ACTA MATHEMATICA SPALATENSIA
Series didactica
Vol.3 (2020) 55–62

Metoda beskonačnog spusta i Fermatov posljednji teorem

Ivona Alković, Marija Bliznac Trebješanin

Sažetak

Priča o Fermatovom posljednjem teoremu i potrazi za njegovim dokazom poznata je i onima koji nisu detaljno proučavali matematiku. U ovom ćemo radu dati kratki uvod u Posljednji teorem te predstaviti konstrukciju Pitagorinih trojki i Fermatovu metodu beskonačnog spusta kojom je Fermat dokazao da je teorem istinit za slučaj $n = 4$, to jest, da diofantska jednadžba $x^4+y^4 = z^4$ nema rješenja u prirodnim brojevima.

Ključni pojmovi: metoda beskonačnog spusta, diofantska jednadžba, pitagorine trojke

1 Uvod

Pierre de Fermat (1601. – 1665.) je jedan od najpoznatijih matematičara, a posebno je poznat po svome Posljednjem teoremu za koji, iako ima jednostavnu formulaciju, nije nikada pronađen kratak i jednostavan dokaz. Fermat je Posljednji teorem zapisao na margini svoje kopije knjige *Aritmetika* Diofanta iz Aleksandrije te je dodao da ima sjajan dokaz te tvrdnje, ali da je margina preuska da on na nju stane. Međutim, taj dokaz nikad nije nađen u njegovoj ostavštini. Za konačan dokaz je bilo potrebno više od 300 godina rada stotine matematičara te je teorem konačno dokazao Andrew Wiles 1995. godine.

Teorem 1 (Fermatov posljednji teorem)**.** *Neka je $n \geq 3$ prirodan broj. Tada diofantska jednadžba*

$$x^n + y^n = z^n \tag{1}$$

nema rješenja u prirodnim brojevima $x,\ y,\ z$.

Ako je $n = 2$, onda jednadžba (1) ima rješenja u prirodnim brojevima. Ta rješenja nazivamo Pitagorine trojke, a o njima ćemo više reći u sljedećem poglavlju.

Nakon toga prezentirat ćemo ukratko metodu beskonačnog spusta i ilustrirati njenu primjenu u dokazu slučaja $n = 4$ Fermatovog posljednjeg teorema. Ta metoda se koristi i u dokazu za još neke slučajeve, npr. $n = 3$, $n = 5$ i $n = 14$, no matematičari su ubrzo uvidjeli da postupak uvelike ovisi o svojstvima broja n i da metoda beskonačnog spusta vjerojatno neće moći dati dokaz teorema za opći slučaj.

Postoji mnoštvo različitih dokaza slučaja $n = 4$. Na primjer, svoj dokaz su dali i Leonhard Euler (1707. – 1783.), Adrien-Marie Legendre (1752. – 1833.), Joseph Bertrand (1822. – 1900.), Joseph-Louis Lagrange (1736. – 1813.) te David Hilbert (1862. – 1943.), a mi ćemo navesti onaj koji je dao sam Fermat. U postupku dokaza koristi se metoda generiranja Pitagorinih trojki pa ćemo se prvo osvrnuti na taj problem.

2 Pitagorine trojke

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

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

Ukoliko su pritom brojevi x, y i z relativno prosti, onda kažemo da je (x, y, z) primitivna Pitagorina trojka.

Primijetimo da jednakost $3^2 + 4^2 = 5^2$, po Pitagorinom teoremu, implicira da je bilo koji trokut kojemu su stranice u omjeru $3 : 4 : 5$ pravokutan trokut, pa stoga postoji beskonačno mnogo Pitagorinih trojki oblika $(3k, 4k, 5k)$, $k \in \mathbb{N}$. Vidimo da u postupku traženja Pitagorinih trojki, važnost ima određivanje primitivnih Pitagorinih trojki, koje zatim generiraju ostale trojke s istim omjerom stranica.

