Neki povijesno-matematički osvrti na posljednji Fermatov teorem

Željko Zrno, kninsko Veleučilište „Marko Marulić“

Uvod

Snažan impuls teoriji brojeva dao je francuski pravnik i matematičar *Pierre de Fermat* (1601.-1665.). Kao amater u matematici, za života nije objavio gotovo ništa od svojih radova, ali je zato u nasljedstvo matematičarima ostavio mnoštvo razrađenih ili nerazrađenih ideja. Mnoge su njegove hipoteze dokazane, neke su oborene, ali jedna koja je najviše odolijevala napadu matematičara i koja je zadnja dokazana, nakon više od 350 godina, poznata pod nazivom *„posljednja Fermatova teorema“*, zaslužuje da joj ovdje poklonimo malo više pažnje.

Fermatova tvrdnja glasi: jednadžba $x^n + y^n = z^n, n \in \mathbf{N}, \ n > 2$, nema rješenja u skupu prirodnih brojeva.

Kad je Pierre de Fermat umro 1665. godine, bio je jedan od najslavnijih matematičara Evrope. Danas je Fermatovo ime gotovo sinonim za teoriju brojeva, ali je u njegovo vrijeme njegov rad u teoriji brojeva bio tako revolucionaran i toliko ispred njegovog vremena da je njegova vrijednost bila jedva shvaćena. Postoje dvije iznenađujuće činjenice o Fermatovoj slavi kao matematičara. Prva je ta da on uopće nije bio matematičar, nego pravnik. Drugo iznenađenje je da on nikad nije objavio matematički rad. Njegova reputacija je rezultat njegove korespondencije s drugim znanstvenicima i niza rasprava koje su kružile u pisanom obliku. Fermat je bio često potican da objavi svoj rad, ali je zbog neobjašnjenih razloga odbijao da njegove rasprave budu objavljene. Mnoga njegova otkrića, naročito njegova otkrića u teoriji brojeva, nikad nisu bila prevedena u oblik dostupan za objavu. Ova činjenica da je Fermat odbijao objavljivanje svog rada je izazvala strah njegovih brojnih obožavatelja da će uskoro biti zaboravljen ne bude li uložen napor radi skupljanja njegovih pisama i

neobjavljenih rasprava i njihove posthumne objave. Taj je zadatak preuzeo njegov sin Samuel. On je tražio pisma i rasprave od korespondenata koji su bili u kontaktu s njegovim ocem. Samuel de Fermat je također pregledavao papire i knjige svog oca i tako je objavljen slavni Fermatov posljednji teorem.

Diofantova ARITMETIKA, jedno od velikih klasičnih djela antičke grčke matematike koje je bilo ponovno otkriveno i prevedeno na latinski kratko prije Fermatovog vremena, bila je knjiga koja je nadahnula Fermatovo proučavanje teorije brojeva. Samuel je otkrio da je njegov otac ispisao mnoge zabilješke na rubovima njegove kopije Bachetovog prijevoda Diofanta. Kao prvi korak u objavljivanju radova njegovog oca on je objavio novo izdanje Bachetovog Diofanta u čijem su dodatku bile Fermatove rubne bilješke i primjedbe. Druga od ovih 48 primjedbi o Diofantu je bila napisana na rubu uz Diofantov problem 8 u knjizi II gdje se traži da se dani kvadrat prikaže u obliku dva kvadrata. Fermatova bilješka tvrdi na latinskom jeziku da *„kub nije moguće prikazati kao sumu dva kuba, niti je četvrta potencija suma četvrtih potencija, niti općenito* n*-ta potencija za* $n \geq 3$ *ne može biti suma dvije* $n-te$ *potencije. Imam doista krasan dokaz ove propozicije, ali je ovaj rub preuzak da se na njemu taj dokaz napiše.“*

Ako je Fermat doista imao dokaz, on je doista morao biti čudesan jer nitko drugi nije uspio pronaći dokaz, kako smo već rekli, u više od 350 godina nakon Fermatovog vremena.

U svibnju 1995. je objavljen dokaz Fermatovog posljednjeg teorema. Dokaz je dao ***Andrew Wiles*** sa sveučilišta Princeton.

U nastavku ćemo iznijeti neke osvrte iz povijesti pokušaja dokazivanja ovog teorema i davanju doprinosa razvoju matematike u kontekstu iznalaženja novih teorija iz matematike. Krenimo od aktualnog vremena, gdje ćemo prikazati dramu koja se odvijala kod profesora Andrew Wilesa na konferenciji u Cambridgu 1993., a zatim slijedi povratak u daleku prošlost i kronološki put kod pokušaja dokazivanja posljednjeg Fermatovog teorema. (vidi [1])

Cambridge, Engleska, srpanj 1993.

