Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Preddiplomski studij matematike

Nikolina Duvnjak

Pitagorine trojke

Završni rad

Osijek, 2015.

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Preddiplomski studij matematike

Nikolina Duvnjak

Pitagorine trojke

Završni rad

Mentor: doc.dr.sc. Ivan Matić

Osijek, 2015.

Sadržaj

Sažetak

U završnom radu ćemo predstaviti Pitagorine trojke. Objasnit ćemo začetak Pitagorinog teorema, razloge nastajanja i način generiranja Pitagorinih trojki. Upoznat ćemo se s primitivnim Pitagorinim trojkama, te objasniti postupak njihova dobivanja. Na kraju ćemo iskazati i dokazati Veliki Fermatov teorem za N=4.

Ključne riječi:

Pitagora, Pitagorine trojke, primitivna rješenja, jedinična kružnica, polinomi, Fermat

Abstract

In this final paper we are going to introduce Pythagorean triples. We will explain beginning of Pythagorean theorem, reasons of its arise and way of generating Pythagorean triples. We will get insight with primitive Pythagorean triples and explaine the process of finding them. Finally, we will demonstrate and prove Fermat's Last Theorem gor N=4.

Keywords:

Pythagoras, Pythagorean triples, primitive solutions, unit circle, polynomials, Fermat

1 Uvod

Pitagora iz Samosa često se prikazuje kao prvi "pravi" matematičar. On je vrlo važna osoba koja je doprinjela razvoju matematike, iako u biti znamo malo o njegovome matematičkom radu. Od Pitagorinih djela, nažalost, ništa nije sačuvano. Tajnovitost i zajedništvo djelovanja njegove škole otežava nam razlikovanje Pitagorinih rezultata od rada njegovih sljedbenika. Glavna područja Pitagorinog zanimanja bila su pojam broja, trokuta i apstraktna ideja dokaza. Naravno, mi danas pamtimo Pitagoru po poznatom Pitagorinom poučku, iako ga on nije prvi otkrio već prvi dokazao. U prvom dijelu rada ćemo se upoznati sa Pitagorinim teorem i njegovim shvaćanjem kroz povijest. Drugo poglavlje je posvećeno Pitagorinim trojkama gdje ćemo proučiti način njihova generiranja i postupak pronalaženja svih primitivnih Pitagorinih trojki. Na kraju rada ćemo iskazati Veliki Fermatov teorem za N=4 i dokazati ga na dva različita načina.

2 Pitagorin teorem

2.1 Pitagorin teorem kroz povijest

Ako postoji jedan teorem koji je poznat svim matematički obrazovanim ljudima, to je sigurno Pitagorin teorem, odnosno Pitagorin poučak.

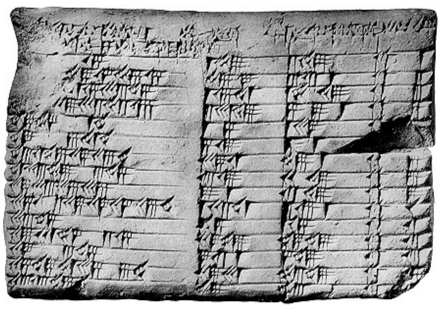
Teorem 1 (Pitagorin poučak)**.** *Zbroj kvadrata nad katetama pravokutnog trokuta jednak je kvadratu nad njegovom hipotenuzom.*

Pitagorejci su spomenuti teorem doživljavali u kontekstu površina. Točnije rečeno, njihovo shvaćanje iskaza Pitagorina poučka jest sljedeće: možemo uzeti kvadrat čija je duljina stranice jednaka duljini hipotenuze pravokutnog trokuta i razrezati ga na dijelove koji preslagivanjem daju dva kvadrata, od kojih jedan ima stranicu duljine jedne katete, a drugi duljine druge katete.

