Kongruentni brojevi

Rajkovača, Monika

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku

Monika Rajkovača

Kongruentni brojevi

Završni rad

Osijek, 2019.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku

Monika Rajkovača

Kongruentni brojevi

Završni rad

Voditelj: doc. dr. sc. Mirela Jukić Bokun

Osijek, 2019.

Sažetak:

U ovom radu bavit ćemo se problemom kongruentnih brojeva te ćemo primijeniti Pitagorine trojke u dokazivanju tvrdnje da 1 nije kongruentan broj. Pokazat ćemo povezanost ovog problema s aritmetičkom progresijom tri kvadrata i eliptičkim krivuljama. Osim toga, navest ćemo Tunnellov teorem i još neke testove kongruentnosti. Na kraju ćemo dati neka poopćenja ovog problema.

Ključne riječi:

kongruentni broj, Pitagorine trojke, Fermatov teorem, aritmetička progresija, eliptička krivulja, Tunnellov teorem, t-kongruentni broj, θ-kongruentni broj

Congruent numbers

Abstract:

In this bachelor's thesis we are going to deal with congruent number problem and we are going to use Pythagorean triples in proving that 1 is not congruent number. We are going to show connection between this problem and arithmetic progression of three squares and elliptic curves. Furthermore, we are going to mention Tunnell's theorem and some other congruency tests. In the end, we are going to generalize this problem.

Key words:

congruent number, Pythagorean triples, Fermat's theorem, arithmetic progression, elliptic curve, Tunnell's theorem, t-congruent number, θ-congruent number

Sadržaj

Uvod

Pojam pravokutnog trokuta poznat nam je otprije, a sada uvodimo pojam racionalnog pravokutnog trokuta. Kažemo da je pravokutni trokut racionalan kada su mu duljine svih triju stranica racionalni brojevi. Svaki takav trokut ima racionalnu površinu, međutim postoje racionalni brojevi koji ne mogu biti površina nekog racionalnog pravokutnog trokuta. Na primjer, niti jedan pravokutan trokut nema površinu 1 kao što ćemo pokazati u Teoremu 2.3. To nas potiče na razmišljanje koji se racionalni brojevi mogu pojaviti kao površina racionalnog pravokutnog trokuta. Kao što ćemo vidjeti, to nas dovodi do pojma kongruentnog broja, odnosno problema kongruentnih brojeva. Taj problem je jedan od najstarijih neriješenih velikih problema u matematici.
U ovom radu će se obraditi važni pojmovi vezani uz ovaj problem i njegovo rješavanje. U prvom poglavlju definirat ćemo kongruentne brojeve i navesti primjere. U drugom poglavlju ćemo opisati Pitagorine trojke i dokazati Fermatov teorem. Aritmetička progresija tri kvadrata kao i kratka povijest bit će navedeni u trećem poglavlju. Kroz četvrto poglavlje navest ćemo poveznicu između kongruentnih brojeva i kubične krivulje $y^2 = x^3 - n^2x$. U petom poglavlju iskazat ćemo Tunnellov teorem i još neke testove kongruentnosti danog broja. U zadnjem poglavlju nalaze se neka poopćenja kongruentnih brojeva.

1. Definicija kongruentnih brojeva

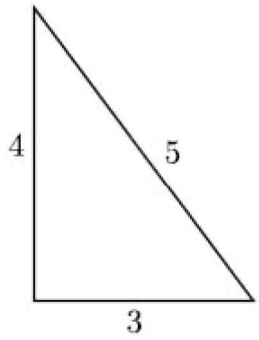
Definicija 1.1. *Za pozitivan racionalan broj n kažemo da je kongruentan ako postoji racionalan pravokutan trokut površine n, to jest postoje racionalni brojevi a, b, $c > 0$ takvi da vrijedi $a^2 + b^2 = c^2$ i $\frac{1}{2}ab = n$.*

Definicija 1.2. *Za prirodan broj n kažemo da je kvadratno slobodan ako je 1 najveći potpuni kvadrat koji ga dijeli, tj. ukoliko iz $m^2|n$, $m \in \mathbb{N}$, slijedi $m = 1$.*

Primjer 1.1. *Brojevi 6 i 15 su kvadratno slobodni.*

Pretpostavimo da je r kongruentan i da su $a, b, c \in \mathbb{Q}$ stranice pravokutnog trokuta površine r. Za svaki $r \in \mathbb{Q}$, $r > 0$, može se naći $s \in \mathbb{Q}$ takav da je $s^2 r$ kvadratno slobodan prirodan broj. Trokut sa stranicama sa, sb, sc ima površinu $s^2 r$. Stoga je dovoljno ispitivati jesu li kvadratno slobodni prirodni brojevi kongruentni.