Krajem srpnja 1993., profesor Andrew Wiles odletio je u Englesku. Vraćao se na sveučilište Cambridge gdje je prije dvadeset godina bio na poslijediplomskim studijima. Wilesov nekadašnji mentor pri izradi doktorske teze, profesor *John Coates*, upriličio je konferenciju o Iwasawinoj teoriji-jednom posebnom području u okviru teorije brojeva na koje se odnosila i disertacija Andrewa Wilesa i u koje je on bio vrlo dobro upućen. Četrdesetogodišnji Wiles izgledao je kao tipičan matematičar kada je došao u Cambridge: bijela košulja s nehajno zavrnutim rukavima, naočale s debelim, rožnatim okvirom, neuredni pramenovi već prorijeđene svijetle kose. Njegov povratak u Cambridge, u kojem se rodio , bio je vrlo poseban-bio je ostvarenje jednoga dječačkog sna. Tragajući za ovim snom, Andrew Wiles proveo je prošlih sedam godina života kao doslovni zatvorenik na vlastitom tavanu.

Prvoga dana Wiles je nagradio dvadesetak matematičara koji su došli na njegovo predavanje jednim velikim i neočekivanim matematičkim rezultatom-a ostala su još dva izlaganja. Što je sljedeće? Svima je postalo jasno da su Wilesova predavanja ona kojima treba biti nazočan. Napetost je počela rasti među matematičarima kojih je sada bilo znatno više.

Drugoga dana, Wilesovo izlaganje se pojačalo. Sa sobom je ponio preko 200 stranica formula i izvoda, originalnih zamisli iskazanih kao novi teoremi, s dugim, apstraktnim dokazima. Dvorana je sada bila ispunjena do posljednjeg mjesta.

Sljedećeg dana, u srijedu 23. srpnja 1993., došao je red na posljednje predavanje. Dok je prilazio dvorani u kojoj ga je trebao održati, Wiles si je morao krčiti put kroz okupljene slušatelje. Ljudi su stajali i u hodniku, zaprečavajući ulaz, a unutra je bilo sve puno. Mnogi su ponijeli fotografske aparate. Dok je Wiles opet ispisivao naizgled beskonačne formule i teoreme na ploči, atmosfera je postojala sve napetija. „Postojao je samo jedan mogući

vrhunac, jedan mogući kraj Wilesovog predavanja“, rekao je kasnije profesor *Ken Ribet* s Kalifornijskog sveučilišta u Berkeleyu. Wiles je bio pri kraju posljednjih redova svoga dokaza jedne zagonetne i složene matematičke zamisli, takozvane pretpostavke *Shimure* i *Taniyame*. Zatim je neočekivano dodao još jedan red na kraju, novi oblik jedne već stoljećima stare jednadžbe, za koju je Ken Ribet sedam godina ranije dokazao da će predstavljati posljedicu spomenute pretpostavke. „Ovo dokazuje posljednji Fermatov teorem“, rekao je Wiles gotovo usput. „Mislim da ću ovdje stati.“

Uslijedio je trenutak mukle tišine u dvorani. A onda se prolomio gromovit, spontani pljesak. Bljeskalice su sijevale dok su svi ustali čestitati ozarenom Wilesu. Samo nekoliko minuta zatim, elektronska pošta i faksovi počeli su slati poruke na sve strane svijeta. Najznamenitiji matematički problem svih vremena bio je, kako izgleda, riješen.

„Najneočekivanije u svemu bilo je to što su nas sljedećeg dana preplavili svjetski mediji“, sjeća se profesor John Coates koji je organizirao konferenciju, uopće ne sluteći da će na njoj biti objavljeno jedno od najvećih matematičkih postignuća. Naslovi u vodećim svjetskim novinama veličali su neočekivani podvig. „Konačno, Eureka!, o davnoj matematičkoj tajni- pojavilo se na naslovnoj strani *New York Timesa* od 24. srpnja 1993. Preko noći, tihi i vrlo povučeni Andrew Wiles postao je svjetsko ime.

Lipanj-kolovoz 1993.-otkrivena je kobna pogreška

Matematičari su bili obazrivo optimistički raspoloženi kada je Wiles sišao s podija one srijede u srpnju. Izgledalo je da je tajna stara 350 godina konačno riješena. Ostalo je da neovisni stručnjaci provjere Wilesov opsežan dokaz, pun složenih matematičkih oznaka i teorija koje uopće nisu bile poznate u Fermatovo doba, odnosno sve do početka dvadesetoga stoljeća. Dokaz je poslan određenom broju vodećih matematičara. Možda se sedmogodišnji samotnjački

rad na tavanu Wilesu konačno isplatio. Ali optimizam nije dugo trajao. Samo nekoliko tjedana kasnije uočena je pukotina u Wilesovoj logici. On ju je pokušao zakrpati, ali se ona nije mogla ukloniti. Matematičar s Princetona Peter Sarnak, blizak prijatelj Andrewa Wilesa, promatrao ga je kako svakoga dana tone sve dublje u beznađe povodom dokaza za koji je prije samo dva mjeseca na Cambridgeu objavio cijelom svijetu da ga ima. Wiles se opet povukao na tavan. Novinari iz *New York Timesa* i ostalih medija ostavili su ga da obavlja svoj samotnjački posao. Kako je vrijeme prolazilo, a dokaz se nije pojavljivao, matematičari i javnost počeli su se pitati je li Fermatov teorem doista točan. Čudesan dokaz za koji je profesor Wiles tvrdio da ga ima postao je nimalo više stvaran od samog Fermatovog *„doista čudesnog dokaza koji se nažalost ne može zapisati na premaloj margini“*

