Slučajevi Fermatovog posljednjeg teorema dokazivi elementarnim metodama

Alković, Ivona

Master's thesis / Diplomski rad

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Split, University of Split, Faculty of science / Sveučilište u Splitu, Prirodoslovno-matematički fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:166:900813

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-06-29**

Repository / Repozitorij:

Repository of Faculty of Science

zir.nsk.hr

UNIVERSITY OF SPLIT

dabar

DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

PRIRODOSLOVNO–MATEMATIČKI FAKULTET
SVEUČILIŠTA U SPLITU

IVONA ALKOVIĆ

SLUČAJEVI FERMATOVOG POSLJEDNJEG TEOREMA DOKAZIVI ELEMENTARNIM METODAMA

DIPLOMSKI RAD

Split, listopad 2019.

PRIRODOSLOVNO–MATEMATIČKI FAKULTET
SVEUČILIŠTA U SPLITU

ODJEL ZA MATEMATIKU

SLUČAJEVI FERMATOVOG POSLJEDNJEG TEOREMA DOKAZIVI ELEMENTARNIM METODAMA

DIPLOMSKI RAD

Studentica:
Ivona Alković

Mentorica:
doc. dr. sc. Marija Bliznac Trebješanin

Split, listopad 2019.

Ovaj rad s ljubavlju posvećujem svojoj majci.

Hvala ti što si vjerovala u mene.

Uvod

Više od tri stoljeća Fermatov Posljednji teorem bio je jedan od najslavnijih neriješenih matematičkih problema. Teorem tvrdi da ne postoje tri prirodna broja x, y i z koji zadovoljavaju jednadžbu $x^n+y^n = z^n$ ako je n prirodni broj veći od 2. Dokaz, za koji je Pierre de Fermat (1601.–1665.) tvrdio da postoji, ali da je predugačak da ga ispiše na margini knjige *Aritmetika* Diofanta iz Aleksandrije, nikad nije nađen u njegovoj ostavštini. U ovom diplomskom radu predstavljeni su odabrani slučajevi Posljednjeg teorema dokazivi elementarnim metodama.

Prvo poglavlje ukratko predstavlja osnovne pojmove potrebne za razumijevanje problema te dokaz slučaja $n = 4$, kao i Fermatovu metodu beskonačnog spusta.

Drugo poglavlje bavi se slavnim matematičarem Leonhardom Eulerom i njegovim dokazom slučaja $n = 3$. U ovom poglavlju spomenut će se i nepotpunost Eulerovog dokaza te lema kojom je Harold Mortimer Edwards upotpunio dokaz.

Treće poglavlje posvećeno je francuskoj matematičarki Sophie Germain koja je živjela u vrijeme velikih predrasuda i koja je zaslužna za jedan od najznačajnijih napredaka u dokazivanju Fermatovog Posljednjeg teorema.

U zadnjem poglavlju govorit ćemo o slučajevima $n = 7$ i $n = 14$ te dati detaljan dokaz potonjeg slučaja.

Sadržaj

Uvod **iv**

Sadržaj **v**

1 Fermat **1**

1.1 Fermatov Posljednji teorem 1

1.2 Pitagorine trojke 2

1.3 Kako pronaći Pitagorine trojke 3

1.4 Metoda beskonačnog spusta 6

1.5 Slučaj $n = 4$ Posljednjeg teorema 8

1.6 Sume dvaju kvadrata i srodne teme 10

1.7 Savršeni brojevi i Fermatov teorem 14

2 Slučaj $n = 3$ **20**

2.1 Euler i slučaj $n = 3$ 20

2.2 Eulerov dokaz slučaja $n = 3$ 21

2.2.1 Prvi slučaj: Relativno prosti 23

2.2.2 Eulerova pogreška 25

2.2.3 Slučaj $3 \mid p$ 28

3 Slučaj $n = 5$ **30**

3.1 Uvod 30
3.2 Sophie Germain 31
3.2.1 "Veliki plan" 31

4 Slučajevi $n = 7$ i $n = 14$ **37**
4.1 Povijesni uvod 37
4.2 Ključni koraci dokaza 38
4.2.1 Djelitelji brojeva x, y i z. 38
4.2.2 Novi zapis jednadžbe 39
4.2.3 Traženje novih četrnaestih potencija 41
4.2.4 Operacije u prstenu $\mathbb{Z}[\sqrt{-7}]$ 41
4.2.5 Traženje novih četrnaestih potencija (nastavak) 42
4.2.6 Novi relativno prosti faktori 44
4.2.7 Ponovno provođenje dokaza 46
4.3 Sažetak 47

Literatura **49**

Poglavlje 1

Fermat

1.1 Fermatov Posljednji teorem

Teorem 1.1 (Fermat) *Jednadžba* $x^n + y^n = z^n$, $n \in \mathbf{N}$, $n > 2$ *nema rješenja u skupu prirodnih brojeva.*

Izvorna tvrdnja na latinskom jeziku, koju je Fermat napisao na marginama Diofantove Aritmetike, glasila je "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." Što u prijevodu znači "Nemoguće je razdvojiti kub na dva kuba, bikvadrat na dva bikvadrata ili, općenito, bilo koju potenciju veću od druge, na dvije potencije istog stupnja".

Dokaz ove matematičke slutnje, varljivo lake za izreći, izmicao je matematičarima više od tri stotine i pedeset godina. Naposljetku, 1995. godine, Andrew Wiles objavio je dokaz pretpostavke za koju se ranije pokazalo da implicira Fermatov Posljednji teorem.

Tvrdnja Fermatovog Posljednjeg teorema često je podijeljena u dva slučaja: Slučaj I vrijedi za eksponent n za koji ne postoje cijeli brojevi x, y i z takvi

da $n \nmid xyz$ i $x^n + y^n = z^n$.

Slučaj II vrijedi za eksponent n za koji ne postoje cijeli brojevi x, y i z, svi različiti od 0, takvi da $n \mid xyz$, $gcd(x, y, z) = 1$ i $x^n + y^n = z^n$.

1.2 Pitagorine trojke

Pravokutni trokut čije su duljine stranica prirodni brojevi nazivamo Pitagorin trokut. Uređenu trojku prirodnih brojeva (x, y, z) zovemo Pitagorina trojka ako su x i y katete, a z hipotenuza nekog Pitagorinog trokuta, tj. ako vrijedi:

$$x^2 + y^2 = z^2. \tag{1.1}$$

Ukoliko su pritom brojevi x, y i z relativno prosti, onda kažemo da je (x, y, z) primitivna Pitagorina trojka. Rješenje diofantske jednadžbe (1.1) svodi se na problem traženja prirodnih brojeva koji zadovoljavaju jednadžbu $x^2+y^2 = z^2$.

Kada je problem postavljen u ovom obliku, njegova veza s Pitagorinim teoremom postaje očita. Jednadžba $3^2 + 4^2 = 5^2$ implicira, po Pitagorinom teoremu, da je trokut kojemu su stranice u omjeru $3 : 4 : 5$ pravokutan trokut. Općenito, bilo koja trojka prirodnih brojeva (x, y, z) koja zadovoljava $x^2 + y^2 = z^2$ određuje skup omjera $x : y : z$ takav da je trokut čije su stranice u tom omjeru zapravo pravokutan trokut.

Pitagorina trojka $3^2 + 4^2 = 5^2$ je najjednostavniji i najpoznatiji primjer. Drugi je primjer $5^2 + 12^2 = 13^2$. Očigledno je u ovim primjerima da je jedino bitan omjer te da je trojka 6, 8, 10, koja ima isti omjer kao 3, 4, 5, također Pitagorina trojka.

1.3 Kako pronaći Pitagorine trojke

Metoda rješavanja koja slijedi je, u klasičnoj grčkoj matematici, bila poznata kao analitička metoda: pretpostavlja se na početku da je dano rješenje jednadžbe $x^2+y^2 = z^2$ (x, y, z su prirodni brojevi). Svojstva danog rješenja analizirana su kako bi se pronašle njihove karakteristike te kako bi se omogućila konstrukciju takvih rješenja.

Primijetimo najprije sljedeće: ako je d neki broj koji dijeli sva tri broja x, y i z, onda se d^2 može ukloniti iz jednadžbe $x^2 + y^2 = z^2$, a brojevi x/d, y/d, z/d i dalje će tvoriti Pitagorinu trojku. Ako je d najveći zajednički djelitelj brojeva x, y, z onda x/d, y/d, z/d nemaju zajedničkog djelitelja osim 1 i tvore trojku koju nazivamo primitivna Pitagorina trojka. Na ovaj se način svaka Pitagorina trojka može reducirati, dijeleći jednadžbu s najvećim zajedničkim djeliteljem, na primitivnu Pitagorinu trojku. Prema tome, bit će dovoljno moći konstruirati primitivnu Pitagorinu trojku te se može na početku pretpostaviti da je dana trojka (x, y, z) primitivna.

Lema 1.2 (Pitagorine trojke) *Za bilo koje prirodne brojeve x, y i z koji su relativno prosti i zadovoljavaju $x^2 + y^2 = z^2$, možemo pronaći prirodne brojeve p i q takve da je*

$$x = 2pq$$
$$y = p^2 - q^2$$
$$z = p^2 + q^2$$

gdje su p i q relativno prosti, različitih parnosti i vrijedi $p > q > 0$. Vrijednosti x i y su međusobno zamjenjive.

Dokaz. Bez smanjena općenitosti, dokaz ćemo provesti za primitivne Pitagorine trojke. Jednom kada nađemo rješenja za primitivne Pitagorine trojke,

možemo ih koristiti za pronalazak ostalih Pitagorinih trojki. Budući da je naša Pitagorina trojka primitivna, dva od tri broja x, y, z ne mogu biti parna (jer bi 2 bio zajednički djelitelj). Dakle, barem su dva neparna. Očito sva tri ne mogu biti neparna jer bi onda iz jednadžbe $x^2 + y^2 = z^2$ slijedilo da je suma dva neparna broja neparna, što je nemoguće. Dakle, točno je jedan od tih brojeva paran. Sada želimo pokazati da je z neparan, a x i y različitih parnosti.

Ako je z paran, može se zapisati kao $2n$, za neki prirodni broj n. Tada su x i y neparni i mogu se zapisati u obliku $2n_1 + 1$ i $2n_2 + 1$ za neke druge prirodne brojeve n_1 i n_2. Koristeći modularnu aritmetiku vidimo da je $x^2 = 4n^2 + 4n + 1 \equiv 1 \pmod 4$ i $z^2 = 4n^2 \equiv 0 \pmod 4$. Ako je $x^2 + y^2 = z^2$ i z paran onda bi to impliciralo da je $1 + 1 \equiv 0 \pmod 4$. Ova kontradikcija pokazuje da je z neparan. Pretpostavimo da je y drugi neparan broj; ako nije, zamijenimo ga s x.

Napišimo sada jednadžbu $x^2 + y^2 = z^2$ kao $x^2 = z^2 - y^2$. Faktorizacijom dobijemo $x^2 = (z-y)(z+y)$ i primijetimo da su x, $z-y$ i $z+y$ parni brojevi. Budući da su svi parni, možemo pronaći prirodne brojeve u, v, w takve da je $x = 2u$, $z + y = 2v$ i $z - y = 2w$. Uvrštavanjem ovih novih vrijednosti u jednadžbu $x^2 = (z - y)(z + y)$ dobije se $(2u)^2 = (2v)(2w)$ odnosno $u^2 = vw$. Vidimo da su v i w relativno prosti jer bi inače njihov djelitelj dijelio $v + w = \frac{1}{2}(z+y) + \frac{1}{2}(z-y) = \frac{1}{2}2z = z$ i $u - w = \frac{1}{2}(z+y)\frac{1}{2}(z-y) = y$. Kako su z i y relativno prosti, znamo da su v i w također relativno prosti, a kako je $vw = u^2$, v i w moraju biti kvadrati jer su relativno prosti. Ovo implicira da postoje cijeli brojevi p i q takvi da je

$$z = v + w = p^2 + q^2$$

$$y = v - w = p^2 - q^2$$

Činjenica da je y prirodan broj implicira da je p veći od q. Kako su z i

y neparni, p i q moraju biti različitih parnosti. Možemo koristiti jednakost $x^2 = z^2 - y^2$ kako bismo pronašli x u terminima p i q.

$$\begin{aligned} x^2 = z^2 - y^2 &= p^4 + 2p^2q^2 + q^4 - p^4 + 2p^2q^2 - q^4 \\ &= 4p^2q^2 \\ &= (2pq)^2 \\ x &= 2pq \end{aligned}$$

Pokazali smo da za bilo koje primitivne Pitagorine trojke za koje je x paran, uvijek možemo pronaći vrijednosti p i q koje zadovoljavaju ove jednadžbe.

Analizu Pitagorinih trojki završavamo pokazujući da za bilo koje p i q takve da su p i q relativno prosti, različitih parnosti i za koje vrijedi $p > q$ brojevi $2pq$, $p^2 - q^2$ i $p^2 + q^2$ čine primitivnu Pitagorinu trojku. Lako je provjeriti da se u jednadžbi

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

nakon množenja i pojednostavljivanja, izrazi koji sadrže $2pq$ poništе. Sada je preostalo samo još pokazati da je to primitivna Pitagorina trojka. Koristit ćemo činjenicu da su p i q relativno prosti kako bismo pokazali da su $2pq$ i $p^2 - q^2$ također relativno prosti. Pretpostavimo suprotno, tj. da d dijeli $2pq$ i $p^2 - q^2$. Kako je $p^2 - q^2$ neparan broj, zajednički djelitelj nije paran. Prema tome, d mora dijeliti p ili q, ali ne oba. Ako $d|p^2 - q^2$ i $d|p^2$ znamo da $d|q^2$. Ovo je kontradikcija s pretpostavkom da p i q nemaju zajedničkog djelitelja većeg od 1. ■

Lema 1.2 u potpunosti rješava problem konstruiranja Pitagorinih trojki. Pitagorine trojke koje odgovaraju parovima p i q za koje je $p \leq 8$ dane su u Tablici 1.1. Primijetimo da ova tablica uključuje standardne primjere

$(3, 4, 5)$, $(5, 12, 13)$ i $(7, 24, 25)$. Primijetimo također da je vrlo jednostavno tablicu proširiti na veće vrijednosti broja p, uključujući samo one vrijednosti q manje od p koje su relativno proste s p i različite parnosti.