Primjer 1.2. *6 je najmanja površina pravokutnog trokuta cjelobrojnih stranica.*

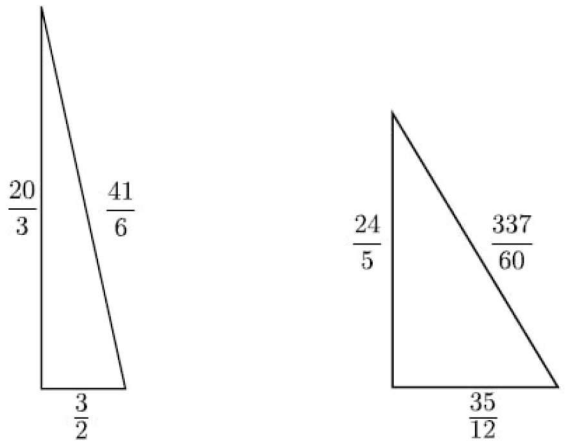


Slika 1: Racionalni pravokutni trokut površine 6

Primjer 1.3. *Brojevi 5 i 7 su kongruentni (Slika 2).*

Primjer 1.4. *Budući da je broj 5 kongruentan, i broj $20 = 4 \cdot 5$ je kongruentan. Stranice trokuta su udvostručene, a površina trokuta je učetverostručena.*

Primjer 1.5. *Brojevi 1, 2, 3, 4, 8, 9 i 10 nisu kongruentni.*



Slika 2: Racionalni pravokutni trokuti s površinama 5 i 7, redom

n	*duljine stranica*
5	3/2, 20/3, 41/6
6	3, 4, 5
7	24/5, 35/12, 337/60
13	780/323, 323/30, 106921/9690
14	8/3, 63/6, 65/6
15	15/2, 4, 17/2
20	3, 40/3, 41/3
21	7/2, 12, 25/2
22	33/35, 140/3, 4901/105
23	80155/20748, 41496/3485, 905141617/72306780

Slika 3: Prvih 10 kongruentnih brojeva s pripadnim duljinama stranica pravokutnih trokuta

2. Pitagorine trojke i Fermatov teorem

U ovom ćemo poglavlju definirati Pitagorine trojke, izvesti formule kojima se generiraju te ih primijeniti na dokazivanje tvrdnje da broj 1 nije kongruentan koju je dokazao Fermat 1640. godine.

Definicija 2.1. *Uređenu trojku prirodnih brojeva (a, b, c) zovemo Pitagorina trojka ako su a, b katete, a c hipotenuza nekog pravokutnog trokuta, to jest ako vrijedi $a^2 + b^2 = c^2$. Ako su a, b, c relativno prosti, onda kažemo da je (a, b, c) primitivna Pitagorina trojka. Takav trokut zovemo (primitivni) Pitagorin trokut.*

Uočimo da je u svakoj primitivnoj Pitagorinoj trojki točno jedan od brojeva a, b neparan. Ako bi a i b bili parni, onda trojka ne bi bila primitivna, a ako bi a i b bili neparni, onda bi iz $a^2 + b^2 \equiv 2 \pmod 4$ i $z^2 \equiv 0 \pmod 4$ dobili kontradikciju.

Teorem 2.1. *Sve primitivne pitagorine trojke (a, b, c) u kojima je b paran, dane su formulama:*

$$a = k^2 - l^2, \;\; b = 2kl, \;\; c = k^2 + l^2, \tag{1}$$

gdje je $k > l$ i k, l su relativno prosti prirodni brojevi različite parnosti.

Dokaz. Jednadžbu $a^2 + b^2 = c^2$ možemo pisati u obliku $b^2 = (c + a)(c - a)$. Neka je $b = 2r$. Brojevi $c+a$ i $c-a$ su parni pa postoje prirodni brojevi s i t takvi da je $c+a = 2s, \;\; c-a = 2t$. Sada je

$$r^2 = st.$$

Iz $c = s + t, \;\; a = s - t$, zaključujemo da je $(s, t) = 1$ pa postoje $k, l \in \mathbb{N}, \;\; (k, l) = 1$ takvi da je $s = k^2, \;\; t = l^2$. Iz toga slijedi:

$$a = k^2 - l^2, \;\; c = k^2 + l^2, \;\; b = 2kl.$$

Brojevi k i l moraju biti različite parnosti jer je broj $a = k^2 - l^2$ neparan.
Lako se provjeri da brojevi definirani sa (1) zadovoljavaju $a^2 + b^2 = c^2$.
Zaista,

$$(k^2 - l^2)^2 + (2kl)^2 = k^4 + 2k^2l^2 + l^4 = (k^2 + l^2)^2.$$

Još treba provjeriti da su relativno prosti. Pretpostavimo da je $(a, c) = d > 1$. Tada je d neparan, $d|(k^2 + l^2) + (k^2 - l^2) = 2k^2$ i $d|(k^2 + l^2) - (k^2 - l^2) = 2l^2$, a to je u kontradikciji s pretpostavkom da su k i l, pa stoga i k^2 i l^2, relativno prosti.

□

Napomena 2.1. *Iz Teorema 2.1 slijedi da su sve Pitagorine trojke dane identitetom:*

$$[d(k^2 - l^2)]^2 + (2dkl)^2 = [d(k^2 + l^2)]^2, \;\; d \in \mathbb{N}.$$

U nastavku ćemo pokazati da ne postoji Pitagorin trokut kojemu je površina potpun kvadrat. U tu svrhu najprije ćemo dokazati sljedeće dvije tvrdnje.

