Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku

Erika Erceg

Pitagorine trojke

Završni rad

Osijek, 2020.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku

Erika Erceg

Pitagorine trojke

Završni rad

Voditelj: doc. dr. sc. Mirela Jukić Bokun

Osijek, 2020.

Sažetak:

U radu se bavimo primitivnim Pitagorinim trojkama, četvorkama i n-torkama. Proučili smo dvije metode za generiranje svih Pitagorinih trojki. Pokazali smo kako se može doći do svih Pitagorinih četvorki i n-torki te kako generirati Pitagorine n-torke iz jednog broja.

Ključne riječi:
Pitagorine trojke, primitivne Pitagorine trojke, relativno prosti brojevi, generiranje, generalizacija, Pitagorine n-torke

Pythagorean triples

Abstract:

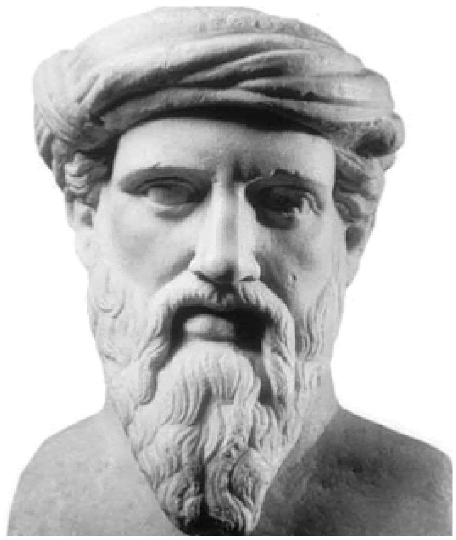
In this paper we deal with primitive Pythagorean triples, quadruples and n-tuples. We studied two methods for generating all Pythagorean triples. We have shown how to get all Pythagorean quadruples and n-tuples and also how to generate Pythagorean n-tuple from a single number.

Key words:
Pythagorean triples, primitive Pythagorean triples, relatively prime numbers, generating, generalization, Pythagorean n-tuples

Sadržaj

Uvod

Pitagora je živio otprilike od 570. do 500. pr. Kr. i osnovao je filozofsko vjersku školu Pitagorejska škola. Pitagorin teorem glasi: Za bilo koji pravokutni trokut je kvadrat duljine hipotenuze c jednak zbroju kvadrata duljina kateta a i b, tj. $c^2 = a^2 + b^2$. Vrijedi i obrat Pitagorinog teorema.



Slika 1: Pitagora[1]

Pitagorina trojka je uređena trojka prirodnih brojeva (a,b,c) koji zadovoljavaju formulu $c^2 = a^2 + b^2$. Pronalaženje Pitagorine trojke ekvivalentno je pronalaženju pravokutnog trokuta čije duljine stranica su prirodni brojevi. Ukoliko su a, b i c relativno prosti, onda je (a,b,c) primitivna Pitagorina trojka. Za bilo koju trojku (a,b,c), ako je x njihov najveći zajednički djelitelj, onda je $(a/x,b/x,c/x)$ primitivna trojka. Stoga da bi pronašli sve Pitagorine trojke dovoljno je pronaći sve primitivne Pitagorine trojke.
O primitivnim Pitagorinim trojkama, generiranju Pitagorinih trojki, kao i o Pitagorinim n-torkama i njihovom generiranju bit će više riječi u poglavljima koja slijede.

[1] Izvor:[2]

1. Osnovne formule za generiranje Pitagorinih trojki

U ovom ćemo poglavlju opisati klasični način kako možemo generirati Pitagorine trojke ([1]). Prvo ćemo dokazati pomoćnu lemu koja nam govori kada je Pitagorina trojka primitivna.

Lema 1.1. *Za Pitagorinu trojku (a,b,c) sljedeće tvrdnje su ekvivalentne:*

1. *a, b i c nemaju zajedničkih djelitelja, tj. trojka je primitivna.*
2. *a, b i c su u parovima relativno prosti.*
3. *neka dva od a, b i c su relativno prosta.*

Dokaz. Da 1. povlači 2. ćemo pokazati kontrapozicijom. Pretpostavimo da a, b i c nisu u parovima relativno prosti. Tada postoji neki prirodan broj p takav da npr. p dijeli a i b. Pošto je $c^2 = a^2 + b^2$, onda p dijeli i c. Znači da a, b i c imaju zajedničkog djelitelja p, što je kontradikcija. Isto bi dobili i da smo uzeli da p dijeli b i c ili a i c.
Očito je da 2. povlači 3., jer ako su a, b i c u parovima relativno prosti, onda su i neka dva od a, b i c relativno prosti.
Pokažimo kontrapozicijom da 3. povlači 1. Pretpostavimo da a, b i c imaju zajednički djelitelj veći od 1. Tada taj broj dijeli i a i b i c pa ni jedan od njih nije sa nekim drugim relativno prost. □

Sada ćemo iskazati i dokazati jako bitan teorem za generiranje Pitagorinih trojki.

Teorem 1.1. *Ako je (a,b,c) primitivna Pitagorina trojka, tada je jedan broj od a i b paran, dok je drugi neparan broj. Ako je b paran, onda je*

$$a = u^2 - v^2, \qquad b = 2uv, \qquad c = u^2 + v^2, \tag{1}$$

za prirodne brojeve u i v koji zadovoljavaju $u > v$, $(u, v) = 1$ i $u \not\equiv v \pmod 2$.
Obrnuto, za takve brojeve u i v, formulama (1) definirane su primitivne Pitagorine trojke.

Dokaz. Pokažimo prvo da su formulama (1) definirane primitivne Pitagorine trojke.

$$a^2 + b^2 = (u^2 - v^2)^2 + (2uv)^2 = u^4 - 2u^2v^2 + v^4 + 4u^2v^2 = (u^2 + v^2)^2 = c^2.$$

Vidimo da je $(u^2 - v^2, 2uv, u^2 + v^2)$ Pitagorina trojka za $u > v > 0$. Provjerimo je li primitivna za $(u, v) = 1$ i $u \not\equiv v \pmod 2$. Ako je prirodan broj x zajednički djelitelj od $u^2 - v^2$ i $u^2 + v^2$ koji su neparni, onda je x također neparan i dijeli njihovu sumu i razliku. Znači x dijeli $2u^2$ i $2v^2$, a pošto je x neparan, onda dijeli u^2 i v^2. Kako je $(u, v) = 1$, zaključujemo da je $x = 1$.
Sada ćemo na dva načina dokazati prvi smjer ovog teorema.

Algebarski dokaz:

Pretpostavimo da su i a i b neparni. Tada je $a^2 \equiv b^2 \equiv 1 \pmod 4$, pa je $c^2 = a^2 + b^2 \equiv 2 \pmod 4$. Niti jedan broj kvadriran nije kongruentan 2 modulo 4 pa je to kontradikcija, znači ili a ili b mora biti paran. Kada bi oba broja bila parna, onda bi i c bio paran broj pa trojka (a,b,c) ne bi bila primitivna. Stoga je jedan od brojeva a i b paran, a drugi neparan i c je neparan.
Uzmimo da je b paran te zapišimo $c^2 = a^2 + b^2$ na sljedeći način

$$b^2 = c^2 - a^2 = (c - a)(c + a). \tag{2}$$

Pošto su i a i c neparni, onda je $c - a$ i $c + a$ parno. Podijelimo li (2) s 4 imamo

$$\left(\frac{b}{2}\right)^2 = \frac{c-a}{2}\frac{c+a}{2}. \tag{3}$$

Zato što su a i c relativno prosti, onda su i $\frac{c-a}{2}$ i $\frac{c+a}{2}$ relativno prosti, jer ako je x njihov najveći zajednički djelitelj, onda on dijeli i $\frac{c+a}{2} - \frac{c-a}{2} = a$ i $\frac{c+a}{2} + \frac{c-a}{2} = c$ pa je $x = 1$. Znamo da je $c > a > 0$ pa su oba faktora jednakosti (3) pozitivni brojevi koji su relativno prosti. Pošto njihov umnožak daje kvadrat, onda je i svaki od njih kvadrat nekog broja pa za neke prirodne brojeve u i v imamo

$$\frac{c+a}{2} = u^2, \ \ \frac{c-a}{2} = v^2. \tag{4}$$

Uočimo da su u i v relativno prosti. Sada kada zbrojimo i oduzmemo formule iz (4) dobijemo