Tablica 1.1: Pitagorine trojke

p	q	x	y	z
2	1	4	3	5
3	2	12	5	13
4	1	8	15	17
4	3	24	7	25
5	2	20	21	29
5	4	40	9	41
6	1	12	35	37
6	5	60	11	61
7	2	28	45	53
7	4	56	33	65
7	6	84	13	85
8	1	16	63	65
8	3	48	55	73
8	5	80	39	89
8	7	112	15	113

1.4 Metoda beskonačnog spusta

Fermat je osmislio metodu beskonačnog spusta, te naveo da svi njegovi dokazi koriste ovu metodu. Ukratko rečeno, metoda dokazuje da su određena svojstva i relacije nemoguće za prirodne brojeve. Ideja je pokazati da ako ta svojstva vrijede za neke brojeve, vrijedit će i za neke manje brojeve; tada, po istoj tvrdnji, vrijedit će i za još manje brojeve, i tako dalje *ad infinitum*[1], što je nemoguće jer niz prirodnih brojeva ne može opadati beskonačno.

Naprimjer, promotrimo tvrdnju koja je korištena u prethodnom odjeljku; *ako su v i w relativno prosti i ako je vw kvadrat, tada v i w oba moraju*

[1]ad infinitum - do beskonačnosti

biti kvadrati. Kako je Fermat sam naglasio, metoda beskonačnog spusta je metoda za opovrgavanje tvrdnji. U ovom slučaju, ono što treba pokazati jest da je nemoguće da postoje brojevi v i w takvi da su (1) v i w relativno prosti, (2) vw je kvadrat, i (3) v i w nisu oba kvadrati.

Pretpostavimo da takvi v i w postoje. Zamjenom v i w ukoliko je potrebno, može se pretpostaviti da v nije kvadrat nekog broja. Posebno, v nije 1. Dakle, v je djeljiv s barem jednim prostim brojem. Neka je P prost broj koji dijeli v, recimo $v = Pk$. Tada P također dijeli vw koji je kvadrat, recimo $vw = u^2$. Prema osnovnom svojstvu prostih brojeva, ako P dijeli $u \cdot u$ onda P mora dijeliti u ili u, tj. P mora dijeliti u, recimo $u = Pm$. Tada se $uw = u^2$ može zapisati kao $Pkw = (Pm)^2 = P^2m^2$ što implicira $kw = Pm^2$. Kako P dijeli desnu stranu jednakosti, mora dijeliti i lijevu. Stoga, P mora dijeliti ili k ili w. Međutim, P ne dijeli w zato što dijeli v, a v i w su relativno prosti. Dakle, P dijeli k, recimo $k = Pv'$. Tada $kw = Pm^2$ postaje $Pv'w = Pm^2$ što daje $v'w = m^2$. Kako je $v = Pk = P^2v'$, bilo koji djelitelj od v' je ujedno i djelitelj od v pa v' i w nemaju zajedničkog djelitelja većeg od 1. Štoviše, ako je v' kvadrat tada bi $v = P^2v'$ također bio kvadrat, što nije. Dakle, v' nije kvadrat. Prema tome, brojevi v' i w imaju svojstva (1), (2), (3) nabrojana prethodno i $v' < v$. Isti argument se može iskoristiti za pokazati da postoji drugi prirodni broj $v'' < v$ takav da v'' i w imaju ista tri svojstva. Uzastopno ponavljanje ovog argumenta dalo bi niz prirodnih brojeva $v > v' > v'' > v''' > \ldots$ koji je beskonačno strogo silazni. Kako je ovo nemoguće (broj v je gornja granica broja puta koliko se može smanjiti), nemoguće je da dva broja v i w imaju navedena svojstva. Ovo dokazuje tvrdnju.

Ukratko, metoda beskonačnog spusta temelji se na sljedećem principu: *Neka pretpostavka da dani prirodni broj koji ima dani skup svojstava impli-*

cira da postoji manji prirodni broj s istim skupom svojstava. Tada nijedan prirodni broj ne može imati ovaj skup svojstava.

1.5 Slučaj $n = 4$ Posljednjeg teorema

Teorem 1.3 (Slučaj $n = 4$) *Ne postoje rješenja jednadžbe*

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

u skupu prirodnih brojeva.

Dokaz. Kako bismo dokazali slučaj $n = 4$ Fermatovog Posljednjeg teorema, dovoljno je kombinirati metodu beskonačnog spusta i metodu generiranja Pitagorinih trojki.

Pretpostavimo da su x, y i z takvi da vrijedi $x^4 + y^4 = z^4$. Kao u slučaju Pitagorinih trojki, možemo pretpostaviti da su x, y i z relativno prosti, odnosno, da nemaju zajedničkog djelitelja većeg od 1. Stoga su x^2, y^2 i z^2 primitivne Pitagorine trojke i možemo pisati

$$x^2 = 2pq$$
$$y^2 = p^2 - q^2$$
$$z^2 = p^2 + q^2$$

gdje su p i q relativno prosti, različitih parnosti i vrijedi $p > q > 0$. Druga od ove tri jednadžbe može se zapisati kao $y^2 + q^2 = p^2$ i slijedi, budući da su p i q relativno prosti, da su y, q i p primitivne Pitagorine trojke. Dakle, p je neparan, a kako su p i q različitih parnosti, q je paran. Stoga,

$$q = 2ab$$
$$y = a^2 - b^2$$
$$p = a^2 + b^2$$

gdje su a i b relativno prosti, različitih parnosti i vrijedi $a > b > 0$. Prema tome,

$$x^2 = 2pq = 4ab(a^2 + b^2).$$

Ovo pokazuje da je $ab(a^2 + b^2)$ kvadrat, odnosno, kvadrat polovine parnog broja x. Međutim, ab i a^2+b^2 su relativno prosti zato što bilo koji prosti broj P koji dijeli ab dijeli a ili b, ali ne i oba (jer su a i b relativno prosti) i stoga ne može dijeliti $a^2 + b^2$. Dakle, ab i $a^2 + b^2$ moraju biti kvadrati nekih prirodnih brojeva. Međutim, kako je ab kvadrat i kako su a i b relativno prosti, a i b oba moraju biti kvadrati. Zapišimo $a = X^2$, $b = Y^2$. Nadalje, $X^4+Y^4 = a^2+b^2$ je kvadrat. Ako su x i y prirodni brojevi takvi da je $x^4 + y^4$ kvadrat, tada prethodni niz koraka daje novi par prirodnih brojeva X i Y takvih da je X^4+Y^4 kvadrat. Štoviše, vrijedi $X^4+Y^4 = a^2+b^2 = p < p^2+q^2 = z^2 < z^4 = x^4+y^4$. Ovime je uspostavljena metoda beskonačnog spusta prirodnih brojeva, što je nemoguće. Dakle, suma dva broja četvrte potencije ne može biti kvadrat nekog broja pa ni četvrta potencija nekog broja. Ovo dokazuje Fermatov Posljednji teorem za slučaj kada je $n = 4$. ■

Očito slijedi da $x^{4m} + y^{4m} = z^{4m}$ nema rješenja kad god je m prirodan broj jer bi inače $X = x^m$, $Y = y^m$, $Z = z^m$ bilo rješenje jednadžbe $X^4+Y^4 = Z^4$. Prema tomu, Fermatov Posljednji teorem je istinit za sve eksponente n djeljive s 4. Eksponent $n > 2$ koji nije djeljiv s 4 nije potencija broja 2 i stoga mora biti djeljiv s nekim prostim brojem $p \neq 2$, recimo $n = pm$. Kako bi se pokazalo da $x^n + y^n = z^n$ nema rješenje u skupu prirodnih brojeva, očito je dovoljno pokazati da $x^p + y^p = z^p$ nema rješenje. Dakle, jednom kada je Fermatov Posljednji teorem bio dokazan za slučaj $n = 4$, dokaz općeg slučaja se reducirao na dokaz slučaja kada je $n > 2$ prost broj. Zbog te činjenice, u ostatku ovog rada razmatrat će se samo slučajevi Fermatovog Posljednjeg

teorema u kojima je n prost, $n \neq 2$.

1.6 Sume dvaju kvadrata i srodne teme

Jedna od prvih tema u teoriji brojeva koju je Fermat proučavao, i ona koja ga je dovela do mnogih drugih važnih pitanja, bio je problem reprezentacije brojeva kao zbroja dvaju kvadrata. Kao i u mnogim drugim slučajevima, Fermatovo zanimanje za ovu temu potjecalo je od Diofantove [2] *Aritmetike* [3].

Najmanje su tri odlomka navedene knjige povezana s reprezentacijom brojeva kao sumom dvaju kvadrata što pokazuje da je Diofantovo znanje o toj temi bilo znatno. U svojoj knjizi Diofant iznosi da se broj 65 može zapisati na dva načina kao suma dvaju kvadrata $65 = 1^2 + 8^2 = 4^2 + 7^2$ i govori da je to "zbog činjenice da je 65 produkt brojeva 13 i 5, od kojih je svaki od brojeva zbroj dva kvadrata." Na drugom mjestu iznosi što je nužan uvjet da bi broj bio reprezentiran kao suma dvaju kvadrata i konačno, primjećuje da 15 nije zbroj dva (racionalna) kvadrata.

Osnovna činjenica u proučavanju brojeva koji su suma dvaju kvadrata jest jednakost

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

koja pokazuje da ako su dva broja sume dvaju kvadrata onda je njihov produkt također zbroj dvaju kvadrata. Također, Diofant pokazuje se da se $65 = 5 \cdot 13$ može zapisati na dva načina kao suma dvaju kvadrata.

$$65 = 5 \cdot 13 = (2^2 + 1^2)(3^2 + 2^2) = (2 \cdot 3 - 1 \cdot 2)^2 + (2 \cdot 2 + 1 \cdot 3)^2 = 4^2 + 7^2$$

$$65 = 5 \cdot 13 = (2^2 + 1^2)(2^2 + 3^2) = (2 \cdot 2 - 1 \cdot 3)^2 + (2 \cdot 3 + 1 \cdot 2)^2 = 1^2 + 8^2$$

[2] Diofant iz Aleksandrije (oko 250. god) - starogrčki matematičar

[3] Aritmetika - najstariji sistematski traktat o algebri

Fermat nije bio prvi koji je pokušao razjasniti Diofantove odlomke o sumama dvaju kvadrata. Drugi koji je pokušao bio je Francois Viète (1540.–1603.), jedan od začetnika moderne algebre. Treći je bio Albert Girard (1595.–1632.) koji je uspio dati nužne i dovoljne uvjete da bi broj bio reprezentiran kao suma dvaju kvadrata i to nekoliko godina prije Fermatovih najranijih zapisa o toj temi. Girard je uključio $0^2 = 0$ kao kvadrat, i njegovi su uvjeti bili da se broj može zapisati kao suma dvaju kvadrata ako i samo ako je (1) kvadrat ili (2) prost broj koji je za jedan veći od višekratnika broja 4 ili (3) broj 2 ili (4) bilo koji produkt takvih brojeva. Međutim, nikada nije tvrdio da je dokazao da su njegovi uvjeti nužni i dovoljni.

Fermat, s druge strane, jest tvrdio da može dokazati nužnost i dovoljnost Girardovih uvjeta [4]. Teži dio ove tvrdnje jest pokazati da su uvjeti dovoljni. Kako je kvadrat a^2 trivijalno zbroj dva kvadrata a^2+0^2, kako je $2 = 1^2+1^2$ te kako jednakost (1.2) pokazuje da je produkt suma dvaju kvadrata i sam suma dvaju kvadrata, ovo pridonosi dokazu da se *svaki prost broj oblika* $4n+1$ *može zapisati kao suma dvaju kvadrata*. Fermat je iznio ovu tvrdnju mnogo puta te je tvrdio da ju može i dokazati, iako, nije poznato da je ikada napisao dokaz. Fermat je također otišao dalje od Girarda navodeći kako može dokazati da postoji samo jedna reprezentacija prostog broja kao sume dvaju kvadrata te da ima općenitu metodu traženja takvih reprezentacija bez korištenja metode pokušaja i pogreške.

Nužnost Girardovih uvjeta može se preformulirati u tvrdnju *ako je rezultat dijeljenja broja s najvećim kvadratom kojeg sadrži djeljiv s prostim brojem oblika* $4n+3$ *onda se taj broj ne može zapisati kao suma dvaju kvadrata*. Ovo je također jedan od Fermatovih teorema.

[4] Ne postoji dokaz da je Fermat bio upoznat s Girardovim radom. Izložio je uvjete neovisno i na malo drukčiji način.

Drugi problem kojim se Fermat detaljno bavio bio je pronalazak broja reprezentacija danog broja kao sume dvaju kvadrata. Ovaj problem nije od velike važnosti za ovaj rad pa se u daljnjem tekstu neće razmatrati.

Fermat je otkrio da se pravila slična onima koja vrijede za broj prikazan u obliku sume dvaju kvadrata mogu, također, primijeniti na broj prikazan u obliku $x^2 + 2y^2$ ili $x^2 + 3y^2$. Reprezentacija oblika $x^2 + 2y^2$ neće biti od nikakve važnosti za Fermatov Posljednji teorem, međutim, ona oblika x^2+3y^2 igra veliku ulogu u proučavanju teorema - posebno u Eulerovom[5] dokazu za slučaj $n = 3$. Tablica 1.2 pokazuje sve brojeve oblika $x^2 + 3y^2$ manje od 169. Proučavanjem tablice možemo naslutiti da vrijedi tvrdnja da *broj može biti prikazan u obliku* $x^2 + 3y^2$ *ako i samo ako je (1) kvadrat ili (2) prost broj ovakvog oblika ili (3) produkt takvih brojeva.* Štoviše, proučavanjem prostih brojeva danih u tablici možemo pretpostaviti i da se, osim prostih brojeva oblika $3 = 0^2+3\cdot 1^2$, što je poseban slučaj, prosti brojevi međusobno razlikuju za višekratnik broja 6 i svi su oni za jedan veći od višekratnika broja 6.

