Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Diplomski studij financijske i poslovne matematike

Iva Ivanković

Veliki Fermatov teorem

Diplomski rad

Osijek, 2011.

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Diplomski studij financijske i poslovne matematike

Iva Ivanković

Veliki Fermatov teorem

Diplomski rad

Voditelj: doc. dr. sc. Ivan Matić

Osijek, 2011.

Sadržaj

Uvod

Godine 1637. pravnik Pierre de Fermat je na margini knjige napisao bilješku danas poznatu kao Veliki Fermatov teorem. Tvrdio je da zna dokazati svoju slutnju no nije ostavio nikakav pisani trag. Teorem je, nakon više od tristo godina bezuspješnog pokušavanja, napokon dokazan 1994. godine. U ovom diplomskom radu je predstavljen Veliki Fermatov teorem.

Prvo poglavlje ukratko predstavlja osnovne pojmove teorije brojeva potrebne za razumjevanje problema i dokazivanje posebnih slučajeva Velikog Fermatovog teorema. Navedene su osnovne definicije i teoremi (bez dokaza).

Drugo poglavlje kronološki prikazuje razvoj problema, od početaka razmatranja u kulturi Babilonaca. Opisan je rad Starogrčkih i srednjovjekovnih matematičara na polju usko vezanom uz Veliki Fermatov teorem, iznesene su osnovne povjesne činjenice iz Fermatova života i dan je kratak pregled njegovih postignuća u matematici. Istaknuti su najznačajniji matematičari koji su dali doprinos dokazivanju teorema te je okvirno prikazan rad Andrewa Wilesa i dokaz Velikog Fermatovog teorema.

Zadnji dio predstavlja posebne slučajeve Velikog Fermatovog teorema. Prikazan je iskaz i dokaz Pitagorinog poučka i način pronalaska Pitagorinih trojki. Detaljno je objašnjena Fermatova metoda beskonačnog silaska, potrebna za dokazivanje posebnih slučajeva teorema. Navedeni su precizni dokazi posebnih slučajeva Velikog Fermatovog teorema kada je $n = 4, 3$ i 5, što je i najvažniji dio ovog rada.

1. Osnovni pojmovi teorije brojeva

Definicija 1.1 *Neka su $a \neq 0$ i b cijeli brojevi. Kažemo da je b djeljiv s a, odnosno da a dijeli b, ako postoji cijeli broj x takav da je $b = ax$. To zapisujemo sa $a \mid b$. 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. Oznaka $a^k \parallel b$ će nam značiti da $a^k \mid b$, ali $a^{k+1} \nmid b$.

Teorem 1.1 (Teorem o dijeljenju s ostatkom)
Za proizvoljan prirodan broj a i cijeli broj b postoje jedinstveni cijeli brojevi q i r takvi da je $b = qa + r$, $0 \leq r < a$.

Definicija 1.2 *Neka su b i c cijeli brojevi. Cijeli broj a zovemo* zajednički djelitelj *od b i c ako $a \mid b$ 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 se 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 je $(b, c) \geq 1$.

Definicija 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 $(a_i, a_j) = 1$ za sve $1 \leq i, j \leq n$, $i \neq j$.*

Propozicija 1.1 *Ako je $(a, m) = (b, m) = 1$, onda je $(ab, m) = 1$.*

Definicija 1.4 *Prirodan broj $p > 1$ s zove* prost *ako 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 1.2 *Svaki prirodan broj $n > 1$ može se prikazati kao produkt prostih brojeva (s jednim ili više faktora).*

Propozicija 1.2 (Euklid) *Ako je p prost i $p \mid ab$, onda $p \mid a$ ili $p \mid b$. Općenitije, ako $p \mid a_1 a_2 \cdots a_n$, onda p dijeli barem jedan faktor a_i.*

Teorem 1.3 (Osnovni teorem aritmetike)
Faktorizacija svakog prirodnog broja $n > 1$ na proste faktore je jedinstvena do na poredak prostih faktora.

Definicija 1.5 *Neka su $a_1, a_2, \ldots, a_n$ cijeli brojevi različiti od nule. Najmanji prirodan broj c za koji vrijedi da $a_i \mid c$ za sve $i = 1, 2, \ldots, n$ zove se* najmanji zajednički višekratnik *i označava s $[a_1, a_2, \ldots, a_n]$.*

Teorem 1.4 (Euklid)
Skup svih prostih brojeva je beskonačan.

Definicija 1.6 *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 $a \not\equiv b \pmod{m}$.*

Propozicija 1.3 *Relacija "biti kongruentan " je relacija ekvivalencije na skupu $\mathbb{Z}$.*

Propozicija 1.4 *Neka je f polinom s cjelobrojnim koeficijentima. Ako je $a \equiv b \pmod{m}$, onda je $f(a) \equiv f(b) \pmod{m}$.*

Teorem 1.5 *Vrijedi: $ax \equiv ay \pmod{m}$ ako i samo ako $x \equiv y \pmod{\frac{m}{(a,m)}}$. Specijalno, ako je $ax \equiv ay \pmod{m}$ i $(a, m) = 1$, onda je $x \equiv y \pmod{m}$.*

Definicija 1.7 *Skup $\{x_1, \ldots, x_m\}$ se zove* potpuni sustav ostataka *modulo m ako za svaki $y \in \mathbb{Z}$ postoji točno jedan x_j takav da je $y \equiv x_j \pmod{m}$. Drugim riječima, potpuni sustav ostataka dobivamo tako da iz svake klase ekvivalencije modulo m uzmemo po jedan član.*

Teorem 1.6 *Neka je $\{x_1, \ldots, x_m\}$ potpuni sustav ostataka modulo m te neka je $(a, m) = 1$. Tada je $\{ax_1, \ldots, ax_m\}$ također potpuni sustav ostataka modulo m.*

Teorem 1.7 *Neka su a i m prirodni te b cijeli broj. Kongruencija $ax \equiv b \pmod{m}$ ima rješenja ako i samo ako $d = (a, m)$ dijeli b. Ako je ovaj uvjet zadovoljen, onda gornja kongruencija ima točno d rješenja modulo m.*

Definicija 1.8 *Reducirani sustav ostataka modulo m je skup cijelih brojeva r_i sa svojstvom da je $(r_i, m) = 1$, $r_i \not\equiv r_j (\mathrm{mod}\, m)$ i da za svaki cijeli broj x takav da je $(x, m) = 1$ postoji r_i takav da je $x \equiv r_i (\mathrm{mod}\ m)$. Jedan reducirani sustav ostataka modulo m je skup svih brojeva $a \in \{1, 2, \ldots, m\}$ takvih da je $(a, m) = 1$. Jasno je da svi reducirani sustavi ostataka modulo m imaju isti broj elemenata. Taj broj označavamo s $\varphi(m)$, a funkciju φ zovemo Eulerova funkcija. Drugim riječima, $\varphi(m)$ je broj brojeva u nizu $1, 2, \ldots, m$ koji su relativno prosti sa m.*

Teorem 1.8 (Euler) *Ako je $(a, m) = 1$, onda je $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\ m)$.*

Teorem 1.9 (Mali Fermatov teorem) *Neka je p prost broj. Ako $p \nmid a$, onda je $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$. Za svaki cijeli broj a vrijedi $a^p \equiv (\mathrm{mod}\ p)$*

Teorem 1.10 (Wilson) *Ako je p prost broj, onda je $(p-1)! \equiv -1 (\mathrm{mod}\ p)$.*

Teorem 1.11 *Neka je p prost broj. Tada kongruencija $x^2 \equiv -1 (\mathrm{mod}\ p)$ ima rješenje ako i samo ako je $p = 2$ ili $p \equiv 1 (\mathrm{mod}\ 4)$.*

Lema 1.1 *Ako je:*

$$\begin{aligned} t &= q^4 + 50q^2r^2 + 125r^4 \\ u &= q^2 + 25r^2 \\ v &= 10r^2 \end{aligned}$$

Onda vrijedi:

$$t = u^2 - 5v^2,$$

(1) $u^2 = (q^2 + 25r^2)^2 = q^4 + 50q^2r^2 + 625r^4$

(2) $-5v^2 = -5(10r^2)^2 = -500r^4$

(3) $(q^2 + 25r^2)^2 - 5(10r^2)^2 = q^4 + 50q^2r^2 + 625r^4 - 500r^4 = q^4 + 50q^2r^2 + 125r^4$

Lema 1.2

$$(p+q)^5 + (p-q)^5 = 2p(p^4 + 10p^2q^2 + 5q^4)$$

Lema 1.3 *Neka su a, b cijeli brojevi koji zadovoljavaju:*

(1) $(a, b) = 1$,

(2) a, b *su suprotne parnosti,*

(3) 5 *ne dijeli* a,

(4) 5 *dijeli* b,

(5) $(a^2 - 5b^2)$ *je peta potencija.*

Tada postoje cijeli brojevi c, d sa svojstvima:

(1) $a = c(c^4 + 50c^2d^2 + 125d^4)$,

(2) $b = 5d(c^4 + 10c^2d^2 + 5d^4)$,

(3) $(c, d) = 1$,

(4) c, d *su suprotnih parnosti,*

(5) 5 *ne dijeli* c,

(6) 5 *dijeli* d,

(7) c, d *su oba različiti od 0.*

Lema 1.4 *Neka su a, b cijeli brojevi takvi da:*

(1) $(a, b) = 1$,

(2) a, b *su neparni,*

(3) 5 *ne dijeli* a*,*

(4) 5 *dijeli* b*,*

(5) $(a^2 - 5b^2)/4$ *je peta potencija.*

Tada postoje cijeli brojevi c, d *sa svojstvima:*

(1) $a = c(c^4 + 50c^2d^2 + 125d^4)/16$*,*

(2) $b = 5d(c^4 + 10c^2d^2 + 5d^4)/16$*,*

(3) $(c, d) = 1$*,*

(4) c, d *su neparni,*

(5) 5 *ne dijeli* c*,*

(6) 5 *dijeli* d*,*

(7) c, d *su oba različiti od 0.*

2. Povijesni razvoj problema

U ovom poglavlju se nalazi kronološki pregled razvoja problema kojeg je Fermat postavio, počevši od brončanog doba i kulture Babilonaca pa sve do Andrewa Wilesa koji je uspješno dokazao teorem 1994. godine.

2.1. Povijest problema do Fermata

2.1.1. Babilonsko razdoblje

Razmatranje Fermatova problema se pojavljuje znatno prije samog Fermata. Korijeni ovog naizgled bezazlenog teorema su stari koliko i sama civilizacija. Oni sežu sve do kulture brončanoga doba koja se razvijala u području između rijeka Eufrat i Tigris u starom Babilonu (današnji Irak). Babilonskim dobom se smatra razdoblje u Mezopotamskoj dolini od dvije tisuće godina do šest stotina godina prije nove ere. Tada je došlo do izuzetnog kulturnog razvoja koji je obuhvaćao umijeće pisanja, korištenje kotača i obrađivanje metala te sustav kanala za navodnjavanje zemljišta između dvaju rijeka. Kako je to područje bogato glinom, za zapisivanje se koristio klinasti zapis. Stilusom su urezivali klinaste zapise u glinene pločice koje su kasnije sušili na suncu. Ta vrsta zapisa je dobila naziv klinasto pismo po obliku ureza u glini i prvo je poznato svjetsko pismo. Kako se u Babilonu razvijala trgovina i graditeljstvo, javila se potreba za točnim mjerenjima. Ljudi iz tog doba su naučili kako odrediti odnos između opsega i promjera kruga, dobivši tako broj blizak onome što ga mi danas nazivamo π. Podigli su divovski Zigurat, biblijsku Babilonsku kulu i Semiramidine Viseće vrtove, jedno od sedam čuda staroga svijeta, tako da su morali ovladati vještinom izračunavanja površina i opsega. Razvijen je složeni heksagezimalni brojevni sustav s bazom šezdeset, što je omogućilo babilonskim inžinjerima i građevinarima da izračunavaju vrijednosti koje su im bile potrebne u svakodnevnom poslu. Kvadrati brojeva su se javljali prirodno, iako to nije očigledno, mogu se vidjeti kao znamenja bogatstva. Dobrobit nekog ratara ovisi o tome koliko je žitarica u stanju proizvesti. Prinos žitarica, sa svoje strane, ovisi o površini zemljišta kojom ratar raspolaže. Površina je umnožak duljine i širine polja pa se tu pojavljuju kvadrati. Polje čije i dužina i širina iznose a ima površinu jednaku a^2, odnosno a puta a. U tom smislu, bogatstvo je kvadratno svojstvo. Babilonci su željeli znati kada se ti kvadrati cijelih brojeva mogu podijeliti na druge kvadrate cijelih brojeva. Ratar koji je imao polje od dvadeset pet kvadratnih jedinica zemljišta mogao ga je mijenjati za dva druga, također kvadratna polja: jedno koje je imalo šesnaest kvadratnih jedinica i drugo od devet kvadratnih jedinica. Dakle, polje koje bi imalo veličinu pet puta pet nekih jedinica imalo je jednaku površinu kao zbroj polja od četiri puta četiri i tri puta tri jedinice, to je bila važna informacija za rješenje praktičnog problema. Danas bismo ovaj odnos napisali u obliku sljedeće jednadžbe: $5^2 = 4^2 + 3^2$. Trojke ovakvih cijelih brojeva, u ovom slučaju 3, 4, i 5, čiji kvadrati zadovoljavaju postavljeni uvjet, nazivamo *Pitagorine trojke* - iako se za njih znalo u

Babilonu, više od tisuću godina prije Pitagore po kojem su dobile naziv. Ove informacije su poznate iz jedne glinene pločice koja potječe približno iz 1900.p.n.e. Pločica se nalazi na sveučilištu Columbia u SAD-u, dobila je naziv Plimpton 322. Sve što ona sadržava jest 15 trojki brojeva. Svaka od trojki se odlikuje istim svojstvom: prvi broj je kvadrat i on je zbroj druga dva koji su također kvadrati - radi se o Pitagorinim trojkama. Postoje različita mišljenja oko toga što je stare Babilonce zainteresiralo za ove brojeve. Prema jednoj teoriji, iza svega su stajale isključivo praktične potrebe. Činjenica da su koristili heksagezimalni sustav, čime je dana prednost cijelim brojevima u odnosu na razlomke, ide u prilog potrebama rješavanja praktičnih problema pomoću kvadrata brojeva. Prema drugim teorijama, Plimpton 322 je pomoćno sredstvo upućivanja učenika u brojeve koji su savršeni kvadrati. Smatra se da Babilonci nisu uspjeli riješiti ovaj problem nekom metodom, samo su nagađali koji brojevi imaju zadana svojstva.

