradikcije s pretpostavkom da je $p \geq 3$, čime je Posljednji Fermatov teorem dokazan za polinome s kompleksnim koeficijentima. □

6.2 Fermatova jednadžba prvog stupnja i *abc slutnja*

Ideja dokaza Posljednjeg Fermatovog teorema za polinome može se na zgodan način upotrijebiti za promatranje rješenja Fermatove jednadžbe prvog stupnja $a + b = c$.

Pretpostavimo da u prstenu $\mathbb{Z}[t]$ vrijedi

$$a + b = c, \tag{6.4}$$

pri čemu su a, b i c polinomi različiti od nul-polinoma. Također, bez smanjenja općenitosti možemo pretpostaviti da polinomi nemaju zajedničkih faktora (u protivnom ih podijelimo s njim) i pokušajmo koristiti postupak nalik onome u dokazu Propozicije 6.1.1. Ponajprije derivirajmo prethodnu jednadžbu da dobijemo

$$a' + b' = c'. \tag{6.5}$$

Potom, iskoristimo linearnu algebru i zapišimo koeficijente od (6.4) i (6.5) u matricu $\begin{pmatrix} a(t) & b(t) \\ a(t)' & b(t)' \end{pmatrix}$, te primijetimo da ćemo rješenja dobiti ukoliko determinanta matrice nije jednaka nula. Stoga, definirajmo

$$\Delta(t) = \begin{vmatrix} a(t) & b(t) \\ a(t)' & b(t)' \end{vmatrix} = a(t)b'(t) - a'(t)b(t). \tag{6.6}$$

Dodavanje prvog stupca drugom, i obratno, formirat će sljedeće determinante

$$\begin{vmatrix} a(t) & a(t)+b(t) \\ a(t)' & a(t)'+b(t)' \end{vmatrix} = \begin{vmatrix} a(t) & c(t) \\ a(t)' & c(t)' \end{vmatrix} \quad \text{i} \quad \begin{vmatrix} a(t)+b(t) & b(t) \\ a(t)'+b(t)' & b(t)' \end{vmatrix} = \begin{vmatrix} c(t) & b(t) \\ c(t)' & b(t)' \end{vmatrix} \tag{6.7}$$

Uočimo da uvjet $\Delta(t) = 0$ povlači $a(t) = \frac{a(t)'}{b(t)'}b(t)$, iz čega slijedi da je b skalarni višekratnik od a i čime smo dobili kontradikciju s pretpostavkom. Iz tog razloga mora vrijediti $\Delta(t) \neq 0$.

Nadalje, kako bi pronašli analogiju s tvrdnjom (6.3), želimo naći potenciju s kojom bi a, b i c dijelili determinantu $\Delta(t)$. Pretpostavimo da je α nultočka polinoma $a(t)$ i neka je $(t-\alpha)^e$ najveća potencija polinoma $(t-\alpha)$ koji dijeli $a(t)$, u oznaci $(t-\alpha)^e \mid a(t)$. Dakle, polinom $a(t)$ možemo zapisati kao

$$a(t) = U(t)\,(t-\alpha)^e\,,$$

pri čemu je $U(t)$ polinom koji nije djeljiv s $(t-\alpha)$. Deriviranjem prethodne jednadžbe dobijemo

$$a(t)' = (t-\alpha)^{e-1}\,V(t), \quad \text{za } V(t) = U(t)'(t-\alpha) + eU(t).$$

Budući da je prvi pribrojnik u izrazu za $V(t)$ djeljiv s $(t-\alpha)$ i $U(t)$ po definiciji nije djeljiv s $(t-\alpha)$, slijedi da je $(t-\alpha, V(t)) = (t-\alpha, eU(t)) = 1$, odnosno $(t-\alpha)^{e-1} \mid a(t)'$. Zapišimo sada determinantu u terminima funkcija $U(t)$ i $V(t)$:

$$\Delta(t) = a(t)b'(t) - a'(t)b(t) = U(t)\,(t-\alpha)^e\, b'(t) - (t-\alpha)^{e-1}\, V(t)b(t)$$