Tablica 1.2: Svi brojevi manji od 169 koji se mogu zapisati u obliku x^2+3y^2.

y\x	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	1	4	9	16	25	36	49	64	81	100	121	144
1	3	4	7	12	19	28	39	52	67	84	103	124	147
2	12	13	16	21	28	37	48	61	76	93	112	133	156
3	27	28	31	36	43	52	63	76	91	108	127	148	
4	48	49	52	57	64	73	84	97	112	129	148		
5	75	76	79	84	91	100	111	124	139	156			
6	108	109	112	117	124	133	144	157					
7	147	148	151	156	163								

Prirodno je sada formulirati slutnju da se *prost broj različit od* 3 *može prikazati u obliku* $x^2 + 3y^2$ *ako i samo ako je taj broj oblika* $6n + 1$. Naime,

[5]Leonhard Euler (1707. - 1783.) - švicarski matematičar, fizičar i astronom

lako je dokazati smjer nužnosti. Po uzoru na jednakost (1.2) promatramo jednakost

$$(a^2 + 3b^2)(c^2 + 3d^2) = (ac - 3bd)^2 + 3(ad + bc)^2$$

te se lako provjeri da iz nje slijedi smjer dovoljnosti. Štoviše, svaki je prost broj različit od 3 oblika $3n+1$ ili $3n+2$, a oni oblika $3n+1$ moraju biti oblika $6n + 1$, zato što ako je n neparan, međutim, $3n + 1$ je paran te zbog toga nije prost. Ova zapažanja reduciraju dva prethodno dana teorema na tvrdnje; *ako broj podijeljen sa najvećim kvadratom kojeg sadrži ima prosti faktor oblika* $3n+2$ *tada taj broj nije oblika* x^2+3y^2 i *svaki se prost broj oblika* $3n+1$ *može zapisati kao* $x^2 + 3y^2$. Kako je reprezentacija u obliku $x^2 + 4y^2$ uključena u reprezentaciju kao zbroj dva kvadrata, sljedeći slučaj kojeg razmatramo nije x^2+4y^2 nego x^2+5y^2. Tablica 1.3 prikazuje sve brojeve manje od 100 koji su oblika x^2+5y^2. Primijetimo da se broj 21 pojavljuje dva puta, kao $1^2+5\cdot 2^2$ i kao $4^2+5\cdot 1^2$, ali se njegovi prosti faktori 3 i 7 ne pojavljuju. Vidimo da ne možemo izvesti zaključke kao u prethodnom slučaju. Iz Fermatovih bilješki o brojevima oblika $x^2 + 5y^2$ možemo primijetiti da je shvatio da se ovaj slučaj razlikuje od ostalih. Pretpostavio je da ako su dva prosta broja p_1 i p_2 oba oblika $4n+3$ i ako oba imaju 3 ili 7 kao zadnju znamenku tada je p_1p_2 oblika $x^2 + 5y^2$. (Prosti brojevi 3, 7, 23, 43, 47, 67, ... su kongruentni 3 modulo 4 i završavaju na 3 ili 7. Pretpostavka je da je produkt bilo koja dva takva broja oblika $x^2 + 5y^2$. Naprimjer, $3 \cdot 3 = 2^2 + 5 \cdot 1^2, 3 \cdot 7 = 4^2 + 5 \cdot 1^2, 7 \cdot 7 = 2^2 + 5 \cdot 3^2, 3 \cdot 23 = 8^2 + 5 \cdot 1^2, 3 \cdot 43 = 2^2 + 5 \cdot 5^2, 7 \cdot 23 = 9^2 + 5 \cdot 4^2, itd.$) Ova pretpostavka ne samo da je točna, nego je središnja činjenica o brojevima oblika $x^2 + 5y^2$. Ovo je još jedan primjer koji govori o veličini Fermata kao teoretičara brojeva.

Tablica 1.3: Svi brojevi manji od 100 koji se mogu zapisati u obliku $x^2 + 5y^2$

y\x	0	1	2	3	4	5	6	7	8	9
0	0	1	4	9	16	25	36	49	64	81
1	5	6	9	14	21	30	41	54	69	86
2	20	21	24	29	36	45	56	69	84	
3	45	46	49	54	61	70	81	94		
4	80	81	84	89	96					

1.7 Savršeni brojevi i Fermatov teorem

Proučavanje "savršenih brojeva" seže još u prapovijest teorije brojeva, sve do njegovih korijena u misticizmu i numerologiji.

Definicija 1.4 (Savršeni broj) *Savršeni broj je prirodni broj jednak zbroju svojih pravih djelitelja* [6].

Primjer savršenog broja je broj 6 jer je $6 = 1 + 2 + 3$.

Euklid [7] je u *Elementima* [8] dokazao da ako je $1+2+4+\ldots+2^{n-1} = 2^n-1$ prost broj, onda je broj $2^{n-1} \times (2^n - 1)$ savršen. Naprimjer, $3 = 1 + 2$ je prost pa je $2 \cdot 3 = 6$ savršen, i $7 = 1 + 2 + 4$ je prost pa je $2^2 \cdot 7 = 28$ savršen. U modernoj je notaciji ovo vrlo jednostavno dokazivo. Primijetimo da ako je broj $p = 2^n - 1$ prost onda su odgovarajući djelitelji broja $2^{n-1}p$ $1, 2, 3, \ldots, 2^{n-1}, p, 2p, 4p, \ldots, 2^{n-2}p$, i suma ovih djelitelja je $1 + 2 + 3 + \ldots + 2^{n-1} + p(1 + 2 + 4 + \ldots + 2^{n-2}) = p + p(2^{n-1} - 1) = 2^{n-1}p$ što je i trebalo pokazati. Euklidov je uvjet dovoljan uvjet da bi broj bio savršen. Do sada nisu poznati drukčiji primjeri savršenih brojeva. Descartes je naveo, a Euler dokazao, da je savršeni broj u Euklidovom obliku ako i samo ako je paran. Postojanje neparnog savršenog broja je poznati neriješeni problem.

[6] pravi djelitelj - djelitelj prirodnoga broja različit od njega samoga

[7] Euklid (330. p.n.e - 275. p.n.e.) - poznati starogrči matematičar iz Atene

[8] Elementi - matematički spisi objavljeni oko 300. pr. Kr. u 13 knjiga

Euklidov uvjet implicira da je dovoljno pronaći proste brojeve u nizu 3, 7, 15, 31, 63, 127, 255, 511, 1023, 2047, 4095, 8191, ... kako bismo pronašli savršene brojeve i to je problem koji će nas zanimati. Ukratko, za koje je vrijednosti n broj $2^n - 1$ prost? Proučavajući ovaj problem, Fermat je otkrio važnu činjenicu koja je danas poznata kao Fermatov teorem.

Najprije, $15, 63, 255, 1023 (= 3 \cdot 341), 4095$ očito nisu prosti. Općenito, ako je n paran i veći od 2 tada $2^n - 1 = 2^{2k} - 1 = (2^k - 1)(2^k + 1)$ nije prost. Neparne vrijednosti broja n, $n = 3, 5, 7$ vode do prostih brojeva $7, 31, 127$, ali neparni broj $n = 9$ vodi do 511, koji je djeljiv sa 7. Ovo vodi do pretpostavke da ako n nije prost, onda $2^n - 1$ nije prost, tvrdnja koja se lako provjeri ako primijetimo da je $2^{km} - 1 = (2^k - 1)(2^{k(m-1)} + 2^{k(m-2)} + \ldots + 2^k + 1)$. Ovo opažanje reducira problem na pitanje: *Za koji prosti broj p je $2^p - 1$ prost broj?* Prosti brojevi ovog oblika zovu se Mersenneovi prosti brojevi u čast Fermatovog suvremenika i čestog dopisnika, Marina Mersennea (1588. -1648.).

Prosti brojevi 2, 3, 5, 7 odgovaraju Mersenneovim prostim brojevima 3, 7, 31, 127 (i stoga i savršenim brojevima 6, 28, 496, 8128), ali ostaje vidjeti je li broj $2^{11} - 1$ prost broj. Ovaj problem može biti jednostavno riješen pronalaskom $2^{11} - 1 = 2047$ eksplicitno i dijeleći sa svim prostim brojevima manjim od $\sqrt{2047}$. Mnogo je poučnije, međutim, pristupiti problemu na drugačiji način koji se može koristiti za testiranje $2^p - 1$ kada je p veći od 11.

Razmotrimo pitanje dijeli li 7 broj $2^{11} - 1$. Zamislimo potencije broja 2 napisane u jednoj liniji i njihove ostatke nakon dijeljenja brojem 7 napisane u drugoj liniji, ispod njih.

potencije od 2:	1	2	4	8	16	32	64	128	256	512	...
ostaci:	1	2	4	1	2	4	1	2	4	1	...

Obrazac ponašanja ostataka je očit, a očito je i to da 2^n dijeljenjem sa 7 daje ostatak 1 ako i samo ako je n višekratnik broja 3, odnosno, 7 *dijeli* $2^n - 1$ *ako i samo ako* 3 *dijeli* n. Stoga, 7 ne dijeli $2^{11} - 1$. Ista se metoda može koristiti za druge proste brojeve. Tablica 1.4 sadrži neke rezultate.

Tablica 1.4:

p=3	1	2	4	8	16	32	64	...						
	1	2	1	2	1	2	1	...						d=2
p=5	1	2	4	8	16	32	64	...						
	1	2	4	3	1	2	4	...						d=4
p=11	1	2	4	8	16	32	64	128	256	512	1024	2048	...	
	1	2	4	8	5	10	9	7	3	6	1	2	...	d=10
p=13	1	2	4	8	16	32	64	128	256	512	1024	2048	...	
	1	2	4	8	3	6	12	11	9	5	10	7	...	d=12
p=17	1	2	4	8	16	32	64	128	256	512	1024	2048	...	
	1	2	4	8	16	15	13	9	1	2	4	8	...	d=8

Definicija 1.5 *Neka je m prirodni broj. Reducirani sustav ostataka modulo m je skup cijelih brojeva r_i sa svojstvom da je $gcd(r_i, m) = 1$, $r_i \not\equiv r_j \pmod{m}$ za $i \neq j$, te da za svaki cijeli broj x takav da je $gcd(x, m) = 1$ postoji r_i takav da je $x \equiv r_i \pmod{m}$. Jedan reducirani sustav ostataka modulo m je skup svih brojeva $a \in \{1, 2, \ldots, m\}$ takvih da je $gcd(a, m) = 1$. Svi reducirani sustavi ostataka modulo m imaju isti broj elemenata. Taj broj označavamo s $\varphi(m)$, a funkciju $\varphi : \mathbb{N} \to \mathbb{N}$ zovemo Eulerova funkcija. Drugim riječima, $\varphi(m)$ je broj brojeva u nizu $1, 2, \ldots, m$ koji su relativno prosti s m.*

Teorem 1.6 *(Mali Fermatov teorem.) Neka je p prost broj. Ako $p \nmid a$, onda je $a^{p-1} \equiv 1 \pmod{p}$. Za svaki cijeli broj a vrijedi $a^p \equiv a \pmod{p}$.*

Definicija 1.7 *Neka su a i n relativno prosti prirodni brojevi. Najmanji prirodni broj d sa svojstvom da je $a^d \equiv 1 \pmod{n}$ zove se red od a modulo n. Još se kaže da a pripada eksponentu d modulo n.*

Teorem 1.8 *Neka je d red od a modulo n. Tada za prirodni broj k vrijedi $a^k \equiv 1 \pmod{n}$ ako i samo ako $d \mid k$. Posebno, $d \mid \varphi(n)$.*

Dokaz. Ako $d \mid k$, recimo $k = d \cdot l$, onda je $a^k \equiv (a^d)^l \equiv 1 \pmod{n}$.
Obratno, neka je $a^k \equiv 1 \pmod{n}$. Podijelimo k sa d, pa dobivamo $k = q \cdot d + r$, gdje je $0 \leq r < d$. Sada je

$$1 \equiv a^k \equiv a^{qd+r} \equiv (a^d)^q \cdot a^r \equiv a^r \pmod{n},$$

pa zbog minimalnosti od d slijedi da je $r = 0$, tj. $d \mid k$. ■

Definicija 1.9 *Ako je red od a modulo n jednak $\varphi(n)$, onda se a zove primitivni korjen modulo n.*

Ova opažanja impliciraju da je, kako bismo odredili je li $2^{11} \equiv 1 \pmod{p}$, dovoljno odrediti odgovarajući d i vidjeti dijeli li 11. Kako je 11 prost broj ovo je analogno pitanju je li $d = 11$. Odgovor na ovo pitanje je negativan za sve proste brojeve razmatrane do sada.

Na isti način možemo pristupiti i problemu određivanja je li $2^{13} - 1$ prost broj (i posljedično je li $2^{12}(2^{13} - 1)$ savršen broj). Problem je odrediti postoji li prost broj p za koji je odgovarajući $d = 13$. Svi su prosti brojevi razmotreni do sada eliminirani (jer njihov d nije bio 13) i sada je pitanje je li $d = 13$ za $p = 29, 31, 37, \ldots$, sve do prostog broja manjeg od $\sqrt{2^{13} - 1} = \sqrt{8191} < 91$. Promotrimo primjer.

p	3	5	7	11	13	17	19	23	29	31	37
d	2	4	3	10	12	8	18	11	28	5	36

Kako imamo d različitih ostataka, d je najviše $p - 1$. Iz prethodnog teorema slijedi da d dijeli $p - 1$. Ovo implicira da d može biti 13 samo

ako 13 dijeli $p-1$. Prema tome, moguće vrijednosti broja p su $13k+1$, $k \in \mathbb{Z}$. Od ovih vrijednosti jedino one za koje je k paran mogu biti proste. Kako 27 nije prost broj i kako je $79+26$ broj veći od $\sqrt{2^{13}-1}$ to znači da moramo ispitati samo dva prosta broja, 53 i 79. Odgovarajući d-ovi, određeni metodom korištenom ranije, su 52 i 39. Budući da su ovi brojevi različiti od 13 slijedi da je $2^{13}-1 = 8191$ prost broj.

Fermatov je teorem jedan od osnovnih svojstava aritmetike cijelih brojeva i bit će od velike važnosti u sljedećim poglavljima ovog rada. Spomenimo još takozvane Fermatove brojeve $2^1+1, 2^2+1, 2^4+1, 2^8+1, 2^{16}+1, 2^{32}+1, \ldots$.

Definicija 1.10 (Fermatovi brojevi) *Brojevi oblika $f_n = 2^{2^n}+1$ nazivaju se Fermatovi brojevi.*

Fermat je smatrao da su svi brojevi ovog oblika prosti te je vjerovao da je riješio drevni problem pronalaska formule koja daje proizvoljno velike proste brojeve. (Primijetimo da broj 2^n+1 nije prost ako n nije potencija broja 2 jer ako n ima neparni faktor k, recimo $n = km$, onda je $2^n+1 = (2^m+1)(2^{m(k-1)} - 2^{m(k-2)} + \ldots + 2^2 - 2 + 1))$.