2.1.2. Antička Grčka

Pitagora sa otoka Samosa (570.-500. p.n.e.) je surađivao sa većinom matematičara tog vremena pa tako i Babiloncima. Upoznat je sa babilonskim proučavanjem brojeva koji su kasnije po njemu nazvani Pitagorine trojke. Tijekom putovanja na Pitagoru su utjecale religijske i filozofske ideje Istoka. Živio je u Krotoni (današnja Italija), gdje je osnovao tajno društvo posvećeno proučavanju brojeva. Smatra se da je to društvo, čiji se članovi nazivaju pitagorejci, ostvarilo mnoga matematička znanja, ali sve u potpunoj tajnosti. Pitagorejci su bili poklonici brojeva, smatrali su da brojevi imaju magična svojstva, njihova zaokupljenost brojevima je nalikovala religiji. Već tada su poznavali osim cijelih i racionalne i iracionalne brojeve no sve su to držali u tajnosti. Prema predaji, Pitagora je vlastitim rukama utopio onog člana koji je obznanio svijetu postojanje iracionalnih brojeva. Iako do danas nisu pronađeni nikakvi dokumenti iz vremena Pitagore, postoji opsežna kasnija literatura o učitelju i njegovim sljedbenicima, a sam Pitagora smatra se jednim od najvećih matematičara antike. Njemu se pripisuje otkriće Pitagorinog poučka, koji se odnosi na stranice pravokutnog trokuta i u bliskoj je vezi sa Pitagorinim trojkama, a u konačnici i sa Velikim Fermatovim teoremom. Iskaz i dokaz Pitagorinog poučka je dan u trećem poglavlju (teorem 3.1).
Matematičar po imenu Diofant je oko 250.p.n.e. živio u Aleksandriji. Napisao je djelo *Aritmetika* u kojem su izložene temeljne algebarske postavke, a i uveden je jedan poseban tip jednadžba, jednadžbe s više nepoznanica kojima se traže cjelobrojna rješenja. Po njemu su dobile naziv *diofantske jednadžbe*. Stoga je $x^n + y^n = z^n$ diofantska jednadžba. Od petnaest napisanih knjiga do našeg je vremena ostalo samo šest. Očuvane Diofantove knjige su među posljednjim prevedenim grčkim tekstovima. Prvi poznati prijevod na latinski je objavljen 1575., no primjerak koji je posjedovao Fermat je pripadao izdanju u prijevodu Claudea Bacheta[1] iz 1621. Upravo je Diofantov problem 8

[1]Claude Gaspard Bachet de Méziriac, 1581.-1638., francuski matematičar, lingvist i pjesnik

iz druge knjige, u sklopu kojeg se traži da se dani kvadrat prikaže kao zbroj dva druga kvadrata, nadahnuo Fermata da na margini stranice napiše svoj Veliki teorem.

2.1.3. Srednji vijek

U razdoblju srednjeg vijeka najveći napredak u matematici se dogodio u arapskim državama. Arapi su upijali matematičke ideje stanovnika sa područja koja su osvajali. Bagdad je bio znanstveni centar arapskog svijeta, tamo je osnovana *Kuća mudrosti* gdje se prevode djela najvećih matematičara antičkog doba. Najznačajniji matematičar toga vremena je Abu Abdallah Muhammad Ibn Al-Magusi Al-Hwarizmi Al-Choresmi (787.-850.). Riječ "algoritam" je izvedena iz njegova imena, dok je riječ "algebra" izvedena iz prvih riječi naslova Al-Hwarizmijeve najpoznatije knjige *Al jabr wa'l mugabalah*. Iako se algebarske zamisli nalaze i u Diofantovoj *Aritmetici*, *Al jabr* stoji u znatno bližoj vezi s današnjom algebrom. Al-Hwarizmi se posebno bavio kvadratnom jednadžbom te problemom usko vezanim sa Diofantovo pitanje pronalaska Pitagorinih trojki: *Kako pronaći Pitagorine trojke ako je poznata površina pravokutnog trokuta koja je cjelobrojna.* Stotinama godina kasnije ovaj problem se pojavio kao temelj knjizi *Liber Quadratorum* koju je 1225. napisao Leonardo iz Pise (1180. - 1250.), poznatiji pod imenom Fibonacci. Glavna zadaća tadašnje algebre bila je pronaći rješenje jednadžbi u kojima se javlja neka nepoznata veličina. Matematičari tog doba se nazivaju *kosisti*, od talijanske riječi *cosa* (tal. cosa = stvar) jer su tragali za nepoznatom "stvari" u jednadžbama. Glavni predstavnici tog doba su Luca Pacioli (1445. - 1514.), Geronimo Cardano (1501. - 1576.) i Niccolo Tartagali (1500. - 1577.), oni su se međusobno nadmetali kao rješavatelji problema u službi obrtnika i trgovaca, a rješenja nekih apstraktnijih problema, kao npr. pronalazak načina rješavanja jednadžbe trećeg stupnja, su koristili kao oblik vlastite promidžbe. Kosisti su smatrani matematičarima niže razine u odnosu na antičke Grke, njihova zaokupljenost praktičnim problemima te posvećenost stjecanju financijske dobiti sprječavali su ih u potrazi za ljepotom u matematici, kao i za stjecanjem znanja zbog samog znanja.

2.2. Pierre de Fermat

Pierre de Fermat je bio francuski pravnik, ali je više zapamćen po svojim matematičkim rezultatima. Rođen je 17. kolovoza 1601. u francuskom gradu Beaumont-de-Lomagne (blizu Toulusea). Umro je u Castresu, također nedaleko Toulusea, 12. siječnja 1665. Fermat je rođen u uglednoj trgovačkoj obitelji, podatak o osnovnom obrazovanju nije pouzdan, ali je to vjerojatno bio lokalni franjevački samostan. Studij je započeo u Toulouseu, nastavio u Bordeauxu, a završio u Orleansu, gdje je diplomirao građansko pravo te 1631. postao član parlamenta u Toulouseu. Bio je poznat kao točan i pouzdan u poslu te uglađen i korektan u komunikaciji. Još za vrijeme studija u Bordeauxu se počeo baviti matematičkim problemima i iz tog doba potječu njegovi prvi rezultati

o ekstremima funkcija. Svoj život je proveo uglavnom u Toulouseu no povremeno je radio u rodnom gradu te u Castresu. Tijekom svog rada u parlamentu postepeno je napredovao do viših pozicija te je 1652. dosegao najviši mogući položaj na kaznenom sudu. Za sve vrijeme svoje pravno-političke djelatnosti, Fermat se u slobodno vrijeme bavio matematikom. Povjesničar matematike, E. T. Bell je nazvao Fermata *Princem amatera*. Neovisno o suvremeniku Descartesu[2] je otkrio analitičku geometriju, a zajedno sa Pascalom[3] je postavio temelje teoriji vjerojatnosti. Bavio se optikom, a njegovi radovi vezani za tangente na krivulje i ekstreme funkcija su bitni prethodnici za otkriće diferencijalnog računa. U to vrijeme je smatran jednim od najvećih matematičara u Europi. Danas je njegovo ime sinonim za teoriju brojeva, ali tada je njegov rad u teoriji brojeva bio toliko ispred svoga vremena da mu je vrijednost bila slabo shvaćena, tako da je Fermatova popularnost ležala u doprinosima ostalim poljima. Njegova reputacija je rasla znatno više od učenih matematičara, mnogo puta se od njega tražilo da objavi svoja djela no to je uvijek odbijao. Neka njegova otkrića, pogotovo u teoriji brojeva, nikad nisu objavljena. S obzirom da tijekom života nije objavljivao svoje radove, članovi obitelji su nakon Fermatove smrti nastojali prikupiti njegove zapise te ih objaviti posthumno. Fermatov sin, Clement Samuel, je pretraživao sve očeve zapise i knjige te slučajno naišao na bilješku u Bachetovom prijevodu *Aritmetike*. Bilješka se nalazila pokraj Problema 8 u Knjizi II, gdje se Diofant zapitao: "Kako dani broj koji je kvadrat nekog broja zapisati kao sumu kvadrata nekih brojeva?". Fermatova bilješka pokraj toga je glasila: *"S druge strane, nemoguće je kub napisati kao sumu dva kuba, bikvadrat na sumu bikvadrata, ili općenito, za bilo koju potenciju koja je veća od kvadrata, nemoguće je napisati kao sumu dva broja s jednakom potencijom. Otkrio sam čudesan dokaz navedenog, ali margina nije dovoljno velika da nastavim."* To je zapisano oko 1637. godine i poznato kao Veliki Fermatov teorem. Sljedećim teoremom je predstavljen precizan matematički zapis Velikog Fermatovog teorema.

Teorem 2.1 *Ne postoje pozitivni cijeli brojevi x, y, z takvi da vrijedi:*

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

za $n > 2$.

To je problem kojeg su mnogi matematičari bezuspješno pokušavali riješiti preko tristo godina. Danas se još uvijek sa sigurnošću ne zna je li Fermat doista znao dokaz tog problema. U tri stoljeća od Fermatove smrti, njegov rad u područjima van teorije brojeva je polako pao u zaborav, ne zato što nije dovoljno dobar, nego zato što je to sada moguće objasniti jednostavnije, koristeći jezik i simbole koji nisu postojali u Fermatovo doba. Nasuprot tome, Fermatov rad u teoriji brojeva je dugovječan i inovativan, ne samo Veliki Fermatov teorem, već i druga otkrića i ideje.

[2]René Descartes, 1596.-1650., francuski filozof, fizičar i matematičar
[3]Blaise Pascal, 1623.-1662., francuski izumitelj, filozof, fizičar i matematičar

2.3. Povijesni pregled dokazivanja teorema do A. Wilesa

Leonhard Euler (1707. - 1783.) je jedan od najproduktivnijih matematičara svih vremena. Može se reći da je stvorio velik dio analize i revidirao gotovo sva područja teorijske matematike poznate u njegovo doba. Pronašao je dva dokaza za slučaj Fermatovog Velikog teorema kada je $n = 3$. Jedan dokaz je sadržavao inovativnu metodu koja se koristi iracionalnim brojevima. Iako je Euler napravio grešku u tom dokazu, metoda je otkrila dobar pristup dokazivanju Velikog Fermatova Teorema i korištena je kasnije. Drugi dokaz je manje generaliziran, ali i dalje briljantan. Dokaz Teorema 3.5 se odnosi na Eulerov drugi dokaz Velikog Fermatovog teorema kada je $n = 3$.
Carl Friedrich Gauss (1777. - 1855.) je nedvojbeno najveći matematičar svoje epohe. U njegovo vrijeme je ponuđena nagrada Pariške akademije onome tko dokaže ili opovrgne Fermatov Veliki teorem. Ipak, Gauss nije sudjelovao u dokazivanju teorema, već je samo pronašao grešku u Eulerovom dokazu za $n = 3$. Izjavio je da ga Veliki Fermatov teorem kao izdvojena pretpostavka sasvim malo privlači jer i on sam može postaviti mnoštvo sličnih pretpostavki koje se ne bi mogle ni dokazati ni opovrgnuti.
Sophie Germain (1776. - 1831.) je ostvarila značajan napredak smjeru dokazivanja Velikog Fermatovog teorema. Ona je pod pseudonimom "Monsieur Leblanc" slala pisma Gaussu o mnogim matematičkim temama. Upotrijebila je muško ime u pismima kako bi spriječila predrasude prema znanstvenicima ženskog spola rasprostranjene u to vrijeme i kako bi privukla Gaussovu ozbiljnu pozornost. Njezin teorem glasi da ako postoji rješenje Teorema 2.1 za $n = 5$, onda sva tri broja moraju biti djeljiva sa 5. Ovaj teorem je razdvojio Veliki Fermatov teorem na dva slučaja: slučaj 1 obuhvaća brojeve koji nisu djeljivi sa pet, a slučaj 2 one koji jesu. Teorem je poopćen i za druge potencije. Bio je to značajan rezultat koji je smanjio moguće slučajeve pri dokazivanju Velikog Fermatovog teorema. Teoremom 3.7 je dan precizan matematički iskaz teorema Sophie Germain.
Évariste Galois (1811. – 1832.) je nadareni francuski matematičar. Njegovi rukopisi, objavljeni tek dvadeset godina nakon njegove smrti, su genijalni. Galoisova teorija se ističe na području apstraktne algebre. Pri dokazivanju Velikog Fermatovog teorema, Andrew Wiles koristi Galoisovu teoriju. U novijim vremenima se Galoisova teorija koristi u analitičkoj mehanici, tj. proračunima gibanja planeta i satelita.
Gabriel Lamé (1795. - 1870.) i Augustin Louis Cauchy (1789. - 1857.) su 1. ožujka 1847. na sjednici Francuske akademije objavili kako imaju dokaz Velikog Fermatovog teorema. Oni su bili slavni matematičari toga vremena, ali i veliki suparnici. Ipak, njihovi dokazi nisu bili točni. Obojici je greške u dokazima pronašao Ernst Kummer (1810. – 1893.), a i objasnio zašto je tadašnje znanje matematike bilo nedovoljno za dokaz Velikog Fermatovog teorema. No, Laméov je rad ipak dokazao tvrdnju u slučaju $n = 7$, a Kummerov za sve neregularne proste brojeve, uključujući sve brojeve veće od 37.
Nakon poraza što su ih doživjeli Lamé i Cauchy, svi pokušaji dokazivanja su zamrli,

sve do Paula Wolfskehla (1856. - 1906.), pedeset godina kasnije. Wolfskehl je bio njemački industrijalac i hobi-matematičar te je pronašao grešku u radu Ernsta Kummera. Nagrada za dokaz ili opovrgnuće slavne Fermatove bilješke je bila sve veća, mnogi matematičari su bezuspješno pokušavali pronaći dokaz, čak je i veliki njemački logičar, Kurt Gödel imao svoje mišljenje o Velikom Fermatovom teoremu. Gödel je 1931., kao dvadesetpetogodišnjak objavio rad "O formalno neodlučivim tvrdnjama", revolucionarno djelo koje danas citiraju ne samo matematičari, već i filozofi i poneki neurobiolozi. Gödel je dokazao da su i u matematici paradoksi neizbježni, i da postoje matematičke tvrdnje, koje premda istinite, nikad nećemo biti u stanju dokazati. Veliki Fermatov teorem je smatrao takvom tvrdnjom. Unatoč trudu tolikog broja velikih umova, dokaz Velikog Fermatova teorema nikada nije bio udaljeniji.
Sljedeće uloge u velikoj potrazi odigrala su dvojica Japanaca. Yutaka Taniyama (1927. - 1958.), tada nadareni dvadesetsedmogodišnjak, 1955. je prvi put uočio nešto što će revolucionirati teoriju brojeva. Taniyama je predlagao da su dva tada potpuno odvojena područja matematike, eliptičke krivulje i modularne forme, ustvari jedno te isto. Nitko ga nije ozbiljno shvaćao jer su eliptičke krivulje i modularne forme potpuno različite matematičke ideje. Tri godine kasnije Taniyama je počinio samoubojstvo. Tek je njegov prijatelj Goro Shimura (1930. -) vjerovao u to što se danas zove *Shimura-Taniyamin teorem*. Shimura je s vremenom skupljao argumente i hipoteza je stjecala sve više poklonika. Godine 1986. je Amerikanac Ken Ribert dokazao ukoliko je Shimura-Taniyamina hipoteza točna, onda je točan i Fermatov teorem. No problem je bio dokazati Shimura-Tanyaminu hipotezu, nitko nije znao kako, sve do Andrewa Wilesa.