Teorem 2.2. *Jednadžba $a^4+b^4 = c^2$ nema rješenja u prirodnim brojevima. Drugim riječima, ne postoji pravokutni trokut kojemu su duljine kateta kvadrati prirodnih brojeva.*

Dokaz. Pretpostavimo da takav trokut postoji i izaberimo među svim takvim trokutima onaj s najmanjom hipotenuzom. Tako dobivamo Pitagorinu trojku (a^2, b^2, c). Pokažimo da su a i b relativno prosti. U protivnom bi vrijedilo $a = xd, b = yd, d > 1$. Tada bi iz $c^2 = d^4(x^4+y^4)$ slijedilo da postoji $z \in \mathbb{N}$ takav da je $c = d^2 z$ te bi dobili Pitagorinu trojku (x^2, y^2, z) s hipotenuzom manjom od c što je kontradikcija.
Dakle, (a^2, b^2, c) je primitivna Pitagorina trojka pa po Teoremu 2.1 (ako odaberemo da je b paran) postoje relativno prosti prirodni brojevi različite parnosti k i l tako da vrijedi:

$$a^2 = k^2 - l^2, \;\; b^2 = 2kl, \;\; c = k^2 + l^2.$$

Iz $a^2 + l^2 = k^2$ slijedi da je k paran, a l neparan. Stavimo: $l = 2s, b = 2t$, pa dobivamo

$$t^2 = ks.$$

Slijedi da postoje prirodni brojevi p i r takvi da je $k = p^2$ i $s = r^2$. Budući da je (a, l, k) primitivna Pitagorina trojka, po Teoremu 2.1 postoje u, v takvi da je $(u, v) = 1, \;\; l = 2uv$, $k = u^2 + v^2$. Sada iz $l = 2r^2$ slijedi da je $r^2 = uv$ pa postoje $x, y \in \mathbb{N}$ takvi da je $u = x^2, v = y^2$. Prema tome, $x^4 + y^4 = p^2$ pa je (x^2, y^2, p) Pitagorina trojka za čiju hipotenuzu vrijedi: $p < p^2 = k < k^2 + l^2 = c$, što je u kontradikciji s minimalnošću od c.
□

Propozicija 2.1. *Ne postoji Pitagorin trokut u kojem su hipotenuza i jedna kateta kvadrati prirodnih brojeva.*

Dokaz. Pretpostavimo suprotno i neka je (a, b, c) Pitagorina trojka s najmanjom hipotenuzom koja ima zadano svojstvo. Očito je da je trojka (a, b, c) primitvna.
Neka je $a = x^2, \;\; c = z^2$.
Ako je b paran, onda postoje $k, l \in \mathbb{N}$ takvi da je

$$x^2 = a = k^2 - l^2, \;\; b = 2kl, \;\; z^2 = c = k^2 + l^2.$$

Odavde je $(xz)^2 = k^4 - l^4$, pa je u Pitagorinoj trojki (l^2, xz, k^2) hipotenuza $k^2 < c$, te smo došli do kontradikcije.
Prema tome, b mora biti neparan, što znači da je x paran. Iz $b^2 = z^4 - x^4 = (z^2 - x^2)(z^2 + x^2)$ slijedi da postoje prirodni brojevi r, s takvi da je

$$z^2 - x^2 = r^2, \;\; z^2 + x^2 = s^2.$$

Slijedi da je $2z^2 = r^2 + s^2$, odnosno

$$z^2 = \left(\frac{s+r}{2}\right)^2 + \left(\frac{s-r}{2}\right)^2.$$

Dakle, postoje $k, l \in \mathbb{N}$ takvi da je

$$\frac{s \pm r}{2} = k^2 - l^2, \;\; \frac{s \mp r}{2} = 2kl, \;\; z = k^2 + l^2,$$

pa je $2x^2 = s^2 - r^2 = 8kl(k-l)(k+l)$. Budući da su k i l relativno prosti brojevi različite parnosti, brojevi $k, k-l, k+l$ su u parovima relativno prosti. Stoga postoje $m, n, p, q \in \mathbb{N}$ takvi da vrijedi:

$$k = m^2, \;\; l = n^2, \;\; k - l = p^2, \;\; k + l = q^2.$$

Odavde je $m^4 - n^4 = (pq)^2$, pa smo dobili Pitagorinu trojku (n^2, pq, m^2) s hipotenuzom $m^2 = k < k^2 + l^2 = z < z^2 = c$, što je kontradikcija.

□

Napomenimo da se metoda korištena u dokazima prethodne dvije tvrdnje naziva Fermatova metoda beskonačnog spusta.

Korolar 2.1. *Ne postoji Pitagorin trokut čija je površina potpun kvadrat.*

Dokaz. Pretpostavimo da takav trokut (a, b, c) postoji. Tada je

$$a^2 + b^2 = c^2 \quad \text{i} \quad ab = 2P.$$

Po pretpostavci, postoji $u \in \mathbb{N}$ takav da je $P = u^2$, odnosno $2ab = (2u)^2$.
Sada je:

$$c^2 + (2u)^2 = (a+b)^2, \;\; c^2 - (2u)^2 = (a-b)^2.$$

Iz toga slijedi:

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

Dakle, dobili smo Pitagorin trokut čija je hipotenuza c^2, a jedna kateta $(2u)^2$, što je u kontradikciji s Propozicijom 2.1.