Kvadrati, kubovi i više dimenzije

Da bi se dokazalo da je posljednji Fermatov teorem pogrešan, sve što je netko trebao napraviti bilo je pronaći triplet cijelih brojeva a,b i c i stupanj n veći od dva, tako da je $a^n + b^n = c^n$. Nitko još nije našao takve cijele brojeve. U devedesetim godinama dvadesetoga stoljeća dokazano je da takvi cijeli brojevi ne postoje za vrijednosti n manje od četiri milijuna. Ali ovo još nije značilo da se takvi brojevi ipak neće pronaći jednoga dana. Teorem je trebalo dokazati za *sve* cijele brojeve i *sve* moguće stupnjeve.

Fermat je sam dokazao svoj posljednji teorem za $n = 4$. Upotrijebio je jednu domišljatu metodu koju je nazvao metoda „beskonačnog opadanja“ dokazujući da ne postoje cijeli brojevi a,b i c za koje bi važilo $a^4 + b^4 = c^4$. Fermat je također dokazao svoj teorem za $n = 3$. Poznati švicarski matematičar *Leonhard Euler* (1707.-1783.) dokazao je slučajeve $n = 3$ i $n = 4$ neovisno o Fermatu, dok je *Peter G. L. Dirichlet* dokazao 1828. slučaj $n = 5$. Isto je dokazao *Adrien-*

Marie Legendre 1830. *Gabriel Lamé* i *Henri Lebesgue*, koji ga je ispravio 1840., izveli su dokaz za $n = 7$. I tako, dvije stotine godina nakon što je Fermat napisao svoju znamenitu bilješku na margini Diofantove knjige, njegov teorem dokazan je jedino za stupnjeve 3, 4, 5, 6 i 7. No, još je dug put do beskonačnosti, a upravo se ona mora imati u obliku da bi se teorem dokazao za *bilo koji* stupanj n. Matematičari su krenuli u potragu za tim neuhvatljivim općim dokazom, ali sve što su nalazili bili su dokazi za posebne potencije.

Karl Friedrich Gauss

Po mnogima najveći matematičar svih vremena *Karl Friedrich Gauss* (1777.-1855.) bavio se i teorijom brojeva, o kojima je on izvještavao kolege običnim dopisivanjem, bili su od ogromne pomoći u svim pokušajima matematičara kako dokazati posljednji Fermatov teorem. Većina ovih rezultata skupljena je u knjizi o teoriji brojeva koju je Gauss objavio na latinskom 1801., kada su mu bile dvadeset četiri godine. Ta knjiga, *Disquisitiones Aritmeticae*, prevedena je na francuski i objavljena u Parizu 1807., privukavši veliku pozornost. Ocijenjena je kao djelo genija.

Zašto, međutim, najveći matematički svjetski genij nikada nije pokušao dokazati posljednji Fermatov teorem? Gaussov prijatelj H. W. M. Olbers poslao mu je pismo iz Bremena 7. ožujka 1816., u kojem ga je izvijestio da je Pariška akademija ponudila veliku nagradu onome tko dokaže da je posljednji Fermatov teorem točan ili pogrešan. Ali Gauss je odolio tom iskušenju. Možda je bio svjestan koliko je, zapravo, zavodljiv posljednji Fermatov teorem. Veliki genij u teoriji brojeva vjerojatno je bio jedini matematičar u cijeloj Europi koji je shvaćao koliko bi bilo teško da se on dokaže.

Idealni brojevi

Matematičar koji se upustio u faktorizaciju bio je *Ernst Eduard Kummer* (1810.-1893.) – čovjek koji se više od bilo kojeg drugog suvremenika približio općem rješenju Fermatovog problema. Kummer je, zapravo, izumio čitavu jednu matematičku teoriju, teoriju *idealnih brojeva*, pokušavajući dokazati posljednji Fermatov teorem.

Kummer se bavio širokim rasponom problema u matematici, od vrlo apstraktnih do vrlo praktičnih. Ali glavni ugled stekao je opsežnim radom na posljednjem Fermatovom teoremu. Francuski matematičar *Augustin-Louis Cauchy* (1789.-1857.) pomislio je u nekoliko navrata da je došao do općeg rješenja Fermatovog problema. Ali neumorni i nehajni Couchy shvatio je svaki put da je problem znatno veći nego što je on pretpostavljao. Couchy je konačno digao ruke od problema i posvetio se drugim stvarima.