2.4. Andrew Wiles i dokaz teorema

Sir Andrew John Wiles je rođen 11. travnja 1953. u Cambridgeu u Velikoj Britaniji. Već sa deset godina je u knjižnici u svom rodnom gradu doznao za Veliki Fermatov teorem, danas Wiles navodi kako je već tada imao želju dokazati teorem. Sedamdesetih godina je upisao fakultet te je nakon diplome primljen kao student-istraživač na katedri za matematiku na Cambridgeu. Do kraja studija Wiles je detaljno znao sva dotadašnja dostignuća matematičara o Velikom Fermatovom teoremu i sve njihove greške. Ipak, Wiles je doktorirao radom o eliptičkim krivuljama, mentor mu je bio profesor John Coates. Nakon doktorata je dobio mjesto na katedri za matematiku sveučilišta Princeton i preselio se u SAD. Kada je Wiles čuo za Ribetov rezultat, odlučio je pokušati dokazati Shimura-Taniyaminu hipotezu. Smatrao je da bi previše promatrača ugrozilo njegovu usmjerenost, a i samo spominjanje Velikog Fermatovog teorema bi privuklo veliku pozornost, stoga je radio u tajnosti. Wiles je napustio sve druge istraživačke projekte i potpuno se posvetio Fermatu. Imao je mogućnost koristiti sve pogodnosti koje mu je pružalo suvremeno stanje algebre, geometrije, analize i drugih matematičkih područja. Također su mu na raspolaganju stajali važni matematički rezultati njegovih

suvremenika. Znao je da je za dokaz Shimura-Taniyamine pretpostavke neophodno prethodno dokazati da je svaka eliptička krivulja modularna forma. Shvatio je da će najbolje biti ako pokuša *izbrojiti* eliptičke krivulje, a onda i modularne forme, kako bi zatim pokazao da se ova dva "broja" poklapaju. Ta konstrukcija će dokazati da su eliptičke krivulje i modularne forme jednake, odnosno da je svaka eliptička krivulja u stvari modularna forma, kako se to tvrdi u hipotezi Shimura-Taniyame. Primjetio je da zapravo ne treba dokazati cijelu pretpostavku Shimura i Taniyame, već samo jedan poseban slučaj: *polustabilne eliptičke krivulje s racionalnim brojevima kao koeficijentima*. Ako dokaže da pretpostavka vrijedi za ovu manju klasu eliptičkih krivulja, to će biti dovoljno za potvrdu Velikog Fermatovog teorema. Kako se radi o beskonačnim skupovima, nije se mogao osloniti na *brojanje*. Pokušao je raščlaniti veliki problem na manje te rješavati manje probleme jedan po jedan. Prije svega, za neke eliptičke krivulje se već znalo da su modularne forme, bili su to vrlo značajni rezultati do kojih su došli mnogi drugi stručnjaci teorije brojeva. Wiles je nakon dvije godine pokušavanja shvatio da usmjerenost samo na eliptičke krivulje i pokušaji da se one prebroje i usporede sa modularnim formama nije najbolja strategija. Pokušao je novi pristup, htio je *transformirati* eliptičke krivulje u Galoisove reprezentacije, a onda izbrojati te Galoisove reprezentacije i usporediti to s modularnim formama. Galoisova teorija omogućava matematičarima koji rade na teoriji brojeva prijelaz s beskonačne klase na takvu koja se može predstaviti kao konačan skup. Ovo premještanje problema znači velik korak naprijed, budući se s konačnim skupom elemenata znatno lakše može koristiti nego beskonačnim. Ovaj pristup se pokazao korisnim kod nekih vrsta eliptičkih krivulja. Bio je to značajan napredak, iako se i dalje suočavao sa poteškoćama. Wilesov kolega sa Princetona, Nick Katz, je provjeravao svaki korak pri dokazivanju. U svibnju 1993. godine Andrew Wiles je dovršio dokaz. Sljedećeg mjeseca se u Cambridgeu održavala konferencija iz područja teorije brojeva. Na toj konferenciji je Wiles održao predavanje te izložio dokaz Shimura-Taniyamine pretpostavke. Sada je došlo vrijeme da drugi stručnjaci provjere njegov rad od 200 stranica. Većina matematičara je smatralo kako je dokaz točan, no čekala se konačna ocjena šestorice stručnjaka. Ipak, Nick Katz je krajem kolovoza uočio jedan problem u trećem poglavlju, u početku se činilo da je problem sitan, no kasnije se pokazalo suprotno. Wiles je u prosincu 1993. javno priznao da greška postoji. Nakon toga je mjesecima pokušavao ispraviti svoj dokaz, no nije napredovao i odlučio je odustati od dokazivanja ukoliko do listopada 1994. ne pronađe rješenje. U ponedjeljak, 19. rujna 1994., Wiles je ponovno pažljivo proučio svoj dokaz te shvatio kako ispraviti grešku. Ovaj put se dokaz pokazao točnim te je u lipnju 1995. objavljen u matematičkom časopisu *Annals of Mathematics*. Andrew Wiles opisuje svoj dokaz kao "tekovinu matematike dvadesetog stoljeća". Dokazivanje teorema na način na koji je to konačno učinjeno u devedesetim godinama dvadesetoga stoljeća pretpostavljalo je znatno višu matematiku od one koja je mogla biti poznata Fermatu. Konačno rješenje problema obuhvaća, a u određenom smislu i objedinjuje,

svekoliku matematiku. Završni dokaz teorema je proizašao iz prividno nespojivih područja matematike, a unatoč činjenici da je Andrew Wiles bio osoba koja je obavila važan konačni rad na teoremu, cijeli pothvat je djelo mnogih matematičara.

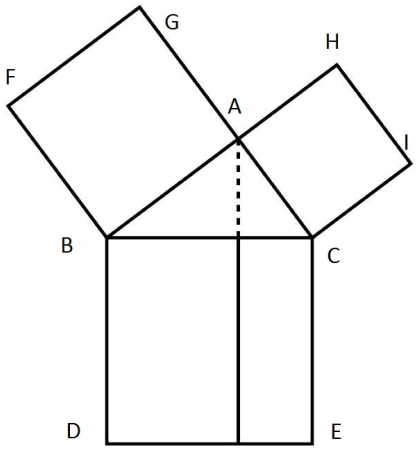
3. Posebni slučajevi Velikog Fermatovog teorema

3.1. Pitagorin poučak

Prema teoremu 2.1, Fermatov Veliki teorem se odnosi za $n > 2$. Ovdje je naveden Pitagorin teorem koji se ponekad u literaturi navodi kao posebni slučaj Velikog Fermatovog teorema za $n = 2$.

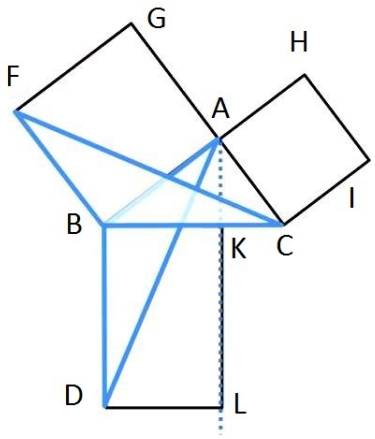
Teorem 3.1 *Kvadrat nad hipotenuzom pravokutnog trokuta jednak je zbroju kvadrata nad dvije katete.*

Dokaz. Neka je $\triangle ABC$ pravokutan. Nacrtajmo kvadrate iznad stranica $\triangle ABC$, kako je prikazano na Slici 1.



Slika 1. *Kvadrati iznad stranica trokuta* $\triangle ABC$

Sada imamo kvadrate $CBDE$, $BAGF$ i $ACIH$. Iz vrha A nacrtamo pravac paralelan sa BD i CE. Taj pravac pod pravim kutom presijeca BC i DE, redom u točkama K i L. Spojimo CF i AD kako bi se formirali trokuti BCF i BDA. Kutevi $\angle CAB$ i $\angle BAG$ su pravi, točke C, A i G su kolinearne. Isto vrijedi i za B, A i H. Kutevi $\angle CBD$ i $\angle FBA$ su također pravi, stoga je $\angle ABD$ jednak $\angle FBC$ (jer su ti kutevi sume pravog kuta i kuta $\angle ABC$).



Slika 2. *Trokut* $\triangle ABD$ *je sukladan trokutu* $\triangle FBC$.

Kako je $AB = FB$ i $BD = BC$, trokut $\triangle ABD$ mora biti sukladan trokutu $\triangle FBC$, što je označeno na Slici 2. Pravac $A - K - L$ je paralelan sa BD, onda paralelogram $BDLK$ je dvostruka površina trokuta$\triangle ABD$.Kako su C, A i G kolinearne, kvadrat $BAGF$ je dvostruka površina trokuta $\triangle FBC$. Prema tome, četverokut $BDLK$ mora biti jednake površine kao kvadrat $BAGF$, $BAGF = AB^2$. Slično, može se pokazati da četverokut $CKLE$ mora imati jednaku površinu kao kvadrat $ACIH$, $ACIH = AC^2$. Zbrajanjem tih dvaju rezultata, slijedi:

$$AB^2 + AC^2 = BD \cdot BK + KL \cdot KC.$$

Kako je $BD = KL$, imamo:

$$BD \cdot BK + KL \cdot KC = BD(BK + KC) = BD \cdot BC.$$

Prema tome je

$$AB^2 + AC^2 = BC^2$$

jer je $CBDE$ kvadrat.

□

3.2. Pitagorine trojke

Propozicija u Diofantovoj Aritmetici koja je inspirirala Fermata za veliki teorem govori o jednom od najstarijih problema u matematici, "napisati kvadrat nekog broja kao sumu dva kvadrata." Jedno rješenje tog problema daje jednakost:

$$5^2 = 4^2 + 3^2 \tag{1}$$

Ako se jednakost (1) podijeli sa 5^2 i pomnoži sa a^2, slijedi:

$$a^2 = (\frac{4a}{5})^2 + (\frac{3a}{5})^2.$$

Na sličan način, svaka trojka pozitivnih cijelih brojeva x, y, z takvih da je:

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

daje rješenje:

$$a^2 = (\frac{xa}{z})^2 + (\frac{ya}{z})^2.$$

Dana je precizna definicija takvih trojki:

Definicija 3.1 *Uređenu trojku prirodnih brojeva (x, y, z) zovemo Pitagorina trojka ako su x, y katete, a z hipotenuza nekog pravokutnog trokuta, tj. ako vrijedi:*

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

Ako su x, y, z relativno prosti, onda kažemo da je (x, y, z) primitivna Pitagorina trojka. (Takav trokut zovemo (primitivni) Pitagorin trokut.)

Kada je problem postavljen na ovaj način, povezanost sa Pitagorinim teoremom postaje očigledna. Jednakost (1), prema Teoremu 3.1, implicira da je trokut kojemu su stranice u omjeru $3 : 4 : 5$ pravokutan. Pitagorine trojke, prema definiciji, određuju omjer $x : y : z$. Trokut kojemu su stranice u omjeru $x : y : z$ je pravokutan. Dakle, Diofantov problem se može geometrijski interpretirati kao traženje pravokutnog trokuta čiji omjer stranica se može zapisati u terminima cijelih brojeva. Najpoznatiji primjer Pitagorine trojke je dan jednakošću (1).

3.2.1. Kako pronaći Pitagorine trojke?

Metoda pronalaska pitagorejskih trojki je analitička. Primjetimo, ako d dijeli sva tri broja x, y, z, koji sačinjavaju Pitagorinu trojku (x, y, z), onda se jednadžba (2) može podijeliti sa d^2. Brojevi

$$\frac{x}{d},\ \frac{y}{d},\ \frac{z}{d}$$

također čine Pitagorinu trojku. Ako je d najveći zajednički djelitelj od x, y, z, onda su $\frac{x}{d}, \frac{y}{d}, \frac{z}{d}$ relativno prosti, tj. čine primitivnu Pitagorinu trojku. Dakle, svaka Pitagorina trojka se može dijeljenjem sa najvećim zajedničkim djeliteljem *skratiti* na primitivnu Pitagorinu trojku. Nasuprot tome, ako je zadana primitivna Pitagorinu trojku, $a^2 + b^2 = c^2$ i ako odaberemo neki cijeli broj d te postavimo:

$$x = ad,\ y = bd,\ z = cd,$$

možemo konstruirati pitagorinu trojku $x^2 + y^2 = z^2$. U svakoj primitivnoj Pitagorinoj trojki točno je jedan od brojeva x, y, z paran. Naime, ako bi x i y bili parni, onda trojka ne bi bila primitivna, a ako bi x i y bili neparni, onda bi iz $x^2 + y^2 \equiv 2 (\mathrm{mod}\ 4)$ i $z^2 \equiv 0 (\mathrm{mod}\ 4)$ dobili kontradikciju.
Da bismo pronašli Pitagorine trojke, moramo pronaći rješenja jednadžbe (2). Pretpostavimo da su x, y, z relativno prosti, tj. $(x, y, z) = 1$. Kada bismo imali zadane x, y, z koji nisu relativno prosti, mogli bismo ih podijeliti sa zajedničkim djeliteljem i ponovno dobiti relativno proste brojeve. Ta pretpostavka je bitna jer pojednostavljuje zadatak analiziranja uvjeta kada postoje rješenja jednadžbe (2). Sljedeće važno jest da je z neparan, o tome govori sljedeća lema:

Lema 3.1 *U jednadžbi $x^2 + y^2 = z^2$, z je neparan broj.*

Dokaz. Pretpostavimo da je z paran. Tada postoji broj Z takav da je $z = 2 \cdot Z$. Također, tada je z^2 djeljiv sa 4 jer

$$z^2 = (2Z)^2 = 4 \cdot Z^2.$$

Ako je z paran, x i y moraju biti neparni jer je $(x, y, z) = 1$. Kako su x i y neparni, moraju postojati X i Y takvi da je:

$$x = 2 \cdot X + 1,$$

$$y = 2 \cdot Y + 1.$$

Međutim, x^2 i y^2 ne mogu biti djeljivi sa 4 jer:

$$\begin{aligned} x^2 + y^2 &= (2 \cdot X + 1)^2 + (2 \cdot Y + 1)^2 \\ &= 4X^2 + 4X + 1 + 4Y^2 + 4Y + 1 \\ &= 4 \cdot (X^2 + X + Y^2 + Y) + 2, \end{aligned}$$

što je kontradikcija sa $x^2 + y^2 = z^2$ i pretpostavkom da je z paran.