□

Teorem 2.3. *(Fermat) Broj 1 nije kongruentan.*

Dokaz. Pretpostavimo da postoji pravokutan trokut s racionalnim stranicama čija je površina jednaka 1. Neka su stranice toga trokuta: $\frac{a}{d}$, $\frac{b}{d}$, $\frac{c}{d}$, pri čemu su a, b, c, d pozitivni cijeli brojevi. Imamo: $a^2 + b^2 = c^2$ i $\frac{1}{2}ab = d^2$. Drugim riječima, ako postoji racionalan pravokutan trokut površine 1, onda postoji Pitagorin trokut čija je površina potpun kvadrat. To je u kontradikciji s Korolarom 2.1 i činjenicom da je broj 1 potpun kvadrat. Dakle, zaključujemo da broj 1 nije kongruentan.

□

Postoji jednostavan algoritam, koji koristeći danu parametrizaciju za primitivne Pitagorine trojke u Teoremu 2.1, generira sve kongruentne brojeve gradeći tablicu kao u Primjeru 2.1. Svaki broj u stupcu 4 i svaki broj u stupcu 5 te tablice je kongruentan broj. Problem je u tome što se za dani n ne može reći koliko dugo se mora čekati da se utvrdi njegova kongruentnost. Stoga taj algoritam nije dobar.

Primjer 2.1. *Tablica na Slici 4 prikazuje listu primitivnih trojki za* $k + l \leq 9$.

Primjer 2.2. *Broj* 53 *je kongruentan broj, ali se pojavljuje tek za* $k = 1873180325$ *i* $l = 115831356$.

Primjer 2.3. *Trokut* $(175, 288, 337)$ *površine* $25200 = 7 \cdot 60^2$ *pojavljuje se za* $k = 16$ *i* $l = 9$.

k	ℓ	(a,b,c)	$(1/2)ab$	kvadratno slobodan dio
2	1	$(3,4,5)$	6	6
4	1	$(15,8,17)$	60	15
3	2	$(5,12,13)$	30	30
6	1	$(35,12,37)$	210	210
5	2	$(21,20,29)$	210	210
4	3	$(7,24,25)$	84	21
8	1	$(63,16,65)$	504	126
7	2	$(45,28,53)$	630	70
5	4	$(9,40,41)$	180	5

Slika 4: Kongruentni brojevi

Primjer 2.4. *Broj* 157 *pokazuje nam kompleksnost problema određivanja je li broj kongruentan ili ne. Naime, najjednostavniji trokut koji ima površinu* 157 *dan je s*

$$\left(\frac{6803298487826435051217540}{411340519227716149383203},\right.$$
$$\frac{411340519227716149383203}{21666555693714761309610},$$
$$\left.\frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}\right).$$

3. Aritmetička progresija tri kvadrata

Neka su a, b, c stranice pravokutnog trokuta površine n. To znači da vrijede dvije jednakosti: $a^2 + b^2 = c^2$ i $\frac{1}{2}ab = n$. Uvjet da je n kongruentan znači da te dvije jednadžbe imaju zajednička rješenja $a, b, c \in \mathbb{Q}$.

Propozicija 3.1. *Neka je n fiksan kvadratno slobodan prirodan broj. Neka su a, b, c, x pozitivni racionalni brojevi takvi da je $a < b < c$. Tada postoji bijekcija između stranica a, b, c pravokutnog trokuta površine n i broja x za koji je svaki od brojeva $x, x + n, x - n$ kvadrat racionalnog broja. Veza je:*

$$a, b, c \rightarrowtail x = \left(\frac{c}{2}\right)^2,$$

$$x \rightarrowtail a = \sqrt{x+n} - \sqrt{x-n}, \quad b = \sqrt{x+n} + \sqrt{x-n}, \quad c = 2\sqrt{x}. \tag{2}$$

Specijalno, n je kongruentan ako i samo ako postoji x takav da su $x, x + n, x - n$ kvadrati racionalnih brojeva.

Dokaz. Prvo pretpostavimo da je a, b, c trojka sa željenim svojstvom: $a^2 + b^2 = c^2$ i $\frac{1}{2}ab = n$. Ako dodamo ili oduzmemo od prve jednadžbe četverostruku drugu, dobijemo:

$$(a \pm b)^2 = c^2 \pm 4n.$$

Podijelimo obje strane sa 4, pa vidimo da broj $x = \left(\frac{c}{2}\right)^2$ ima svojstvo da su brojevi $x \pm n$ kvadrati od $\frac{a \pm b}{2}$.
Obratno, ako je dan x s traženim svojstvom, lako se vidi da tri racionalna broja dana formulama (2) zadovoljavaju: $ab = 2n$ i $a^2 + b^2 = 4x = c^2$.
Da bi dokazali bijektivnost, potrebno je samo dokazati da n i x ne mogu dati dvije različite trojke. Fiksirajmo n i x (pa je fiksan i c). Trojku koja odgovara x-u dobijemo iz presjeka $a^2 + b^2 = c^2$ i $\frac{1}{2}ab = n$ u ab-ravnini. Dobijemo četiri točke presjeka, ali za danu točku presjeka (a, b), preostale tri su $(-a, -b), (b, a), (-b, -a)$ pa stoga dobivamo točno jednu trojku.