Prvih nekoliko Fermatovih brojeva su prosti brojevi: $2^1+1 = 3, 2^2+1 = 5, 2^4+1 = 17$. Može se pokazati da je broj $2^8+1 = 257$ također prost.

Primjer 1.11 *Broj $2^8+1 = 257$ je prost.*

Ako p dijeli 2^8+1, onda dijeli i $(2^8+1)(2^8-1) = 2^{16}-1$. Stoga, d koji odgovara ovom p (za $a = 2$) mora dijeliti 16. Međutim, jedini djelitelji broja 16 su $1, 2, 4, 8, 16$, a d ne može biti $1, 2, 4$ ili 8 jer bi p onda dijelio 2^8-1, što bi bilo u kontradikciji s pretpostavkom da p dijeli 2^8+1. Prema tome, $d = 16$ i po Fermatovom teoremu $p = 16n+1$, za neki cijeli broj n. No, najmanji takav prost broj $p = 17$ je veći od $\sqrt{2^8+1}$ pa 2^8+1 nema pravih djelitelja, što je i trebalo pokazati. ■

Slično prethodnom primjeru, jedini prosti djelitelji koje bi broj $2^{16}+1$ mogao imati bili bi oblika $p = 32n+1$. Kako je $\sqrt{2^{16}+1}$ samo malo veći broj od $2^8 = 256$, onda su jedini prosti brojevi koje treba provjeriti dani u nizu brojeva $33, 65, 97, 129, 161, 193, 225$, a taj niz uključuje samo dva prosta broja 97, 193. Nijedan od tih brojeva ne dijeli $2^{16}+1$ jer su ostaci nakon djeljenja s 97: 1, 2, 4, 8, 16, 32, 64, 31, 62, 27, 54, 11, 22, 44, 88, 79, 61 pa $2^{16}+1$ djeljenjem s 97 daje ostatak 62, a ostaci nakon djeljenja sa 193 su 1, 2, 4, 8, 16, 32, 64, 128, 63, 126, 59, 118, 43, 86, 172, 151, 109 pa $2^{16}+1$ dijeljenjem sa 193 daje ostatak 110. Stoga, je $2^{16}+1$ prost.

Međutim, pokazat ćemo da je Fermatov broj $f_5 = 2^{2^5}+1 = 2^{32}+1$ složen broj. Euler je dokazao da je svaki djelitelj broja f_n oblika $k2^{n+1}+1$. Činjenica da je 641 djelitelj broja f_5 može se lako zaključiti iz jednakosti $641 = 2^7 \cdot 5+1$ i $641 = 2^4+5^4$. Iz prve jednakosti slijedi da je $2^7 \cdot 5 \equiv -1 \pmod{641}$ i prema tome da je $2^{28} \cdot 5^4 \equiv 1 \pmod{641}$. Nadalje, druga nejednakost implicira da je $5^4 \equiv -2^4 \pmod{641}$. Iz ovih kongruencija zaključujemo da je $-2^{32} \equiv 1 \pmod{641}$.

Poznato je da je nekoliko sljedećih Fermatovih brojeva složeno; $2^{64}+1, 2^{128}+1, 2^{256}+1$. Još nije pronađen nijedan Fermatov prost broj veći od $2^{16}+1$. Stoljeće i pol nakon što je Fermat iznio svoju pretpostavku, mladi je Gauss pokazao da je Euklidova konstrukcija peterokuta ravnalom i šestarom u čvrstoj vezi s tim da je $5 = 2^2+1$ Fermatov broj. Općenito, Gauss je pokazao ako je n prosti Fermatov broj da je tada moguća konstrukcija pravilnog $n-terokuta$ ravnalom i šestarom. Kao poslijedica toga što je Gauss iskazao, a Wantzel dokazao, jedini regularni n-terokuti koje se mogu konstruirati korištenjem ravnala i šestara su oni za koje vrijedi $n = 2^k p_1 p_2 \dots p_m$ gdje su p-ovi različiti Fermatovi brojevi i $k \geq 0$.

Poglavlje 2

Slučaj $n = 3$

2.1 Euler i slučaj $n = 3$

Leonhard Euler (1707.-1783.) bio je, bez sumnje, jedan od navećih matematičara u svoje vrijeme. Uz Eulerovo se ime vežu mnoge grane matematike, od primjenjene matematike do algebarske topologije i teorije brojeva. Njegovi doprinosi nisu bili samo u obliku novih teorema i novih metoda, nego i kao niz knjiga o algebri, analizi, matematičkoj fizici i drugim poljima, što je dalo temelje edukacije za sljedećih nekoliko generacija matematičara.

Naravno, najveće zanimanje za Eulera u ovom radu je zbog njegovog doprinosa teoriji brojeva i posebno zbog doprinosa Fermatovom Posljednjem teoremu. Euler je pokazao cjeloživotni interes za teoriju brojeva i njegovi su doprinosi od velike važnosti.

Smatra se da je Euler dao dokaz Fermatovog Posljednjeg teorema za slučaj $n = 3$, ali da je njegov dokaz bio nepotpun. Dokaz koji je Euler dao sadržavao je elementarnu pogrešku, međutim, ispravak dokaza najdirektnijom metodom - osiguravanjem alternativnog dokaza tvrdnje zbog koje je Eulerov dokaz pogrešan - nije bio nimalo lak. No, kao što će biti pokazano, dokaz može biti

ispravljen na manje direktan način.

2.2 Eulerov dokaz slučaja $n = 3$

Osnovna metoda Eulerovog dokaza slučaja $n = 3$ Fermatovog Posljednjeg teorema jest Fermatova metoda beskonačnog spusta. Kao što smo već vidjeli, metoda se svodi na činjenicu ako se mogu pronaći prirodni brojevi x, y, z za koje je $x^3 + y^3 = z^3$, onda se mogu naći i manji prirodni brojevi sa istim svojstvom; tada bi bilo moguće naći niz takvih trojki prirodnih brojeva koje neprestano opadaju i nikad ne završavaju, što je očigledno nemoguće. Prema tome, ne postoje takvi x, y, z.

Pregled Prvo ćemo opisati glavni tijek dokaza. Nakon što pretpostavimo da postoji rješenje jednadžbe $x^3+y^3 = z^3$, dat ćemo neka osnovna zapažanja o brojevima x, y i z. Pokazat ćemo zašto možemo pretpostaviti da su relativno prosti i da je z paran te x i y neparni. Brojeve x i y zapisat ćemo koristeći nove cijele brojeve p i q. Ako zamijenimo $x = p + q$ i $y = p - q$ u jednadžbi $x^3 + y^3$, dobit ćemo izraz $2p(p^2 + 3q^2) = z^3$. Ako znamo da su ovi brojevi relativno prosti, tada oba moraju biti kubovi. Međutim, postoji mogućnost da su oba djeljiva s 3 pa ćemo dokaz podijeliti u dva slučaja. U slučaju kad su $2p$ i $p^2 + 3q^2$ relativno prosti, pokazat ćemo da je $p^2 + 3q^2$ kub ako je $p = a^3 - 9ab$ i $q = 3a^2b - 3b^2$. Ovo je trenutak u dokazu kada je Euler napravio grešku zbog nedovoljno znanja o računu u prstenu kompleksnih brojeva. Ponovnim pokazivanjem da su brojevi relativno prosti, dolazimo do dokaza da su $2a$, $a-3b$ i $a+3b$ relativno prosti i da je $2p = 2a(a-3b)(a+3b)$. Kako je $2p$ kub, sva tri manja broja također moraju biti kubovi. Primijetimo da je $(a-3b)+(a+3b) = 2a$. Sada smo pronašli tri kuba koja zadovoljavaju jednadžbu $\alpha^3 + \beta^3 = \gamma^3$. Nakon ovoga razmotrit ćemo drugi slučaj, kada su

$2p$ i $p^2 + 3q^2$ djeljivi s 3. Ovaj se slučaj dokaže na sličan način. Konačno, uvjerit ćemo se da je novo rješenje koje smo našli uistinu manje od početnog i dokaz će slijediti iz metode beskonačnog spusta.

Teorem 2.1 (Slučaj $n = 3$) *Ne postoje cjelobrojna rješenja jednadžbe* $x^3 + y^3 = z^3$.

Dokaz. Pretpostavimo suprotno, tj. da postoje prirodni brojevi x, y i z takvi da je $x^3 + y^3 = z^3$. Prvo ćemo dati nekoliko tvrdnji o brojevima x, y i z. Možemo pretpostaviti da su x, y i z relativno prosti i pozitivni. Ako postoji broj koji dijeli sva tri broja, cijelu jednadžbu možemo podijeliti tim brojem. Ako neki broj dijeli dva broja, onda mora dijeliti i treći. Dakle, najviše je jedan broj paran. Ne možemo imati tri neparna broja jer ako su x i y neparni, onda je z paran. Dakle, imamo točno jedan paran broj. Pretpostavimo da su x i y neparni, a z paran. Ako ovo nije slučaj, možemo preurediti našu jednadžbu. Na primjer, ako znamo da je x paran u jednadžbi $x^3 + y^3 = z^3$, tada znamo da je $x^3 = z^3 + (-y^3)$. Brojevi $x + y$ i $x - y$ su parni pa ih možemo možemo pisati u obliku $2p$ i $2q$ kako slijedi:

$$x = \frac{1}{2}((x + y) + (x - y)) = \frac{1}{2}(2p + 2q) = p + q$$
$$y = \frac{1}{2}((x + y) - (x - y)) = \frac{1}{2}(2p - 2q) = p - q.$$

Sada možemo ponovno zapisati $x^3 + y^3 = (x + y)(x^2 - xy + y^2)$ koristeći nove izraze za x i y kao

$$2p[(p + q)^2 - (p + q)(p - q) + (p - q)^2] = 2p(p^2 + 3q^2).$$

Donesimo nekoliko zaključaka o p i q. Kako su $p+q$ i $p-q$ oba neparna, p i q moraju biti različitih parnosti. Također, moraju biti relativno prosti jer bi

u suprotnom, ako imaju zajedničkog djelitelja, taj djelitelj dijelio $x = p+q$ i $y = p-q$. Možemo pretpostaviti da su oba pozitivna jer možemo promijeniti poredak od x i y u slučaju da je $x - y$ negativan broj. Također, znamo da ni p ni q nisu nula jer je slučaj $x = y$ nemoguć. Kako su relativno prosti, ovo bi impliciralo $x = y = 1$ i stoga $z^3 = 2$. Dakle, s obzirom na naše pretpostavke da su x i y pozitivna rješenja jednadžbe, vidimo da je

$$2p(p^2 + 3q^2) = n^3$$

gdje su p i q relativno prosti prirodni brojevi različitih parnosti.

Dva slučaja: Relativno prosti ili djeljivi s 3 U sljedećem dijelu dokaza pokazat ćemo da su ili $2p$ i $p^2 + 3q^2$ djeljivi s 3, ili relativno prosti pa prema tome moraju biti potpuni kubovi. Jedini slučaj kada nisu relativno prosti je ako je njihov djelitelj 3. Kako su p i q različitih parnosti znamo da je $p^2 + 3q^2$ neparan broj. Ovo je lako vidjeti ako razmotrimo slučajeve kada je p paran, a q neparan i kada je q paran, a p neparan. Ako $2p$ i $p^2 + 3q^2$ imaju zajednički faktor, p i $p^2 + 3q^2$ moraju imati isti zajednički faktor. Ako $d \mid p$ i $d \mid p^2 + 3q^2$, tada znamo da $d \mid 3q^2$. Dakle, ako $2p$ i $p^2 + 3q^2$ imaju zajednički faktor, on također mora biti zajednički faktor od p i $3q^2$. Međutim, znamo da su p i q relativno prosti pa je jedini mogući zajednički faktor broj 3. Ako $3 \mid p$ i $3 \mid 3q^2$ tada znamo da $3 \mid 2p$ i $3 \mid p^2 + 3q^2$. Dakle, $2p$ i $p^2 + 3q^2$ su ili relativno prosti ili im je zajednički djelitelj broj 3. Rastavit ćemo dokaz u dva slučaja.

2.2.1 Prvi slučaj: Relativno prosti

Prvo ćemo razmotriti slučaj kada $2p$ i $p^2 + 3q^2$ nisu djeljivi s tri i prema tome relativno su prosti. Koristeći algebarske manipulacije pokazat ćemo ako je $p = a^3 - 9ab^2$ i $q = 3a^2b - 3b^2$ onda je $p^2 + 3q^2$ kub. Koristimo sljedeću

formulu koja se lako provjeri koristeći zakone komutativnosti, asocijativnosti i distributivnosti. Jednakost

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$$

pokazuje da ako su dva broja zbroj dvaju kvadrata, onda je njihov produkt zbroj dvaju kvadrata. Preformulirat ćemo jednakost kako bi odgovarala našim brojevima dodavajući 3 s jedne strane i mijenjajući drugu stranu kako slijedi

$$(a^2 + 3b^2)(c^2 + 3d^2) = (ac - 3bd)^2 + 3(ad + bc)^2.$$

Dokaz zahtijeva samo osnovne algebarske manipulacije. Umjesto korištenja četiri varijable a, b, c i d razmotrit ćemo samo produkt

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

imamo

$$\begin{aligned}(a^2 + 3b^2)^3 &= (a^2 + 3b^2)[(a^2 - 3b^2)^2 + 3(2ab)^2] \\ &= [a(a^2 - 3b^2) - 3b(2ab)]^2 + 3[a(2ab) + b(a^2 - 3b^2)]^2 \\ &= (a^3 - 9ab^2)^2 + 3(3a^2b - 3b^3)^2.\end{aligned}$$

Uzimajući a i b proizvoljne, možemo pronaći kubove oblika p^2+3q^2 stavljajući

$$\begin{aligned}p &= a^3 - 9ab^2 \\ q &= 3a^2b - 3b^3.\end{aligned} \tag{2.1}$$

Vidimo da je $p^2 + 3q^2 = (a^2 + 3b^2)^3$.

2.2.2 Eulerova pogreška

Operacije u prstenu $\mathbf{Z}[\sqrt{-3}]$

Lema 2.2 *Neka je $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} : a, b \in \mathbb{Z}\}$. Za a, b, c, $d \in \mathbb{Z}$ definiramo zbrajanje i množenje s:*

$$(a + b\sqrt{-3}) + (c + d\sqrt{-3}) = (a + c) + (b + d)\sqrt{-3},$$
$$(a + b\sqrt{-3}) \cdot (c + d\sqrt{-3}) = ac - 3bd + (ad + bc)\sqrt{-3}.$$

Uz ovako definirane binarne operacije, $\mathbb{Z}[\sqrt{-3}]$ je prsten s jedinicom.