odnosno

$$\Delta(t) = (t-\alpha)^{e-1}\, W(t),$$

pri čemu je $W(t) = U(t)(t-\alpha)b'(t) - V(t)b(t)$. Kako $a(t)$ i $b(t)$ nemaju zajedničkih faktora, $t-\alpha$ ne dijeli $b(t)$. Budući da smo već pokazali da $t-\alpha$ ne dijeli $V(t)$, zaključujemo da mora vrijediti $(t-\alpha, W(t)) = (t-\alpha, V(t)b(t)) = 1$. Dakle, istinita je tvrdnja da

$$(t-\alpha)^{e-1} \mid \Delta(t),$$

iz čega slijedi da $(t-\alpha)^e$ dijeli $\Delta(t)(t-\alpha)$. Množenjem svih faktora $(t-\alpha)^e$ i korištenjem činjenice da su u parovima relativno prosti, dobijemo sljedeću tvrdnju:

$$\prod_{a(\alpha)=0} (t-\alpha)^e = a(t) \quad \text{dijeli} \quad \Delta(t) \prod_{a(\alpha)=0} (t-\alpha).$$

Uočimo da slične tvrdnje možemo dobiti i za $b(t)$ i $c(t)$. Budući da $a(t)$, $b(t)$ i $c(t)$ nemaju zajedničkih nultočaka, dobivene tvrdnje možemo kombinirati, iz čega proizlazi da

$$a(t)b(t)c(t) \quad \text{dijeli} \quad \Delta(t) \prod_{(abc)(\alpha)=0} (t-\alpha). \tag{6.8}$$

Zatim u obzir uzmimo stupnjeve polinoma, pritom se prisjetivši da je stupanj od $\prod_{(abc)(\alpha)=0} (t-\alpha)$ zapravo broj različitih nultočaka polinoma $a(t)b(t)c(t)$, u oznaci $\#\{\alpha \in \mathbb{C} : (abc)(\alpha) = 0\}$, te koristeći formulu $\text{stupanj}(abc) = \text{stupanj}(a) + \text{stupanj}(b) + \text{stupanj}(c)$. Dakle, promatranjem (6.8) slijedi:

$$\text{stupanj}(a) + \text{stupanj}(b) + \text{stupanj}(c) \leq \text{stupanj}(\Delta) + \#\{\alpha \in \mathbb{C} : (abc)(\alpha) = 0\}$$

Koristeći različite zapise $\Delta(t)$ dane u (6.6) i (6.7), mogu se formulirati nejednakosti:

$$\text{stupanj}(\Delta) \leq \begin{cases} \text{stupanj}(a) + \text{stupanj}(b) - 1 \\ \text{stupanj}(a) + \text{stupanj}(c) - 1 \\ \text{stupanj}(c) + \text{stupanj}(b) - 1 \end{cases}$$

Iz prethodnih nejednakosti sada slijedi

$$\text{stupanj}(a),\ \text{stupanj}(b),\ \text{stupanj}(c) < \#\{\alpha \in \mathbb{C} : (abc)(\alpha) = 0\}.$$

Ovime smo dobili tvrdnju koju možemo zapisati u obliku teorema:

Teorem 6.2.1 (*abc* teorem za polinome)**.** *Ukoliko polinomi $a(t)$, $b(t)$, $c(t) \in \mathbb{C}[t]$ nemaju zajedničkih nultočaka i daju netrivijalno rješenje jednadžbe $a(t) + b(t) = c(t)$, tada vrijedi*

$$max\{stupanj(a),\ stupanj(b),\ stupanj(c)\} < stupanj(rad(abc)),$$

pri čemu je $rad(abc)$ oznaka za umnožak svih različitih prostih faktora od $a(t)b(t)c(t)$.