$$a = u^2 - v^2, \ \ c = u^2 + v^2.$$

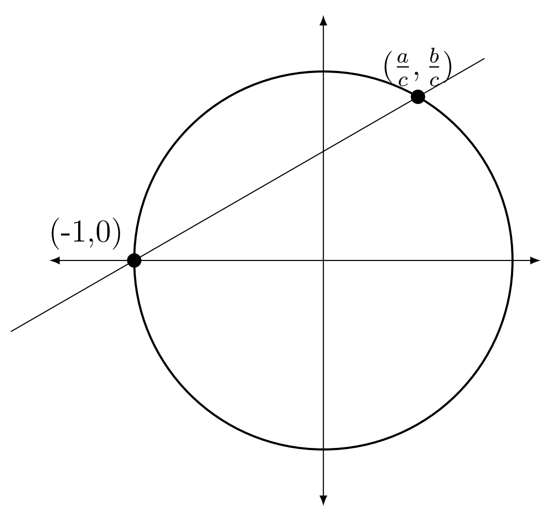
Odavde (uzimajući u obzir da su b, u i v prirodni brojevi) zaključujemo sljedeće

$$\left(\frac{b}{2}\right)^2 = u^2v^2 \implies b^2 = 4u^2v^2 \implies b = 2uv.$$

Još je ostalo provjeriti $u \not\equiv v \pmod 2$. Znamo da su u i v relativno prosti što znači da nisu oba parni. Kada bi oba bili neparni, onda bi $u^2 - v^2$, $2uv$ i $u^2 + v^2$ svi bili parni pa trojka ne bi bila primitivna što je kontradikcija.

Geometrijski dokaz:

Pitagorine trojke su povezane s točkama jedinične kružnice. Uočimo da se $c^2 = a^2 + b^2$ može zapisati kao $1 = \left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2$ što nas podsjeća na jediničnu kružnicu $1 = x^2 + y^2$. Iz toga vidimo da je točka $(\frac{a}{c}, \frac{b}{c})$ racionalna točka na jediničnoj kružnici.



Slika 2: Kružnica određena jednadžbom $x^2 + y^2 = 1$.

Iz algebarskog dokaza znamo da za primitivnu Pitagorinu trojku (a,b,c) možemo uzeti da je a neparan, a b paran broj. Sada ćemo povući pravac kroz $(-1, 0)$ i $(\frac{a}{c}, \frac{b}{c})$ kao na Slici

2.
Koeficijent smjera ovog pravca jednak je

$$k = \frac{\frac{b}{c} - 0}{\frac{a}{c} - (-1)} = \frac{b}{a+c}$$

pa znamo i jednadžbu pravca

$$y = \frac{b}{a+c}(x - (-1)) = k(x+1).$$

Sada možemo jednadžbu pravca uvrstiti u jednadžbu kružnice i dobijemo

$$\begin{aligned} 1 &= x^2 + (k(x-1))^2, \\ 1 &= x^2 + k^2x^2 - 2k^2x + k^2, \\ 1 &= (1+k^2)x^2 - 2k^2x + k^2, \\ 0 &= (1+k^2)x^2 - 2k^2x + k^2 - 1. \end{aligned} \tag{5}$$

Iz jednadžbe (5) možemo izračunati nultočke, ali mi već znamo da su to x-koordinate u kojima se pravac i kružnica sijeku, tj. $x_1 = -1$ i $x_2 = \frac{a}{c}$. Računanjem nultočki ćemo dobiti x_1 i x_2 zapisane preko k

$$\begin{aligned} x_{1,2} &= \frac{-2k^2 \pm \sqrt{4k^2 - 4(1+k^2)(k^2-1)}}{2(1+k^2)}, \\ x_{1,2} &= \frac{-k^2 \pm \sqrt{k^4 - k^4 + 1}}{1+k^2} = \frac{-k^2 \pm 1}{1+k^2}, \\ x_1 &= -1, \qquad x_2 = \frac{a}{c} = \frac{-k^2+1}{1+k^2}. \end{aligned} \tag{6}$$

Sjetimo se da je i točka $(\frac{a}{c}, \frac{b}{c})$ na pravcu $y = k(x+1)$ pa imamo

$$\frac{b}{c} = k\left(\frac{a}{c} + 1\right) = k\left(\frac{-k^2+1}{1+k^2} + 1\right) = k\left(\frac{-k^2+1+1+k^2}{1+k^2}\right) = \frac{2k}{1+k^2}. \tag{7}$$

Pošto je k koeficijent smjera pravca koji siječe jediničnu kružnicu u prvom kvadrantu, onda je $1 > k > 0$. Tada $k = \frac{b}{a+c}$ možemo zapisati ovako $k = \frac{v}{u}$ za relativno proste prirodne brojeve u i v. Uvrstimo sada takav k u (6) i (7), uzimajući u obzir da je $u > v$, zbog $k < 1$, dobivamo

$$\frac{a}{c} = \frac{1 - \left(\frac{v}{u}\right)^2}{1 + \left(\frac{v}{u}\right)^2} = \frac{u^2 - v^2}{u^2 + v^2}, \tag{8}$$

$$\frac{b}{c} = \frac{2\left(\frac{v}{u}\right)^2}{1 + \left(\frac{v}{u}\right)^2} = \frac{2uv}{u^2 + v^2}. \tag{9}$$

Moramo provjeriti uvjet $u \not\equiv v \pmod 2$. Brojevi u i v nisu oba parna jer ne bi bili relativno prosti. Ako su oba broja neparna, onda su i $2uv$ i $u^2 + v^2$ parni pa možemo formulu (9) ovako zapisati

$$\frac{b}{c} = \frac{2uv}{u^2 + v^2} = \frac{uv}{\frac{u^2+v^2}{2}}.$$

Pošto je uv neparan broj, a b je paran došli smo do kontradikcije.
Znamo da $u^2 - v^2$, $2uv$, $u^2 + v^2$ čine Pitagorinu trojku. Također znamo i da su $u^2 + v^2$ i

$u^2 - v^2$ relativno prosti pa zbog Leme 1.1 znamo da čine primitivnu Pitagorinu trojku. Sada kada znamo da su ta tri broja relativno prosta i da su a, b i c relativno prosti, iz formula (8) i (9) možemo zaključiti da je

$$a = u^2 - v^2, \qquad b = 2uv, \qquad c = u^2 + v^2$$

i s time smo završili ovaj dokaz. $\square$

Zanimljiva posljedica dobivene geometrijske formule za primitivnu Pitagorinu trojku (a,b,c) je da možemo znati koji će od u i v biti paran, a koji neparan. Imamo

$$k = \frac{b}{a+c} = \frac{v}{u}$$

i znamo da je ili u ili v paran. Kada je $a + c$ djeljiv sa većom potencijom broja 2 nego što je b, onda je u paran, a v je paran kada je b djeljiv sa većom potencijom broja 2 nego što je $a + c$.
Navest ćemo sada nekoliko primjera.

Primjer 1.1. *Pogledajmo kako za različite u i v dobivamo različite Pitagorine trojke. Uzimajući u obzir da je $u > v$ i da je jedan od njih paran a drugi neparan dobivamo sljedeću tablicu.*

u	v	a	b	c
2	1	3	4	5
3	2	5	12	13
5	2	21	20	29
5	4	9	40	41
6	1	35	12	37

Primjer 1.2. *Pogledajmo Pitagorine trojke (a,b,c) iz Primjera 1.1.*
Pitagorina trojka (3,4,5): vidimo da $a+c = 8 = 2^3$ ima veću potenciju broja 2 nego $b = 4 = 2^2$ pa bi zaključili da je u paran, što je istina jer je $u = 2$.
Pitagorina trojka (5,12,13): $a+c = 18 = 2 \cdot 9$ ima manju potenciju broja 2 nego $b = 12 = 3 \cdot 2^2$ pa zaključujemo da je v paran, vidimo iz tablice da je $v = 2$.
Pitagorina trojka (9,40,41): $a+c = 50 = 5^2 \cdot 2$ ima manju potenciju broja 2 nego $b = 40 = 5 \cdot 2^3$ pa je v paran, vidimo iz tablice da je $v = 4$.