Kako bismo objasnili Eulerovu pogrešku, trebamo definirati teoriju djeljivosti za prsten $\mathbb{Z}[\sqrt{-3}]$. Definirajmo najprije normu na skupu $\mathbb{Z}[\sqrt{-3}]$.

Definicija 2.3 *Funkciju $N : \mathbb{Z}[\sqrt{-3}] \to \mathbf{N_0}$ zadanu s*

$$N(a + b\sqrt{-3}) = \mid a + b\sqrt{-3} \mid^2 = a^2 + 3b^2$$

nazivamo norma.

Važno je primijetiti da je norma multiplikativna: $N(xy) = N(x)N(y)$ za sve $x, y \in \mathbb{Z}[\sqrt{-3}]$.

Definicija 2.4 *Broj čija je norma veća od 1 te koji se ne može prikazati kao produkt brojeva manje norme nazivamo prostim brojem.*

Slično, vrijedi da ako β dijeli α u $\mathbb{Z}[\sqrt{-3}]$, onda $N(\beta)$ dijeli $N(\alpha)$ u skupu $\mathbb{Z}$. Dakle, α je prost u $\mathbb{Z}[\sqrt{-3}]$ ako $N(\alpha)$ nije djeljiva niti s jednom normom različitom od 1, to jest, niti s jednim brojem oblika $a^2 + 3b^2 \neq 1$.

Primjer 2.5 *Primjeri prostih brojeva u $\mathbb{Z}[\sqrt{-3}]$ su:*

$$2, \quad \textit{jer je } N(2) = 4,$$
$$1 - \sqrt{-3}, \quad \textit{jer je } N(1 - \sqrt{-3}) = 4$$
$$1 + \sqrt{-3}, \quad \textit{jer je } N(1 + \sqrt{-3}) = 4.$$

Zaključujemo da 4 ima dva različita rastava na proste faktore u $\mathbb{Z}[\sqrt{-3}]$:

$$4 = 2 \cdot 2 = (1 - \sqrt{-3})(1 + \sqrt{-3}).$$

Vrijedi sljedeća tvrdnja.

Teorem 2.6 *Prsten $\mathbb{Z}[\sqrt{-3}]$ nije domena jedinstvene faktorizacije.*

Eulerova pogreška

Euler je dokazao da je jedini način na koji $p^2 + 3q^2$ može biti kub jest ako postoje brojevi a i b takvi da su p i q dani kao u jednadžbi (2.1). Njegov je dokaz bio pogrešan jer je koristio aritmetiku cijelih brojeva pri razmatranju brojeva oblika $a + b\sqrt{-3}$. Pretpostavio je jedinstvenu faktorizaciju u prstenu $\mathbb{Z}[\sqrt{-3}]$ zato što je istinita u skupu cijelih brojeva, međutim, u prstenu $\mathbb{Z}[\sqrt{-3}]$ jedinstvena faktorizacija ne vrijedi nužno. No, moguće je popraviti dokaz koristeći ideje koje je objavio u drugim člancima. Dokaz sljedeće leme dao je Edwards [1].

Lema 2.7 *Neka su p i q relativno prosti brojevi takvi da je $p^2 + 3q^2$ kub. Tada postoje cijeli brojevi a i b takvi da je $p + q\sqrt{-3} = (a + b\sqrt{-3})^3$*

Dokaz. Oblik koji se pojavljuje u iskazu malo je drugačiji od onoga koji se pojavljuje u dokazu, ali može se lako preoblikovati. Faktorizirajmo najprije izraz $p^2 + 3q^2$ na sljedeći način:

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

Prema tome, ako je jedan od ovih faktora kub, recimo $p + q\sqrt{-3} = (a + b\sqrt{-3})^3$ tada je i njegov konjugat također kub; tj. $p - q\sqrt{-3} = (a - b\sqrt{-3})^3$. Dakle, iz svojstva komutativnosti množenja slijedi $(p + q\sqrt{-3})(p - q\sqrt{-3}) =$

[1] Harold Mortimer Edwards, Jr. (rođen 1936.) - američki matematičar.

$[(a + b\sqrt{-3})(a - b\sqrt{-3})]^3$, tj. $p^2 + 3q^2 = (a^2 + 3b^2)^3$. Proširimo sada izraz $(a + b\sqrt{-3})^3$ koristeći binomni teorem

$$\begin{aligned} p + q\sqrt{-3} &= a^3 + 3a^2b\sqrt{-3} + 3ab^2(-3) + b^3(-3)\sqrt{-3} \\ &= a^3 - 9ab^2 + (3a^2b - 3b^3)\sqrt{-3} \end{aligned}$$

Množenjem i pregrupiranjem izraza koji sadrže $\sqrt{3}$ vidimo da, ako je $p^2 + 3q^2$ kub, onda postoje cijeli brojevi a i b takvi da je $p = a^3 - 9ab^2$ i $q = 3a^2b - 3b^3$. ■

Metoda beskonačnog spusta Možemo faktorizirati izraze p i q na sljedeći način

$$p = a(a - 3b)(a + 3b)$$

$$q = 3b(a - b)(a + b).$$

Ako bi a i b imali zajednički faktor, onda bi taj faktor dijelio zbroj od a i b, a stoga i p i q. Kako su p i q relativno prosti onda i a i b moraju biti relativno prosti. Budući da otprije znamo da je $2p$ kub, jednostavnim množenjem gornje jednakosti s 2 vidimo da postoji cijeli broj n takav da

$$2p = 2a(a - 3b)(a + 3b) = n^3.$$

Znamo da a i b ne mogu biti iste parnosti jer bi inače p i q oba bila parna. Ovo jednostavno slijedi iz proučavanja jednadžbe i primjećivanja da će $a+b$ i $a+3b$ biti parni ako su a i b iste parnosti. Prema tome, $a-3b$ i $a+3b$ su oba neparna. Ako postoji zajednički faktor za $2a$ i $a \pm 3b$ onda je to zajednički faktor i za a i $a \pm 3b$. Kako a dijeli a onda to mora biti i zajednički faktor od a i $3b$. Ako brojevi $a + 3b$ i $a - 3b$ imaju zajednički faktor onda bi on dijelio njihovu sumu i razliku. Dakle, bilo koji zajednički faktor bio bi faktor od a i $3b$. Broj 3 je jedini mogući zajednički faktor brojeva a i $3b$ budući da su a i b relativno prosti. Međutim, znamo $3 \nmid a$ jer $a \mid p$ i prema pretpostavci

$3 \nmid p$. Ovo pokazuje da su $2a$, $a - 3b$ i $a + 3b$ relativno prosti i kako je $2p$ kub, svi moraju biti kubovi. Prema tome, moraju postojati vrijednosti α, β, γ takvi da je $2a = \alpha^3, a - 3b = \beta^3$ i $a + 3b = \gamma^3$. Zbrajajući izraze dobije se $a - 3b + a + 3b = 2a$. Supstitucijom s novim izrazima dobije se $\beta^3 + \gamma^3 = \alpha^3$. Ovo je rješenje Fermatove jednadžbe za $n = 3$ za cijele brojeve manje od x, y, z. Sada je još potrebno dokazati da novo rješenje koristi manje cijele brojeve i da su ti brojevi pozitivni prije nego je naš dokaz gotov.

Dokaz da su novi cijeli brojevi manji od početnih Primijetimo da

$$\alpha^3\beta^3\gamma^3 = 2a(a - 3b)(a + 3b) = 2p.$$

Prisjetimo se da smo definirali $z^3 = 2p(p^2 + 3q^2)$. Stoga $2p$ dijeli z^3. Mogao bi biti slučaj da je $2p = z^3$, ali ako nije, onda mora biti manji. Znamo da je $2p$ pozitivan. Kako je $2p$ paran broj, onda je djelitelj od z^3 ako je z paran i djelitelj od x^3 ako je x paran. U svakom slučaju, onda su α^3, β^3 i γ^3 manji od z^3. Također, moramo razmotriti što bi se dogodilo da su α, β i γ negativni. Kako je $(-\alpha)^3 = -\alpha^3$ možemo jednostavno prebaciti negativne kubove na drugu stranu jednadžbe. Jednadžba koju bismo onda dobili još bi uvijek imala sve kubove manje od z^3. Prema tome, doista bismo imali beskonačni spust prirodnih brojeva, ali samo u slučaju kada $3 \nmid p$. Kako bismo završili dokaz pretpostavit ćemo $3 \mid p$.

2.2.3 Slučaj $3 \mid p$

S obzirom da smo pretpostavili da je p djeljivo s 3, možemo pisati $p = 3s$. Također znamo da $3 \nmid q$. Dakle, možemo pisati $2p(p^2 + 3q^2) = 3^2 2s(3s^2 + q^2)$. Primijetimo da je $2p(p^2 + 3q^2)$ kub pa je sljedeći logični korak pokazati da su $3^2 2s$ i $3s^2 + q^2$ relativno prosti. Ovaj je korak sličan onome što smo već napravili. Pretpostavimo da je m prost broj takav da $m \mid 3^2 2s$. Ovo znači

da $m \mid 3$, $m \mid 2$ ili $m \mid s$. Ako $m \mid 3$ tada znamo da je $m = 3$ i stoga da $3 \mid q$. No, već znamo da ovo nije istina jer su p i q relativno prosti. Ako $m \mid 2$ tada je $m = 2$. Međutim, $3s^2 + q^2$ nije paran broj jer su q i s različitih parnosti. Ovo slijedi iz činjenice da su p i q različitih parnosti, a prema tome, različitih su parnosti s i q. Konačno, ako $m \mid s$ onda $m \nmid 3s^2 + q^2$ jer su s i q relativno prosti. Kako su $3^2 2s$ i $3s^2 + q^2$ relativno prosti onda oba moraju biti kubovi.

Lema 2.8 *Neka su s i q relativno prosti brojevi takvi da je $3s^2+q^2$ kub. Tada postoje cijeli brojevi a i b takvi da je $q = a(a-3b)(a+3b)$ i $s = 3b(a-b)(a+b)$.*

Ova je lema ekvivalentna Lemi 2.7 s manjim promjenama u algebri i nazivima varijabli. Supstitirajmo s u izrazu $3^2 2s$ sa s danim u Lemi 2.8 primijetimo da je $3^3 2b(a-b)(a+b)$ kub. Prema tome, $2b(a-b)(a+b)$ je kub. Ako su a i b relativno prosti, lako je vidjeti da su svi faktori relativno prosti. Možemo reći da su a i b relativno prosti jer je $gcd(s, q) = 1$ pa je $gcd(a(a-3b)(a+3b), 3b(a-b)(a+b)) = 1$. Ako bi vrijedilo da je $gcd(a, b) = k$ onda bi s i q također imali zajednički faktor k.

Kako su faktori međusobno relativno prosti, moraju biti kubovi. Stoga je $2b = \alpha^3, a - b = \beta^3, a + b = \gamma^3$, odnosno $\alpha^3 = 2b = \gamma^3 - \beta^3$. Pokazat ćemo još da je $\gamma < z$. Primijetimo da $\gamma^3 \mid 3^2 2s$ i $3^2 2s \mid 2p(p^2 + 3q^2) = z^3$. Prema tome, našli smo rješenje s manjim cijelim brojevima i dokazali smo da, u oba slučaja, jednadžba $x^3 + y^3 = z^3$ nema rješenja u skupu prirodnih brojeva. ■

Poglavlje 3

Slučaj $n = 5$

3.1 Uvod

Kada je Euler rekao Goldbachu u svom pismu 4. kolovoza 1753. da je uspio dokazati Fermatov Posljednji teorem u slučaju $n = 3$, primijetio je da se dokaz podosta razlikuje od dokaza u slučaju $n = 4$. U sljedećih devedeset godina došlo se do nekoliko - vrlo malo - posebnih slučajeva i djelomičnih rezultata, međutim, konačni dokaz Fermatovog Posljednjeg teorema činio se poprilično nedostižnim.

Ovo je poglavlje posvećeno najvažnijim rezultatima dobivenim tijekom ovog devedesetogodišnjeg perioda. Potpoglavlje 3.2 posvećeno je istraživanjima i dokazu teorema Sophie Germain, Potpoglavlje 3.2.1 dokazu slučaja $n = 5$ Fermaovog Posljednjeg teorema do kojeg su došli Legendre i Dirichlet, i Poglavlje 4 opažanjima o dokazu teorema u slučajevima $n = 14$ i $n = 7$ koje su dokazali Dirichlet i Lame.

3.2 Sophie Germain

Marie Sophie Germain bila je francuska matematičarka rođena 1. travnja 1776. u Parizu. Njezino zanimanje za teoriju brojeva razvilo se nakon čitanja *Essai sur la théorie des nombres* [1] Adriena Mariea Legendrea i *Disquisitiones Arithmeticae* [2] Carla Friedricha Gaussa.

Unatoč predrasudama, jer je u to vrijeme bilo neprilično da ženu zanima znanost, Sophie je ustrajala u učenju. 1794. godine Sophie je, unatoč zabranama, upisala akademiju Echole Polytechnique u Parizu i tako dobila priliku učiti od najboljih matematičara tog vremena. Pod pseudonimom M. LeBlanc, Sophie je predala svoj rad tada najvećem francuskom matematičaru J. L. Lagrangeu, koji je, impresioniran radom, tražio da upozna autora. Unatoč postupnom prihvaćanju žena u znanosti, Sophie je zapriječen napredak na Akademiji, jer je pripadala srednjem sloju francuskog društva, kojemu nije bilo dozvoljeno visoko školovanje. Godine 1804. Sophie je počela surađivati s njemačkim matematičarom Carlom Friedrichom Gaussom.

3.2.1 "Veliki plan"

Mnogi su matematičari radili na dokazivanju Fermatovog Posljednjeg teorema, uključujući Eulera, Legendrea, Gaussa, Abela, Dirichleta, Kummera i Cauchya. Germain je, zapravo, imala "veliki plan" u dokazivanju teorema za sve proste brojeve p, umjesto dokazivanja posebnih slučajeva. Fermat je dokazao slučaj $n = 4$, a Euler je 1770. objavio dokaz za slučaj $n = 3$ i u vrijeme kad je Germain počela raditi na Fermatovom Posljednjem teoremu, to su bili jedini poznati dokazani slučajevi. Sophiein plan nije napredovao očekivano, ali je putem došla do drugih zanimljivih rezultata i uvelike doprinijela do-

[1] Essai sur la théorie des nombres - Eseji o teoriji brojeva, Adrien Marie Legendre, 1789.