□

Kongruentne brojeve prvi su sistematski proučavali arapski matematičari desetog stoljeća. Bavili su se pitanjem je li za dani n moguće pronaći racionalan broj x takav da su i $x^2 + n$ i $x^2 - n$ kvadrati racionalnih brojeva. U prethodnoj propiziciji pokazali smo da je to moguće. Podrijetlo izraza "kongruentan broj" povezano je upravo s tim i dolazi iz Fibonaccijeve knjige *Liber Quadratorum* iz 1225. On je cijeli broj n nazivao *congruum* ako postoji takav broj x da vrijedi gore navedeno. To bi značilo da je trojka $x^2 - n, x^2, x^2 + n$ aritmetička progresija tri kvadrata. Svaki *congruum* je kongruentan broj.

4. Krivulja $y^2 = x^3 - n^2x$

Ispitivanje kongruentnosti broja n povezano je s rješivošću para jednadžbi: $a^2 + b^2 = c^2$ i $\frac{1}{2}ab = n$ za pozitivne racionalne brojeve a, b, c. Ispostavlja se da je svojstvo kongruentnosti ekvivalentno (netrivijalnoj) rješivosti jednadžbe $y^2 = x^3 - n^2x$ kao što ćemo pokazati u Teoremu 4.1. Ova jednadžba ima tri očita racionalna rješenja: $(0, 0)$, $(n, 0)$ i $(-n, 0)$. To su rješenja u kojima je $y = 0$.
Prvi koji je ovo iskoristio u netrivijalnom smislu bio je Heegner koji je razvio teoriju koja je danas poznata kao teorija Heegnerovih točaka. On je 1952. godine dokazao da ako je $p \equiv 5 \pmod 8$ ili $p \equiv 7 \pmod 8$ prost, tada je p kongruentan broj.

Teorem 4.1. *Za $n > 0$ postoji bijekcija između sljedeća dva skupa:*

$$\begin{aligned} \{(a, b, c) &: a^2 + b^2 = c^2, \quad \frac{1}{2}ab = n\}, \\ \{(x, y) &: y^2 = x^3 - n^2x, \quad y \neq 0\}. \end{aligned}$$

Međusobno inverzna bijekcija između ovih skupova je:

$$\begin{aligned} (a, b, c) &\mapsto \left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right), \\ (x, y) &\mapsto \left(\frac{x^2 - n^2}{y}, \frac{2nx}{y}, \frac{x^2 + n^2}{y}\right). \end{aligned}$$

Dokaz. Neka je $n \neq 0$ fiksan broj, $a, b, c \in \mathbb{R}$, $a, b, c \neq 0$, stranice pravokutnog trokuta. Pretpostavimo da $a^2 + b^2 = c^2$ i $n = \frac{1}{2}ab$ opisuju dvije plohe u $\mathbb{R}^3$. Želimo definirati presjek ovih dviju površina.
Neka je $c = t + a$. Primjetimo da je $t \neq 0$ jer bi u suprotnom vrijedilo da je $c = a$ što bi impliciralo da je $b^2 = 0$, odnosno $b = 0$ što nije moguće jer je b duljina stranice trokuta. Slijedi,

$$\begin{aligned} a^2 + b^2 &= c^2 = t^2 + 2at + a^2 \\ b^2 &= t^2 + 2at \\ 2at &= b^2 - t^2 \end{aligned}$$

i

$$\begin{aligned} n &= \frac{1}{2}ab \\ a &= \frac{2n}{b}. \end{aligned}$$

Uvrštavanjem u prethodno dobivenu jednakost dobivamo

$$\begin{aligned} 2at &= \frac{4nt}{b} = b^2 - t^2 \\ 4nt &= b^3 - bt^2 \\ \frac{4n}{t^2} &= \frac{b^3}{t^3} - \frac{b}{t} \\ \frac{4n^4}{t^2} &= \frac{n^3b^3}{t^3} - \frac{n^2b}{t} \\ \left(\frac{2n^2}{t}\right)^2 &= \left(\frac{nb}{t}\right)^3 - n^2\left(\frac{nb}{t}\right). \end{aligned}$$

Ako stavimo $x = \frac{nb}{c-a}$ i $y = \frac{2n^2}{c-a}$ pri čemu je $t = c - a$ dobivamo preslikavanje

$$(a, b, c) \rightarrowtail \left(\frac{nb}{c-a}, \frac{2n^2}{c-a} \right) \in \mathbb{R}^2.$$

Definiramo novu krivulju $E_n : y^2 = x^3 - n^2 x$. Svaka točka na toj krivulji može biti prevedena u pravokutan trokut s racionalnim stranicama sljedećim preslikavanjem:

$$(x, y) \rightarrowtail \left(\frac{x^2 - n^2}{y}, \frac{2nx}{y}, \frac{x^2 + n^2}{y} \right).$$