Primjer 2. *Trojka* $(3, 4, 5)$ *je najočitiji i najpoznatiji primjer Pitagorine trojke. Sljedeći primjer s najmanjom katetom je* $(5, 12, 13)$*, zatim* $(6, 8, 10)$*, ali vidimo da je ta trojka generirana primitivnom trojkom* $(3, 4, 5)$.

Metoda kojom ćemo tražiti rješenja jednadžbe (1) je, u klasičnoj grčkoj matematici, bila poznata kao analitička metoda. Pretpostavimo da je dano jedno rješenje jednadžbe $x^2 + y^2 = z^2$ u prirodnim brojevima te analiziramo svojstva tog rješenja kako bismo pronašli njegove karakteristike i metodu za konstrukciju ostalih rješenja.

Primijetimo najprije sljedeće: ako je (x, y, z) jedno rješenje jednadžbe (1) te ako je $d > 1$ neki prirodni broj koji dijeli sva tri broja x, y i z, onda uvrštavanjem tog rješenja u (1) i skraćivanjem s d^2, dobivamo da brojevi x/d, y/d, z/d i dalje tvore Pitagorinu trojku. Zato, bez smanjenja općenitosti, možemo pretpostaviti da je rješenje kojeg promatramo primitivna Pitagorina trojka.

Lema 3 (Primitivne Pitagorine trojke)**.** *Za bilo koje prirodne brojeve x, y i z koji su relativno prosti i zadovoljavaju jednakost $x^2 + y^2 = z^2$, postoje prirodni brojevi p i q takvi da je*

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

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

Dokaz. Budući da je naša Pitagorina trojka primitivna, najviše jedan od brojeva x, y, i z može biti paran. Inače, kad bi dva broja bila parna, onda bi morao biti i treći pa trojka ne bi bila primitivna jer bi 2 bio zajednički djelitelj od x, y i z. Dakle, barem su dva neparna. Očito ne mogu sva tri broja biti neparna jer bi onda iz jednakosti $x^2 + y^2 = z^2$ slijedilo da je suma dvaju neparnih broja neparna, što je nemoguće. Dakle, samo je jedan od tih brojeva paran. Sada želimo pokazati da je z neparan, iz čega slijedi da su x i y različite parnosti. Ako je z paran, može se zapisati kao $2n$, za neki prirodni broj n. Tada su x i y neparni i mogu se zapisati u obliku $2n_1 + 1$ i $2n_2 + 1$ redom, za neke prirodne brojeve n_1 i n_2. Vidimo da je $x^2 = 4n_1^2 + 4n_1 + 1 = 4(n_1^2 + n_1) + 1$ pa ima ostatak 1 pri dijeljenju s 4. Slično se vidi da i y^2 ima ostatak 1 pri dijeljenju s 4. Znamo da je $z = 2n$ paran pa imamo da je $z^2 = 4n^2$ djeljiv s 4. U jednakosti $x^2 + y^2 = z^2$ lijeva strana ima ostatak $1 + 1 = 2$ pri dijeljenju s 4, a desna strana ostatak 0, što očito ne može vrijediti. Ovo pokazuje da z mora biti neparan. Dakle, ili je x ili y paran broj pa, bez smanjenja općenitosti, pretpostavimo da je x paran.

Zapišimo sada jednakost $x^2 + y^2 = z^2$ u obliku $x^2 = z^2 - y^2$. Faktorizacijom dobijemo $x^2 = (z - y)(z + y)$, gdje su očito x, $z - y$ i $z + y$ parni brojevi pa postoje prirodni brojevi u, v i w takvi da je $x = 2u$, $z + y = 2v$ i $z - y = 2w$. Uvrštavanjem u jednakost $x^2 = (z - y)(z + y)$ dobije se $(2u)^2 = (2v)(2w)$, odnosno $u^2 = vw$.