Kummer je također postao opsjednut posljednjim Fermatovim teoremom, a njegovi pokušaji da dođe do rješenja uputili su ga istom besplodnom stazom kojom je išao i Couchy. Ali umjesto da digne ruke kada se pokazalo da brojno polje koje se tu javljalo nema odgovarajuće svojstvo, on je jednostavno izumio nove brojeve s osobinom koje su njemu bile potrebne. Te brojeve nazvao je „idealni brojevi“. U jednom trenutku učinilo mu se da je konačno došao do općeg dokaza, ali pokazalo se nažalost da ipak nije tako. Do sredine devetnaestog stoljeća, zahvaljujući Kummerovom nevjerojatnom podvigu, ustanovljeno je da posljednji Fermatov teorem vrijedi za sve potencije manje od $n = 100$, kao i za beskonačno mnogo multiplikatora prostih brojeva iz tog raspona. Bilo je to veliko dostignuće, iako nije predstavljalo opći dokaz, budući da je postojalo još beskonačno mnogo brojeva za koje se nije znalo vrijedi li teorija i za njih. Kummer je neumorno nastavio raditi na dokazivanju posljednjeg Fermatovog teorema, obustavivši istraživanje tek 1874.

Zbog povijesne kronologije, vezano za posljednji Fermatov teorem, ovdje bi samo kratko spomenuli još neke matematičare: godine 1922. engleski matematičar *Louis J. Mordell* otkrio je nešto za što mu se učinilo da je vrlo neobična veza između rješenja algebarskih jednadžbi i topologije.
Dvadeset sedmogodišnji njemački matematičar *Gerd Faltings* uspio je dokazati 1983. Mordellovu pretpostavku, što je koristilo u daljnjem dokazivanju i za sve veće potencije. Status posljednjeg Fermatovog teorema 1983. godine bio je, dakle, sljedeći: on je dokazan za sve vrijednosti n do milijun (ovo je pomaknuto 1992. godine na 4 milijuna.)

Konačno dokaz

Kada je prošlo više od godinu dana od njegovog kratkotrajnog trijumfa u Cambridgu, Andrew Wiles počeo je gubiti nadu i bio je već spreman dići ruke od nepotpunog dokaza. Odlučio je još jednom, posljednji put, razmotriti svoj dokaz prije nego što ga odbaci i odustane od nade da će riješiti posljednji Fermatov teorem. Wiles se udubio u papire pred sobom, pažljivo ih proučavajući dvadesetak minuta. A onda je jasno zamijetio gdje je zapelo. Konačno je shvatio što nije bilo kako treba. „Bio je to najvažniji trenutak u cijelom mom radnom životu“, opisao je on kasnije osjećaje koje ga je tada ispunilo.“Odjednom, potpuno neočekivano, uslijedilo je nevjerojatno otkriće. Ništa što će u budućnosti napraviti ne može se…“ Suze su ispunile Wilesove oči, a glas mu je zakazao od uzbuđenost. Ono što je razaznao u tom ključnom trenutku bilo je „tako neopisivo lijepo, tako jednostavno i tako elegantno…a ja sam samo zurio u nevjerici.“ Ostao je dugo zagledan u svoj rad. Vjerojatno sanjam, pomislio je, ovo je previše lijepo da bi bilo istinito. Kasnije će reći da je, zapravo, stvar bila previše lijepa da bi bila pogrešna. Otkriće je bilo tako snažno, tako skladno, da je jednostavno *moralo* bit točno.

Wiles je ispisao novi dokaz, koristeći sada vodoravnu Iwasawinu teoriju. Konačno, sve je savršeno došlo na svoje mjesto. Pristup koji je koristio prije tri godine bio je točan. Uzbuđen, Andrew Wiles, uspostavio je vezu s internetom. Poslao je istu poruku elektronskom poštom na adrese više matematičara širom svijeta: „Očekujte hitnu pošiljku od mene za koji dan." Tijekom sljedećih nekoliko tjedana, matematičari koji su dobili novu verziju Wilesovog rada iz Cambridgea, pažljivo su provjerili svaku pojedinost iz nje. Nisu uspjeli naći nikakav nedostatak. Umjesto da postupi kao što je to učinio u Cambridgeu godinu i pol dana ranije, poslao je rad jednom profesionalnom časopisu, *Annals of Mathematics*, tako da je on prije objavljivanja prošao postupak provjere i ocjenjivanja stručnjaka. Ovo je potrajalo nekoliko mjeseci, ali sada nije uočena nikakva pogreška. U svibanjskom broju za 1995. ovog časopisa objavljeni su Wilesov prvobitni rad iz Cambridgea i ispravak ispod kojeg su bili potpisani Wiles i *Richard Taylor*, matematičar koji mu je asistirao oko ispravka. *Posljednji Fermatov teorem konačno je bio dokazan.*

Je li Fermat imao dokaz?