Napomena 6.2.2. *Uočimo da je tvrdnja teorema ekvivalentna tvrdnji da je*

$$max\{stupanj(a),\ stupanj(b),\ stupanj(c)\} \leq stupanj(rad(abc)) - 1.$$

Abc teorem za polinome poznat je i pod nazivom *Mason–Stothers teorem* prema britanskim matematičarima Stothersu[1] i Masonu[2] koji su ga nezavisno jedan o drugome dokazali 1981. i 1984. godine. Inspirirani rezultatom za polinome, Masser[3] i Oesterlé[4] su 1985. godine formulirali *abc slutnju* za pozitivne cijele brojeve, koja glasi ovako:

Teorem 6.2.3 (abc slutnja)**.** *Za svaki $\epsilon > 0$ postoji konstanta $k_\epsilon > 0$ takva da za sve relativno proste cijele brojeve a, b, c koji zadovoljavaju $1 \leq a < b < c$, te $a + b = c$, vrijedi*

$$c < k_\epsilon\, rad(abc)^{1+\epsilon}.$$

Napomena 6.2.4. *Lako se pokaže da vrijedi sljedeća implikacija:*

Istinitost abc slutnje $\implies$ Posljednji Fermatov teorem istinit za dovoljno velike eksponente

Zaista, ukoliko su x, y, z su relativno prosti prirodni brojevi koji zadovoljavaju jednakost

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

tada uzmimo sljedeće vrijednosti u abc slutnji*:*

$$a = x^n,\ b = y^n,\ c = z^n.$$

Iako ne znamo točno odrediti umnožak prostih brojeva koji dijele $x^n y^n z^n$, znamo da su to točno prosti brojevi koji dijele xyz, pa tako i njihov umnožak mora biti manji ili jednak xyz. Štoviše, budući da su x i y pozitivni i oba su manja od z, mora vrijediti $xyz < z^3$, odnosno

$$rad(x^n y^n z^n) = \prod_{p | x^n y^n z^n} p = \prod_{p | xyz} p \leq xyz < z^3.$$

[1] Walter Wilson Stothers, 1946. - 2009., britanski matematičar
[2] Richard Clive Mason, britanski matematičar
[3] David William Masser, 1948. - , britanski matematičar
[4] Joseph Oesterlé, 1954. - , francuski matematičar

Koristeći abc slutnju*, za svaki* $\epsilon > 0$ *dobijemo*

$$z^n < k_\epsilon \, rad\,(x^n y^n z^n)^{1+\epsilon} \leq k_\epsilon \left(z^3\right)^{1+\epsilon},$$

odnosno

$$z^{n-3(1+\epsilon)} \leq k_\epsilon.$$

Ukoliko uvrstimo $\epsilon = \frac{1}{6}$ *i* $n > 3$ *takav da vrijedi* $n - 3(1+\epsilon) \geq \frac{n}{8}$*, dobijemo nejednakost*

$$z^n \leq k_{\frac{1}{6}}^8.$$

Time smo pokazali da u svakom rješenju Fermatove jednadžbe s $n > 3$*, brojevi* x^n*,* y^n *i* z^n *su svi manji od neke apsolutne granice. Drugim riječima, možemo pronaći* n_0 *takav da je Posljednji Fermatov teorem istinit za svaki* $n > n_0$*.*

Kad bismo imali eksplicitnu varijantu abc slutnje*, odnosno varijantu s danim vrijednostima* k_ϵ*, tada bismo mogli definirati jasnu granicu za sva rješenja Fermatove jednadžbe i utvrditi postoje li uopće rješenja koristeći tu granicu.*

Nažalost, *abc slutnja* i dalje nije dokazana, no njeno bi dokazivanje imalo izvanredan utjecaj na razumijevanje teorije brojeva. Više o njenim primjenama i brojnim rezultatima kojima je ekvivalentno proširenje može se pronaći u članku [8].

Poglavlje 7

Zaključak

Riječ *dokaz* može imati različito značenje u različitim područjima. Primjerice, u nekim disciplinama dokaz može označavati nekoliko različitih primjera koji opravdavaju izrečenu hipotezu, ali to je neprimjereno u matematici. Možemo imati tisuću primjera koji funkcioniraju kako je predviđeno hipotezom, ali tisuću i prvi bi joj mogao proturječiti. Stoga, da bi se dokazao teorem, potrebno je izgraditi nepobitni argument krenuvši od osnovnih principa, tako da izjava bude istinita u svakom slučaju, uz pretpostavku da su korišteni argumenti valjani.