Pokažimo da su v i w također relativno prosti brojevi. Uočimo prvo da su z i y relativno prosti jer su brojevi x, y i z relativno prosti i vrijedi $x^2 + y^2 = z^2$. Budući da najveći zajednički djelitelj od v i w dijeli $v + w = \frac{1}{2}(z + y) + \frac{1}{2}(z - y) = z$ i $v - w = \frac{1}{2}(z + y) - \frac{1}{2}(z - y) = y$, a

brojevi z i y su relativno prosti, onda su v i w također relativno prosti brojevi pa kako je $vw = u^2$, v i w moraju biti kvadrati prirodnih brojeva. Ovo povlači da postoje relativno prosti prirodni brojevi p i q takvi da je

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

Činjenica da je y prirodan broj povlači da je p veći od q, a kako su z i y neparni, p i q moraju biti različite parnosti. Možemo koristiti jednakost $x^2 = z^2 - y^2$ kako bismo x zapisali pomoću p i q. Imamo

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

što daje $x = 2pq$.

Pokazali smo da za bilo koju primitivnu Pitagorinu trojku u kojoj je x paran uvijek možemo pronaći vrijednosti p i q koje zadovoljavaju tražene uvjete.

Analizu konstrukcije Pitagorinih trojki dovršimo pokazujući da je za bilo koje prirodne brojeve p i q takve da su p i q relativno prosti, različite parnosti i za koje vrijedi $p > q$, trojka $(2pq, p^2 - q^2, p^2 + q^2)$ primitivna Pitagorina trojka. Lako je provjeriti da vrijedi željena jednakost

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

Sada je preostalo još pokazati da su brojevi $2pq$, $p^2 - q^2$ i $p^2 + q^2$ relativno prosti. Koristit ćemo činjenicu da su p i q relativno prosti kako bismo pokazali da su $2pq$ i $p^2 - q^2$ također relativno prosti. Pretpostavimo suprotno, tj. da postoji prost broj d koji dijeli brojeve $2pq$ i $p^2 - q^2$. Kako je $p^2 - q^2$ neparan broj, mora vrijediti $d \neq 2$. Prema tome, d mora dijeliti p ili q, ali ne oba jer su relativno prosti. Pretpostavimo da $d \mid p$. Tada $d \mid p^2 - q^2$ i $d \mid p^2$ pa bi slijedilo da $d \mid q^2$, to jest $d \mid q$, što ne može biti. Analogno se pokaže kontradikcija i ako pretpostavimo da $d \mid q$. □

Lema 3 u potpunosti rješava problem konstruiranja svih Pitagorinih trojki. Primitivne Pitagorine trojke koje odgovaraju parovima p i q za koje je $p \leq 8$ dane su u Tablici 1. Sada ćemo ilustrirati primjerom konstrukciju Pitagorinih trokuta s jednom zadanom stranicom.

Zadatak 4. *Pronađimo sve Pitagorine trokute koji imaju hipotenuzu duljine* 25.

Rješenje. Neka je $(x, y, 25)$ Pitagorina trojka i neka je d najveći zajednički djelitelj brojeva x, y i 25. Kako $d \mid 25$ vidimo da je $d \in \{1, 5, 25\}$.

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

Tablica 1: Pitagorine trojke

Očito $d \neq 25$ jer bismo imali Pitagorin trokut s hipotenuzom 1, a takav nije mogući.

Promotrimo slučaj $d = 5$. Tada je Pitagorina trojka $(x/5, y/5, 5)$ primitivna. Iz Tablice 1 vidimo da je jedina primitivna Pitagorina trojka s hipotenuzom 5 trojka $(3, 4, 5)$ (znamo da se vrijednost $z = 5$ neće postići za $p > 2$ ili $q > 1$ jer je $z > \max\{p^2, 2q^2\}$). Ova primitiva trojka, množenjem s 5, daje Pitagorinu trojku $(15, 20, 25)$.