[2] Disquisitiones Arithmeticae - Aritmetička istraživanja, Carl Friedrich Gauss, 1798.

kazivanju Fermatovog teorema. Germaine je dokazala sljedeći teorem koji je danas poznat pod njezinim imenom.

Teorem 3.1 *Ako je $x^5 + y^5 = z^5$ onda jedan od brojeva x, y, z mora biti djeljiv s 5.*

Dokaz. Iako je Fermatov teorem iskazan u obliku $x^5 + y^5 \neq z^5$ za prirodne brojeve, pogodno je premjestiti z^5 na drugu stranu jednadžbe $x^5 + y^5 + (-z^5) \neq 0$ i izreći slučaj $n = 5$ u obliku: "Jednadžba $x^5 + y^5 + z^5 = 0$ nema rješenje za cijele brojeve x, y i z različite od nula." Prednost ovakvog zapisa leži u tome što uloge brojeva x, y i z postaju zamjenjive. Kako je nula djeljiva s 5 teorem kojeg treba dokazati prelazi u formu: "Ako su x, y, i z cijeli brojevi takvi da $x^5 + y^5 + z^5 = 0$ tada jedan od tih brojeva mora biti djeljiv s 5."

Prvi je korak u dokazu zapisati jednadžbu u obliku

$$-x^5 = (y + z)(y^4 - y^3z + y^2z^2 - yz^3 + z^4)$$

Kao i obično, možemo pretpostaviti da su x, y i z u parovima relativno prosti. Tada su oba faktora s desne strane relativno prosta jer bi inače vrijedilo da postoji prosti broj p koji dijeli $y + z$, odnosno $y \equiv -z \pmod{p}$ i $y^4 - y^3z + y^2z^2 - yz^3 + z^4 \equiv 5y^4 \pmod{p}$. Ako p dijeli oba faktora tada je ili $p = 5$ i u tom je slučaju x djeljiv s 5 što je i trebalo pokazati, ili p dijeli y i $y + z$ i u tom slučaju y i z nisu relativno prosti. Drugim riječima, ako je $x^5 + y^5 + z^5 = 0$, ako su x, y i z u parovima relativno prosti i ako su sva tri broja relativno prosta s 5, onda su $y + z$ i $y^4 - y^3z + y^2z^2 - yz^3 + z^4$ relativno prosti. Kako je njihov produkt peta potencija $y^5 + z^5 = -x^5 = (-x)^5$, ovo implicira da svaki broj mora biti peta potencija cijelog broja. Simetrično, isti se argument primjenjuje na $-y^5 = x^5 + z^5$ i $-z^5 = x^5 + y^5$ kako bismo

pokazali da postoje cijeli brojevi a, α, b, β, c, γ takvi da je

$$\begin{array}{lll} y+z=a^5 & y^4-y^3z+y^2z^2-z^3+z^4=\alpha^5 & x=-a\alpha \\ z+x=b^5 & z^4-z^3x+z^2x^2-zx^3+x^4=\beta^5 & y=-b\beta \\ x+y=c^5 & x^4-x^3y+x^2z^2-xy^3+y^4=\gamma^5 & z=-c\gamma. \end{array}$$

Pokazat ćemo da ovo nije moguće.

U ovom dokazu važno je uočiti da pete potencije modulo 11 daju ostatke -1, 0 i 1. Prema tome, $x^5+y^5+z^5 \equiv 0 \pmod{11}$ vrijedi samo ako su x ili y ili $z \equiv 0 \pmod{11}$ jer je $\pm 1 \pm 1 \pm 1 = 0$ nemoguće.

Pretpostavimo da imamo rješenje jednadžbe $x^5+y^5+z^5=0$ takvo da su x, y i z u parovima relativno prosti i 5 nije djelitelj ni jednog od tih brojeva. Tada se mogu pronaći a, α, b, β, c, γ koji zadovoljavaju gornje jednadžbe. Jedan od brojeva x, y i z mora biti djeljiv s 11. Pretpostavimo, bez smanjenja općenitosti, da je to x. Tada je $2x = b^5+c^5+(-a)^5$ djeljiv s 11 te jedan od brojeva a, b i c mora biti djeljiv s 11. Međutim, b ne može biti djeljiv s 11 jer je x djeljiv s 11, a onda bi x i z imali zajednički djelitelj 11, suprotno pretpostavci da su relativno prosti. Slično, c ne može biti djeljiv s 11. Dakle, a mora biti djeljiv s 11. Međutim, ovo je također nemoguće jer bi onda vrijedilo $y \equiv -z \pmod{11}$, $\alpha^5 \equiv 5y^4 \pmod{11}$, dok bi s druge strane vrijedilo $x \equiv 0 \pmod{11}$, $\gamma^5 \equiv y^4 \pmod{11}$, iz čega slijedi $\alpha^5 \equiv 5 \cdot \gamma^5 \pmod{11}$. Budući da su 0, ± 1 ostaci petih potencija modulo 11 to implicira da je $\alpha \equiv \gamma \equiv 0 \pmod{11}$ što je u kontradikciji s pretpostavkom da su x i z relativno prosti. Prema tome, vrijedi tvrdnja teorema.

■

Srž onoga čime se Sophie Germain bavila leži u sljedećem teoremu.

Teorem 3.2 (Teorem Sophie Germain) *Neka su n i p različiti neparni prosti brojevi koji zadovoljavaju sljedeće uvjete:*

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

2. *Ako su* x, y *i* z *cijeli brojevi takvi da je*

$$x^n + y^n + z^n \equiv 0 \ (mod\ p),$$

onda p *dijeli* x, y *ili* z.

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

Dokaz. Kako je p prost broj, Fermatov Posljednji teorem za p može se preformulirati u tvrdnju da ne postoje cijeli brojevi x, y i z različiti od nule takvi da je $x^n + y^n + z^n = 0$. Slučaj I Fermatovog Posljednjeg teorema za n je tvrdnja da ne postoje cijeli brojevi x, y i z koji nisu djeljivi s n, a za koje vrijedi da je $x^n + y^n = z^n$.

Pretpostavimo da n i p zadovoljavaju pretpostavke teorema i da su x, y, z cijeli brojevi, od kojih niti jedan nije djeljiv s n, za koje vrijedi $x^n + y^n + z^n = 0$. Pokazat će se da ove pretpostavke dovode do kontradikcije.

Kao i obično, može se pretpostaviti da su x, y i z u parovima relativno prosti cijeli brojevi. Jednadžba $(-x)^n = y^n + z^n = (y + z)(y^{n-1} - y^{n-2}z + y^{n-3}z^2 - \ldots + z^{n-1})$ pokazuje da su $y + z$ i $y^{n-1} - y^{n-2}z + \ldots + z^{n-1}$ oba n-te potencije jer su relativno prosti. Ako bi postojao prost broj q koji dijeli oba izraza tada bi bilo $x + z \equiv 0 \pmod{q}$, $y^{n-1} - y^{n-2}z + \ldots + z^{n-1} \equiv 0 \pmod{q}$, $y \equiv 0 \pmod{q}$, $ny^{n-1} \equiv 0 \pmod{q}$ iz čega slijedi da je $n \equiv 0 \pmod{q}$ ili $y \equiv 0 \pmod{q}$. Prvi slučaj nije moguć jer bi onda $n = q$ dijelio x, a drugi slučaj nije moguć jer bi q dijelio i y i $y + z$. Jednadžba $(-y)^n = x^n + z^n$ i $(-z)^n = x^n + y^n$ može se faktorizirati na isti način te slijedi da moraju postojati cijeli brojevi $a, \alpha, b, \beta, c, \gamma$ takvi da

$$\begin{array}{lll} y+z=a^n & y^{n-1}-y^{n-2}z+\ldots+z^{n-1}=\alpha^n & x=-a\alpha \\ z+x=b^n & z^{n-1}-z^{n-2}x+\ldots+x^{n-1}=\beta^n & y=-b\beta \\ x+y=c^n & x^{n-1}-x^{n-2}y+\ldots+y^{n-1}=\gamma^n & z=-c\gamma. \end{array}$$

Promotrimo sada aritmetiku modulo p. Kako je $x^n+y^n+z^n \equiv 0 \pmod{p}$, drugi uvjet na p implicira da x, y ili z moraju biti kongruentni nula modulo p. Pretpostavimo, bez smanjenja općenitosti, da je $x \equiv 0 \pmod{p}$. Tada je $2x = b^n + c^n + (-a)^n \equiv 0 \pmod{p}$ i, ponovno po drugom uvjetu na p, slijedi da a, b ili c moraju biti kongruentni nula modulo p. Ako bi b ili c bili kongruentni nula modulo p tada bi $y = -b\beta \equiv 0 \pmod{p}$ ili $z = -c\gamma \equiv 0 \pmod{p}$, što bi, zajedno s $x \equiv 0 \pmod{p}$, bilo u kontradikciji s pretpostavkom ta su x, y i z u parovima relativno prosti. Prema tome, $a \equiv 0 \pmod{p}$. Medutim, ovo implicira da je $y \equiv -z \pmod{p}$, $\alpha^n \equiv ny^{n-1} \equiv n\gamma^n \pmod{p}$. Kako je $\gamma \not\equiv 0 \pmod{p}$ onda postoji cijeli broj g takav da je $\gamma g \equiv 1 \pmod{p}$, iz čega slijedi $(\alpha g)^n \equiv n \pmod{p}$, što je u kontradikciji s drugom pretpostavkom o p. Ova kontradikcija dokazuje Teorem Sophie Germain. ■

Teorem Sophie Germain obično se iskazuje u slabijoj formi:

Teorem 3.3 (Sophie Germain) *Neka je $x^n + y^n = z^n$. Ako je n neparan prost broj i ako vrijedi da je $p = 2n + 1$ također prost broj, onda n mora dijeliti xyz, i prema tome Slučaj I Fermatovog Posljednjeg teorema je istinit za p.*

Dokaz. Dovoljno je provjeriti da prosti brojevi n i $p = 2n+1$ zadovoljavaju pretpostavku 2 Teorema 3.2.

Ako je $n \equiv a^n \pmod{p}$, računanjem Legendreovog simbola dobit ćemo

$$\pm\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} = a^n \equiv n \pmod{p}$$

pa je $p \equiv \pm 1 \pmod{q}$, što je nemoguće.

Nadalje, pretpostavimo da je $x^n + y^n + z^n \equiv 0 \pmod{p}$ i $p \nmid xyz$. Kako je $n = (q-1)/2$, Mali Fermatov teorem implicira da je

$$\begin{aligned} x^p &\equiv \pm 1 \pmod{p}, \\ y^p &\equiv \pm 1 \pmod{p}, \\ z^p &\equiv \pm 1 \pmod{p}. \end{aligned}$$

Dakle, $0 = x^n + y^n + z^n \equiv \pm 1 \pm 1 \pm 1 \pmod{q}$ što je opet nemoguće. ■

Brojeve oblika $2n + 1$, gdje je n prost broj, nazivamo prostim brojevima Sophie Germain.

Koristeći ovaj teorem Sophie Germain je uspjela dokazati Slučaj I Fermatovog Posljednjeg teorema za sve proste brojeve manje od 100. Drugim riječima, za svaki neparni prosti broj n manji od 100, Sophie je mogla pronaći drugi prosti broj p koji zadovoljava uvjete prethodnog teorema. Legendre je proširio ove rezultate na sve proste brojeve manje od 197 kao i na mnoge druge proste brojeve. S ovim rezultatima, koji su ostvareni prije nego je Posljednji Fermatov teorem bio dokazan, postalo je jasno da pažnju treba usmjeriti na Slučaj II.

Poglavlje 4

Slučajevi $n = 7$ i $n = 14$

4.1 Povijesni uvod

Godine 1837., sedam godina nakon što su Dirichlet i Legendre dokazali slučaj $n = 5$, Dirichlet je objavio dokaz slučaja $n = 14$. Bilo je mnogo poželjnije dokazati sluča $n = 7$ jer je svaka četrnaesta potencija ujedno i sedma potencija. Tek je 1839. Lamè uspio dokazati slučaj $n = 7$. Ni dokaz ovog slučaja nije davao nadu da će se pronaći općenito rješenje jer je uvelike ovisio o svojstvima broja 7. Dokaz slučaja $n = 14$ oslanja se na tehnike slične onima korištenim u dokazima slučajeva $n = 5$ i $n = 3$, ali zahtijeva znatnu kreativnost u algebarskim manipulacijama. Suština dokaza ponovno je metoda beskonačnog spusta, ali u nešto kompleksnijem obliku. Treba naglasiti kako je dokaz za slučaj $n = 7$ znatno složeniji od dokaza za slučaj $n = 14$, pa dokaz tog slučaja neće biti obrađen u ovom radu.

4.2 Ključni koraci dokaza

Pretpostavimo da postoje u parovima relativno prosti cijeli brojevi x, y i z koji zadovoljavaju jednadžbu $x^{14} + y^{14} = z^{14}$. Koristeći alate teorije brojeva pokazat ćemo da z nije djeljiv sa 7, ali da x ili y moraju biti djeljivi sa 7. Definiramo nove, relativno proste, manje cijele brojeve a i b. Kreativno birajući vrijednosti za a i b možemo pisati $y^{14} = 7c^2(7^5c^6 + b^2)$ gdje je $c = 7a$. Imajući na umu da prstenovi $\mathbb{Z}[\sqrt{-d}]$, gdje je $d > 0$ kvadratno slobodan, nemaju nužno svojstvo jedinstvene faktorizacije, možemo faktorizirati $b^2 + 7^5c^6$ kao $(b - 7^2c^3\sqrt{-7})(b + 7^2c^3\sqrt{-7})$ te pokazati da su ovo relativno proste četrnaeste potencije. Oduzimanjem ovih četrnaestih potencija dobit ćemo jednadžbu oblika $z^{14} - x^{14}$ te definirati nove varijable a i b. Korištenjem kreativnije algebarske manipulacije četrnaesta potencija oblika $d \pm e\sqrt{-7}$ konačno dovodi do jednadžbe oblika $Z^{14} - X^{14} = 2^4Y^{14}$ gdje je Y djeljivo sa 7. Zatim se proces ponavlja, obraćajući pažnju na 2^4 koji utječe samo na nekoliko koraka računanja. Dokazujemo da ako jednadžba $Z^{14} - X^{14} = 2^kY^{14}$ ima rješenje onda $Z_1^{14} - X_1^{14} = 2^{4+9k}Y_1^{14}$, gdje su Z_1, X_1 i Y_1 manji cijeli brojevi, a Y djeljivo sa 7. Nakon tri ponavljanja dolazimo do druge jednadžbe oblika $Z_2^{14} - X_2^{14} = Y_2^{14}$. Time započinjemo metodu beskonačnog spusta te dolazimo do kontradikcije. Prema tome, jednadžba $x^{14} + y^{14} = z^{14}$ nema rješenje.