Primjer 1.3. *Pitagorine trojke iz Primjera 1.1 su sve primitivne, ali iz njih možemo dobiti i one koje nisu primitivne. Primitivna Pitagorina trojka je (5,12,13), a Pitagorine trojke koje nisu primitivne i koje dobijemo iz (5,12,13) su (10,24,26), (15,36,39), (50,120,130), (500,1200,1300), itd.*

Napomena 1.1. *Iz Teorema 1.1 smo vidjeli kako dobiti primitivne Pitagorine trojke, a sve Pitagorine trojke možemo dobiti pomoću ove formule*

$$[d(u^2 - v^2)]^2 + (2duv)^2 = [d(u^2 + v^2)]^2, d \in \mathbb{N}. \tag{10}$$

Primjer 1.4. *Odredite sve Pitagorine trojke u kojima jedna kateta ima duljinu 15.*
Vidimo iz formule (10) da d može biti neki od brojeva 1, 3 ,5 ,15.

- *Ako je* $d = 1$ *onda je trojka primitivna i jedna kateta joj je jednaka 15. Tada je* $u^2 - v^2 = 15$ *pa imamo primitivnu Pitagorinu trojku* $(15, 8, 17)$.

- *Ako je* $d = 3$ *onda možemo podijeliti Pitagorinu trojku s 3 i dobijemo primitivnu Pitgorinu trojku čija je jedna kateta jednaka 5. Tada je* $u^2 - v^2 = 5$ *pa je primitivna Pitagorina trojka* $(5, 12, 13)$.

- *Ako je* $d = 5$ *onda možemo podijeliti Pitagorinu trojku s 5 i dobijemo primitivnu Pitgorinu trojku čija je jedna kateta jednaka 3. Tada je* $u^2 - v^2 = 3$ *pa je primitivna Pitagorina trojka* $(3, 4, 5)$.

- *Ako je* $d = 15$ *onda možemo podijeliti Pitagorinu trojku s 15 i dobijemo primitivnu Pitgorinu trojku čija je jedna kateta jednaka 1. Pošto su u i v različite parnosti ovaj slučaj nije moguć.*

2. Direktna metoda za generiranje Pitagorinih trojki i generalizacija metode na Pitagorine n-torke

U prvom poglavlju smo uveli formule (1) koje generiraju primitivne Pitagorine trojke (a,b,c) te formulu (10) pomoću koje možemo dobiti sve Pitagorine trojke. Postoji više načina za generiranje svih Pitagorinih trojki, ovdje ćemo govoriti o metodi koja je opisana u [8]. Ova metoda koristi činjenicu da razlika između duljine hipotenuze c i duljine jednog od krakova a (ili b) pravokutnog trokuta može imati samo određenu vrijednost ovisnu o duljini drugog kraka. Ono što je također dobro kod ove metode je što kada faktoriziramo u možemo prognozirati koliko će biti primitivnih, a koliko Pitagorinih trojki koje nisu primitivne i prije nego što ih sve izračunamo. Motivacija za generiranje Pitagorinih trojki je njihova primjena u svakodnevnom životu, kao npr. u kriptografiji i zaštiti podataka ([3]).

Zapišimo sada $c - b = d$, tj. $c = d + b$. Tada iz opće formule $a^2 + b^2 = c^2$ dobijemo ovo

$$\begin{aligned} a^2 + b^2 &= (d+b)^2, \\ a^2 + b^2 &= b^2 + 2bd + d^2, \\ a^2 &= d(2b+d), \\ b &= \frac{a^2 - d^2}{2d}. \end{aligned} \tag{11}$$

Broj d mora zadovoljavati sljedeća dva uvjeta: d mora biti djelitelj od a^2 i pošto je b prirodan broj mora biti $a^2 - d^2 > 0$, tj.

$$a > d.$$

U Potpoglavlju 2.1. ćemo pokazati kako možemo pomoću ovog generiranja doći do primitivnih Pitagorinih trojki, a u Potpoglavlju 2.2. ćemo napraviti generiranje za sve Pitagorine trojke. Nakon toga ćemo u Potpoglavlju 2.3. napraviti generalizaciju posebno za Pitagorine četvorke, te nakon toga u Potpoglavlju 2.4. općenito za Pitagorine n-torke.

2.1. Generiranje primitivnih Pitagorinih trojki

Znamo iz Poglavlja 1. da je Pitagorina trojka (a,b,c) primitivna kada su a, b i c relativno prosti te da je c neparan broj, a da su a i b jedan paran, a drugi neparan broj. Sada kada gledamo formulu $c - b = d$ znamo da ako uzmemo da je a paran onda je i d paran, te ako je a neparan, onda imamo neparan broj c minus paran broj b, a to je neparan broj d. Problem ćemo rastaviti na tri slučaja:

1. parni brojevi koji se sastoje samo od potencija broja 2
2. neparni brojevi koji se sastoje od potencija prostih brojeva
3. parni brojevi koji se sastoje i od potencija broja 2 i od potencija prostih brojeva.

Promotrimo u nastavku nabrojane slučajeve.

1. Neka je $a = 2^m$ i $d = 2^n$, gdje su m i n cijeli brojevi.
   Zbog uvjeta na d mora biti $m > n$. Iz formule (11) dobijemo

$$\begin{aligned}(2^m)^2 &= 2^n(2b + 2^n),\\ 2^{2m} &= 2^{n+1}b + 2^{2n},\\ b &= \frac{2^{2m} - 2^{2n}}{2^{n+1}},\end{aligned}$$

   dijeljenjem i brojnika i nazivnika s 2^{2n} dobijemo

$$b = 2^{n-1}(2^{2m-2n} - 1). \tag{12}$$

   Pošto je a oblika 2^m znamo da je a paran iz čega slijedi da je b neparan broj pa je zbog formule (12) $n = 1$. Trojka će izgledati ovako

$$(2^m, 2^{2m-2} - 1, 2^{2m-2} + 1), \tag{13}$$

   jer kada $n = 1$ uvrstimo u formulu (12) imamo $b = 2^{2m-2} - 1$ te kada uvrstimo u $c - b = d$ imamo $c = 2^1 + 2^{2m-2} - 1 = 2^{2m-2} + 1$.

   Primjer 2.1. *Neka je $a = 2^4 = 16$. Znamo da je $d = 2$ i $m = 4$.*
   Sada možemo izračunati iz (13) da je $b = 63$ i $c = 65$ te imamo primitivnu Pitagorinu trojku (16,63,65). Da nismo uzeli $d = 2$, da smo npr. uzeli $d = 4$ imali bi (16,30,34), a to je Pitagorina trojka koja nije primitivna.

2. Neka je $a = p^r k$, p je prost djelitelj od a, k je produkt ostalih prostih faktora, a r je neki prirodan broj.
   Tada je $d = p^t$, gdje je t prirodan broj. Iz formule (11) imamo

$$\begin{aligned}(p^r k)^2 &= p^t(2b + p^t),\\ p^{2r}k^2 &= 2p^t b + p^{2t},\\ b &= \frac{p^{2r}k^2 - p^{2t}}{2p^t}\end{aligned}$$

   i sada podijelimo i brojnik i nazivnik sa p^t i imamo

$$b = \frac{p^{2r-t}k^2 - p^t}{2}. \tag{14}$$

   Pošto je p djelitelj od a, a mi tražimo primitivne trojke, onda p ne smije biti djelitelj od b. Zbog toga t može biti ili 0 ili $2r$. Sada vidimo da su onda primitivne Pitagorine trojke oblika

$$\left(p^r k, \frac{k^2 - p^{2r}}{2}, \frac{k^2 + p^{2r}}{2}\right)$$

   za $d = p^{2r}$, a za $d = 1$ su ovog oblika

$$\left(p^r k, \frac{p^{2r}k^2 - 1}{2}, \frac{p^{2r}k^2 - 1}{2}\right). \tag{15}$$

   Uočimo da se formula (15) može zapisati ovako $\left(a, \frac{a^2-1}{2}, \frac{a^2-1}{2}\right)$, što znači da za svaki neparan broj postoji barem jedna primitivna Pitagorina trojka tog oblika.

Primjer 2.2. *Neka je* $a = 3^2 \cdot 5 = 45$. *Tada* d *može biti samo oblika* $d = 1$ *jer je* $d = 3^4 = 81 > 45 = a$. *Kada je* $d = 1$ *primitivna Pitagorina trojka je oblika* $(45, 1012, 1013)$.