Preostaje promotriti slučaj $d = 1$. Tada je Pitagorina trojka $(x, y, 25)$ primitivna. Znamo da mora vrijediti $p^2 + q^2 = 25$ za neke prirodne brojeve $p > q$ različite parnosti. Kratkim ispitivanjem ili iščitavanjem Tablice 1 vidimo da je jedina takva primitivna Pitagorina trojka $(24, 7, 25)$ za $(p, q) = (4, 3)$.

Time smo promotrili sve mogućnosti i dokazali da su jedini Pitagorini trokuti s hipotenuzom duljine 25 oni kojima su duljine stranica $(15, 20, 25)$ i $(24, 7, 25)$. □

3 Metoda beskonačnog spusta

Fermat je osmislio metodu beskonačnog spusta te naveo da svi njegovi dokazi koriste ovu metodu. Ta metoda se koristi za opovrgavanje tvrdnji vezanih za prirodne brojeve. Ideja je sljedeća: ako pokažemo da iz pretpostavke da tvrdnja vrijedi za neki proizvoljan prirodan broj, slijedi da tvrdnja mora vijediti i za neki strogo manji prirodan broj, onda, analognim zaključivanjem slijedi da će vrijediti i za još manje brojeve, i tako dalje *ad infinitum*[1], što je nemoguće jer ne postoji beskonačan strogo padajući niz prirodnih brojeva.

Na primjer, dokažimo tvrdnju koja je korištena u prethodnom odjeljku: *ako su v i w relativno prosti prirodni brojevi i ako je vw kvadrat, onda v i w oba moraju biti kvadrati.* U ovom slučaju, ono što treba pokazati jest da je nemoguće da postoje brojevi v i w takvi da su 1) v i w relativno prosti, 2) vw je kvadrat, i 3) v i w nisu oba kvadrati.

[1] ad infinitum - do beskonačnosti

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

Ukratko, metoda beskonačnog spusta temelji se na sljedećem principu: *Ako pretpostavka da postoji prirodni broj, koji ima dani skup svojstava, povlači da postoji strogo manji prirodni broj s istim skupom svojstava, onda ne postoji prirodni broj s tim skupom svojstava.*

4 Slučaj $n = 4$ Posljednjeg teorema

Teorem 5 (Slučaj $n = 4$)**.** *Ne postoje rješenja jednadžbe*

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

u skupu prirodnih brojeva.

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

Pretpostavimo da su x, y i z prirodni brojevi za koje vrijedi $x^4+y^4 = z^4$. Promatrat ćemo prirodan broj x koji ima svojstvo da postoji prirodni broj y takav da je $x^4 + y^4$ kvadrat nekog prirodnog broja (u prethodnoj jednakosti je to broj z^2). Cilj nam je pokazati da ako postoji takav prirodan broj x, onda postoji i strogo manji prirodni broj X s istim

svojstvom, što, po metodi beskonačnog spusta, povlači da prirodan broj x s danim svojstvom ne postoji.

Kao u slučaju Pitagorinih trojki, možemo bez smanjenja općenitosti pretpostaviti da su x, y i z relativno prosti. Stoga je (x^2, y^2, z^2) primitivna Pitagorina trojka pa brojeve x^2, y^2 i z^2 možemo zapisati u obliku

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

gdje su p i q relativno prosti prirodni brojevi, različite parnosti i vrijedi $p > q$. Druga od ove tri jednakosti može se zapisati u obliku $y^2 + q^2 = p^2$ pa lako vidimo, budući da su p i q relativno prosti, da je (y, q, p) primitivna Pitagorina trojka. Dakle, p mora biti neparan pa kako su p i q različite parnosti, q je paran. Stoga,

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

gdje su a i b relativno prosti prirodni brojevi, različite parnosti i vrijedi $a > b$. Prema tome, vrijedi jednakost