4.2.1 Djelitelji brojeva x, y i z.

Pretpostavimo da postoji rješenje jednadžbe $x^{14} + y^{14} = z^{14}$. Pretpostavimo da su x, y i z u parovima relativno prosti prirodni brojevi. Navest ćemo svojstva brojeva x, y i z koja će nam kasnije u dokazu koristiti.

Lema 4.1 *Broj z nije djeljiv brojem 7.*

Dokaz. Dokaz ćemo provesti svođenjem na kontradikciju. Pretpostavimo da $7 \mid z$. Ovo implicira da $7 \mid x^{14} + y^{14}$. Kako je 14 paran broj možemo pisati $7 \mid (x^7)^2 + (y^7)^2$. Neka je $a = x^7$ i $b = y^7$, tada $7 \nmid a$ i $7 \nmid b$, ali $7 \mid a^2 + b^2$ ili $a^2 + b^2 \equiv 0 \pmod 7$. Gledajući sve moguće slučajeve, lako je zaključiti da suma dva kvadrata nije ekvivalentan 0 modulo 7. Brojevi koji nisu djeljivi sa 7 ekvivalentni su s $1, 2, 3, 4, 5, 6$ modulo 7. Kvadratni ostaci modulo 7 su 1, 2 i 4 pa se lako provjeri da zbroj bilo koja dva broja neće biti 7. Prema tome, $7 \nmid z$. ■

Sada ćemo navesti još neka svojstva brojeva x, y i z.

Lema 4.2 *Ako su x, y i z u parovima relativno prosti prirodni brojevi za koje vrijedi da je $z^{14} - x^{14} = y^{14}$ tada jedan od njih mora biti djeljiv sa 7.*

Kako bismo dokazali prethodno navedenu lemu, koristit ćemo sljedeći teorem.

Teorem 4.3 *Neka su x, y i z u parovima relativno prosti prirodni brojevi. Ako za neki prosti broj p Fermatova jednadžba*

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

ima rješenje uz uvjet $p \nmid xyz$, tada je

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

U našem je slučaju $p = 7$. Lako se vidi da $2^6 \not\equiv 1 \pmod{49}$ pa 7 mora dijeliti x, y ili z.

4.2.2 Novi zapis jednadžbe

Nakon određivanja nekih važnih činjenica o rješenju, supstituirat ćemo i faktorizirati rješenje kako bismo dobili pogodniji zapis. Sljedeću lemu navodimo bez dokaza jer nije od velike važnosti za razumijevanje dokaza.

Lema 4.4 *Vrijedi* $z^{14} - x^{14} = a(a^6 + 7b^2)$ *gdje je* $a = z^2 - x^2$ *i* $b = zx(z^4 - z^2x^2 + x^4)$.

Lema 4.5 *Cijeli brojevi* a *i* b *su relativno prosti i različitih parnosti.*

Dokaz. Dokazat ćemo da su a i b relativno prosti svođenjem na kontradikciju. Pretpostavimo da postoji prosti broj p takav da $p \mid a$ i $p \mid b$. Kako $p \mid zx(z^4 - z^2x^2 + x^4)$ znamo da $p \mid z$, $p \mid x$ ili $p \mid z^4 - z^2x^2 + x^4$. Ako $p \mid z$ možemo iskoristiti činjenicu da $p \mid z^2 - x^2$ kako bismo zaključili da $p \mid x$. Ovo je kontradikcija s početnom pretpostavkom da su x i z u parovima relativno prosti. Ako $p \mid x$, slično kao u prethodnom slučaju, dolazimo do kontradikcije. Nadalje, pretpostavimo da $p \mid z^4 - z^2x^2 + x^4$, $p \nmid x$ i $p \nmid z$. Direktnim dokazom pokazat ćemo da ako $p \mid b$ onda $p \nmid a$. Budući da znamo da $p \nmid x^4$ znamo i da $p \nmid z^4 - z^2x^2$. Odnosno, nakon faktoriziranja $p \nmid z^2(z^2 - x^2)$. Ovo znači da $p \nmid z^2$ i $p \nmid z^2 - x^2$. Dakle, ako $p \mid b$ onda $p \nmid a$. Pokazali smo da a i b nemaju zajednički faktor p.

Svođenjem na kontradikciju pokazat ćemo da su a i b različitih parnosti. Najprije, znamo da a i b ne mogu oba biti parni budući da nemaju zajedničkog djelitelja. Pretpostavimo da su a i b neparni brojevi. Znamo da je $z^{14} - x^{14} = a(a^6 + 7b^2)$. Ako su a i b neparni brojevi, tada je $z^{14} - x^{14}$ paran broj. To znači da je y^{14} paran broj, a x^{14} i z^{14} oba neparni. Ako je x^{14} neparan broj, onda je x neparan. Ako su x i y oba neparni, onda je $z^2 - x^2$ paran broj. Međutim, $a = z^2 - x^2$ i po pretpostavci, a je neparan. Dakle, svođenjem na kontradikciju pokazali smo da a i b ne mogu oba biti neparni. Prema tome, a i b su različitih parnosti. ■

Lema 4.6 *Neka je* a *definiran kao prije. Broj* a *je djeljiv sa* 7.

Dokaz. Kako je $y^{14} = a(a^6 + 7b^2)$ i $7 \mid y$, znamo da $7 \mid a(a^6 + 7b^2)$. Iz činjenice da je 7 prost broj, slijedi da $7 \mid a$ ili $7 \mid a^6 + 7b^2$. Budući da $7 \mid 7b^2$,

ako $7 \mid a^6 + 7b^2$ onda $7 \mid a^6$. U svakom slučaju vidimo da $7 \mid a$, a kako su a i b relativno prosti, znamo da $7 \nmid b$. ■

Uvođenjem supstitucije $a = 7c$ u našu jednadžbu dobivamo $y^{14} = 7c(7^6c^6 + 7b^2)$.

4.2.3 Traženje novih četrnaestih potencija

U ovom odjeljku pokazat ćemo da y^{14} možemo zapisati kao produkt dvije četrnaeste potencije. Faktorizacijom se dobije $y^{14} = 7^2c(7^5c^6 + b^2)$. Odnosno, $y^{14} = 7^2c(7(7^2c^3)^2 + b^2)$. Ako je produkt dvaju relativno prostih cijelih brojeva četrnaesta potencija tada je svaki od njih također četrnaesta potencija. Moramo pokazati da su 7^2c i $b^2 + 7(7^2c^3)^2$ relativno prosti.

Lema 4.7 *Neka su c i b definirani kao prije. Vrijednosti 7^2c i $b^2 + 7(7^2c^3)^2$ su relativno proste četrnaeste potencije.*

Dokaz. Dokaz provodimo svođenjem na kontradikciju. Pretpostavimo da je p prost broj takav da $p \mid 7^2c$ i $p \mid b^2 + 7(7^2c^3)^2$. Budući da je $gcd(a, b) = 1$ znamo da je $gcd(7c, b) = 1$ i prema tome $gcd(c, b) = 1$. Također, $7 \nmid b$. Kako $p \mid 7^2c$ znamo da $p \mid 7$ ili $p \mid c$. Ako $p \mid c$ tada $p \mid 7(7^2c^3)^2$. Po pretpostavci $p \mid b^2 + 7(7^2c^3)^2$. Ovo dokazuje da $p \mid b^2$. Međutim, ovo je kontradikcija jer su b i c relativno prosti. U drugom slučaju, $p = 7$. Ako $7 \mid b^2 + 7(7^2c^3)^2$ onda $7 \mid b^2$ jer $7 \mid 7(7^2c^3)^2$. Ovo je također kontradikcija jer znamo da $7 \nmid b$.

Prema tome $gcd(7^2c, b^2 + 7(7^2c^3)^2) = 1$ i zaključujemo da su oba broja četrnaeste potencije. ■

4.2.4 Operacije u prstenu $\mathbb{Z}[\sqrt{-7}]$

Sljedeća lema nužna je za dokaz slučaja $n = 14$, ali njezin dokaz prelazi okvire ovog rada. Važno je napomenuti da zaključci nisu trivijalni jer smo u

prstenu koji ima drukčija svojstva od prstena cijelih brojeva. Pojmovi norma i prosti broj definirani u Potpoglavlju (2.2.2) za prsten $\mathbb{Z}[\sqrt{-3}]$ analogno se definiraju i u prstenu $\mathbb{Z}[\sqrt{-7}]$.

Lema 4.8 *Ako je A^2+7B^2 četrnaesta potencija nekog prirodnog broja i ako $7 \mid B$ onda je $A + B\sqrt{-7} = (a + b\sqrt{-7})^{14}$ za neke cijele brojeve a i b.*

U Lemi 4.7 dokazali smo da je $b^2 + 7(7^2c^3)^2$ četrnaesta potencija. Ovo možemo zapisati kao $b^2 - (-7)(7^2c^3)^2$ te faktorizirati koristeći razliku kvadrata. Dobije se,

$$b^2 - (-7)(7^2c^3)^2 = (b - 7^2c^3\sqrt{-7})(b + 7^2c^3\sqrt{-7}).$$

Neka je $A = b$ i $B = 7^2c^3$. Po Lemi 4.8 znamo da je $b + 7^2c^3\sqrt{-7} = (d + e\sqrt{-7})^{14}$.

4.2.5 Traženje novih četrnaestih potencija (nastavak)

Budući da smo pronašli nove četrnaeste potencije znamo da

$$b + 7^2c^3\sqrt{-7} = (d + e\sqrt{-7})^{14}$$

i

$$b - 7^2c^3\sqrt{-7} = (d - e\sqrt{-7})^{14}.$$

Oduzimanjem ovih dviju jednadžbi dobije se $2 \cdot 7^2c^3\sqrt{-7} = (d+e\sqrt{-7})^{14} - (d - e\sqrt{-7})^{14}$ što možemo zapisati kao $z^{14} - x^{14}$. Pratimo iste korake, ali zamjenimo $z = d + e\sqrt{-7}$ i $x = d - e\sqrt{-7}$. Kao i ranije definiramo $a = z^2 - x^2$ i $b = zx(z^4 - z^2x^2 + x^4)$ ali koristeći supstitucije s d i e. Algebarskim manipulacijama približit ćemo se cilju pronalaska jednadžbe s tri četrnaeste potencije.

Lema 4.9 *Jednadžba* $2 \cdot 7^2c^3\sqrt{-7} = (d + e\sqrt{-7})^{14} - (d - e\sqrt{-7})^{14}$ *može se zapisati kao*

$$7^2c^3 = 2 \cdot de[2^{12}(-7)^3d^6e^6 + 7f^2]$$

gdje je $f = (d^2 + 7e^2)(d^4 - 98d^2e^2 + 49e^4)$.

Dokaz ove leme zahtijeva određene algebarske manipulacije te nije od velike važnosti za razumijevanje dokaza teorema. Jedino na što treba obratiti pažnju kako bi se razumjeli kasniji koraci jest činjenica da je $f = b$.

Lema 4.10 *Cijeli brojevi d, e i f su relativno prosti.*

Dokaz. Pretpostavimo da postoji prosti broj k takav da $k \mid d$ i $k \mid e$. Koristeći Lemu 4.9 vidimo da $k \mid 7^2c^3$. Budući da $k \mid d$ i $k \mid e$ znamo da $k \mid d + e\sqrt{-7}$ dokle god smo u prstenu $Z[\sqrt{-7}]$. Norma ima svojstvo da ako $x \mid z$ u $\mathbb{Z}[\sqrt{-7}]$, onda $N(x) \mid N(z)$ u $\mathbb{Z}$. Kako je $N(k) = k^2$ i $N(b + 7^2c^3\sqrt{-7}) = b^2 + 7^5c^6$ vrijedi da ako $k \mid (d + e\sqrt{-7})^{14} = b + 7^2c^3\sqrt{-7}$, onda $k^2 \mid b^2 + 7^5c^6$. Kako $k \mid 7c^2$ znamo da $k^2 \mid 7^5c^6$ i prema tome $k^2 \mid b^2$. Ovo znači da $k \mid b^2$, a kako je k prost, $k \mid b$. Budući da $7 \nmid b$ znamo da $k \neq 7$ pa $k^2 \mid 7^5c^6$ implicira da $k \mid c$. Ovo je kontradikcija jer su b i c relativno prosti. Prema tome d i e moraju biti relativno prosti. Sada ćemo dokazati da je f također relativno prost s d i e. Pretpostavimo da postoji cijeli broj k takav da $k \mid d$ i $k \mid f$. Ovo povlači da $k \mid d^2 + 7e^2$ ili $k \mid d^4 - 98d^2e^2 + 49e^4$. Kako $k \mid d$ vidimo da $k \mid 7e^2$ ili $k \mid 49e^4$. Znamo da $k \neq 7$ jer $7 \nmid f$. Prema tome $k \mid e$. Već smo pokazali da su d i e relativno prosti, prema tome, došli smo do kontradikcije. ■

Lema 4.11 *Cijeli brojevi d i e su različitih parnosti, a f je neparan broj.*

Dokaz. Brojevi d i e povezani su s b i c jednadžbom $b + 7^2c^3\sqrt{-7} = (d + e\sqrt{-7})^{14}$. Znamo da su b i c relativno prosti i različitih parnosti. Ako su d i

e oba parna, onda je $b + 7^2c^3\sqrt{-7}$ paran, a b i c su iste parnosti. Ako su d i e oba neparna, onda je $b + 7^2c^3\sqrt{-7}$ paran i dođemo do iste kontradikcije. Sada ćemo ispitati broj f. Ako pretpostavimo da je d paran, a e neparan broj, vidjet ćemo da je f produkt neparnih brojeva, odnosno, f je neparan. Kad zamijenimo parnosti od d i e vidimo da je f još uvijek neparan. Znamo da $7 \nmid f$ jer smo definirali $f = b$ u gornjoj jednadžbi i znamo da $7 \nmid b$. ■

4.2.6 Novi relativno prosti faktori

Dijeleći izraz u Lemi 4.9 sa -7 dobijemo

$$7^2c^3 = 2 \cdot 7de[f^2 - (2^6 7d^3e^3)^2)].$$

Ovaj se izraz može rastaviti kao produkt triju faktora, $2 \cdot 7de$ i $f \pm 2^6 7d^3e^3$. Već smo pokazali da su d, e i f relativno prosti te da su d i e različitih parnosti. Sada ćemo pokazati da su ovi faktori također relativno prosti.