□

Kako je z neparan, jedan od brojeva x ili y mora biti paran. Pretpostavimo da je x paran (isti argumenti bi vrijedili i da pretpostavimo da je y paran). Znamo:

$$x^2 = z^2 - y^2 = (z - y) \cdot (z + y).$$

Brojevi $z - y$, $z + y$ moraju biti parni jer su z i y neparni. Dakle, postoje u, v, w takvi da je:

$$x = 2 \cdot u,$$

$$z + y = 2 \cdot v,$$

$$z - y = 2 \cdot w,$$

što znači da:

$$(2 \cdot u)^2 = (2 \cdot v) \cdot (2 \cdot w). \tag{3}$$

Ako obje strane jednakosti (3) podijelimo sa 4, slijedi da je

$$u^2 = v \cdot w. \tag{4}$$

Potrebno je uočiti da su v i w relativno prosti. O tome govori sljedeća lema.

Lema 3.2 *v i w su relativno prosti.*

Dokaz. Pretpostavimo da v i w nisu relativno prosti. Tada $\exists$ broj d, $d > 1$ takav da $d|v$, $d|w$. Također, $d|v + w$ i $d|v - w$. Stavimo:

$$z + y + z - y = 2v + 2w,$$

$$2z = 2v + 2w.$$

To znači da je $z = v + w$ pa $d|z$. Također:

$$z + y - (z - y) = 2v + 2w,$$

$$2y = 2v - 2w.$$

Iz toga slijedi da $y = v - w$ pa $d|y$, što je kontradikcija sa pretpostavkom da su z i y relativno prosti.

□

Prema Teoremu 3.2: iz jednakosti (4) i Leme 3.2, znamo da su v i w kvadrati. Dakle, postoje p i q takvi da je $v = p^2$ i $w = q^2$. Imamo rješenje:

$$z = v + w = p^2 + q^2,$$
$$y = v - w = p^2 - q^2,$$
$$x = 2u = 2pq.$$

Također znamo da su p i q relativno prosti (inače z, x, y ne bi bili relativno prosti) i različitih parnosti (jer je z neparan).

3.3. Metoda beskonačnog silaska

Fermat je sam kreirao metodu beskonačnog silaska te ju koristio u mnogim dokazima na području teorije brojeva. Svrha ideje je pokazati da su određena svojstva i relacije nemoguća za cijele brojeve. Prvo se pokaže da ako zadana svojstva i relacije vrijede za neke brojeve, onda vrijede i za neke manje brojeve od tih. Zatim, po istom argumentu, se dokaže da su svojstva moguća za još manje brojeve i tako u beskonačnost. Kako se radi o pozitivnim cijelim brojevima, poznato je da niz pozitivnih cijelih brojeva ne može beskonačno opadati pa se ta svojstva i relacije pokazuju nemogućim. Fermat je ostavio malo detalja primjeni ove metode, naveo je primjer dokazivanja da površina pravokutnog trokuta ne može biti jednaka kvadratu nekog broja, dokaz navedenog se može naći u [4]. Elegantna primjena ove metode se vidi u slučaju Velikog Fermatovog teorema za $n = 4$. Upotreba metode beskonačnog silaska je prikazana na dokazivanju Propozicije 3.1 i Teorema 3.2 koji pomažu pri dokazivanju nekih posebnih slučajeva.

Propozicija 3.1 *Ako su v i w relativno prosti i ako je vw kvadrat, tada v i w oba moraju biti kvadrati.*

Dokaz. U ovom slučaju treba pokazati da je nemoguće da postoje brojevi v i w takvi da:

(1) v i w su relativno prosti,

(2) $v \cdot w$ je kvadrat,

(3) v i w nisu oba kvadrati.

Pretpostavimo da se takvi v i w mogu pronaći te da v nije kvadrat, preciznije, da v nije 1. Prema tome, v je djeljiv sa barem jednim prostim brojem. Neka je P prost broj koji dijeli v, $v = P \cdot k$. Tada P također dijeli vw, što je kvadrat, neka $vw = u^2$. Po svojstvu prostih brojeva koje kaže da ako P dijeli $u \cdot u$, onda P mora dijeliti u ili u, tj. P mora dijeliti u, recimo $u = P \cdot m$. Tada se $vw = u^2$ može zapisati kao:

$$Pkw = (Pm)^2 = P^2m^2.$$

Kako P dijeli desnu stranu jednakosti, mora dijeliti i lijevu. Prema tome, P mora dijeliti ili k ili w. No, znamo da P ne dijeli W jer dijeli v, a v i w su relativno prosti. Dakle, P dijeli k. Neka je $k = P \cdot v'$, 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 djelitelj od v. Prema tome, v' i w ne mogu imati većeg zajedničkog djelitelja od 1. Štoviše, da je v' kvadrat, tada bi $v = P^2v'$ bio kvadrat, što nije, pa je očigledno da v' nije kvadrat. Dakle, v' i w ispunjavaju svojstva 1, 2, 3 i $v' < v$. Isti argument pokazuje da postoji $v'' < v'$ takav da v'' i w također imaju ta tri svojstva. Ponavljanjem tog argumenta beskonačno mnogo puta dobili bismo niz pozitivnih cijelih brojeva $v > v' > v'' > v''' > \ldots$ Koji pada u beskonačnosti. Kako je to nemoguće za pozitivne cijele brojeve, nemoguće je da v iw zadovoljavaju ta tri svojstva.

□

Teorem 3.2 *Relativno prosti djelitelji n-tih potencija su i sami n-te potencije, preciznije:* $(v, w) = 1,\ v \cdot w = z^n \ \Rightarrow \exists x, y$ *takvi da je* $v = x^n,\ w = y^n$.

Dokaz. Neka su v i w cijeli brojevi takvi da je $(v, w) = 1$ i $v \cdot w = z^n$. Dakle, v i w su relativno prosti djelitelji broja z koji je n-ta potencija. Pretpostavimo da v nije jednak nekom broju oblika x^n, prema tome $v \neq 1$. Prema Teoremu 1.3, v je djeljiv prostim brojem p pa postoji k takav da je $v = p \cdot k$. Prema Propoziciji 1.2, poznato je da $p|z$ jer $z^n = v \cdot w = p \cdot k \cdot w$. Dakle, postoji m takav da je $z = p \cdot m$. Nadalje,

$$z^n = v \cdot w = p \cdot k \cdot w = (p \cdot m)^n = p^n \cdot m^n. \tag{5}$$

Ako jednakost (5) podijelimo sa p, dobivamo:

$$k \cdot w = p^{n-1} \cdot m^n.$$

Prema Propoziciji 1.2, zaključujemo da p ili dijeli k ili w. No, p ne može dijeliti w jer dijeli v, a $(v, w) = 1$. Prema tome, p dijeli k. Taj isti argument se može primjeniti za svaki p u p^{n-1} pa se može zaključiti da p^{n-1} dijeli k. Dakle, $\exists V$ takav da je $k = p^{n-1} \cdot V$ pa je:

$$k \cdot w = p^{n-1} \cdot m^n = p^{n-1} \cdot V \cdot w. \tag{6}$$

Ako jednakost (6) podijelimo sa p^{n-1}, dobivamo: $V \cdot w = m^n$. Brojevi V i w su relativno prosti, tj. $(V, w) = 1$ jer V dijeli v i $(v, w) = 1$. Također, Vne može biti n-ta potencija, inače bi $v = p^n \cdot V$, što bi v činilo n-tom potencijom. Na kraju, V je manji od v jer $p^{n-1} > 1$, što je kontradikcija po metodi beskonačnog silaska.

□

3.4. Veliki Fermatov teorem u slučaju $n = 4$

Ovaj slučaj Velikog Fermatovog teorema je najjednostavnije za dokazati. Dokaz direktno slijedi iz sljedećeg teorema.

Teorem 3.3 *Jednadžba $x^4 + y^4 = z^2$, $xyz \neq 0$ nema cjelobrojnih rješenja.*

Dokaz. Pretpostavimo da postoji rješenje dane jednadžbe, takvo da je $xyz \neq 0$. Uzmimo takvo rješenje s najmanjim z. Prema Teoremu 3.2 se može pretpostaviti da $(x^2, y^2, z) = 1$. Iz rješenja za Pitagorine trojke, vidljivog u potpoglavlju 3.2.1., poznato je da postoje p i q takvi da je:

$$\begin{aligned} z &= p^2 + q^2, \\ y^2 &= p^2 - q^2, \\ x^2 &= 2pq. \end{aligned}$$

Ovdje postoji druga Pitagorina trojka jer $y^2 + q^2 = p^2$. Kao i u prethodnom slučaju, postoje a i b, $(a, b) = 1$, takvi da je:

$$\begin{aligned} q &= 2ab, \\ y &= a^2 - b^2, \\ p &= a^2 + b^2. \end{aligned}$$

Kombiniranjem gornjih dvaju sustava jednadžbi, slijedi:

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

Kako su $a \cdot b$ i $a^2 + b^2$ relativno prosti, onda su i kvadrati, prema dokazu Teorema 3.2. Stoga postoji P takav da $P^2 = a^2 + b^2$. Dalje se može nastaviti dokazivanje metodom beskonačnog silaska jer $P^2 = a^2 + b^2$ je manje od $p^2 + q^2 = z$, što je manje od z^2. Treba napomenuti da ovaj argument stoji samo ako je $xyz \neq 0$. Dakle, postojanje rješenja početne jednadžbe nužno vodi postojanju manjeg kvadrata koji ima jednaka svojstva.

□

Slučaj Velikog Fermatovog teorema za $n = 4$ je dan sljedećim korolarom.

Korolar 3.1 *Jednadžba $x^4 + y^4 = z^4$, $xyz \neq 0$ nema cjelobrojnih rješenja.*

Dokaz. $x^4 + y^4 = z^4$ se može zapisati kao: $x^4 + y^4 = (z^2)^2$, po prethodnom teoremu, ne postoje cjelobrojna rješenja koja zadovoljavaju tu jednadžbu.

□

Sljedeći korolar pokazuje da ne postoji cjelobrojno rješenje za slučaj Velikog Fermatovog teorema kada je n djeljiv sa 4.

Korolar 3.2 *Jednadžba $x^{4n'} + y^{4n'} = z^{4n'}$, $xyz \neq 0$ nema cjelobrojnih rješenja.*

Dokaz. $x^{4n'} + y^{4n'} = z^{4n'}$ se može zapisati kao: $(x^{n'})^4 + (y^{n'})^4 = (z^{2n'})^2$, prema Teoremu 3.3, ne postoje cjelobrojna rješenja koja zadovoljavaju tu jednadžbu.

□

Sada možemo zaključiti da je Veliki Fermatov teorem potrebno dokazati samo za proste brojeve n, tj. dovoljno je dokazati.

Teorem 3.4 *Jednadžba $x^n + y^n = z^n$, $xyz \neq 0$ nema cjelobrojnih rješenja za $n > 2$, n prost broj.*

Ako se dokaže Fermatov Veliki teorem za dani prost broj, onda slijedi da je dokaz valjan i za bilo koji broj djeljiv s tim prostim brojem. Npr., ako se dokaže da ne postoji cjelobrojno rješenje za $x^3 + y^3 = z^3$, tada je dokazano i da ne postoji rješenje za $x^9 + y^9 = z^9$, odnosno $(x^i)^3 + (y^i)^3 = (z^i)^3 = x^{3i} + y^{3i} = z^{3i}$.

3.5. Veliki Fermatov teorem u slučaju $n = 3$

Teorem 3.5 *Neka $x^3 + y^3 = z^3$ ima cjelobrojna rješenja, tada je $xyz = 0$.*

Dokaz. Neka su x, y, z rješenja jednadžbe teorema. Pretpostavimo da su x, y, z relativno prosti, to je vidljivo iz sljedeće leme.

Lema 3.3 *Svako rješenje od:*

$$x^n + y^n = z^n \tag{7}$$

se može reducirati na formu gdje su x, y i z relativno prosti.

Dokaz. Da bismo dokazali ovu lemu, potrebno je pokazati sljedeće:

(1) Ako neki broj dijeli dva rješenja jednadžbe $x^n + y^n = z^n$, tada njegova n-ta potencija dijeli n-tu potenciju trećeg rješenja jednadžbe.

(2) Ako n-ta potencija broja koji dijeli dva rješenja jednadžbe $x^n + y^n = z^n$ dijeli n-tu potenciju rješenja, tada taj broj dijeli i samo rješenje.

Korak 1.
Slučaj 1. Pretpostavimo da d dijeli x i y. Dakle, postoje x', y' takvi da je $x = d(x')$, $y = d(y')$. Može se zapisati:

$$\begin{aligned} z^n &= x^n + y^n \\ &= (dx')^n + (dy')^n \\ &= d^n x'^n + d^n y'^n \\ &= d^n(x'^n + y'^n). \end{aligned}$$

Slučaj 2. Neka d dijeli z i x. Isti argumenti bi vrijedili i da d dijeli z i y. Prema tome, postoje x', z' takvi da je $x = dx'$, $z = dz'$. Zapiše li se jednakost (7) u obliku $y^n = z^n - x^n$, dokaz se može nastaviti analogno kao u slučaju 1.
Korak 2.
Neka je c najveći zajednički djelitelj od d i x. Neka je

$$D = \frac{d}{c},\ X = \frac{x}{c}. \tag{8}$$

Dakle, $(X, D) = 1$ pa je i $(X^n, D^n) = 1$. Kako d^n dijeli x^n, postoji k takav da je $x^n = k \cdot d^n$. Primjenom jednakosti (8) dobije se: $(cX)^n = k \cdot (cD)^n$, što daje:

$$c^n X^n = k \cdot c^n D^n \tag{9}$$

Podijelimo li jednakost (9) sa c^n, slijedi: $X^n = D^n \cdot k$. Može se zaključiti da je $(D^n, k) = 1$, što je lako pokazati kontradikcijom. Prema Teoremu 3.2, možemo zaključiti da je k n-ta potencija, što znači da postoji u takav da je $u^n = k$. Dakle, $D^n \cdot u^n = X^n$ i $(Du)^n = X^n$. Prema tome, $Du = X$, množenjem sa c slijedi da d dijeli x, što je i trebalo dokazati.

□

Nastavak dokaza Teorema 3.5:
Sljedeća lema govori o egzistenciji rješenja jednadžbe $x^3 + y^3 = z^3$.

Lema 3.4 *$x^3 + y^3 = z^3$ ima rješenje ako postoje p i q takvi da:*

(1) $(p, q) = 1$,

(2) p i q su pozitivni,

(3) p i q su različitih parnosti,

(4) $2p \cdot (p^2 + 3q^2)$ *je kub.*

Dokaz. Pretpostavimo da su x, y, z relativno prosti. Znači da je najviše jedan od njih paran. Također, najmanje jedan od njih je paran jer ako su npr. x i y neparni, tada z mora biti paran. Dokaz ove leme se može podijeliti na dva slučaja:

(1) z je paran,

(2) x je paran.