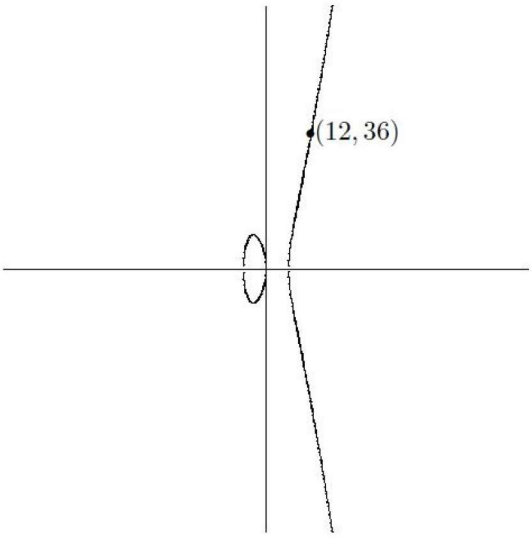
□

Bijekcija u Teoremu 4.1 čuva pozitivnost: ako su a, b, c pozitivni, tada je $(c-a)(c+a) = b^2 > 0$ pa je $c-a$ pozitivan te $x = \frac{nb}{c-a} > 0$ i $y = \frac{2n^2}{c-a} > 0$. S druge strane, ako su x i y pozitivni onda iz $y^2 = x^3 - n^2 x = x(x^2 - n^2)$ vidimo da $x^2 - n^2$ mora biti pozitivan pa su a, b, c pozitivni. Također, za racionalan n, (a, b, c) je racionalna ako i samo ako je (x, y) racionalan.
Svako rješenje od $a^2 + b^2 = c^2$ i $\frac{1}{2}ab = n$ zahtijeva da a i b imaju isti predznak (zbog $ab = 2n > 0$).
Uočimo da se naš problem s kongruentnim brojevima sada može formulirati na sljedeći način: Pozitivan racionalan broj nije kongruentan ako i samo ako jedino rješenje od $y^2 = x^3 - n^2 x$ ima $y = 0$: $(0, 0), (n, 0)$ i $(-n, 0)$.
Ovaj problem svodi se na određivanje netrivijalnih točaka na navedenoj krivulji. Ovakva krivulja naziva se eliptička krivulja. Određivanje racionalnih točaka na eliptičkim krivuljama je netrivijalan problem u koji nećemo ulaziti. Spomenimo samo da se iz jedne netrivijalne racionalne točke na eliptičkoj krivulji (ukoliko takva točka postoji) uvijek može izgenerirati beskonačno mnogo racionalnih točaka na toj istoj krivulji.

Primjer 4.1. *Broj* 1 *nije kongruentan i racionalna rješenja od* $y^2 = x^3 - n^2 x$ *imaju* $y = 0$.

Primjer 4.2. *Budući da je broj* 6 *površina pravokutnog trokuta sa stranicama* 3, 4 *i* 5, *jednadžba* $y^2 = x^3 - 36x$ *ima racionalno rješenje u kojemu je* $y \neq 0$. *Rješenje dano korištenjem Teorema 4.1 je* $(x, y) = (12, 36)$; *vidi Sliku* 5.

Primjer 4.3. *Racionalno rješenje jednadžbe* $y^2 = x^3 - 49x$ *je* $(25, 120)$. *Pomoću Teorema 4.1, iz ovog rješenja dobivamo racionalan pravokutan trokut* $\left(\frac{24}{5}, \frac{35}{12}, \frac{337}{60}\right)$ *površine* 7.



Slika 5: Racionalna točka $(12, 36)$ na krivulji $y^2 = x^3 - 36x$

5. Tunnellov teorem i drugi testovi

Prethodno je navedeno da postoji algoritam koji generira kongruentne brojeve, ali koristeći taj algoritam za dani broj se ne može reći koliko se dugo treba čekati da se utvrdi njegova kongruentnost, tj. ako nije utvrđeno, ne znamo znači li to da broj nije kongruentan ili nismo dovoljno dugo čekali. Sljedeći teorem daje efikasnije rješenje za ispitivanje kongruentnosti.

Teorem 5.1 (Tunnellov teorem)**.** *Neka je n kvadratno slobodan prirodan broj. Neka su*

$$\begin{aligned} f(n) &= \#\left\{(x,y,z) \in \mathbb{Z}^3 : x^2+2y^2+8z^2 = n\right\}, \\ g(n) &= \#\left\{(x,y,z) \in \mathbb{Z}^3 : x^2+2y^2+32z^2 = n\right\}, \\ h(n) &= \#\left\{(x,y,z) \in \mathbb{Z}^3 : x^2+4y^2+8z^2 = \frac{n}{2}\right\}, \\ k(n) &= \#\left\{(x,y,z) \in \mathbb{Z}^3 : x^2+4y^2+32z^2 = \frac{n}{2}\right\}. \end{aligned}$$

Za neparni n, ako je n kongruentan, onda je $f(n) = 2g(n)$. Za parni n, ako je n kongruentan, onda je $h(n) = 2k(n)$. Dodatno, ako vrijedi slabi oblik Birch-Swinnerton-Dyerove slutnje[1]*, onda vrijedi i obrat prethodne tvrdnje, tj. za neparni n iz $f(n) = 2g(n)$ slijedi da je n kongruentan, a za paran n iz $h(n) = 2k(n)$ slijedi da je n kongruentan.*

Dokaz. Vidi [12]. □

Tunnellov teorem daje gotovo potpuno rješenje problema pronalaska jednostavnog kriterija koji određuje je li dani prirodni broj n površina nekog racionalnog pravokutnog trokuta ili nije.