U ovom su radu glavnu ulogu imala dva teorema sličnih iskaza, ali potpuno različitih smjerova dokazivanja. S jedne strane se nalazi Pitagorin teorem, koji je dokazan na više od 400 različitih načina, pri čemu su neki toliko jednostavni da ih razumiju i osnovnoškolci, dok su drugi nadasve kompliciran i potrebne su posebne matematičke vještine kako bi ih se shvatilo. Dok je s druge strane naizgled jednostavan Fermatov problem, poopćenje Pitagorina teorema, na čiji se zamršen dokaz, raspisan na približno dvjesto stranica teksta, čekalo gotovo četiri stoljeća. Iako se čini da im se dokazi u potpunosti razlikuju, ujedinjuje ih činjenica da se u njima iskoristila čitava širina matematike i njenih različitih grana. Pitagorin je teorem dokazan u mnogo različitih područja, uključujući algebru, geometriju i mnoge druge. Nalik tome, za dokaz Fermatovog problema bilo je potrebno iskoristiti i smisleno objediniti naizgled nepomirljive objekte u složenoj matematici, poput modularnih formi, eliptičkih krivulja, te Galoisovih reprezentacija pridruženih eliptičkim krivuljama.

Jedna od stvari po kojoj se navedeni teoremi razlikuju je njihova primjena. Posljednji Fermatov teorem je apstraktna tvrdnja bez jednostavne primjene u znanosti, pa čak i u svom vlastitom području - teoriji brojeva. Dok je za razliku od njega, primjena Pitagorina teorema utkana u svakodnevni život ljudi, od početaka civilizacije pa do današnjeg doba. Iako nosi Pitagorino ime, teorem koji povezuje duljine stranica pravokutnog trokuta korišten je u različite svrhe davno prije Pitagorina doba, primjerice na područjima Mezopotamije, Kine i Indije. Štoviše, čini se da ova 4000 godina stara priča o Pitagorinom teoremu

i njegovoj generaliziranoj verziji nema kraja, budući da se svake godine studenti, znanstvenici i amateri s matematičkim sklonostima hvataju s njim u koštac u pokušaju stvaranja novih, originalnih dokaza.

Upravo su pokušaji rješavanja ovih problema, ma koliko god oni bili nepotpuni ili neuspješni, nerijetko bili puno bitniji nego sam njihov iskaz ili dokaz. Zaista, pokušaji dokazivanja doveli su do razvoja nekih od najvažnijih grana moderne matematike. Kako je Wiles opisao:

The definition of a good mathematical problem is the mathematics it generates rather than the problem itself.

Povijest je puna slučajeva u kojima su matematičari pokušavajući riješiti jedan problem završili formuliranjem i dokazivanjem nečeg sasvim drugog. Tako je u 19. stoljeću Kummer smatrao da je pronašao dokaz Posljednjeg Fermatovog teorema, no Dirichlet mu je ukazao na grešku. U pokušaju da grešku ispravi, Kummer je razvio ideju o idealnim brojevima, koja je kasnije dovela Dedekinda do definicije ideala. Slično, rezultati koji su Wilesa doveli do konačnog rješenja Fermatovog problema pojavili su se u područjima za koje se isprva činilo da nemaju nikakve veze s njim. Poput babilonskog tornja koji je bio nadahnuće mnogim umjetnicima i stvarateljima unatoč tome što nikada nije dosegnuo željenu visinu neba, tako je i Posljednji Fermatov teorem kroz godine i godine neuspjelih pokušaja dokazivanja iznjedrio mnoštvo korisnih zaključaka.

Također, valja napomenuti da unatoč činjenici da je Wiles obavio važan završni rad na teoremu dokazujući oblik Shimura - Taniyama pretpostavke, cijeli poduhvat bio je zasluga mnogih njegovih suvremenika i prethodnika, velikih matematičara koji su možda javnosti manje poznati, ali su njihovi doprinosi jednako bitni jer su doveli do rješavanja cjelokupne slagalice. Primjerice, bez Kummerovog djela ne bi bilo teorije ideala, a bez ideala ne bi bilo Mazurovog djela. Bez Mazurovog djela ne bi bilo Freyeve pretpostavke, a bez Serreove teorije ne bi bilo Ribetovog dokaza da Shimura - Taniyama pretpostavka povlači Posljednji Fermatov teorem. I nijedan dokaz Fermatovog problema ne bi bio moguć bez pretpostavke koju je iznio Yutaka Taniyama 1955. godine, a zatim precizirao Goro Shimura.