Kako su x i y simetrični, slučaj 2 će pokriti slučaj kada je y paran.

Slučaj 1. Kako je z paran, x i y su neparni, $x+y$ i $x-y$ su parni. Neka je $2p = x+y$, $2q = x-y$, tada:

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

Sada $(p,q) = 1$. Kada p, q ne bi bili relativno prosti, postojao bi f takav da je $f = (p,q)$, $f > 1$. Također, postojali bi P, Q takvi da je $p = fP$, $q = fQ$, ali onda bi f dijelio x i y jer $x = f(P+Q)$, $y = f(P-q)$, što je kontradikcija sa tim da su x i y relativno prosti. Može se zaključiti da je $(p,q) = 1$.
Nadalje, možemo pretpostaviti da su p i q pozitivni. Iz $2p = x+y$, $2q = x-y$ je $p = \frac{1}{2}(x+y)$, $q = \frac{1}{2}(x-y)$. x ne može biti jednak y jer su relativno prosti. Ako je $x+y$ negativan, može se zamijeniti sa $-x, -y$ jer $x^3+y^3 = z^3$ povlači da $-x^3+(-y)^3 = -z^3$. Ako je y veći od x, tada se zamijeni x, y jer su simetrični. To pokriva sve slučajeve.
Kako su x i y neparni, p i q moraju biti suprotnih parnosti.
$2p \cdot (p^2+3q^2)$ je kub jer $z^3 = x^3+y^3 = (x+y)(x^2-xy+y^2) = (p+q+p-q)[(p+q)^2-(p+q)(p-q)+(p-q)^2] = 2p(p^2+3q^2)$. Time je dokazan slučaj 1.
Slučaj 2. Kako je x paran, z i y su neparni jer su relativno prosti sa x. $x+y$ i $x-y$ su parni. Postoje p, q takvi da je $2p = z-y$, $2q = z+y$ i

$$z = \frac{1}{2}[(z-y)+(z+y)] = \frac{1}{2}(2p+2q) = p+q,$$
$$y = \frac{1}{2}[(z+y)-(z-y)] = \frac{1}{2}(2q-2p) = q-p.$$

Kako su z i y neparni, p i q moraju biti različitih parnosti.
Po istom argumentu kao i u slučaju 1, $(p,q) = 1$ i p i q su pozitivni.
$2p \cdot (p^2+3q^2)$ je kub jer

$$\begin{aligned} x^3 &= z^3-y^3 = (z-y)(z^2+zy+y^2) \\ &= (q+p-(q-p))[(q+p)^2-(q+p)(q-p)+(q-p)^2] \\ &= 2p(p^2+3q^2). \end{aligned}$$

□

Za daljnje dokazivanje Teorema 3.5, potrebna nam je sljedeća lema.

Lema 3.5 *Ako su p i q relativno prosti i različitih parnosti, tada je $(2p, p^2+3q^2) = 1$ ili $(2p, p^2+3q^2) = 3$.*

Dokaz. Neka je f prost broj koji dijeli oba broja, $2p$ i p^2+3q^2. Broj f ne može biti 2 jer p^2+3q^2 je neparan (zato što su p i g različitih parnosti). Neka je f veći od 3,

tako da postoje P i Q takvi da je: $2p = fP$, $p^2 + 3q^2 = Qf$. Broj f nije 2 pa se vidi da 2 mora dijeliti P, stoga postoji vrijednost H koja je polovica od P i $p = fH$. Kombiniranjem prethodnih jednadžbi dobije se:

$$3q^2 = qf - p^2 = Qf - f^2H^2 = f(Q - fH^2).$$

Kako je f veći od 3, ne dijeli 3. Po Propoziciji 1.2, mora dijeliti q. No to je kontradikcija sa pretpostavkom da su p i q relativno prosti jer f također dijeli p pa odbacujemo pretpostavku.

□

Sljedećom lemom je dan osnovni dio dokaza.

Lema 3.6 *Uz dane uvjete:*

(1) x, y, z *je rješenje jednadžbe* $x^3 + y^3 = z^3$,

(2) Dvije vrijednosti od x, y, z *su dobivene iz* $p + q$, $p - q$,

(3) p *i* q *su relativno prosti,*

(4) p *i* q *su različitih parnosti,*

(5) p *i* q *su pozitivni,*

(6) $2p(p^2 + 3q^2)$ *je kub,*

(7) $(2p, p^2 + 3q^2) = 1$,

postoji manje rješenje A, B, C *takvo da* $A^3 + B^3 = C^3$.

Dokaz. Prema Teoremu 3.2 su p^2 i $p^2 + 3q^2$ kubovi. Prvo treba prikazati da postoje brojevi a i b takvi da je: $p = a^3 - 9ab^2$, $q = 3a^2b - 3b^3$, $(a, b) = 1$ te da su a i b različitih parnosti. O tome govori sljedeća lema.

Lema 3.7 *Neka postoje* p *i* q *sa danim svojstvima:*

(1) p *i* q *su relativno prosti,*

(2) p *i* q *su različitih parnosti,*

(3) $p^2 + 3q^2$ *je kub.*

Tada postoje a *i* b *takvi da je:*

(a) $p = a^3 - 9ab^2$,

(b) $q = 3a^2b - 3b^3$,

(c) $(a, b) = 1$,

(d) *a i b su različitih parnosti.*

Dokaz. Kako je $p^2 + 3q^2$ kub, može se zapisati:

$$u^3 = p^2 + 3q^2. \tag{10}$$

Kako su p i q različitih parnosti, u je neparan. Također, u mora biti oblika $a^2 + 3b^2$, dokaz čega se može pronaći u [4]. Sada,

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

jer je:

$$\begin{aligned}(a^2 + 3b^2)^2 &= a^4 + 6a^2b^2 + 9b^4 \\ &= a^4 + 12a^2b^2 - 6a^2b^2 + 9b^4 \\ &= (a^2 - 3b^2)^2 + 3(2ab)^2.\end{aligned}$$

Također,

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

te:

$$[a(a^2 - 3b^2) - 3b(2ab)]^2 + 3[a(2ab) + b(a^2 - 3b^2)]^2 \;=\; (a^3 - 9ab^2)^2 + 3(3a^2b - 3b^3)^2.$$

Kombinacija prethodne jednakosti i jednakosti (10) daje:

$$p^2 + 3q^2 = (a^3 - 9ab^2)^2 + 3(3a^2b - 3b^3)^2,$$

što znači da se mogu definirati a i b takvi da je $(a, b) = 1$, $p = a^3 - 9ab^2$ i $q = 3a^2b - 3b^3$. Također, poznato je da su a i b različitih parnosti jer ako bi oba bila neparna, tada bi p bio paran i q bi bio paran, a to je nemoguće jer su p i q različitih parnosti. Kad bi a i b bili oba parna, p i q bi bili parni, što je opet nemoguće.

□

Nastavak dokaza Leme 3.6. Lema 3.7 daje:

$$2p = 2a^3 - 18ab^2 = 2a(a - 3b)(a + 3b).$$

Potrebno je dokazati da su $2a$, $a - 3b$, $a + 3b$ međusobno relativno prosti. Prvo, $2a$ je relativno prost sa $a - 3b$ i $a + 3b$. Oba broja, $a - 3b$, $a + 3b$ su neparna jer a i b su različitih parnosti. Ako bi a imao zajedničkih djelitelja sa $a - 3b$ i $a + 3b$, tada bi dijelili i b, što je suprotno pretpostavci. Ako bilo koji prost broj veći od 3 dijeli $a - 3b$ i $a + 3b$ onda mora dijeliti i a jer $2a = a - 3b + a + 3b$ i mora dijeliti b jer $6b = a + 3b - (a - 3b)$,

ali to je nemoguće. Već je pokazano da 2 ne može dijeliti $a-3b$ i $a+3b$, stoga, samo je potrebno dokazati da 3 također ne može dijeliti oba ta broja. Ako bi 3 dijelio $a-3b$ i $a+3b$, onda bi dijelio i a jer $2a = a-3b+a+3b$, također, dijelio bi i p jer $p = a^3-9ab^2$. No prema pretpostvci da je $(2p, p^2+3q^2) = 1$, ne može dijeliti p. Dakle, 3 ne može dijeliti $a-3b$ i $a+3b$. Prema Teoremu 3.5, brojevi $2a$, $a-3b$, $a+3b$ su kubovi. Može se zapisati:

$$2a = A^3,$$

$$a-3b = B^3,$$

$$a+3b = C^3,$$

što daje drugo rješenje za Veliki Fermatov teorem kada je $n = 3$:

$$A^3 = 2a = a-3b+a+3b = B^3+C^3.$$

Ovo rješenje je manje od x, y, z jer:

$$A^3B^3C^3 = 2a(a-3b)(a+3b) = 2p,$$

a prema prethodnim rezultatima je $x^3 = 2p(p^2+3q^2)$ ili je $z^3 = 2p(p^2+3q^2)$. Ovim je Lema 3.6 dokazana.

□

Također, ako je $(2p, p^2+3q^2) = 3$, mora postojati manje rješenje Velikog Fermatovog teorema za $n = 3$. O tome govori sljedeća lema.

Lema 3.8 *Uz dane uvjete:*

(1) x, y, z *je rješenje jednadžbe* $x^3+y^3 = z^3$,

(2) Dvije vrijednosti od x, y, z *su dobivene iz* $p+q$, $p-q$,

(3) p *i* q *su relativno prosti,*

(4) p *i* q *su različitih parnosti,*

(5) p *i* q *su pozitivni,*

(6) $2p(p^2+3q^2)$ *je kub,*

(7) $(2p, p^2+3q^2) = 3$,

postoji manje rješenje A, B, C *takvo da* $A^3+B^3 = C^3$.

Dokaz. Prvo treba uočiti da 3 dijeli p, ali ne i q, zato što 3 dijeli $2p$, a p i q su relativno prosti. Znači, postoji s takav da je $p = 3s$ i

$$\begin{aligned} 2p(p^2+3q^2) &= 2p(3s\cdot 3s+3q^2) \\ &= 2\cdot 3s\cdot(3\cdot 3s^2+3q^2) \\ &= 3^{2\cdot 2s(3s^2+q^2)}. \end{aligned}$$

Sada treba pokazati da su $3^{2\cdot 2s}$ i $3s^2+q^2$ relativno prosti: 3 ne dijeli q, pa 3 ne dijeli ni $3s^2+q^2$. Kako je $p = 3s$, s je iste parnosti kao i p, što znači da su q i s različite parnosti. Zbog toga 2 ne može dijeliti $3s^2+q^2$ jer je to neparan broj. Na kraju, $(s,q) = 1$ jer $(p,q) = 1$.
Dakle, prema Teoremu 3.2, $3^{2\cdot 2s}$ i $3s^2+q^2$ su kubovi jer $3^{2\cdot 2s(3s^2+q^2)} = 2p\cdot(p^2+3q^2)$ i $2p\cdot(p^2+3q^2)$ je kub.
Uz pretpostavke da $(s,q) = 1$, q, s su suprotnih parnosti i $3s^2+q^2$ je kub. Po Lemi 3.7 znamo da postoje a i b takvi da je:

$$\begin{aligned} q &= a^3-9ab^2, \\ s &= 3a^2b-3b^3, \\ (a,b) &= 1. \end{aligned} \tag{11}$$

Iz jednakosti (11) se može pokazati da su $2b$, $a-b$ i $a+b$ kubovi:
a i b su različitih parnosti jer kad bi bili iste parnosti onda bi i q i s bili iste parnosti, što je suprotno sa pretpostavkom. Brojevi $a+b$ i $a-b$ su neparni jer su su a i b različitih parnosti. Broj b je relativno prost sa $a+b$ i $a-b$, inače bi dijelio a, što je suprotno sa $(a,b) = 1$. Nadalje, $a+b$ i $a-b$ su relativno prosti jer bilo koji zajednički djelitelj bi bio neparan i dijelio bi i a i b jer $2a = a+b+a-b$, $2b = a+2-(a-b)$. Već smo pokazali da je $3^{2\cdot 2s}$ kub pa je

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

također kub. Ako je $3^{3\cdot 2b(a+b)(a-b)}$ kub, tada je i $2b(a+b)(a-b)$ kub. S obzirom da je $(2b, a+b, a-b) = 1$ i $2b(a+b)(a-b)$ kub, prema Teoremu 3.2 su $2b$, $a-b$ i $a+b$ kubovi. Znači da postoje A, B, C takvi da je:

$$A^3 = 2b,$$

$$B^3 = a-b,$$

$$C^3 = a+b.$$

To znači da postoji još jedno rješenje Velikog Fermatovog teorema za $n = 3$:

$$A^3 = 2b = a+b-(a-b) = C^3-B^3.$$

Kako je $C^3 = a + b$ manje od $s = 3b(a-b)(a+b)$, što je opet manje od $p = 3s$, a to je manje od x^3 ili od z^3 jer: $z^3 = 2p(p^2 + 3q^2)$ ili $x^3 = 2p(p^2 + 3q^2)$. Vidimo da rješenje nužno vodi manjem rješenju Velikog Fermatovog teorema za $n = 3$.

□

Znači da nužno postoji manje rješenje i isti argument se može koristiti na tom novom rješenju da bi se pokazala egzistencija još manjeg rješenja. Time su dobiveni uvjeti za metodu beskonačnog silaska. Ovim je dokazan Teorem 3.5.

□

3.6. Veliki Fermatov teorem u slučaju $n = 5$

Teorem 3.6 *Neka $x^5 + y^5 = z^5$ ima cjelobrojna rješenja, tada je $xyz = 0$.*

Dokaz. Pretpostavimo da postoji rješenje x, y, z za $x^5 + y^5 = z^5$ gdje $xyz \neq 0$. Prema Teoremu 3.2, možemo pretpostaviti da je $(x, yz) = 1$. Također, može se pretpostaviti da su x, y neparni, a z paran. To je poznato iz sljedećeg:
Najmanje dva od tri broja su neparna jer $(x, y, z) = 1$, znači da najviše jedan može biti paran. Ako su dva neparna, onda je treći paran jer *neparan + neparan = paran* i *neparan - neparan = paran.* Neka je x paran, te neka $z' = -z$ i $x' = -x$. Sada:

$$-1^5 x'^5 + y^5 = -1^5 z'^5. \tag{12}$$

Ako se doda $(z')^5$ objema stranama jednakosti (12), dobije se:

$$-1^5 x'^5 + y^5 + z'^5 = 0. \tag{13}$$

Tada se doda x'^5 objema stranama jednakosti (13) pa je:

$$y^5 + z'^5 = x'^5.$$

Čak i u ovom slučaju, kad je x paran, dobiven je oblik $z^5 = x^5 + y^5$, gdje je z paran. Prema teoremu Sophie Germain, možemo pretpostaviti da 5 dijeli xyz. Ovdje je naveden iskaz i dokaz tog teorema.