Pitagorin teorem nije samo najstariji matematički teorem, nego i izvor triju matematičkih pojmova: brojeva, geometrije i beskonačnosti. Tijek brojeva počinje s uređenom trojkom (a, b, c) sa svojstvom $a^2 + b^2 = c^2$. Tijek geometrije počinje interpretacijom brojeva a^2, b^2 i c^2 kao kvadrata stranica pravoknutnog trokuta sa katetama a i b, te hipotenuzom c, te se beskonačnost odnosi na otkriće da je iracionalni broj $\sqrt{2}$ hipotenuza pravokutnog trokuta sa katetama duljine 1.

Pitagorejci su živjeli oko 500 godina prije Krista, ali priča o Pitagorinom teoremu počinje puno ranije, bar 1800 godina prije Krista u Babilonu. Dokaz je glinena pločica, poznata kao Plimpton 322 (*Slika 1.*), na kojoj je sustavno naveden velik broj uređenih parova (a, c) za koje postoji cijeli broj b koji zadovoljava:

$$a^2 + b^2 = c^2. \tag{1}$$



Slika 1: Plimpton 322

Prijevod ove ploče, zajedno sa njenom interpretacijom i povijesnom pozadinom, su prvi objavili Neugebauer i Sachs 1945. godine. Uređene trojke (a, b, c) koje zadovoljavaju (1) su npr, $(3, 4, 5), (5, 12, 13), (8, 15, 17)$ poznate kao Pitagorine trojke. Pretpostavlja se da su Pitagorejci bili zainteresirani za Pitagorine trojke zbog njihove interpretacije pravokutnog trokuta.

U svakom slučaju, problem pronalaženja Pitagorinih trojki su smatrali zanimljivim i u drugim drevnim civilizacijama koje su znale za Pitagorin teorem. Najpotpunije shvaćanje problema u drevnim vremenima je postignuto u grčkoj matematici između Euklida i Diofanta. Sada znamo da je formula za generiranje Pitagorinih trojki:

$$a = (p^2 - q^2)r, \quad b = 2qpr, \quad c = (p^2 + q^2)r,$$

gdje su

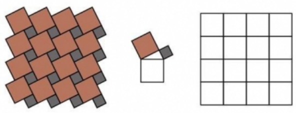
$$p, q, r \in \mathbb{N}, p > q.$$

Lako se vidi da je $a^2 + b^2 = c^2$ kad su a, b i c dani po ovim formulama. Iako Babilonci nisu imali naš algebarski zapis, formula:

$$a = p^2 - q^2, \quad b = 2qp, \quad c = p^2 + q^2$$

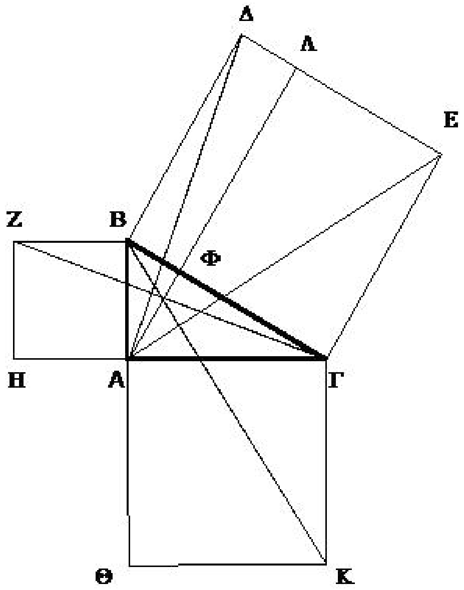
koja daje rješenja za a, b i c, bez zajedničkog djelitelja, je bila osnovna za ispis trojki. Manje općenite formule se pripisuju Platonu i samom Pitagori. Rješenje koje odgovara općoj formuli je dano u Euklidovim knjigama. Koliko je poznato, to je prvi iskaz i dokaz općeg rješenja.