Zajednički rad svih navedenih matematičara, ali i onih koji su svojim djelom pridonijeli rješavanju Posljednjeg Fermatovog teorema, a ostali nespomenuti, čisti je dokaz da se značajni rezultati ne ostvaruju preko noći. U potrazi za svojim snom, Wiles je proveo sedam godina života kao zatvorenik na vlastitom tavanu, a riječi kojima je završio trodnevno predavanje u Cambridgeu postale su metafora matematičkog uspjeha. Time je ohrabrio brojne matematičare da se uhvate u koštac s mnogim drugim neriješenim problemima. Njegova je veličina bila u tome što je imao vjere u svoje zamisli kada je gotovo svaki matematičar na svijetu mislio suprotno, da se Shimura - Taniyama pretpostavka ne može dokazati u dvadesetom stoljeću. Svoju sedmogodišnju potragu za dokazom matematičkog Svetog grala, kako mnogi nazivaju Posljednji Fermatov teorem, opisao je ovako:

Perhaps I could best describe my experience of doing mathematics in terms of entering a dark mansion. You go into the first room and it's dark, completely dark. You stumble around, bumping into the furniture. Gradually, you learn where each piece of furniture is. And finally, after six months or so, you find the light switch and turn it on. Suddenly, it's all illuminated and you can see exactly where you were. Then you enter the next dark room...

Iako je Andrew Wiles 1994. godine dovršio dugotrajno traganje za dokazom jedne od najintrigantnijih tvrdnji u matematičkoj povijesti, mnogi nadareni umovi današnjice pitaju se je li Wilesov dokaz uistinu jedini mogući dokaz ovog teorema ili postoji jednostavnija verzija koju tek treba otkriti. Vrijeme će pokazati je li Fermat stvarno bio u pravu i postoji li kratak, elementaran dokaz koji i dalje čeka svoje otkriće. Poučeni lekcijama o ponavljanju povijesti, moguće je da će i to otkriće doći potpuno nenadano, prilikom rada na nekom naizgled nepovezanom matematičkom problemu.

Bibliografija

[1] A. D. Aczel, *Fermat's Last Theorem*, Delta, 1997 (engleski).

[2] R. P. Agarwal, *Pythagorean theorem before and after Pythagoras*, Adv. Stud. Contemp. Math (2020), 357–389 (engleski).

[3] T. Andreescu, D. Andrica i I. Cucurezeanu, *An introduction to Diophantine equations: a problem-based approach*, Birkhäuser, 2010 (engleski).

[4] F. M. Brückler, *Povijest matematike*, Sveučilište u Zagrebu, 2022 (hrvatski).

[5] A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019 (hrvatski).

[6] H. M. Edwards, *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*, Springer Science & Business Media, 1996 (engleski).

[7] A. Granville, *Number Theory Revealed: A Masterclass*, American Mathematical Society, 2019 (engleski).

[8] A. Granville i T. Tucker, *It's as Easy as Abc*, Notices of the AMS **49** (2002), br. 10, 1224–1231 (engleski).

[9] Y. Hellegouarch, *Invitation to the Mathematics of Fermat - Wiles*, Academic Press, 2002 (engleski).

[10] A. Klobučar i A. Vidić, *Pitagora i Pitagorin poučak*, Poučak: časopis za metodiku i nastavu matematike (2015), 38–46 (engleski).

[11] E. S. Loomis, *The Pythagorean Proposition*, National Council of Teachers of Mathematics, 1968 (engleski).

[12] E. Maor, *The Pythagorean Theorem: A 4,000-Year History*, Princeton University Press, 2019 (engleski).