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

Ovo pokazuje da je broj $ab(a^2+b^2)$ kvadrat, preciznije, kvadrat polovine parnog broja x. Međutim, ab i a^2+b^2 su relativno prosti zato što bilo koji prosti broj P koji dijeli ab, dijeli a ili b, ali ne i oba (jer su a i b relativno prosti) i stoga ne može dijeliti $a^2 + b^2$. Dakle, ab i $a^2 + b^2$ moraju biti kvadrati nekih prirodnih brojeva. Međutim, kako je ab kvadrat i kako su a i b relativno prosti, a i b oba moraju biti kvadrati. Zapišimo $a = X^2$, $b = Y^2$. Tada je $X^4 + Y^4 = a^2 + b^2$ kvadrat nekog prirodnog broja i vrijedi $X < x$ budući da je $x^2 = 4ab(a^2 + b^2) > a = X^2$. Štoviše, imamo $X^4 + Y^4 = a^2 + b^2 = p < p^2 + q^2 = z^2 < z^4 = x^4 + y^4$. Dakle, iz početne pretpostavke da postoje prirodni brojevi x i y takvi da je $x^4 + y^4$ kvadrat, dobili smo novi par prirodnih brojeva X i Y takav da je $X^4 + Y^4$ kvadrat prirodnog broja pri čemu je $X < x$. Stoga, po metodi beskonačnog spusta, prirodan broj x s danim svojstvom ne postoji, odnosno, suma četvrtih potencija dva prirodna broja ne može biti kvadrat pa posebno ni četvrta potencija nekog broja. Na ovaj način smo dokazali Fermatov posljednji teorem za slučaj $n = 4$. □

Iz Teorema 5 očito slijedi da jednažba $x^{4m}+y^{4m} = z^{4m}$ nema rješenja u prirodnim brojevima kad god je m prirodan broj jer bi inače $X = x^m$,

$Y = y^m$, $Z = z^m$ bilo rješenje diofantske jednadžbe $X^4 + Y^4 = Z^4$. Prema tome, Fermatov posljednji teorem je istinit za sve eksponente n djeljive s 4. Eksponent $n > 2$ koji nije djeljiv s 4 nije potencija broja 2 i stoga mora biti djeljiv s nekim prostim brojem $p \neq 2$, recimo $n = pm$. Kako bi se pokazalo da $x^n + y^n = z^n$ nema rješenje u skupu prirodnih brojeva, očito je preostalo pokazati da $x^p + y^p = z^p$ nema rješenje za nijedan prost broj $p > 2$. Dakle, jednom kada je Fermatov posljednji teorem bio dokazan za slučaj $n = 4$, dokaz općeg slučaja se reducirao na dokaz slučaja kada je $n > 2$ prost broj. Međutim, iako se još neki slučajevi mogu riješiti metodom beskonačnog spusta, koraci metode ovise o svojstvima samog prostog broja p. Za slučaj $p = 3$, Leonhard Euler je dao dokaz, no on je sadržavao veliku grešku zbog nerazumijevanja rastava na proste faktore u prstenu $\mathbb{Z}[\sqrt{-3}]$. Kasnije je Euler dokazao lemu kojom je popravio i dovršio dokaz pa se smatra da je ipak on dao prvi dokaz tog slučaja Fermatovog posljednjeg teorema.

Literatura

[1] C. Byerley, *Applications of Number Theory to Fermats Last Theorem*, `https://www.whitman.edu/Documents/Academics/Mathematics/byerleco.pdf` (pristup ostvaren 24. 10. 2019.)

[2] A. Dujella, *Teorija brojeva*, Školska knjiga, 2019.

[3] H. M. Edwards, *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*, Springer-Verlag, 1996.

[4] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, New York, 1979.

Ivona Alković
studentica, Sveučilište u Splitu, Prirodoslovno-matematički fakultet, Ruđera Boškovića 33, Split
E-mail adresa: `ivona.alkovic@gmail.com`

Marija Bliznac Trebješanin
Sveučilište u Splitu, Prirodoslovno-matematički fakultet, Ruđera Boškovića 33, Split
E-mail adresa: `marbli@pmfst.hr`

Zaprimljen: 28. listopada 2019.
Prihvaćen: 28. siječnja 2020.