Poznato je da je Pitagorin teorem dokazan prvi put pomoću podnih pločica (*Slika 2.*). Jednostavnost dokaza je pokazao Heath, 1925. godine. Svaki veliki kvadrat sadrži četiri kopije danog pravokutnog trokuta. Oduzimanjem ovih četiri trokuta od velikih kvadratnih listova, s jedna strane imamo sumu kvadrata duljina kateta, a s druge strane imamo kvadrat duljine hipotenuze trokuta. Ovaj dokaz, kao i stotine drugih koji daju Pitagorin teorem se oslanja na određene geometrijske pretpostavke. Zapravo je moguće zaobići geometrijske pretpostavke koristeći brojeve kao temelj geometrije, te tada istinitost Pitagorinog teorema slijedi direktno iz definicije, kao neposredna posljedica definicije udaljenosti.



Slika 2: Dokaz Pitagorinog teorema na podnim pločicama

Naime, Grci su smatrali da nije moguće graditi geometriju na osnovi brojeva zbog sukoba između njihovih predodžbi o broju i duljini. Euklidov prvi dokaz Pitagorinog teorema (*Slika 3.*) se također temelji na površinama. On ovisi samo o tome da trokuti s jednakim bazama i jednakom visinom imaju jednaku površinu, iako se radi o vrlo kompliciranom liku.



Slika 3: Euklidov dokaz Pitagorinog teorema

3 Pitagorine trojke

3.1 Parametrizacija pitagorinih trojki

3.1.1 Definicija i osnovna svojstva

Pod imenom Pitagorina trojka mislimo na uređenu trojku (x, y, z), $x, y, z \in \mathbb{Z}$ oblika

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

Kad imamo jedno rješenje, na primjer (3,4,5), možemo generirati i mnoga ostala. Naime, ako je (x, y, z) Pitagorina trojka i a bilo koji cijeli broj, onda je i (ax, ay, az) također Pitagorina trojka:

$$(ax)^2 + (ay)^2 = a^2(x^2 + y^2) = a^2z^2 = (az)^2.$$

Ovo svojstvo je karakteristično svojstvo nultočaka $(x_1, \ldots, x_n)$ homogenih polinoma n-tog stupnja $P(t_1, \ldots, t_n)$. Prisjetimo se što to znači: Monom je izraz oblika $ct_1^{a_1}, \ldots, t_n^{a_n}$, i stupanj monoma je definiran kao suma eksponenata $a_1 + \ldots + a_n$. Za polinom kažemo da je homogen stupnja d ako svaki od njegovih monoma ima stupanj d. Na primjer, polinom $P(x, y, z) = x^2+y^2-z^2$ je homogen stupnja 2, dok Fermatov polinom

$$P_N(x, y, z) = x^N + y^N - z^N,$$

je homogen stupnja N. Povrh toga, za svaki (nekonstantni) homogeni polinom $P(t_1, \ldots, t_n)$ vrijedi da je $P(0, \ldots, 0) = 0$ pa je $(0, \ldots, 0)$ nultočka svakog homogenog polinoma koja se naziva trivijalna nultočka.

Vratimo se Pitagorinim trojkama, ova razmatranja pokazuju da za svaki $a \in \mathbb{Z}$, $(3a, 4a, 5a)$ je Pitagorina trojka. Za Pitagorinu trojku kažemo da je primitivna ako je $(a, b, c) = 1$, odnosno ako su a, b i c relativno prosti. Svaka netrivijalna uređena trojka (a, b, c) je pozitivan višekratnik jedinstvene primitivne trojke, tj. $(\frac{a}{d}, \frac{b}{d}, \frac{c}{d})$ gdje je $d = (a, b, c)$. Naš cilj je pronaći sve primitivne Pitagorine trojke. Postoje mnogi načini, ali u radu smo odlučili opisati sljedeći način, zbog jednostavnosti i zato što motivira proučavanje ne samo cjelobrojnih, već i racionalnih rješenja polinomijalne jednadžbe.