3. Neka je $a = 2^m p^r k$, p je neparan prost djelitelj od a, k je produkt ostalih prostih faktora, a m i r su prirodni brojevi.
Tada je $d = 2^s p^t$, s i t su cijeli brojevi. Iz formule (11) imamo

$$\begin{aligned} (2^m p^r k)^2 &= 2^s p^t (2b + 2^s p^t), \\ 2^{2m} p^{2r} k^2 &= 2^{s+1} p^t b + 2^{2s} p^{2t}, \\ b &= \frac{2^{2m} p^{2r} k^2 - 2^{2s} p^{2t}}{2^{s+1} p^t} \end{aligned}$$

i kada podijelimo i brojnik i nazivnik sa $2^{2s} p^t$ dobijemo

$$b = 2^{s-1}(2^{2m-2s} p^{2r-t} k^2 - p^t). \tag{16}$$

(a) Kada je $m > s$, iz formule (16) vidimo da s mora biti jednak 1 jer je b neparan broj, te p ne može biti djelitelj od b jer onda trojka ne bi bila primitivna. Zaključujemo da je ili $t = 0$ ili $t = 2r$.
Primitivna Pitagorina trojka će izgledati ovako

$$(2^m p^r k, 2^{2m-2} p^{2r} k^2 - 1, 2^{2m-2} p^{2r} k^2 + 1)$$

za $d = 2$, a za $d = 2p^{2r}$ ovako

$$(2^m p^r k, 2^{2m-2} k^2 - p^{2r}, 2^{2m-2} k^2 + p^{2r}).$$

Primjer 2.3. *Neka je* $a = 2^2 \cdot 5^2 \cdot 9 = 900$. *Tada je* $d = 2$, *ne može biti* $d = 5^4 \cdot 2 = 1250$ *jer je* $1250 > 900$. *Za* $d = 2$ *je* $(900, 202499, 202501)$ *primitivna Pitagorina trojka.*

(b) Kada je $m < s$, formulu (16) zapisujemo ovako

$$b = 2^{s-1}\left(\frac{p^{2r-t} k^2}{2^{2s-2m}} - p^t\right) = 2^{2m-s-1}(p^{2r-t} k^2 - 2^{2s-2m} p^t).$$

Zbog toga što b treba biti neparan je $s = 2m - 1$, te p ne smije dijeliti b pa je $t = 0$ ili $t = 2r$.
Primitivna Pitagorina trojka će izgledati ovako

$$(2^m p^r k, p^{2r} k^2 - 2^{2m-2}, p^{2r} k^2 + 2^{2m-2})$$

za $d = 2^{2m-1}$, a za $d = 2^{2m-1} p^{2r}$ ovako

$$(2^m p^r k, k^2 - 2^{2m-2} p^{2r}, k^2 + 2^{2m-2} p^{2r},).$$

Primjer 2.4. *Neka je* $a = 2^2 \cdot 3^2 \cdot 7 = 252$. *Tada je* $d = 2^3 = 8$, *ne može biti* $d = 2^3 \cdot 3^4 = 648$ *jer je* $648 > 252$. *Za* $d = 8$ *je* $(252, 3965, 3973)$ *primitivna Pitagorina trojka.*

(c) Kada je $m = s$, iz formule (16) imamo

$$b = 2^{s-1}(p^{2r-t}k^2 - p^t).$$

Ako je $s \geq 1$, b će uvijek biti paran, tako da je trojka primitivna jedino kad je $m = s = 0$. Kada to uvrstimo u b dobit ćemo formulu (14) koju smo već prokomentirali u 2. slučaju.

Sada možemo te slučajeve sve povezati u jedan: ako je $a = 2^m p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$, onda je $d = 2^s q$ gdje je $q = \prod_{i=1}^{N} q_i^{t_i}$, a $t_i = 0$ ili $t_i = 2r_i$, $i = 1, 2, \ldots, n$. Na ovaj način smo generirali sve primitivne Pitagorine trojke, ali ne smijemo zaboraviti da i dalje d mora zadovoljavati uvjet $a > d$.

Primjer 2.5. *Neka je $a = 2^2 \cdot 3^3 \cdot 11 = 1188$, tada je $p_1 = 3$, a $p_2 = 11$. Pokazat ćemo tablicom sve moguće kombinacije za primitivne Pitagorine trojke u kojima je $a = 1188$.*

d	b	(a,b,c)
$2^1 \cdot 3^0 \cdot 11^0 = 2$	*352835*	*(1188,352835,352837)*
$2^1 \cdot 3^6 \cdot 11^0 = 1458$	-	-
$2^1 \cdot 3^0 \cdot 11^2 = 242$	*2795*	*(1188,2795,3037)*
$2^1 \cdot 3^6 \cdot 11^2 = 176418$	-	-
$2^3 \cdot 3^0 \cdot 11^0 = 8$	*88205*	*(1188,88205,88213)*
$2^3 \cdot 3^0 \cdot 11^2 = 968$	*245*	*(1188,245,1213)*
$2^3 \cdot 3^6 \cdot 11^0 = 5832$	-	-
$2^3 \cdot 3^6 \cdot 11^2 = 705672$	-	-

Ova četiri slučaja za d smo isključili jer ne zadovoljava uvjet $a > d$.

2.2. Generiranje svih Pitagorinih trojki

Da bi generirali Pitagorine trojke koje nisu primitivne jedini uvjet je da je $a > d$. Stoga prvo faktoriziramo broj a i onda d uzmemo da je bilo koja kombinacija tih brojeva osim one koja daje primitivnu trojku. Ako je a paran, onda je i d paran broj, a ako je a neparan, onda je i d neparan broj.

Primjer 2.6. *Neka je $a = 2^2 \cdot 3^2 \cdot 5 = 180$. Prikazat ćemo sada tablicom za $a = 180$ sve moguće Pitagorine trojke koje nisu primitivne.*

d	b	(a,b,c)
$2^1 \cdot 3^1 \cdot 5^1 = 30$	*525*	*(180,525,555)*
$2^1 \cdot 3^0 \cdot 5^1 = 10$	*1615*	*(180,1615,1625)*
$2^1 \cdot 3^2 \cdot 5^0 = 18$	*891*	*(180,891,909)*
$2^1 \cdot 3^2 \cdot 5^1 = 90$	*135*	*(180,135,225)*
$2^2 \cdot 3^0 \cdot 5^0 = 4$	*4048*	*(180,4048,4052)*
$2^2 \cdot 3^1 \cdot 5^0 = 12$	*1344*	*(180,1344,1356)*
$2^2 \cdot 3^0 \cdot 5^1 = 20$	*800*	*(180,800,820)*
$2^2 \cdot 3^1 \cdot 5^1 = 60$	*240*	*(180,240,300)*
$2^2 \cdot 3^2 \cdot 5^0 = 36$	*432*	*(180,432,468)*

Znači kada ne bi isključili d za koje je trojka primitivna imali bi sve moguće Pitagorine trojke.

2.3. Pitagorine četvorke

Pitagorina četvorka je uređena četvorka prirodnih brojeva (a,b,c,d) za koje vrijedi

$$a^2 + b^2 + c^2 = d^2. \tag{17}$$

U ovom dijelu ćemo pokazati kako doći do svih Pitagorinih četvorki ako imamo zadan (a, b). Stavimo da je $a^2 + b^2 = u$ i $d = c + v$. Kada to uvrstimo u formulu (17) dobijemo

$$\begin{aligned} u + c^2 &= (c+v)^2, \\ u + c^2 &= c^2 + 2cv + v^2, \\ c &= \frac{u - v^2}{2v}. \end{aligned} \tag{18}$$

Iz toga možemo vidjeti da, pošto c mora biti cijeli broj, mora vrijediti ako je u paran onda je i v paran broj, a ako je u neparan onda je i v neparan broj. Kada je u paran on mora biti djeljiv s $2v$ te da bi c bio pozitivan mora biti $u > v^2$.
Rastavit ćemo problem na tri slučaja:

1. a je paran broj, a b je neparan (ili obrnuto)
2. i a i b su parni brojevi
3. i a i b su neparni brojevi.

Razmotrimo gornje slučajeve.

1. $u = a^2 + b^2$ je neparan broj, pa je i v neparan.

   (a) Pretpostavimo da a i b imaju zajedničke djelitelje $p_1, p_2, \ldots, p_n$. Tada u možemo zapisati kao $u = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n} q_1^{s_1} q_2^{s_2} \cdots q_N^{s_N}$, a v će biti oblika $v = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n} q_1^{t_1} q_2^{t_2} \cdots q_N^{t_N}$, gdje su m_i, s_i, r_i i t_i cijeli brojevi za sve i. Iz formule (18) imamo

   $$c = \frac{p_1^{m_1-r_1} p_2^{m_2-r_2} \cdots p_n^{m_n-r_n} q_1^{s_1-t_1} q_2^{s_2-t_2} \cdots q_N^{s_N-t_N} - p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n} q_1^{t_1} q_2^{t_2} \cdots q_N^{t_N}}{2}.$$

   Vidimo da je za primitivno rješenje $r_i = 0$ ili $r_i = m_i$, $i = 1, 2, \ldots, n$, a t_j može biti bilo koji cijeli broj između 0 i s_j, uz uvjet da je $u > v^2$.