Teorem 3.7 (**Sophie Germain**) *Ako $x^n + y^n = z^n$ i $n \geq 3$, $2n + 1$ prosti brojevi, tada n mora dijeliti xyz.*

Dokaz. Prema Teoremu 3.2, možemo pretpostaviti da $(x, yz) = 1$. Neka n dijeli xyz. Kako je n neparan, z' se ne može zapisati kao $-z$ i dobiti $x^n + y^n + z'^n = 0$, ali možemo ga zapisati u obliku:

$$-x^n = (y + z)(y^{n-1} - y^{n-2}z + \ldots - yz^{n-2} + z^{n-1}) \tag{14}$$

Korak 1.
Iz jednakosti (14) se kontradikcijom može pokazati da su $y+z$ i $y^{n-1}-y^{n-2}z+\ldots-yz^{n-2}+z^{n-1}$ relativno prosti:
Pretpostavimo da nisu relativno prosti. Tada postoji prost broj p koji dijeli $y+z$ i $y^{n-1}-y^{n-2}z+\ldots-yz^{n-2}+z^{n-1}$. Prema tome, $z\equiv -y(\text{mod } p)$. Koristeći činjenicu da su kongruentni, dobije se:

$$\begin{aligned} y^{n-1}-y^{n-2}z+\ldots-yz^{n-2}+z^{n-1} &\equiv \\ y^{n-1}-y^{n-2}(-y)+\ldots-y(-y)^{n-2}+(-y)^{n-1} &\equiv \\ y^{n-1}-y^{n-1}+\ldots-y^{n-1}+y^{n-1} &\equiv (n)y^{n-1}(\text{mod } p), \end{aligned}$$

prema Propoziciji 1.2, p ili dijeli n ili y^{n-1}. No, p ne dijeli n jer:
Broj n je prost pa bi p trebao biti jednak n ili 1. Tada bi n dijelio $-x^n$, što znači da bi, po propoziciji 1.2 dijelio x, to je suprotno sa pretpostavkom da n ne dijeli xyz.
Korak 2.
Preostaje dokazati da p dijeli y^{n-1}. Pretpostavimo suprotno, tj. neka p ne dijeli y^{n-1}. Tada bi p dijelio y i z (jer bi dijelio y i $y+z$), ali to je nemoguće jer su x,y,z relativno prosti. Time je dokazano je da su $y+z$ i $y^{n-1}-y^{n-2}z+\ldots-yz^{n-2}+z^{n-1}$ relativno prosti. Iz toga se može zaključiti, metodom beskonačnog silaska, da postoji a takav da:

$$y+z=a^n. \tag{15}$$

Isto se može pokazati i za $z+x$ i $x+y$, dakle:

$$\begin{aligned} -y^n &= (x+z)(x^{n-1}-x^{n-2}z+\ldots-xz^{n-2}+z^{n-1}), \\ -z^n &= (x+y)(x^{n-1}-x^{n-2}y+\ldots-xy^{n-2}+y^{n-1}). \end{aligned}$$

Nadalje, postoje i b i c takvi da je:

$$\begin{aligned} z+x &= b^n, \\ x+y &= c^n. \end{aligned} \tag{16}$$

Također, poznato je da bilo koja vrijednost

$$u^n\equiv \pm 1 \text{ ili } 0(\text{mod } 2n+1). \tag{17}$$

Ako pretpostavimo da $2n+1$ ne dijeli u^n (treba samo razmotriti slučaj kada u^n nije kongruentno 0), može se primijeniti Mali Fermatov teorem (Teorem 1.9) jer je $2n+1$ prost broj. Tada dobivamo: $(u^n)^2\equiv 1(\text{mod } 2n+1)$, tako da je $u^n\equiv\pm 1(\text{mod } 2n+1)$.
Prema navedenom se može zaključiti da $2n+1$ dijeli xyz':
Pretpostavimo suprotno, tj. da $2n+1$ ne dijeli xyz', tada po prethodnom rezultatu vrijedi:

$$\begin{aligned} x^n &\equiv \pm 1 \ (\text{mod } 2n+1), \\ y^n &\equiv \pm 1 \ (\text{mod } 2n+1), \\ z^n &\equiv \pm 1 \ (\text{mod } 2n+1), \end{aligned}$$

no to je nemoguće jer $x^n + y^n + (-z)^n \equiv 0(\text{mod } 2n+1)$. $\pm 1 \pm 1 \pm 1$ ne može biti kongruentno 0 (mod $2n+1$) pa odbacujemo pretpostavku da $2n+1$ ne dijeli xyz'.
Neka $2n+1$ dijeli x (isti argumenti bi se koristili i za y i z). Tada $2x = b^n + c^n + (-a)^n$.
Iz jednakosti (15) i (16), poznato je da:

$$2x = z + x + x + y - y - z = b^n + c^n + (-a)^n.$$

Korak 3.
Možemo zaključiti da $2n+1$ dijeli acb zbog:
Pretpostavljeno je da $2n+1$ dijeli x, što daje:

$$b^n + c^n + (-a)^n \equiv 0(\text{mod } 2n+1).$$

Nadalje, pretpostavimo suprotno, neka $2n+1$ ne dijeli acb. Primjenom jednakosti (17), vidimo: $b^n, c^n, (-a)^n \equiv \pm 1 \text{ (mod } 2n+1)$. No to je nemoguće zbog toga što $\pm 1 \pm 1 \pm 1$ ne može biti kongruentno 0 (mod $2n+1$). Dakle, $2n+1$ dijeli acb.

Korak 4.
Sada dokažimo da $(2n+1)$ ne može dijeliti abc.
Broj $2n+1$ ne može dijeliti b jer bi u suprotnom $2n+1$ dijelio b^n pa bi, prema jednakosti (16), slijedilo da $2n+1$ dijeli $z+x$. Poznato je da $2n+1$ dijeli x pa ako bi dijelio i $x+z$, onda bi dijelio i z. To je nemoguće jer su x, z relativno prosti. Po istom argumentu $2n+1$ ne može dijeliti c.
Pokažimo da $2n+1$ ne može dijeliti a:
Pretpostavimo suprotno, neka $2n+1$ dijeli a. Tada $2n+1$ dijeli $y+z$ što znači da

$$z \equiv -y \text{ (mod } 2n+1). \tag{18}$$

Poznato je iz Koraka 1 da postoje vrijednosti d, e takve da:

$$d^n = y^{n-1} - y^{n-2}z + \ldots - yz^{n-2} + z^{n-1},$$
$$e^n = x^{n-1} - x^{n-2}y + \ldots - xy^{n-2} + y^{n-1}.$$

Prema jednakosti (18) slijedi:

$$d^n \equiv (n)y^{n-1}(\text{mod } 2n+1). \tag{19}$$

Zbog pretpostavke da $2n+1$ dijeli x, tj. $x \equiv 0 \text{ (mod } 2n+1)$, slijedi:

$$\begin{aligned} e^n &\equiv 0^{n-1} - 0^{n-2}y + \ldots - 0y^{n-2} + y^{n-1} \\ &\equiv y^{n-1}(\text{mod } 2n+1) \end{aligned} \tag{20}$$

Primjenom jednakosti (19), dobije se:

$$d^n \equiv ne^n(\text{mod } 2n+1). \tag{21}$$

Prema jednakosti (17), poznato je da su d^n, e^n jednaki $0, 1$ ili -1, znači da te obje vrijednosti moraju biti 0 jer je to jedini način da vrijedi $0 \equiv n \cdot 0 \pmod{2n+1}$. Ako $2n+1$ dijeli d^n i e^n, tada po Propoziciji 1.2 dijeli i d i e, ali ako $2n+1$ dijeli e, po jednakosti (20), također dijeli y. Tada dijeli i x i y, što je u suprotnosti sa pretpostavkom da su x i y relativno prosti pa se odbacuje pretpostavka da $2n+1$ dijeli a. To znači da je korak 4 u kontradikciji sa korakom 3 pa odbacujemo pretpostavku da n ne dijeli xyz.

□

Nastavak dokaza Teorema 3.6. Teoremom 3.7 smo pokazali da možemo pretpostaviti kako 5 dijeli xyz. Sljedeća lema pokazuje da ako 5 dijeli z, tada ne postoje cjelobrojna rješenja jednadžbe $x^5 + y^5 = z^5$.

Lema 3.9 *Ne postoje cijeli brojevi x, y, z; x i y neparni brojevi, z paran, 5 dijeli z takvi da je $x^5 + y^5 = z^5$, $xyz \neq 0$, $(x, y, z) = 1$.*

Dokaz.
Korak 1.
Pretpostavimo suprotno, tj. neka postoje takvi x, y, z. Poznato je da postoje m, n, z' takvi da $z = 2^m 5^n z'$, $m \geq 1$, $n \geq 1$ jer 5 dijeli z i z je paran. Također, $(z', 2) = 1$, $(z', 5) = 1$ i $z^5 = 2^{5m} 5^{5n} z'^5$ pa je:

$$2^{5m} 5^{5n} z'^5 = x^5 + y^5 \tag{22}$$

Korak 2.
Postoje cijeli brojevi p, q sa sljedećim svojstvima:

(1) $(p, q) = 1$,

(2) p, q su različitih parnosti,

(3) $2^{5m} 5^{5n} z'^5 = 2p(p^4 + 10p^2q^2 + 5q^4)$,

(4) $p, q \neq 0$.

Dokaz koraka 2.
Kako su x i y neparni, znači da je $x+y$ paran broj i $x-y$ paran broj. Iz toga, poznato je da postoje p, q takvi da:

$$\begin{aligned} x + y &= 2p, \\ x - y &= 2q. \end{aligned} \tag{23}$$

Također je poznato da $(p, q) = 1$ jer:

$$\begin{aligned} x &= \frac{1}{2}(x + y + x - y) = \frac{1}{2} \cdot 2x = \frac{1}{2}(2p + 2q) = p + q, \\ y &= \frac{1}{2}[x + y - (x - y)] = \frac{1}{2} \cdot 2y = \frac{1}{2}(2p - 2q) = p - q. \end{aligned} \tag{24}$$

Ako postoji broj $d > 1$ koji dijeli p i q, prema jednakosti (24), d bi dijelio i x i y, što je nemoguće jer su relativno prosti. Također, iz jednakosti (24) se može zaključiti da su p i q različitih parnosti, inače bi x bio paran, što je suprotno sa pretpostavkom. Uvrstavanjem u jednakost (22) i prema Lemi 1.2, direktno slijedi:

$$2^{5m}5^{5n}z'^5 = (p + q)^5 + (p - q)^5 = 2p(p^4 + 10p^2q^2 + 5q^4). \tag{25}$$

Brojevi $p, q \neq 0$ jer $(x, y) = 1$ (ako $x + y = 0$ ili $x - y = 0$, onda bi $x = y$ ili $x = -y$, što je nemoguće).
Korak 3.
Postoji cijeli broj r sa svojstvima:

1. $p = 5r$,
2. $(q, r) = 1$,
3. q, r su različitih parnosti,
4. $2^{5m}5^{5n}z'^5 = 2 \cdot 5^2 r(q^4 + 5oq^2r^2 + 15 \cdot 5r^4)$,
5. 5 dijeli r,
6. $r \neq 0$.

Dokaz koraka 3. Prema jednakosti (25) i Propoziciji 1.2, 5 dijeli $2p$ ili 5 dijeli $p^4 + 10p^2q^2 + 5q^4$. Ako dijeli $2p$, onda dijeli i p. Također, ako dijeli $p^4 + 10p^2q^2 + 5q^4$, mora dijeliti i p. Zaključak je da 5 dijeli p. Tada mora postojati r takav da je $p = 5r$. Iz jednakosti (24) i $(p, q) = 1$ je $(r, q) = 1$. Kada neparan broj podjelimo sa 5, dobijemo neparan broj, a kada se paran podijeli sa 5, dobije se paran broj, stoga je r iste parnosti kao p. Brojevi r, q su različite parnosti jer je r iste parnosti kao i p. Kada u jednakost (25) uvrstimo r, dobijemo:

$$\begin{aligned} 2p(p^4 + 10p^2q^2 + 5q^4) &= 2 \cdot 5r[(5r)^4 + 10(5r)^2q^2 + 5q^4] \\ &= 2 \cdot 5r \cdot 5(125r^4 + 50r^2q^2 + q^4) \\ &= 2 \cdot 5^2 r(q^4 + 50q^2r^2 + 125r^4). \end{aligned} \tag{26}$$

Iz jednakosti (25) i (26) se vidi da 5^{5n} dijeli $2 \cdot 5^2 r(q^4 + 50q^2r^2 + 125r^4)$, tako da 5^{5n-2} dijeli $2 \cdot r(q^4 + 50q^2r^2 + 125r^4)$. Kako je $n \geq 1$, $5n \geq 5$, što znači da je $5n$ veće od 2 pa

5 dijeli $2 \cdot r(q^4 + 50q^2r^2 + 125r^4)$. Poznato je da 5 ne dijeli q jer dijeli p, a $(p, q) = 1$ pa 5 ne može dijeliti $q^4 + 50q^2r^2 + 125r^4$, nego dijeli $2r$. Po Propoziciji 1.2, kako 5 dijeli $2r$, mora dijeliti r. Broj $r \neq 0$ jer $p \neq 0$.

Korak 4.
Definiramo vrijednosti a, b, t na slijedeći način:

(1) Neka je $t = q^4 + 50q^2r^2 + 125r^4$,

(2) Neka $a = q^2 + 25r^2$,

(3) Neka $b = 10r^2$,

(4) a i b su pozitivni cijeli brojevi.

Prema Lemi 1.1 je $t = a^2 - 5b^2$. Može se izdvojiti nekoliko svojstava od a i b:

(1) $(a, b) = 1$,

(2) 5 ne dijeli a, 5 dijeli b,

(3) a i b su različite parnosti,

(4) $(2 \cdot 5^2r, t) = 1$,

(5) $t = a - 5b^2$ je peta potencija.

Dokaz svojstva 1.
Pretpostavimo da je (a, b) veći od 1, tada postoji prost broj f koji dijeli i a i b. Kako f dijeli a, onda dijeli i $10r^2$, što nam po Propoziciji 1.2 daje tri moguća slučaja:

Slučaj 1. f dijeli 2 (u ovom slučaju, $f = 2$):
a je neparan, mora biti neparan jer q, r su različitih parnosti, a kako $(\text{neparan})^2 + 25(\text{paran})^2 = \text{neparan} + \text{paran} = \text{neparan}$ i $(\text{paran})^2 + 25(\text{neparan})^2 = \text{paran} + \text{neparan} = \text{neparan}$. Prema tome, Slučaj 1 je netočan.

Slučaj 2. f dijeli 5 (u ovom slučaju, $f = 5$): f ne može biti 5 jer dijeli p i $(p, q) = 1$. To znači da 5 ne dijeli q, prema tome 5 ne dijeli $q^2 + 25r^2$. Slučaj 2 je također netočan.