Promotrimo krivulju $x^2 + y^2 = 1$ u $\mathbb{R}^2$. Pretpostavimo da je (a, b, c) primitivna Pitagorina trojka, te vrijedi $a^2 + b^2 = c^2$, gdje je $c \neq 0$. Cijelu jednadžbu možemo podijeliti s c, te dobivamo

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

Tada su $(\frac{a}{c}, \frac{b}{c})$ racionalne točke jedinične kružnice. Nadalje, postupak može biti obrnut: pretpostavimo da su $(r, s) \in \mathbb{Q}^2$ takvi da je $r^2 + s^2 = 1$. Zatim je $r = \frac{a}{c}$ i $s = \frac{b}{d}$ uz uvijet da je $cd \neq 0$, iz čega slijedi:

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

pa je (da, bc, bd) netrivijalna Pitagorina trojka. Ako iz primitivne Pitagorine trojke (a, b, c) želimo doći do racionalnih rješenja $(\frac{a}{c}, \frac{b}{c})$ te zatim skratiti nazivnike koristeći gornju formulu, dobivamo (ca, cb, c^2). Ovo nije primitivna trojka s kojom smo započeli, ali je jednostavno izmijenjena.

3.1.2 Racionalna parametrizacija jedinične kružnice

Fiksirajmo bilo koju racionalnu točku $P_\bullet = (x_\bullet, y_\bullet)$ jedinične kružnice. Sad uzmimo bilo koju drugu racionalnu točku $P = (x_P, y_P)$ jedinične kružnice. Tada postoji jedinsteni pravac p koji prolazi točkama $P_\bullet$ i P, te su njegovi koeficijenti racionalni brojevi:

$$p : y - y_P = \frac{y_P - y_\bullet}{x_P - x_\bullet}(x - x_P)$$

Konkretno, koeficijent smjera pravca:

$$m_P = \frac{y_P - y_\bullet}{x_P - x_\bullet}$$

je racionalan broj. Ovo ograničava broj racionalnih rješenja, jer većina pravaca koji prolaze kroz fiksnu točku P imaju iracionalan koeficijent smjera. Zanimljiviji je obrat: za bilo koji $m \in \mathbb{Q}$, definiramo pravac p_m jednadžbom:

$$p_m : y = (y - y_\bullet) = m(x - x_\bullet) = m(x + 1)$$

kao pravac koji prolazi točkom $P_\bullet = (-1, 0)$ i ima koeficijent smjera jednak m. Također, tvrdimo i da je skup racionalnih točaka jedinične kružnice upravo jednak uniji skupa koji sadrži točku $P_\bullet = (-1, 0)$ i skupa točaka P_m gdje m prolazi skupom racionalnih brojeva.

Pridružimo li linearnu jednadžbu p_m kvadratnoj jednadžbi $x^2 + y^2 = 1$, dobivamo kvadratnu jednadžbu sa racionalnim koeficijentima. Obzirom da znamo da ova jednadžba ima barem jedno racionalno rješenje, koordinate točke $P_\bullet$, drugo rješenje također mora biti racionalno što slijedi iz kvadratne jednadžbe. Dobivamo sustav jednadžbi:

$$x^2 + y^2 = 1$$

$$y = m(x + 1).$$

Uvrštavanjem druge jednadžbe u prvu, dobivamo:

$$x^2 + m^2(x + 1)^2 = 1$$

ili

$$(1 + m^2)x^2 + 2m^2 x + m^2 - 1 = 0.$$

Primjenjujući formulu za rješenje kvadratne jednadžbe, imamo:

$$x = \frac{-2m^2 \pm \sqrt{4m^4 - 4(1 + m^2)(m^2 - 1)}}{2(1 + m^2)}.$$

Ispod korijena se nalazi:

$$4m^4 - 4(1+m^2)(m^2-1) = 4(m^4 - (m^4-1)) = 4,$$

pa je time $\sqrt{4m^4 - 4(1+m^2)(m^2-1)} = 2$ i

$$x = \frac{-2m^2 \pm 2}{2(1+m^2)} = \frac{-m^2 \pm 1}{1+m^2}.$$

Primjetimo da, uzimajući predznak minus, dobivamo rješenje $x = \frac{-m^2-1}{1+m^2} = -1$ što je x-koordinata točke $P_\bullet$, a drugo rješenje je:

$$x_m = \frac{1-m^2}{1+m^2}$$

odakle slijedi:

$$y_m = m(1+x_m) = m\left(1 + \frac{1-m^2}{1+m^2}\right) = \frac{2m}{m^2+1},$$

tj,

$$P_m = \left(\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2}\right)$$

što je upravo rješenje koje smo i htjeli. Prije nego se vratimo Pitagorinim trojkama, promotrimo:

$$\lim_{m\to\pm\infty} P_m = \left(\lim_{m\to\pm\infty} \frac{1-m^2}{1+m^2}, \lim_{m\to\pm\infty} \frac{2m}{1+m^2}\right) = (-1,0) = P_\bullet.$$

Geometrijska interpretacija je jednostavna: tangenta na jediničnu kružnicu kroz točku $(-1,0)$ je paralelna sa osi y, pa koeficijent smjera pravca p_m teži ka $+\infty$ ili ka $-\infty$, drugo sjecište P_m teži ka $P_\bullet$ i sekanta teži tagenti, pa racionalne točke jedinične kružnice odgovaraju upravo skupu svih racionalnih pravaca kroz $P_\bullet$.

3.1.3 Skaliranje do primitivnih rješenja

Htjeli bismo eksplicitno zapisati sve primitivne Pitagorine trojke (a, b, c). Kao ranije, to postižemo kraćenjem nazivnika u općem racionalnom rješenju $P_m = (x_m, y_m)$. Naime, ako stavimo da je $m = \frac{u}{v}$ gdje je $(u, v) = 1$, tada je:

$$P_m = \left(\frac{1 - u^2/v^2}{1 + u^2/v^2}, \frac{2u/v}{1 + u^2/v^2}\right) = \left(\frac{v^2 - u^2}{v^2 + u^2}, \frac{2uv}{v^2 + u^2}\right),$$

te množeći s $v^2 + u^2$, dobivamo familiju cjelobrojnih rješenja:

$$(v^2 - u^2, 2uv, v^2 + u^2).$$

Kako bismo znali da smo na ovaj način dobili rješenja primitivne Pitagorine trojke, trebamo provjeriti da li je $(v^2 - u^2, 2uv, v^2 + u^2) = 1$.

Pretpostavimo da neparan prost broj p dijeli $v^2 - u^2$ i $v^2 + u^2$. Tada p također dijeli $(v^2 - u^2) + (v^2 + u^2) = 2v^2$ i $(v^2 - u^2) - (v^2 + u^2) = 2u^2$. Obzirom da je p neparan, slijedi da $p|u^2$ i $p|v^2$ što povlači da $p|u$ i $p|v$, čime dobivamo kontradikciju. Znači da je zajednički djelitelj brojeva $v^2 - u^2, 2uv, v^2 + u^2$ jednak 1 ili 2.

Razlikujemo tri slučaja:

Prvi slučaj: Neka su u i v različitih parnosti. Tada je $v^2 - u^2$ neparan broj, pa je najveći zajednički djelitelj 1. Primjetimo da je u ovom slučaju, prva koordinata $v^2 - u^2$ je neparna i druga $2uv$ parna, te na ovaj način nije moguće konstruirati sve primitive Pitagorine trojke.

Drugi slučaj: Neka su u i v neparni brojevi. Tada su $v^2 - u^2, 2uv, v^2 + u^2$ parni brojevi, pa je najveći zajednički djelitelj jednak 2. U ovom slučaju, $(\frac{v^2-u^2}{2}, uv, \frac{v^2+u^2}{2})$ je primitivno rješenje koje smo tražili.