Primjer 5.1. *([4]) Budući da vrijedi $f(1) = g(1) = 2$ i $f(3) = g(3) = 4$ imamo $f(n) \neq 2g(n)$ za $n = 1$ i $n = 3$ pa Tunnellov teorem pokazuje da brojevi 1 i 3 nisu kongruentni.*

Primjer 5.2. *([4]) Budući da je $h(2) = k(2) = 2$, onda je $h(2) \neq 2k(2)$ pa po Tunnellovom teoremu broj 2 nije kongruentan.*

U nastavku navodimo još neke testove za provjeravanje kongruentnosti danog broja. Kao što ćemo vidjeti, važnu ulogu u većini rezultata imaju Legendreovi simboli.

Teorem 5.2. *Neka su p_k, q_k prosti brojevi kongruentni k modulo 8. Tada*

- p_3, $2p_5$, p_3q_3, $2p_5q_5$;
- $2p_1p_5$ *ako* $\left(\frac{p_1}{p_5}\right) = -1$;
- $p_3^{(1)}p_3^{(2)}\cdots p_3^{(t)}$ *ako* $\left(\frac{p_3^{(m)}}{p_3^{(n)}}\right) = -1$ *za* $m < n$

nisu kongruentni brojevi.

Dokaz. Vidi [10]. □

[1] Vidi [11].

Teorem 5.3. *Neka su p_k, q_k prosti brojevi kongruentni k modulo 8. Tada su*

- p_5, p_7, $2p_7$, $2p_3$;
- p_3p_5, p_3p_7, $2p_3p_5$, $2p_5p_7$;
- p_1p_5 *ako* $\left(\frac{p_1}{p_5}\right) = -1$;
- $2p_1p_3$ *ako* $\left(\frac{p_1}{p_3}\right) = -1$;
- p_1p_7, $2p_1p_7$ *ako* $\left(\frac{p_1}{p_7}\right) = -1$

konguentni brojevi.

Dokaz. Vidi [9]. □

Teorem 5.4. *Za svaki nenegativan $k \in \mathbb{Z}$, postoji beskonačno mnogo kvadratno slobodnih kongruentnih brojeva sa točno $k+1$ neparnih prostih djelitelja u svakoj klasi ostataka $5, 6, 7$ modulo 8.*

Dokaz. Vidi [9]. □

Novije rezultate vezane za ispitivanje kongruentnosti izreći ćemo idućim teoremima.

Teorem 5.5. *Neka su g, k, l pozitivni cijeli brojevi takvi da je $g \geq k > l$. Neka su $p_1, p_2, ..., p_g$ prosti brojevi kongruentni 3 modulo 8, takvi da za sve $i > j$, vrijedi*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ako je } (i,j) \neq (k,l), \\ -1, & \text{inače.} \end{cases}$$

Definiramo

$$\mathcal{N}_{k,l}^{neparan} := \{n = p_1p_2 \cdots p_g\},$$
$$\mathcal{N}_{k,l}^{paran} := \{n = 2p_1p_2 \cdots p_g | g \ \ je \ \ paran\}.$$

Ako $k - l$ nije djeljivo s 2, onda nijedan element unije $\mathcal{N}_{k,l}^{neparan} \cup \mathcal{N}_{k,l}^{paran}$ nije kongruentan broj.

Dokaz. Vidi [2]. □

Teorem 5.6. *Uz oznake iz Teorema 5.5, ako $k - l$ nije djeljivo s 2, onda nijedan element od $\mathcal{N}_{k,l}^{neparan}$ nije kongruentan.*

Dokaz. Vidi [2]. □

6. Poopćenje problema kongruentnih brojeva

U ovom poglavlju razmotrit ćemo generalizirani problem kongruentnih brojeva. Taj se problem svodi na pitanje može li neki prirodan broj n biti površina trokuta s racionalnim stranicama za dani kut θ.

6.1. t-kongruentni brojevi

Trokut kojemu su duljine stranica i površina racionalni brojevi nazivamo *Heronov* trokut. Heron je prije gotovo 2000 godina dokazao da se površina n trokuta sa stranicama a, b, c računa po formuli:

$$n^2 = s(s-a)(s-b)(s-c),$$

pri čemu je

$$s = \frac{a+b+c}{2}.$$

Primjer 6.1. *Trokut sa stranicama* $(13, 14, 15)$ *ima površinu* 84.

Veliki doprinos u proučavanju Heronovih trokuta dali su u sedamnaestom stoljeću F. Viete, C. G. Bachet i F. von Shooten. Oni su konstruirali Heronove trokute spajajući pravokutne trokute. Rasprava o problemima vezanim za Heronove trokute uspon je doživjela u devetnaestom stoljeću u Britaniji.
Prirodan broj n je površina Heronovog trokuta ako i samo ako postoje pozitivni brojevi $a, b, c \in \mathbb{Q}$ i broj θ, $0 < \theta < \pi$, takvi da vrijedi

$$a^2 = b^2 + c^2 - 2bc\cos\theta \quad \text{i} \quad 2n = bc\sin\theta. \tag{3}$$

Izraz dan formulama (3) povlači da je $(\cos\theta, \sin\theta)$ racionalna točka različita od točaka $(\pm 1, 0)$ na gornjoj polukružnici pa stoga postoji $t \in \mathbb{Q}$, $t > 0$, takav da je

$$\sin\theta = \frac{2t}{1+t^2} \quad \text{i} \quad \cos\theta = \frac{t^2-1}{t^2+1}.$$

Fiksirajmo sada racionalan broj $t > 0$.