Slučaj 3. Ako f dijeli r i f dijeli a, tada bi f dijelio q (jer je $a = q^2 + 25r^2$): To je nemoguće jer $(r, q) = 1$. Slučaj 3 je netočan.
Kako su sva tri slučaja netočna, ne može postojati takav prost broj f.

Dokaz svojstva 2.Iz $b = 10r^2$ se vidi da 5 dijeli b. Prema prethodnom svojstvu je $(a, b) = 1$ pa 5 ne može dijeliti a.

Dokaz svojstva 3. Iz $b = 10r^2$ se vidi da je b paran, tako da 2 dijeli b, ali 2 ne može dijeliti a jer $(a, b) = 1$.

Dokaz svojstva 4. Pretpostavimo da postoji prost broj f takav da dijeli oba broja,

$2 \cdot 5^2 r$ i t. Znamo da je t neparan iz:
Prema definiciji $t = q^4 + 50q^2r^2 + 125r^4$ te q, r su različitih parnosti. Razlikujemo dva slučaja,

Slučaj 1. q je neparan, r je paran:
$((\text{neparan})^2 + 25(\text{paran})^2)^2 - 5(10(\text{paran})^2)^2 = (\text{neparan} + 25(\text{paran}))^2 - 5(\text{paran})^2 = (\text{neparan} + \text{paran})^2 - \text{paran} = \text{neparan}^2 - \text{paran} = \text{neparan}$. Dakle, t je neparan u ovom slučaju.

Slučaj 2. q je paran, $r$je neparan:
$((\text{paran})^2+25(\text{neparan})^2)^2-5(10(\text{neparan})^2)^2 = (\text{paran}+25(\text{neparan}))^2-5(\text{neparan})^2 = (\text{paran} + \text{neparan})^2 - \text{neparan} = \text{paran}^2 - \text{neparan} = \text{paran}$. I u ovom slučaju je t neparan.

Iz ta dva slučaja se može zaključiti da je t neparan. Poznato je da $f \neq 5$ jer 5 ne dijeli t zbog toga što ne dijeli q. Na kraju, f ne može dijeliti r jer $(r, t) = 1$:
Pretpostavimo da postoji prost broj p' koji dijeli t i r. Tada p' dijeli i q, što nije moguće jer su q i r relativno prosti. Dakle, takav prost broj ne postoji pa je svojstvo 4 dokazano.

Dokaz svojstva 5. Prema jednakosti (26) je $z^5 = 2 \cdot 5^2 r$ i kako $(2 \cdot 5^2 r, t) = 1$, može se zaključiti, prema Teoremu 3.2, da su t i $(2 \cdot 5^2 r)$ pete potencije.

Dokaz svojstva 6. Svojstvo 6 vrijedi zato što su q, r cijeli brojevi različiti od 0, a kvadrat broja različitog od 0 je pozitivan broj.

Korak 5.
Prema svojstvima od a, b i t, po Lemi 1.3, postoje cijeli brojevi c i d takvi da je:

(1) $a = c(c^4 + 50c^2d^2 + 125d^4)$,

(2) $b = 5d(c^4 + 10c^2d^25d^4)$,

(3) $(c, d) = 1$,

(4) 5 ne dijeli c,

(5) 5 dijeli d,

(6) $c, d \neq 0$.

Neka je:

$$u' = c + 5d^2, \quad v' = 2d^2.$$

Možemo primjetiti da u', v' imaju sljedeća svojstva:

(1) $(u', v') = 1$,

(2) 5 ne dijeli u', 5 dijeli v',

(3) u', v' su različite parnosti,

(4) $u' - 5v'^2$ je peta potencija.

Dokaz svojstva 1. Pretpostavimo da postoji prosti broj f koji dijeli $c+5d^2$ i $2d^2$. Tada moramo obratiti pozornost na tri slučaja:

Slučaj 1. $f = 2$:
Taj slučaj je netočan jer $u' = c + 5d^2$ je neparan zato što su c i d različitih parnosti.

Slučaj 2. $f = 5$:
Taj slučaj nije točan jer 5 ne dijeli c.

Slučaj 3. f dijeli ci d:
Ovaj slučaj je također netočan jer $(c, d) = 1$.

Dokaz svojstva 2. Znamo da 5 dijeli d pa 5 dijeli $v' = 2d^2$. Broj 5 ne dijeli u' jer $(u', v') = 1$.

Dokaz svojstva 3. Broj v' je po definiciji paran broj, a već je pokazano da je u' neparan.

Dokaz svojstva 4. Izraz $c^4+10c^2d^2+5d^4$ se može zapisati u obliku $(c^2+5d^2)^2-5(2d^2)^2$ jer:

$$(c^2 + 5d^2)^2 = c^4 + 10c^2d^2 + 25d^4,$$

$$5(2d^2)^2 = -20d^4.$$

Sada, $2 \cdot 5^2r$ je peta potencija pa je $(2 \cdot 5^2r)^2$ također peta potencija:

$$\begin{aligned}(2 \cdot 5^2r)^2 &= 2 \cdot 5^3 \cdot 10r^2 \\ &= (2 \cdot 5^3) \cdot v \\ &= 2 \cdot 5^3[5d(c^4 + 10c^2d^2 + 5d^4)] \\ &= 2 \cdot 5^4d(c^4 + 10c^2d^2 + 5d^4)\end{aligned}$$

Sljedeće što moramo pokazati jest $(2 \cdot 5^4d, c^4 + 10c^2d^2 + 5d^4) = 1$:
Pretpostavimo da postoji prost broj f koji dijeli oba zadana broja. Tada moramo razmotriti tri slučaja:

Slučaj 1. $f = 2$:
Ovaj slučaj je nemoguć jer je $c^4 + 10c^2d^2 + 5d^4$ neparan zato što su c i d različite parnosti.

Slučaj 2. $f = 5$:
I ovaj slučaj je nemoguć jer 5 ne dijeli c.

Slučaj 3. f dijeli c i d:
Također nemoguć slučaj jer $(c, d) = 1$. Kombinacijom ovih rezultata, prema Teoremu 3.2, zaključujemo da su $2 \cdot 5^4d$ i $c^4 + 10c^2d^2 + 5d^4$ pete potencije.

Korak 6.
Uz pomoć svojstava navedenih u koraku 5 i prema Lemi 1.3, možemo pokazati da:

$$\begin{aligned} c + 5d^2 &= c'(c'^4 + 50c'^2d'^2 + 125d'^4), \\ 2d^2 &= 5d'(c'^4 + 10c'^2d'^2 + 5d'^4), \\ (c', d') &= 1, \\ c', d' &\text{ su različitih parnosti}, \\ 5 &\text{ ne dijeli } c', \\ 5 &\text{ dijeli } d', \\ c', d' &\neq 0. \end{aligned}$$

Možemo zapisati:

$$2 \cdot 5^8(2d^2) = 2^2 \cdot 5^8 d^2 = (2 \cdot 5^4 d)^2 \tag{27}$$

Znamo da je $2 \cdot 5^4 d$ peta potencija pa je i $(2 \cdot 5^4 d)^2$ također peta potencija.

Korak 7.
Izraz $2 \cdot 5^9 d'(c'^4 + 10c'^2d'^2 + 5d'^4)$ je peta potencija.

Dokaz koraka 7. Možemo primjetiti da je $(2 \cdot 5^8)2d^2$ peta potencija jer je prema jednakosti (27), $(2 \cdot 5^8)2d^2 = (2 \cdot 5^4 d)^2$, a $(2 \cdot 5^4 d)^2$ je peta potencija. To pokazuje da je $2 \cdot 5^9 d'(c'^4 + 10c'^2d'^2 + 5d'^4)$ peta potencija zato što:

$$\begin{aligned} 2 \cdot 5^9 d'(c'^4 + 10c'^2d'^2 + 5d'^4) &= (2 \cdot 5^8) \cdot 5d'(c'^4 + 10c'^2d'^2 + 5d'^4) \\ &= 2 \cdot 5^8 \cdot 2d^2. \end{aligned}$$

Korak 8.
$(2 \cdot 5^9 d', c'^4 + 10c'^2d'^2 + 5d'^4) = 1$

Dokaz Koraka 8. Pretpostavimo suprotno, tj. da postoji prost broj f koji dijeli oba broja, $2 \cdot 5^9 d'$ i $c'^4 + 10c'^2d'^2 + 5d'^4$. Po Propoziciji 1.2, moramo razmotriti tri slučaja.

Slučaj 1. $f = 2$:
Kako je $c'^4 + 10c'^2d'^2 + 5d'^4$ neparan broj, možemo eliminirati slučaj 1.

Slučaj 2. $f = 5$:
Možemo eliminirati i ovaj slučaj jer 5 ne dijeli c' koji ne može dijeliti $c'^4 + 10c'^2d'^2 + 5d'^4$.

Slučaj 3. f dijeli d' i $c'^4 + 10c'^2d'^2 + 5d'^4$:
Kako je $(c', d') = 1$, niti ovaj slučaj nije točan. Time je dokazan korak 8.

Sada prema koraku 8 i Teoremu 3.2 znamo da su $2 \cdot 5^9 d'$ i $c'^4 + 10c'^2d'^2 + 5d'^4$ pete potencije. Vidimo da smo u istoj poziciji kao i u koraku 5. To znači da koristeći isti argument možemo primjeniti Lemu 1.3 koliko god puta želimo.

Korak 9.

d' je veći od 0 i manji od d jer:
Prema koraku 6:

$$25d'^5 \leq 5d'(c'^4 + 10c'^2d'^2 + 5d'^4) = 2d^2.$$

Primjećujemo da:

$$5d'(c'^4 + 10c'^2d'^2 + 5d'^4) = 25d'^5 + 5d'(c'^4 + 10c'^2d'^2)$$

i:

$$25d'^5 \leq 2d^2 \ \rightarrow \ d'^5 \leq (2d^2)/25 \ \rightarrow \ d' \leq \sqrt[5]{(2d \cdot 2d)/25}.$$

Trebamo pokazati da je $\sqrt[5]{(2d \cdot 2d)/25}$ manje od d: Ako obje strane nejednakosti stavimo na petu potenciju slijedi da je $(2d^2)/25$ manje od d^5. Množenje sa 25 daje: $2d^2$ je manje od $25d^5$. Kako je $d \geq 1$, znamo da je $d^2 < d^5$. Kako smo pokazali da je $\sqrt[5]{(2d \cdot 2d)/25}$ manje od d, znamo da je onda d' manji od d.
Ako bismo nastavili ovu proceduru, došli bismo do pozitivnog cijelog broja d'' koji je manji od 1, što je nemoguće.

□

Za nastavak dokaza Teorema 3.6, pokazati ćemo da ako 5 ne dijeli z, onda ne postoje cjelobrojna rješenja jednadžbe $x^5 + y^5 = z^5$.

Lema 3.10 *Ne postoje cijeli brojevi x, y, z takvi da $x^5 + y^5 = z^5$, $xyz \neq 0$, pri čemu $(x, y, z) = 1$; x i y su neparni, z je paran i 5 dijeli x ili y.*

Dokaz. Pretpostavimo suprotno, tj. neka postoje takvi x, y, z. U svrhu dokazivanja ove leme, pretpostavit ćemo da 5 dijeli x. Isti argumenti bi vrijedili i uz pretpostavku da 5 dijeli y. Kako je x djeljiv s 5, znamo da postoje n, x' takvi da:

$$x = 5^n x', n \geq 1, \ (x', 5) = 1$$

i

$$5^{5n} x'^5 = y^5 + z^5. \tag{28}$$

Ako obje strane jednakosti (28) pomnožimo s 2^5, dobivamo:

$$2^5 5^{5n} x'^5 = 2^5(y^5 + z^5).$$

Korak 1.
Iz prethodnih jednakosti znamo da postoje dva cijela broja p, q koja zadovoljevaju sljedeća svojstva:

(1) $(p, q) = 1$,

(2) p i q su neparni brojevi,

(3) $2^5 5^{5n} x'^5 = 2p(p^4 + 10p^2q^2 + 5q^4)$,

(4) $p, q \neq 0$.

Dokaz svojstva 2. Neka je $p = y + z$, $q = y - z$, prema tome su p i q neparni.

Dokaz svojstva 1. Pretpostavimo da postoji prost broj f koji dijeli oba p i q, tj. $p = fp'$, $q = fq'$. Kako su p i q neparni, onda je i f neparan. No onda bi f dijelio i z jer $p - q = f(p' - q') = y + z - y + z = 2z$ i jer je neparan. To je nemoguće jer $(y, z) = 1$.

Dokaz svojstva 3. Prema Lemi 1.2 je:

$$\begin{aligned} 2^5 5^{5n} x'^5 &= 2^5(y^5 + z^5) \\ &= (2y)^5 + (2z)^5 \\ &= (p + q)^5 + (p - q)^5 \\ &= 2p(p^4 + 10p^2q^2 + 5q^4). \end{aligned} \tag{29}$$

Dokaz svojstva 4. Ako bi $y + z = 0$ ili $y - z = 0$, tada bi vrijedilo: $y = z$ ili $y = -z$, što je nemoguće jer $(y, z) = 1$ pa je $p, q \neq 0$.

Korak 2.

Postoji cijeli broj r sa svojstvima:

(1) $p = 5r$,

(2) $(q, r) = 1$,

(3) $2^{5m} 5^{5n} x'^5 = 2 \cdot 5^2 r(q^4 + 50q^2r^2 + 125r^4)$,

(4) 5 dijeli r,

(5) $r \neq 0$.

Dokaz svojstva 1. Prema jednakosti (29) i Propoziciji 1.2, 5 dijeli $2p$ ili 5 dijeli $p^4 + 10p^2q^2 + 5q^4$. Ako dijeli $2p$, onda dijeli p. Isto tako, ako 5 dijeli $p^4 + 10p^2q^2 + 5q^4$, onda mora dijeliti p pa postoji vrijednost r takva da je $p = 5r$.

Dokaz svojstva 2. Kako je $(p, q) = 1$, onda je i $(r, q) = 1$. Također, znamo da su r i q neparni jer neparan broj podjeljen sa 5 daje neparan broj.

Dokaz svojstva 3. Primjećujemo da primjenom r na svojstvo 4 iz koraka 1, slijedi:

$$\begin{aligned} 2p(p^4 + 10p^2q^2 + 5q^4) &= \\ 2 \cdot r[(5r)^4 + 10(5r)^2q^2 + 5q^4] &= \\ 2 \cdot 5r \cdot 5(125r^4 + 50r^2q^2 + 5q^4) &= \\ 2 \cdot 5^2 r(q^4 + 50q^2r^2 + 125r^4) \end{aligned}$$

Dokaz svojstva 4. Prema svojstvu 4 iz koraka 1 i prema prethodnom svojstvu, znamo da 5^{5n} dijeli $2 \cdot 5^2 r(q^4 + 50q^2r^2 + 125r^4)$. Prema tome 5^{5n-2} dijeli $2 \cdot r(q^4 + 50q^2r^2 + 125r^4)$. Kako je $n \geq 1$, onda $5n \geq 5$. To znači da je $5n > 2$ pa se vidi da 5 dijeli $2 \cdot r(q^4 + 50q^2r^2 + 125r^4)$. Pošto 5 dijeli p, a $(p, q) = 1$, znamo da 5 ne dijeli q. Stoga 5 ne može dijeliti $q^4 + 50q^2r^2 + 125r^4$. Prema Propoziciji 1.2, kako 5 dijeli $2 \cdot r$, mora dijeliti r.