Treći slučaj: Neka su u i v parni brojevi. To nije moguće, jer je $(u, v) = 1$.

Ako je $x = 2k + 1$ neparan broj, tada je $x^2 = 4k^2 + 4k + 1 \equiv 1 \pmod 4$. Ako su u i v neparni brojevi, ne samo da je $u^2 - v^2$ paran broj, nego vrijedi i $v^2 - u^2 \equiv 1 - 1 = 0 \pmod 4$, pa je $\frac{v^2-u^2}{2}$ paran i uv neparan. Tada su sve primitive trojke u drugom slučaju dobivene zamjenom prve i druge koordinate primitivnih trojki iz prvog slučaja.

Teorem 2 (Klasifikacija Pitagorinih trojki). *a) Racionalna rješenja jednadžbe $x^2 + y^2 = 1$ su $\{(-1, 0) \cup (\frac{1-m^2}{1+m^2}, \frac{2m}{1+m^2}); m \in \mathbb{Q}\}$.*
b) $(0, 0, 0)$ je trivijalna Pitagorina trojka. Svaka netrivijalna Pitagorina trojka je oblika (da, db, dc), gdje je $d \in \mathbb{N}$. Za Pitagorinu trojku (a, b, c) za koju vrijedi da je $(a, b, c) = 1$ kažemo da je primitivna.
c) U svakoj primitivnoj Pitagorinoj trojci (a, b, c), točno jedan od brojeva a

ili b *je paran broj. Svaka primitivna trojka s neparnim* a *je oblika* $(v^2 - u^2, 2uv, v^2 + u^2)$ *gdje su* $u, v \in \mathbb{Z}$ *relativno prosti brojevi različitih parnosti.*

3.2 Veliki Fermatov teorem za N=4

U ovom poglavlju ćemo dokazati Veliki Fermatov teorem za N=4.

Teorem 3 (Fermat)**.** *Jednadžba $x^4 + y^4 = z^2$ nema rješenja za $x, y, z \in \mathbb{Z} \backslash \{0\}$.*

Dokaz.
Teorem ćemo dokazati u tri koraka.

Prvi korak: Neka je (x, y, z) pozitivno cjelobrojno rješenje jednadže $x^4 + y^4 = z^2$. Tvrdimo da postoji pozitivno cjelobrojno rješenje (x', y', z') za koje vrijedi da je $(x', y') = 1$ i $z' \leq z$. Ako x i y nisu relativno prosti, tada su oba djeljiva nekim prostim brojem p. Tada $p^4 | x^4 + y^4 = z^2$, odakle slijedi da $p|z$. Dakle, $\frac{x}{p}, \frac{y}{p}, \frac{z}{p} \in \mathbb{N}$ i

$$\left(\frac{x}{p}\right)^4 + \left(\frac{y}{p}\right)^4 = \frac{1}{p^4}(x^4 + y^4) = \frac{1}{p^4}z^2 = \left(\frac{z}{p^2}\right)^2,$$

pa je $(\frac{x}{p}, \frac{y}{p}, \frac{z}{p^2})$ drugo pozitivno cjelobrojno rješenje, gdje je z-koordinata manja od početne. Postupak se može ponavljati sve dok je z-koordinata strogo manja od prethodne, te se zaustavlja sa rješenjem (x', y', z').

Drugi korak: Neka je zadano pozitivno cjelobrojno rješenje (x, y, z) jednadžbe $x^4 + y^4 = z^2$ uz uvijet da je $(x, y) = 1$. Pronaći ćemo drugo pozitivno rješenje (u, v, w), gdje je $w < z$. Možemo pretpostaviti, bez smanjenja općenitosti da je x neparan, a y paran. Obzirom da su relativno prosti, ne mogu biti oba parna. Trebamo provjeriti jesu li oba x i y neparni. Promatrajući $x^4 + y^4 = z^2$ modulo 4, dobivamo $2 \equiv z^2 \pmod 4$, što je nemoguće jer $0^2 \equiv 2^2 \equiv 0 \pmod 4, 1^2 \equiv 3^2 \equiv 1 \pmod 4$. Sada dolazimo do našeg kompletnog rješenja Pitagorinih trojki: obzirom da je $(x^2)^2 + (y^2)^2 = z^2$ i x i y su relativno prosti, (x, y, z^2) je primitivna Pitagorina trojka sa neparnom prvom koordinatom. Dakle, po Teoremu 2 postoje relativno prosti m i n različitih parnosti takvi da je:

$$x^2 = m^2 - n^2$$

$$y^2 = 2mn$$

$$z = m^2 + n^2.$$

Sada zapišemo prvu jednadžbu u obliku $n^2 + x^2 = m^2$. Obzirom da je $(m, n) = 1$ ovo je ponovo primitivna Pitagorina trojka. Štoviše, dok je x neparan, n mora biti paran broj. Sada našu parametrizaciju možemo zapisati u obliku:

$$x = r^2 - s^2$$

$$n = 2rs$$
$$m = r^2 + s^2$$

za relativno proste r i s različitih parnosti. Sada je:

$$m\left(\frac{n}{2}\right) = \frac{2mn}{4} = \frac{y^2}{4} = \left(\frac{y}{2}\right)^2.$$

Kako su m i $\frac{n}{2}$ relativno prosti, njihov produkt je potpun kvadrat, pa su i oni potpuni kvadrati. Slično,

$$rs = \frac{2rs}{2} = \frac{n}{2} = \square,$$

gdje je $\square$ oznaka za potpun kvadrat, pa r i s moraju biti kvadrati. Stavimo da je $r = u^2, s = v^2, m = w^2$, i zamijenimo ove vrijednosti sa $m = r^2 + s^2$ kako bismo dobili

$$u^4 + v^4 = w^4.$$

Znamo da je $w \geq 1$, pa slijedi:

$$w \leq w^4 < w^4 + n^2 = m^2 + n^2 = z,$$

što daje novo pozitivno cjelobrojno rješenje (u, v, w) uz uvijet da je $w < z$.

Treći korak: Prvi i drugi korak dovode do kontradikcije: ako imamo jedno rješenje (x, y, z) jednadžbe $x^4 + y^4 = z^2$, tada po prvom koraku postoji (x', y', z'), gdje je $z' \leq z$, $(x', y') = 1$. Po drugom koraku imamo drugo pozitivno rješenje (u', v', w'), $w' \leq w < z' \leq z$, gdje je $(u', v') = 1$ i tada po drugom koraku dobivamo još jedno rješenje čija je zadnja koordinata strogo manja od w. Drugim riječima, pretpostavka da postoji beskonačan niz pozitivnih cjelobrojnih rješenja (x_n, y_n, z_n) gdje je $z_{n+1} < z_n$, za sve n nije moguća. $\square$

Lema 1. *Neka su A i B relativno prosti. Tada:*
a) Ako su A i B iste parnosti, tada je $(A + B, A - B) = 2$.
b) Ako su A i B različitih parosti, tada je $(A + B, A - B) = 1$.

Pokazat ćemo još jedan dokaz Velikog Fermatovog teorema koji koristi Lemu 1, koju u ovom radu nećemo dokazati.

Dokaz. Pretpostavimo da jednadžba $x^4 + y^4 = z^2$ ima rješenje (x, y, z), gdje je $z \neq 0$. Među svim rješenjima, odaberimo rješenje sa najmanjim z^2. Za to rješenje mora vrijediti da je $(x, y) = 1$. Zaista, ako prost broj p dijeli