   Primjer 2.7. *Neka je $a = 10$ i $b = 15$. Tada je $u = 325 = 5^2 \cdot 13$, a $v = 1$ ili $v = 13$. Ne može biti $v = 5^2 = 25$, niti $v = 5^2 \cdot 13$ jer je tada $v^2 > u$. Pa za $v = 1$ imamo $c = 162$ i $d = 163$, a za $v = 13$ imamo $c = 6$ i $d = 19$.*

   (b) Sada pretpostavimo da a i b nemaju zajedničkih djelitelja. Tada je $u = q_1^{s_1} q_2^{s_2} \cdots q_N^{s_N}$, a $v = q_1^{t_1} q_2^{t_2} \cdots q_N^{t_N}$, gdje t_i može biti bilo koji cijeli broj između 0 i s_j uzimajući u obzir da mora vrijediti $u > v^2$. Iz formule (18) imamo

   $$c = \frac{q_1^{s_1-t_1} q_2^{s_2-t_2} \cdots q_N^{s_N-t_N} - q_1^{t_1} q_2^{t_2} \cdots q_N^{t_N}}{2}.$$

   Primjer 2.8. *Neka je $a = 10$ i $b = 11$. Tada je $u = 221 = 13 \cdot 17$, a $v = 1$ ili $v = 13$. Ne može biti $v = 17$, niti $v = 17 \cdot 13$ jer je narušen uvjet $u > v^2$. Pa za $v = 1$ imamo $c = 110$ i $d = 111$, a za $v = 13$ imamo $c = 2$ i $d = 15$.*

Napomena 2.1. *Uočimo da kada god imamo da je jedan od brojeva a i b paran, a drugi neparan, tada ćemo imati barem jednu primitivnu trojku koja ima $v = 1$.*

2. $u = a^2 + b^2$ je paran broj pa će i v biti paran. Sada će u biti ovog oblika $u = 2^m p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n} q_1^{s_1} q_2^{s_2} \cdots q_N^{s_N}$, a v oblika $v = 2^r p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n} q_1^{t_1} q_2^{t_2} \cdots q_N^{t_N}$. Iz formule (18) imamo

$$c = 2^{m-r-1} p_1^{m_1-r_1} p_2^{m_2-r_2} \cdots p_n^{m_n-r_n} q_1^{s_1-t_1} q_2^{s_2-t_2} \cdots q_N^{s_N-t_N} - 2^{r-1} p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n} q_1^{t_1} q_2^{t_2} \cdots q_N^{t_N}.$$

Da bi četvorka bila primitivna mora vrijediti da je $r = 1$ ili $r = m - 1$, uzimajući u obzir uvjet $u > v^2$, te $r_i = 0$ ili $r_i = m_i$, a t_j je bilo koji cijeli broj između 0 i s_j.

Primjer 2.9. *Neka je $a = 6 = 2 \cdot 3$ i $b = 28 = 2^2 \cdot 7$. Tada je $u = 820 = 2^2 \cdot 5 \cdot 41$. Moguće kombinacije dane su u sljedećoj tablici.*

v	c	d	(a,b,c,d)
$2^1 \cdot 5^0 \cdot 41^0 = 2$	*204*	*206*	*(6,28,204,206)*
$2^1 \cdot 5^1 \cdot 41^0 = 10$	*36*	*46*	*(6,28,36,46)*
$2^1 \cdot 5^0 \cdot 41^1 = 82$	-	-	-
$2^1 \cdot 5^1 \cdot 41^1 = 410$	-	-	-

Za dva slučaja nije moguće naći Pitagorinu trojku pošto je $v^2 > u$.

Napomena 2.2. *Primjetimo da ako imamo zadana dva parna broja uvijek možemo naći primitivnu Pitagorinu četvorku koja ima $u = 2$.*

3. Pošto su u ovom slučaju i a i b neparni zapisat ćemo ih ovako $a = 2x+1$, $b = 2y+1$, za x i y prirodne brojeve. Tada je $u = (2x+1)^2 + (2y+1)^2 = 4x^2 + 4x + 1 + 4y^2 + 4y + 1 = 4(x^2 + y^2) + 4(x + y) + 2$. Vidimo da je u paran i zaključujemo da i v mora biti paran. Ranije smo zaključili da kada je v paran, onda je u oblika $2v$, tj. u bi morao biti djeljiv s 4, što je nemoguće pa u ovom slučaju ne dobivamo ni jednu Pitagorinu četvorku.

Sada kada smo pokazali kako doći do primitivnih Pitagorinih četvorki možemo doći i do ne primitivnih. Kada izračunamo i faktoriziramo u, onda v može biti bilo koja kombinacija tih faktora osim onih za koje je četvorka primitivna, uz uvjet $u > v^2$.
Na taj način možemo generirati sve Pitagorine četvorke.

Primjer 2.10. *Neka je $a = 100$ i $b = 105$. Tada je $u = 21025 = 5^2 \cdot 29^2$, a tablicom ćemo pokazati sve moguće kombinacije Pitagorinih četvorki za zadane a i b.*

v	c	d	(a,b,c,d)
$5^0 \cdot 29^0 = 1$	*10512*	*10513*	*(100,105,10512,10513)*
$5^0 \cdot 29^1 = 29$	*36*	*46*	*(6,28,36,46)*
$5^1 \cdot 29^0 = 5$	*348*	*377*	*(100,105,348,377)*
$5^2 \cdot 29^0 = 25$	*408*	*433*	*(100,105,408,433)*

Ostale v smo isključili jer narušavaju uvjet $u > v^2$.

2.4. Pitagorine n-torke

Pitagorina n-torka je uređena n-torka prirodnih brojeva $(a_1, a_2, \ldots, a_n)$ za koju vrijedi

$$a_1^2 + a_2^2 + \cdots + a_{n-1}^2 = a_n^2.$$

Kada imamo zadana $(n-2)$ broja, onda možemo izračunati i ostala dva broja n-torke. Izračunat ćemo ih na sličan način kao što smo to radili s Pitagorinim četvorkama u prošlom poglavlju. Uzmimo da je $u = a_1^2 + a_2^2 + \cdots + a_{n-2}^2$ i $v = a_n - a_{n-1}$.
Među brojevima $a_1, a_2, \ldots, a_{n-2}$ neki će bit parni, a neki neparni. Neka je α broj neparnih brojeva među ta $(n-2)$ broja.

1. Kada je $\alpha = 2$, onda će se kvadrati od ta dva neparna broja zbrojiti i imat ćemo parni broj plus kvadrati ostalih brojeva koji su parni, stoga je u paran broj oblika $u = 2x$, gdje je x neparan broj. Ovdje, kao i u zadnjem slučaju kod Pitagorinih četvorki, ne postoji Pitagorina n-torka koja to zadovoljava.

2. Kada je α neparan broj, onda imamo zbroj kvadrata neparnih brojeva, to je neparan broj plus zbroj kvadrata parnih brojeva, što sve zajedno daje neparan broj u. Tada je u oblika $u = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n} q_1^{s_1} q_2^{s_2} \cdots q_N^{s_N}$, gdje su $p_1, p_2, \ldots, p_n$ zajednički djelitelji brojeva $a_1, a_2, \ldots, a_{n-2}$. Tada je $v = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n} q_1^{t_1} q_2^{t_2} \cdots q_N^{t_N}$, gdje je $r_i = 0$ ili $r_i = m_i$, a t_j može biti bilo koji broj između 0 i s_j za kojega je zadovoljen uvjet $u > v^2$.