Dokaz svojstva 5. Kako je $p \neq 0$, onda je i $r \neq 0$.

Korak 3
Neka je:

(1) $t' = q^4 + 50q^2r^2 + 125r^4$,

(2) $a' = q^2 + 25r^2$,

(3) $b' = 10r^2$.

Možemo primjetiti, prema Lemi 1.1, da je $t' = a'^2 - 5b'^2$ te da su a' i b' parni (b' je višekratnik broja 10, $a' = (\text{neparni})^2 + 25(\text{neparni})^2 = \text{neparan} + \text{neparan} = \text{paran}$). Prema tome, znamo da postoje a, b takvi da je:

$$\begin{aligned} a &= \frac{1}{2}a', \\ b &= \frac{1}{2}b'. \end{aligned} \tag{30}$$

Neka je:

$$\begin{aligned} t &= \frac{1}{4}t' \\ &= \frac{1}{4}(a'^2 - 5b'^2) \\ &= [\frac{1}{2}a']^2 - 5[\frac{1}{2}b']^2 \\ &= a - 5b^2. \end{aligned}$$

Korak 4.
Brojevi a, b, t imaju sljedeća svojstva:

(1) $(a, b) = 1$,

(2) 5 ne dijeli a, 5 dijeli b,

(3) a i b su neparni,

(4) $(5^2r) \cdot (\frac{t}{4})$ je peta potencija,

(5) $(5^2r, \frac{t}{4}) = 1$,

(6) $\frac{t}{4} = \frac{1}{4}(a - 5b^2)$ je peta potencija,

(7) a, b su pozitivni cijeli brojevi.

Dokaz svojstva 1. Prema jednakosti (30),

$$a = \frac{1}{2}(q^2 + 25r^2), \tag{31}$$

$$b = 5r^2. \tag{32}$$

Pretpostavimo da postoji prost broj f koji dijeli a i b. Tada je potrebno razmotriti tri slučaja:
Slučaj 1. $f = 2$:
Kako je r neparan, onda je i b neparan pa 2 ne može dijeliti b. Stoga je ovaj slučaj netočan.

Slučaj 2. $f = 5$:
Ovaj slučaj je netočan zato što 5 ne dijeli a. Ako bismo pomnožili obje strane jednakosti (31) sa 2, prema Propoziciji 1.2, onda bi broj 5 dijelio $q^2 + 25r^2$. No 5 ne dijeli q jer dijeli p, a $(p, q) = 1$. Stoga 5 ne može dijeliti $q^2 + 25r^2$.

Slučaj 3. f dijeli q i r:
Kako je $(q, r) = 1$, ovaj slučaj ne može biti točan. Možemo zaključiti da su a i b relativno prosti.

Dokaz svojstva 2. Iz koraka 3 znamo da 5 dijeli b, a iz prethodnog svojstva znamo da $(a, b) = 1$ pa 5 ne može dijeliti a.

Dokaz svojstva 3. Već smo pokazali da je b neparan pa je još potrebno dokazati da a također neparan. Ako je neki broj neparan, možemo ga zapisati u obliku neparan $= 2u + 1$, $(\text{neparan})^2 = (2u + 1)^2 = 4u^2 + 4u + 1$. Prema tome, $(\text{neparan})^2 \equiv 1 (\text{mod } 4)$,

$$a' \equiv q^2 + 25r^2 \equiv 1 + 1 \cdot 1 \equiv 2 (\text{mod } 4).$$

Ako je $a' \equiv 2 (\text{mod } 4)$, postoji vrijednost v takva da je $a' - 2 = 4v$ i $2a - 2 = 4v$, što znači da $a - 1 = 2v$ i $a = 2v + 1$, tj. a je neparan.

Dokaz svojstva 4. Iz svojstva 3 u koraku 1 imamo:

$$2^{5m}5^{5n}x'^5 = 2 \cdot 5^2 r(q^4 + 50q^2r^2 + 125r^4).$$

Primjenom koraka 2, dobivamo:

$$2^5 5^{5n} x'^5 = 2 \cdot 5^2 r t' = 2^3 5^2 r t. \tag{33}$$

Ako jednakost (33) podijelimo sa 2^5, slijedi:

$$5^{5n} x'^5 = \frac{5^2 r t}{4}.$$

Dokaz svojstva 5. Pretpostavimo da postoji prost broj f koji dijeli oba zadana broja. Moramo razmotriti dva slučaja:

Slučaj 1. $f = 5$:
Kako 5 ne dijeli q, ne dijeli niti t' jer $t' = q^4 + 50q^2r^2 + 125r^4$, stoga je ovaj slučaj netočan.

Slučaj 2. Broj f dijeli r i t, f je neparan (jer je r neparan):
Da bi f dijelio t, morao bi dijeliti q, ali $(r, q) = 1$. Prema tome je i ovaj slučaj netočan.

Dokaz svojstva 6. Prema koraku 3 možemo zaključiti da je $\frac{t}{4} = \frac{1}{4}(a - 5b^2)$ peta potencija.

Dokaz svojstva 7. Kako su $q, r \neq 0$, a kvadrati cijelih brojeva različitih od nule su pozitivni.

Korak 5.
Prema Lemi 1.4, možemo zaključiti da postoje c, d takvi da je:

$$\begin{aligned} a = c(c34 + 50c^2d^2 + 125d^4)/16, \\ b = 5d(c^4 + 10c^2d^2 + 5d^4)/16, \\ (c, d) = 1, \\ c, d \text{ su neparni}, \\ 5 \text{ ne dijeli } c, \\ 5 \text{ dijeli } d, \\ c, d \neq 0. \end{aligned}$$

Korak 6.
Vrijedi:

$$5^3a = \frac{1}{4}(5^4d)[(\frac{[c^2 + 5d^2]}{2})^2 - 5d^4].$$

Dokaz koraka 6.

$$\begin{aligned} 5^3a &= \frac{5^35^d(c^4 + 10c^2d^2 + 5d^4)}{16} \\ &= \frac{5^4d}{4} \cdot \frac{c^4 + 10c^2d^2 + 5d^4}{4}, \end{aligned}$$

$$(\frac{c^2 + 5d^2}{2})^2 = \frac{c^4 + 10c^2d^2 + 25d^4}{4},$$

$$\begin{aligned} (\frac{c^2 + 5d^2}{2})^2 - 5d^4 &= \frac{c^4 + 10c^2d^2 + 25d^4}{4} - 20d^4 \\ &= \frac{c^4 + 10c^2d^2 + 5d^4}{4}. \end{aligned}$$

Korak 7.
Vrijedi:

$$(\frac{c^2+5d^2}{2})^2 - 5d^4 \equiv 0(\text{mod } 4).$$

Dokaz koraka 7. Kako je c neparan i prema svojstvu 3 iz koraka 4, vrijedi:

$$c^2 \equiv 1(\text{mod } 4).$$

Kako je d neparan i prema svojstvu 3 iz koraka 4, vrijedi:

$$5d^2 \equiv 1 \cdot 1 \equiv 1(\text{mod } 4).$$

Nadalje,

$$5d^4 \equiv 5(d^2)^2 \equiv 1 \cdot 1 \equiv 1(\text{mod } 4),$$

$$\begin{aligned}(\frac{c^2+5d^2}{2})^2 - 5d^4 &\equiv \frac{1+1}{2} \cdot \frac{1+1}{2} - 1 \\ &\equiv 1 \cdot 1 - 1 \\ &\equiv 0(\text{mod } 4)\end{aligned}$$

Korak 8.
Vrijedi:

$$(\frac{5^4 d}{4}, (\frac{c^2+5d^2}{2})^2 - 5d^4) = 1$$

Dokaz koraka 8. Pretpostavimo da postoji prost broj f takav da dijeli oba broja. Prema Propoziciji 1.2, $f = 5$ ili f dijeli d. Kako 5 ne dijeli c, f ne može biti 5. Također, ako bi f dijelio d, onda bi dijelio i $(\frac{c^2+5d^2}{2})^2 - 5d^4$, što znači da bi dijelio i c. To je nemoguće jer $(c, d) = 1$.

Korak 9.
Prema Teoremu 3.2, znamo da su $5^4 d$ i $\frac{1}{4}(\frac{c^2+5d^2}{2})^2 - 5d^4$ pete potencije.

Korak 10.
Prema Lemi 1.4, znamo da postoje c', d' takvi da je

$$\begin{aligned}a &= c'(c'^4 + 50c'^2d'^2 + 125d'^4), \\ b &= 5d'(c'^4 + 10c'^2d'^2 + 5d'^4)/16, \\ (c', d') &= 1, \\ c', d' &\text{ su neparni}, \\ 5 &\text{ ne dijeli } c', \\ 5 &\text{ dijeli } d', \\ c', d' &\neq 0.\end{aligned}$$

Korak 11.
Možemo primjetiti da vrijedi:

$$5^8 d^2 = \frac{1}{4} 5^9 d'[(\frac{c'^2+5d'^2}{2})^2 - 5(d'^2)^2].$$

Dokaz koraka 11.

$$\begin{aligned} 5^8 d^2 &= \frac{5^9 d'(c'^4 + 10c'^2 d'^2 + 5d'^4)}{16} \\ &= \frac{5^9 d'}{4} \cdot \frac{c'^4 + 10c'^2 d'^2 + 5d'^4}{4}, \end{aligned}$$

$$(c'^2 + 5d'^2)^2 = c'^4 + 10c'^2 d'^2 + 25d'^2,$$

$$\begin{aligned} \frac{c'^4 + 10c'^2 d'^2 + 5d'^4}{4} &= \frac{(c'^2 + 5d'^2)^2 - 20d'^2}{4} \\ &= (\frac{(c'^2 + 5d'^2)^2}{2})^2 - 5(d'^2)^2. \end{aligned}$$

Korak 12.

$$(5^9 d', \frac{1}{4}(\frac{(c'^2 + 5d'^2)^2}{2})^2 - 5(d'^2)^2) = 1$$

Dokaz koraka 12. Pretpostavimo da postoji prost broj f koji dijeli oba dana broja. Tada je $f = 5$ ili f dijeli d'. Kako 5 ne dijeli c', onda je $f \neq 5$. Kada bi f dijelio d', onda bi dijelio i $\frac{1}{4}(\frac{(c'^2+5d'^2)^2}{2})^2 - 5(d'^2)^2$, što je nemoguće jer $(c', d') = 1$.

Korak 13.

Možemo primjetiti da je $5^8 d^2$ peta potencija.

Dokaz koraka 13. Kako $5^8 d^2 = (5^4 d)^2$, a $5^4 d$ je peta potencija, onda je $5^8 d^2$ također peta potencija.

Korak 14.

Prema Teoremu 3.2, možemo zaključiti da su $5^9 d'$ i $\frac{1}{4}(\frac{(c'^2+5d'^2)^2}{2})^2 - 5(d'^2)^2)$ pete potencije.

Korak 15.

$d' \geq 1$ i $d' < d$.

Dokaz koraka 15. Prema koraku 10 je $25d'^5 < 16d^2$ i $d' > 0$. Pretpostavimo da je $d' \geq d$. U tom slučaju bi $25d'^5$ bilo veće od $16d^2$ jer su d', d cijeli brojevi, 25 je veće od 16 i d'^5 je veće od d'^2, a $d'^2 \geq d^2$. No to je nemoguće pa odbijamo pretpostavku.

Korak 16.

Ovaj proces možemo ponavljati d puta koristeći Lemu 1.4 i dobiti cijeli broj d'' koji je manji od 1 i veći od 0, što je nemoguće.

□

Imamo kontradikciju pa možemo odbaciti početnu pretpostavku. Time je dokazan Teorem 3.6.

□

Literatura

[1] A. D. Aczel, Posljednji Fermatov teorem, Izvori, Zagreb, 2001.

[2] F.M.Brückler, Pierre de Fermat, Osječki matematički list 5, Odjel za matematiku, Sveučilište J.J.Strossmayera u Osijeku i Udruga matematičara Osijek, Osijek, 2005., 37-42

[3] B. Dakić, P. Mladinac, B. Pavković, Elementarna teorija brojeva, HMD -Element, Zagreb, 1994.

[4] H. M. Edwards, Fermat's Last Theorem, Springer-Verlag, New York, 1977.

[5] G. A. Jones, J. Mary Jones, Elementary Number Theory, Springer, London, 2003.

[6] M. Šušak, Fermatov posljednji teorem: diplomski rad, Osijek, 2001.

Sažetak

U radu je obrađena tema Fermatov Veliki teorem. Objašnjeni su osnovni pojmovi iz područja teorije brojeva koji su potrebni za razumjevanje samog problema i rješavanje posebnih slučajeva teorema. Prikazan je povijesni kontekst nastanka teorema, od samog začetka problema i kulture Babilonaca do Pierrea de Fermata i njegove bilješke na margini knjige te razvoja i napokon dokazivanja teorema 1994. Također su navedeni dokazi za posebne slučajeve Velikog Fermatovog teorema koji se mogu riješiti elementarnim metodama.

Ključne riječi: Fermatov Veliki teorem, Andrew Wiles, posebni slučajevi Velikog Fermatovog teorema

Summary

This paper deals with Fermat's last theorem. There are shown basic concepts of number theory that are necessary for understanding the problem and solving the special cases of theorem. Also, there is an overview of historical context of the inception, development and finally proving of the problem in 1994. Paper also identifies proves for special cases of Fermat's last theorem which can be solved by elementary methods.

Key words: Fermat's last theorem, Fermat, Andrew Wiles, Special cases of Fermat's last theorem

Životopis

Rođena sam 29. prosinca 1987. godine u Našicama. Osnovnu školu sam završila u Koški, a Prirodoslovno matematičku gimnaziju u Našicama. Obrazovanje sam nastavila na Preddiplomskom studiju matematike, na Odjelu za matematiku u Osijeku 2005. godine koji sam završila 2008. godine, uz završni rad *Redovi realnih brojeva*, pod vodstvom mentora prof.dr.sc. Dragana Jukića te stekla naziv Sveučilišnog prvostupnika (baccalaurea) matematike. Iste godine sam nastavila studiranje na Sveučilišnom diplomskom studiju matematike - smjer Financijska i poslovna matematika. U ljetnom semestru akademske godine 2008./2009. sudjelovala sam u projektu "Matematika s 1/2 muke" tijekom kojeg su podučavani studenti Sveučilišta Josipa Jurja Strossmayera u Osijeku.