x i y, tada $p^4|z^2$, pa $p^2|z$ i možemo uzeti da je $x = px', y = py', z = p^2z'$ kako bismo dobili rješenje (x', y', z') sa $(z')^2 < z^2$. Štoviše, x i y moraju biti različitih parnosti: ako su relativno prosti, ne mogu oba biti parna, a ako su oba neparna tada promatranjem ostataka koje daju modulo 4 dobivamo kontradikciju. Bez smanjenja općenitosti, pretpostavimo da je x neparan, a y paran broj, pa slijedi da je z neparan. Tvrdimo da je $(z + y^2, z - y^2) = 1$. Neka je $d = (z + y^2, z - y^2)$. Obzirom da je y paran, a x neparan, $z + y^2$ je paran broj, stoga je d neparan. Pretpostavimo da je p neparan prost broj koji dijeli d. Tada $p|(z + y^2) + (z - y^2) = 2z$, odakle slijedi da $p|z$ i $p|(z + y^2) + (z - y^2) = 2y^2$, te $p|x$ što daje kontradikciju sa $(x, y) = 1$. Zbog jedinstvenosti faktorizacije, postoje relativno prosti brojevi r i s za koje vrijedi:

$$z - y^2 = r^4, z + y^2 = s^4.$$

Slijedi da je $(s^2 + r^2)(s^2 - r^2) = s^4 - r^4 = 2y^2$, gdje je y paran, dok su r i s neparni brojevi. Kako su s^2 i r^2 relativno prosti brojevi jednake parnosti, po Lemi 1, slijedi da je $(s^2+r^2, s^2-r^2) = 2$. Kako su r i s neparni, onda je i $\frac{s^2+r^2}{2}$ neparan broj pa je $(\frac{s^2+r^2}{2}, s^2 - r^2) = 1$, te zbog jedinstvenosti faktorizacije postoje relativno prosti brojevi a i b takvi da je

$$r^2 + s^2 = 2b^2, (r + s)(r - s) = r^2 - s^2 = a^2.$$

Po Lemi 1, $(r + s, r - s) = 2$, pa je $(\frac{r+s}{2}, \frac{r-s}{2}) = 1$ i postoje relativno prosti brojevi u i v takvi da je

$$s - r = 2u^2, s + r = 2v^2.$$

Slijedi da je

$$4(u^4 + v^4) = (s - r)^2 + (s + r)^2 = 2(s^2 + r^2) = 4b^2,$$

te je

$$u^4 + v^4 = b^2.$$

Obzirom da je x nepran broj, različit od nule i $x^4 + y^4 = z^2, y^2 \leq y^4 < z^2$, slijedi:

$$2b^2 = s^2 + r^2 \leq (s^2 + r^2)(s^2 - r^2) = 2y^2 < 2z^2.$$

Primjetimo da je i $b \neq 0$, inače bi vrijedilo da je $u = v = 0$ što daje kotradikciju sa činjenicom da su oni relativno prosti. Dakle, pronašli smo rješenje (u, v, b) jednadžbe $x^4 + y^4 = z^2$, gdje je $0 < b^2 < z^2$ što daje kontradikciju s pretpostavkom da je z^2 minimalno rješenje. $\square$

Korolar 1. *Jednadžba $x^4 + y^4 = z^4$, gdje su $x, y, z \in \mathbb{Z}\backslash\{0\}$ nema rješenja.*

Dokaz. Pretpostavimo da postoje $x, y, z \in \mathbb{Z}\backslash\{0\}$ takvi da je $x^4 + y^4 = z^4$. Možemo pretpostaviti da su x, y, z pozitivni brojevi. Tada, kako je $z^4 = (z^2)^2$, uređena trojka (x, y, z^2) je cjelobrojno pozitivno rješenje jednadžbe $x^4 + y^4 = z^2$, što daje kontradikciju sa Teoremom 3.

$\square$

Literatura

[1] F.M. Brueckler: Matematički dvoboji, Školska knjiga, Zagreb, 2011

[2] P.L. Clark: Number Theory: A Contemporary Introduction. Dostupno na: `http://math.uga.edu/~pete/4400FULL.pdf`

[3] J. Stillwell: Mathematics and Its History, Third Edition, Springer, 2010