   Primjer 2.11. *Neka je $a_1 = 15$, $a_2 = 10$, $a_3 = 5$, $a_4 = 25$, $a_5 = 40$ i $a_6 = 30$. Tada je $u = 3475 = 5^2 \cdot 139$. Prikazat ćemo sada tablicom primitivne osmorke.*

v	a_7	a_8	$(a_1, a_2, a_3, a_4, a_5.a_6, a_7, a_8)$
$5^0 \cdot 139^0 = 1$	*1737*	*1738*	*(15,10,5,25,40,30,1737,1738)*
$5^0 \cdot 139^1 = 139$	-	-	-
$5^2 \cdot 139^0 = 25$	*57*	*82*	*(15,10,5,25,40,30,57,82)*
$5^2 \cdot 139^1 = 3475$	-	-	-

3. Kada je α paran broj različit od 2, ili $\alpha = 0$, tada je i u paran broj oblika $u = 2^m p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n} q_1^{s_1} q_2^{s_2} \cdots q_N^{s_N}$, gdje je m prirodan broj veći od 1, a $p_1, p_2, \ldots, p_n$ su zajednički djelitelji brojeva $a_1, a_2, \ldots, a_{n-2}$. Tada je $v = 2^r p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n} q_1^{t_1} q_2^{t_2} \cdots q_N^{t_N}$, gdje je $r = 1$ ili $r = m - 1$, $r_i = 0$ ili $r_i = m_i$, a t_j može biti bilo koji broj između 0 i s_j koji zadovoljava uvjet $u > v^2$.

   Primjer 2.12. *Neka je $a_1 = 4$, $a_2 = 10$, $a_3 = 16$, $a_4 = 22$, $a_5 = 50$, $a_6 = 20$ i $a_7 = 32$. Tada je $u = 4780 = 5 \cdot 2^2 \cdot 239$. Prikazat ćemo sada tablicom primitivne devetorke.*

v	a_8	a_9	$(a_1, a_2, a_3, a_4, a_5.a_6, a_7, a_8, a_9)$
$2^1 \cdot 5^0 \cdot 239^0 = 2$	*1194*	*1196*	*(4,10,16,22,50,20,32,1194,1196)*
$2^1 \cdot 5^1 \cdot 239^0 = 10$	*234*	*244*	*(4,10,16,22,50,20,32,234,244)*
$2^1 \cdot 5^1 \cdot 239^1 = 2390$	-	-	-

Na ovaj način smo dobili primitivne Pitagorine n-torke, da bi dobili sve n-torke morali bi dopustiti da v može biti kombinacija bilo kojih faktora od u, uz uvjet $u > v^2$.

2.5. Generiranje Pitagorinih n-torki iz jednog broja

U ovom potpoglavlju ćemo pokazati nešto jako zanimljivo, kako preko Pitagorinih trojki iz samo jednog broja možemo doći do Pitagorinih n-torki proizvoljne duljine.
Neka je zadan a_1, tada možemo izračunati trojku (a_1, a_2, b_3) koja zadovoljava $a_1^2 + a_2^2 = b_3^2$. Nakon toga od b_3 možemo opet izračunati trojku (b_3, a_3, b_4) koja zadovoljava $b_3^2 + a_3^2 = b_4^2$, kada to uvrstimo umjesto b_3 imamo $a_1^2 + a_2^2 + a_3^2 = b_4^2$. Tu radnju možemo nastaviti raditi dok ne dodjemo do željene n-torke, pa nakon $(n-2)$ koraka dođemo do

$$a_1^2 + a_2^2 + \cdots + a_{n-1}^2 = a_n^2.$$

Napomena 2.3. *Primjetite da za broj a_1 možemo dobiti više različitih Pitagorinih trojki i za svaku tu trojku možemo dobiti više različitih četvorki, itd. Tako da od jednog broja možemo dobiti puno različitih Pitagorinih n-torki, a te n-torke će biti primitivne ako je svaka trojka preko koje dolazimo do n-torke primitivna.*

Napomena 2.4. *Ovom metodom ne možemo doći do svih Pitagorinih n-torki.*

Primjer 2.13. *Neka je $a = 15$. U nastavku navodimo nekoliko n-torki koje možemo dobiti iz ovog broja:*

$$15^2 + 36^2 + 760^2 + 289560^2 = 289561^2,$$
$$15^2 + 20^2 + 60^2 + 2112^2 + 2232384^2 = 2232385^2,$$
$$15^2 + 8^2 + 144^2 + 348^2 + 71064^2 = 71065^2.$$

3. Metoda za generiranje svih Pitagorinih trojki jednom formulom

U ovom poglavlju ćemo govoriti o još jednoj metodi generiranja Pitagorinih trojki ([5]). Najveći problem kod generiranja je naći sve Pitagorine trojke bez ponavljanja.
Označimo skup svih Pitagorinih trojki sa $\mathcal{P}$, a skup svih primitivnih Pitagorinih trojki sa $\mathcal{R}$, te neka je skup svih Pitagorinih trojki oblika $(a,b,c) = (u^2 - v^2, 2uv, u^2 + v^2)$, pri čemu su $u, v \in \mathbb{N}$ i $u > v$, označen s $\mathcal{E}$. Zbog načina na koji smo definirali $\mathcal{P}$, $\mathcal{R}$ i $\mathcal{E}$ vidimo da vrijedi $\mathcal{P} \supset \mathcal{E} \supset \mathcal{R}$, jer znamo od prije da se u $\mathcal{E}$ nalaze sve primitivne Pitagorine trojke, ali tu se također nalazi i npr. Pitagorina trojka $(27, 36, 45)$ za $u = 6$ i $v = 3$ koja nije primitivna.
Promotrimo sada podskup $\mathcal{C}$ skupa $\mathcal{E}$ koji sadrži sve Pitagorine trojke u kojima je točno jedan od brojeva a i b neparan i c je neparan, a to vrijedi ako i samo ako je točno jedan od brojeva u i v neparan, tj.

$$\begin{aligned}\mathcal{C} &= \{(a,b,c) \in \mathcal{E} : a - b \ i \ c \ su \ neparni\} \\ &= \{(u^2 - v^2, 2uv, u^2 + v^2) : u, v \in \mathbb{N}, \ \ u > v, \ \ u - v \ je \ neparan\}.\end{aligned}$$

Sada vrijedi $\mathcal{P} \supset \mathcal{E} \supset \mathcal{C} \supset \mathcal{R}$.

Lema 3.1. *Za Pitagorinu trojku $(a,b,c) \in \mathcal{C}$ vrijedi*

- $\exists\, m \in \mathbb{N}$ *takav da je* $c - b = (2m-1)^2$*;*
- $\exists\, n \in \mathbb{N}$ *takav da je* $c - a = 2n^2$*.*

Obrnuto, za neke $m, n \in \mathbb{N}$ $\exists\, (a,b,c) \in \mathcal{C}$ takva da je $c - b = (2m-1)^2$ i $c - a = 2n^2$.

Dokaz. Pokažimo prvo da za $(a,b,c) \in \mathcal{C}$ vrijedi $c - b = (2m-1)^2$. Iz definicije skupa $\mathcal{C}$ znamo da postoje $u, v \in \mathbb{N}$, $u > v$ takvi da je $a = u^2 - v^2$, $b = 2uv$ i $c = u^2 + v^2$ te da je $u - v$ neparan broj. Stoga $c - b$ možemo zapisati ovako, za neki $m \in \mathbb{N}$,

$$c - b = u^2 + v^2 - 2uv = (u - v)^2 = (2m-1)^2.$$

Sada pokažimo da za $(a,b,c) \in \mathcal{C}$ vrijedi i $c - a = 2n^2$. Vidimo da je

$$c - a = u^2 + v^2 - (u^2 - v^2) = 2v^2,$$

a trebamo pokazati da postoji $n \in \mathbb{N}$ takav da je $c - a = 2n^2$. Iz toga slijedi da je $n = v$.
Da bi dokazali obrat treba pokazati da sustav jednadžbi

$$\begin{aligned}u^2 + v^2 - 2uv - 2uv &= (2m-1)^2, \\ u^2 + v^2 - (u^2 - v^2) &= 2n^2,\end{aligned}$$

ima rješenje takvo da su $u, v \in \mathbb{N}$, $u > v$ i $u - v$ je neparan broj. Kada taj sustav riješimo imamo da je $v = n$ i $u = n + 2m - 1$ što zadovoljava sve uvjete pa je to rješenje. $\square$

Direktna posljedica ove leme je da je $c - b$ uvijek neparan broj iz skupa $\{1, 9, 25, 49, \ldots\}$, te da je $c - a$ uvijek paran broj iz skupa $\{2, 8, 18, 32, \ldots\}$. Ta informacija nam omogućuje uvođenje iduće definicije.