Andrew Wiles opisuje svoj dokaz kao „tekovinu matematike dvadesetog stoljeća". On se doista oslanjao na radove mnogih matematičara dvadesetoga stoljeća. Koristio je i djela ranijih matematičara. Mnoštvo elemenata koji tvore Wilesovu građevinu plod su rada mnogih drugih autora. Prema Wilesu, Fermat nikako nije mogao imati na umu ovaj dokaz kada je napisao svoju znamenitu bilješku na margini. To je očito, budući da se pretpostavka *Shimure* i *Taniyame* pojavila tek u dvadesetom stoljeću. Ali je li moguće da je Fermat imao u vidu neki drugi dokaz? Odgovor je vjerojatno niječan. Ali stvar ipak nije sasvim izvjesna. To nikada nećemo doznati. S druge strane, Fermat je živio još 28 godina nakon što je na margini zapisao svoj teorem. A više ga nikada nije spomenuo. Možda je znao da ga ne može dokazati. Ili je možda pogrešno

pomislio da se njegova metoda beskonačnog opadanja, koja je koristila da bi dokazao jednostavan slučaj kada je $n = 3$, može proširiti na opće rješenje. Ili je možda jednostavno zaboravio na ovaj teorem i prešao na druge probleme.

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. Završni dokaz teorema proizašao je iz udruživanja prirodno nespojivih područja matematike. A unatoč činjenici da je Andrew Wiles bio osoba koja je obavila važan konačni rad na teoremu, dokazavši jedan oblik pretpostavke Shimure i Taniyame neophodan da bi se dokazao Fermatov teorem, cijeli podhat je djelo mnogih ljudi.

Fermat, dakako, nikako nije mogao oblikovati tako složenu pretpostavku koja objedinjuje dvije vrlo različite grane matematike. Ili je možda mogao? Stvar nije do kraja jasna. Sve što sigurno znamo da je teorem konačno potvrđen, kao i to da su dokaz provjerili i potvrdili do najsitnijih pojedinosti mnogi matematičari iz cijelog svijeta. Ali okolnost da ovaj složen dokaz postoji ne znači nužno da neki jednostavniji nije moguć. Prema tome, je li Fermat doista imao „doista čudesni dokaz“ svoga teorema, koji nije mogao stati na malom raspoloživom prostoru, zauvijek će ostati tajna.

U nastavku ovog članka osvrnut ćemo se kratko na matematički dio Fermatovog teorema uz prethodnu obradu jednadžbe $x^2 + y^2 = z^2,\ x, y, z \in \boldsymbol{N}$, poznate kao Pitagorin teorem. Naravno za ovu razinu napraviti ćemo elementaran pristup i to u povijesnom kontekstu, a čitatelja upućujemo na literaturu u kojoj može naći više razine i opći dokaz posljednjeg Fermatovog teorema, u kojem se koristi složen matematički aparat.

Pitagorine trojke

Bavljenje posljednjim Fermatovim problemom počinje slučajem $n = 2$, to jest Pitagorinom jednadžbom $x^2 + y^2 = z^2$. Pri tome treba primijetiti da ako je d bilo koji divizor brojeva x, y, z, tada se faktor d^2 može izlučiti iz jednadžbe $x^2 + y^2 = z^2$, pa brojevi $\frac{x}{d}, \frac{y}{d}, \frac{z}{d}$ također formiraju Pitagorinu trojku. Ako je d najveći zajednički divizor brojeva x, y, z, tada brojevi $\frac{x}{d}, \frac{y}{d}, \frac{z}{d}$ nemaju zajednički divizor osim 1, pa ta tri broja tvore ono što se zove *primitivna Pitagorina trojka*. Na taj način svaka Pitagorina trojka može biti reducirana (dijeljenjem s najvećim zajedničkim divizorom) na primitivnu Pitagorinu trojku. Obrnuto, za danu primitivnu Pitagorinu trojku (a, b, c) se može dobiti opća Pitagorina trojka (x, y, z) izborom odgovarajućeg cijelog broja d tako da se stavi $x = ad, y = bd, z = cd$. Zbog toga je za bavljenje jednadžbom $x^2 + y^2 = z^2$ dovoljno baviti se primitivnom Pitagorinom trojkom.

Ova pretpostavka (o primitivnosti Pitagorine trojke x, y, z) znači da nijedan par od tri broja x, y, z nema zajednički divizor veći od 1. Na primjer, ako je d divizor od x, y, tada iz $x^2 + y^2 = z^2$ slijedi da je d^2 divizor od z^2, a to znači da je d divizor od z. Dakle je d divizor od x, y, z, ali iz primitivnosti Pitagorine trojke slijedi $d = 1$. Na sličan način, jedini zajednički divizor od x, z i od y, z mora biti 1.

Posebno, nijedan par među brojevima x, y, z ne može sadržavati parne brojeve, to jest imati divizor jednak 2. Zbog toga su barem dva broja među brojevima x, y, z neparna. No, očigledno je da sva tri ne mogu biti neparni jer $x^2 + y^2 = z^2$ tada znači neparan+neparan=neparan što je nemoguće. Zato je točno jedan među brojevima x, y, z paran. To sigurno nije broj z jer ako je z paran, a x, y neparni, tada je z^2 djeljiv brojem 4, a x^2(zbog neparnosti od x) dijeljenjem s 4 daje ostatak 1, a to isto vrijedi za y^2, što znači da je $x^2 + y^2 \equiv 2 \pmod 4$ odnosno $z^2 \equiv 2 \pmod 4$ što je nemoguće jer smo vidjeli da je $z^2 \equiv 0$

(mod 4). Prema tome, u primitivnoj Pitagorinoj trojki (x, y, z) broj z je neparan, a brojevi x, y su suprotne parnosti-jedan je među njima paran, a drugi je neparan.