Lema 4.12 *Brojevi $f + 2^6 7d^3e^3$ i $f - 2^6 7d^3e^3$ su relativno prosti.*

Dokaz. Tvrdnju ćemo dokazati svođenjem na kontradikciju. Pretpostavimo da $k \mid f + 2^6 7d^3e^3$ i $k \mid f - 2^6 7d^3e^3$, gdje je k prost broj. Prema tome, k dijeli zbroj i razliku navedenih izraza, odnosno $k \mid 2f$ i $k \mid 2^7 7d^3e^3$. Najprije primijetimo da su $f + 2^6 7d^3e^3$ i $f - 2^6 7d^3e^3$ neparni pa je $k \neq 2$. Dakle, $k \mid f$ i $k \mid 7d^3e^3$. Prije smo pokazali da je $f = b$ i da b nije djeljivo sa 7. Iz toga slijedi $k \neq 7$ i $k \mid e^3$ ili $k \mid d^3$. Ovo znači da k dijeli f i također e ili d. Međutim, ovo je kontradikcije jer su f, d i e u parovima relativno prosti. ■

Lema 4.13 *Brojevi $2 \cdot 7d$ i $f \pm 2^6 7d^3e^3$ su u parovima relativno prosti.*

Dokaz. Tvrdnju ćemo dokazati svođenjem na kontradikciju. Pretpostavimo da $k \mid 2 \cdot 7de$ i $k \mid f \pm 2^6 7d^3e^3$. Ovo implicira da $k \mid 2 \cdot 7de$ i $k \mid f \pm 2^6 7d^3e^3$.

Znamo da $k \neq 2$ jer je $f \pm 2^6 7d^3e^3$ neparan. Kako $k \mid 2 \cdot 7de$ znamo da $k \mid 2^6 7d^3e^3$ i prema tome $k \mid f$. Kao i ranije, znamo da $7 \nmid f$ pa $k \neq 7$. Dakle, $k \mid 7de$ implicira da $k \mid d$ ili $k \mid e$. Ovo je kontradikcija jer su f, d i e u parovima relativno prosti. ■

Koristeći ove leme i nekoliko koraka algebarskih manipulacija, pronaći ćemo nove četrnaeste potencije.

Lema 4.14 *Postoje cijeli brojevi Z i X takvi da je $Z^{14} = f + 2^6 \cdot 7d^3e^3$ i $X^{14} = f - 2^6 \cdot 7d^3e^3$. Primijetimo da je $Z^{14} - X^{14} = 2^7 \cdot 7d^3e^3$, gdje je $2 \cdot 7^5de$ četrnaesta potencija.*

Dokaz. Znamo da je

$$7^2c^3 = (2 \cdot 7de)(f \pm 2^6 7d^3e^3).$$

Množeći obje strane sa 7^4 dobije se $7^6c^3 = (2 \cdot 7^5de)(f \pm 2^6 \cdot 7d^3e^3)$. Prisjetimo se da je 7^2c četrnaesta potencija i primijetimo da jednadžbu možemo zapisati u obliku $(7^2c)^3 = (2 \cdot 7^5de)(f \pm 2^6 \cdot 7d^3e^3)$. Znamo da izrazi $f \pm 2^6 \cdot 7d^3e^3$ nisu djeljivi sa 7 jer su relativno prosti s $2 \cdot 7de$. Prema tome, faktori $2 \cdot 7^5de$ i $f \pm 2^6 7d^3e^3$ su relativno prosti i oba moraju biti četrnaeste potencije.

Neka je $Z^{14} = f + 2^6 \cdot 7d^3e^3$ i $X^{14} = f - 2^6 \cdot 7d^3e^3$. Primijetimo da je $Z^{14} - X^{14} = 2^7 \cdot 7d^3e^3$. ■

Znamo da je $2 \cdot 7^5de$ četrnaesta potencija. Ako taj izraz kubiramo, on je još uvijek četrnaesta potencija. Vidjet ćemo da je $2^3 \cdot 7d^3e^3 \cdot 7^{14}$ četrnaesta potencija i prema tome je $2^3 \cdot 7d^3e^3$ također četrnaesta potencija. Dakle, $2^7 \cdot 7d^3e^3$ je produkt od 2^4 i četrnaeste potencije. Ove ćemo činjenice koristiti u metodi beskonačnog spusta.

Pronašli smo rješenje jednadžbe $Z^{14} - X^{14} = 2^4Y^{14}$ gdje je $Z = f + 2^6 \cdot 7d^3e^3$ i $X = f - 2^6 \cdot 7d^3e^3$. Počevši od ove jednadžbe, ponovit ćemo postupak

kako bismo pronašli rješenje jednadžbe $Z_1^{14} - x_1^{14} = 2^{12}Y_1^{14}$. Ponavljajući postupak još tri puta dolazimo do druge jednadžbe oblika $x^{14} + y^{14} = z^{14}$.

4.2.7 Ponovno provođenje dokaza

Lema 4.15 *Brojevi X, Y i Z koji zadovoljavaju $Z^{14} - X^{14} = 2^4Y^{14}$ su u parovima relativno prosti.*

Dokaz. Prvo ćemo utvrditi da su Z i X neparni kako bismo lakše riješili problem dodavanja 2^4 u jednadžbu. Znamo da je $Z = f + 2^6 \cdot 7d^3e^3$ te da je f neparan. Dakle, Z mora biti neparan. Koristeći isti argument vidimo da je X također neparan. Pretpostavimo da Z i X imaju zajednički faktor k. Znamo da k nije paran. Ako $k \mid Z$ i $k \mid X$ tada znamo da $k \mid Z^{14} - X^{14}$ pa $k \mid Y^{14}$. Prema tome, mogli bismo podijeliti jednakost s k kako bi ostale u parovima reativno proste varijable. Ako k dijeli Z i Y, ili, ako k dijeli X i Y može se pokazati, s istim argumentu, da k dijeli i treću varijablu te da se može izlučiti. ■

Pokazali smo ranije da je $2^4Y^{14} = 2^7d^3e^3$. Pokazat ćemo da $7 \mid Y$. Znamo da $7 \nmid Z$ ili X jer $7 \nmid f$ i $Z, X = f \pm 2^6 \cdot 7d^3e^3$. Prema tome, znamo da $7 \mid Y$.

Lema 4.16 *Ako je $z^{14} - x^{14} = 2^k y^{14}$, $(k \geq 0)$ onda je $Z^{14} - X^{14} = 2^{4+9k}Y^{14}$ gdje $7 \mid Y$.*

Dokaz. Kao i ranije, možemo pisati $Z^{14} - X^{14} = a(a^6 + 7b^2)$ gdje su a i b relativno prosti i različitih parnosti. Sljedeću ćemo jednadžbu malo modificirati. Ako pomnožimo obe strane jednadžbe $7^2c(b^2 + 7(7^2c^3)^2) = 2^4Y^{14}$ s 2^{10} možemo zaključiti da su $2^{10}7^2c$ i $b^2 + 7(7^2c^3)^2$ relativno prosti. Primijetimo da je c paran, a kako je relativno prost s $b^2 7(7^2c^3)^2$ znamo da množenjem 2^{10} sa 7^2c ne mijenja zaključak da su brojevi relativno prosti. Faktorizira-

njem izraza $b^2 7(7^2c^3)^2$ na isti način kao i ranije, dolazimo do zaključka da je $7^2c^3 = 2 \cdot 7 \cdot de(f \pm 2^6 \cdot 7d^3e^3)$ gdje su faktori u parovima relativno prosti.

Dokaz se sada djelomično mijenja. Ovaj put koristimo činjenicu da je $2^{10}c^2$ četrnaesta potencija. Ovo implicira da je $2^{30}7^6c^3$ također četrnaesta potencija. Množenjem obe strane jednadžbe $7^2c^3 = 2 \cdot 7 \cdot de(f \pm 2^6 \cdot 7d^3e^3)$ s $2^{30}7^4$ dobije se

$$2^{10}7^6c^3 = 2^{31} \cdot 7^5 \cdot de(f \pm 2^6 \cdot 7d^3e^3).$$

Ovi su brojevi relativno prosti pa znamo da je $2^3 7^5 de$ 14-a potencija. Dakle, $2^9 \cdot 7^{15}d^3e^3$ je 14-a potencija i $2^7 \cdot 7d^3e^3$ je, s jedne strane, razlika 14-ih potencija, a s druge, umnožak 2^{12} i 14-e potencije. Dakle, pronašli smo rješenje jednadžbe $Z_1^{14} - X_1^1 = 2_1^{12}14$ gdje $7 \mid Y_1$. Radeći istu stvar još jedanput pronalazimo rješenje jednadžbe $X_2 + Y_2 = Z_2$ te uspostavljamo beskonačni spust. Možemo nastaviti ovaj proces kako bismo pokazali da općenito jednadžba $z^{14} - x^{14} = 2^k y^{14}$, $(k \geq 0)$ dovodi do $Z^{14} - X^{14} = 2^{4+9k}Y^{14}$ gdje $7 \mid Y$. Novi brojevi X, Y i Z su po definiciji mnogo manji. Dakle, pokazali smo metodom beskonačnog spusta da jednadžba $z^{14} - x^{14} = 2^k y^{14}$ nema rješenje. ■

4.3 Sažetak

Iako je dokaz slučaja $n = 14$ dug i monoton, on zapravo dijeli strukturu dokaza sa slučajevima $n = 3$ i $n = 5$. Mnogo je teži od dokaza slučaja $n = 4$ jer se uvode kompleksni prstenovi. Uspoređujući dokaze za slučajeve $n = 3$, $n = 5$ i $n = 14$ možemo naslutiti poteškoće pri generaliziranju dokaza te korištenju metode beskonačnog spusta kako bi se dokazao Fermatov Posljednji teorem. Iako dokazi imaju određenih sličnosti, račun svakog od njih je različit i zahtijeva znatnu dozu kreativnosti. Ovakvi pristupi ne dovode do

dokaza općenitog slučaja. Sophie Germain je uspjela postići značajan napredak dokazujući Fermatov Posljednji teorem za cijelu jednu klasu brojeva, ali je to još uvijek bilo daleko od potpunog dokaza. Zapravo, opći dokaz Fermatovog Posljednjeg teorema koristi mnogo naprednije i modernije tehnike koje su izvan okvira ovog rada. On se temelji, ne na metodi beskonačnog spusta, već koristi moderne teoreme o eliptičkim krivuljama i modularnim formama. Postoje objašnjenja ovog dokaza na nekoliko razina matematičke složenosti, ali njihovo razumijevanje u cijelosti je veliki matematički podvig.

Literatura

[1] Alkalay-Houlihan, Colleen. Sophie Germain and Special Cases of Fermat's Last Theorem.

[2] Byerley, Cameron (2006). Applications of Number Theory to Fermat's Last Theorem.

[3] Conrad, Brian; Landesman Aron. Math 154. Algebraic number theory. URL: http://virtualmath1.stanford.edu/∼conrad/154Page/handouts/undergraduate-number-theory.pdf (25.09.2019.)

[4] Dujella, Andrej. Uvod u teoriju brojeva. Skripta. PMF - Matematički odjel Sveučilišta u Zagrebu.

[5] Edwards, Harold M. (1977). Fermat's Last Theorem. A Genetic Introductioon to Algebraic Number Theory. Springer-Verlag, New York.

[6] Ribenboim, Paulo (1979). 13 Lectures on Fermat's Last Theorem. Springer-Verlag, New York.

TEMELJNA DOKUMENTACIJSKA KARTICA

PRIRODOSLOVNO–MATEMATIČKI FAKULTET
SVEUČILIŠTA U SPLITU
ODJEL ZA MATEMATIKU

DIPLOMSKI RAD

SLUČAJEVI FERMATOVOG POSLJEDNJEG TEOREMA DOKAZIVI ELEMENTARNIM METODAMA

Ivona Alković

Sažetak:

U ovom diplomskom radu predstavljeni su odabrani slučajevi Fermatovog Posljednjeg teorema. Prvo poglavlje ukratko predstavlja osnovne pojmove potrebne za razumijevanje problema te dokaz slučaja $n = 4$. Drugo poglavlje bavi se slavnim matematičarem Leonhardom Eulerom i njegovim dokazom slučaja $n = 3$. Treće poglavlje posvećeno je francuskoj matematičarki Sophie Germain dok se u zadnjem poglavlju govori se o slučajevima $n = 7$ i $n = 14$.

Ključne riječi:

Metoda beskonačnog spusta, Pitagorina trojka, Savršeni brojevi, Eulerova pogreška.

Podatci o radu:

48 stranica, 4 tablice, 6 literaturnih navoda, jezik izvornika: hrvatski

Mentorica: *doc. dr. sc. Marija Bliznac Trebješanin*

Članovi povjerenstva:

prof. dr. sc. Borka Jadrijević

Ivan Jelić, mag. math

Povjerenstvo za diplomski rad je prihvatilo ovaj rad *30.09.2019.*

TEMELJNA DOKUMENTACIJSKA KARTICA

FACULTY OF SCIENCE, UNIVERSITY OF SPLIT

DEPARTMENT OF MATHEMATICS

MASTER'S THESIS

CASES OF FERMAT'S LAST THEOREM PROVABLE BY ELEMENTARY METHODS

Ivona Alković

Abstract:

This thesis presents selected cases of Fermat's Last Theorem. The first chapter briefly presents the basic concepts needed to understand the problem and the proof of the case $n = 4$. The second chapter deals with the famous mathematician Leonhard Euler and his proof of the case $n = 3$. The third chapter deals with the French mathematician Sophie Germain while the last chapter deals with cases $n = 7$ and $n = 14$.

Key words:

Infinite Descent Method, Pythagoras Three, Perfect Numbers, Euler Error.

Specifications:

48 pages, 4 tables, 6 literary quotes, original language: Croatian

Mentor: *assisstant professor Marija Bliznac Trebješanin*

Committee:

professor Borka Jadrijević

Ivan Jelić, mag. math

This thesis was approved by a Thesis committee on *30.09.2019.*