Definicija 3.1. *Za $m, n \in \mathbb{N}$, niz neparnih Pitagorinih trojki iz $\mathcal{C}$ definiramo kao*

$$N(m) := \{(a,b,c) \in \mathcal{C} : c - b = (2m-1)^2\}$$

te niz parnih Pitagorinih trojki iz $\mathcal{C}$ definiramo kao

$$P(n) := \{(a,b,c) \in \mathcal{C} : c - a = 2n^2\}.$$

Primjer 3.1. $(3,4,5), (5,12,13), (7,24,25) \in N(1)$ *i* $(3,4,5), (15,8,17), (35,12,37) \in P(1)$.

Teorem 3.1. *Iduće tvrdnje su istinite:*

1. $\mathcal{C} = \bigcup_{m \in \mathbb{N}} N(m) = \bigcup_{n \in \mathbb{N}} P(n)$.

2. *Za $m_1, m_2 \in \mathbb{N}$, $m_1 \neq m_2$ vrijedi $N(m_1) \cap N(m_2) = \emptyset$. Također za $n_1, n_2 \in \mathbb{N}$, $n_1 \neq n_2$ vrijedi $P(n_1) \cap P(n_2) = \emptyset$.*

3. *Za $(a,b,c) \in \mathcal{C}$, $\exists\, m, n \in \mathbb{N}$ takvi da je $(a,b,c) \in N(m) \cap P(n)$. Obrnuto, za $m, n \in \mathbb{N}$ presjek $N(m) \cap P(n) \in \mathcal{C}$ sadrži jedinstvenu Pitagorinu trojku.*

4. *Neka su $m, n \in \mathbb{N}$. Tada trojku $(a,b,c) \in \mathcal{C}$ za koju vrijedi $c - b = (2m-1)^2$ i $c - a = 2n^2$ možemo zapisati na jedinstven način u sljedećem obliku:*

$$a = -2n + 4nm + 4m^2 - 4m + 1, \tag{19}$$
$$b = 2n^2 - 2n + 4nm, \tag{20}$$
$$c = 2n^2 - 2n + 4nm + 4m^2 - 4m + 1. \tag{21}$$

Dokaz. Tvrdnje $1. - 3.$ su direktne posljedice Leme 3.1 stoga njih nećemo dokazivati. Ostalo je onda dokazati tvrdnju 4. Također iz Leme 3.1 znamo da je

$$a = (n + 2m - 1)^2 - n^2, \tag{22}$$
$$b = 2(n + 2m - 1)n, \tag{23}$$
$$c = (n + 2m - 1)^2 + n^2, \tag{24}$$

što raspisivanjem dovodi do formula (19)-(21). Vidimo da je trojka $(a,b,c) \in \mathcal{C}$ zapisana na jedinstven način kao funkcija od $m, n \in \mathbb{N}$. Tada iz (19) imamo

$$n = \frac{a - (2m-1)^2}{2(2m-1)}$$

te kada to uvrstimo u (20) dobijemo

$$(2m-1)^4 + 2b(2m-1) - a^2 = 0.$$

Rješavanjem te bikvadratne jednadžbe dobijemo samo jedno pozitivno rješenje

$$m = \frac{1 + \sqrt{c-b}}{2}.$$

Kada to uvrstimo u n dobijemo

$$n = \frac{a + b - c}{2\sqrt{c-b}}.$$

Ovo nam pokazuje da za danu trojku $(a,b,c) \in \mathcal{C}$ imamo jedinstvene $m, n \in \mathbb{N}$ koji zadovoljavaju formule (19)-(21). □

Napomena 3.1. *Primjetimo da formule (19)-(21) možemo zapisati na ovaj način*

$$\begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 2n^2 \\ 2n(2m-1) \\ (2m-1)^2 \end{bmatrix}.$$

Zamislimo sada pravokutan trokut ΔABC s pravim kutom u vrhu C. Neka je $a = |\overline{BC}|$, $b = |\overline{AC}|$ i $c = |\overline{AB}|$. Pretpostavimo da je $d = c - b$ neparan broj, a $e = c - a$ paran. Tada definiramo $f = a - d$ i imamo

$$\begin{aligned} a &= f + d, \\ b &= e + f, \\ c &= e + d + f, \end{aligned}$$

što je ekvivalentno ovome

$$\begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} e \\ f \\ d \end{bmatrix}. \tag{25}$$

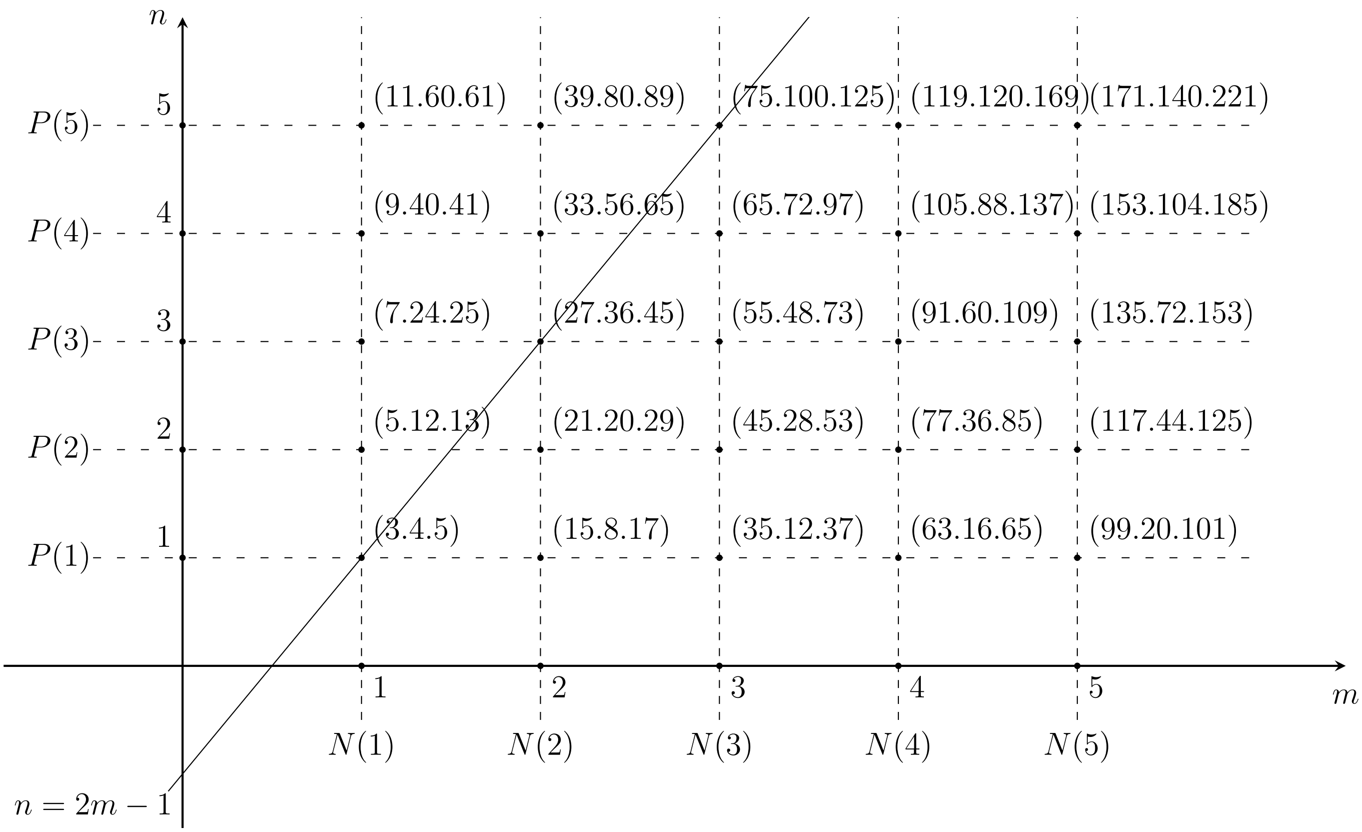
Pošto je $\begin{vmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{vmatrix} = -1$ *matrica je regularna i iz toga slijedi da je $e = 2n^2$ i $d = (2m-1)^2$.*

Napomena 3.2. *Sve Pitagorine trojke koje dobijemo na taj način, za $m, n \in \mathbb{N}$, su takve da je c neparan. No ako dopustimo da m može biti $\frac{1}{2}, \frac{3}{2}, \frac{5}{2}, \ldots$, tada će a, b i c i dalje biti prirodni brojevi koji čine Pitagorinu trojku, ali će i a i b i c biti parni brojevi. To znači da $\mathcal{C}$ sadrži sve Pitagorine trojke iz $\mathcal{E}$ osim onih za koje su a, b i c svi parni brojevi. Označimo sada $\mathbb{N}_{\frac{1}{2}} := \mathbb{N} \cup \{p + \frac{1}{2} : p \in \mathbb{N} \cup \{0\}\}$ i $\mathcal{C}' := \bigcup\limits_{m \in \mathbb{N}_{\frac{1}{2}}} N(m)$. Ako stavimo $s = 2m$ i to uvrstimo u formule (22)-(24) dobijemo*

$$a = (n+s-1)^2 - n^2, \qquad b = 2(n+s-1)n, \qquad c = (n+s-1)^2 + n^2.$$

Za $u = n + s - 1$ i $v = n$ slijedi da je $(a, b, c) \in \mathcal{E}$, stoga je $\mathcal{C}' = \mathcal{E}$.