Kako dobiti proizvoljno primitivno rješenje Pitagorine jednadžbe? Neka je (x, y, z) primitivna Pitagorina trojka koja zadovoljava jednadžbu $x^2 + y^2 = z^2$. Pretpostavljamo da je broj x paran, a brojevi y, z neparni. Vrijedi $x^2 = z^2 - y^2$ ili $x^2 = (z - y)(z + y)$. Brojevi $z - y, z + y$ su parni, pa je $z - y = 2u,\ z + y = 2v$ za neke $u, v \in \mathbf{N}$. Brojevi u, v su uzajamno prosti jer ako je $u = \omega\alpha, v = \omega\beta$ za neke $\omega, \alpha, \beta \in \mathbf{N}$, tada je $z = \omega(\alpha + \beta),\ y = \omega(\beta - \alpha)$. Međutim, brojevi y, z su uzajamno prosti, pa je nužno $\omega = 1$. Drugim riječima $u = \omega\alpha, v = \omega\beta \Rightarrow \omega = 1$, čime je pokazano da su y, z uzajamno prosti. Iz $x^2 = 4uv$ i parnosti broja x slijedi da je u, v kvadrat. Budući da su u, v uzajamno prosti, svaki od njih je kvadrat. Neka je $u = q^2, v = p^2$. Tada je $z - y = 2q^2,\ z + y = 2p^2$ ili $z = p^2 + q^2, y = p^2 - q^2, x = 2pq$.
Iz $y = p^2 - q^2$ vidimo da je $p > q$. Također su p, q uzajamno prosti zbog $u = q^2, v = p^2$ i zato jer su u, v uzajamno prosti. Iz neparnosti broja y slijedi da su brojevi p, q različite parnosti. Time je dokazano:
Ako je (x, y, z) *primitivno rješenje od* $x^2 + y^2 = z^2$, *tada postoje uzajamno prosti* $p, q \in \boldsymbol{N}$ *suprotne parnosti sa svojstvom* $p > q$ *tako da je* $x = 2pq,\ y = p^2 - q^2,\ z = p^2 + q^2$.

Fermatov teorem za slučaj $\boldsymbol{n = 4}$

Prethodni rezultat omogućava dokaz posljednjeg Fermatovog teorema za jednadžbu četvrtog stupnja $x^4 + y^4 = z^4$, to jest da ne postoje prirodni brojevi $x, y, z \in \mathbf{N}$ sa svojstvom $x^4 + y^4 = z^4$. Dokaz provodimo metodom kontradikcije uz pretpostavku da postoje x, y, z s tim svojstvom.

Smatramo da trojka maksimalno skraćena što znači da su brojevi x, y, z u parovima uzajamno prosti. Tada je x^2, y^2, z^2 primitivna Pitagorina trojka jer $x^4 + y^4 = z^4$ zapravo znači $(x^2)^2 + (y^2)^2 = (z^2)^2$. To pak znači da postoje $p, q \in \mathbf{N}$ sa svojstvom:

$$x^2 = 2pq,\ y^2 = p^2 - q^2,\ z^2 = p^2 + q^2 \qquad (*)$$

uz uvjet $p > q$, brojevi p, q su uzajamno prosti i suprotne parnosti. Iz $y^2 + q^2 = p^2$ slijedi da je y, q, p Pitagorina trojka u kojoj su p, q uzajamno prosti, pa je to primitivna Pitagorina trojka. Iz $y^2 + q^2 = p^2$ slijedi da je p neparan, pa je q paran (jer su p, q suprotne parnosti). Zbog toga postoje $a, b \in \mathbf{N}$ sa svojstvom:

$$q = 2ab,\ y = a^2 - b^2,\ p = a^2 + b^2 \qquad (**)$$

pri čemu je $a > b$, uz uvjet da su $a, b \in \mathbf{N}$ uzajamno prosti i suprotne parnosti.

Sada iz (*) i (**) slijedi $x^2 = 4ab(a^2 + b^2)$, pa je $ab(a^2 + b^2) = \left(\frac{x}{2}\right)^2$ što znači da je $ab(a^2 + b^2)$ kvadrat.