[13] F. Najman, *Eliptičke krivulje nad poljima algebarskih brojeva*, Sveučilište u Zagrebu, 2013 (hrvatski).

[14] B. Pavković i D. Veljan, *Elementarna matematika 2*, Školska knjiga, 1995 (hrvatski).

[15] B. Ratner, *Pythagoras: Everyone knows his famous theorem, but not who discovered it 1000 years before him*, Journal of Targeting, Measurement and Analysis for Marketing (2009), 229–242 (engleski).

[16] P. Ribenboim, *Fermat's Last Theorem for Amateurs*, Springer, 1999 (engleski).

[17] R. Sharifi, *Iwasawa Theory: a Climb Up the Tower*, sv. 66, Notices of the American Mathematical Society, 2019 (engleski).

[18] W. Sierpinski, *Pythagorean Triangles*, Yeshiva University, 1962 (engleski).

[19] I. Stewart i D. Tall, *Algebraic Number Theory and Fermat's Last Theorem*, AK Peters/CRC Press, 2001. (engleski).

Sažetak

Teorija brojeva, grana matematike koja proučava svojstva i međusobne odnose različitih vrsta brojeva, na prvu možda odaje dojam jedne od najjednostavnijih grana matematike. Međutim, ona sadrži mnoštvo jednostavno oblikovanih, ali teško dokazivih problema, od kojih neki ostaju nerazriješeni čak i stoljećima nakon svog izricanja. Posljednji Fermatov teorem primjer je ovakvog problema i glavna tema rada. Iako nema jednostavne primjene u znanosti, njegova važnost leži u tome što su pokušaji dokazivanja ovog, naizgled nerješivog problema doveli do razvoja nekih od najvažnijih grana moderne matematike. Također, njegov je dokaz ujedinio mnoštvo nadarenih matematičara i objedinio cijelu širinu matematike, čak i objekte koji su djelovali nepomirljivima. Svrha ovog rada je predstaviti povijesno-matematički tijek konstruiranja i dokazivanja Posljednjeg Fermatovog teorema, počevši od njegovih korijena u vidu Pitagorina teorema. Pitagorin teorem, čije se verzije javljaju u drevnim babilonskim, kineskim i indijskim zapisima, usko je vezan za Pitagorine trojke, koje se također obrađuju u ovom radu. Posljednji se dio bavi razmatranjem Posljednjeg Fermatovog teorema u prstenu polinoma s kompleksnim koeficijentima.

Summary

Number theory which is a branch of mathematics that studies the properties and relationships of different types of numbers, at first may seem like one of the simplest branches of mathematics. However, it contains a multitude of simply formulated yet problems that are difficult to prove, and some of them remain unsolved centuries after their formulation. Fermat's Last theorem is an example of this kind of problem and also the main topic of this thesis. Although it has no straightforward application in science, its importance lies in attempts to prove this seemingly unsolvable problem which has led to the development of some of the most important branches of modern mathematics. Nevertheless, its proof has united a multitude of gifted mathematicians and unified the entire breadth of mathematics, including objects that seemed irreconcilable. The purpose of this thesis is to present the genealogical historical-mathematical process of constructing and proving Fermat's Last Theorem, starting from its roots in the form of the Pythagorean theorem. The Pythagorean theorem, versions of which already had appeared in ancient Babylonian, Chinese and Indian records, is closely related to the Pythagorean triples, which are also discussed in this thesis. The last part analyzes Fermat's Last Theorem over the ring of polynomials with complex coefficients.

Životopis

Rođena sam 25. listopada 1996. godine u Slavonskom Brodu. Odrasla sam u Županji, gdje sam 2011. godine završila Osnovnu školu Mate Lovraka, te iste godine upisala Gimnaziju u Županji, opći smjer. Srednjoškolsko obrazovanje završavam 2015. godine. Nakon završetka srednje škole upisujem preddiplomski studij Matematike na Prirodoslovno-matematičkom fakultetu u Zagrebu. Studij završavam 2019. godine te potom upisujem diplomski studij Matematičke statistike i zapošljavam se kao student u EdTech tvrtki Photomath, kreatoru istoimene aplikacije za pomoć pri učenju matematike.