Svaka Pitagorina trojka $(a, b, c) \in \mathcal{C}$ se može zapisati kao funkcija p od m i n, pa možemo pisati $(a, b, c) = p(m, n)$. Trojke čine rešetku u koordinatnom sustavu (m, n) što se vidi na Slici 3.



Slika 3: Rešetka Pitagorinih trojki u $\mathcal{C}$.

Iz Slike 3 također vidimo da $\mathcal{C}$ sadrži i Pitagorine trojke koje nisu primitivne. Sve trojke koje leže na pravcu $n = 2m - 1$ možemo dobiti kao $k^2(3, 4, 5)$, gdje je k neparan prirodan broj.

Teorem 3.2. *Neka su $(a, b, c) \in \mathcal{C}$ i $m, n \in \mathbb{N}$ takvi da je $(a, b, c) = p(m, n)$. Tada je (a, b, c) primitivna Pitagorina trojka ako i samo ako su n i $2m - 1$ relativno prosti brojevi.*

Dokaz. Neka je $\mu = 2m - 1$. Uvrštavanjem u formule (22)-(24) dobijemo

$$a = \mu(2n + \mu), \tag{26}$$

$$b = 2n(n + \mu), \tag{27}$$

$$c = 2n^2 + \mu(2n + \mu). \tag{28}$$

Prvo pokažimo da ako n i μ imaju zajednički faktor trojka nije primitivna. Neka je $n = kn_1$ i $\mu = k\mu_1$, gdje su $k, n_1, \mu_1 \in \mathbb{N}$. Kada to uvrstimo u (26)-(28) imamo

$$a = k^2\mu_1(2n_1 + \mu_1),$$
$$b = 2k^2 n_1(n_1 + \mu_1),$$
$$c = k^2(2n_1^2 + 2n_1\mu_1 + \mu_1^2),$$

iz čega vidimo da a, b i c imaju zajednički djelitelj k pa trojka nije primitivna. Iz toga vidimo da ako trojka $(a, b, c) \in \mathcal{C}$ nije primitivna, n i μ nisu relativno prosti brojevi.
Ako trojka (a, b, c) nije primitivna možemo ju zapisati u obliku $k(\alpha, \beta, \gamma)$, gdje je $k \in \mathbb{N}$ i (α, β, γ) je primitivna trojka. Stoga postoje $n_1, \mu_1 \in \mathbb{N}$ takvi da je $(\alpha, \beta, \gamma) = p(n_1, \mu_1)$ te

ako to uvrstimo u (22)-(24) imamo

$$\mu(2n+\mu) = k\mu_1(2n_1+\mu_1), \tag{29}$$

$$2n(n+\mu) = 2kn_1(n_1+\mu_1), \tag{30}$$

$$2n^2+\mu(2n+\mu) = k(2n_1^2+2n_1\mu_1+\mu_1^2). \tag{31}$$

Kada formulu (29) uvrstimo u formulu (31) dobijemo $k=\frac{n^2}{n_1^2}$, te kada to uvrstimo u formulu (30) dobijemo

$$l=\frac{n}{n_1}=\frac{\mu}{\mu_1}.$$

Uočimo da je $l \in \mathbb{N}$ i da je $l^2 = k$, iz toga slijedi da je l zajednički djelitelj od n i μ pa oni nisu relativno prosti. □

Napomena 3.3. *Posebni slučajevi parametrizacije iz Teorema 3.1 su:*

1. *Pitagorina familija neparnih trojki* $(2n+1, 2n^2+2n, 2n^2+2n+1)$, *koju možemo zapisati i ovako* $p(1,n) = N(1) = \{(3,4,5),(5,12,13),(7,24,25),\ldots\}$. *Kada u fomulu (25) uvrstimo m=1 imamo*

$$p(1,n) = \left\{(a,b,c)\in\mathbb{N}^3 : \begin{bmatrix}a\\b\\c\end{bmatrix} = \begin{bmatrix}0&1&1\\1&1&0\\1&1&1\end{bmatrix}\begin{bmatrix}2n^2\\2n\\1\end{bmatrix} \; za \;\; n\in\mathbb{N}\right\}.$$

2. *Platonova familija parnih trojki* $(4m^2-1, 4m, 4m^2+1)$, *koju možemo zapisati i ovako* $p(m,1) = P(1) = \{(3,4,5),(15,8,17),(35,12,37),\ldots\}$. *Kada u fomulu (25) uvrstimo n=1 imamo*

$$p(m,1) = \left\{(a,b,c)\in\mathbb{N}^3 : \begin{bmatrix}a\\b\\c\end{bmatrix} = \begin{bmatrix}0&1&1\\1&1&0\\1&1&1\end{bmatrix}\begin{bmatrix}2\\2(2m-1)\\(2m-1)^2\end{bmatrix} \; za \;\; m\in\mathbb{N}\right\}.$$

Jedina trojka koja je i u Pitagorinoj familiji trojki, i u Platonovoj familiji trojki je $(3,4,5)$, iz čega slijedi da je $p(1,1) = (3,4,5)$.
Kombiniranjem Pitagorine i Platonove familije trojki dobije se formula koja generira sve Pitagorine trojke a dana je s

$$p(m,n) = \left\{(a,b,c)\in\mathbb{N}^3 : \begin{bmatrix}a\\b\\c\end{bmatrix} = \begin{bmatrix}0&1&1\\1&1&0\\1&1&1\end{bmatrix}\begin{bmatrix}2n^2\\2n(2m-1)\\(2m-1)^2\end{bmatrix} \; za \;\; m,n\in\mathbb{N}\right\}$$

i iz nje dobijemo ove jednakosti

$$\begin{aligned}
&e = 2n^2, \qquad d = (2m-1)^2, \qquad f = 2n(2m-1),\\
&a = d+f = 4mn-2n+4m^2-4m+1,\\
&b = e+f = 2n^2+4mn-2n,\\
&c = d+e+f = 2n^2+4mn-2n+4m^2-4m+1.
\end{aligned}$$

Ova parametrizacija je već uspješno iskorištena za brže izračune zlatnog i srebrnog reza ([6],[7]).

Literatura

[1] K. Conrad, *Pythagorean triples*,
http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/pythagtriple.pdf

[2] M. Curić, K. Jurkovic, *Pitagorin poučak*,
URL: https://sites.google.com/site/8bpitagorinpoucak/pitagora?fbclid=IwAR1MjrA2luQVxy

[3] A. Luma, B. Rauf, *Data Encryption and Decryption Using New Pythagorean Triple Algorithm*,
http://www.iaeng.org/publication/WCE2014/WCE2014_pp516-519.pdf

[4] I. Matić, *Uvod u teoriju brojeva*, Odjel za matematiku Sveučilišta J. J. Strossmayera u Osijeku, 2013.

[5] A. Overmars, L. Ntogramatzidis, S. Venkatraman, *A new approach to generate all Pythagorean triples*, AIMS Mathematics, **4**(2019), 242—253,
https://www.aimspress.com/fileOther/PDF/Math/math-04-02-242.pdf

[6] A. Overmars, S. Venkatraman, *A new method of golden ratio computation for faster cryptosystems*, Proceedings of IEEE Cybersecurity and Cyberforensics Conference, London, 21–23 Nov. 2017., DOI: 10.1109/CCC.2017.12.

[7] A. Overmars, S. Venkatraman, S. Parvin, *Revisiting square roots with a fast estimator*, London J. Res. Comput. Sci. Technol., 18 (2018), Compilation 10.

[8] T. Roy, F. J. Sonia, *A Direct Method to Generate Pythagorean Triples and its Generalization to Pythagorean Quadruples and n-tuples*,
https://arxiv.org/ftp/arxiv/papers/1201/1201.2145.pdf