Brojevi $ab, a^2 + b^2$ su uzajamno prosti jer brojevi q, p takvi, pa ako je broj $ab(a^2 + b^2)$ kvadrat, to je svaki od brojeva $ab, a^2 + b^2$ kvadrat. Brojevi a, b su također uzajamno prosti, pa je svaki od njih kvadrat, uzmimo $a = u^2, b = v^2$. Odavde slijedi ovaj lanac zaključaka:

$$u^4 + v^4 = a^2 + b^2 = p < p^2 + q^2 = z^2 < z^4 = x^4 + y^4.$$

Time je dokazano: ako je $x^4 + y^4$ kvadrat (z^4 je naime kvadrat), tada postoje $u, v \in \mathbf{N}$ sa svojstvom $u^4 + v^4 < x^4 + y^4$. No, broj $u^4 + v^4$ je kvadrat, pa postoje $r, s \in \mathbf{N}$ sa svojstvom $r^4 + s^4 < u^4 + v^4$ tako da je $r^4 + s^4$ kvadrat. Analognim zaključivanjem slijedi da postoje $c, d \in \mathbf{N}$ sa svojstvom $c^4 + d^4 < r^4 + s^4$ tako da je $c^4 + d^4$ kvadrat, pa dobivamo silazni beskonačni niz kvadrata prirodnih brojeva što je nemoguće jer je skup prirodnih brojeva ograničen odozdo najmanjim brojem 1. Prema tome ne postoje brojevi $x, y \in \mathbf{N}$ za koje je $x^4 + y^4 = z^4$. Time je posljednji Fermatov teorem dokazan u slučaju $n = 4$.

U dokazu $x^4 + y^4 \neq z^4$ je korištena metoda beskonačnog spuštanja koja je na neki način metoda matematičke indukcije unatrag. Fermat je izumio tu metodu i na nju je bio vrlo ponosan. U dugačkom pismu koje je napisao potkraj života je napravio osvrt na svoja otkrića u teoriji brojeva da je tu metodu koristio u svim svojim dokazima. Kratko rečeno, metoda dokazuje da stanovita svojstva ili relacije nisu moguće za cijele brojeve dokazom da ako bi oni vrijedili za neke brojeve, tada bi vrijedili za neke manje brojeve i tako dalje u beskonačnost, a to je nemoguće jer niz pozitivnih cijelih brojeva ne može opadati u beskonačnost.
Tu metodu je nazvao-*metoda beskonačnog spoštanja*.

Fermatov teorem za slučaj $n = 3$

Dokaz ovog slučaja dao je Euler. Leonhard Euler je nesumnjivo bio najveći matematičar svog vremena. Dao je doprinose na svakom zamislivom području, od primijenjene matematike do algebarske topologije i teorije brojeva. Bez obzira što postoje kontroverze oko toga da li je Euler dokazao slučaj $n = 3$, najuobičajeniji stav je da je Euler dao dokaz slučaja $n = 3$, ali da je njegov dokaz „nepotpun“ u jednom važnom pogledu, uz postojanje defekta koji je u međuvremenu otklonjen, ali mu se odaje priznanje eleganciji pristupa.
Temeljna metoda Eulerovog dokaza slučaja $n = 3$ je metoda beskonačnog spuštanja. On pokazuje da ako postoje prirodni brojevi x, y, z sa svojstvom $x^3 + y^3 = z^3$, tada je moguće pronaći manje prirodne brojeve s istim svojstvom. Na taj način je moguće pronaći niz takvih trojki koje kontinuirano opadaju i nikad ne završavaju, a to je očigledno nemoguće. Dokaz počinje od pretpostavke da imamo trojku prirodnih brojeva za koje vrijedi $x^3+y^3=z^3$. Svaki zajednički divizor bilo koja dva od ta tri broja je zbog te jednadžbe istovremeno divizor trećeg broja. Zbog toga je sve zajedničke faktore moguće ukloniti, pa je na samom početku moguće pretpostaviti da su brojevi x, y, z u

parovima relativno prosti, a to znači da je najveći zajednički divizor od x, y ili x, z ili od y, z jednak 1. Posebno je tada najviše jedan od ova tri broja paran jer ako bi još jedan bio paran, tada bi i onaj treći morao biti paran, pa bi njihov zajednički divizot bio barem 2. S druge strane je barem jedan od brojeva x, y, z paran jer ako bi svi bili neparni, tada bismo imali situaciju neparan+neparen=neparan što je nemoguće. Zbog toga je točno jedan od ovih brojeva paran, a preostala dva su neparna. (više i detaljnije o ovom slučaju vidi u [2])