Definicija 6.1. *Za cijeli broj n kažemo da je t-kongruentan ako postoje racionalni brojevi $a, b, c > 0$ takvi da vrijedi*

$$a^2 = b^2 + c^2 - 2bc\frac{t^2-1}{t^2+1} \quad i \quad 2n = bc\frac{2t}{1+t^2}.$$

Može se pokazati da vrijedi sljedeća tvrdnja o t-kongruentnim brojevima.

Teorem 6.1. *Svaki kvadratno slobodan prirodan broj n je t-kongruentan broj za neki $t \in \mathbb{Q}^+$.*

Dokaz. Vidi [11]. □

U slučaju kada je $t = 1$ imamo standardni problem kongruentnih brojeva.

6.2. θ-kongruentni brojevi

Pretpostavimo da postoji trokut s racionalnim stranicama i kutom θ. Tada je i $\cos\theta$ racionalan broj i zapišemo ga u obliku

$$\cos\theta = \frac{s}{r},$$

pri čemu su $r, s \in \mathbb{Z}, |s| \leq r, (r,s) = 1$. Primjetimo da je

$$\sin\theta = \frac{1}{r}\sqrt{r^2 - s^2}$$

te zbog toga sljedeća definicija ima smisla.

Definicija 6.2. *Neka je θ realan broj, $0 < \theta < \pi$ takav da je $\cos\theta = \frac{s}{r}$ pri čemu je $r, s \in \mathbb{Z}, |s| \leq r, (r,s) = 1$. Za prirodan broj n kažemo da je θ-kongruentan ako je $n\sqrt{r^2 - s^2}$ površina nekog trokuta s racionalnim stranicama i kutom θ.*

Uz iste oznake kao ranije, n je θ-kongruentan kada postoje pozitivni racionalni brojevi a, b, c takvi da je

$$c^2 = a^2 + b^2 - \frac{2abs}{r} \quad \text{i} \quad 2nr = ab.$$

Problem t-kongruentnih brojeva je specijalan slučaj problema θ-kongruentnih brojeva. Zapišimo $t = \frac{k}{l}$ za $l \geq k \geq 1$, $(k,l) = 1$. Uzmimo θ takav da je

$$\cos\theta = \frac{t^2 - 1}{t^2 + 1}, \quad 0 < \theta < \pi.$$

Tada je u novim oznakama:

$$\cos\theta = \frac{l^2 - k^2}{l^2 + k^2},$$

u slučaju ako je jedan od brojeva k, l paran, a

$$\cos\theta = \frac{\frac{l^2 - k^2}{2}}{\frac{l^2 + k^2}{2}},$$

u slučaju kada su oba broja k, l neparna. Iz toga slijedi da je n θ-kongruentan kada je kln t-kongruentan (kada su k, l neparni), odnosno $2kln$ je θ-kongruentan (kada je jedan od k, l paran). Posebno, standardni problem kongruentnih brojeva jednak je problemu θ-kongruentnih brojeva za $\theta = \frac{\pi}{2}$.

Literatura

[1] G. Brown, *The congruent number problem*,
http://www.graemebrownart.com/congruent.pdf

[2] W. Cheng, X. Guo, *Some new families of non-congruent numbers*, Journal of Number Theory **196** (2019), 291–305.
http://maths.nju.edu.cn/~guoxj/articles/JNT2018.pdf

[3] J. H. Coates, *Congruent Number Problem*, Pure and Applied Mathematics Quarterly **1** (2005), 14–27.

[4] K. Conrad, *The Congruent Number Problem*,
http://www.aimath.org/news/congruentnumbers/congruentnumbers.pdf

[5] A. Dujella, *Uvod u teoriju brojeva*, PMF - Matematički odjel, Sveučilište u Zagrebu (skripta)

[6] A. Dujella, M. Maretić, *Kriptografija*, Element, Zagreb, 2007.

[7] A. Jurasić, M. Rukavina, *Pseudoprosti brojevi*, Matematičko fizički list **62** (2011), 20–25.

[8] I. Matić, *Uvod u teoriju brojeva*, Osijek, 2014.

[9] P. Monsky, *Mock Heegner points and congruent numbers*, Mathematische Zeitschrift **204** (1990), 45–67.

[10] L. K. Reinholz, *Families of Congruent and Non-congruent Numbers*, The University of British Columbia, 2011.

[11] J. Top, N. Yui, *Congruent number problems and their variants*, Algorithmic Number Theory **44** (2008), 613-639.
https://www.math.leidenuniv.nl/~psh/ANTproc/19yui.pdf

[12] J. Tunnell, *A Classical Diophantine Problem and Modular Forms of Weight 3/2*, Invent. Math. **72** (1983), 323–334.

[13] Y. Yeo, *The Congruent Number Problem*,
https://www.math.upenn.edu/~yeya/pizza_2018-03-16.pdf