Opći dokaz Fermatovog teorema uz jedno ograničenje na z

Opći dokaz Fermatovog posljednjeg teorema u najopćenitijem slučaju, da ne postoje $x, y, z \in \mathbf{N}$, $n \geq 3$, $x^n + y^n = z^n$ je vrlo težak i opsežan. (vidi [5])
Ipak, postoji jednostavan dokaz tog teorema uz jedno ograničenje, a to je $z < 1 + \frac{1}{\sqrt[n]{2}-1}$.
Ovdje je taj dokaz. (vidi [4])
Neka je dakle za dani eksponent $n \in \mathbf{N} \setminus \{1,2\}$ broj $z \in \mathbf{N}$ takav da je
$z < 1+\frac{1}{\sqrt[n]{2}-1}$. Dakle je $z - 1 < \frac{1}{\sqrt[n]{2}-1}$.
Jasno je zbog $x^n + y^n = z^n$ da je $z > 1$ pa vrijedi $\frac{1}{z-1} > \sqrt[n]{2} - 1$. Dakle je $1 + \frac{1}{z-1} > \sqrt[n]{2}$. Znači:
$\frac{z}{z-1} > \sqrt[n]{2}$, pa dizanjem na n-tu potenciju imamo $\frac{z^n}{(z-1)^n} > 2$, iz čega zaključujemo:

$$z^n > 2(z-1)^n. \qquad (*)$$

Iz $z^n = x^n + y^n$ slijedi $z \geq y + 1, z \geq x + 1$ ili $z - 1 \geq y, z - 1 \geq x$. Znači

$(z-1)^n \geq y^n, (z-1)^n \geq x^n$.

Zbrajanje prethodnih nejednakosti daje $x^n + y^n \leq 2(z-1)^n$, pa iz (*) slijedi $z^n > 2(z-1)^n \geq x^n + y^n$ ili $z^n > x^n + y^n$. Što je u kontradikciji sa $x^n + y^n = z^n$. Dakle x, y, z u slučaju $z < 1 + \frac{1}{\sqrt[n]{2}-1}$ ne predstavljaju rješenje jednadžbe $x^n + y^n = z^n$.

Jedan problem iz vjerojatnosti koji se svodi na posljednji Fermatov teorem

Postavljamo sljedeći problem: (vidi [3])

U svakoj od dvije kutije nalazi se isti broj kuglica, s tim da su u svakoj kutiji samo bijele i crne kuglice. Iz tih se kutija n puta izvlači po jedna kuglica i ona se ponovno vraća natrag. Odrediti broj izvlačenja n i sadržaj obje kutije ako je vjerojatnost da su iz prve kutije izvučene samo bijele kuglice jednaka vjerojatnosti da su iz druge kutije izvučene ili samo crne ili samo bijele kuglice.

Rješenje:

Ako se provode dva izvlačenja, tada je ovo Pitagorin problem koji ima beskonačno mnogo rješenja. Uzmimo kao primjer $x = 3, y = 4, z = 5$. To znači da u drugoj kutiji ima $x + y = 7$ kuglica i od toga su tri bijele i četiri crne. U prvoj kutiji ima $z = 5$ bijelih kuglica, ali onda moraju u njoj biti i dvije crne kuglice jer u obje kutije mora biti sedam kuglica.

Vjerojatnost da u dva izvlačenja iz prve kutije izvučemo samo bijelu kuglicu je $\left(\frac{5}{7}\right)^2$. Vjerojatnost da su iz druge kutije izvučene samo bijele kuglice je $\left(\frac{3}{7}\right)^2$, a samo crne kuglice $\left(\frac{4}{7}\right)^2$.

Doista je $\left(\frac{5}{7}\right)^2 = \left(\frac{3}{7}\right)^2 + \left(\frac{4}{7}\right)^2$.

Ako se pak radi o jednom izvlačenju, tada imamo jednadžbu $z = x + y$. Tada u prvoj kutiji trebaju biti samo bijele kuglice (z bijelih kuglica), a u drugoj treba

biti x bijelih kuglica i y crnih kuglica. Drugim riječima, sastav druge kutije je proizvoljan, a u prvoj kutiji su samo bijele kuglice i ima toliko koliko ima ukupno svih kuglica (bijelih i crnih) u drugoj kutiji.

Općenito:

Ako sa z označimo broj bijelih kuglica u prvoj kutiji, s x broj bijelih, a s y broj crnih kuglica u drugoj kutiji, onda se problem svodi na nalaženje brojeva $n, x, y, z \in \mathbf{N}$, takvih da je

$$\left(\frac{z}{x+y}\right)^n = \left(\frac{x}{x+y}\right)^n + \left(\frac{y}{x+y}\right)^n \text{ ili } z^n = x^n + y^n .$$

Dakle, prepoznajemo posljednji Fermatov teorem, za koji znamo, zahvaljujući mnogim matematičarima kroz povijest ali ipak najviše Andrew Wilesu, nema rješenje za $n > 2$. *Zaključujemo da postavljeni problem nema rješenje ako je broj izvlačenja veći od dva.*

Literatura

[1] Amir Aczel, *Fermatov posljednji teorem*, Biblioteka LUČ, preveo Damir Mikuličić, Zagreb, 2001.

[2] Harold M. Edwards, *Fermat̀s Last Theorem*, Springer, travanj 1977.

[3] Pavković-Svrtan-Veljan, *Matematika 3*., *Zbirka zadataka s uputama i rješenjima*, Školska knjiga, Zagreb, 1975.

[4] *Matematika* (stručno –metodički časopis), Sarajevo, broj 2, 1980.

[5] *Annals of Mathematics*, Modulator Elliptic Curves And Fermaťs Last Theorem, 1995.